Configurations in Fractal Sets in Euclidean and Non-Archimedean Local Fields

by

Robert Fraser

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

The Faculty of Graduate and Postdoctoral Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

March 2018

Abstract

We discuss four different problems. The first, a joint work with Malabika Pramanik, concerns large subsets of $\mathbb{R}^n$ that do not contain various types of configurations. We show that a collection of v points satisfying a continuously differentiable v-variate equation in $\mathbb{R}$ can be avoided by a set of Hausdorff dimension $\frac{1}{v-1}$ and Minkowski dimension 1. The second problem concerns large subsets of vector spaces over non-archimedean local fields that do not contain configurations. Results analogous to the real-variable cases are obtained in this setting. The third problem is the construction of measure-zero Besicovitch-type sets in K^n for non-archimedean local fields K. This construction is based on a Euclidean construction of Wisewell and an earlier construction of Sawyer. The fourth problem, a joint work with Kyle Hambrook, is the construction of an explicit Salem set in $\mathbb{Q}_p$. This set is based on a Euclidean construction of Kaufman.

Lay Summary

How large can a set be if the set does not contain a certain pattern? This problem remains open in some important cases: for example, in the case where the pattern is an equilateral triangle and the space is three-dimensional. We obtain bounds on the answer for generic patterns.

Suppose that a set in the plane contains a line segment in every direction. How large must it be? Surprisingly, such sets can have zero area. We show that, in a different 2-dimensional space, such sets can also have area zero.

Can we construct a non-random set that does not correlate well with high-frequency waves? Such behaviour is typical of random sets, but constructing non-random examples is difficult. This question has been solved in 1 and 2 dimensions, but not in higher dimensions. We consider the 1-dimensional version of this question in a slightly different setting.

Preface

This thesis is based on four previous works, one of which has been published and the other three of which are submitted for publication in academic journals.

The material in Chapters 2 and 3 is based on the work “Large Sets Avoiding Patterns.” This is a joint work with Malabika Pramanik that has been accepted for publication in Analysis and PDE. I proved the building block lemma in the case where the gradient of the function was nonvanishing. I also devised the queueing procedure used in the construction of the set.

The material in Chapters 4 and 5 is based on the work “Large Subsets of Local Fields Not Containing Configurations.” This is a single-author work. I was responsible for all aspects of the project, starting from the formulation of the problem, developing the methodology, and the solution.

The material in Chapters 6 and 7 is based on the paper “Kakeya-type sets in local fields with finite residue field” appearing in Mathematika, Volume 62, Pages 614-629. I was responsible for all aspects of this project, including finding the problem, finding the relevant literature, and developing the construction appearing in this work.

The material in Chapters 8 and 9 is based on the work “Explicit Salem sets, Fourier restriction, and metric Diophantine approximation in the p-adic numbers.” This is a joint work with Kyle Hambrook. I established the exponential sum estimate used in the construction and proved the theorem in the one-dimensional case.

Table of Contents

Abstract . . . ii

Lay Summary . . . iii

Preface . . . iv

Table of Contents . . . v

Acknowledgements . . . viii

Dedication . . . ix

1 Introduction . . . 1
- 1.1 Sets Avoiding Configurations . . . 1
- 1.2 Sets Avoiding Configurations in Local Fields . . . 3
- 1.3 Besicovitch Sets . . . 6
- 1.4 Salem Sets . . . 7
- 1.5 Layout . . . 9

2 Dimensions of Sets . . . 10
- 2.1 Minkowski Dimension . . . 10
- 2.2 Hausdorff Dimension . . . 11
- 2.3 Frostman's Lemma . . . 13

3 Configurations . . . 16
- 3.1 Background . . . 16
  - 3.1.1 Two Constructions of Keleti . . . 16
  - 3.1.2 The Constructions of Maga and Máthé . . . 17
- 3.2 Discussion of Main Results . . . 19
  - 3.2.1 Nonsimultaneous Avoidance . . . 19
  - 3.2.2 Polygons and Polyhedra . . . 25
  - 3.2.3 Simultaneous Avoidance . . . 26
- 3.3 A Single Step . . . 27

3.3.1 One Dimension, Nonvanishing Gradient 28
3.3.2 One Dimension, General Case 33
3.3.3 Higher Dimensions 35
3.4 Construction of E 41
3.4.1 Construction 42
3.4.2 Nonexistence of Solutions 44
3.4.3 Hausdorff Dimension of E 45
3.4.4 Minkowski Dimension of E 47
3.5 Simultaneous Avoidance 47

4 Background on Local fields 54
4.1 Examples 54
4.2 Introduction 55
4.3 K-Valued Functions 57
4.4 Hensel's Lemma 58
4.5 The Height Function 60
4.5.1 Finite Characteristic Case 61
4.5.2 p-Adic Case 61
4.5.3 Negatives of Elements of Finite Height 62

5 Configurations II 63
5.1 Introduction 63
5.2 A Single Step 64
5.2.1 Polynomial, Nonsingular Case 64
5.2.2 One Dimension, Nonsingular Case 65
5.2.3 One Dimension, General Case 67
5.2.4 Multidimensional Case 69
5.3 Construction of E 71
5.3.1 General Procedure 71
5.3.2 Hausdorff Dimension of E 74
5.3.3 Minkowski Dimension of E 77
5.4 Simultaneous Avoidance 78

6 Besicovitch Sets 80
6.1 The Kakeya Problem 80
6.2 The Kakeya Problem for Finite Fields 81

7 Local Field Besicovitch Sets 83
7.1 Background 83
7.1.1 Previous Constructions 83

7.1.2 A Besicovitch Set in $\mathbb{F}_q[[t]]^2$ . . . 85
7.2 Adapting to Local Fields . . . 87
7.2.1 Construction of ϕ . . . 87
7.2.2 Estimates on the Range of $f(x, \phi(x))$ . . . 88
7.2.3 Kakeya-Like Sets . . . 92
7.2.4 Examples . . . 93
7.2.5 A Kakeya Needle Set . . . 95

8 Background on Salem Sets . . . 96
8.1 Fourier Dimension . . . 96
8.2 Fourier Analysis on Non-Archimedean Local Fields . . . 98
8.3 The Fourier Transform on Spaces Other than L^1 . . . 101
8.4 The Case $K = \mathbb{Q}_p$ . . . 102
8.5 Hausdorff and Minkowski Dimension . . . 104

9 An Explicit Salem Set . . . 106
9.1 Introduction . . . 106
9.2 A Salem Set in $\mathbb{Z}_p$ . . . 107
9.2.1 Setup . . . 107
9.2.2 Estimates on $\widehat{F}_M$ . . . 108
9.2.3 Estimates on $\widehat{\mu_k}$ . . . 110
9.3 Fourier Dimension of $W(m, n, \tau)$ . . . 111
9.3.1 Fourier Transform of $\phi_{q,r}$ . . . 113
9.3.2 Estimate on $\widehat{F_M}$ . . . 114
9.3.3 Concluding Remarks Regarding $W(m, n, \tau)$ . . . 116

10 Conclusion . . . 117
10.1 Configurations . . . 117
10.1.1 Squares of Differences . . . 117
10.1.2 Configurations and Fourier Dimension . . . 118
10.1.3 Local Fields . . . 119
10.2 Besicovitch Sets on Local Fields . . . 119
10.3 Salem Sets . . . 120

Bibliography . . . 122

Acknowledgements

I would like to thank my supervisory committee members Izabella Łaba and Jozsef Solymosi for their help and support.

I would like to thank all of my friends in the mathematics department for all of their encouragement.

I would like to extend a special thanks to Myrto Mavraki and Pam Sargent for their help with keeping me on track to finish my thesis.

I would like to thank my family for their emotional support throughout the process of writing this thesis.

I would like to thank my Master's supervisor and former Ph.D. co-supervisor Akos Magyar for everything he taught me as a Master's student and as a first-year Ph. D. student.

I would like to thank the senior students in UBC's harmonic analysis group for welcoming me into the department.

I would like to thank my friend and collaborator, Kyle Hambrook, for all of his contributions to our joint project.

Most of all, I would like to thank my supervisor, Malabika Pramanik, for all of the advice and support she provided. Without her, none of the work in this thesis would have been possible.

Dedication

To my friends and family

Chapter 1

Introduction

We start with an overview of the main results of this thesis.

1.1 Sets Avoiding Configurations

In a joint work with Pramanik, [19], we consider questions of the following form: given a collection of patterns, how large can a set E be if it does not contain any v distinct points in any of those patterns? To answer this question, we need a notion of the size of Lebesgue-null subsets of $\mathbb{R}^n$, which will be discussed in Chapter 2.

This question was motivated by results of Keleti [28] [29], Maga [33], and Máthé [34]. For example, given a linear three-point configuration in one dimension [29] (resp. 2 dimensions [33]), there is a subset of $\mathbb{R}$ (resp. $\mathbb{R}^2$) of Hausdorff dimension 1 (resp. 2) that does not contain any similar copy of the three-point configuration. As another example, given an angle θ, Máthé constructs a set of Hausdorff dimension $\frac{n}{8}$ (or $\frac{n}{4}$ if $\cos^2(\theta)$ happens to be rational) that does not contain 3 points that form an angle θ.

We prove a result that applies for a broader class of configurations. We define a configuration to be the locus of points $x_1, \ldots, x_v$ in $\mathbb{R}^n$ such that $f(x_1, \ldots, x_v) = 0$ for some function $f : \mathbb{R}^{nv} \to \mathbb{R}^m$. We consider functions satisfying certain smoothness and nondegeneracy conditions. We primarily concern ourselves with the case $m = 1$ but also prove a weaker result for $m > 1$. In the $m = 1$ case, we have the following theorem.

Theorem 1.1.1 (Theorem 1.1 from [19])**.** *For any $\eta > 0$ and integer $v \geq 3$, let $f_q : \mathbb{R}^v \to \mathbb{R}$ be a countable family of functions in v variables with the following properties:*

(a) There exists $r_q \geq 1$ such that $f_q \in C^{r_q}([0, \eta]^v)$,

(b) For each q, some partial derivative of f_q of order $r_q \geq 1$ does not vanish at any point of $[0, \eta]^v$.

Then there exists a set $E \subseteq [0,\eta]$ of Hausdorff dimension at least $\frac{1}{v-1}$ and Minkowski dimension 1 such that $f_q(x_1,\dots,x_v)$ is not equal to zero for any v-tuple of distinct points $x_1,\dots,x_v \in E$ and any function f_q.

This theorem can be used to locate large sets that simultaneously avoid a countable collection of sufficiently smooth configurations.

Of special note is that there is no need to assume that f_q has a nonvanishing partial first derivative: all that is needed is that each f_q has some nonvanishing partial derivative of some order on $[0,\eta]^v$.

Notice that, if the sequence $\{f_q\}$ consists of a single function f, the conditions of Theorem 1.1.1 will always hold provided that f is analytic on some interval $[0,\eta]$ and not identically zero. This gives a wide range of functions for which this theorem is applicable.

One application of Theorem 1.1.1 that will be further discussed in Chapter 3 involves subsets of a curve that avoid isosceles triangles. It is shown that, regardless of the ambient dimension, any smooth curve in $\mathbb{R}^d$ contains a subset of Hausdorff dimension $\frac{1}{2}$ that does not contain the vertices of any isosceles triangle.

For functions $f : \mathbb{R}^{nv} \to \mathbb{R}^m$ with $m > 1$, we have the following weaker theorem that requires a non-degeneracy condition on the first derivative.

Theorem 1.1.2 (Theorem 1.2 from [19]). *Fix $\eta > 0$ and positive integers m, n, v such that $v \geq 3$, and $m \leq n(v-1)$. Let $f_q : \mathbb{R}^{nv} \to \mathbb{R}^m$ be a countable family of C^2 functions with the following property: for every q, the derivative $Df_q(x_1,\cdots,x_v)$ has full rank on $[0,\eta]^{nv}$ at every point $(x_1,\cdots,x_v)$ in the zero set of f_q such that $x_r \neq x_s$ for all $r \neq s$.*

Then there exists a set $E \subseteq [0,\eta]^n$ of Hausdorff dimension at least $\frac{m}{v-1}$ and Minkowski dimension n such that $f_q(x_1,\dots,x_v)$ is not equal to zero for any v-tuple of distinct points $x_1,\dots,x_v \in E^n$ and any function f_q.

This result can be used for certain geometric constructions that will be further detailed in Chapter 3.

We also construct a set that does not contain any configurations with a specified linearization.

Theorem 1.1.3 (Theorem 1.3 from [19]). *Given any constant $K > 0$ and a vector $\alpha \in \mathbb{R}^v$ such that*

$$\alpha \cdot u \neq 0 \text{ for every } u \in \{0,1\}^v \text{ with } u \neq 0, u \neq (1,1,\dots,1) \tag{1.1}$$

and such that

$$\sum_{j=1}^{v} \alpha_j = 0, \tag{1.2}$$

there exists a positive constant $c(\alpha)$ *and a set* $E = E(K, \alpha) \subseteq [0, 1]$ *of Hausdorff dimension* $c(\alpha) > 0$ *with the following property.*

The set E *does not contain any nontrivial solution of the equation*

$$f(x_1, \cdots, x_v) = 0, \qquad x_1, \cdots, x_v \text{ not all identical},$$

for any C^2 *function* f *of the form*

$$f(x_1, \cdots, x_v) = \sum_{j=1}^{v} \alpha_j x_j + G(x_1, \cdots, x_v) \tag{1.3}$$

$$\text{where } |G(x)| \leq K \sum_{j=2}^{v} (x_j - x_1)^2. \tag{1.4}$$

This theorem is useful for simultaneously avoiding related configurations of a given type. For example, this theorem is used to construct a subset $E \subset \mathbb{R}$, such that, for any sufficiently smooth injective mapping with bounded second derivative from $\mathbb{R}$ to $\mathbb{R}^n$, E maps to a set of points that does not contain the vertices of an isosceles triangle.

1.2 Sets Avoiding Configurations in Local Fields

We are also interested in non-archimedean local fields, such as the p-adic numbers $\mathbb{Q}_p$, as a model for the Euclidean setting. The field $\mathbb{Q}_p$ consists of numbers of the form

$$\sum_{j=M}^{\infty} d_j p^j$$

where $d_j \in \{0, 1, \ldots, p-1\}$ and M is an integer. If the sum has only finitely many nonzero terms, then this sum lies in $\mathbb{Q}$. An absolute value is defined on this field in the following way: if d is a p-adic number such that M satisfies $d_M \neq 0$ and $d_j = 0$ for all $j < M$, then $|d| = p^{-M}$. With respect to this norm, $\mathbb{Q}_p$ is a locally compact abelian group. More details about $\mathbb{Q}_p$ and other non-archimedean local fields will be given in Chapter 4.

The ring of integers of $\mathbb{Q}_p$ is known as the ring $\mathbb{Z}_p$ of p-adic integers, and consists of sums of the form

$$\sum_{j=0}^{\infty} d_j p^j.$$

We will also concern ourselves with the local field $\mathbb{F}_q((t))$, consisting of formal Laurent series with coefficients in the finite field $\mathbb{F}_q$, and $\mathbb{F}_q[[t]]$, the ring of formal power series with coefficients in $\mathbb{F}_q$.

The main results from [34] and from [19] apply to the non-archimedean local fields $\mathbb{Q}_p$ and $\mathbb{F}_q((t))$ [18]. Here is the adaptation of Máthé's theorem.

Theorem 1.2.1 (Theorem 1.1 from [18])**.** *Let $\{f_\ell\} : R^{nv_\ell} \to R$ be a countable family of nonzero polynomials of degree at most d with integer coefficients, where $R = \mathbb{Z}_p$ or $\mathbb{F}_q[[t]]$. Then there exists a set $E \subset R^n$ of Hausdorff dimension $\frac{n}{d}$ and Minkowski dimension n such that, for all ℓ, the set E does not contain v_ℓ distinct points $x_1, \ldots, x_{v_\ell}$ such that $f_\ell(x_1, \ldots, x_{v_\ell}) = 0$.*

One important application of this result is the case where $f(x_1, x_2, x_3) = x_1 - 2x_2 + x_3$. This function is equal to zero whenever x_1, x_2, and x_3 lie in arithmetic progression. Thus Theorem 1.2.1 gives a subset of K of Hausdorff dimension 1 that does not contain 3-term arithmetic progressions for $K = \mathbb{Q}_p$ or $\mathbb{F}_q((t))$.

We also establish analogues of Theorems 1.1.1, 1.1.2, and 1.1.3 in non-archimedean local fields. However, a stronger assumption than continuous differentiability is needed here because the mean value theorem does not apply to local fields. The notion of **strict differentiability** will be discussed in Chapter 4.

Theorem 1.2.2 (Theorem 1.2 from [18])**.** *Let $K = \mathbb{Q}_p$ and $R = \mathbb{Z}_p$, or let $K = \mathbb{F}_q((t))$ and $R = \mathbb{F}_q[[t]]$. For any ball $B \subset R$ and integer $v \geq 3$, let $f_\ell : R \to K$ be a countable family of functions in v variables with the following properties:*

(a) There exists $r_\ell < \infty$ such that f_ℓ is r_ℓ times strictly differentiable.

(b) For each ℓ, some partial derivative of f_ℓ of order $r_\ell \geq 1$ does not vanish at any point of B^v.

Then there exists a set $E \subseteq B$ of Hausdorff dimension at least $\frac{1}{v-1}$ and Minkowski dimension 1 such that $f_\ell(x_1, \ldots, x_v)$ is not equal to zero for any v-tuple of distinct points $x_1, \ldots, x_v \in E$ and any function f_ℓ.

This theorem does not have the same consequences regarding, say, isosceles triangles for non-archimedean local fields as Theorem 1.1.1 does for the real numbers. This is because, for a fixed x and for y not close to x, the distance function $d(x, y)$ on K^n is a locally constant function of y, so the partial derivative condition does not hold. Nonetheless, many important functions on local fields, such as the exponential function, are defined by power series and thus Theorem 1.2.2 applies to them.

Theorem 1.2.3 (Theorem 1.3 from [18]). *Let $K = \mathbb{Q}_p$ and $R = \mathbb{Z}_p$, or let $K = \mathbb{F}_q((t))$ and $R = \mathbb{F}_q[[t]]$. Fix a ball $B \subset R$ and positive integers m, n, v such that $v \geq 3$, and $m \leq n(v-1)$. Let $f_\ell : (R^n)^v \to K^m$ be a countable family of twice strictly differentiable functions with the following property: the first derivative Df_ℓ has full rank on the portion of the zero set of f_ℓ contained in B^{nv} for every ℓ.*

Then there exists a set $E \subseteq B^n$ of Hausdorff dimension at least $\frac{m}{v-1}$ and Minkowski dimension n such that $f_\ell(x_1, \ldots, x_v)$ is not equal to zero for any v-tuple of distinct points $x_1, \ldots, x_v \in E^n$ and any function f_ℓ.

Again, caution is required when considering functions involving distance: unlike the Euclidean case, the distance function does not satisfy the requirements of this theorem.

Theorem 1.2.4 (Theorem 1.4 from [18]). *Let $K = \mathbb{Q}_p$ and $R = \mathbb{Z}_p$, or let $K = \mathbb{F}_q((t))$ and $R = \mathbb{F}_q[[t]]$. Given any constant $C > 0$ and a vector $\alpha \in K^v$ such that*

$$\alpha \cdot u \neq 0 \text{ for every } u \in \{0,1\}^v \text{ with } u \neq 0, u \neq (1,1,\ldots,1) \tag{1.5}$$

and such that

$$\sum_{j=1}^{v} \alpha_j = 0, \tag{1.6}$$

there exists a positive constant $c(\alpha, K)$ and a set $E = E(C, \alpha, K) \subseteq R$ of Hausdorff dimension $c(K, \alpha) > 0$ with the following property.

The set E does not contain any nontrivial solution of the equation

$$f(x_1, \cdots, x_v) = 0, \qquad x_1, \cdots, x_v \text{ not all identical,}$$

for any twice strictly differentiable function f of the form

$$f(x_1, \cdots, x_v) = \sum_{j=1}^{v} \alpha_j x_j + G(x_1, \cdots, x_v) \tag{1.7}$$

$$\text{where } |G(x)| \leq C \sum_{j=2}^{v} |x_j - x_1|^2. \tag{1.8}$$

Here, the absolute value on K is chosen so that a uniformizing element t satisfies $|t| = q$, where q is the number of elements of $\mathbb{F}_q$ in the case of $\mathbb{F}_q((t))$ or $q = p$ in the case of $\mathbb{Q}_p$.

This theorem, once again, can be used to find large sets that avoid configurations that are "close" to 3-term arithmetic progressions. However, unlike the Euclidean case, this will not map to a set that is free of isosceles triangles under a strictly smooth function γ. However, it will map to a set that is free of triples $(x_j, y_j) \in K^2 : j = 1, 2, 3$ such that, for example, $\exp(y_3 - y_2) + \exp(x_3 - x_2) = \exp(y_2 - y_1) + \exp(x_2 - x_1)$. To see this, consider three points t_1, t_2, t_3: under the map $\gamma(t) = (x(t), y(t))$, we want to avoid solutions to

$$\exp(y(t_3) - y(t_2)) + \exp(x(t_3) - x(t_2)) = \exp(y(t_2) - y(t_1)) + \exp(x(t_2) - x(t_1)).$$

Near the diagonal (t, t, t) the linearization of this equation is

$$y'(t)(t_3 - t_2) + x'(t)(t_3 - t_2) = y'(t)(t_2 - t_1)x'(t)(t_2 - t_1)$$

This simplifies to

$$(x'(t) + y'(t))(t_3 - 2t_2 + t_1) = 0$$

so, regardless of the function $(x(t), y(t))$, so long as $x'(t) + y'(t)$ does not vanish, the linearization is $t_3 - 2t_2 + t_1$ and therefore Theorem 1.2.3 applies provided that $x'(t) + y'(t)$ remains bounded and that $x''(t)$ and $y''(t)$ remain bounded.

1.3 Besicovitch Sets

A Besicovitch set in $\mathbb{R}^n$ is a set that contains a line segment of length 1 in every direction. Besicovitch [3] constructed the first example of Besicovitch sets in $\mathbb{R}^n, n \geq 2$ with Lebesgue measure zero. A brief introduction to the theory of Besicovitch sets in $\mathbb{R}^n$ is presented in Chapter 6.

Let K be a non-archimedean local field. In contrast to the $\mathbb{R}^n$ definition, a subset E of K^n is called a **Besicovitch Set** if it contains a line in every direction; that is, for every vector $v \in K^n$, there is a point $x \in K^n$ such that the line

$$\ell = \{x + tv : t \in K\}$$

is contained in E. Note that t ranges over all of K and not just a subset.

Although Besicovitch sets in K^n had been previously constructed by Wright, the construction was unavailable in the literature. In [20], a construction of a measure-zero Besicovitch set is presented. In the process of constructing this set, the following result is established.

Theorem 1.3.1 (Wisewell function for non-archimedean local fields, [20, Theorem 1.1])**.** *Let $R = \mathbb{Z}_\ell$ or $R = \mathbb{F}_\ell[[t]]$. Let K be the field of fractions of R (i.e., $K = \mathbb{Q}_\ell$ or $\mathbb{F}_\ell((t))$). There is a continuous function $\phi : K^p \to K^q$ with the following property. Let $f(x, y) : K^p \times K^q \to K^{n-d}$ where $p \leq n - d \leq q$ be a measurable function that is very strongly differentiable in the x and y variables on every compact subset of $K^p \times K^q$, and such that the Jacobian $\partial f/\partial y$ has full rank a.e. in x and y with respect to the Haar measure on $K^p \times K^q$. Then the set*

$$\{f(x, \phi(x)) : x \in K^p\}$$

has measure zero with respect to the Haar measure on K^{n-d}.

This is an equivalent of a result of Wisewell [52] for the non-archimedean local fields $\mathbb{Q}_\ell$ and $\mathbb{F}_\ell((t))$.

Theorem 1.3.1 requires that R is a complete discrete valuation ring, which was erroneously omitted from the assumptions in [20]. One distinctive feature here is that the function described in Theorem 1.3.1 is *continuous*, which contrasts with the real-variable case.

Theorem 1.3.1 allows for the construction of Besicovitch sets of measure zero. In fact, it allows for the construction of sets containing a smoothly-parameterized family of smooth surfaces, provided that the family of surfaces satisfies appropriate dimensionality conditions.

Theorem 1.3.2 (Wisewell Set for Non-Archimedean Local Fields, [20, Theorem 1.2])**.** *Let K be either $\mathbb{Q}_p$ or $\mathbb{F}_q((t))$, and let $f(x, y, w) : K^p \times K^q \times K^d \to K^{n-d}$ be a measurable function such that $f(\cdot, \cdot, w)$ satisfies the same differentiability properties in the x and y variables as in Theorem 1.3.1. Then the set*

$$T := \{(w, z) : z = f(x, \phi(x), w); x \in K^p, w \in K^d\}$$

has measure zero with respect to the Haar measure on K^n.

The proof of this theorem, as well as some applications, is given in Chapter 7.

1.4 Salem Sets

The Fourier dimension of a set $E \subset \mathbb{R}^n$ relates to the decay of the Fourier transform of measures supported on E. A set that is additively random or curved will have large Fourier dimension. If the Hausdorff dimension of E is equal to its Fourier dimension, E is called a **Salem set**. Salem sets and Fourier dimension on $\mathbb{R}^n$ and on K^n will be discussed in more detail in Chapter 8.

Most known examples of Salem sets in $\mathbb{R}^n$ of non-integer dimension are constructed through random constructions. The first such construction was due to Salem [44]. Kaufman [27] gave an explicit example of a Salem set in $\mathbb{R}$. Kaufman's example consists of well-approximable numbers and is discussed in more detail in Chapter 8. A detailed exposition of Kaufman's result was authored by Bluhm [4].

The study of Salem sets over non-archimedean local fields was initiated by Papadimitropoulos. Papadimitropoulos adapted Salem's construction in order to locate Salem sets in $\mathbb{Q}_p$ [40], and later over every non-archimedean local field [39].

In a joint work with Hambrook, we identify an explicit Salem set in the local field $\mathbb{Q}_p$ and its ring of integers $\mathbb{Z}_p$. Our set is given by

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

Theorem 1.4.1 (Theorem 1.4.1 from [21]). *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*

$$|\widehat{\mu}(\xi)| \lesssim |\xi|_p^{-1/\tau} \log^3(1 + |\xi|_p) \quad \forall \xi \in \mathbb{Q}_p, \xi \neq 0$$

We also obtain a Fourier dimension bound on a related set $W(m, n, \tau)$ in $\mathbb{Z}_p^{m \cdot n}$ defined by

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

The Fourier dimension bound obtained on this set is not sufficient to show that $W(m, n, \tau)$ is a Salem set.

Theorem 1.4.2. *For every $\tau > (m + n)/m$, there exists a Borel probability measure μ supported on $W(m, n, \tau)$ such that*

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

Background on Fourier analysis on non-archimedean local fields will be given in Chapter 8, and the proofs of Theorems 1.4.1 and 1.4.2 will be given in Chapter 9.

1.5 Layout

Chapter 2 introduces the concepts of Hausdorff dimension and Minkowski dimension, which will be used throughout the thesis. Frostman's lemma, which is used in several later chapters, is introduced here. All of the background necessary for Chapter 3 is presented in Chapter 2.

Chapter 3 concerns the proof of Theorems 1.1.1, 1.1.2, and 1.1.3. Some examples of these theorems are discussed.

Chapter 4 discusses local fields, with a particular focus on the p-adic numbers $\mathbb{Q}_p$ and the function field $\mathbb{F}_q((t))$. The material in this chapter is used in all subsequent chapters.

Chapter 5 contains the proof of Theorems 1.2.1, 1.2.2, 1.2.3, and 1.2.4. Some differences between these Theorems and their Euclidean counterparts are discussed.

Chapter 6 discusses the theory of Besicovitch sets in both the Euclidean and Local Field settings. This material sets the stage for Chapter 7.

Chapter 7 discusses the proof of Theorems 1.3.1 and 1.3.2. Some specific examples of these theorems are also presented.

Chapter 8 concerns Salem sets as well as p-adic Fourier analysis. A description of the characters on $\mathbb{Q}_p$ is presented as well as some basic theorems of Fourier analysis on $\mathbb{Q}_p$.

Chapter 9 contains the proof of Theorems 1.4.1 and 1.4.2. The chapter concludes with a brief discussion of the gap between the Hausdorff dimension of $W(m, n, \tau)$ and the Fourier dimension computed in Theorem 1.4.2.

Chapter 2

Dimensions of Sets

2.1 Minkowski Dimension

In the context of fractal sets, it is useful to have a notion of dimension that allows for non-integer dimensions. One notion of dimension that plays an important role in geometric measure theory is Minkowski (or box-counting) dimension.

Let $E \subset \mathbb{R}^n$ be compact. Consider covers of E by balls of radius r. If E is, for example, a line segment of length ℓ, then E can always be covered by $\ell r^{-1} + O(1)$ balls of radius r. If E is a square of side length ℓ, then E can be covered by $\ell^2 r^{-2} + O(1)$ balls of radius r. The main feature here is that the exponent on r is -1 in the case of a line segment (which should have dimension 1), and the exponent on r is -2 in the case of a square (which should have dimension 2).

This motivates a definition for the Minkowski dimension of a set E:

Definition 2.1.1 (Definition of Minkowski Dimension)**.** *Let $E \subset \Omega \subset \mathbb{R}^n$ where $\Omega \subset \mathbb{R}^n$ is compact, and E is a Borel set. Let $C_r(E)$ be the minimal number of balls of radius r in $\mathbb{R}^n$ required to cover E. Then we define the upper Minkowski dimension of E by*

$$\overline{dim_M} E = \limsup_{r \to 0} \frac{-\log C_r(E)}{\log r}$$

and the lower Minkowski dimension of E by

$$\underline{dim_M} E = \liminf_{r \to 0} \frac{-\log C_r(E)}{\log r}.$$

If these two dimensions are the same, we call this quantity the ***Minkowski dimension*** *of E [35, Section 5.3].*

The upper and lower Minkowski dimension measure the size of the set E at different scales r. A set with large upper Minkowski dimension appears large at some sequence of scales r approaching zero; a set with large lower Minkowski dimension appears large at *all* sufficiently small scales.

The Minkowski dimension can often behave unpredictably. For example, the Minkowski dimension is not countably stable. A standard example of this is the family of points $\{1/n : n \in \mathbb{N}\} \cup \{0\}$. Each singleton $\{1/n\}$ has Minkowski dimension 0 (since it can always be covered by a single ball of arbitrarily small radius), so we would expect that this set $\{1/n : n \in \mathbb{N}\} \cup \{0\}$ should also have Minkowski dimension 0. However:

Example 2.1.2 (Countable set with positive Minkowski dimension)**.** *The set of points*

$$E := \{1/n : n \in \mathbb{N}\} \cup \{0\}$$

has Minkowski dimension $\frac{1}{2}$*.*

Proof. Consider coverings of E by balls of radius $r := t^{-2}$ for some $t \in \mathbb{R}$. For any $k > t$, we have

$$\frac{1}{k} - \frac{1}{k+1} = \frac{1}{k^2 + k} \leq \frac{1}{k^2} \leq t^{-2}.$$

Therefore, E contains a point in each t^{-2} neighbourhood of any $x \in [0, t^{-1}]$. It follows that at least $t/3$ balls are necessary to cover all of E, and since $t = r^{-1/2}$ we have that the lower Minkowski dimension of E is at least $\frac{1}{2}$.

Conversely, let $t \in \mathbb{R}$. Then the number of k such that $\frac{1}{k} > t^{-1}$ is at most t. Therefore, the set $[t^{-1}, 1] \cap E$ can be covered by at most t balls of radius t^{-2}. Using the fact that $[0, t^{-1}]$ can be covered by t balls of radius t^{-2}, we conclude that E can be covered by at most t balls of radius t^{-2}, which shows that the upper Minkowski dimension of E is at most 1/2. □

This example shows that a countable compact set can have positive Minkowski dimension. The bizarre behaviour exhibited by this example occurred because the balls were required to have the same radius. If we instead allow for coverings by balls of different radii, we arrive at a notion of dimension that is compatible with countable unions.

2.2 Hausdorff Dimension

Definition 2.2.1 (Definition of Hausdorff Dimension)**.** *Let* $E \subset \Omega \subset \mathbb{R}^n$ *where* Ω *is compact and* E *is a Borel set. We define the quantities* $H_r^s(E)$ *by*

$$\inf_{\mathcal{U}} \sum_{U \in \mathcal{U}} diam(U)^s$$

where the infimum is taken over collections $\mathcal{U}$ *of balls of diameter at most* r *that cover* E*. Evidently the infimum will increase as* r *decreases since the* *infimum is taken over a smaller set of coverings. Define the* s***-dimensional Hausdorff measure*** *of* E *by:*

$$H^s(E) := \lim_{r\to 0} H^s_r(E).$$

The expressions H^s *are Borel measures [35, Theorem 4.5]. There exists a unique* s_0 *such that* $H^s_r(E) = \infty$ *for* $s < s_0$ *and* $H^s_r(E) = 0$ *for* $s > s_0$ *[35, Theorem 4.7]. This exponent* s_0 *is called the* ***Hausdorff dimension*** *of* E *[35, Definition 4.8].*

We will now show that the countable set in Example 2.1.2 has Hausdorff dimension zero.

Example 2.2.2 (Computation of Hausdorff dimension for a countable set)**.** *The set of points*

$$E := \{1/n : n \in \mathbb{N}\} \cup \{0\}$$

has Hausdorff dimension 0*.*

Proof. Let $s, r > 0$ and let $0 < \epsilon < \frac{r}{2}$. We will define the covering $\mathcal{U}_{s,\epsilon}$ in the following way: Place a ball of diameter $\epsilon n^{-2/s}$ centered at each point $\frac{1}{n}$, and a ball of diameter ϵ centered at 0. Clearly $\mathcal{U}$ covers E, each ball of $\mathcal{U}$ has radius at most $2\epsilon < r$, and we have that

$$\sum_{u\in\mathcal{U}_{s,\epsilon}} \mathrm{diam}(U)^s = \epsilon^s + \epsilon^s \sum_{n=1}^{\infty} n^{-2} = (1+\pi^2/6)\epsilon^s$$

This quantity approaches 0 as $\epsilon \to 0$. Therefore $H^s_r(E) = 0$ for every $r, s > 0$ and $H^s(E) = 0$ for every $s > 0$. This establishes that the Hausdorff dimension of E is 0. □

In fact, the proof given in Example 2.2.2 can be modified to show that the Hausdorff dimension of *any* countable set is zero. This example illustrates how Definition 2.2.1 is useful when obtaining upper bounds for the Hausdorff dimension of a Borel set E: all that needs to be done is to show that there exist coverings $\mathcal{U}_j$ of E such that $\sum_{U\in\mathcal{U}_j} \mathrm{diam}(U)^s \to 0$. On the other hand, using this definition to obtain lower bounds on the Hausdorff dimension of a Borel set E can be more involved: in order to obtain lower bounds, it is necessary to consider all coverings of E by balls of radius at most r, and consider the behaviour as $r \to 0$.

2.3 Frostman's Lemma

It is usually better to refer to Frostman's lemma [22] when computing lower bounds for the Hausdorff dimension of a set. Frostman's lemma relates the Hausdorff dimension of a Borel set E to the behaviour of Borel measures supported on E. We present the version of Frostman's lemma appearing in Wolff's lecture notes [55, Proposition 8.2].

Theorem 2.3.1 (Frostman's Lemma)**.** *Let E be a Borel set in $\mathbb{R}^n$. Then the Hausdorff dimension of E is the supremum of the values of t such that E supports a Borel probability measure μ with the property that, for all balls $B \subset \mathbb{R}^n$,*

$$\mu(B) \lesssim_{t,\mu} diam(B)^t.$$

Since μ is a probability measure, the ball condition from Theorem 2.3.1 is automatically satisfied for large balls B, and this characterization only depends on the small-scale behaviour of the measure μ.

Example 2.3.2 (The Cantor middle-thirds set has Hausdorff dimension $\frac{\log 2}{\log 3}$)**.** *We will define a sequence E_j of nested sets in the following way. The set $E_0 = [0, 1]$. For $j > 0$, E_j will be obtained from E_{j-1} by deleting the (open) middle third of each interval in E_{j-1}. Thus*

$$\begin{aligned} E_1 &= [0, 1] \setminus (1/3, 2/3) \\ &= [0, 1/3] \cup [2/3, 1], \end{aligned}$$

and

$$\begin{aligned} E_2 &= ([0, 1/3] \setminus (1/9, 2/9)) \cup ([2/3, 1] \setminus (7/9, 8/9)) \\ &= [0, 1/9] \cup [2/9, 1/3] \cup [2/3, 7/9] \cup [8/9, 1]. \end{aligned}$$

The intervals that constitute E_j are called the jth stage basic intervals of E. We define $E = \bigcap_{j=1}^{\infty} E_j$. Then the set E has Hausdorff dimension $\log 2/\log 3$.

Proof. To see that E has Hausdorff dimension at most $\log 2/\log 3$, consider the sequence of coverings $\mathcal{U}_{j,\epsilon}$ of E obtained by extending the basic intervals of E by ϵ. We extend by ϵ because the balls in our covering are technically required to be open. This gives a family of 2^j balls of radius $3^{-j} + \epsilon$. Therefore, we have that $H_1^s(E) \leq 2^j(3^{-j} + \epsilon)^s \leq C_s 2^j 3^{-js} + 2^j \epsilon^s$. If we have $s > \log 2/\log 3$, then this quantity goes to zero as $\epsilon \to 0$ and $j \to \infty$, so $H_1^s(E) = 0$ and thus $H^s(E) = 0$.

To see that E has Hausdorff dimension at least $\log 2/\log 3$, we will define a measure μ on E satisfying the condition in Theorem 2.3.1. To do this, we define the measures $d\mu_j(x) = \frac{\mathbf{1}_{E_j}}{|E_j|}dx$ to be the uniformly distributed probability measure on E_j. The measure μ will be taken to be the weak limit of these measures. We have that $\mu_k(F) = \mu_j(F) = 2^{-j}$ for any j-th level basic interval F. Each such interval has Lebesgue measure 3^{-j}, and a simple geometric argument shows that no intervals of length 3^{-j} can be assigned a μ_k-measure larger than 2^{-j} for any $k \geq j$. It remains to show the ball condition for intervals of length between 3^{-j-1} and 3^{-j}. Of course, such intervals can only intersect at most 3 of the $j+1$-stage basic intervals occurring in the construction of E, and therefore will be assigned a μ-measure of no more than $3 \times 2^{-j-1}$. In any case we get a bound of $C2^{-j}$ on the μ_k measures of any such interval for $k \geq j$. Passing to the weak limit gives that the same holds for μ and therefore that E has Hausdorff dimension $\frac{\log 2}{\log 3}$. □

This example illustrates the power of Frostman's lemma: by placing a natural measure on the set E, we manage to obtain an optimal lower bound on the Hausdorff dimension of E.

Frostman's lemma has a formulation in terms of energy integrals from Mattila's textbook [36, Section 2.5].

Definition 2.3.3 (Definition of s-energy of a measure)**.** *Let μ be a Borel Measure. Then the s-energy $I_s(\mu)$ is defined by the integral*

$$I_s(\mu) = \iint_{x,y} |x-y|^{-s} d\mu(x) d\mu(y).$$

We are interested in when the energy integral $I_s(\mu)$ is finite. Notice that the singularity becomes more severe the larger s is. The following theorem restates Frostman's lemma in terms of energy integrals [36, Theorem 2.8].

Theorem 2.3.4 (Energy integral formulation of Frostman's lemma)**.** *If $E \subset \Omega \subset \mathbb{R}^n$ is a Borel set, where Ω is compact, then the Hausdorff dimension of E is the supremum value of t such that there exists a measure μ_t supported on E such that $I_t(\mu_t) < \infty$.*

There is a Fourier-analytic expression for the energy integral $I_s(\mu)$ [36, Theorem 3.10].

Theorem 2.3.5 (Fourier-analytic expression for energy integrals)**.** *Let μ be a compactly supported Borel probability measure. Then*

$$I_s(\mu) = C(n,s) \int |\widehat{\mu}(\xi)|^2 |\xi|^{s-n}\, d\xi$$

for some constant $C(n,s)$ depending only on n and s.

Combining Theorem 2.3.5 and Theorem 2.3.4 gives a Fourier-analytic version of Frostman's lemma:

Corollary 2.3.6 (Fourier-analytic version of Frostman's lemma)**.** *Let $E \subset \Omega \subset \mathbb{R}^n$ be a Borel set, where Ω is compact. Then the Hausdorff dimension of E is the supremum value of t such that there exists a measure μ_t supported on E such that*

$$\left(\frac{1}{|B(0,r)|}\int_{B(0,r)} |\widehat{\mu}_t(\xi)|^2 d\xi\right)^{1/2} \lesssim_{\mu_t,t} (1+|\xi|)^{-t/2}.$$

The left-hand side of this expression is an L^2-average of $\widehat{\mu}$ over the ball of radius r centered at 0.

Chapter 3

Configurations

3.1 Background

3.1.1 Two Constructions of Keleti

In 1998, Keleti [28] constructed a set E of Hausdorff dimension 1 such that E does not contain 4 points x_1, x_2, x_3, x_4 such that

$$x_2 - x_1 = x_4 - x_3$$

for any $x_1 < x_2 \leq x_3 < x_4 \in E$. Keleti later modified this construction in 2008 [29].

Theorem 3.1.1. *[Keleti's construction of a set avoiding countably many linear configurations] Let $\{\alpha_j\}$ be a countable collection of real numbers strictly greater than 1. Then there exists a set $E \subset \mathbb{R}$ of Hausdorff dimension 1 such that the equation*

$$x_3 - x_1 = \alpha_j(x_2 - x_1) \tag{3.1}$$

does not have any solutions for distinct $x_1, x_2, x_3 \in E$.

Keleti constructs the set E using a Cantor-like construction that is summarized here. The construction begins with the set $E_0 = [0, 1]$, and continues in the following way. Given a set E_k, which is a union of $m_1 \cdots m_k$ intervals of length δ_k. m_k and δ_k are chosen appropriately in order to guarantee that the set E has Hausdorff dimension 1.

Given E_k, Keleti effectively constructs a list of triples of intervals

$$\Gamma'_k := \{(I^k_a, I^k_b, I^k_c) : a, b, c \in \mathbb{N}; a < b < c \leq m_1 \cdots m_k\}.$$

Keleti does not give an explicit ordering on this list Γ'_k, but for simplicity and by analogy to the rest of the section, we will order the list lexicographically in the triple (a, b, c). We define the queue

$$\Gamma_k := \bigcup_{j=1}^{k} \Gamma'_j.$$

This list contains all of the triples of intervals at stage j for every $j < k$.

At step k, we consider the kth element of the queue Γ_k. This will consist of a triple of intervals, which Keleti calls (J_k, K_k, L_k). Given E_{k-1}, Keleti defines E_k so that (3.1) does not have any solutions for $x_1 \in E_{k-1} \cap J_k$, $x_2 \in E_{k-1} \cap K_k$, or $x_3 \in E_{k-1} \cap L_k$.

To do this, Keleti retains subintervals of each interval I in E_{k-1} according to whether $I \subset J_k$, $I \subset K_k$, $I \subset L_k$, or $I \subset E_{k-1} \setminus (J_k \cup K_k \cup L_k)$. For intervals $I \subset J_k$, Keleti retains m_k subintervals of length δ_k whose left endpoint is of the form $3\left(i + \frac{1}{2}\right)\frac{\alpha_k \delta_k}{\alpha_k - 1}$ for some integer i. For $I \subset K_k$, Keleti retains m_k intervals of length δ_k with left endpoints of the form $3j\alpha_k\delta_k$ for some $j \in \mathbb{Z}$. For $I \subset L_k$, Keleti retains m_k intervals of length δ_k with left endpoints of the form $3\ell\delta_k$ for some $\ell \in \mathbb{Z}$. For other intervals I, Keleti does not impose any restrictions other than that m_k intervals of length δ_k are retained, and that the retained intervals are separated by at least δ_k. A quick algebraic calculation shows that there are no x_1, x_2, x_3 satisfying (3.1) with $x_1 \in J_k \cap E_k$, $x_2 \in K_k \cap E_k$, and $x_3 \in L_k \cap E_k$.

A careful selection of the quantities δ_k and m_k guarantees that E has Hausdorff dimension 1, and the fact that each triple (J, K, L) of intervals in E_k occurs in each queue Γ_j for all $j > k$ guarantees that there can be no nontrivial solution to (3.1).

A similar principle to this queue is the key to the construction [19], conducted jointly with Malabika Pramanik, that is the main subject of this chapter.

3.1.2 The Constructions of Maga and Máthé

The construction in [28] was extended to $\mathbb{R}^d$ by Maga [33, Theorem 2.3]:

Theorem 3.1.2. *[Parallelogram-free set] For any $d = 1, 2, \cdots$ there exists a subset A of $\mathbb{R}^d$ of full Hausdorff dimension such that A does not contain the vertices of any parallelogram.*

This is a vector-valued version of the result appearing in [28], because the vertices of a parallelogram satisfy the equation (3.1).

Maga also used a complex-valued version of Keleti's argument [29] to establish the following result in $\mathbb{R}^2$ [33, Theorem 2.8]:

Theorem 3.1.3. *[Set not containing similar copies of countably many triangles] Let $\{P_j\} = (p_1^{(j)}, p_2^{(j)}, p_3^{(j)}) \subset \mathbb{R}^{2\times 3}$ be a collection of triangles in $\mathbb{R}^2$; that is, $p_1^{(j)}, p_2^{(j)}, p_3^{(j)}$ are distinct for each j. Then there exists a compact $E \subset \mathbb{R}^2$ such that $\dim_H(E) = 2$ and E does not contain a triangle similar to any triangle P_j.*

In fact, Theorem 2.8 of [33] states this only for a single triangle P, but Maga observes at the beginning of Section 3 that the proof of this theorem can be modified to show Theorem 3.1.3.

Máthé [34, Theorem 2.3] establishes a result that further generalizes the results of Keleti and Maga.

Theorem 3.1.4. *[Set not containing any of a countable set of rational polynomial configurations] Let $n \geq 1$. Let J be a countable set. For each $j \in J$, let v_j be a positive integer and let $P_j : \mathbb{R}^{nv_j} \to \mathbb{R}$ be a (non identically zero) polynomial in nv_j variables with rational coefficients. Assume that d is the maximum degree of the polynomials P_j $(j \in J)$. Then there exists a compact set $E \subset \mathbb{R}^n$ of Hausdorff dimension n/d such that for every $j \in J$, E does not contain v_j distinct points $x_1, \ldots, x_{v_j}$ satisfying $P_j(x_1, \ldots, x_{v_j}) = 0$.*

This theorem directly implies Keleti's result [28] on parallelograms, and Maga's result, Theorem 3.1.2. While it is not immediately apparent that this implies Theorems 3.1.1 or 3.1.3, the proof of this theorem yields a stronger result mentioned later in the paper [34, Theorem 6.1]:

Theorem 3.1.5. *[Set not containing any of a countable set of rational polynomial configurations applied to diffeomorphisms] Let $n \geq 1$. Let J be a countable set. For each $j \in J$, let v_j be a positive integer, let $P_j : \mathbb{R}^{nv_j}$ be a (non identically zero) polynomial in nv_j variables with rational coefficients, and let $\Phi_{j,1}, \ldots, \Phi_{j,v_j}$ be C^1-smooth diffeomorphisms of $\mathbb{R}^n$. Assume that d is the maximum degree of the polynomials P_j $(j \in J)$. Then there exists a compact set $E \subset \mathbb{R}^n$ of Hausdorff dimension n/d such that for every $y \in J$, E does not contain v_j distinct points $x_1, \ldots, x_{m_j}$ satisfying*

$$P_j(\Phi_{j,1}(x_1), \ldots, \Phi_{j,v_j}(x_{v_j})) = 0.$$

This theorem immediately implies Theorem 3.1.1, since the functions $(x_3 - x_1) - \alpha_j(x_3 - x_2)$ are polynomials in x_1, $\alpha_j x_2$, and $(\alpha_j - 1)x_3$, and multiplication by α_j and by $\alpha_j - 1$ is a diffeomorphism of $\mathbb{R}$. Less obviously, it also implies Theorem 3.1.3 using a similar argument where the α_j are replaced by similarity matrices A_j. This argument does not work in dimensions 3 and higher because there is no unique similarity carrying the vectors $b - a$ to $c - a$ in the class of triangles abc that are similar to a given triangle T.

We now discuss the main results of [19]: Theorems 1.1.1, 1.1.2, and 1.1.3.

3.2 Discussion of Main Results

3.2.1 Nonsimultaneous Avoidance

Notice that if Theorem 1.1.1 is being applied to a single function f, the theorem gives a nontrivial result only if the components of ∇f sum to zero; otherwise, a set E of positive measure can be constructed simply by taking an appropriate translate of a small interval centered at the origin.

The points in E are taken to be distinct; however, this assumption can sometimes be circumvented by choosing the sequence f_j appropriately. For example, suppose we wanted to, as in [28], avoid parallelograms of points that satisfy

$$(x_4 - x_3) - (x_2 - x_1) = 0$$

where x_3 could possibly equal x_2. Then we can simply take

$$f_1(x_1, x_2, x_3, x_4) = (x_4 - x_3) - (x_2 - x_1)$$

and

$$f_2(x_1, x_2, x_3, x_4) = x_4 - 2x_2 + x_1.$$

This trick is only possible if it preserves the nonvanishing condition on the partial derivatives of f. Note that Theorem 1.1.1 gives a suboptimal result in this instance: $\frac{1}{v-1}$ is only equal to $\frac{1}{3}$, which is inferior to the Hausdorff dimension obtained by Keleti [28]. This example illustrates a weakness of Theorem 1.1.1: this theorem gives poor bounds if the functions f are polynomials of low degree with integer coefficients.

Another weakness of Theorem 1.1.1 relative to other results in the literature is that Theorem 1.1.1 requires that the number of variables be bounded. For example, a simple consequence of Theorem 3.1.4 is that there is a Hausdorff dimension 1 subset of $\mathbb{R}$ that is linearly independent over $\mathbb{Q}$. However, this example requires avoiding configurations with an arbitrary number of variables, so Theorem 1.1.1 does not apply to this example.

For illustrative purposes, we give the following examples.

Example 3.2.1 (Avoiding isosceles triangles)**.** *Let Γ be a C^1 curve in $\mathbb{R}^d$. How large a subset of Γ can be found that does not contain an isosceles triangle or 3-term arithmetic progression (which will be considered a degenerate isosceles triangle)?*

We can apply some of the results in the literature to this problem, as well as Theorem 1.1.1. Theorem 3.1.1 applies if the curve Γ is a line segment: in this case Γ is parameterized by a function $\gamma(t)$ where all components of

γ are affine-linear functions of t, so the problem is equivalent to finding a 3-term AP-free subset of $[0,1]$, which was considered in [28]. The result in this paper implies that we can find a subset of Γ of Hausdorff dimension 1 that does not contain any 3-term arithmetic progressions.

If the curve Γ has a parameterization given by $\gamma(t) = (\gamma_1(t), \cdots \gamma_d(t))$ where each $\gamma_j(t)$ is a polynomial with rational coefficients of degree at most D, then we can apply Máthé's result, Theorem 3.1.4. We assume that this parameterization is bi-Lipschitz, which can be guaranteed provided we choose an appropriately small arc of Γ. We will define the function

$$f_2(t_1, t_2, t_3) := \sum_{j=1}^{d} (\gamma_j(t_3) - \gamma_j(t_2))^2 - \sum_{j=1}^{d} (\gamma_j(t_2) - \gamma_j(t_1))^2,$$

for $t_1 < t_2 < t_3$, which is zero precisely when the distance between $\gamma(t_1)$ and $\gamma(t_2)$ is equal to the distance between $\gamma(t_2)$ and $\gamma(t_3)$. It is possible to argue, as in [19], that it suffices to apply Theorem 3.1.4 to this example. However, we will argue somewhat differently here. Let

$$f_1(t_1, t_2, t_3) := \sum_{j=1}^{d} (\gamma_j(t_3) - \gamma_j(t_1))^2 - \sum_{j=1}^{d} (\gamma_j(t_1) - \gamma_j(t_2))^2,$$

and

$$f_3(t_1, t_2, t_3) := \sum_{j=1}^{d} (\gamma_j(t_2) - \gamma_j(t_3))^2 - \sum_{j=1}^{d} (\gamma_j(t_1) - \gamma_j(t_3))^2.$$

Then locating $E \subset [0,1]$ such that there are no solutions to $f_k(t_1, t_2, t_3) = 0$ for $k = 1, 2, 3$, we have that $\gamma(E)$ will be a subset of Γ with no isosceles triangles.

So if each component of γ has degree at most D, then we can apply Theorem 3.1.4 to $\{f_1, f_2, f_3\}$ to locate a set $E \subset [0,1]$ of Hausdorff dimension $\frac{1}{2D}$ such that $\gamma(E)$ contains no isosceles triangles. Since γ is bi-Lipschitz, this implies that $\gamma(E)$ also has Hausdorff dimension $\frac{1}{2D}$.

In fact, this result is improved by Theorem 1.1.1. Simply apply this theorem to $\{f_1, f_2, f_3\}$: each function is a real function of three real variables, so this theorem gives a set of Hausdorff dimension $\frac{1}{2}$ that does not contain any isosceles triangles.

Here is another example of Theorem 1.1.1.

Example 3.2.2 (A Transcendental Function)**.** *Consider the function*

$$f(x_1, x_2, x_3) = \sin(x_3 - x_2) - (x_2 - x_1).$$

How large a subset of $\mathbb{R}$ can we find that does not contain three points x_1, x_2, x_3 that satisfy $f(x_1, x_2, x_3) = 0$?

There is no obvious family of diffeomorphisms ϕ_1, ϕ_2, ϕ_3 such that $f(\phi_1(x), \phi_2(x), \phi_3(x))$ is a polynomial. So we cannot apply Theorem 3.1.4. Nonetheless, Theorem 1.1.1 still applies, and we can locate a subset of $\mathbb{R}$ of Hausdorff dimension $\frac{1}{2}$ that does not contain this configuration.

We present an example of Theorem 1.1.2 with $m > 1$. In order to present this example, we need a signed distance function d, defined along a parameterized curve $\gamma(t)$. We define

$$d(\gamma(t_1), \gamma(t_2)) = \begin{cases} |\gamma(t_1) - \gamma(t_2)| & \text{if } t_1 \geq t_2 \\ -|\gamma(t_1) - \gamma(t_2)| & \text{if } t_1 < t_2. \end{cases} \tag{3.2}$$

The point of this definition is that the function d is differentiable in t_1 and t_2.

Lemma 3.2.3 (Lemma 6.1 from [19])**.** *Given a C^2 parameterization $\gamma : [0, \eta] \to \mathbb{R}^n$ of a curve Γ. Then the distance function $F(t_1, t_2) := d(\gamma(t_1), \gamma(t_2))$ is differentiable on $[0, \eta]^2$. Furthermore, if γ is parameterized by its arclength; that is, $|\gamma'(t)| \equiv 1$, then*

$$\frac{\partial F}{\partial t_1}(t, t) = 1$$
$$\frac{\partial F}{\partial t_2}(t, t) = -1$$

Proof. We only need to check the case $t_1 = t_2$, since d is clearly differentiable for $t_1 \neq t_2$. Consider $t_1 = t_2 = t$. Let $h \geq k$. Then

$$\begin{aligned} F(t+h, t+k) = d(\gamma(t+h), \gamma(t+k)) &= |\gamma(t+h) - \gamma(t+k)| \\ &= |\gamma'(t)|\,|h-k| + O(h^2 + k^2) \\ &= |\gamma'(t)|(h-k) + O(h^2 + k^2). \end{aligned}$$

Where we used the fact $h \geq k$ to conclude both that $d(\gamma(t+h), \gamma(t+k)) = |\gamma(t+h) - \gamma(t+k)|$, and that $|h-k| = h-k$.

If $h < k$, we have

$$\begin{aligned} d(\gamma(t+h), \gamma(t+k)) &= -|\gamma(t+h) - \gamma(t+k)| \\ &= -|\gamma'(t)|\,|h-k| + O(h^2+k^2) \\ &= |\gamma'(t)|(h-k) + O(h^2+k^2). \end{aligned}$$

This time, because $h < k$, we have $d(\gamma(t+h), \gamma(t+k)) = -|\gamma(t+h) - \gamma(t+k)|$, but we also have that $|h-k| = -(h-k)$. The two minus signs "cancel out" and we therefore get that $\frac{\partial f}{\partial t_1} = \gamma'(t)$ when $t_1 = t_2 = t$ and $\frac{\partial f}{\partial t_2} = -|\gamma'(t)|$ when $t_1 = t_2 = t$. □

In addition to the case $t_1 = t_2 = t$ discussed in Lemma 3.2.3, we can compute the derivative of $d(\gamma(t_1), \gamma(t_2))$ for $t_1 \neq t_2$. If $t_1 > t_2$, then $d(\gamma(t_1), \gamma(t_2))$ is the usual distance $|\gamma(t_1) - \gamma(t_2)|$. The derivative of this in the γ_1 variable is precisely the quantity

$$\gamma'(t_1) \cdot \frac{\gamma(t_1) - \gamma(t_2)}{|\gamma(t_1) - \gamma(t_2)|},$$

the projection of $\gamma'(t_1)$ onto the one-dimensional space spanned by the vector $\gamma(t_1) - \gamma(t_2)$. A similar argument allows for the calculation of the partial derivative in the t_2 variable and the partial derivatives in the case where $t_1 < t_2$.

Example 3.2.4. *Let $\Gamma \subset \mathbb{R}^2$ be a curve parameterized by a smooth function $\gamma : \mathbb{R} \to \mathbb{R}^2$. Call a trapezoid $ABCD$, with AD parallel to BC,* special *if its sidelengths satisfy the relation $|BC|^2 = |AB||CD|$. How large a subset of Γ can we find that does not contain the vertices of any special trapezoid?*

If we take $A = \gamma(t_1)$, $B = \gamma(t_2)$, $C = \gamma(t_3)$, and $D = \gamma(t_4)$, we need t_1, t_2, t_3, t_4 to satisfy two linearly independent conditions: the sides AD and BC must be parallel, and the side lengths must satisfy the special relation. We then define

$$f_1(t_1, t_2, t_3, t_4) = \det[(\gamma(t_4) - \gamma(t_1))^t, (\gamma(t_3) - \gamma(t_2))^t] \tag{3.3}$$
$$f_2(t_1, t_2, t_3, t_4) = d(\gamma(t_4), \gamma(t_3))d(\gamma(t_2), \gamma(t_1)) - d(\gamma(t_3), \gamma(t_2))^2. \tag{3.4}$$

Here $d(x, y)$ is the signed distance function given in equation (3.2), t represents the transpose operation, and det represents the determinant. This determinant is zero if the vectors $\gamma(t_4) - \gamma(t_1)$ and $\gamma(t_3) - \gamma(t_2)$ are parallel (or if either vector is zero).

Lemma 3.2.5 (Full Rank Condition for Special Trapezoids)**.** *Letting* $f = (f_1, f_2)$*, The derivative* Df *has full rank on the points of the zero set of* f *where* t_1, t_2, t_3, t_4 *are distinct.*

It will follow from Lemma 3.2.5 and Theorem 1.1.2 that there is a set E of Hausdorff dimension $\frac{2}{3}$ that does not contain any special trapezoids. We now prove this lemma.

Proof of Lemma 3.2.5, Lemma 6.3 of [19]. By symmetry, and by taking a small enough arc of Γ, we can (and do) assume Γ is strictly convex, and that all components of γ' are positive. We consider the 2-by-2 submatrix of Df consisting of the entries $\partial f_i/\partial t_j$ where $i \in \{1,2\}$ and $j \in \{1,4\}$. We aim to show that this submatrix has nonzero determinant, which will be accomplished by showing that $\partial f_1/\partial t_j$ is nonzero for $j = 1,4$, and that these two derivatives have the same sign, but $\partial f_2 \partial t_j$ are nonzero and have opposite signs. This is sufficient to show that the second row of the Jacobian is not a scalar multiple of the first row; therefore, Df must be nonsingular.

We begin by computing the derivatives $\partial f_1/\partial t_j$ on the set of t_1, t_2, t_3, t_4 for which f_1 is zero. On this set, we have

$$\frac{\gamma_2(t_3) - \gamma_2(t_2)}{\gamma_1(t_3) - \gamma_1(t_2)} = \frac{\gamma_2(t_4) - \gamma_2(t_1)}{\gamma_1(t_4) - \gamma_1(t_1)}. \tag{3.5}$$

In words, this equation says that the slope of the line connecting $\gamma(t_2)$ to $\gamma(t_3)$ is equal to the slope of the line connecting $\gamma(t_1)$ to $\gamma(t_4)$.

If we write out the determinant in (3.3) explicitly, we get the expression

$$f_1(t_1, t_2, t_3, t_4) := (\gamma_1(t_4) - \gamma_1(t_1))(\gamma_2(t_3) - \gamma_2(t_2)) \tag{3.6}$$
$$- (\gamma_2(t_4) - \gamma_2(t_1))(\gamma_1(t_3) - \gamma_1(t_2)) \tag{3.7}$$

Therefore, we have the partial derivatives

$$\frac{\partial f_1}{\partial t_1} = -\gamma_1'(t_1)(\gamma_2(t_3) - \gamma_2(t_2)) + \gamma_2'(t_1)(\gamma_1(t_3) - \gamma_1(t_2)) \tag{3.8}$$
$$\frac{\partial f_1}{\partial t_4} = \gamma_1'(t_4)(\gamma_2(t_3) - \gamma_2(t_2)) - \gamma_2'(t_4)(\gamma_1(t_3) - \gamma_1(t_2)). \tag{3.9}$$

We can substitute (3.5) into (3.8) and (3.9):

$$\frac{\partial f_1}{\partial t_1} = -\gamma_1'(t_1)(\gamma_1(t_3) - \gamma_1(t_2))\frac{\gamma_2(t_4) - \gamma_2(t_1)}{\gamma_1(t_4) - \gamma_1(t_1)} + \gamma_2'(t_1)(\gamma_1(t_3) - \gamma_1(t_2)).$$
$$\frac{\partial f_1}{\partial t_4} = \gamma_1'(t_4)(\gamma_1(t_3) - \gamma_1(t_2))\frac{\gamma_2(t_4) - \gamma_2(t_1)}{\gamma_1(t_4) - \gamma_1(t_1)} - \gamma_2'(t_4)(\gamma_1(t_3) - \gamma_1(t_2)).$$

We now let F_1 and F_4 be defined by $F_1 = \left[-\frac{\gamma_2(t_4)-\gamma_2(t_1)}{\gamma_1(t_4)-\gamma_1(t_1)} + \frac{\gamma_2'(t_1)}{\gamma_1'(t_1)}\right]$ and $F_4 = \left[\frac{\gamma_2(t_4)-\gamma_2(t_1)}{\gamma_1(t_4)-\gamma_1(t_1)} - \frac{\gamma_2'(t_4)}{\gamma_1'(t_4)}\right]$. With these definitions, we arrive at the equations

$$\frac{\partial f_1}{\partial t_1} = \gamma_1'(t_1)(\gamma_1(t_3) - \gamma_1(t_2))F_1 \tag{3.10}$$

$$\frac{\partial f_1}{\partial t_4} = \gamma_1'(t_4)(\gamma_1(t_3) - \gamma_1(t_2))F_4. \tag{3.11}$$

It is now time to use our assumptions about γ. By assumption, γ_1' is nonnegative, and therefore, the sign of $\frac{\partial f_1}{\partial t_1} \cdot \frac{\partial f_1}{\partial t_4}$ is equal to the sign of F_1F_4.

The expressions for F_1 and F_4 are handled using the convexity of γ. The quantity $\frac{\gamma_2'(t_1)}{\gamma_1'(t_1)}$ is the slope of the tangent line to γ at t_1, $\frac{\gamma_2'(t_4)}{\gamma_1'(t_4)}$ is the slope of the tangent line to γ at t_4, and $\frac{\gamma_2(t_4)-\gamma_2(t_1)}{\gamma_1(t_4)-\gamma_1(t_1)}$ is the slope of the secant line connecting $\gamma(t_1)$ to $\gamma(t_4)$. The convexity of Γ thus guarantees that F_1 and F_4 have the same sign, and thus that $\frac{\partial f_1}{\partial t_1}$ and $\frac{\partial f_4}{\partial t_4}$ also have the same sign.

Now, we need to show that $\frac{\partial f_2}{\partial t_j}$ have opposite signs for $j = 1$ and $j = 4$. Evidently f_2 is nonzero if $t_4 - t_3$ and $t_2 - t_1$ have opposite signs. So we assume that $t_4 - t_3$ and $t_2 - t_1$ have the same sign: $(t_4 - t_3)(t_2 - t_1) > 0$. From the discussion following the proof of Lemma 3.2.3, we have the equations

$$\frac{\partial}{\partial t_4} d(\gamma(t_4), \gamma(t_3)) = \gamma'(t_4) \cdot \frac{\gamma(t_4) - \gamma(t_3)}{|\gamma(t_4) - \gamma(t_3)|}$$

and

$$\frac{\partial}{\partial t_1} d(\gamma(t_2), \gamma(t_1)) = -\gamma'(t_1) \cdot \frac{\gamma(t_2) - \gamma(t_1)}{|\gamma(t_2) - \gamma(t_1)|}$$

Thus

$$\frac{\partial f_2}{\partial t_4} = \gamma'(t_4) \cdot \frac{\gamma(t_4) - \gamma(t_3)}{|\gamma(t_4) - \gamma(t_3)|} d(\gamma(t_2), \gamma(t_1)) \tag{3.12}$$

$$\frac{\partial f_2}{\partial t_1} = -\gamma'(t_1) \cdot \frac{\gamma(t_2) - \gamma(t_1)}{|\gamma(t_2) - \gamma(t_1)|} d(\gamma(t_4), \gamma(t_3)) \tag{3.13}$$

$$\tag{3.14}$$

Here, $\gamma'(t_4) \cdot (\gamma(t_4) - \gamma(t_3))$ has the same sign as $\gamma'(t_1) \cdot (\gamma(t_2) - \gamma(t_1))$, and $d(\gamma(t_2), \gamma(t_1))$ and $d(\gamma(t_4), \gamma(t_3))$ have the same sign because $t_4 - t_3$ and $t_2 - t_1$ have the same sign. Thus $\frac{\partial f_2}{\partial t_1}$ and $\frac{\partial f_2}{\partial t_4}$ have opposite signs. $\square$

3.2.2 Polygons and Polyhedra

For example, consider the problem of finding a subset of $\mathbb{R}^2$ that does not contain any equilateral triangles. Maga [33] has shown that it is possible to find such a set with Hausdorff dimension 2. This is a 3-point configuration (hence $v = 3$) consisting of points (x_1, x_2, x_3) that satisfy the conditions: $d(x_1, x_2) = d(x_1, x_3)$ and $d(x_1, x_2) = d(x_2, x_3)$. Here $d(x, y)$ is the usual Euclidean distance from x to y: a function that is differentiable on the set of points where x_1, x_2 and x_3 are distinct. So, for this example, we have $m = 2$ and $v = 3$, so Theorem 1.1.2 will give a set of Hausdorff dimension 1 that does not contain any equilateral triangles. Not only is this inferior to Maga's result, it is entirely trivial: a line, for example, is a set of Hausdorff dimension 1 that does not contain any equilateral triangles.

The situation is improved somewhat if we consider regular polygons with more sides. For example, a square in $\mathbb{R}^2$ is a family of 4 points $(x_j, y_j) : j = 1, 2, 3, 4$ satisfying the following family of equations:

$$\begin{aligned}(y_2 - y_1)^2 + (x_2 - x_1)^2 &= (y_3 - y_1)^2 + (x_3 - x_1)^2 \\ (x_2 - x_1)(y_2 - y_1) &= -(x_3 - x_1)(y_3 - y_1) \\ (y_2 - y_4)^2 + (x_2 - x_4)^2 &= (y_3 - y_4)^2 + (x_3 - x_4)^2 \\ (x_2 - x_4)(y_2 - y_4) &= -(x_3 - x_4)(y_3 - y_4)\end{aligned}$$

Where $(x_1, y_1), (x_2, y_2), (x_3, y_3)$, and (x_4, y_4) are distinct. Notice that as long as these points are distinct, the corresponding Jacobian matrix has full rank. Thus Theorem 1.1.2 applies (with $n = 2, m = 4, v = 4$) to give a set of Hausdorff dimension $\frac{4}{3}$ that does not contain the vertices of any square. This dimension can be taken to be as large as $\frac{2v-4}{v-1}$ if the configuration to be avoided is a regular v-gon. Note that even this bound, while nontrivial, is inferior to that of Maga: Maga's result can be applied to any 3 points in a regular v-gon in order to find a subset of $\mathbb{R}^2$ of Hausdorff dimension 2 that does not contain any regular v-gons.

Máthé poses the problem of finding a set of large Hausdorff dimension in $\mathbb{R}^3$ that does not contain any regular tetrahedron [34, Remark 6.3]. Unfortunately, Theorem 1.1.2 does not shed any light on this question: there are 4 points in a regular tetrahedron that satisfy 5 conditions, giving a set of Hausdorff dimension 1 that does not contain a regular tetrahedron. This bound is, of course, unsatisfactory: a plane also does not contain any regular tetrahedra. Nonetheless, if we consider similarity classes of larger polyhedra, we can get a nontrivial result. For example, a regular dodecahedron has 20 vertices. After 2 vertices (x_1, y_1, z_1) and (x_2, y_2, z_2) are placed, a vertex adjacent to (x_1, y_1, z_1) must lie in a specific circle in $\mathbb{R}^3$. Once this point is placed, there are only a finite number of possible choices for the remaining points, so we can think of the 20 points of a regular dodecahedron as satisfying 53 independent conditions. Thus Theorem 1.1.2 gives a set of Hausdorff dimension $\frac{53}{19}$ that does not contain any regular dodecahedra. A similar argument can show that there is a subset of $\mathbb{R}^3$ of Hausdorff dimension $\frac{6v-9}{2v-1}$ that does not contain a right v-prism, and a subset of $\mathbb{R}^3$ of Hausdorff dimension $\frac{3v-7}{v-1}$ that does not contain any regular v-gon. Note that these quantities approach 3 as $v \to \infty$.

3.2.3 Simultaneous Avoidance

Theorem 1.1.3, although stated for a single configuration, can be modified (with a reduction in the Hausdorff dimension) to apply to a finite number of configurations. However, the theorem does not apply for countably many configurations.

In order to shed some light on Theorem 1.1.3, we will consider an example similar to Example 3.2.1. Let Γ be a smooth curve with arclength parameterization γ. This means that $|\gamma'(t)| \equiv 1$ for all t. Suppose the curvature of γ is bounded above by a constant, so that $\gamma(t_2) - \gamma(t_1)$ is equal within $K(t_2 - t_1)^2$ of $\gamma'(t_1)(t_2 - t_1)$ for t_2, t_1 with $|t_2 - t_1|$ sufficiently small. Then, for a fixed K, we have the following result.

Example 3.2.6. *For any fixed $K > 0$ There exists a set E_K with positive Hausdorff dimension (not depending on K) such that, for any curve γ satisfying the above conditions, $\gamma(E)$ does not contain the vertices of any isosceles triangle. The set E does not depend on the curve γ. Furthermore, the dimension of this set can be taken to be $\frac{\log 2}{\log 3}$.*

In fact, the set E that we will use is simply a slightly shrunken version of the Cantor middle thirds set. We can arrive at the set E by applying Theorem 1.1.3.

Here, we will need the following lemma.

Lemma 3.2.7 (Lemma 6.2 from [19])**.** *Let $\gamma : [0, \eta] \to \mathbb{R}^n$ be an injective parametrization of a C^2 curve with*

$$\gamma'(0) \neq 0 \quad \textit{and} \quad \sup\{||\gamma''(t)|| : t \in [0, \eta]\} \leq K.$$

If η is sufficiently small depending on $|\gamma'(0)|$ and K, then there are no isosceles triangles $\gamma(t_1), \gamma(t_2), \gamma(t_3)$ with $0 \leq t_1 < t_2 < t_3 \leq \eta$ whose sides of equal length meet at $\gamma(t_1)$ or at $\gamma(t_3)$.

Proof. We showed in Lemma 3.2.3 that d is differentiable. So we can write

$$\begin{aligned} d(\gamma(t_3),\gamma(t_1)) - d(\gamma(t_2),\gamma(t_1)) &= \int_{t_2}^{t_3} \frac{\partial}{\partial t} d(\gamma(t),\gamma(t_1))\,dt \\ &= \int_{t_2}^{t_3} \gamma'(t)\cdot \frac{\gamma(t)-\gamma(t_1)}{|\gamma(t)-\gamma(t_1)|}\,dt. \end{aligned}$$

We estimate the direction vector $\frac{\gamma(t)-\gamma(t_1)}{|\gamma(t)-\gamma(t_1)|}$ as follows:

$$\begin{aligned} \frac{\gamma(t)-\gamma(t_1)}{|\gamma(t)-\gamma(t_1)|} &= \frac{\left[\gamma'(t_1)(t-t_1)+O(K(t-t_1)^2)\right]}{|\left[\gamma'(t_1)(t-t_1)+O(K(t-t_1)^2)\right]|} \\ &= \frac{\gamma'(t_1)+O(K\eta)}{|\gamma'(t_1)+O(K\eta)|} \\ &= \frac{\gamma'(0)+O(K\eta)}{|\gamma'(0)+O(K\eta)|} \\ &= \frac{\gamma'(0)}{|\gamma'(0)|}\left[1+O\left(\frac{K\eta}{|\gamma'(0)|}\right)\right]. \end{aligned}$$

The estimate in the last line holds provided that η is sufficiently small because the $\gamma'(0)$ term in the denominator is nonzero and does not depend on η.

This gives us, upon plugging into the integrand:

$$\begin{aligned} \gamma'(t)\cdot\frac{\gamma(t)-\gamma(t_1)}{|\gamma(t)-\gamma(t_1)|} &= \left[\gamma'(0)+O(K\eta)\right]\cdot\frac{\gamma'(0)}{|\gamma'(0)|}\left[1+O\left(\frac{K\eta}{|\gamma'(0)|}\right)\right] \\ &\geq \frac{|\gamma'(0)|}{2} \neq 0, \end{aligned}$$

provided that η is sufficiently small. A similar argument shows that $\gamma(t_3)$ cannot be in the middle, either. ☐

Therefore, in order to avoid isosceles triangles in our example, it is enough to avoid the zeros of $d(\gamma(t_3),\gamma(t_2)) - d(\gamma(t_2),\gamma(t_1))$. But Lemma 3.2 shows that the linearization of this function at a point (t,t,t) is always $t_3-2t_2+t_1$, so Theorem 1.1.3 applies, giving a set E with positive Hausdorff dimension with the desired property. The specific bound $\dim E > \frac{\log 2}{\log 3}$ will be calculated alongside the proof of Theorem 1.1.3.

3.3 A Single Step

The proofs of Theorems 1.1.1 and 1.1.2 are based on an iterative construction. We will describe a typical step of this construction.

We start with a function $f : \mathbb{R}^{nv} \to \mathbb{R}^m$, and a set $T \subset \mathbb{R}^{nv}$. We construct a set $S \subset T$ such that $f(x_1, \ldots, x_v)$ is nonzero for $(x_1, \ldots, x_v) \in S$. This does not immediately give the desired set, because S cannot be expressed as the v-fold product of a set in $\mathbb{R}^n$ with itself. This is similar to Keleti's strategy for proving Theorem 3.1.1.

3.3.1 One Dimension, Nonvanishing Gradient

We will begin with a real-valued continuously differentiable function f in v variables with nonvanishing gradient defined in a neighbourhood of the origin containing $[0, \eta]^v$. Note that this assumption is stronger than the assumption in Theorem 1.1.1; nonetheless, an iterative argument will allow us to overcome this difficulty.

Suppose that we are given $i_0 \in \{1, 2, \cdots v\}$, an integer $M \geq 1$, a small constant $c_0 > 0$ and compact subsets $T_1, \ldots, T_v \subset [0, 1]$.

1. Each T_i is a union of closed intervals of length M^{-1} with disjoint interiors. Let us denote by $\mathcal{J}_M(T_i)$ this collection of intervals.
2. The interior of T_i is disjoint from the interior of $T_{i'}$ if $i \neq i'$.
3. $\left|\frac{\partial f}{\partial x_{i_0}}(x)\right| \geq c_0$ and $|\nabla f(x)| \leq c_0^{-1}$ for all $x \in T_1 \times \cdots \times T_v$.

Proposition 3.3.1 (Proposition 3.1 from [19])**.** *Given f, M, i_0, c_0 and $\mathbb{T} = (T_1, \cdots, T_v)$ satisfying these assumptions, there exist a small rational constant $c_1 > 0$ and an integer N_0 (depending on all these quantities), for which the following conclusions hold.*

There is a sequence of arbitrarily large integers $N \geq N_0$ with $\frac{N}{M}, c_1 N \in \mathbb{N}$ such that for each N in this sequence, one can find compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $J \in \mathcal{J}_M(T_i)$, let us decompose J into closed intervals of length N^{-1} with disjoint interiors and call the resulting collection of intervals $\mathcal{I}_N(J, i)$. Then for each $i \neq i_0$ and each $I \in \mathcal{I}_N(J, i)$, the set $S_i \cap I$ is an interval of length $c_1 N^{1-v}$.

(c) For every $J \in \mathcal{J}_M(T_{i_0})$, there exists $\mathcal{I}'_N(J, i_0) \subseteq \mathcal{I}_N(J, i_0)$ with

$$\#\big(\mathcal{I}'_N(J, i_0)\big) \geq \big(1 - \frac{1}{M}\big)\#\big(\mathcal{I}_N(J, i_0)\big) \tag{3.15}$$

such that for each $I \in \mathcal{I}'_N(J, i_0)$,

$$|S_{i_0} \cap I| \geq \frac{c_1}{N}. \tag{3.16}$$

Unlike part (b), $S_{i_0} \cap I$ need not be an interval; however, it can be written as a union of intervals of length $c_1 N^{1-v}$ with disjoint interiors.

The reader should imagine that N_0 and thus N appearing in this proposition is much larger than M. Thus, accruing additional powers of M in this argument will be considered only a small loss.

Proof. In order to simplify the proof, we will assume without loss of generality that $i_0 = v$. The proof will proceed in the following manner: we will select sets $S_1, \dots, S_{v-1}$ using a very simple procedure, and then select S_v to avoid the places where $f(x_1, \dots, x_v) = 0$ for some $(x_1, \dots, x_{v-1})$ in $S_1 \times \cdots \times S_{v-1}$. This is exactly the strategy that Keleti uses to prove Theorem 3.1.1.

We select, for $1 \leq i \leq v - 1$:

$$S_i = \bigcup \{[a_i, a_i + c_1 N^{1-v}] : [a_i, b_i] = I \in \mathcal{I}_N(J_i) \text{ for some } J \in \mathcal{J}_M(T_i)\}.$$

Here, c_1 is a small positive rational constant, and N will be specified later. This means that we take the leftmost interval of length $c_1 N^{1-v}$ of each $\frac{1}{N}$-interval that constitutes T_i. Part (b) of the proposition clearly holds for this choice of S_i.

We define the family of points $\mathbb{A}$ in $\mathbb{R}^{v-1}$ to be the bottom-left corners of the Cartesian product of the S_i for $i \leq v - 1$:

$$\mathbb{A} := \prod_{i=1}^{v-1} \{a_i : [a_i, b_i] = I \in \mathcal{I}_N(J, i) \text{ for some } J \in \mathcal{J}_M(T_i)\}.$$

Note that for each i, there are (assuming $\eta < 1$) at most N possible choices for a_i; therefore, we have a bound

$$\#\mathbb{A}_N \leq N^{v-1}. \tag{3.17}$$

In Lemma 3.3.2 we will show that for every fixed $a' \in \mathbb{A}_N$, we have that

$$\#\{x_v : f(a', x_v) = 0\} \leq M.$$

We will define

$$\mathbb{B} := \{x_v : \exists a' \in \mathbb{A}_N \text{ such that } f(a', x_v) = 0\},$$

a set that, by (3.17) and by Lemma 3.3.2 has at most MN^{v-1} elements.

We select $\mathcal{I}'_N(J,v) \subset \mathcal{I}_N(J,v)$ as follows: we declare that

$$I \in \mathcal{I}'_N(J,v) \quad \text{if} \quad \#(\mathcal{B} \cap I) \leq 2M^3N^{v-2}.$$

Now we do a quick count. There are at most MN^{v-1} points in $\mathcal{B}$, and we have that if $I \in \mathcal{I}_N(J,v) \setminus \mathcal{I}'_N(J,v)$, there are at least $2M^3N^{v-2}$ points of $\mathcal{B}$ in I. Because these intervals are essentially disjoint, it follows from the pigeonhole principle that there are at most $M^{-2}N$ intervals in $\mathcal{I}_N(J,v) \setminus \mathcal{I}'_N(J,v)$. Because there are $\frac{N}{M}$ intervals in $\mathcal{I}_N(J,v)$ implies the bound in part (c) of the lemma.

Now, we partition $I \in \mathcal{I}'_N(J,v)$ into consecutive subintervals of length C_0c_1/N^{v-1} with disjoint interiors, and denote the successive intervals by $\tilde{I}_\ell(I)$. Here, C_0 is an integer depending on f, M, $T_1,\ldots,T_v$ (but not on N) that will be specified in Lemma 3.3.3. It is convenient that c_1 is rational, so that we can select N in order to guarantee that $\frac{N^{v-2}}{C_0c_1}$ is an integer.

We then discard intervals from $\tilde{I}_\ell(I)$ that contain an element of $\mathbb{B}$ or are adjacent to an interval containing an element of $\mathbb{B}$, as well as the leftmost and rightmost intervals of $\tilde{I}_\ell(I)$. The union of the remaining intervals is chosen as S_v:

$$S_v = \bigcup \left\{ \tilde{I}_\ell(I) : \begin{array}{l} \tilde{I}_k(I) \cap \mathbb{B} = \emptyset \text{ for } |k-\ell| \leq 1, I \in \mathcal{I}'_N(J,v), \\ J \in \mathcal{J}_M(T_v),\ 1 < \ell < N^{v-2}/(C_0c_1) \end{array} \right\}.$$

S_v is a union of intervals of length c_1/N^{v-1}. Because of the way $I'_N(J,v)$ was defined, there can only be at most $6M^3N^{v-2}+2 \leq 7M^3N^{v-2}$ removed intervals. This implies that the total length of the intervals removed is at most
$7C_0c_1M^3N^{v-2}/N^{v-1}$. This is at most $7M^3C_0c_1/N$. This is bounded above by $\frac{(1-c_1)}{N}$ provided that c_1 is chosen small enough to guarantee that $7M^3C_0c_1$ is no more than $1-c_1$.

Then, by Lemma 3.3.3, given any $x' = (x_1,\ldots,x_{v-1}) \in S_1 \times S_2 \times \cdots \times S_{v-1}$, we have that the x_v such that $f(x',x_v)=0$ must lie within a C_0c_1/N^{v-1} neighbourhood of the set $\mathbb{B}$. This establishes (a), completing the proof of the Lemma. □

This selection algorithm ultimately results in a set of Hausdorff dimension $\frac{1}{v-1}$ because of the factor of N^{1-v} occurring in part (b) of the Lemma.

Suppose that $f : \mathbb{R}^v \to \mathbb{R}$ is a linear function with nonzero integer coefficients:

$$f(x_1,\ldots,x_v) = \sum_{i=1}^{v} \alpha_i x_i.$$

This is the case in Keleti's paper [28]. Without loss of generality, assume that each T_i is a finite union of intervals J of the form $\mathbb{Z}/M + [0, 1/M]$. We could select S_i for $i < v$ differently from the method in Proposition 3.3.1. Take

$$S_i \cap I := [k/N, (k + c_1)/N]$$

where c_1 will be selected shortly. If $x_i \in S_i$ for $i < v$, and $f(x_1, \ldots, x_v) = 0$, then it is easily seen that x_v has to be of the form

$$x_v = -\frac{1}{\alpha_v} \sum_{k=1}^{v-1} \alpha_i x_i.$$

If we select c_1 such that

$$c_1 \sum_{i=1}^{v-1} |\alpha_i| < \frac{1}{4},$$

then we have that any such x_v is within $\frac{1}{4|\alpha_v|}N$ of an integer multiple of $\frac{1}{|\alpha_v|N}$.

$$\operatorname{dist}\Big(x_v, \frac{\mathbb{Z}}{|\alpha_v|N}\Big) < \frac{1}{4|\alpha_v|N} \tag{3.18}$$

whenever $f(x_1, \ldots, x_v) = 0$ for some $x_1 \in S_1, \ldots, x_{v-1} \in S_{v-1}$.

Choose S_v as follows: for any $I = |\alpha_v|^{-1}[k/N, (k + 1)/N] \subset T_v$,

$$S_v \cap I := \frac{1}{|\alpha_v|} \left[\frac{k}{N} + \frac{1 - c_1}{2N}, \frac{k}{N} + \frac{1 + c_1}{2N}\right].$$

Now, we remember that c_1 is bounded above by $\frac{1}{4}$, so it follows that if $x_v \in S_v \cap I$, then x is within $\frac{c_1}{2N} \leq \frac{1}{8N}$ of an odd multiple of $\frac{1}{2N}$. This means that x_v is a distance of at least $\frac{3}{8N}$ from any integer multiple of $\frac{1}{N}$. Thus, by (3.18), $f(x_1, \ldots, x_v)$ is nonzero for $x_1 \in S_1, \ldots, x_v \in S_v$.

We now prove Lemmas 3.3.2 and 3.3.3, which will complete the proof of Proposition 3.3.1. Both of these lemmas will make use of the fact that $\frac{\partial f}{\partial x_v}$ is nonzero on $T_1 \times \cdots \times T_v$.

Lemma 3.3.2 (Lemma 3.2 from [19]). *Let $\mathbb{A}_N$ and f be defined as in Proposition 3.3.1. Then we have that, for any fixed a' in $\mathbb{A}_N$, there are at most M numbers x_v such that $f(a', x_v) = 0$.*

Proof. For any fixed $a' \in \mathbb{A}_N$, we will consider the solutions to $f(a', x_v) = 0$ with $x_v \in J$ for each $J \in \mathcal{J}_M(T_v)$. Since the number of such J is at most

M, we will be done if we can show that there is at most one solution in each such J.

As a matter of fact, this follows directly from Rolle's theorem and the fact that $\frac{\partial f}{\partial x_v}$ is nonzero on $T_1 \times \cdots \times T_v$. If we assume that there exist $x_v^{(1)}, x_v^{(2)} \in J$ such that $f(a', x_v^{(1)}) = f(a', x_v^{(2)}) = 0$, then Rolle's theorem implies that $\frac{\partial f}{\partial x_v}(a', x_v)$ must be equal to zero for some point in J, which contradicts the assumption on f. □

Lemma 3.3.3 (Lemma 3.3 from [19])**.** *Let f, M, and $T_1, \ldots, T_v$ be as in Proposition 3.3.1. Then there exists an integer C_0 depending on f, M, and on $T_1, \ldots, T_v$ such that for the choice of $S_1, \ldots, S_{v-1}$ given in the proof of Proposition 3.3.1*

$$\textit{dist}(x_v, \mathbb{B}) \leq \frac{C_0 c_1}{N^{v-1}}$$

for any x_v such that $f(x) = 0$, where $x' = (x_1, \ldots, x_{v-1}) \in S_1 \times \cdots \times S_{v-1}$.

Proof. Let $\mathbb{J} = J_1 \times \cdots \times J_v = \mathbb{J}' \times J_v \in \prod_{j=1}^{v} \mathcal{J}_M(T_i)$ be a v-dimensional cube of sidelength $\frac{1}{M}$ that contains a point of the zero set of f. Since $\frac{\partial f}{\partial x_v}$ is nonvanishing on $\mathbb{J}$, it follows from the implicit function theorem that exists a $(v-1)$-variate C^1 function $g_{\mathbb{J}}$ defined on $\mathbb{J}'$ and a constant C_0 (which can be chosen to be an integer) such that

$$f(x) = 0, x \in \mathbb{J} \quad \text{implies} \quad x_v = g_{(J)}(x'), \tag{3.19}$$

and

$$|\nabla g_{\mathbb{J}}| \leq \frac{C_0}{\sqrt{v}} \text{ on } \mathbb{J}'. \tag{3.20}$$

Given $x = (x', x_v) \in S_1 \times \cdots \times S_v$ such that $f(x) = 0$, let $\mathcal{J}_x$ denote the v-dimensional $\frac{1}{m}$ cube $\mathbb{J}$ in which x lies (if x lies on the boundary of such cubes, simply select one), and let $\mathbb{I}'_x = I_1 \times \cdots \times I_{v-1} = \prod_{i=1}^{v-1}[a_i, b_i] \in \prod \mathcal{I}_N(J_i, i)$ be the $(v-1)$-dimensional subcube of $\mathbb{J}'_x$ of sidelength $1/N$ containing x'. Then

$$x_v = g_{\mathbb{J}}(x'), \quad a' = (a_1, \cdots, a_{v-1}) \in \mathbb{A}_N,$$

$$g_{\mathbb{J}}(a') \in \mathbb{B}, \quad \text{and} \quad |x' - a'| \leq \frac{c_1\sqrt{v}}{N^{v-1}}.$$

Thus, we have that the distance from x_v to $\mathbb{B}$ is bounded above by $\|\nabla g_{\mathbb{J}}\|_\infty |x' - a'|$. The bound (3.20) implies that $\|\nabla g_{\mathbb{J}}\|_\infty |$ is bounded above by $\frac{C_0}{\sqrt{v}}$, so we have that the distance from x_v to $\mathbb{B}$ is bounded above by $\frac{C_0 c_1}{N^{v-1}}$. □

3.3.2 One Dimension, General Case

Now, our presentation will diverge somewhat from [19].

Instead of directly using Proposition 3.3.1 as the basis for the construction, we will iterate this proposition in order to prove a version that does not require the gradient to be nonvanishing. Proving this proposition now will greatly simplify the construction of the set in Theorem 1.1.1.

We use the usual multi-index notation for derivatives: If $\alpha = (\alpha_1, \ldots, \alpha_v)$ is a multi-index, we define $|\alpha| = \alpha_1 + \cdots + \alpha_v$. For a $C^{|\alpha|}$ function f, we then define

$$\partial^\alpha f = \frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_v}}{\partial x_v^{\alpha_v}} f.$$

Because f is assumed to be $C^{|\alpha|}$, the order of the partial differential operators is irrelevant.

We will outline the assumptions required to state this proposition. Suppose that we have a multi-index α satisfying $|\alpha| = r$, an integer $M \geq 1$, a small constant $c_0 > 0$, compact subsets $T_1, \ldots, T_v \subset [0,1]$, and a C^r function f. We will make the following assumptions:

1. Each T_i is a union of closed intervals of length M^{-1} with disjoint interiors. Let us denote by $\mathcal{J}_M(T_i)$ this collection of intervals. We will consider a function f such that the derivative $\partial^\alpha f$ is nonzero.

2. The interior of T_i is disjoint from the interior of $T_{i'}$ if $i \neq i'$.

3. The partial derivative $\partial^\alpha f$ does not vanish on $T_1 \times \cdots \times T_v$, and is bounded below by c_0 on this set.

Proposition 3.3.4. *Given f, M, α, c_0 and $\mathbb{T} = (T_1, \cdots, T_v)$ satisfying these assumptions, there exist a small rational constant $c_1 > 0$ and an integer N_0 (depending on all these quantities), for which the following conclusions hold.*

There is a sequence of arbitrarily large integers $N \geq N_0$ with $\frac{N}{M}, c_1 N \in \mathbb{N}$ such that for each N in this sequence, one can find compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $J \in \mathcal{J}_M(T_i)$, let us decompose J into closed intervals of length N^{-1} with disjoint interiors and call the resulting collection of intervals $\mathcal{I}_N(J, i)$.

For every $J \in \mathcal{J}_M(T_i)$ *and every* i*, there exists* $\mathcal{I}'_N(J,i) \subseteq \mathcal{I}_N(J,i)$ *with*

$$\#\left(\mathcal{I}'_N(J,i)\right) \geq c_2 \# \left(\mathcal{I}_N(J,i)\right) \tag{3.21}$$

such that for each $I \in \mathcal{I}'_N(J,i)$*,* $|S_i \cap I|$ *is nonempty.* $S_i \cap I$ *need not be an interval; however, it can be written as a union of intervals of length* $c_1 N^{1-v}$ *with disjoint interiors. Here,* $c_2 > 0$ *and may depend on* f, r, v, c_0*, and* M *but not on* N*.*

We lose some control over the structure of the sets S_j in passing from Proposition 3.3.1 to Proposition 3.3.4. However, much of the structure of Proposition 3.3.1 is not necessary for the proof of Theorem 1.1.1.

Given such a function f, we define, for $0 \leq k \leq r$, a sequence of differential operators

$$\mathcal{D}^k = \frac{\partial^{\alpha_k}}{\partial x^{\alpha_k}}$$

that lead to α in the following way: α_{k-1} is obtained by reducing the largest entry of α_k by 1, and leaving the others unchanged. In the case of a tie, we pick one maximal index arbitrarily. Then $|\alpha_k| = k$.

We will prove Proposition 3.3.4 by induction: assuming we have sets $T_1^{(k)} \times \cdots \times T_v^{(k)}$ on which $\mathcal{D}^k f$ is nonvanishing, we apply Proposition 3.3.1 in order to locate $S_1^{(k)}, \ldots, S_v^{(k)}$ on which $\mathcal{D}^{k-1} f$ is nonzero. We then take the sets $S_1^{(k)}, \ldots, S_v^{(k)}$ to be the sets $T_1^{(k-1)}, \ldots, T_v^{(k-1)}$.

Proof of Proposition 3.3.4. The proof proceeds by induction on the variable r. The $r = 1$ case is implied by Proposition 3.3.1.

Now, suppose that $\mathcal{D}^r f = \partial^\alpha f$, and the sets $T_1, \ldots, T_v$, satisfy the conditions of the proposition. We will show that the sets $S_1, \ldots, S_v$ promised by applying Proposition 3.3.1 to the function $f^* = \mathcal{D}^{r-1} f$ satisfy the requirements for $T_1, \ldots, T_v$ in Proposition 3.3.4 for $\partial^\beta f = \mathcal{D}^{r-1} f$ (though not with the same constants), completing the induction.

Accordingly, we define $f^* := \mathcal{D}^{r-1} f$, and check the three assumptions of Proposition 3.3.1. Then

1. Evidently, each T_i can be expressed as a union of intervals of sidelength M^{-1}, by the first assumption in Proposition 3.3.4.

2. The condition that T_i and $T_{i'}$ have disjoint interiors is also clearly implied by the second assumption in Proposition 3.3.4.

3. The third condition in Proposition 3.3.1 implies that $\frac{\partial f^*}{\partial x_{i_0}}$ is nonzero for the index i_0 of the derivative that is taken to get from $\mathcal{D}^{k-1}$ to $\mathcal{D}^k$.

Furthermore, there exists c_0' such that $|\nabla f(x)| \leq (c_0')^{-1}$, because f is r times continuously differentiable, and hence all rth order derivatives of f are continuous and thus bounded on the compact set $T_1 \times \cdots \times T_v$. Then assumption 3 of Proposition 3.3.1 holds for the constant c_0^*, taken to be the minimum of c_0 and c_0'.

Thus we can apply Proposition 3.3.1 to f^*, the sets $T_1, \ldots, T_v$, the constant c_0^*, the constant M, and an appropriately large number N'. In so doing, we arrive at sets $S_1', \ldots, S_v'$ such that $\mathcal{D}^{k-1} f$ is nonzero on $S_1' \times \cdots \times S_v'$, each S_j' is a union of intervals of length $c_1'(N')^{1-v}$ with disjoint interiors, and, for each $J \in \mathcal{J}_M(T_i)$, a family $\mathcal{I}_{N'}'(J,i)$ such that for each $I \in \mathcal{I}_{N'}'(J,i)$, the intersection $S_{i_0}' \cap I$ contains at least one interval of length $c_1'(N')^{1-v}$ (many such intervals if $i = i_0$; one such interval for other values of i).

We will now apply the inductive assumption. We will take the sets $T_1^*, \ldots, T_v^*$ to be $S_1', \ldots, S_v'$ respectively, and take $M^* \geq (c_1')^{-1}(N')^{v-1}$. Let $N \gg N'$ be some value for which the inductive assumption applies. Let $S_1, \ldots, S_v$ be the sets resulting from the application of the inductive assumption, and let c_2^* be the value of c_2 in this application of the inductive assumption. Evidently $f(x_1, \ldots, x_v) \neq 0$ for $x_1 \in S_1, \ldots, x_v \in S_v$.

Decompose $T_1, \ldots, T_v$ into subintervals of length N. We have that for each $J \in J_M(T_i)$, there is a collection $\mathcal{I}_{N'}'(J,i) \subset \mathcal{I}_{N'}(J,i)$ such that $\#\mathcal{I}_{N'}'(J,i) \geq \left(1 - \frac{1}{M}\right) \#\mathcal{I}_{N'}(J,i)$ and such that each element of $\mathcal{I}_{N'}'(J,i)$ contains an interval of length $c_1'(N')^{1-v}$ that is contained in S_i' Furthermore, the inductive assumption implies that each such interval contains $c_2^*(c_1')^{-1}c_1(N')^{v-1}N^{-1}$ intervals of length N that contain at least one subinterval of length $c_1(N)^{1-v}$ in S_i. It therefore follows that a $c_1'\left(1 - \frac{1}{M}\right)(N')^{2-v}c_2^*$ fraction of the intervals of length N^{-1} in J contain an interval of length $c_1(N)^{1-v}$ as desired. The proof is complete because $c_2 := c_1'\left(1 - \frac{1}{M}\right)(N')^{2-v}c_2^*$ does not depend on N. □

3.3.3 Higher Dimensions

For the higher-dimensional case, we do not concern ourselves with situations in which the derivative is singular. Unlike the one-dimensional case, however, we need to make a size assumption on M in order for the proof to succeed. Let $m, n \geq 1$ and $v \geq 3$ satisfy $m \leq n(v-1)$, and let $f : \mathbb{R}^{nv} \to \mathbb{R}^m$ be a C^2 function whose zero set has a nontrivial intersection with $[0,1]^{nv}$. Suppose $M \geq M^*$ is a large integer, C_0, C_1, C_2 are real constants and $T_1, \ldots, T_v \subset [0,1]^n$ are sets with the following properties:

1. Each T_i is expressible as a union of closed disjoint balls of radius $q^{-\mu}$, the collection of which will be called $\mathcal{J}_\mu(T_k)$. The sets T_i and $T_{i'}$ will be disjoint for $i \neq i'$.

2. On $\{x \in T_1 \times \cdots \times T_v : f(x) = 0\}$, the matrix Df is of full rank, with a submatrix B whose determinant is bounded below by C_0, and whose entries are bounded above by C_1.

3. On $[0, \eta]^{nv}$ the matrix norm of the Hessian $D^2 f$ is bounded above by C_2.

We are now ready to state the main proposition in the multidimensional setting. This proposition is a slight modification of Proposition 3.4 from [19].

Proposition 3.3.5 (Proposition 3.4 from [19])**.** *Given f, M, C_0, C_1, and C_2 as above, there exists a rational constant $C_3 > 0$ and an integer N_0 depending on these quantities for which the following conclusions hold. For $N \geq N_0$, set $\ell = C_3 N^{n(1-v)/m}$. If N is such that $\frac{N}{M}$, $1/(\ell N) \in \mathbb{Z}$, then one can find compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that*

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $1 \leq i \leq v$ and $J \in \mathcal{J}_M(T_i)$, let us decompose J into closed axis-parallel cubes of length N^{-1} with disjoint interiors and call the resulting collection of cubes $\mathcal{I}_N(J, i)$. There exists $\mathcal{I}'_N(J, i) \subseteq \mathcal{I}_N(J, i)$ such that

$$S_i \subseteq \bigcup \left\{ I : J \in \mathcal{J}_M(T_i),\ I \in \mathcal{I}'_N(J, i) \right\}.$$

More precisely, for each $I \in \mathcal{I}'_N(J, i)$, the set $S_i \cap I$ is a single axis-parallel cube of sidelength $\ell = C_3 N^{n(1-v)/m}$, provided $i \neq v$. For $i = v$ and $I \in \mathcal{I}'_N(J, v)$, the set $S_v \cap I$ is not necessarily a single cube of sidelength ℓ, but a union of such cubes, with the property that

$$|S_v \cap I| \geq \left(1 - \frac{1}{M}\right) \frac{1}{N^n}. \tag{3.22}$$

(c) The subcollections $\mathcal{I}'_N(J, i)$ of cubes are large subsets of the ambient collection $\mathcal{I}_N(J, i)$, in the sense that for all $1 \leq i \leq v$, $J \in \mathcal{J}_M(T_i)$,

$$\#\big(\mathcal{I}'_N(J, i)\big) \geq \left(1 - \frac{1}{M}\right) \#\big(\mathcal{I}_N(J, i)\big). \tag{3.23}$$

As in the one-dimensional case, the specific dependence of C_3 on the parameter M in the estimates of Proposition 3.3.5 does not impact the Hausdorff dimension obtained in Theorem 1.1.2. The power of N is essential for the Hausdorff dimension bound.

The restriction $m \leq n(v-1)$ is essential for Theorem 1.1.2; otherwise, the theorem could not hold since the claimed Hausdorff dimension $\frac{m}{v-1}$ would be larger than n. This assumption is also used in the proof of Proposition 3.3.5 in order to have $\ell \ll N^{-1}$. In the case $m < n(v-1)$, the value of ℓ, selected to be $\epsilon_0 M^{-R} N^{-n(v-1)/m}$ will be less than $\frac{1}{N}$ if N is sufficiently large depending on ϵ_0 and M; in the case $m = N^{v-1}$, ℓ will be less than $\frac{1}{N}$ provided that M^* is sufficiently large.

The special treatment of x_v is not necessary for the proof; x_v could be replaced with any x_{i_0}.

Proof. Let $Z_f = \{x = (x_1, \ldots, x_v) \in ([0,1]^n)^v : f(x) = 0\}$ be the zero set of the function f. A co-area formula argument can be used to show that Z_f can be covered by at most $C\epsilon^{m-nv}$ cubes of sidelength ϵ for some large constant C that is independent of ϵ; however, we present an alternative proof in Lemma 3.3.6 because this lemma will be convenient in Chapter 5.

We will project Z_f successively onto the coordinates $x_1, x_2, \ldots$, and select the sets S_i so as to avoid the projected zero sets. The main ingredient of this argument is described in Lemma 3.3.7.

Fix $\ell \ll \frac{1}{N}$, which will be specified later. We use $\mathcal{I}_{\alpha^{-1}}(J, i)$ to denote the collection of axis-parallel subcubes of sidelength α that constitute a partition of $J \in \mathcal{J}_M(T_i)$. We will define a collection of bad boxes, $\mathbb{B}_1$, defined as follows:

$$\mathbb{B}_1 = \{Q \in \prod_{i=1}^{v} \mathcal{I}_{\ell^{-1}}(J_i, i) : Q \text{ intersects } Z_f;\ J_i \in J_M(T_i)\}. \tag{3.24}$$

Lemma 3.3.6 establishes that $\#(\mathbb{B}_1) \leq CM^{nv}\ell^{m-nv}$, where C is a constant depending only on the function f and on the value c_0.

We construct $S_1, \ldots, S_v$ as follows. First, we project the boxes in $\mathbb{B}_1$ onto their $(x_2, \ldots, x_v)$ coordinates (each n-dimensional), and use Lemma 3.3.7 with $r = v$, $T = T_1$, $T' = T_2 \times \cdots \times T_v$ and $\mathbb{B} = \mathbb{B}_1$ to arrive at $S_1 \subset T_1$ and a family of $n(v-1)$-dimensional boxes $\mathbb{B}' = \mathbb{B}_2$ satisfying the conclusions of that lemma. S_1, of course, satisfies the conclusions of Part b of Proposition 3.3.5. Lemma 3.3.7 also gives a bound on

$$\#(\mathbb{B}_2) \leq M^{n+1} N^n \ell^n \#(\mathbb{B}_1) \leq CM^{nv+(n+1)} N^n \ell^{m-n(v-1)}$$

and that $f(x) \neq 0$ for any $x = (x_1, x')$ such that $x_1 \in S_1$ and $x' \in T_2 \times \cdots \times T_v$ that is not contained in the cubes that constitute $\mathbb{B}_2$.

We iterate this procedure. At the end of step j, we will have selected $S_1 \subset T_1, \ldots, S_j \subset T_j$, and we will be left with a family $\mathbb{B}_{j+1}$ of cubes of dimension $n(v-j)$ of sidelength ℓ such that

$$\#\mathbb{B}_{j+1} \leq CM^{nv+(n+1)j} N^{jn} \ell^{m-n(v-j)} \tag{3.25}$$

and so that $f(x'', x')$ is nonzero for any $(x_1, \ldots, x_j) \in \prod_{i=1}^{j} S_i$, any $x' \in \prod_{i=j+1}^{v} T_i$, and any x' that avoids the cubes in $\mathbb{B}_{j+1}$. We now apply Lemma 3.3.7 with

$$T = T_{j+1}, \quad T' = T_{j+1} \times \cdots \times T_v, \quad \mathbb{B} = \mathbb{B}_{j+1}$$

to arrive at $S_{j+1} \subset T_{j+1}$ that satisfy the requirements of part b. The lemma also gives $\mathbb{B}' = \mathbb{B}_{j+2}$ of $n(v-j-1)$-dimensional cubes of side length ℓ, whose cardinality obeys (3.25) with j replaced by $j+1$. This allows us to continue the induction.

We use this strategy for $v-1$ steps, ultimately obtaining sets $S_1, \ldots, S_{v-1}$ and a collection $\mathbb{B}_v$ containing at most $CM^{nv+(n+1)(v-1)} N^{n(v-1)} \ell^{m-n}$ cubes of side length ℓ and dimension n contained in T_v. We then define S_v using Lemma 3.3.8, the conclusion of which satisfies both parts of the proposition. □

Lemma 3.3.6. *There exists $M_0(C_0, C_1, C_2) > 0$ such that the following statement holds for all $M \geq M_0$. Let $\mathbb{T}$ be an nv-dimensional closed cube of sidelength M^{-1} and let $f(x_1, \ldots, x_v) : \mathbb{T} \to \mathbb{R}^m$ be a function such that Df has an m-by-m minor that is, in absolute value, at least a constant C_0 on all of $\mathbb{T}$ and whose entries are bounded above in absolute value by a constant C_1. Suppose further that C_2 is an upper bound for the operator norm of the second derivative of f. Let Z_f be the set of $(x_1, \ldots, x_v) \in \mathbb{T}$ such that $f(x_1, \ldots, x_v) = 0$. Subdivide the cube $\mathbb{T}$ into balls of radius ℓ. If ℓ is sufficiently small, then the number of balls that intersect the zero set of f is at most $C_3(M\ell)^{(m-nv)}$ where M_0 and C_3 can depend on C_0, C_1, and C_2 but not on ℓ.*

Proof. Let x_0 be an arbitrary point in $Z_f \cap \mathbb{T}$ (If this set is empty there is nothing to show). If M is large enough depending on C_0, C_1, and C_2, then there exists a fixed submatrix B of Df such that $|\det(B)| \geq C_0$ for all $x \in \mathbb{T}$. Let $(j_1, \ldots, j_m)$ be the indices of the columns of B. Consider the vector space U spanned by e_{j_i}, where the j_ith component of e_{j_1} is equal to 1, and all of the other components of e_{j_i} are equal to zero. Consider points of the form $x_0 + u$, where $u \in U$ and $\|u\| \le M^{-1}$. By the assumption on Df, we have that $f(x_0 + u) = f(x_0) + Df_{x_0}(u) + O(\|u\|^2)$. Here $f(x_0) = 0$, $\|Df_{x_0}u\| > k_0 \|u\|$, where k_0^{-1} is the operator norm of B^{-1}. The implicit constant in the $O(\|u\|^2)$ depends on C_0, C_1, and C_2.

We can estimate k_0 using the adujgate formula for B^{-1}. The operator norm of B^{-1} is bounded above by the sum of the absolute values of the entries of B^{-1}. Each such entry is bounded above by a constant depending on the dimension and on C_0 and C_1, so the same is true for $||B^{-1}||$. Therefore, we have that $\|f(x_0 + u)\| \ge k_0 \|u\| - O(\|u\|^2)$, which is positive if M is large enough.

Let $\ell < M^{-1}$. For a given $x \in Z_f$, consider the set consisting of points $x+U+w$ where w has a zero in each j_i component; i.e. w is in the orthogonal complement $U^{\perp}$ of U. The set of points $x + U + w$ is the ℓ-neighbourhood of $x + U$. Let $x + u + w$ be a point in this slab. We have that

$$f(x + u + w) = f(x) + Df_x(u + w) + O(\|u + w\|^2).$$

This has norm at least $k_0 \|u\| - mC_1 \|w\| + O(\|u + w\|^2)$. Therefore $f(x+u+w)$ is nonzero provided that $\|u\|$ is larger than $\frac{2C_1 m}{k_0} \|w\|$, which will happen as long as $\|u\| \ge \frac{2C_1 m}{k_0}\ell$, and provided that M is sufficiently large that the $O(\|u + w\|^2)$ term has norm smaller than $\frac{k_0}{4} \|u\|$. We make this assumption on M_0. If we subdivide the slab $x + U + w$ into ℓ-cubes, we get that Z_f will only intersect at most $\left(\frac{2C_1 m}{k_0}\right)^m$ cubes of sidelength ℓ in the slab. Taking the union over essentially disjoint parallel slabs covering $\mathbb{T}$, we have that a total of $O\left(\left(\frac{C_1}{k_0}\right)^m (M\ell)^{m-nv}\right)$ cubes of sidelength ℓ that intersect Z_f. $\square$

Fix $2 \le r \le v$ and consider sets $T \subset [0, 1]^n$ and $T' \subset [0, 1]^{n(r-1)}$ expressible as unions of axis-parallel cubes of sidelength M^{-1} and disjoint interiors. We use $\mathcal{J}_M(T)$ and $\mathcal{J}_M(T')$ to denote the collections of these cubes. Given any $J \in \mathcal{J}_M(T)$, we decompose J into axis-parallel cubes of sidelength N^{-1}; the corresponding collection is called $\mathcal{I}_N(J)$. We will also fix a subset $B \subset T \times T'$, a union of a collection $\mathbb{B}$ of cubes of sidelength ℓ. Here M, N, and ℓ are as specified in Proposition 3.3.5. Since $\frac{N}{\ell}$ is taken to be an integer, we may assume that each cube in $\mathcal{B}$ is contained in exactly one cube in $\mathcal{I}_N(J)$.

Lemma 3.3.7 (Lemma 3.5 from [19])**.** *Given T, T', B as above, there exist sets $S \subseteq T$, $B' \subseteq T'$ and a collection of boxes $\mathbb{B}'$ with the following properties:*

(a) The set S is a union of closed axis-parallel cubes of sidelength ℓ and disjoint interiors. More precisely, for every $J \in \mathcal{J}_M(T)$, there exists

$\mathcal{I}'_N(J) \subseteq \mathcal{I}_N(J)$ such that

$$\#(\mathcal{I}'_N(J)) \geq (1 - M^{-1})\#(\mathcal{I}_N(J)),$$

and $S \cap I$ is a single ℓ-cube for each $I \in \mathcal{I}'_N(J)$. For $I \in \mathcal{I}_N(J) \setminus \mathcal{I}'_N(J)$, the interior of the set $S \cap I$ is empty.

(b) The set B' is the union of the ℓ-cubes in $\mathbb{B}'$.

(c) $\#(\mathbb{B}') \leq M^{n+1} N^n \ell^n \#(\mathbb{B})$.

(d) $(S \times T') \cap B \subseteq S \times B'$

Proof. Fix $J \in \mathcal{J}_M(T)$. For $I \in \mathcal{I}_N(J)$, define a slab

$$W_N[I] := \bigcup \{Q = I \times I' \text{for some } I' \in \mathcal{I}_N(J) \text{ for some } J \in \mathcal{J}$$

So a slab is the union of all of the boxes of sidelength $\frac{1}{N}$ whose projection onto the x_1-coordinate is the cube I. We define the wafers $W_{\ell^{-1}}[I]$ to be the union of all cubes of sidelength ℓ that project onto I in x_1-space. Observe that a slab is an essentially disjoint union exactly $N^{-n}\ell^{-n}$ wafers, and the total number of wafers supported by a cube J is $M^{-n}\ell^{-n}$. A wafer is in turn a union of ℓ-cubes.

We will call a wafer $W_{\ell^{-1}}[I]$ good if it contains at most $M^{n+1}\ell^n\#(B)$ boxes of $\mathbb{B}$. By the pigeonhole principle, the fraction of wafers that are bad is at most $\frac{1}{M}$. Now, call a slab good if it contains at least one good wafer. Clearly, at most a $\frac{1}{M}$-fraction of the slabs can be bad. Let us define $\mathcal{I}_N(J)$ as the collection of all cubes I such that the slab $W_N[I]$ is good. For each cube $I \in \mathcal{I}'_N(J)$, we select a cube $I_0 = I_0(I) \subset I$ such that the wafer $W_{\ell^{-1}}[I_0]$ is good. Take S to be the union of all ℓ-cubes $I_0(I)$, with $I \in \mathcal{I}'_N(J)$ and $J \in \mathcal{J}_M(T)$. This covers everything in part (a) of the lemma.

Let B' be the union of the collection $\mathbb{B}'$ of all ℓ-cubes $Q' \subset T'$ such that $Q \times Q' \in \mathbb{B}$ for some ℓ-cube $Q \subset S$. Then (b) and (d) hold by definition. (c) Follows from the good wafer property: for any of the selected cubes $Q \subset S$ the number of cubes Q' such that $Q \times Q' \in \mathbb{B}$ is at most $M^{n+1}\ell^n\#\mathbb{B}$. On the other hand, each Q comes from a distinct slab, so the number of such Q is at most N^n. This gives the bound in part (c). □

When $r = 1$, we need a small variant of this Lemma. It is very similar to Lemma 3.3.7.

Lemma 3.3.8 (Lemma 3.6 from [19])**.** *Fix $\ell \ll N^{-1} \ll M^{-1}$. Let $T \subset [0,1]^n$ be a union of closed axis-parallel cubes of sidelength M^{-1} and disjoint interiors. Let $B \subset T$ be a union of similar cubes with sidelength ℓ. Decompose T into axis-parallel cubes of sidelength N^{-1}, denoting the corresponding collection $\mathbb{T}$. Suppose that*

$$\#\mathbb{B} \leq CM^{nv+(n+1)(v-1)}N^{n(v-1)}\ell^{m-n}$$

with

$$\ell \leq C^{-1/m}M^{-1/m(nv+(n+1)v+1)}N^{-\frac{n(v-1)}{m}}.$$

Then there exist $S \subset T$ and $\mathbb{T}^* \subset \mathbb{T}$ such that

(a) $S \cap B$ is empty.

(b) $\#\mathbb{T}^* \geq (1 - 1/M)\#\mathbb{T}$

(c) S is a union of a large number of ℓ-cubes coming from $\mathbb{T}^*$. More precisely, $|S \cap I| \geq (1 - M^{-1})N^{-n}$ for each $I \in \mathbb{T}^*$.

Proof. Decomposing each cube $I \in \mathbb{T}$ into subcubes of sidelength ℓ, we declare I to be good if it contains at most $M^{n+1}N^{-n}\#\mathbb{B}$ subcubes of $\mathbb{B}$. As in the proof of Lemma 3.3.7, the pigeonhole principle implies that the fraction of bad cubes in $\mathbb{T}$ is at most M^{-1}. We define $\mathbb{T}^*$ to be the collection of good cubes in $\mathbb{T}$, and S to be the union of all the subcubes of sidelength ℓ that are disjoint from B. Then, for every $I \in \mathbb{T}^*$,

$$|I \cap B| \leq M^{n+1}N^{-n}\#\mathbb{B}\ell^n \leq CM^{nv+(n+1)v}N^{n(v-2)}\ell^m \leq M^{-1}N^{-n}.$$

□

3.4 Construction of E

The construction of the set E is similar to Keleti's construction: we will create an appropriate queue, and at each stage the corresponding queue element will tell us which configuration to avoid, and the intervals on which the configuration will be avoided.

3.4.1 Construction

We will construct the set E together with a queue that will keep track of v-tuples of intervals contained in the set E. We will describe the first few steps of the construction and then describe a general step j.

The details of this construction are slightly different from those in [19] in order to simplify the presentation. We will perform the constructions for Theorems 1.1.1 and 1.1.2 together.

Step 0: At the initializing step, we set, in the case of Theorem 1.1.1, for $k = 1, \dots, v$:

$$I_k[0] = \left[(k-1)\frac{\eta}{v}, \frac{k\eta}{v}\right],\ \mathcal{E}_0 = \{I_1[0], \dots, I_v[0]\},\ M_0 = \frac{v}{\eta}.$$

In the case of Theorem 1.1.2, we instead define $\{I_k[0], 1 \le k \le v^n\}$ to be some enumeration of the n-dimensional cubes formed from these v intervals. We also need to take M_0 to be the least common multiple of $\frac{v}{\eta}$ and the value M^* required to apply Proposition 3.3.5 to the function f_1. Let $L_0 = v$ or v^n as is appropriate, and let Σ_0 denote the collection of injections from $\{1, \dots, v\}$ into $\{1, \dots, L_0\}$. We define an ordered queue

$$\mathcal{Q}_0 = \{(1, \sigma, 0) : \sigma \in \Sigma_0\}$$

We order $\mathcal{Q}_0$ lexicographically in σ (viewing σ as a collection of v-tuples taking values in $\{1, \dots, v\}$). Then $(1, \sigma, 0)$ will precede $(1, \sigma', 0)$ if $\sigma < \sigma'$ with respect to this lexicographic ordering.

For any σ, we define the ordered v-tuple of intervals

$$\mathcal{I}_\sigma[0] = (I_{\sigma(1)}[0], \dots, I_{\sigma(v)}[0]).$$

Step 1 Consider the first member of $\mathcal{Q}_0$, which is $(1, \sigma, 0)$. We will apply Proposition 3.3.4 in the case of Theorem 1.1.1, or Proposition 3.3.5 in the case of Theorem 1.1.2, to the function f on the sets $T_i = I_{\sigma_1(i)}$, with $M = M_0$. The conclusion of the appropriate proposition then holds for some constant $d_0 = c_1(M_0, \mathbb{T}) > 0$ and for arbitrarily large integers N_1. In applying Proposition 3.3.4, we also have a constant $e_0 = c_2(M_0, \mathbb{T}) > 0$. We select $N_1 > e^{M_0/d_0 e_0}$. The proposition then ensures the existence of large subsets $S_j \subset T_j$ for $1 \le j \le v$, each of which is a union of cubes of sidelength $\ell_1 = \frac{d_0}{N^{\frac{v-1}{m}}}$ with

$$f_1(x) \neq 0 \text{ for } x = (x_1, \dots, x_v) \in S_1 \times \cdots \times S_v.$$

For any cubes not contained in $T_1, \ldots, T_v$, we retain all cubes of length ℓ_1 contained in these cubes.

These are the basic cubes for the first stage.

We will let $\mathcal{E}_1 = \{I_1[1], I_2[1], \ldots, I_{L_1}[1]\}$ be an enumeration of the first-stage basic cubes, Σ_1 the collection of injective mappings from $\{1, \ldots, v\}$ to $\{1, \ldots, L_1\}$. We view an element of Σ_1 as an ordered v-tuple of distinct indices from $\{1, \ldots, L_1\}$. As before, Σ_1 is arranged lexicographically. Set

$$\mathcal{Q}'_1 = \{(q, \sigma, 1); 1 \leq q \leq 2; \sigma \in \Sigma_1\}.$$

The list $\mathcal{Q}'_1$ is ordered in the following way: $(q, \sigma, 1)$ precedes $(q', \sigma', 1)$ if $\sigma < \sigma'$, and $(q, \sigma, 1)$ precedes $(q', \sigma, 1)$ if $q < q'$. $\mathcal{Q}'_1$ is appended to $\mathcal{Q}_0$ to form the queue $\mathcal{Q}_1$, which concludes the first step.

Step j At the end of step j, we have the following:

- The jth iterate E_j of the construction: a union of jth level basic cubes of length $\ell_j = d_{j-1}/N_j^{v-1}$. Here , $\{d_{j'} : j' < j\}$ is a sequence of small constants obtained as c_1 from applications of Proposition 3.3.4 or 3.3.5, that depends on the collection of functions $\{f_q : q \leq j\}$. Thus, d_j depends only on the parameters from the first j steps of the construction, even though it has no direct bearing on the size of E_j or on the intervals in $\mathcal{E}_j$. The sequence N_j is chosen in order to satisfy

  $$N_j > \exp\left(\prod_{k=1}^{j}\left(\frac{N_k}{e_{k-1}d_k}\right)^R\right) \quad \text{for all } j \geq 1.$$

  for some large constant R. Here, e_{k-1} is the value of c_2 from applying Proposition 3.3.4 or equal to $\left(1 - \frac{1}{M_{k-1}}\right)$ in the case of Proposition 3.3.5.

- The collection of basic cubes $\mathcal{E}_j$ that constitute E_j. This is denoted by $\mathcal{E}_j = \{I_1[j], I_2[j], \ldots, I_{L_j}[j]\}$.

- The queue $\mathcal{Q}_j = \mathcal{Q}_{j-1} \cup \mathcal{Q}'_j$, where

  $$\mathcal{Q}'_j = \{(q, \sigma, j) : 1 \leq q \leq j, \sigma \in \Sigma_j\}.$$

  Here, Σ_j is the collection of all injections from $\{1, \ldots, v\}$ into $\{1, \ldots, L_j\}$. This can also be viewed as the collection of all v-dimensional vectors with distinct entries taking values in

$\{1, \ldots, L_j\}$ and endowed with the lexicographical order. The new list $\mathcal{Q}'_j$ is ordered the same way as described in step 1 and appended to $\mathcal{Q}_{j-1}$. Notice that the number of members in $\mathcal{Q}_j$ is much larger than j.

We also know that $f_q(x)$ is nonzero for appropriate choices of q and x. Given any 3-tuple of the form (q, σ, j), we know from the application of Proposition 3.3.4 or 3.3.5 that $f_q(x)$ does not vanish for $x_1 \in I_{\sigma(1)}[j], \ldots, x_j \in I_{\sigma(v)}[j]$.

Now, consider the $(j+1)$st entry of the queue $\mathcal{Q}_j$, which is denoted by (q_0, σ_0, j'). We would like to apply Proposition 3.3.4 or 3.3.5 straightaway, to the function f_{q_0} with $T_1 = I_{\sigma(1)}[j'] \cap E_j, \ldots, T_v = I_{\sigma(v)}[j'] \cap E_j$, and with $M^{-1} = \ell_j$. This will work for the case of Proposition 3.3.4, but there is a problem in trying to apply Proposition 3.3.5: ℓ^{-1} may not be larger than the quantity M^* appearing in the statement of that proposition. Thus we split the cubes of $\mathcal{E}_j$ into sub-cubes of sidelength M_j where $M_j = \max(M^*, \ell_j^{-1})$. This does not modify the sets $T_1, \ldots, T_v$, but changes the way these sets are partitioned into smaller cubes.

After this step, we can apply Proposition 3.3.4 or 3.3.5. We obtain a collection of $\mathcal{E}_{j+1}$ of $(j+1)st$ basic cubes of side length $\ell_{j+1} = \frac{d_j}{N_{j+1}^{\frac{n(v-1)}{m}}}$. For each cube of side length M_j that is not contained in $T_1, \ldots, T_v$, we partition the cubes into cubes of sidelength ℓ_{j+1} and retain all of the cubes. This collection of cubes, $\mathcal{E}_{j+1} = \{I_1[j+1], \ldots, I_{L_{j+1}}[j+1]\}$, will be the collection of stage $j+1$ basic cubes.

We now use these newly constructed basic cubes to form the queue $\mathcal{Q}'_{j+1}$: The elements of $\mathcal{Q}'_{j+1}$ are triples of the form $(q, \sigma, j+1)$, where $1 \leq q \leq j+1$, and $\sigma \in \Sigma_{j+1}$, the collection of injective functions from $\{1, \ldots, v\}$ into $\{1, \ldots, L_{j+1}\}$. Append $\mathcal{Q}'_{j+1}$ to $\mathcal{Q}_j$ to form the queue $\mathcal{Q}_{j+1}$. This concludes step j of the construction.

3.4.2 Nonexistence of Solutions

Fix $q \geq 1$ and a tuple $(x_1, \ldots, x_v)$ of distinct points in E. Since $\ell_j \to 0$, there is some j' for which the points $x_1, \ldots, x_v$ are $\ell_{j'}$-separated. Then there exists some $j' \geq q$ in the construction of E such that these points lie in distinct basic cubes $E_1, \ldots, E_v$ in $\mathcal{E}_{j'}$. For an appropriate j, the jth element of of the queue will be (q, σ, j'), where σ is such that $I_{\sigma(1)}[j'], \ldots, I_{\sigma(v)}[j']$. It follows from the conclusion of Proposition 3.3.4 or 3.3.5 that there are no solutions to $f_q(y_1, \ldots, y_v) = 0$ with $y_1 \in E_1, \ldots, y_v \in E_v$. Thus $f(x_1, \ldots, x_v) \neq 0$.

3.4.3 Hausdorff Dimension of E

We will use the version of Frostman's lemma presented as Lemma 2.3.1 in order to determine the Hausdorff dimension of E. Any ball can be covered by a cube of side length equal to the diameter, and that any cube can be covered by a finite number of balls (which may depend on the dimension n) whose diameter is equal to the side length of a given cube, so Lemma 2.3.1 is just as effective if cubes are considered instead of spheres.

We therefore aim to construct a probability measure μ on E with the property that for every $\epsilon > 0$, there exists $C_\epsilon > 0$ such that

$$\mu(I) \leq C_\epsilon l(I)^{\frac{m}{v-1}-\epsilon}. \tag{3.26}$$

Here, $l(I)$ denotes the side length of the cube I.

Let us recall that $\mathcal{E}_j$ denotes the collection of all basic cubes with a side length of ℓ_j at step j. We decompose each cube $\mathcal{E}_j$ into subcubes of length N_j^{-1}, and let $\mathcal{F}_{j+1}$ denote the collection of such that contain a cube in $\mathcal{E}_{j+1}$. Let F_{j+1} be the union of the cubes in $\mathcal{F}_{j+1}$. We define a sequence of measures μ_j, ν_j on the sets E_j, F_j defined recursively.

We begin by defining μ_0 on E_0 to be the uniform measure on $[0, \eta]^n$. Given a measure μ_j supported on the set E_j, we define ν_j to be the measure supported on F_{j+1} defined by evenly splitting the measure μ_j of each cube in $\mathcal{E}_j$ among its children in $\mathcal{F}_{j+1}$. Given ν_j, the measure μ_j will be supported on E_j and will be defined by evenly splitting the measure ν_j of each cube in $\mathcal{F}_j$ among its children in $\mathcal{E}_j$. It follows from the mass distribution principle that the measures μ_j have a weak limit μ. We claim that μ obeys the requirement (3.26).

The proof of this claim depends on the following proposition.

Proposition 3.4.1 (Proposition 4.1 from [19]). *Let $K \in \mathcal{E}_j, J \in \mathcal{F}_{j+1}$ with $J \subset K$. Then*

(a)

$$\mu(K)/|K| \leq \mu(J)/|J| \leq e_j^{-1}\mu(K)/|K|.$$

(b)

$$\mu(J) \leq A_j|J|, \quad \textit{where } A_j = \prod_{k=1}^{j} e_k^{-1}(\ell_k N_k)^{-n}.$$

Proof. We first prove Part (a). Each $K \in \mathcal{E}_j$ is decomposed into $(M_{j+1}\ell_j)^n$ subcubes of length M_{j+1}^{-1}. Each of these subcubes is further split into

$\left(\frac{N_{j+1}}{M_{j+1}}\right)^n$ subcubes of sidelength N_{j+1}^{-1}. Propositions 3.3.4 and 3.3.5 assert that at least an e_j-fraction of each of these subcubes contain a cube from $\mathcal{E}_{j+1}$ and hence lie in $\mathcal{F}_{j+1}$. Thus, the number of descendants $J \in \mathcal{F}_{j+1}$ of a given cube $K \in \mathcal{E}_j$ is therefore at most $(\ell_j N_{j+1})^n$ and at least $e_j(\ell_j N_{j+1})^n = e_j|K|/|J|$. Since $\mu(K)$ is evenly distributed among such J, part (a) follows.

We prove Part (b) by applying Part (a) iteratively. Suppose that $\bar{J}$ is the cube in $\mathcal{F}_j$ that contains K. Then

$$\frac{\mu(J)}{|J|} \leq e_j^{-1} \frac{\mu(K)}{|K|} \leq e_j^{-1} \frac{\mu(\bar{J})}{K} = \frac{e_j^{-1}|\bar{J}|}{|K|} \frac{\mu(\bar{J})}{|\bar{J}|} = \frac{e_j^{-1}}{(\ell_j N_j)^n} \frac{\mu(\bar{J})}{|\bar{J}|}.$$

□

Now, we will apply Proposition 3.4.1 to prove (3.26). Suppose that I is a cube with sidelength $l(I)$ between ℓ_{j+1} and ℓ_j. There are two possibilities that will be considered: the first case is the one for which

$$N_{j+1}^{-1} \leq l(I) \leq \ell_j$$

and the second case is the one for which

$$\ell_{j+1} \leq l(I) \leq N_{j+1}^{-1}.$$

In the first case, I can be covered by at most $C|I|N_{j+1}^n$ cubes of sidelength $\frac{1}{N_{j+1}}$. A priori, all of these cubes could be in $\mathcal{F}_{j+1}$. If J is a generic element of $\mathcal{F}_{j+1}$, we obtain from Proposition 3.4.1 that

$$\begin{aligned}\mu(I) &\leq C|I|N_{j+1}^n \mu(J) \leq C|I|N_{j+1}^n A_j|J| \leq CA_j|I| \\ &\leq C\frac{e_j^{-1}A_{j-1}}{(\ell_j N_j)^n}|I| \leq CA_{j-1}e_j^{-1}d_{j-1}^{-\frac{m}{v-1}}\ell_j^{\frac{m}{v-1}-n}|I| \\ &\leq C_\epsilon \ell_j^{\frac{m}{v-1}-n-\epsilon}|I| \leq C_\epsilon l(I)^{\frac{m}{v-1}-\epsilon}.\end{aligned}$$

Here, we used the growth rate of the N_j, together with the definition of ℓ_j.

Next, we will consider the case in which $\ell_{j+1} \leq l(I) \leq N_{j+1}^{-1}$. If $\mu(I) > 0$, the cube I intersects at least one cube J in $\mathcal{F}_{j+1}$ in which case it is contained in the union of at most $(3^n - 1)$ cubes of the same dimension adjacent to it. Proposition 3.4.1 then yields that

$$\begin{aligned}\mu(I) &\leq C_n\mu(J) \leq C_n A_j|J| = C_n A_j N_{j+1}^{-n} \\ &= C_n A_j d_j^{-\frac{m}{v-1}} \ell_{j+1}^{\frac{m}{v-1}} \leq C_\epsilon \ell_{j+1}^{\frac{m}{v-1}-\epsilon} \leq C_\epsilon l(I)^{\frac{m}{v-1}-\epsilon},\end{aligned}$$

applying the growth rate of the N_j and the definition of ℓ_j, as before. This proves the inequality (3.26).

3.4.4 Minkowski Dimension of E

We would like to show that E has Minkowski dimension n. In order to show this, it is enough to show that for any ℓ we have

$$\mathcal{N}_\ell(E) \geq c_\epsilon \ell^{-n+\epsilon} \quad \text{for any } 0 < \ell \ll 1.$$

Here, $\mathcal{N}_\ell(A)$ refers to the minimum number of closed cubes of sidelength ℓ required to cover A. Given $0 < \ell \ll 1$, we first fix the index j such that $\ell_j \leq \ell < \ell_{j-1}$. Because it is enough to show this for small values of ℓ, we may assume j is as large as necessary.

If j is sufficiently large, then there exists a cube I in $\mathcal{E}_{j-2}$ such that I is not contained in any of the sets $T_1^{(j-1)}, \ldots, T_v^{(j-1)}$ or $T_1^{(j)}, \ldots, T_v^{(j)}$ that play the role of $T_1, \ldots, T_v$ at step $j-1$ or step j of the construction of E. By construction, all of the cubes of sidelength ℓ_j occurring from the appropriate partition of I are retained as elements of $\mathcal{E}_j$. There are $\ell_{j-2}^n \ell_j^{-n}$ such boxes. Furthermore, each element of $\mathcal{E}_j$ intersects E.

A box of sidelength ℓ such that $\ell_j \leq \ell < \ell_{j-1}$ can only intersect at most a constant times $\ell^n \ell_j^{-n}$ of the elements of $\mathcal{E}_j$. Therefore, we require at least $(\ell_{j-2}^n \ell_j^{-n}) \cdot (\ell^{-n} \ell_j^n) = \ell_{j-2}^n \cdot \ell^{-n}$ boxes of sidelength ℓ to cover the set E. By construction, this is at least $\ell^{-n+\epsilon}$, establishing the desired bound for $\mathcal{N}_\ell(E)$.

3.5 Simultaneous Avoidance

We will now prove Theorem 1.1.3. This is also a Cantor-like set. For this construction, we will not need to use a queue as in the proofs of Theorems 1.1.1 or 1.1.2. The construction will instead proceed in the following way: we will begin with an interval $E_0 = [0, \eta]$ for a small constant η and retain two small subintervals of this original interval. These two subintervals will form the set E_1. We then retain two small subintervals of each constituent interval of E_1 in order to form the set E_2. The set E_j will be composed of 2^j intervals, and we will retain two small subintervals from each such interval in order to form the set E_{j+1}.

Proposition 3.5.2 will describe the procedure for choosing the subintervals of E_j to be retained at each stage. This proposition will follow by iterating Lemma 3.5.1.

Let $\alpha \in \mathbb{R}^v$ be as in the statement of Theorem 1.1.3, and let $\mathfrak{C}$ be a nonempty proper subset of the index set $\{1, 2, \ldots, v\}$. Let $\delta > 0$. Consider disjoint intervals $[a_1, b_1]$ and $[a_2, b_2]$ of length λ, with $a_1 < b_1 \leq a_2 < b_2$.

We define two quantities ϵ_{left} and ϵ_{right} depending on $\mathfrak{C}, a_1, b_1, a_2, b_2$, and δ as follows.

$$\begin{aligned}\epsilon_{\text{left}} &:= \sup \epsilon : \\ &\qquad |\sum_{j=1}^{v} \alpha_j z_j| \geq \delta\lambda \text{ for } \begin{cases} z_j \in [a_1, a_1 + \epsilon\lambda] \text{ for all } j \notin \mathfrak{C} \\ z_j \in [a_2, a_2 + \epsilon\lambda] \text{ for all } j \in \mathfrak{C}. \end{cases} \qquad (3.27) \\ \epsilon_{\text{right}} &:= \sup \epsilon : \\ &\qquad |\sum_{j=1}^{v} \alpha_j z_j| \geq \delta\lambda \text{ for } \begin{cases} z_j \in [a_1, a_1 + \epsilon\lambda] \text{ for all } j \notin \mathfrak{C} \\ z_j \in [b_2 - \epsilon\lambda, b_2] \text{ for all } j \in \mathfrak{C}. \end{cases} \qquad (3.28)\end{aligned}$$

Lemma 3.5.1 (Lemma 5.1 from [19])**.** *Given any $\alpha \in \mathbb{R}^v$ as in Theorem 1.1.3, there exists $\delta_0 > 0$ depending only on α such that for any $\lambda > 0$ and any choice of intervals $\mathcal{J}_1 = [a_1, b_1]$ and $\mathcal{J}_2 = [a_2, b_2]$ of equal length λ with $a_1 < b_1 \leq a_2 < b_2$, the following property holds. For any $\delta < \delta_0$, there exists $\epsilon_0 = \epsilon_0(\mathfrak{C}, \delta)$ that does not depend on a_1, a_2, b_1, b_2, or λ such that* $\max(\epsilon_{left}, \epsilon_{right}) \geq \epsilon_0$.

In particular, there exist subintervals $\widehat{\mathcal{J}_1} \subset J_1$,and $\widehat{\mathcal{J}_2} \subset \mathcal{J}_2$ with $|\widehat{\mathcal{J}_1}| = |\widehat{\mathcal{J}_2}| = \epsilon_0\lambda$ and $dist(\widehat{\mathcal{J}_1}, \widehat{\mathcal{J}_2}) \geq (1 - \epsilon_0)\lambda$ such that

$$|\alpha \cdot x| \geq \delta\lambda \quad \text{for all } x \in \mathbb{R}^v \text{ such that} \begin{cases} x_j \in \widehat{\mathcal{J}_1} & \text{for } j \notin \mathfrak{C}, \\ x_j \in \widehat{\mathcal{J}_2} & \text{for } j \in \mathfrak{C}. \end{cases}$$

Proof. Set $g(y) = \sum_j \alpha_j y_j$, and consider $g(z^*)$, where $z^* = (z_1^*, \dots, z_v^*)$ is defined to be the v-dimensional vector with $z_j^* = a_1$ if $j \notin \mathfrak{C}$ and $z_j^* = a_2$ if $j \in \mathfrak{C}$. Setting $C^* = \sum_j |\alpha_j|$, we have

$$|g(z) - g(z^*)| \leq C^*\epsilon\lambda \quad \text{whenever } z_j - z_j^*| \leq \epsilon\lambda, 1 \leq j \leq v. \qquad (3.29)$$

We will split into two cases depending on the value of $g(z^*)$.

If $|g(z^*)| > (\delta + \epsilon_0 C^*)\lambda$, then (3.29)) implies that $|g(z)| \geq \delta\lambda$ for any $z = (z_1, \dots, z_v)$ with $z_j \in [a_1, a_1 + \epsilon_0\lambda]$ for $j \notin \mathfrak{C}$ and $z_j \in [a_2, a_2 + \epsilon_0\lambda]$ for $j \in \mathfrak{C}$. Thus $\epsilon_{\text{left}} \geq \epsilon_0$, and the conclusion of the lemma holds with $\widehat{\mathcal{J}_1} = [a_1, a_1 + \epsilon_0\lambda]$, and $\widehat{\mathcal{J}_2} = [a_2, a_2 + \epsilon\lambda]$.

On the other hand, if $|g(z^*)| \leq \delta + \epsilon_0 C^*\lambda$, let $\widehat{z} = (\widehat{z}_1, \dots, \widehat{z}_v)$ be the v-dimensional vector with $\widehat{z}_j = a_1$ if $j \notin \mathfrak{C}$. Then, we have that $g(\widehat{z}) = g(z^*) + \alpha \cdot (\widehat{z} - z^*) = g(z^*) \pm (b_2 - a_2)C_0 = g(z^*) \pm \lambda C_0$, where $C_0 = \left|\sum_{j \in \mathfrak{C}} \alpha_j\right|$. C_0 is nonzero by the assumptions in Theorem 1.1.3. So, if z is such that $z_j \in [a_1, a_1 + \epsilon_0\lambda]$ for $j \notin \mathfrak{C}$ and $z_j \in [b_2 - \epsilon_0\lambda, b_2]$ if $j \in \mathfrak{C}$, then we can use

(3.29) to obtain the estimate

$$\begin{aligned}|g(z)| \geq |g(\widehat{z})| - |\alpha\cdot(z-\widehat{z})| &\geq |C_0\lambda \pm g(z^*)| - C^*\epsilon_0\lambda \\ &\geq C_0\lambda - (\delta + C^*\epsilon_0)\lambda - C^*\epsilon_0\lambda \geq C_0\lambda - (\delta + 2\epsilon_0 C^*)\lambda,\end{aligned}$$

, which is greater than or equal to $\delta\lambda$ provided that $\delta < C_0/2 =: \delta_0$ and $\epsilon_0 \leq (C_0 - 2\delta)/(2C^*)$. One has $\epsilon_{\text{right}} \geq \epsilon_0$ for this choice of ϵ_0, with the conclusion of the lemma verified for $\widehat{\mathfrak{I}}_1 = [a_1, a_1 + \epsilon_0\lambda]$, $\widehat{\mathfrak{I}}_2 = [b_2 - \epsilon_0\lambda, b_2]$. □

We will now present an illustrative example: we will discuss the case when $\alpha = (1, -2, 1)$, which is relevant to Example 3.2.6. We will consider the case where $\mathfrak{C}$ is equal to $\{3\}$. We will obtain bounds on both ϵ_{left} and ϵ_{right}. Note that $\alpha \cdot (x_1, x_2, x_3)$ is zero precisely when x_1, x_2, and x_3 are in arithmetic progression. For $x_1, x_2 \in [a_1, a_1 + \epsilon\lambda]$, and $x_3 \in [a_2, a_2 + \epsilon\lambda]$, it is easy to see that

$$x_1 - x_2 + x_3 \geq a_1 + a_2 - 2(a_1 + \epsilon\lambda = a_2 - a_1 - 2\epsilon\lambda \geq (1 - 2\epsilon)\lambda.$$

Therefore, we can select $\epsilon_{\text{left}} = \frac{1-\delta}{2}$ for this choice of α, and for any a_1, a_2, b_1, and b_2.

If $x_1, x_2 \in [a_1, a_1 + \epsilon\lambda]$, and $x_3 \in [b_2 - \epsilon\lambda, b_2]$, then

$$x_1 - 2x_2 + x_3 \geq a_1 + b_2 - \epsilon\lambda - 2(a_1 + \epsilon\lambda) = b_2 - a_1 - 3\epsilon\lambda$$

Therefore $\epsilon_{\text{right}} = \frac{2-\delta}{3}$.

The bound on ϵ_0 obtained in the statement of Lemma 3.5.1 may not be optimal for a specific α because the signs of the components of α are not taken into account.

Proposition 3.5.2 (Proposition 5.2 from [19]). *Given any $\alpha \in \mathbb{R}^v$ satisfying the hypotheses of Theorem 1.1.3, there exist fixed small constants $0 < \epsilon < 3/4$ and $\delta(\epsilon) > 0$ depending on α with the following property. Let I be any interval say of length ℓ, and let I_1 and I_2 denote the two halves of I. Then one can find subintervals I_1' and I_2' of I_1 and I_2 of length $\epsilon\ell$ such that*

$$|\alpha\cdot x| \geq \delta\ell \text{ for every sufficiently small } \delta \leq \delta(\epsilon),$$

and for any choice of $x_1, x_2, \ldots, x_v \in I_1' \cup I_2'$, not all of which are in I_i' for a single $i = 1, 2$. The subintervals I_1' and I_2' are separated by at least $\ell/4$.

Proof. Let $\{\mathfrak{C}_1, \dots, \mathfrak{C}_R\}$ be an enumeration of the nonempty proper subsets of $\{1, \dots, v\}$. We will iteratively apply Lemma 3.5.1 for each of these choices of $\mathfrak{C}$. Given any $x = (x_1, \dots, x_v)$ such that $x_j \in I$ for all j, with not all x_j in I_1 and not all x_j in I_2, there exists $1 \leq m \leq R$ such that $j \in \mathfrak{C}_m$ if and only if $x_j \in I_2$. Set

$$C_m := \left| \sum_{j \in \mathfrak{C}_m} \alpha_j \right| \quad \text{and} \quad \delta_0 = \frac{1}{2} \min(C_1, \dots, C_R).$$

With these choices, Lemma 3.5.1 can be applied for any $\delta < \delta_0$ and any $\mathfrak{C} = \mathfrak{C}_m, 1 \leq m \leq R$.

We will start with I_1 and I_2 and apply Lemma 3.5.1 with $\mathfrak{C} = \mathfrak{C}_1$, $\mathcal{J}_1 = I_1$, $\mathcal{J}_2 = I_2$, and $\lambda = \ell/2$. For a small but fixed $\delta_1 > 0$ with $2\delta_1 \leq \delta_0$, this gives a constant $\epsilon_1 = \epsilon_0(\mathfrak{C}_1, 2\delta_1) > 0$ and two subintervals $I_1^{(1)} \subset I_1$ and $I_2^{(1)} \subset I_2$ of length $\epsilon_1 \ell/2$ obeying the conclusions of the lemma. Without loss of generality, we can assume that $\epsilon_1 \leq \frac{1}{2}$, so that

$$\operatorname{dist}(I_1^{(1)}, I_2^{(1)}) \geq (1 - \epsilon_1)\frac{\ell}{2} \geq \frac{\ell}{4}. \tag{3.30}$$

We apply this procedure recursively. Let $2 \leq k \leq R$, with the same value for δ_1, and

$$\mathfrak{C} = \mathfrak{C}_k, \mathcal{J}_1 = I_1^{(k-1)}, \mathcal{J}_2 = I_2^{(k-1)}, \lambda = \epsilon_1 \cdots \epsilon_{k-1}\ell/2$$

After the kth step, this yields a constant $\epsilon_k = \epsilon_0(\mathfrak{C}_k, 2\delta)$ and subintervals $I_1^{(k)} \subset I_1^{(k-1)} \subset \cdots \subset I_1$, $I_2^{(k)} \subset I_2^{(k-1)} \subset I_2$, each of length $\epsilon_1 \cdots \epsilon_k \ell/2$ such that, for any $m \leq k$:

$$|\alpha \cdot x| \geq \delta_1 \epsilon_1 \cdots \epsilon_{k-1}\ell \text{ for all } x \text{ such that } \begin{cases} x_j \in I_1^{(k)} & \text{for } j \notin \mathfrak{C}_m \\ x_j \in I_2^{(k)} \text{for } j \in \mathfrak{C}_m \end{cases}$$

This establishes the conclusion of Proposition 3.5.2 for

$$I_1' = I_1^{(R)}, \quad I_2' = I_2^{(R)}, \quad \epsilon = \frac{1}{2}\prod_{k=1}^{R} \epsilon_k, \quad \text{and} \quad \delta(\epsilon) = \delta_1 \epsilon_1 \cdots \epsilon_{R-1}.$$

The separation condition follows from the first application of in 3.5.1 and the fact that $I_1' \subset I_1^{(1)}$ and $I_2' \subset I_2^{(1)}$. □

We would again like to point out what happens in the case of Example 3.2.6. In particular, this is the case in which $\alpha = (1, -2, 1)$. Recall that $\alpha \cdot (x_1, x_2, x_3) = 0$ whenever $x_2 - x_1 = x_3 - x_2$. However, notice that in any interval $[a, a + \ell]$, we can consider the intervals $I_1' = [a, a + (1 - \delta)\ell/3]$ and $I_2' = [a + \ell - (1 - \delta)\ell/3, a + \ell]$. It is easily seen that these intervals meet the requirements of Proposition 3.5.2, and therefore optimal choice for ϵ is greater than or equal to $(1 - \delta)/3$.

In general, we have the estimate

$$\epsilon \geq \prod_{m=1}^{R} \frac{(C_m - 2\delta_1)}{(2C^*)}. \tag{3.31}$$

Here C^* is defined as $\sum_{j=1}^{v} |\alpha_j|$. We are now ready to prove Theorem 1.1.3.

Proof of Theorem 1.1.3. Let ϵ and $\delta = \delta(\epsilon)$ be the positive α-dependent constants given by Proposition 3.5.2. We will continue to use the notation $g(x_1, \dots, x_v) = \sum_{j=1}^{v} \alpha_j x_j$.

We will begin with the interval $[0, \eta]$, where the positive constant $0 < \eta \ll 1$ is chosen so that $2Kv\eta < \delta$ (Here, K is the constant in the statement of Theorem 1.1.3. Applying Proposition 3.5.2 with $I = E_0$, we will arrive at intervals $I_1' =: J_1 \subset [0, \eta/2]$ and $I_2' =: J_2 \subset [\eta/2, \eta]$ of length $\ell_1 = \epsilon\eta$ that obey its conclusions. Let $E_1 = J_1 \cup J_2$. In general, if E_j is a disjoint union of 2^j basic intervals of length $\ell_j = \epsilon^j \eta$,t hen at step $(j + 1)$, we apply Proposition 3.5.2 in order to arrive at two further subintervals of length $\ell_{j+1} := \epsilon\ell_j = \epsilon^{j+1}\eta$, and separated by a distance of at least $\ell_j/4$. The union of the resulting 2^{j+1} intervals forms the set E_{j+1}.

We now define $E = \bigcap_{j=1}^{\infty} E_j$. We will show, for f as in the statement of Theorem 1.1.3, and for $x_1, \dots, x_v \in E$ not all identical, that $f(x_1, \dots, x_v) \neq 0$. For any such choice of $x_1, \dots, x_v$, there exists a largest index j such that $x_1, \dots, x_v$ lie in the same basic interval I in E_j. This means that if I_1' and I_2' are the two subintervals of I generated by Proposition 3.5.2, then $x_1, \dots, x_v$ lie in $I_1' \cup I_2'$, but not all of $x_1, \dots, x_v$ lie in the same interval I_1' or I_2'. Therefore, the conclusion of Proposition 3.5.2 implies that $|g(x)| \geq \delta\ell_j$. But because $|f(x) - g(x)| \leq Kv\ell_j^2$, and by the fact that $2Kv\eta < \delta$, it follows that $|f(x)| \geq \frac{\delta\ell_j}{2}$ for $\ell_j < \eta$.

The only remaining task is to compute the Hausdorff dimension of E. The $(j + 1)$st step of the construction generates exactly two children from each parent. We define μ_j to be the measure on E_j that is evenly spread about the intervals in E_j. It is clear that μ_j has a weak limit μ. We will show that μ is a Frostman measure on E.

Consider an interval I of length $\ell < \eta$ that intersects the set E. We select j such that $\ell_{j+1} \le \ell \le \ell_j$. An interval of length ℓ can only intersect at most 2 constituent intervals of E_j and at most $\frac{\ell}{\ell_{j+1}}+1$ constituent intervals of E_{j+1}. Thus $\mu_{j+1}(\ell)$ is bounded above by $2^{-j-1} \cdot \left(\frac{\ell}{\ell_{j+1}} + 1\right) \le 2^{-j-1} \cdot (\epsilon^{-1} + 1)$.

Now we consider $\mu_{j+k}(I)$ for $k > 1$. Recall that I intersects at most $\frac{\ell}{\ell_{j+1}} = \epsilon^{-1} + 1$ of the constituent intervals of E_{j+1}. Because each interval of E_{j+1} has exactly 2^{k-1} children in E_{j+k}, it follows that I intersects at most $2^{k-1}\left(\epsilon^{-1}+1\right)$ constituent intervals of E_{j+k}. Furthermore, each constituent interval of E_{j+k} has μ_{j+k}-measure equal to 2^{-j-k}. Therefore, the μ_{j+k}-measure of I is at most $2^{-j-k} \cdot 2^{k-1} \cdot \left(\epsilon^{-1}+1\right)$. This is equal to $2^{-j-1} \cdot (\epsilon^{-1}+1)$.

Therefore, it follows that for I satisfying $\eta\epsilon^{j+1} \le |I| < \eta\epsilon^j$, we have that $\mu(I) \ge 2^{-(j+1)}\left(\epsilon^{-1}+1\right)$. Therefore, $\mu(I)$ is at least $C_\epsilon 2^{-j} = C_\epsilon |I|^{-\frac{\log 2}{\log \epsilon}}$, which, together with Lemma 2.3.1, implies that E has Hausdorff dimension at least $\frac{\log 2}{-\log \epsilon}$. □

Notice that this proof will also succeed if the condition 1.4 in Theorem 1.1.3 is weakened to $|G(x)| \le K \sum_{j=2}^{v} (x_j - x_1)^{1+\epsilon}$. for any $\epsilon > 0$.

We will once again consider the example $\alpha = (1, -2, 1)$ in order to complete the Hausdorff dimension calculation for Example 3.2.6.

Let δ_j be the sequence $\delta_j = \frac{1}{j+C}$ for some large constant C. (The point is that δ_j is a sequence that slowly decreases to zero. It follows from the discussion following the proof of Proposition 3.5.2 that $\epsilon(\delta_j) = \epsilon_j$ can be chosen as $(1-\delta_j)/3$. We will now use the same construction as in the proof of Theorem 1.1.3, but instead of using a fixed δ, we will use the parameter δ_j at step j at step j instead of using a fixed δ for the entire proof.

The following consequences are immediate:

$$\ell_j = \epsilon_1 \cdots \epsilon_j \eta \quad \text{so that} \quad \ell_j \le \frac{C\eta 3^{-j}}{j+C}.$$

$$|g(x)| \ge \delta_j \ell_j \quad \text{and} \quad |f(x) - g(x)| \le Kv\ell_j^2 \text{ so that}$$

$$|f(x)| \ge (\delta_j - Kv\ell_j)\ell_j \ge \left(\frac{1}{j+C} - \frac{Kv\eta C}{j+C} 3^{-j}\right)\ell_j > 0$$

when x is such that all of the components of x lie in the same constituent interval of E_j but not of E_{j+1}. Furthermore, an argument similar to the one in the proof of Theorem 1.1.3 shows that the Hausdorff dimension of E is bounded from below by

$$\lim_{j\to\infty} \frac{\log(2^j)}{-\log(2\ell_j)} = \lim_{j\to\infty} \frac{\log(2^j)}{-\log\left(3^{-j}\eta\prod_{k=1}^{j}(1-\delta_k)/2\right)} = \frac{\log 2}{\log 3}.$$

where the last limit follows from the slow decay of the δ_j.

Chapter 4

Background on Local fields

4.1 Examples

We will present two examples of non-archimedean local fields. The discussion of non-archimedean local fields in this thesis will be primarily limited to these two examples. The first such example will be the field $\mathbb{Q}_p$, known as the p-adic numbers.

Each $x \in \mathbb{Z}$ has a finite base-p expansion

$$\sum_{j=0}^{\infty} x_j p^j$$

where only finitely many x_j are nonzero. If $x \neq 0$, we define $|x|_p$ to be p^{-j}, where x_j is the lowest-degree nonzero term in the expansion. If we take the completion of $\mathbb{Z}$ with respect to this absolute value, we get the ring of elements of the form

$$\sum_{j=0}^{\infty} x_j p^j.$$

This ring is called the **ring of p-adic integers**, denoted $\mathbb{Z}_p$. This ring is equipped with an absolute value defined as follows: $|x|_p = p^{-M}$ if x_M is nonzero and $x_j = 0$ for all $j < M$, and $|0|_p = 0$. Any element of $\mathbb{Z}_p$ with absolute value equal to 1 has a multiplicative inverse in $\mathbb{Z}_p$. Therefore, $\mathbb{Z}_p$ contains every rational number $\frac{r}{q}$ whose denominator q is relatively prime to p. This is a compact abelian group under addition.

$\mathbb{Z}_p$ has a unique prime ideal $p\mathbb{Z}_p$, generated by the element p. Furthermore every ideal of $\mathbb{Z}_p$ is a power of this prime ideal. It therefore follows that each ideal of $\mathbb{Z}_p$ is generated by a power p^k and therefore $\mathbb{Z}_p$ is a principal ideal domain. A principal ideal domain with a unique prime ideal is called a **discrete valuation ring**.

The field of fractions of $\mathbb{Z}_p$ is denoted $\mathbb{Q}_p$ and is known as the **field of p-adic numbers**. As an additive group, $\mathbb{Q}_p$ is locally compact. The field $\mathbb{F}_p$ is called the **residue class field** of $\mathbb{Q}_p$: it is the quotient field $\mathbb{Z}_p/p\mathbb{Z}_p$.

A second example of a non-archimedean local field is the field $\mathbb{F}_q((t))$ of formal Laurent series over the finite field $\mathbb{F}_q$. Such fields are sometimes known as **function fields**. The ring of integers $\mathbb{F}_q[[t]]$ consists of formal power series over $\mathbb{F}_q$. Unlike the case for $\mathbb{Q}_p$, the field $\mathbb{F}_q((t))$ has finite characteristic p where $q = p^f$. The ring $\mathbb{F}_q[[t]]$ is also a discrete valuation ring with prime ideal $t\mathbb{F}_q[[t]]$. This time, the quotient $\mathbb{F}_q[[t]]/t\mathbb{F}_q[[t]]$ is isomorphic to the finite field $\mathbb{F}_q$. The field $\mathbb{F}_q$ is called the residue class field of $\mathbb{F}_q((t))$.

These two examples are central to the theory of non-archimedean local fields. Every non-archimedean local field is either isomorphic to $\mathbb{F}_q((t))$ or to a finite extension of $\mathbb{Q}_p$. [51, Theorem 5 of Section 1.3 and Theorem 8 of Section 1.8].

4.2 Introduction

We now generalize some of the concepts from the previous section.

A **discrete valuation ring** R is a principal ideal domain with a unique prime ideal [46]. Because R is a principal ideal domain, the prime ideal of R is generated by a single element of R; such elements are called **uniformizers** or **uniformizing elements** of R. Let t be a uniformizing element of R. Because tR is the only prime ideal of R, it follows that tR is not properly contained in any other prime ideals of R; therefore, tR is a maximal ideal. It follows that the quotient R/tR is a field. This field R/tR is called the **residue class field** of R. We will exclusively consider the situation in which R/tR is a finite field $\mathbb{F}_q$.

Suppose $q = p^f$ for some f. Then $\mathbb{F}_q$ has characteristic p, and $p \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{p \text{ times}}$ belongs to the ideal tR. If $p \cdot 1 = 0$, then the ring R has characteristic p; otherwise, R has characteristic zero. For example, $\mathbb{Z}_p$ has characteristic zero and $\mathbb{F}_p[[t]]$ has characteristic p.

Let S be a family of additive cosets of tR in R with the property that $0 \in S$. Every element x of R can be expressed uniquely in the form

$$x = \sum_{j=0}^{\infty} x_j t^j \tag{4.1}$$

where x_j runs over a family S of the additive cosets of tR such that $0 \in S$. If each infinite sum of this form corresponds to an element $x \in R$, then the discrete valuation ring R is called **complete**.

For the rest of this section, we will assume R is a complete discrete valuation ring. Let $x \in R$ and write x as in (4.1). We define the absolute value $|x|$ of x to be 0 if $x = 0$, and q^{-j} if $x_j \neq 0$ and $x_k = 0$ for all $k < j$. With respect to this absolute value, R forms a complete metric space. This absolute value is discrete (this is the origin of the term *discrete valuation ring*), taking only values $\{q^{-j} : j \in \mathbb{Z}\}$ and zero. The closed balls of radius q^{-j} in the metric induced by this absolute value are nonzero. This absolute value respects multiplication: $|xy| = |x||y|$. Furthermore, the absolute value satisfies the ultrametric inequality

$$|x + y| \leq \max(|x|, |y|). \tag{4.2}$$

We will take a few moments to consider the importance of inequality (4.2). Consider the (closed) ball of radius $r = q^{-j}$ centered at x. Let y be any point in R such that $|x - y| \leq r$, and let $z \in R$ be such that $|y - z| \leq r$. Then we have

$$|x - z| = |(x - y) + (y - z)| \leq \max(|x - y|, |y - z|) \leq r.$$

So the closed ball of radius r centered at x is precisely the same ball as the closed ball of radius r centered at y. This implies that if two closed balls of radius r intersect, then they must be equal.

The discrete nature of the absolute value also has some profound implications for the topology on R. For example, consider the family of balls of radius q^{-j-1} contained in a closed ball of radius q^{-j} centered at x. If $|x - y| = q^{-j-1}$ exactly, then x and y lie in the same coset of $t^{j-1}R$ but not in the same coset of $t^j R$. Since there are q cosets of $t^j R$ contained in each coset of $t^{j-1}R$, it follows that there are precisely q balls of radius q^{-j} contained in each ball of radius q^{-j}. We can also conclude that if two balls of radius q^{-j} differ, then they are separated by a distance of at least q^{-j}.

In the same spirit as for R, we define a norm on R^n by

$$\left\|(x^{(1)}, \ldots, x^{(n)})\right\| = \max(|x^{(1)}|, \ldots, |x^{(n)}|).$$

This norm also satisfies the ultrametric property under addition, and therefore also has the property that two distinct balls of the same radius q^{-j} are separated by at least q^{-j}, and has the further property that each ball of radius q^{-j-1} contains exactly q^n balls of radius q^{-j}.

We now describe the Haar probability measure dx on R: The ball $B(0, 1) = R$ is assigned a measure of 1, and any closed ball of radius q^{-j} is assigned a measure of q^{-j}. With respect to this Haar measure, any coset of $t^j R$ has measure q^{-j}. We will also write dx for the Haar measure on R^n, which is the n-fold product of the Haar measure on R.

Given a complete discrete valuation ring R, we let K be the field of fractions over R. Each nonzero element of K is of the form

$$x = \sum_{j=M}^{\infty} x_j t^j \tag{4.3}$$

for some M with $x_M \neq 0$. The field K is called a **non-archimedean local field**. We extend the absolute value on R to all of K by defining $|x| = q^{-M}$, where M is as in (4.3). We extend the Haar probability measure on R to a σ-finite Haar measure on K by defining the measure of a closed ball of radius q^j to be q^j, and extend the Haar measure on R^n to a σ-finite Haar measure on K^n that assigns a measure of q^{jn} to a closed ball of radius q^j.

Note that R can be recovered from K algebraically as the ring of integers of K, and topologically as the closed unit ball of K.

4.3 K-Valued Functions

We will briefly discuss the notions of continuity and differentiability of functions from K to K for non-archimedean lcoal fields K. A good resource for this is [41].

Continuity of functions is defined in the same way as for any metric space. Note that a series of functions

$$\sum_{j=0}^{\infty} f_j(x),$$

where $f_j : K \to K$, is uniformly convergent on some set S whenever the absolute values of $f_j(x)$ approach zero uniformly on S. This follows from the fact that a series of elements of K converges if and only if the terms approach zero.

A function f is said to be *differentiable* at the point x if the limit

$$\lim_{h \to 0} \frac{f(x+h) - f(x)}{h}$$

exists at the point h. The function f is said to be continuously differentiable on a set E if f is differentiable for all $x \in E$ and $f'(x)$ is continuous for all x in E.

The main point of departure from complex-valued functions is the following. If a complex-valued function f is continuously differentiable on a compact set E, it follows that $f(x+h) = f(x) + hf'(x) + o(h)$, where the $o(h)$

term is independent of x. This follows because of the uniform continuity of the derivative on E and the mean value theorem: given $\epsilon > 0$, there is a δ independent of x such that $|f'(x) - f'(y)| < \epsilon$ whenever $|x - y| < \delta$, so by the mean value theorem, we have that $f(x) - f(y)$ must be within $\epsilon(y - x)$ of $f'(x)(y - x)$. This shows the desired inequality.

There is no simple "mean value theorem" for non-archimedean local fields K, and in fact it we do **not** have an x-independent estimate of the form $f(x+h) = f(x) + hf'(x) + o(h)$ for K-valued continuously differentiable functions on a compact set E. The following example is presented in Robert's book [41, Chapter 5, Subsection 1.1, Example 1]:

Example 4.3.1 (Example of a continuously differentiable function that is not strictly differentiable)**.** *Let $K = \mathbb{Q}_p$, and let Let $f(x)$ be the function that is equal to p^{2n} on the open ball of radius p^{-2n} centered at p^n, and 0 off of such open balls. For all nonzero x, we have that $f'(x) = 0$ because $f(x)$ is locally constant away from zero. At 0, it is easily seen that $f'(0) = 0$ because the difference quotient $\frac{f(x)-f(0)}{x}$ will always be at most p^{-n} in absolute value for $|x| \leq p^{-n}$. However, the difference quotient for $x = p^n$ and $y = p^n + p^{2n}$ is seen to be 1: the numerator and denominator are both p^{2n}.*

To prevent such behaviour, we need a condition that is stronger than continuous differentiability.

Definition 4.3.2 (Strictly Differentiable Function)**.** *A function $f : K \to K$ is said to be strongly differentiable on a compact set E if $f(x + h) = f(x) + hf'(x) + o(h)$, where the $o(h)$ constant does not depend on $x \in E$.*

Of course, such a function is necessarily continuously differentiable.

In [20], the term **Very Strongly Differentiable** is used for functions where the error term $o(h)$ is in fact $O(h^k)$ for some $k > 1$, where the implicit constant cannot depend on x. This implies a Hölder condition of order $k - 1$ on f'.

4.4 Hensel's Lemma

Nonarchimedean local fields K have a special property that guarantees the existence of solutions to certain kinds of equations given the existence of "near-solutions". This fact is very useful for locating configurations in such fields. We will follow the presentation of Hensel's lemma in [41].

Lemma 4.4.1. *[Hensel's Lemma] Let $f : R \to K$ be a strictly differentiable function satisfying the inequality $|f(x+h) - f(x) - hf'(x)| < |h|$ for all $x \in R$.*

(For instance, any polynomial with coefficients in R has this property.) Let x_0 be such that $|f(x_0)| < 1$ and $|f'(y)| = 1$ for all y such that $|y - x_0| < 1$. (If f is a polynomial with coefficients in R, it is enough to verify that $|f(x_0)| < 1$ and that $f'(x_0) = 1$ in order for this condition to hold.) Then there exists a point x such that $|x - x_0| < 1$ and such that $f(x) = 0$.

Proof. We will use a procedure similar to Newton's method to locate a zero x of f in K. If $f(x_0) = 0$, then we can simply take $x = x_0$. So we suppose instead that $x \neq x_0$. We consider the quantity $x_1 = x_0 - f(x_0)/f'(x_0)$. I claim that $f(x_1)$ has absolute value less than q^{-1}, where q^{-1} is the absolute value of a uniformizing element of K.

To see this, notice that $f(x_1) = f(x_0 - f(x_0)/f'(x_0))$. By the assumptions on f, x_1 satisfies the inequality

$$|f(x_1)| = \left| f(x_1) - \left(f(x_0) - f'(x_0) \frac{f(x_0)}{f'(x_0)} \right) \right| < \left| f(x_0)/f'(x_0) \right|.$$

Therefore, by the bound on $f'(x_0)$, we have that $|f(x_1)| \leq |f(x_0)|$. Furthermore, by assumption, we have that $|f'(x_1)| = 1$

We can iterate this procedure. Suppose by induction that $|x_j - x_0| < 1$, $|f'(x_j)| = 1$ and $f(x) \leq q^{-j}$ for some j. We let $x_{j+1} = x_j - \frac{f(x_j)}{f'(x_j)}$. Then x_{j+1} satisfies the inequality

$$|f(x_{j+1})| = \left| f(x_{j+1}) - \left(f(x_j) - f'(x_j) \frac{f(x_j)}{f'(x_j)} \right) \right| < \left| f(x_j)/f'(x_j) \right|$$

and by the discrete nature of the absolute value it follows that $f(x_{j+1})$ is strictly less than $q^{-(j+1)}$. We have that $f'(x_{j+1}) = 1$ by assumption because $|x_{j+1} - x_0| \leq \max(|x_{j+1} - x_j|, |x_j - x_0|) < 1$.

Therefore, x_j is a Cauchy sequence of points in R such that $f(x_j) \to 0$. It follows that the limit of this sequence, x, satisfies $f(x) = 0$. □

This proof works under somewhat weaker assumptions than those given above.

Lemma 4.4.2. *[Hensel's Lemma, General Version] Let $B \subset K$ be an open ball and let $f : B \to K$ be a strictly differentiable function satisfying the inequality $|f(x+h) - f(x) - hf'(x)| < |hf'(x)|$ for all $x \in B$ and all $h <$ rad(B). Suppose there exists $x_0 \in B$ such that $\left|\frac{f(x_0)}{f'(x_0)}\right|$ is less than the radius of B. Then there exists a unique point x such that $x \in B$ and such that $f(x) = 0$.*

The proof of this lemma is a straightforward adaptation of Lemma 4.4.1 and will be omitted.

The most important application of this lemma is the case where f is a polynomial (or power series) with coefficients in R. In this instance, the error in approximating $f(x+h)$ linearly is bounded above in absolute value by $|h^2| < |hr|$. Taking $r = f'(x_0)$, we have that the error in the linear approximation is bounded above by $hf'(x_0)$ on a ball of radius $f'(x_0)$. As long as there exists x_0 such that $\left|\frac{f(x_0)}{f'(x_0)}\right| \leq f'(x_0)$, i.e. $|f(x_0)| < |f'(x_0)|^2$, then there will be a unique zero in the ball of radius $f'(x_0)$ centered at x_0.

It is important to note that the condition that $|f(x+h)-f(x)-hf'(x)| < |hf'(x)|$ implies that $|f'(x)|$ is constant on B. To see this, suppose that there are $x, y \in B$ such that $|f'(x)| \neq |f'(y)|$. Because $|f(y)-f(x)-(y-x)f'(x)|$ is strictly smaller than $|(y-x)f'(x)|$, we have that $|f(y)-f(x)| = |(y-x)f'(x)|$. Then, on the one hand, we have that $|f(y) - f(x)| = |(y - x)f'(x)| = |y - x||f'(x)|$, and on the other hand, we have that $|f(y)-f(x)| = |(y-x)f'(y)| = |y - x||f'(y)|$ so $|f'(x)| = |f'(y)|$.

This theorem can be further strengthened to show that, under the conditions of the lemma, f maps B bijectively onto a ball of radius $\mathrm{rad}(B)/|f'(x)|$ centered at 0. The uniqueness follows from the fact that if $f(x) = 0$, then $|f(x+h)-hf'(x)| < |hf'(x)|$, and so $|f(x+h)| = |hf'(x)|$ by the ultrametric inequality.

Theorem 4.4.3 (Inverse Function Theorem for Local Fields)**.** *Let $f : B \to K$ be a strictly differentiable function defined on a ball $B \subset K$ such that $|f(x + h) - f(x) - hf'(x)| < |hf'(x)|$ and such that $|f'(x)| \geq rad(B)$ for all x in some open ball B and all $|h| < rad(B)$. Then $|f'(x)|$ is constant on B. Furthermore, f maps B bijectively onto an open ball $f(B)$ of radius $f'(x)rad(B)$. Thus, f^{-1} is well-defined on $f(B)$ and the derivative of f^{-1} is given by $(f^{-1})'(y) = \frac{1}{f'(f^{-1}(y))}$ for all such y. In particular, $|(f^{-1})'(y)|$ is constant and equal to $\frac{1}{|f'(x)|}$ on $f(B)$.*

4.5 The Height Function

For the purposes of this section, we will assume that $K = \mathbb{Q}_p$ or $K = \mathbb{F}_q((t))$. The results in Chapter 5 require a notion of the height of an element of K^n for $K = \mathbb{Q}_p$ and $\mathbb{F}_q((t))$. We will first define a height function for the local fields $\mathbb{F}_q((t))$ and for $\mathbb{Q}_p$, and build up a height function for arbitrary local fields using these two examples. This function is discussed in [18].

4.5.1 Finite Characteristic Case

Let K be a function field $\mathbb{F}_q((t))$: a local field of finite characteristic. Let x be an element of R, the ring of integers of K. We can write x in the form

$$\sum_{j=0}^{\infty} x_j t^j$$

which is a power series in the variable t, where $x_j \in \mathcal{F}_q$ for $q = p^f$. Addition in R is componentwise: if $x = \sum_{j=0}^{\infty} x_j t^j$ and $y = \sum_{j=0}^{\infty} y_j t^j$ then

$$x + y = \sum_{j=0}^{\infty} (x_j + y_j) t^j$$

and

$$xy = \sum_{j=0}^{\infty} \left(\sum_{k_1+k_2=j} x_{k_1} y_{k_2} \right) t^j.$$

Each sum $\sum_{k_1+k_2=j} x_{k_1} y_{k_2}$ is finite, so this product is well-defined.

If x and y are known to be polynomials (i.e., they only have a finite number of nonzero terms), then $\deg(x + y) \leq \max(\deg(x), \deg(y))$ and $\deg(xy) \leq \deg(x) + \deg(y)$. We can then define a height on R in the following way: if $x \neq 0$ is a polynomial in R, then the height $h_{\mathbb{F}_q((t))}(x)$ of x will be defined to be the degree of x; if x has infinitely many nonzero terms, then the height $h_{\mathbb{F}_q((t))}(x)$ will be defined to be ∞.

4.5.2 p-Adic Case

Something similar can be done if $K = \mathbb{Q}_p$ and $R = \mathbb{Z}_p$. We can write $x \in \mathbb{Z}_p$ in the form

$$x = \sum_{j=0}^{\infty} x_j p^j.$$

If the sum is finite, then x can be thought of as an integer written in base p. So we can define a height function on $\mathbb{Z}_p$ as follows: the height $h_{\mathbb{Q}_p}(x)$ of $x \in \mathbb{Z}_p$ is the number of digits in the base p expansion of x minus one if x has a finite expansion in $\mathbb{Z}_p$, and infinity if x has infinitely many nonzero terms.

It would have been convenient if this function $h_{\mathbb{Q}_p}$ had the same addition and multiplication bounds as the function $h_{\mathbb{F}_q((t))}$; however, this is not the case: the sum $h_{\mathbb{Q}_p}(x + y)$ may be as large as $\max(h_{\mathbb{Q}_p}(x), h_{\mathbb{Q}_p}(y)) + 1$. However, $h_{\mathbb{Q}_p}(xy) \leq h_{\mathbb{Q}_p}(x) + h_{\mathbb{Q}_p}(y)$.

4.5.3 Negatives of Elements of Finite Height

In the case where $K = \mathbb{F}_q((t))$, the height function satisfies $h_{\mathbb{F}_q((t))}(-x) = h_{\mathbb{F}_q((t))}(x)$ for all x of finite height. Unfortunately, no analogue of this equation exists for $\mathbb{Q}_p$. For example, the element 1 has height equal to 1. However, the element -1 is equal to

$$\sum_{j=0}^{\infty}(p-1)^j$$

and therefore does not have finite height. However, the negative of an element of $\mathbb{Z}_p$ of finite height still has a predictable pattern.

Let $z \in \mathbb{Z}_p$. Then z has an expansion of the form 4.1:

$$z = \sum_{j=0}^{\infty} z_j p^j.$$

We will call the collection of digits $\{z_0, \ldots, z_{d-1}\}$ the d least significant digits of z. We will say that $z^{(1)}$ and $z^{(2)} \in \mathbb{Z}_p$ differ only in the d least significant digits if $z_j^{(1)} = z_j^{(2)}$ for all $j \geq d$.

If z has height at most h, then $-z$ will differ from -1 in only the h least significant digits. This fact allows us to prove the following lemma

Lemma 4.5.1 (Corollary 2.2 from [18]). *Let x and y be elements of $\mathbb{Z}_p$ of height at most h, and let $\delta \in R$, $\delta \neq 0$ satisfy the inequality $|\delta| \leq p^{-(h+1)}$. Then we have that $|(-x+\delta) - y| \geq |\delta|$.*

Proof. We first consider the case in which $x = 0$. If $y = 0$ as well, then $(-x+\delta) - y$ is equal to δ. If $x = 0$ and y is nonzero, then $|(-x+\delta) - y|$ is equal to $|y - \delta|$. Since y is nonzero and has height at most h, it follows that $|y| \geq p^{-h+1}$. Because $|\delta| \leq p^{-(h+1)} < p^{-h+1}$, it follows from the ultrametric inequality that $|y - \delta| = |y| > |\delta|$.

So we are left with the case in which $x \neq 0$. Because x has height at most h, it follows from the above discussion that $-x$ differs from -1 in only the first h digits. In particular, this implies that if we write$-x$ as in (4.1), then $(-x)_h$ must be equal to $p-1$. Thus $(-x)_h$ is nonzero. Then the nonzero term $(-x)_h p^h$ in the expansion of $-x$ has absolute value exactly p^{-h}. Thus the term $(-x+\delta)_h$ is also equal to $p-1$ because of the condition on $|\delta|$. However, $y_h^{(k_1,k_2)} = 0$ because y has height at most h. Thus $|(-x+\delta) - y| \geq p^{-h} > p^{-h-1} \geq |\delta|$ as desired. $\square$

Chapter 5

Configurations II

5.1 Introduction

We will now discuss the proofs of Theorems 1.2.1, 1.2.2, 1.2.3, and 1.2.4. We will begin by giving some context for these results.

A major problem in additive combinatorics is locating arithmetic progressions in sets. A classic result in the area is due to Roth [42]. Roth establishes that, for any δ, and any sufficiently large $N \geq N_0(\delta)$, any subset of $\mathbb{Z}/N\mathbb{Z}$ containing at least δN elements must contain a 3-term arithmetic progression. On the other hand, for any $\epsilon > 0$ Behrend [2] presents an example of a subset of $\mathbb{Z}/N\mathbb{Z}$ for $N \geq N_1(\epsilon)$ with at least $C_\epsilon N^{1-\epsilon}$ elements that does not contain a 3-term arithmetic progression.

The question of how large a set guarantees the existence of a 3-term arithmetic progression remained open for finite abelian groups other than $\mathbb{Z}/N\mathbb{Z}$. The problem of obtaining bounds on the maximum size of a subset of $(\mathbb{Z}/3\mathbb{Z})^n$ that does not contain a 3-term arithmetic progression is called the **capset problem**.

The largest known construction of a subset of $(\mathbb{Z}/3\mathbb{Z})^n$ that does not contain a 3-term arithmetic progression is due to Edel [13]. This set contains C_1^n elements for some $C < 3$. The best known upper bound, of the form C_2^n for some $C_1 < C_2 < 3$ is due to Ellenberg and Gijswijt [16], who use a polynomial method based on a similar argument of Croot, Lev, and Pach [9]. A summary of the history of problems related to arithmetic progressions in finite groups prior to the 2017 results is given by Wolf [53].

It is natural to ask about infinite versions of the capset problem. Theorem 1.2.1 establishes that there are subsets of $K = \mathbb{F}_3((t))$ of Hausdorff dimension 1 that do not contain 3-term arithmetic progressions. This is somewhat surprising, because the ring of integers R of K (viewed as an abelian group) is the projective limit of the groups $(\mathbb{Z}/3\mathbb{Z})^n$.

The proofs of all four theorems follow the same general procedure of Chapter 3.

5.2 A Single Step

5.2.1 Polynomial, Nonsingular Case

We will start by describing a step of the construction for Theorem 1.2.1. We will make use of the height function described in Chapter 4.

Proposition 5.2.1. *[Proposition 2.3 from [18]] Let $T_1, \ldots, T_v$ be sets, each of which is a union of balls of radius $q^{-\mu}$, and let $p(x_1, \ldots, x_v)$ be a polynomial satisfying $\left|\frac{\partial p}{\partial x_{i_0}}\right| \geq q^{-A}$ for some i_0 and for all $(x_1, \ldots, x_v) \in T_1 \times \ldots \times T_v$. Then there exists a positive real number c depending on A, on the field K, and on μ with the following property. Subdivide each ball of radius $q^{-\mu}$ into balls of radius $q^{-\nu}$. Then, if μ is sufficiently large, there exist sets $S_1 \subset T_1, \ldots, S_v \subset T_v$ such that:*

(a) There are no solutions to $p(x_1, \ldots, x_v) = 0$ with $x_1 \in S_1, \ldots, x_v \in S_v$. Furthermore, p satisfies the bound $|p(x_1, \ldots, x_v)| \geq cq^{-\nu}$ on $S_1 \times \cdots \times S_v$.

(b) For $1 \leq i \leq v$ and any ball U of radius $q^{-\nu}$ contained in one of the $q^{-\mu}$-balls of T_i, we have that $S_i \cap U$ is a ball of radius $\geq cq^{-\nu n/D}$.

Proof. For convenience, we will also assume that the index $i_0 = v$.

Each closed ball B of radius $q^{-\nu}$ contains exactly one element of R^n of height at most ν (here, the height of an element of R^n is the maximum of the heights of the components.) Suppose $x_1, \ldots, x_v \in R^n$ and each of $x_1, \ldots, x_v$ has height at most ν. Let p be an nv-variate polynomial of degree at most d, with coefficients of height at most b. Let $s := \binom{d+nv}{nv}$ be the dimension of the space of nv-variate polynomials of degree d. Then $p(x_1, \ldots, x_v)$ is a sum of at most s terms, each of which is either of height at most $b + hd$, or the negative of an element of height at most $b + d\nu$. For us, the important point is that the coefficient of ν is equal to d. Thus we can write $p(x_1, \ldots, x_v)$ as a sum of two terms: a term with height at most $b + d\nu + s$, and the negative of such a term (the s is unnecessary in the case of $\mathbb{F}_q((t))$). It follows from Corollary 4.5.1 (or, in the case of $\mathbb{F}_q((t))$, the fact that the negative of an element of finite height also has finite height) that if $|\delta| \leq q^{-(b+d\nu+s+1)}$ that $|p(x_1, \ldots, x_v) + \delta| \geq |\delta|$.

This fact will serve as a local-field substitute for the following algebraic fact in $\mathbb{R}^n$: if p is an nv-variate polynomial of degree d with coefficients in $\mathbb{Z}$ and $x_1, \ldots, x_v$ are multiples of N^{-1} for some integer N, then $p(x_1, \ldots, x_v)$ is a multiple of N^{-d}, so $p(x_1, \ldots, x_v)$ is a multiple of N^{-d}, so $p(x_1, \ldots, x_v) + \delta$ differs from 0 by at least δ provided that $|\delta| < 2N^{-d}$. This simple algebraic fact is the key to Máthé's construction of the set in Theorem 3.1.4.

We now use the fact that, if $\delta < 1$ and if p satisfies the bound $q^{-A} \le \left|\frac{\partial p}{\partial x_v}\right|$ uniformly on a compact set $T_1 \times \cdots \times T_v$, then $q^{-A}|\delta| \le |p(x_1,\ldots,x_v+\delta) - p(x_1,\ldots,x_v)| \le \delta$, where the last inequality holds because any polynomial with coefficients in R has derivatives bounded in absolute value by 1 on R. This implies that if $|\delta| < q^{-(b+d\nu+s+1)}$ and $x_1,\ldots,x_v$ all have height at most h, then $p(x_1,\ldots,x_v+\delta)$ is not within $q^{-A}|\delta|$ of zero.

Finally, since all of the derivatives of p are bounded above by 1 in absolute value, we have that the same bound holds provided that $x_1,\ldots,x_v$ are all within closed balls of radius $q^{-A-(b+d\nu+s+1)-1}$ determined in the following way: given $B \subset T_j$ of radius $q^{-\nu}$ for $1 \le j \le v-1$, select $S_j \cap B$ to be the unique ball containing an element of height h. Then, selecting any δ with $|\delta| = q^{-A-(b+d\nu+s+1)-1}$, we define $S_v \cap B$ to be the unique ball containing $x_B + \delta$, where x_B is the unique element of height at most ν in B. □

5.2.2 One Dimension, Nonsingular Case

We will establish an analogue of Proposition 3.3.1. The proof follows a similar strategy. The analogue of Rolle's theorem that will be used for this purpose is Theorem 4.4.3.

Let f be a strictly differentiable K-valued function in v variables with nonvanishing gradient defined in an open ball $B \subset R$ containing the origin.

Suppose that we are given $i_0 \in \{1,2,\cdots v\}$, an integer $\mu \ge 1$, a small constant $c_0 > 0$ and compact subsets $T_1,\ldots,T_v \subset R$. We will assume that the sets $T_1,\ldots,T_v$ satisfy the following conditions.

1. Each T_i is a union of disjoint closed balls of radius $q^{-\mu}$. Let us denote by $\mathcal{J}_\mu(T_i)$ this collection of balls.

2. The set T_1 is disjoint from the set $T_{i'}$ if $i \ne i'$.

3. $\left|\frac{\partial f}{\partial x_{i_0}}(x)\right| \ge c_0$ and $|\nabla f(x)| \le c_0^{-1}$ for all $x \in T_1 \times \cdots \times T_v$.

Proposition 5.2.2. *Given f, μ, i_0, c_0 and $\mathbb{T} = (T_1,\cdots,T_v)$ satisfying these assumptions, there exist a small rational constant $c_1 > 0$ and an integer ν_0 (depending on all these quantities), for which the following conclusions hold.*

For all $\nu \ge \nu_0$, one can find compact subsets $S_i \subseteq T_i$ for all $1 \le i \le v$ such that

(a) There are no solutions of $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) *For each $J \in \mathcal{J}_\mu(T_i)$, we decompose J into closed balls of radius $q^{-\nu}$ with disjoint interiors and call the resulting collection of intervals $\mathcal{I}_\nu(J,i)$. Then for each $i \neq i_0$ and each $I \in \mathcal{I}_\nu(J,i)$, the set $S_i \cap I$ is an interval of length $c_1 q^{(1-v)\nu}$.*

(c) *For every $J \in \mathcal{J}_\mu(T_{i_0})$, there exists $\mathcal{I}'_\nu(J,i_0) \subseteq \mathcal{I}_\nu(J,i_0)$ with*

$$\#\big(\mathcal{I}'_\nu(J,i_0)\big) \geq \big(1 - \frac{1}{q^\mu}\big)\#\big(\mathcal{I}_\nu(J,i_0)\big) \tag{5.1}$$

such that for each $I \in \mathcal{I}'_\nu(J,i_0)$,

$$|S_{i_0} \cap I| \geq c_1 q^{-\nu}. \tag{5.2}$$

Unlike part (b), $S_{i_0} \cap I$ need not be a ball; however, it can be written as a union of disjoint balls of radius $c_1 q^{\nu(1-v)}$.

Proof. We want to mimic the strategy of the proof of Proposition 3.3.1.

Let $f(x_1,\ldots,x_v)$ be a strictly differentiable, nonsingular function defined on $\mathbb{T}$ satisfying the above conditions. For simplicity, we will assume $i_0 = v$. Then, by the definition of strict differentiability, there exists an integer μ_0 such that $q^{\mu_0} > c_0^{-1}$ and such that, for any open ball B of radius at most $q^{-\mu_0}$, $x \in B$, and $h < \mathrm{rad}(B)$,

$$|f(x+h) - f(x) - hf'(x)| \leq |hf'(x)|. \tag{5.3}$$

If $\mu < \mu_0$, then decompose each constituent ball of $T_1 \times \cdots \times T_v$ into balls of radius μ_0. Because we can always perform this operation without affecting the proof of the lemma, we will always assume that $\mu \geq \mu_0$ for this value of μ. Let $\nu > \mu$. For each ball B of radius $q^{-\nu}$ contained in T_i for any $i \neq v$, we will take $S_i \cap B$ to consist of a single (arbitrarily chosen) ball of radius $c_1 q^{-\nu(v-1)}$, where c_1 is a constant to be determined later.

For a fixed $x_1 \in S_1, \ldots, x_{v-1} \in S_{v-1}$, we will define the function $f_{x_1,\ldots,x_{v-1}} : T_v \to K$ by $f_{x_1,\ldots,x_{v-1}}(x_v) = f(x_1,\ldots,x_v)$. We will consider the behaviour of this function on a single ball of radius $q^{-\mu}$. Let $J \in \mathcal{J}_\mu(T_v)$. We have that $\left|\frac{\partial f}{\partial x_v}\right| \geq c_0$ for $x \in \mathbb{T}$. Furthermore, by the choice of μ_0, we have that $f_{x_1,\ldots,x_{v-1}}$ satisfies the inequality (5.3) on J. Therefore, we can apply Theorem 4.4.3 on J. This theorem states that $|f'_{x_1,\ldots,x_{v-1}}(x)|$ is constant on J and that $f_{x_1,\ldots,x_{v-1}}$ maps J bijectively onto a ball of radius equal to $|f'_{x_1,\ldots,x_{v-1}}(x)|q^{-\mu}$. The bijectivity of this map guarantees that, for a fixed $x_1,\ldots,x_{v-1}$ there is at most one $x \in J$ such that $f_{x_1,\ldots,x_{v-1}}(x) = 0$.

Let $\mathbb{A}$ be a collection of points $(x_1, \ldots, x_{v-1})$ such that $\mathbb{A}$ contains a single representative from each of the cubes of radius $c_1 q^{-\nu(v-1)}$ that constitute $S_1 \times \cdots \times S_{v-1}$. Then $\mathbb{A}$ will have no more than $q^{\nu(v-1)}$ elements. Let I be a ball of radius $c_1 q^{-\nu(v-1)}$ contained in S_v. For each $x' = (x_1, \ldots, x_{v-1})$ in $\mathbb{A}$, we will consider the image $f_{x'}(I)$. By the argument in the previous paragraph, this image has radius at most $c_0^{-1} c_1 q^{-\nu(v-1)}$.

Now we will consider $f_{x'+h}(J)$ for $|h| < c_1 q^{-\nu(v-1)}$ and an arbitrary ball $J \in \mathcal{J}_\mu(T_i)$. By assumption each component of the derivative of f is bounded above by c_0^{-1} on $\mathbb{T}$; therefore, $f_{x'+h}(x)$ differs from $f_{x'}(x)$ by an amount that is strictly less than $c_0^{-1} c_1 q^{-\nu(v-1)}$. Thus $f_{x'+h}(x)$ is contained inside the ball $f_{x'}(I)$. It follows from this argument that if x satisfies $f_{x^*}(x) = 0$ for some $x^* \in S_1 \times \cdots \times S_{v-1}$ and some $x \in J$ that x is within a $c_0^{-1} c_1 q^{-\nu(v-1)}$-neighbourhood of a zero of $f_{x'}$ for some $x' \in \mathbb{A}$. Call these zeros bad points. There are at most $q^{\nu(v-1)}$ such values of x', so there are at most $q^{\nu(v-1)}$ bad points. Let S_v be the union of balls of radius $c_0^{-1} c_1 q^{-\nu(v-1)}$ that do not contain a bad point.

Select $c_1 = c_0 q^{-3\mu}$. Then each ball in $\mathcal{J}_\mu(T_v)$ contains $q^\nu q^{-\mu}$ balls of radius $q^{-\nu}$, each of which contains $c_0 c_1^{-1} q^{\nu(v-2)} = q^{3\mu} q^{\nu(v-2)}$ balls of radius $c_0^{-1} c_1 q^{-\nu(v-1)}$. Consider the balls of radius $q^{-\nu}$ that contain more than $q^{2\mu} q^{\nu(v-2)}$ balls of radius $c_1 q^{\nu(v-1)}$ that contain a bad point. The pigeonhole principle implies that the maximum possible number of such balls is $\frac{q^{\nu(v-1)} q^{-2\mu}}{q^{\nu(v-2)}} = q^{-2\mu} q^\nu$. Therefore, for each $J \in \mathcal{J}_\mu(T_v)$, we have that all except for at most a $q^{-\mu}$-fraction of the balls in $\mathcal{I}(J, v)$ contain at least $(c_0 c_1^{-1} - q^{2\mu}) q^{\nu(v-2)} = (q^{3\mu} - q^{2\mu}) q^{\nu(v-2)}$ balls of S_v. This is at least a $(1 - q^{-\mu})$ fraction, as desired. □

5.2.3 One Dimension, General Case

We will iterate Proposition 5.2.2 or Proposition 5.2.1 in order to establish the following proposition, which applies even in situations where ∇f vanishes somewhere on $\mathbb{T}$.

Suppose that we have a multi-index α satisfying $|\alpha| = r$, an integer $\mu \geq 1$, a small constant $c_0 > 0$ and compact subsets $T_1, \ldots, T_v \subset R$, and an r-times strictly differentiable function f. We will make the following assumptions:

1. Each T_i is a union of disjoint closed balls of radius $q^{-\mu}$. Let us denote by $\mathcal{J}_\mu(T_i)$ this collection of balls. We will consider a function f such that the derivative $\partial^\alpha f$ is nonzero.

2. T_1 and $T_{i'}$ are disjoint if $i \neq i'$.
3. The partial derivative $\partial^\alpha f$ does not vanish on $T_1 \times \cdots \times T_v$, and is bounded below in absolute value by c_0 on this set.

Proposition 5.2.3. *Given f, μ, α, c_0 and $\mathbb{T} = (T_1, \cdots, T_v)$ satisfying these assumptions, there exist a small constant $c_1 > 0$ and an integer ν_0 (depending on all these quantities), for which the following conclusions hold.*

For $\nu \geq \nu_0$, there exist compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $J \in \mathcal{J}_\mu(T_i)$, let us decompose J into disjoint closed balls of radius $q^{-\mu}$ and call the resulting collection of balls $\mathcal{I}_N(J, i)$.

For every $J \in \mathcal{J}_\mu(T_i)$ and every i, there exists $\mathcal{I}'_\nu(J, i) \subseteq \mathcal{I}_\nu(J, i)$ with

$$\#\left(\mathcal{I}'_\nu(J, i)\right) \geq c_2 \#\left(\mathcal{I}_N(J, i)\right) \tag{5.4}$$

such that for each $I \in \mathcal{I}'_\nu(J, i)$, $|S_i \cap I|$ is nonempty. $S_i \cap I$ need not be a ball; however, it can be written as a union of disjoint balls of radius $c_1 q^{-\nu(v-1)}$. Here, $c_2 > 0$ and may depend on f, r, c_0, v, and μ, but not on ν.

The proof of this proposition is omitted because of its similarity to the proof of Proposition 3.3.4. We can similarly iterate Proposition 5.2.1 to arrive at the following proposition.

Proposition 5.2.4. *Given a polynomial function f of degree d, with integer coefficients, and a set $\mathbb{T} = (T_1, \cdots, T_v)$ that is expressible as a disjoint union of $q^{-\mu}$-balls, there exist a small constant $c_1 > 0$ and an integer ν_0 (depending on all these quantities), for which the following conclusions hold.*

For $\nu \geq \nu_0$, there exist compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $J \in \mathcal{J}_\mu(T_i)$, let us decompose J into disjoint closed balls of radius $q^{-\mu}$ and call the resulting collection of balls $\mathcal{I}_N(J, i)$.

For every $J \in \mathcal{J}_\mu(T_i)$ and every i, there exists $\mathcal{I}'_\nu(J, i) \subseteq \mathcal{I}_\nu(J, i)$ with

$$\#\left(\mathcal{I}'_\nu(J, i)\right) \geq c_2 \#\left(\mathcal{I}_N(J, i)\right) \tag{5.5}$$

such that for each $I \in \mathcal{I}'_\nu(J, i)$, $|S_i \cap I|$ is nonempty. $S_i \cap I$ is a ball of radius $c_1 q^{-\nu(n/d)}$. Here, $c_2 > 0$ and may depend on f, c_0, v, and μ, but not on ν.

This is proven by iterating Proposition 5.2.1 in the same way as in Propositions 3.3.4 and 5.2.3.

5.2.4 Multidimensional Case

We begin by proving a proposition, which is an analogue of Proposition 3.3.5.

Let $m, n \geq 1$ and $v \geq 3$ satisfy $m \leq n(v-1)$, and let $f : K^{nv} \to K^m$ be a twice strictly differentiable function whose zero set has a nontrivial intersection with R. Suppose $\mu \geq \mu^*$, where μ^* is a large integer to be selected later, $c_0 > 0$ is a small constant and $T_1, \ldots, T_v \subset R^n$ are sets with the following properties:

1. Each T_i is expressible as a union of closed disjoint balls of radius $q^{-\mu}$, the collection of which will be called $\mathcal{J}_\mu(T_k)$. The sets T_i and $T_{i'}$ will be disjoint for $i \neq i'$.

2. On $\{x \in T_1 \times \cdots \times T_v : f(x) = 0\}$, the matrix Df is of full rank, with a submatrix B whose determinant is bounded below by C_0, and whose entries are bounded above by C_1.

3. On R^{nv} the operator norm of the Hessian $D^2 f$ is bounded above by C_2.

We are now ready to state the main proposition in the multidimensional setting.

Proposition 5.2.5. *Given f, μ C_0, C_1 and C_2 as above, there exists a constant $c_1 > 0$ and an integer ν_0 depending on these quantities for which the following conclusions hold. For $\nu \geq \nu_0$, set $q^\lambda = c_1 q^{-\nu(v-1)}$. There exist compact subsets $S_i \subseteq T_i$ for all $1 \leq i \leq v$ such that*

(a) There are no solutions to $f(x) = 0$ with $x \in S_1 \times \cdots \times S_v$.

(b) For each $1 \leq i \leq v$ and $J \in \mathcal{J}_\mu(T_i)$, let us decompose J into disjoint closed balls of radius $q^{-\nu}$ and call the resulting collection of balls $\mathcal{I}_\nu(J, i)$. There exists $\mathcal{I}'_\nu(J, i) \subseteq \mathcal{I}_\nu(J, i)$ such that

$$S_i \subseteq \bigcup \left\{ I : J \in \mathcal{J}_M(T_i),\ I \in \mathcal{I}'_\nu(J, i) \right\}.$$

More precisely, for each $I \in \mathcal{I}'_\nu(J, i)$, the set $S_i \cap I$ is a single ball of radius $q^{-\lambda}$, provided $i \neq v$. For $i = v$ and $I \in \mathcal{I}'_\nu(J, v)$, the set $S_v \cap I$

is not necessarily a single ball of radius $q^{-\lambda}$, but a union of such balls, with the property that

$$|S_v \cap I| \geq \left(1 - q^{-\mu}\right) q^{-n\nu}. \tag{5.6}$$

(c) *The subcollections $\mathcal{I}'_\nu(J,i)$ of balls are large subsets of the ambient collection $\mathcal{I}_\nu(J,i)$, in the sense that for all $1 \leq i \leq v$, $J \in \mathcal{J}_\mu(T_i)$,*

$$\#\left(\mathcal{I}'_\nu(J,i)\right) \geq \left(1 - q^{-\mu}\right) \#\left(\mathcal{I}_\nu(J,i)\right). \tag{5.7}$$

Except for the proof of Lemma 3.3.6, the proof of Proposition 3.3.5 depends only on the combinatorial structure of the bad boxes (recall that a ball in R^n is an n-fold Cartesian product of balls in R), and therefore can be repeated in the non-archimedean setting. Therefore, we will restrict ourselves to proving a non-archimedean version of Lemma 3.3.6.

Lemma 5.2.6 (Lemma 3.1 from [18]). *There exists $\mu_0(C_0, C_1, C_2) > 0$ such that the following statement holds for all $\mu \geq \mu_0$. Let $\mathbb{T}$ be an nv-dimensional ball of radius $q^{-\mu}$ and let $f(x_1, \ldots, x_v) : \mathbb{T} \to K^m$ be a function such that Df has an m-by-m minor that is, in absolute value, at least a constant C_0 on all of $\mathbb{T}$ and whose entries are bounded above in absolute value by a constant C_1. Suppose further that C_2 is an upper bound for the operator norm of the second derivative of f. Let Z_f be the set of $(x_1, \ldots, x_v)$ such that $f(x_1, \ldots, x_v) = 0$. Subdivide the ball $\mathbb{T}$ into balls of radius $q^{-\lambda}$. If λ is sufficiently large, then the number of balls that intersect the zero set of f is at most $C_3 q^{-\mu+\lambda(nv-m)}$ where μ_0 and C_3 can depend on C_0, C_1, and C_2 but not on λ.*

Proof. Let x_0 be a point in Z_f. If μ is sufficiently large, then there exists a fixed m-by-m submatrix B of Df, indexed by the columns $(j_1, \ldots, j_m)$, such that B has determinant with absolute value at least C_0 for all $x \in \mathbb{T}$. Consider the vector space U spanned by the vectors e_{j_i} whose j_i component is 1 and whose other components are 0. Consider points of the form $x_0 + u$ where u is a vector in the vector space U of magnitude at most $q^{-\mu}$. By the assumptions on Df, we have $f(x_0 + u) = f(x_0) + Df_{x_0} u + O(\|u\|^2)$. Here, $f(x_0) = 0$, and $\|Df_{x_0} u\| \geq k_0 \|u\|$, where $k_0 = C_0 C_1^{-(m-1)}$, as can be seen from the adjugate formula for the inverse of B. So we have that $\|f(x_0 + u)\| \geq C_0 \|u\| + O(\|u\|^2)$. This is guaranteed to be positive provided that μ is sufficiently large.

Let λ be larger than μ. For a given $x \in Z_f$, consider the slab consisting of points $x + U + w$ where w has a zero in each of the j_i components and satisfies $|w| \leq q^{-\lambda}$; i.e., the $q^{-\lambda}$-neighbourhood of $x + U$. Let $x + u + w$ be some point in this slab. We have that $f(x+u+w) = f(x) + Df_x(u+w) + O(\|u+w\|^2) = Df_x(u+w) + O(\|u+w\|^2)$. This has norm at least $k_0 \|u\| - C_1 \|w\| + O(\|u+w\|^2)$. Therefore, $f(x+u+w)$ is nonzero provided that $\|u\|$ is greater than $\frac{C_1}{k_0} \|w\|$, and provided that μ is sufficiently large that the $O(\|u+w\|^2)$ term has norm smaller than $k_0 \|u\|$. Recall that $\|w\| \leq q^{-\lambda}$, so if μ is sufficiently large this inequality will hold provided that $\|u\|$ is at least $\frac{2C_1}{k_0} q^{-\lambda}$. Thus, subdividing this slab into $q^{-\lambda}$-balls, we have Z_f will intersect only at most $\left(\frac{2C_1}{k_0}\right)^m$ balls in the slab. Taking the union over disjoint parallel slabs that cover the $q^{-\mu}$ ball, we have a total of $O\left(\left(\frac{C_1}{k_0}\right)^m q^{\lambda(nv-m)-\mu}\right)$ intersections. □

5.3 Construction of E

The construction of E is very similar to the construction of the set E in Chapter 3. We will start with $E_0 = B^n$, where $B \subset R$ is a sufficiently small ball to satisfy the conditions of Theorem 1.2.1, 1.2.2, or 1.2.3. We will let D be equal to the dimension in the appropriate theorem statement: $D = \frac{n}{d}$ in the case of Theorem 1.2.1, $D = \frac{1}{v-1}$ in the case of Theorem 1.2.2, and $D = \frac{m}{v-1}$ in the case of Theorem 1.2.3.

5.3.1 General Procedure

We will keep a running queue $\mathcal{Q}$ that will guide the construction.

One minor difference in the proof of Theorem 1.2.1 is that the number of variables v is allowed to vary. For the cases of Theorems 1.2.2 and 1.2.3, take $v = v_1 = v_2 = \cdots$ throughout the rest of this argument.

Fix a sequence ϵ_j such that $\epsilon_j \to 0$. We select λ_0 sufficiently large so that the ball E_0 contains at least $v_1 + 1$ balls of radius $q^{-\lambda_0}$. Let $B_1^{(0)}, \ldots, B_{M_0}^{(0)}$ be an enumeration of the balls of radius $q^{-\lambda_0}$ contained in B^n and let Σ_0 be the family of v_1-tuples of distinct such balls, ordered lexicographically and identified in the usual way with the family of injections from $\{1, \ldots, v_1\}$ into $\{1, \ldots, M_0\}$. Let $\mathcal{Q}_0$ be the queue consisting of 3-tuples

$$\{(1, \sigma, 0) : \sigma \in \Sigma_0\},$$

where the queue elements are ordered so that $(1, \sigma, 0)$ precedes $(1, \sigma', 0)$ whenever $\sigma < \sigma'$.

Stage 1 At Stage 1, we consider the first queue element $(1, \sigma, 0)$. Let $T_1 = B^{(0)}_{\sigma(1)}$, ..., $T_v = B^{(0)}_{\sigma(v)}$.

First, we will consider the case of Theorems 1.2.1 and 1.2.2. Let $f = f_1$. We have by assumption that there is a lower bound q^{-A_1} on the derivative $|\partial^\alpha f|$ for some appropriate i_0. We decompose each ball of radius $q^{-\lambda_0}$ into balls of radius $q^{-\mu_1}$, where $\mu_1 \geq \lambda_0$ and $\mu_1 > \mu^*$, where μ^* is as in Proposition 5.2.3 or 5.2.4 applied to $T_1, \ldots, T_v$. We apply either Proposition 5.2.3 or Proposition 5.2.4 to arrive at sets $S_1, \ldots, S_v$ with the properties guaranteed by the corresponding proposition. Let e_0 be the quantity c_2 appearing in the proposition. We can select $\nu = \nu_1$ in the proposition to be sufficiently large that the quantity $q^{-\lambda_j} := c_2 q^{-\nu_1 n/D}$ appearing in Proposition 5.2.4 or in Proposition 5.2.3 is larger than $q^{-\nu_1(n/D+\epsilon_1)}$. We will also select ν sufficiently large that $q^{-\nu_1\epsilon_1} < e_0$ and so that $\nu_1 > \exp(\mu_1)$.

Now, we will consider the case of Theorem 1.2.3. In the case of Theorem 1.2.3, we know that Df_1 has full rank on $T_1 \times \cdots \times T_v$ by assumption. Because this set is compact, it follows that there exists some C_0 such that, for each $x \in T_1 \times \cdots \times T_v$, Df_1 has a minor with absolute value greater than or equal to C_0 at x, and that each of the entries of Df will be bounded above in absolute value by C_1 for some C_1. The uniform continuity of $D^2 f$ also guarantees that $D^2 f$ will be bounded above by C_2 in operator norm, for some appropriate value C_2. We can then select $\mu_1 \geq \mu^*$, where μ^* is as in Proposition 5.2.5. Select $\nu = \nu_1$ in Proposition 5.2.5 to be sufficiently large so that that the quantity $q^{-\lambda_1} := cq^{-\nu_1/D + C\mu_1}$ appearing in Proposition 5.2.5 is larger than $q^{-\nu_1(n/D+\epsilon_1)}$ For convenience, we will simply take $e_0 = \frac{1}{2} < \left(1 - \frac{1}{q^{\mu_1}}\right)$. We also will take $\nu_1 > \exp(\mu_1)$.

In any case, we arrive at sets $S_1 \subset T_1, \ldots, S_v \subset T_v$ with the property that f_1 is nonzero for $x_1 \in S_1, \ldots, x_v \in S_v$. We will define a subset $E_1 \subset E_0$ in the following way. We take $E_1 \cap T_1 = E_0 \cap S_1$, $E_1 \cap T_2 = E_0 \cap S_2$, ..., $E_1 \cap T_v = E_0 \cap S_v$. All $x \in E_0 \setminus (T_1 \cup \cdots \cup T_v)$ will be in E_1. This gives a subset $E_1 \subset E_0$ that can be expressed as a disjoint union of balls of radius $q^{-\lambda_1}$.

Let $\mathcal{E}_1$ be the collection of balls of radius $q^{-\lambda_1}$ whose disjoint union is E_1. Enumerate the balls of $\mathcal{E}_1$ as $B^{(1)}_1, \ldots, B^{(1)}_{M_1}$. For $\ell = 1, 2$, define $\Sigma^{(\ell)}_1$ to be the collection of v_ℓ tuples of distinct such balls, ordered lexicographically and identified in the usual way with the family of injections from $\{1, \ldots, v_\ell\}$ into $\{1, \ldots, M_1\}$. We then form the queue $\mathcal{Q}'_1$ consisting of 4-tuples of the form

$$\{(\ell, \sigma, 1) : 1 \leq \ell \leq 2; \sigma \in \Sigma^{(\ell)}_1\},$$

arranged so that $(\ell, \sigma, 1)$ precedes $(\ell', \sigma', 1)$ if $\ell < \ell'$, and so that $(\ell, \sigma, 1)$

precedes $(\ell, \sigma', 1)$ if $\sigma < \sigma'$. Arrive at the queue $\mathcal{Q}_1$ by appending the queue $\mathcal{Q}_1'$ to $\mathcal{Q}_0$.

Stage j We will now describe Stage j of the construction for $j > 1$. We follow essentially the same procedure as in Stage 1. We begin with a decreasing family of sets $E_0, \ldots E_{j-1}$. Each $E_{j'}$ is a union of balls of radius $q^{-\lambda_{j'}}$, the collection of which is called $\mathcal{E}_{j'}$. The family of $v_{\ell'}$ tuples of distinct balls in $\mathcal{E}_{j'}$ will be denoted $\Sigma_{j'}^{(\ell')}$. We have a queue $\mathcal{Q}_{j-1}$ consisting of 3-tuples (ℓ', σ', j'), where we have $0 \leq j' \leq j-1$, $1 \leq \ell \leq j'+1$, and $\sigma' \in \Sigma_{j'}^{(\ell')}$. The set E_{j-1} has the property that $f_{\ell'}(x_1, \ldots, x_v) \neq 0$ for $x_1 \in B_{\sigma'(1)}^{(j')} \cap E_{j-1}, \ldots, x_v \in B_{\sigma'(v_{\ell'})}^{(j')} \cap E_{j-1}$ for any (ℓ', σ', j') in the first $j-1$ elements of the queue $\mathcal{Q}_{j-1}$. Consider the jth queue element (ℓ, σ, j_0), where $\ell \leq j_0 \ll j$. Let $T_1, \ldots, T_v$ be the sets $B_{\sigma(1)} \cap E_{j-1}, \ldots, B_{\sigma(v_\ell)} \cap E_{j-1}$. We consider a variety of cases depending on whether we are considering Theorem 1.2.1, Theorem 1.2.2, or Theorem 1.2.3.

Case 1: Theorem 1.2.1 or 1.2.2 Let $f = f_\ell$. In this case, we have by assumption that $|\partial^\alpha f|$ is nonzero on all of $T_1 \times \cdots \times T_v$ for an appropriate multi-index α. Let q^{-A} be the lower bound on this partial derivative. Select $\mu_j \geq \lambda_{j-1}$ to be larger than the quantity μ^* appearing in Proposition 5.2.3 or Proposition 5.2.4, as is appropriate. We can then apply Proposition 5.2.3 or Proposition 5.2.4 to the sets $T_1, \ldots, T_v$, with the quantity $\nu = \nu_j$ taken to be sufficiently large that the quantity $q^{-\lambda_j} := c_1 q^{-n\nu_j/D}$ appearing in Proposition 5.2.4 or in Proposition 5.2.3 is larger than $q^{-\nu_j(n/D+\epsilon_j)}$ Furthermore, we also need $q^{-\epsilon_j \nu_j} < e_{j-1}$, where e_{j-1} is the quantity appearing as c_0 in the appropriate proposition. We will also select $\nu_j > \exp(\mu_j)$.

Case 2: Theorem 1.2.3. We have that on $T_1 \times \cdots \times T_v$ that Df has a nonvanishing minor and that $D^2 f$ is continuous. By compactness, we conclude that Df is bounded below in absolute value by some value C_0 and the entries of Df are bounded above in absolute value by some number C_1 on $T_1 \times \cdots \times T_v$. We also have an upper bound C_2 on the operator norm of $D^2 f$. We can then select $\mu_j \geq \lambda_{j-1}$ to be larger than the quantity μ^* appearing in Proposition 5.2.5. We can then apply Proposition 5.2.5 to the sets $T_1, \ldots, T_v$ with the quantity ν_j taken to be sufficiently large that the quantity $q^{-\lambda_j} := c_1 q^{-\nu_j/D}$ appearing in Proposition 5.2.5 is larger than $q^{-\nu_j(n/D+\epsilon_j)}$. We will select $\epsilon_{j-1} = \frac{1}{2}$ in this case. We will also select ν_j so that $\nu_j > \exp(\mu_j)$.

In any case, we arrive at sets $S_1 \subset T_1, \ldots, S_v \subset T_v$ such that f_ℓ is nonzero for $(x_1, \ldots, x_v) \in S_1 \times \cdots \times S_v$. We will define a subset $E_j \subset E_{j-1}$ in the following way. We take $E_j \cap T_1 = E_{j-1} \cap S_1$, $E_j \cap T_2 = E_{j-1} \cap S_2$, $\ldots$, $E_j \cap T_v = E_{j-1} \cap S_v$. All $x \in E_{j-1} \setminus (T_1 \cup \cdots \cup T_v)$ will be in E_j. This gives a subset $E_j \subset E_{j-1}$ that can be expressed as a disjoint union of balls of radius $q^{-\lambda_j}$. Call the collection of such balls $\mathcal{E}_j$, and let $B_1^{(j)}, \ldots, B_{M_j}^{(j)}$ be an enumeration of the balls in $\mathcal{E}_j$. For each $1 \leq \ell \leq j$, we define $\Sigma_j^{(\ell)}$ to be the collection of v_ℓ-tuples of distinct balls in $\mathcal{E}_j$. We equip $\Sigma_j^{(\ell)}$ with the lexicographic order and identify $\Sigma_j^{(\ell)}$ with the set of injections from $\{1, \ldots, v_\ell\}$ into $\mathcal{E}_j$. Consider the queue $\mathcal{Q}'_j$ consisting of 3 tuples (ℓ, σ, j), where $1 \leq \ell \leq j+1$ and $\sigma \in \Sigma_j^{(\ell)}$. We order the queue $\mathcal{Q}'_j$ in the following way: (ℓ, σ, j) will precede (ℓ', σ', j) if $\ell < \ell'$, and (ℓ, σ, j) precedes (ℓ, σ', j) if $\sigma < \sigma'$. We append the queue $\mathcal{Q}'_j$ to $\mathcal{Q}_{j-1}$ to arrive at the queue $\mathcal{Q}_j$.

5.3.2 Hausdorff Dimension of E

We compute the Hausdorff dimension of the set E. Unlike the calculation in Chapter 3, we use the definition of Hausdorff dimension directly instead of appealing to Frostman's lemma.

Let $\mathcal{U}$ be a disjoint covering of a set E. Define the *s-contribution* of a ball V (not necessarily in $\mathcal{U}$) to be

$$s(V) := \sum_{\substack{U \in \mathcal{U} \\ U \subset V}} r(U)^s$$

where $r(U)$ is the radius. Note that if $U \in \mathcal{U}$, then we have that $s(U) = r(U)^s$, and that if $V_1, \ldots, V_r$ are disjoint subsets of V, then $s(V_1) + \ldots + s(V_r) \leq s(V)$.

Lemma 5.3.1. *Let V be a ball of radius $q^{-\mu_j}$, and let $s < D$, where D is the dimension promised for E in Theorem 1.2.1, 1.2.2, or 1.2.3. Suppose j is sufficiently large that $\frac{s}{D} < 1 - 10\epsilon_j$. Then:*

1. *If the majority of the volume of $\mathcal{U}$ contained in V is in balls of $\mathcal{U}$ of radius strictly larger than $q^{-\lambda_{j+1}}$, then $s(V) \geq \frac{1}{4} q^{-\mu_j s}$.*

2. *If the majority of the volume of $\mathcal{U}$ contained in V is in balls of $\mathcal{U}$ of radius no more than $q^{-\lambda_{j+1}}$, then V contains at least $q^{(\lambda_{j+1} - \mu_j)s}$ balls of radius $q^{-\lambda_{j+1}}$ that contain a ball of $\mathcal{U}$.*

Proof of 1. We consider two cases: the case in which

$$\sum_{\substack{U\in\mathcal{U}\\ r(U)\geq q^{-\nu_j}}} r(U)^n \geq \frac{q^{-\mu_j n}}{4} \tag{5.8}$$

and the case in which this inequality is not satisfied.

Case 1 If the inequality (5.8) is satisfied, then we have

$$\begin{aligned}\frac{q^{-\mu_j n}}{4} &\leq \sum_{\substack{U\in\mathcal{U}\\ r(U)\geq q^{-\nu_j}}} r(U)^n \\ &= \sum_{\mu_j\leq\rho\leq\nu_j} \#(\rho)q^{-n\rho} \\ &= \sum_{\mu_j\leq\rho\leq\nu_j} \#(\rho)q^{-s\rho}q^{(s-n)\rho} \\ &\leq \sum_{\mu_j\leq\rho\leq\nu_j} \#(\rho)q^{-s\rho}q^{(s-n)\mu_j}\end{aligned}$$

where $\#(\rho)$ is the number of balls of radius $q^{-\rho}$ in $\mathcal{U}$, and the last line holds because $s-n$ is negative. Dividing both sides of the inequality by $q^{(s-n)\mu_j}$ gives

$$\sum_{\mu_j\leq\rho\leq\nu_j} \#(\rho)q^{-s\rho} \geq \frac{q^{-s\mu_j}}{4}$$

as desired.

Case 2 Suppose that the inequality (5.8) is not satisfied. Let $\mathcal{U}'$ be the collection of balls U' of radius $q^{-\nu_j}$ that contain a ball of $\mathcal{U}$. By Proposition 5.2.4, Proposition 5.2.3, or Proposition 5.2.5 whichever is appropriate, we have that at least an e_j-fraction of the balls of radius $q^{-\nu_j}$ contained in B intersect E, and since the balls of radius larger than $q^{-\nu_j}$ cover a set of measure strictly smaller than $\frac{q^{-\mu_j n}}{4}$, it follows that $\mathcal{U}'$ must cover a set of measure at least $\frac{q^{-\mu_j n}}{4}$. Therefore $\mathcal{U}'$ must consist of at least $\frac{e_j q^{(\nu_j-\mu_j)n}}{4}$ balls.

Each ball in $\mathcal{U}'$ intersects E and therefore contains at least one ball in $\mathcal{E}_{j+1}$. Thus, letting $\mathcal{U}''\subset\mathcal{U}$ be the collection of balls in $\mathcal{U}$ that are contained in a ball in $\mathcal{U}'$, we have that

$$\sum_{U\in\mathcal{U}''} r(U)^s \geq e_j q^{-\frac{n}{D}\nu_j s} q^{\nu_j n-\mu_j n}$$
$$= \frac{e_j}{4} q^{\nu_j(n-\frac{n}{D}s)}.$$

Since we assumed $\frac{s}{D} < 1 - 10\epsilon_j$, we know that the coefficient on ν_j is larger than $10\epsilon_j$. Because $\nu_j > \exp(\mu_j)$ and because $q^{-\epsilon_j\nu_j} < e_j$, it follows that, for sufficiently large j, this is larger than $\frac{1}{4}q^{-\mu_j s}$. □

Proof of 2. This argument is similar to Case 2 above. We define $\mathcal{U}'$ to be the collection of balls of radius $q^{-\lambda_{j+1}}$ that contain a ball of $\mathcal{U}$. By the statements in Propositions 5.2.4, 5.2.3 and 5.2.5, we have that V contains at least $e_j q^{\nu_j-\mu_j}$ balls of radius $q^{-\lambda_{j+1}}$ that intersect E. Therefore, if at least half of the volume of $\mathcal{U}'$ is contained in balls of radius at most $q^{-\lambda_{j+1}}$, this means that there must be at least $e_j q^{(\nu_j-\mu_j)n}/2$ balls of radius $q^{-\mu_{j+1}}$ that contain a ball of $\mathcal{U}'$. But because $\frac{s}{D} < 1 - 10\epsilon_j$, it follows from the fact that $\nu_j \geq \exp(\mu_j)$ and the choice of λ_j that $e_j q^{\nu_j-\mu_j}/2 > q^{(\lambda_{j+1}-\mu_j)s}$ for sufficiently large j, as in Case 2 above. □

In the second part of the statement, provided that no more than a quarter of the measure of $\mathcal{U}'$ is contained in balls of radius between $q^{-\mu_{j+1}}$ and $q^{-\lambda_{j+1}}$, we can in fact replace λ_{j+1} by μ_{j+1} because if B is a ball of radius $q^{-\lambda_{j+1}}$ that intersects E, then each ball of radius $q^{-\mu_{j+1}}$ contained in B also intersects E. Therefore, the proposition also holds with μ_{j+1} replaced by λ_{j+1}.

If, on the other hand, at least a quarter of the volume is contained in such balls, then we can replace $\mathcal{U}$ by a covering $\mathcal{U}'$ in which any ball of radius $q^{-\lambda_{j+1}}$ containing such an intermediate ball is replaced by $\mathcal{U}'$; the s-contribution of $\mathcal{U}'$ will then be bounded by q^s times the s-contribution of $\mathcal{U}$.

So up to a constant factor, the statement in the preceding proposition also applies with μ_{j+1} in place of λ_{j+1}. This will allow us to use an inductive argument to compute the Hausdorff dimension of the set E:

Proposition 5.3.2. *Let V be a ball of radius $q^{-\mu_j}$ in $\mathcal{E}_j$, and let $\mathcal{U}$ be a covering of $V \cap E$ by balls of radius larger than $q^{-\mu_k}$ contained in V, where $k > j$. Let $s < D$. If j is sufficiently large depending on s, then for the covering $\mathcal{U}$ we have $s(V) \geq Cq^{-\mu_j s}$ for some appropriate constant C.*

Proof. Let $s < t < n/D$. We prove this statement by induction on $k - j$. If $k - j = 1$, this statement is implied by part 1 of Lemma 5.3.1 and the discussion following that lemma. So it only remains to show the inductive step.

Suppose first that the majority of the volume of $\mathcal{U}$ is contained in balls of radius strictly larger than $q^{-\mu_{j+1}}$. Then we can apply part 1 of Lemma 5.3.1, and the following discussion, to conclude that $s(V) \geq Cq^{-\mu_j s}$, and we're done. Therefore, we can assume that the majority of the volume of $\mathcal{U}$ is contained in balls of radius at most $q^{-\mu_{j+1}}$. Then by part 2 of Lemma 5.3.1, there exist balls $V_1, \ldots, V_r$ of radius $q^{-\mu_{j+1}}$, where $r > q^{(\mu_{j+1}-\mu_j)s}$, such that each ball V_j contains an element of $\mathcal{U}$. By the additivity of s we have $s(V_1) + \ldots + s(V_r) \leq s(V)$, and by the inductive assumption we have that $s(V_t) \geq Cq^{-\mu_{j+1}s}$ for each t. Thus $s(V) \geq Cq^{-\mu_j s}$ as desired. □

5.3.3 Minkowski Dimension of E

Lemma 5.3.3. *The Minkowski dimension of the set E is equal to* 1 *(in the case of Theorem 1.2.2) or n (in the case of Theorems 1.2.1 and 1.2.3).*

Proof. Let $N_\mu(E)$ be the number of closed balls of radius $q^{-\mu}$ that are required to cover E. Notice that this is equivalent to the number of balls of radius $q^{-\mu}$ that intersect E. So we need to count the number of such balls that intersect E. Let $q^{-\mu_j}$ denote the radius of the balls in $\mathcal{E}_j$.

If $\mu = \mu_j$ for some j, and B is a ball of radius $q^{-\mu_{j-1}}$ that is not contained in $T_1, \ldots, T_v$ at stage j of the construction, then the number of balls of radius $q^{-\mu_j}$ required to cover B is precisely $\left(\frac{q^{-\mu_{j-1}}}{q^{-\mu_j}}\right)^n$. This is greater than or equal to $(q^{\mu_j})^{-n+\epsilon}$ (provided that q^μ is sufficiently small) by the growth rate of the ν_j.

Now suppose $\mu_j < \mu < \mu_{j+1}$, and consider any ball B of radius $q^{-\mu_{j-1}}$ such that B is not contained in $T_1 \cup \cdots \cup T_v$ at either stage j or stage $j+1$ of the construction. Such a ball will always exist provided that j is large enough.

Then by the argument from before, E intersects all of the balls of radius $q^{-\mu}$ contained in B, and thus at least $(q^{-\mu_j})^{-n+\epsilon}$ of radius $q^{-\mu_j}$ inside the ball B. Evidently E must then intersect at least $(q^{-\mu_j+\mu})^n \cdot q^{-\mu_j(-n+\epsilon)} \geq q^{\mu(n-\epsilon)}$ of the balls of radius $q^{-\mu}$, as desired. □

This completes the proofs of Theorems 1.2.1, 1.2.2, and 1.2.3.

5.4 Simultaneous Avoidance

The other result applies to a (possibly uncountable) family of functions $f(x_1, \ldots, x_v)$ that have agreeing, unchanging, nondegenerate linearizations along the diagonal. The specific conditions are outlined in the statement of Theorem 1.2.4.

As in the case of the Theorems 1.2.2, and 1.2.3, the construction is a Cantor-like set constructed in the same manner as Chapter 3. This lemma outlines the strategy for a single step of the construction.

Lemma 5.4.1. *Let $B_1, B_2 \subset B$ be distinct (and thus disjoint) balls of radius $q^{-\lambda}$. Let $\mathcal{A} \subset \{1, \ldots, v\}$ be an arbitrary nonempty proper subset of $\{1, \ldots, v\}$. Then we can find $B_1' \subset B_1$, $B_2' \subset B_2$ of radius at least $C_1 q^{-\lambda}$ such that $|\alpha_1 x_1 + \cdots + \alpha_v x_v| \geq C_1 r$ for $x_j \in B_1'$ if $j \in \mathcal{A}$ and $x_j \in B_2'$ if $j \notin \mathcal{A}$, where C_1 is a constant depending on the vector α, the local field K, and on $\mathcal{A}$.*

Proof. Since the bounds in this lemma are allowed to depend on α, we will normalize α so that every component of α is in R and at least one component of α is invertible in R; that is, the norm of α will be taken to be 1.

Assuming this normalization, let $C_1 = q^{-1} \left| \sum_{j \notin \mathcal{A}} \alpha_j \right|$. This was assumed to be strictly positive in the statement of Theorem 1.2.4.

Then, selecting B_1' and B_2'' to be any balls of radius $C_1 q^{-\lambda}$ contained in B_1 and B_2, we consider the set $\alpha \cdot \mathcal{B}$, where $\mathcal{B} = B^{(1)} \times \cdots \times B^{(v)}$, and $B^{(j)} = B_1'$ if $j \in \mathcal{A}$ and $B^{(j)} = B_2''$ otherwise. Since each component of α is in R, we have immediately that $\alpha \cdot \mathcal{B}$ is contained in a ball $A \subset R$ of radius at most $C_1 q^{-\lambda}$. If this ball is not the unique $C_1 q^{-\lambda}$-ball containing zero, then we can take $B_2' = B_2''$ to complete the proof. If not, then select any element $b \in R$ with $|b| = q^{-\lambda-1}$ and define $B_2' := B_2'' + b \subset B_2$. Then defining the ball $\mathcal{B}'$ to be $B^{(1)*} \times \cdots \times B^{(v)*}$, with $B^{(j)*} = B_1'$ if $j \in \mathcal{A}$ and $B^{(j)*} = B_2'$ otherwise, we have that $\alpha \cdot \mathcal{B}'$ maps into $A + b \sum_{j \in \mathcal{A}^C} \alpha_j$, which is a ball of radius $C_1 q^{-\lambda}$ that does not contain 0. □

This lemma can be applied iteratively in the following way: Starting with a ball B of radius $q^{-\lambda}$, we can pick two balls $B_1, B_2 \subset B$ of radius $q^{-\lambda-1}$. Then, for some $\mathcal{A}$, apply Lemma 5.4.1 to arrive B_1' and B_2'. Now, pick a different $\mathcal{A}$ and apply the lemma to these balls to arrive at B_1'' and B_2''. Repeat this process for all nonempty proper subsets $\mathcal{A} \subset \{1, \ldots, v\}$, and we arrive at $B_1^* \subset B_1, B_2^* \subset B_2$ where B_1 and B_2 have radius at least $C^* q^{-\lambda}$ for some C^*, and $\alpha_1 x_1 + \cdots + \alpha_v x_v$ is at least $C^* q^{-\lambda}$ in absolute value for all $x_1, \ldots, x_v \in B_1^* \cup B_2^*$ not all coming from B_1^* and not all coming from B_2^*.

Proposition 5.4.2. *There exists C^* depending only on α and on the local field K with the following property. For any ball B with $q^{-\lambda} := radius(B)$, there exist $B_1^*, B_2^* \subset B$ such that B_1^*, B_2^* are balls of radius $C^* q^{-\lambda}$ and such that $\alpha_1 x_1 + \cdots + \alpha_v x_v$ has absolute value at least $C^* q^{-\lambda}$ for $x_1, \cdots, x_v \in B_1^* \cup B_2^*$ provided that not all of the $x_1, \cdots, x_v$ are in B_1^*, and not all of the $x_1, \ldots, x_v$ are in B_2^*.*

We are now ready to prove Theorem 1.2.4.

Proof of Theorem . This construction closely follows the one appearing in Chapter 3.

In order to construct the set E, we begin by selecting a ball E_0 of radius $q^{-\lambda_0}$ where λ_0 is chosen sufficiently large so that $Cq^{-\lambda_0}v < (C^*)^3$, where C^* is the constant from Proposition 5.4.2.

We will construct the set E by applying Proposition 5.4.2 inductively. E_j will always be a union of 2^j balls of radius $(C^*)^j q^{-\lambda_0}$ with the property that $|\alpha \cdot (x_1, \ldots, x_v)| \geq (C^*)^j q^{-\lambda_0}$ for $x_1, \ldots, x_v \in E_j$ unless $x_1, \ldots, x_v$ all belong to the same ball in E_j. To construct E_{j+1}, we apply Proposition 5.4.2 to each of the balls that constitute E_j. The result will be a collection E_{j+1} of 2^j balls of radius $(C^*)^{j+1} q^{-\lambda_0}$ with the property that $|\alpha \cdot (x_1, \ldots, x_v)| \geq (C^*)^{j+1} q^{-\lambda_0}$ unless $x_1, \ldots, x_v$ belong to the same ball in E_{j+1}. Let $E = \bigcap_{j=0}^{\infty} E_j$. It follows from a routine computation that the Cantor set E has positive Hausdorff dimension.

It remains to be seen that $f(x_1, \ldots, x_v)$ is nonzero for $x_1, \ldots, x_v \in E$ not identical. To see this, notice that there exists a minimal ball B such that $x_1, \ldots, x_v \in B$. Say that this ball B is a basic ball of E_{j-1}. Let B_1 and B_2 be the children of this ball in the construction. Then we have $|\alpha \cdot (x_1, \ldots, x_v)| \geq (C^*)^j q^{-\lambda_0}$. Since $x_1, \ldots, x_v \in B_1 \cup B_2 \subset B$, we have that

$$(|x_2 - x_1|^2 + \cdots + |x_v - x_1|^2) \leq v(C^*)^{2j-2} q^{-2\lambda_0}.$$

Therefore we have that

$$|f(x_1, \ldots, x_v)| \geq (C^*)^j q^{-\lambda_0} > 0$$

as long as

$$Cv(C^*)^{2j-2} q^{-2\lambda_0} < (C^*)^j q^{\lambda_0}$$

by the ultrametric inequality. Noting that $Cq^{-\lambda_0}v < (C^*)^3$, we get

$$Cv(C^*)^{2j-2} q^{-2\lambda_0} \leq (C^*)^{2j+1} q^{-\lambda_0} \leq C^* j q^{-\lambda_0}$$

as desired. □

Chapter 6

Besicovitch Sets

6.1 The Kakeya Problem

In the early 20th century, Kakeya asked the following question: Let E be a measurable subset of $\mathbb{R}^2$ through which a line segment of unit length can be continuously rotated all the way around, so that the line segment ends up in the same orientation as it began. How small is it possible for the Lebesgue measure of E to be? This problem is known as the **Kakeya needle problem**, and a set E with this property is called a **Kakeya needle set**. Evidently, a circle with radius $\frac{1}{2}$ is a Kakeya needle set with Lebesgue measure $\frac{\pi}{4}$. Kakeya conjectured that the smallest such set was a 3-pointed hypocycloid.

In 1928, Besicovitch showed, remarkably, that such a set can have arbitrarily small Lebesgue measure. In order to construct such sets, Besicovitch began with a triangle, and performed a sequence of translations of the triangle in order to minimize the possible area. Then, he connected various parts of the figure with narrow hallways to arrive at a Kakeya needle set.

As a byproduct of this construction, Besicovitch arrived at a method for constructing a subset of $\mathbb{R}^2$ of Lebesgue measure zero that contains a unit-length line segment pointing in every direction. Such a set is now known as a **Besicovitch set** or **Kakeya set**.

Besicovitch's construction also implies the existence of measure-zero Besicovitch sets in dimensions $d > 2$: Simply taking the Cartesian product of a 2-dimensional Besicovitch set with the rectangle $[0, 1]^{d-2}$ gives an example.

Although Besicovitch sets can have Lebesgue measure zero, for $d > 2$ it is unknown whether a Besicovitch set in $\mathbb{R}^d$ can have Hausdorff dimension strictly less than d. The question of whether such sets exist is known as the **Kakeya problem**. The **Kakeya conjecture** is the claim that a Besicovitch set in $\mathbb{R}^d$ necessarily has Hausdorff dimension d. This was established in the $d = 2$ case by Roy Davies [10].

6.2 The Kakeya Problem for Finite Fields

In order to help tackle the study of Euclidean Kakeya problems, Tom Wolff [54] introduced the finite field version of the Kakeya conjecture. Let $\mathbb{F}_q$ be the finite field with q elements. A **Besicovitch Set** in $\mathbb{F}_q^d$ is a subset of $\mathbb{F}_q^d$ that contains a line $t\mathbf{a}_\omega + \mathbf{b}_\omega$ with a_ω parallel to ω for every direction ω in the projective space $\mathbb{P}\mathbb{F}_q^{d-1}$. The **Finite Field Kakeya Conjecture** asks whether a Besicovitch set in $\mathbb{F}_q^d$ must contain a constant (depending on d but not q) fraction of the q^d elements of $\mathbb{F}_q^d$.

Theorem 6.2.1 (Finite Field Kakeya Conjecture)**.** *Every Besicovitch set in $\mathbb{F}_q^d$ contains at least $C_d q^d$ elements.*

This conjecture was established by Dvir in 2009 [12]. Dvir used a technique known as the polynomial method to establish this result.

Proof taken from [12]. Let K be some Besicovitch set in $\mathbb{F}_q^d$. Then there is a polynomial $p \neq 0$ of degree $\lesssim_d |K|^{1/d}$ that vanishes on all of K. Let s be the degree of this polynomial. Let $y \in \mathbb{F}_q^d$ and let $x \in \mathbb{F}_q^d$ be such that K contains the line $x+ty$. Because p vanishes on K we have that $p(x+ty) = 0$ on all of K. If we assume that $|K| \lesssim_d (q-1)^d$, then we get that the degree s of p is no more than $q-1$, and therefore $p(x+ty)$, as a polynomial in t, is the zero polynomial. The coefficient of the t^s term of this polynomial is precisely $p_s(y)$, the homogeneous degree s part of p. Then $p_s(y)$ is a nonzero polynomial that vanishes for all y, which is a contradiction. □

This short proof showed the power of the polynomial method, and since this proof of Dvir emerged in 2009, variants of the polynomial method have been applied to solve all kinds of problems in incidence geometry, additive combinatorics, and harmonic analysis.

The result in [12] was improved by Ellenberg, Oberlin, and Tao in [17]. In the Euclidean setting, the Kakeya conjecture is implied by an estimate on the Kakeya maximal operator. Ellenberg, Oberlin, and Tao define an analogue of the Kakeya maximal operator for finite fields:

Definition 6.2.2 (Kakeya Maximal Operator)**.** *Let $\mathbb{P}\mathbb{F}_q^{d-1}$ $d-1$-dimensional projective space over $\mathbb{F}_q$, and let f be a complex-valued function defined on $\mathbb{F}_q^d$. Then the Kakeya maximal function Mf is defined by the formula*

$$Mf(\omega) = \frac{1}{q} \sup_x \sum_t |f(x+ty)|$$

where the vector y *points in the direction* ω *and* t *ranges over* $\mathbb{F}_q$ *(the sum does not depend on which* y *is chosen for each* ω*).*

Ellenberg, Oberlin and Tao obtain the following L^d-to-L^d estimate for the Kakeya maximal operator M:

Theorem 6.2.3 (Kakeya maximal operator estimate on $\mathbb{F}_q$)**.** *The Kakeya Maximal operator* M *satisfies the bound*

$$||Mf||_{L^d(\nu)} \leq C_d ||f||_{L^d(\mu)}$$

where the measure μ *is the normalized counting measure on* $\mathbb{F}_q^d$*, and* ν *is the normalized counting measure on* $\mathbb{PF}_q^{d-1}$*.*

In the last section of [17], the authors posed the question of whether Theorems 6.2.1 and 6.2.3 can be shown for local fields.

Chapter 7

Local Field Besicovitch Sets

7.1 Background

7.1.1 Previous Constructions

In 1987, Sawyer [45] constructed a measure-zero Besicovitch set in $\mathbb{R}^2$ using a novel trick. Sawyer observed that, for any Borel measurable function ϕ, the family of line segments $E := \{(x, tx - \phi(t)) : x \in [0,1]; t \in \mathbb{R}\}$ forms a Besicovitch set (with the minor caveat that this set does not contain a vertical line segment). Of course, it is enough to restrict t to be in $[0,1]$ because $\mathbb{R}$ is a countable union of dilates of the interval $[0,1]$ and a reflection about the point 0, and thus a Besicovitch set can be obtained by stretching the line segments vertically and reflecting about the line $y = 0$. If the function ϕ is chosen appropriately, the set E can be taken to have Lebesgue measure 0 in $\mathbb{R}^2$.

Sawyer uses the following strategy to construct an appropriate function ϕ. Suppose that ϕ has the property that, for each $a \in [0,1]$, the range of the function $\ell_a(t) = at - \phi(t) : [0,1] \to \mathbb{R}$ has measure zero as a subset of $\mathbb{R}$. Then we have that

$$\begin{aligned} |E| &= \iint [0,1] \mathbf{1}_E(x,y)\, dx\, dy \\ &= \int_{[0,1]} |\{y : y = tx - \phi(t) \text{ for some } t\}|\, dx \end{aligned}$$

We now observe that the set $\{y : y = tx - \phi(t) \text{ for some } t\}$ must have measure zero for any fixed x: this follows from the choice of ϕ. Thus the Lebesgue measure of E is zero.

So it is possible to construct a measure-zero Besicovitch set by constructing a function ϕ with this property. We will define ϕ as an infinite sum of piecewise constant functions ϕ_j. Let $q_1, q_2, \ldots$ be a sequence of rational numbers in $[0,1]$ that contains each rational number in $[0,1]$ an infinite number of times. Define $\phi_1(t)$ to be a function that is equal to $q_1 \cdot \frac{0}{1} = 0$ everywhere.

Next, define $\phi_2(1/2) = \frac{q_2}{2}$, and define $\phi_2(t)$ by

$$\phi_2(t) = \begin{cases} q_2 \cdot \frac{0}{2} & \text{if } 0 \le t < \frac{1}{2} \\ q_2 \cdot \frac{1}{2} & \text{if } \frac{1}{2} \le t \le 1 \end{cases}$$

In particular, notice that $\phi_2(t)$ is bounded above by $\frac{q_2}{2} \le \frac{1}{2}$. Note further that the range of $q_2 t - \phi_2(t)$ is contained in the interval $[0, \frac{q_2}{2}]$.

Now we define $\phi_3(t)$ in the following way:

$$\phi_3(t) = \begin{cases} q_3 \cdot \frac{0}{6} & \text{if } \frac{0}{6} \le t < \frac{1}{6} \\ q_3 \cdot \frac{1}{6} & \text{if } \frac{1}{6} \le t < \frac{2}{6} \\ q_3 \cdot \frac{2}{6} & \text{if } \frac{2}{6} \le t < \frac{3}{6} \\ q_3 \cdot \frac{0}{6} & \text{if } \frac{3}{6} \le t < \frac{4}{6} \\ q_3 \cdot \frac{1}{6} & \text{if } \frac{4}{6} \le t < \frac{5}{6} \\ q_3 \cdot \frac{2}{6} & \text{if } \frac{5}{6} \le t \le \frac{6}{6} \end{cases}$$

Now, we have that $\phi_3(t)$ is bounded above by $\frac{q_3}{3} \le \frac{1}{3}$, and that, because ϕ_1 and ϕ_2 are both constant on the interval $[0, \frac{1}{2})$, we have, for $t \in [\frac{0}{2}, \frac{1}{2})$

$$\left| q_3 t - (\sum_{r=1}^{3} \phi_r(t)) + (\phi_1(0) + \phi_2(0)) \right|$$

$$\begin{aligned} &= |q_3 t - \phi_3(t) + (\phi_2(0) - \phi_2(t)) + (\phi_1(0) - \phi_1(t))| \\ &= |q_3 t - \phi_3(t)| \\ &\le \frac{q_3 t}{6} \end{aligned}$$

We get a similar inequality for $t \in [\frac{1}{2}, 1]$ where $\phi_1(0)$ and $\phi_2(0)$ are replaced by $\phi_1(\frac{1}{2})$ and $\phi_2(\frac{1}{2})$.

We then continue this strategy. We define ϕ_M to be constant on intervals of the form $[\frac{j}{M!}, \frac{j+1}{M!})$, and to be equal to $q_M \cdot \frac{j-k}{M!}$ on this interval, where k is the largest multiple of M that is less than or equal to j. Thus, $0 \le \phi_M \le \frac{1}{(M-1)!}$, and ϕ_M is constant on intervals of the form $[\frac{j}{M!}, \frac{j+1}{M!})$. Furthermore, since $\phi_1, \ldots, \phi_{M-1}$ are constant on intervals of the form $[\frac{j}{(M-1)!}, \frac{j+1}{(M-1)!})$, we have that $q_M x - \sum_{r=1}^{M} \phi_r(x) + \sum_{r=1}^{M-1} \phi_r(\frac{k}{(M-1)!})$ is bounded above by $\frac{1}{M!}$ on the interval $[\frac{k}{(M-1)!}, \frac{k+1}{(M-1)!})$. Thus, $q_M x - \sum_{r=1}^{M} \phi_r(x)$ is contained within $(M-1)!$ intervals of length $\frac{1}{M!}$, a set with Lebesgue measure at most $\frac{1}{M}$.

Furthermore, if we let c be a number such that $|c - q_M| < \epsilon$, then the error in approximating $cx + d$ by $q_M x$ for an appropriate d on the interval $[\frac{k}{(M-1)!}, \frac{k+1}{(M-1)!})$ is bounded above by $\frac{\epsilon}{(M-1)!}$. Thus we get that $cx - \sum_{j=1}^{M} \phi_j(x)$ is contained in at most $(M-1)!$ intervals of length at most $\frac{\epsilon}{(M-1)!} + \frac{1}{M!}$ for such numbers c. Using the estimate $0 \leq \phi(x) - \sum_{j=1}^{M} \phi_j(x) = \sum_{j=(M+1)}^{\infty} \phi_j(x) \leq \sum_{j=(M+1)}^{\infty} \frac{1}{(j-1)!} \leq \frac{2}{M!}$, we get that for such c, $cx - \phi(x)$ is contained in at most $(M-1)!$ intervals of length at most $\frac{3}{M!} + \frac{\epsilon}{(M-1)!}$, a set of measure at most $\frac{3}{M} + \epsilon$. By the density of the rational numbers and by the choice of the sequence q_j, it follows that $\phi(x) - cx$ has measure zero for any number $c \in [0, 1]$.

Sawyer extends this observation in the following way: by replacing the lines qx by an appropriate family of C^1 functions, it is possible to construct a Borel measurable function $\phi(t) : [0, 1] \to \mathbb{R}$ with the property that, for any differentiable function $f(t) : [0, 1] \to \mathbb{R}$, the range of the function $f - \phi$ has measure zero. Furthermore, Sawyer selects the function ϕ in a way that guarantees that the function ϕ is right-continuous and has only countably many discontinuities. This construction allows for measure zero sets containing translates of a one-dimensional families of smooth curves that are parameterized in a smooth way.

Sawyer's construction was improved by Wisewell [52, Lemma 4]. Wisewell observed that Sawyer's method could be adapted to construct a Borel measurable function ψ with the following property.

Theorem 7.1.1 (Wisewell's function)**.** *There exists a function $\psi : \mathbb{R}^p \to \mathbb{R}^q$ with the following property: Let $f(y, \omega) : \mathbb{R}^p \times \mathbb{R}^q \to \mathbb{R}^{n-d}$, with $p \leq n-d \leq q$ and $d < n$. If f is C^1 and $\frac{\partial f}{\partial \omega}$ always has rank $n - d$ and is Lipschitz, then the range of $f(\cdot, \psi(\cdot))$ is of measure zero.*

This function ψ is then used in the following way. Let $\Gamma(y, \omega)$ be the surface consisting of points $(t, f(y, \omega, t))$ for $t \in \mathbb{R}^d$, $f : \mathbb{R}^p \times \mathbb{R}^q \times \mathbb{R}^d \to \mathbb{R}^{n-d}$ a differentiable function with full rank as a function of y and ω for a.e. t. This is a d-dimensional surface in $\mathbb{R}^n$ parameterized by the variable t. The family itself is parameterized by y and ω. Using this function ψ, Wisewell constructs a set E of measure zero containing the surface $\Gamma(y, \psi(y))$ for every $y \in \mathbb{R}^p$. Of special note is that this function ψ does not depend on f.

7.1.2 A Besicovitch Set in $\mathbb{F}_q[[t]]^2$

As a matter of fact, Sawyer's Besicovitch set construction [45] can be adapted to all non-archimedean local fields. This was first discovered by Wright in an unpublished work in the 1990s. Nonetheless, in 2010, Ellenberg, Oberlin, and Tao [17] proposed the problem of constructing a measure-zero Besicovitch set in $\mathbb{F}_q[[t]]^2$. Dummit and Hablicsek [11] constructed such a set using a linear-algebraic method.

Let $a \in \mathbb{F}_q[[t]]$. Then a has an expansion of the form (4.1). Here, the coefficients are elements of $\mathbb{F}_q$, addition is defined componentwise, and multiplication is defined as multiplication of power series. Dummit and Hablicsek define the $*$ function $a \mapsto a^*$ where

$$a_i^* = \begin{cases} 0 & \text{if } i = 2^k - 2 \text{ for some natural number } k \\ a_{i+1} & \text{otherwise.} \end{cases}$$

This $*$-function is used to construct a half-Besicovitch set H:

$$H := \{(x, y) \in \mathbb{F}_q[[t]]^2 : ax + y = a^* \text{ for some } a \in \mathbb{F}_q[[t]]\}. \tag{7.1}$$

This set of points contains a line of "slope" a for every $a \in \mathbb{F}_q[[t]]$. Although this does not quite cover all of the possible directions for lines in $\mathbb{F}_q[[t]]^2$, a Besicovitch set can be constructed by taking the union of this set with its "transpose" in which the roles of x and y are swapped. Therefore, establishing that H has Haar measure zero yields a measure-zero Besicovitch set construction in $\mathbb{F}_q[[t]]^2$.

In order to show that H has Haar measure zero, the equation appearing in (7.1) is re-written as an infinite system of linear equations over $\mathbb{F}_q$. Notice that this step is impossible for other discrete valuation rings such as $\mathbb{Z}_p$: in $\mathbb{Z}_p$ addition is not done term-by-term but has a carry as well. This spoils the linearity so the construction does not work over such rings.

The linear system that characterizes H consists of equations of the form

$$a_n x_0 + a_{n-1} x_1 + \cdots + a_0 x_n + y_n = a_n^*. \tag{7.2}$$

One key point here is that the $n = 0$ equation does not involve any component of a other than a_0; the equations for $n \leq 2$ do not involve any component of a other than a_0, a_1, a_2; and, in fact, the $n \leq 2^k - 2$ equation does not involve any component of a other than $a_0, a_1, \ldots, a_{2^k-1}$.

A point (x, y) belongs to H if and only if the system of equations (7.2) has a solution in a. Dummit and Hablicsek interpret the Haar measure on $\mathbb{F}_q[[t]]$ as a probability measure and show that, conditioned on the system of equations for $n \leq 2^k - 2$ having exactly q^ℓ solutions, the system of equations with $n \leq 2^{k+1} - 2$ will have 0 solutions with probability $\frac{q-1}{q^{\ell+2}}$, q^ℓ with probability $1 - \frac{q}{q^{\ell+1}}$, and $q^{\ell+1}$ with probability $\frac{1}{q^{\ell+2}}$. By a Markov-chain argument, it follows that the number of solutions to (7.2) for a randomly chosen point (x, y) will, with probability 1, be equal to zero at some finite cutoff point. Therefore H has measure zero.

7.2 Adapting to Local Fields

7.2.1 Construction of ϕ

The construction of this function ϕ follows the construction of ϕ in [45] and ψ in [52]. For convenience, the function ϕ will be taken to be defined on R, the ring of integers of K, instead of all of K; this is sufficient because we can define extend ϕ to all of K periodically.

We will fix a family of coset representatives of K. Define $S_k \subset K$ to be the set of elements of K whose lowest-degree term is at least $-\log k$ and whose highest-degree term has degree at most k. Notice that the set S_k is finite, and $\bigcup_{k=0}^{\infty} S_k$ is dense in K. We define the families Ω_k of functions $R^p \to S_k$ to be the functions that are locally constant on balls of radius ℓ^{-k}, where ℓ is the number of elements of the residue field of K. Such locally constant functions are continuous (in fact they are smooth). Because R contains only finitely many open balls of radius ℓ^{-k} and S_k is finite, it follows that each set Ω_k is also finite. It is easily seen that $\bigcup_k \Omega_k$ is the set of all locally constant functions from R^p to K, which is a dense subspace of the space of continuous functions on R^p(recalling that R^p is compact, so continuous functions are bounded).

We let r_j be a family of all the $q \times p$ matrices with elements in Ω_0, followed by a list of all the matrices whose entries are contained in Ω_1, et cetera. Each matrix consisting of elements of Ω_k occurs infinitely many times in the sequence r_j, because $\Omega_k \subset \Omega_{k'}$ for all $k' > k$.

An analogue of the factorial expansion, which was key to the constructions in [52] and [45], is provided by the sequence of projection functions p_j. For nonnegative integers j, define $\eta(j) = j(j+1)/2$. Given $x \in R$ with expansion (4.1), define the projection $p_j(x)$ to be the finite sum

$$\sum_{i=\eta(j)}^{\eta(j+1)-1} x_i t^i.$$

Then we have that $|p_j(x)| \leq \ell^{-\eta(j)}$. For vectors $x \in R^p$, we define $p_j(x)$ to be the componentwise application of p_j. We then take

$$\phi(x) := \sum_{k=0}^{\infty} r_j(x) p_j(x),$$

an absolutely convergent sum.

Note that each function $r_j(x)p_j(x)$ is a locally constant K^q-valued function on R^p. Because the sum of the $r_j(x)p_j(x)$ is absolutely and uniformly convergent on R^p, it follows that $\phi(x)$ is a continuous function from R^p to K^q. In fact, ϕ is bounded with $|\phi(x)| \leq 1$ for all x; hence, the range of ϕ is contained in R^q.

7.2.2 Estimates on the Range of $f(x, \phi(x))$

We are now ready to prove Theorem 1.3.1. In order to prove Sawyer's result [45], points of the form $x = \frac{1}{N!}$, and their images under ϕ, were used as landmarks for the function ϕ. We will use the partial sums

$$x^{(m)} := \sum_{j=0}^{m-1} p_j(x) \tag{7.3}$$

and

$$\phi^{(m)}(x) = \sum_{j=0}^{m-1} r_j(x) p_j(x) \tag{7.4}$$

as landmarks for the local field setting.

We will show that the range of $f(x, \phi(x))$ has measure at most ℓ^{-A} for any fixed $A > 0$, showing that the range must therefore have measure zero.

The function $f(x, \phi(x))$ is decomposed into six pieces $\mathrm{I}, \ldots, \mathrm{VI}$ with VI being the main term- which will only take finitely many values.

The six pieces are

$$\begin{aligned}
\mathrm{I} &:= f(x,\phi(x)) - f(x^{(N)},\phi(x)) - \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))}(x - x^{(N)})\\
\mathrm{II} &:= f(x^{(N)},\phi(x)) - f(x^{(N)},\phi^{(N)}(x)) - \left.\frac{\partial f}{\partial y}\right|_{(x^{(N)},\phi(x))}(\phi(x) - \phi^{(N)}(x))\\
\mathrm{III} &:= \left.\frac{\partial f}{\partial y}\right|_{(x^{(N)},\phi(x))}(\phi(x) - \phi^{(N)}(x)) - \left.\frac{\partial f}{\partial y}\right|_{(x,\phi(x))}(\phi(x) - \phi^{(N)}(x)).\\
\mathrm{IV} &:= \left.\frac{\partial f}{\partial y}\right|_{(x,\phi(x))}(\phi(x) - \phi^{(N+1)}(x)) + \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))}(x - x^{(N+1)})\\
\mathrm{V} &:= \left.\frac{\partial f}{\partial y}\right|_{(x,\phi(x))} r_N(x)p_N(x) + \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))} p_N(x)\\
\mathrm{VI} &:= f(x^{(N)},\phi^{(N)}(x)).
\end{aligned}$$

It is not difficult to verify that the sum $\mathrm{I} + \mathrm{II} + \mathrm{III} + \mathrm{IV} + \mathrm{V} + \mathrm{VI}$ adds up to $f(x,\phi(x))$ remembering that

$$p_N(x) + (x - x^{(N+1)})) = x - x^{(N)}$$

and

$$r_N(x)p_N(x) + (\phi(x) - \phi^{(N-1)}(x)) = \phi(x) - \phi^{(N)}(x),$$

which are simple consequences of equations (7.3) and (7.4), respectively.

We will briefly summarize the strategy for estimating these terms. We will then describe the estimates in detail.

There exist natural numbers N_{I}, N_{II}, N_{III}, and N_{IV} such that I, II, III, and IV are all bounded above by $\ell^{-\eta(N)-A}$. For I and II, such bounds follow directly from the very strong differentiability of f in the x and y variables, respectively. III follows from a Hölder condition on $\frac{\partial f}{\partial y}$, which is weaker than the very strong differentiability assumed for f. The bound on IV follows from the boundedness of $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$, together with the fact that $\eta(N+1) = \eta(N) + N$ for all N.

Lemma 7.2.1. *Given $A > 0$, there exists N_{I} such that for $N \geq N_{\mathrm{I}}$, term* I *has norm no more than $\ell^{-\alpha(N)-A}$.*

Proof. Pick N_{I} so that we have for every $x \in R^p$, $y \in R^q$ and $h \in R^p$ such that $\|h\| < \ell^{-N_{\mathrm{I}}}$, that

$$\left\| f(x+h,y) - f(x,y) - \left.\frac{\partial f}{\partial x}\right|_{(x,y)} h \right\| \leq \ell^{-A}\|h\|.$$

We can do this by the strict differentiability assumption on f, and the fact that $R^p \times R^q$ is a compact set. Then if $N > N_{\mathrm{I}}$, $\left\|x - x^{(N)}\right\|$ is no more than $\ell^{-\eta(N)} \leq \ell^{-\eta(N_{\mathrm{I}})} \leq \ell^{-N_{\mathrm{I}}}$, so the above bound applies with $h = x^{(N)} - x$, and we have that

$$\|\mathrm{I}\| \leq \ell^{-A}\ell^{-\eta(N)},$$

as desired. □

Lemma 7.2.2. *Given $A > 0$, there exists N_{II} such that for $N \geq N_{\mathrm{II}}$, term* II *has norm no more than $\ell^{-\eta(N)-A}$.*

Proof. We will select N_{II} to take advantage of the very strong differentiability in the y-variable. The choice of N_{II} should be large enough so that $\eta(N) - \log(N) > N$ for all $N \geq N_{\mathrm{II}}$. We will also want N_{II} to have the property that for any h with $\|h\| = \ell^{-s} < \ell^{-N_{\mathrm{II}}}$, and any $x \in R^p$, $y \in R^q$,

$$\left\| f(x, y+h) - f(x,y) - \left.\frac{\partial f}{\partial y}\right|_{(x,y)} h \right\| < \ell^{-A-\log(s)} \|h\|.$$

This is possible because of the very strong differentiability- $\|h\|^{1+\alpha}$ is equal to $\ell^{-(1+\alpha)s}$, which is smaller than $\ell^{-s-\log s - A}$ if s is large enough.

For any N, we have that $\left\|\phi^{(N)}(x) - \phi(x)\right\|$ is no more than $\ell^{-\eta(N)+\log(N)}$. So if $N > N_{\mathrm{II}}$ then, taking h to be $\phi^{(N)}(x) - \phi(x)$, the error in the linear approximation will be bounded above by

$$\ell^{-A-\eta(N)+\log(N)-\log(\eta(N)-\log(N))},$$

which is in turn smaller than $\ell^{-A-\eta(N)}$ because $\eta(N) - \log(N)$ is larger than N. This proves the desired bound. □

Lemma 7.2.3. *Given $A > 0$, there exists an N_{III} such that for $N \geq N_{\mathrm{III}}$, term* III *has norm no more than $\ell^{-\eta(N)-A}$.*

Proof. Pick N_{III} for the Hölder condition on $\frac{\partial f}{\partial y}$ discussed after the definition of very strong differentiability to guarantee that for the value $h = x^{(N)} - x$,

$$\left\| \left.\frac{\partial f}{\partial y}\right|_{(x,\phi(x))} - \left.\frac{\partial f}{\partial y}\right|_{(x+h,\phi(x))} \right\| \leq \ell^{-A}\ell^{-\log(s)}$$

if $\|h\| = \ell^{-s}$ where $s \geq N_{\mathrm{III}}$. Also, we must select N_{III} sufficiently large that $\eta(N) - \log N > N$ for all $N > N_{\mathrm{III}}$.

Then, because we have the bound $\left\|\phi(x) - \phi^{(N)}(x)\right\| \leq \ell^{-\eta(N)+\log(N)}$, we obtain the bound

$$\|\mathrm{III}\| \leq \ell^{-A}\ell^{-\log(\eta(N)-\log(N))}\ell^{-\eta(N)+\log(N)},$$

and by the choice of N_{III} this is no more than $\ell^{-\eta(N)-A}$. □

Lemma 7.2.4. *There exists an integer N_{IV} such that for $N \geq N_{\mathrm{IV}}$, term* IV *has norm no more than $\ell^{-\eta(N)-A}$.*

Proof. Let B be the integer such that

$$\ell^B = \max_{\substack{x\in R^p \\ y\in R^q}} \max\left(\left\|\left.\frac{\partial f}{\partial x}\right|_{(x,y)}\right\|, \left\|\left.\frac{\partial f}{\partial y}\right|_{(x,y)}\right\|, \left\|\left.\frac{\partial f}{\partial x}\right|_{(x,y)}\right\| \cdot \left\|\left.\frac{\partial f}{\partial y}\right|_{(x,y)}\right\|\right).$$

Pick N_{IV} for which $N_{\mathrm{IV}} \geq \log(N_{\mathrm{IV}} + 1) + A + B$. For any $N > N_{\mathrm{IV}}$, it follows that this same inequality holds with N in place of N_{IV}. Let $N > N_{\mathrm{IV}}$. Because $\eta(N + 1) = \eta(N) + N$, it follows from the choice of N_{IV} that p_{N+j} has norm no more than $\ell^{-(\eta(N)+A+B+\log(N+j))}$ for every $j > 0$, and by assumption r_{N+j} has norm no more than $\ell^{\log(N+j)}$. Performing the multiplication gives

$$\|\mathrm{IV}\| \leq \ell^{-\eta(N)-A}.$$

□

In contrast, V is only small for certain choices of N. Nonetheless, there are infinitely many such choices: choosing r_N to approximate the matrix

$$-\left.\frac{\partial f}{\partial y}^{-1}\right|_{(x,\phi(x))} \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))},$$

which is possible because of the rank assumption on $\frac{\partial f}{\partial y}$, we obtain a satisfactory bound of $\ell^{-\eta(N)-A}$ for such values of N. Here, $\frac{\partial f}{\partial y}^{-1}$ is the right inverse of $\frac{\partial f}{\partial y}$.

Lemma 7.2.5. *There exist arbitrarily large values of N for which the term* V *has norm no more than $\ell^{-\eta(N)-A}$ for almost every value of x.*

Proof. As in Lemma 7.2.4, define B so that

$$\ell^B = \max_{\substack{x\in R^p \\ y\in R^q}} \max\left(\left\|\left.\frac{\partial f}{\partial x}\right|_{(x,y)}\right\|, \left\|\left.\frac{\partial f}{\partial y}\right|_{(x,y)}\right\|, \left\|\left.\frac{\partial f}{\partial x}\right|_{(x,y)}\right\| \cdot \left\|\left.\frac{\partial f}{\partial y}\right|_{(x,y)}\right\|\right).$$

We selected r_N to be a dense sequence of q-by-p matrices of continuous functions from R^p into K. Note that $\frac{\partial f}{\partial y}$ has a right inverse for almost every x by the assumption that $\frac{\partial f}{\partial y}$ has full rank and the assumption that $q \geq n-d$. Therefore, we can pick arbitrarily large N for which

$$\left\| r_N(x) + \left.\frac{\partial f}{\partial y}^{-1}\right|_{(x,\phi(x))} \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))} \right\|$$

is almost everywhere smaller than ℓ^{-A-B} as a function of x. V can be written as

$$\mathrm{V} = \left(\left.\frac{\partial f}{\partial y}\right|_{(x,\phi(x))} r_N(x) + \left.\frac{\partial f}{\partial x}\right|_{(x,\phi(x))} \right) p_N(x).$$

The norm of $p_N(x)$ is no larger than $\ell^{-\eta(N)}$ by the definition of p_N, and the choice of N guarantees that the term multiplying $p_N(x)$ has norm no larger than ℓ^{-A}. □

Therefore, we can pick an N larger than $\max(N_{\mathrm{I}}, N_{\mathrm{II}}, N_{\mathrm{III}}, N_{\mathrm{IV}})$ that satisfies the condition in Lemma 7.2.5. For this value of N, the norm of I+II+III+IV+V is, by the ultrametric inequality, no more than the largest of the norms of I, II, III, IV, and V, which is bounded almost everywhere by $\ell^{-A-\eta(N)}$. Therefore, for almost every x, the value $f(x, \phi(x))$ is contained in balls of radius $\ell^{-A-\eta(N)}$ centered at each point $f\left(x^{(N)}, \phi^{(N)}(x)\right)$. But the values of $x^{(N)}$ and $\phi^{(N)}(x)$ depend only on the coefficients $x_0, \ldots, x_{\eta(N)-1}$. This means that $f(x^{(N)}, \phi^{(N)}(x))$ can only take on at most $\ell^{\eta(N)p}$ values. So $f(x, \phi(x))$ is contained in at most $\ell^{\eta(N)p}$ balls of radius at most $\ell^{-\eta(N)-A}$ in K^{n-d} for almost every x. Each such ball has measure $\ell^{(-\eta(N)-A)(n-d)}$, so the total measure of the union of the balls is no more than $\ell^{(-\eta(N)-A)(n-d)}\ell^{\eta(N)p}$. If $n-d \geq p$, then this is no more than $\ell^{(-A(n-d))}$. Since A was arbitrary, this is sufficient to show that the range of $f(x, \phi(x))$ has measure zero.

7.2.3 Kakeya-Like Sets

We can use the function ϕ from Theorem 1.3.1 to construct Kakeya-like sets of the type described in Theorem 1.3.2. Specifically, suppose that $f(x, y, w)$ is a measurable function such that for almost every w, the Jacobian $\frac{\partial f}{\partial y}$ has full rank almost everywhere. We will think of f as a family of surfaces, where x and y index the family of surfaces, and each surface is parameterized by the w variable. We want to include one surface $\{(w, z) : z = f(x, y, w); w \in K^d\}$ for each $x \in K^p$.

We claim that the set

$$T := \{(w, z) : z = f(x, \phi(x), w); x \in K^p, w \in K^d\}$$

has measure zero. We know from Theorem 1.3.1 that, for almost every w, the "cross-section" $\{f(x, \phi(x), w) : w \in K^n\}$ has measure zero. By Fubini's theorem, this implies that if T is measurable, then it must have measure zero. Therefore, the only thing that remains to be seen is that T is measurable.

Note that it is enough to show that the set

$$T' := \{(w, z) : z = f(x, \phi(x), w); x \in R^p, w \in K^d\}$$

is measurable, because T can be expressed as the countable union

$$\bigcup_a \{(w, z) : z = f(x + a, \phi(x + a), w); x \in R^p, w \in K^d\}$$

where a ranges over the elements of K^p such that all the terms have negative degree. Writing T this way is useful because R^p is a compact set.

We will now write T' in a way that makes its Borel measurability clear. The next thing we use is that T' can be thought of as the set of (w, z) for which there exists a sequence x_n in R^p with $\|f(x_n, \phi(x_n), w) - z\| < \frac{1}{n}$. This is sufficient to be in T' because the compactness of R^p guarantees that a subsequence of the x_n will have a limit x, and the continuity of the functions f and ϕ guarantees that $\|f(x, \phi(x), w) - z\|$ will equal zero. Furthermore, we can also impose the condition that the sequence elements x_n lie in a countable dense subset $\tilde{R}^p$ of R^p. Therefore, T' can be realized as the set

$$\bigcap_{n \in \mathbb{Z}} \bigcup_{x \in \tilde{R}^p} \left\{(w, z) : ||f(x, \phi(x), w) - z|| < \frac{1}{n}\right\}.$$

This set is measurable because $f(x, \phi(x), \cdot)$ is measurable for every x. Therefore, the set T' is measurable, and T is measurable and has measure zero.

7.2.4 Examples

The motivating example for this problem is that of Besicovitch sets:

Example 7.2.6 (Measure-Zero Besicovitch Sets in Non-Archimedean Local Fields)**.** *The vector space K^2 has a Besicovitch set of Haar measure zero for any non-archimedean local field K.*

Proof. We apply Theorem 1.3.2 to the function $f(x, y, w) = xw - y$. The variables x and y parameterize the space of lines in K^2, with w as the independent variable in the equation for the line. Here, $p = 1$ and $q = 1$: x is K^p-valued and y is K^q-valued. So Theorem 1.3.2 says that the set T defined by

$$T := \{(w, z) : z = f(x, \phi(x), w); x \in K^p, w \in K^d\}$$

has measure zero. This set will contain the line consisting of points of the form $(w, xw - \phi(x))$ for each x. This guarantees that w contains a line of every non-vertical slope. □

Of course, Example 7.2.6 implies the existence of Besicovitch sets of measure zero for any K^n, $n \geq 2$, by taking the Cartesian product $T \times K^{n-2}$.

Notice that the dimensionality constraints on Theorem 1.3.2 mean that Theorem 1.3.2 (and, in the Euclidean case, Theorem 7.1.1) cannot be used to locate (n, k) Besicovitch sets of measure zero- that is, sets of measure zero containing a k-flat pointing in every possible direction- because the (n, k)-dimensional Grassmannian has dimension $p = k(n - k)$ but the family of translations that do not fix a given plane has dimension only $q = n - k$, which is strictly less than p unless $k = 1$ In fact, for $n \geq 4, 2 \leq k \leq n/2$ we have $k(n-k) \geq n$, so there is no hope of ever achieving the bound $p \leq n-d$ required for the application of theorem 1.3.2, even if we're allowed to apply some non-translation transformations such as folding the k-planes somehow.

Another example given in [20] concerns paraboloids.

Example 7.2.7. *[Set of Haar measure zero containing a* 1*-dimensional family of Paraboloids] Consider the family of paraboloids* $P(a, b)$ *in* K^n *given by*

$$w_n = a(w_1 - b)^2 + \cdots + a(w_{n-1} - b)^2.$$

Each such paraboloid is $d = n - 1$ *dimensional, and parameterized by* $w_1, \ldots, w_{n-1}$*. Defining* A *and* B *by*

$$A := \bigcup_a P(a, \phi(a))$$

$$B := \bigcup_b P(\phi(b), b)$$

we have that both A *and* B *have measure zero.*

A final example concerns the Veronese map. This example, as presented in [20], is erroneous: the first d components should be $w_1, \ldots, w_d$ instead of $a_1 w_1 + b_1, \ldots, a_d w_d + b_d$.

Example 7.2.8. *[Family of Veronese-like Curves of Measure Zero] Consider the surfaces $f_{a,b}$ of the form*

$$f_{a,b}(w_1, \ldots, w_d) := \begin{pmatrix} w_1 \\ w_2 \\ \vdots \\ w_d \\ a_{d+1}w_1^2 + b_{d+1} \\ \vdots \\ a_{\binom{d+s}{s}} w_d^s + b_{\binom{d+s}{s}} \end{pmatrix}$$

These are d-dimensional surfaces, as they are parameterized by d variables $w_1, \ldots, w_d$. These surfaces are contained in K^n, where $n = \binom{d+s}{s}$. We define sets A and B:

$$A := \bigcup_a \{f_{a,\phi(a)}(w) : w \in K^d\},$$
$$B := \bigcup_b \{f_{\phi(b),b}(w) : w \in K^d\}$$

and these sets have measure zero. Here, $p = n - d = q = \binom{d+s}{s} - d$.

7.2.5 A Kakeya Needle Set

In $\mathbb{R}^2$, a set E is called a **Kakeya Needle Set** if a line segment of length 1 can be continuously rotated through the set and return to its original location in reverse orientation. Such Kakeya needle sets necessarily have positive measure as they must contain a circle sector of radius at least $1 - \epsilon$ through a circle arc of angle at least δ for some $\epsilon, \delta > 0$. However, Besicovitch [3] observed that such sets can have arbitrarily small Lebesgue measure.

Over non-archimedean local fields K, Caruso [7] defines a Kakeya needle set as a set E such that, for every direction in K^n, E contains a line $xw + \phi(x)$ where $\phi(x)$ is a continuous function of x. This agrees with the usual definition of Kakeya needle sets in $\mathbb{R}^2$. Under this definition, the set constructed in Example 7.2.6 is a Kakeya-needle set of Haar measure zero. Caruso shows that, under an appropriate probability measure on Lipschitz continuous functions ϕ with Lipschitz constant 1, the set of points

$$\{(w, xw + \phi(x)) : w \in K\}$$

will have Haar measure zero a.s., providing an abundance of measure-zero Kakeya needle sets.

Chapter 8

Background on Salem Sets

8.1 Fourier Dimension

Before defining the notion of Fourier dimension, We consider an explicit example from [55]. Let σ_n be the surface area measure on S^{n-1}. Seeing as how the sphere S^{n-1} is a hypersurface of dimension $n-1$ and the measure σ_n is spread out over S^{n-1}, we expect from Corollary 2.3.6 that $|\widehat{\sigma}(\xi)|$ should, on average, be on the order of $|\xi|^{-\frac{n-1}{2}}$, possibly with an ϵ-loss in the exponent. In fact, we have the formula from [55, Corollary 6.7]

Example 8.1.1 (Asymptotic formula for Fourier transform of σ_n)**.** *The surface measure of σ_n has the asymptotic formula*

$$\widehat{\sigma}_n(\xi) = 2|\xi|^{-(n-1)/2} \cos(2\pi(|\xi| - \frac{n-1}{8})) + O(|x|^{-(n+1)/2})$$

For this example, we have a pointwise estimate of the form $|\widehat{\sigma}(\xi)| \lesssim |\xi|^{-(n-1)/2}$. It turns out that this is a feature of the curvature of the set S^{n-1}. We will now consider the hyperplane $H_n := \{x : x_n = 0\}$, and show that this kind of pointwise Fourier decay cannot occur for any Borel probability measure μ supported on the hyperplane H_n:

Example 8.1.2 (Lack of Fourier decay for Borel probability measures supported on H_n)**.** *Let μ be any measure supported on H_n. Then $\widehat{\mu}(\xi)$ does not depend on ξ_n, so there exists a constant $C > 0$ and ξ arbitrarily far away from zero such that $|\widehat{\mu}(\xi)| \geq C$.*

In fact, for any hyperplane $a \cdot x = b$, there will be no Fourier decay in lines pointing in the direction a. We define a notion of dimension that depends on the pointwise Fourier decay of measures supported on E [36, Definition 3.12].

Definition 8.1.3 (Definition of Fourier Dimension)**.** *Let $E \subset \Omega \subset \mathbb{R}^n$ be a Borel set, and let Ω be compact. Then the Fourier dimension of E is the supremum value of t such that E supports a measure μ_t satisfying*

$$|\widehat{\mu}_t(\xi)| \lesssim_{t,\mu} |\xi|^{-t/2}.$$

It follows from Definition 8.1.3 and Corollary 2.3.6 that the Fourier dimension of a Borel set E is no more than the Hausdorff dimension of E. In the case of S^{n-1}, the Fourier dimension is $n-1$, and in the case of the hyperplane H_n, the Fourier dimension is zero.

This is a general principle: flat sets and self-similar fractals will tend to have Fourier dimension zero; curved sets and random fractals will tend to have positive Fourier dimension. A set whose Fourier dimension and Hausdorff dimension are equal is called a Salem set (definition taken from [36], Definition 3.11 and the discussion below Definition 3.12).

Example 8.1.4. *The middle-thirds Cantor set has Fourier dimension* 0*.*

The computation of the Fourier dimension of this set is difficult and is therefore omitted.

Unlike for Hausdorff dimension, the Fourier dimension is not countably stable. This was shown by Ekström, Persson, and Schmeling [15]. However, a countable set will necessarily have Fourier dimension 0 because the Fourier dimension is bounded above by the Hausdorff dimension.

The first examples of Salem sets with non-integer dimension were exhibited by Raphaël Salem [44]. Salem used a random construction that involves a Cantor-like construction with random interval lengths at each stage. This construction gives a set that almost surely has Fourier dimension 1. Many other random Cantor set constructions in the same spirit exist.

An explicit example of a Salem set has been provided by Kaufman [27], and an exposition of Kaufman's example was provided by Bluhm [5]. Consider the set of real numbers

$$\begin{aligned} E(\tau) := \{x \in [0,1] : |qx - r| \leq \max(q,r)^{\tau} \\ \text{for infinitely many pairs of integers } q, r\}. \end{aligned}$$

This set is called the set of **τ-approximable numbers**. For $\tau \leq 1$, $E(\tau)$ is the interval $[0,1]$, as is implied by the Dirichlet principle, but for $\tau > 1$, $E(\tau)$ is a proper subset of $[0,1]$ with Hausdorff dimension $\frac{2}{1+\tau}$. Kaufman established that the Fourier dimension of $E(\tau)$ is also $\frac{2}{1+\tau}$ by constructing a measure on $E(\tau)$ that has the appropriate pointwise Fourier decay. Explicit Salem sets of arbitrary dimension in $\mathbb{R}^2$ have been constructed by Hambrook [23] using a complex version of Kaufman's construction, but there are no known explicit Salem set constructions in higher dimensions.

8.2 Fourier Analysis on Non-Archimedean Local Fields

Let K be a non-archimedean local field with ring of integers R. There is a non-unique continuous, unitary character χ on K that is equal to 1 on all of R, but not equal to 1 on all of the fractional ideal $t^{-1}R$. We will fix such a χ. Every continuous, unitary character of K is of the form $\chi(xs)$ for some $s \in K$. Given a complex-valued L^1 function f on K, we define the Fourier transform of f at s to be

$$\widehat{f}(s) = \int_{x \in K} f(x)\chi(xs)\, dx.$$

This defines $\widehat{f}(s)$ as a function on $\chi(xs)$.

In order to establish the basic properties of the Fourier transform, we need a basic theorem on the orthogonality of characters. This is somewhat more powerful than the orthogonality of characters for Euclidean functions.

Lemma 8.2.1 (Orthogonality of Characters on Balls)**.** *Suppose* $|s_1 - s_2| > q^{-j}$*. Then we have that*

$$\int_{B(x,q^j)} \chi(xs_1)\overline{\chi(xs_2)} = 0$$

for any ball $B(x, q^j) \subset K$*.*

Proof. Let $x \in K$, and let $s_1, s_2 \in K$ such that $|s_1 - s_2| > q^{-j}$. We want to calculate

$$\int_{B(x,q^j)} \chi(s_1 y)\overline{\chi(s_2 y)}\, dy$$

We quickly make a change of variables to re-center the integral at the origin:

$$\chi((s_1 - s_2)x) \int_{B(0,q^j)} \chi(s_1 y)\overline{\chi(s_2 y)}\, dy$$

And we perform another change of variables to focus on the ball of radius 1:

$$q^j \chi((s_1 - s_2)x) \int_{B(0,1)} \chi(s_1 q^{-j} y)\overline{\chi(s_2 q^{-j} y)}\, dy$$

The last line requires a small bit of explanation. Unlike the Euclidean case, we have a minus sign appearing in this exponent in the integral. This is because $B(0, q^j)$ is precisely the set of points of the form $q^{-j}x$ where

$x \in B(0,1)$, unlike the Euclidean setting. Notice that since $|s_1 - s_2| > q^{-j}$, it follows that $|(s_1 - s_2)q^{-j}| > 1$. Therefore, it is enough to show the theorem for $|s_1 - s_2| > 1$ and for the ball $B(0,1)$.

So consider the integral

$$\int_{B(0,1)} \chi(s_1 x)\overline{\chi(s_2 x)} = \int_{B(0,1)} \chi((s_1 - s_2)x)$$

where s_1 and s_2 differ by more than 1 in absolute value. Letting $s = s_1 - s_2$, we have

$$\int_{B(0,1)} \chi(sx)$$

where $s > 1$. But the character $\chi(sx)$ is nonconstant on the locally compact abelian group $R = B(0,1)$ for $|s| > 1$ by assumption, and a nonconstant character on a locally compact abelian group always integrates to 0. □

We will briefly focus on the case of $K = \mathbb{Q}_p$.

We can define the Fourier series of a function f supported on $\mathbb{Z}_p$ in a similar way. We define the p-adic integer part $[x]_p$ of a p-adic number x with expansion as in (4.3) by

$$[x]_p = \sum_{j=0}^{\infty} x_j p^j$$

and we define the p-adic fractional part by

$$\{x\}_p = \sum_{j=-M}^{-1} x_j p^j.$$

Then $|[x]_p|_p \leq 1$. Using this notation, we can extend a function $f : \mathbb{Z}_p \to \mathbb{C}$ to all of $\mathbb{Q}_p$ by

$$f(x) = f([x]_p).$$

A function of this form will be called a $\mathbb{Z}_p$-periodic function.

Using this definition, we define the Fourier series of $f(x)$ for L^1 functions $f : \mathbb{Z}_p \to \mathbb{C}$ by

$$\widehat{f}(s) = \int_{x \in \mathbb{Z}_p} f(x)\chi(sx)\, dx$$

Here s ranges over those values in $\mathbb{Q}_p$ such that $[s]_p = 0$ (modifying the integer part of s would not change the value of the character). As an additive group, this has the same structure as the quotient $\mathbb{Q}_p/\mathbb{Z}_p$, known as the Prüfer group.

In fact, for any non-archimedean local field K, the group of characters on the ring of integers R of K will be isomorphic to the additive group K/R, and the reasoning is similar to the case for $\mathbb{Q}_p$.

A central fact when dealing with local fields is the uncertainty principle [49].

Theorem 8.2.2 (Uncertainty principle)**.** *Let $f(x) \in L^1$ be a complex-valued function on a local field. Then*

1. *If $f(x)$ is supported on a ball of radius q^j, then $|\widehat{f}(s)|$ is constant on balls of radius q^{-j}.*
2. *If $f(x)$ is supported on a ball of radius q^j centered at the origin, then $\widehat{f}(s)$ is constant on balls of radius q^{-j}.*
3. *If $f(x)$ is constant on balls of radius q^j, then $\widehat{f}(s)$ is supported on a ball of radius q^{-j} centered at the origin.*

Proof. Let $s \in K$. For part 1 of this theorem, we assume that $f(x)$ is supported on $B(y, q^{-j})$ and compute

$$\begin{aligned}\widehat{f}(s) &= \int_K f(x)\chi(sx)\,dx \\ &= \int_{B(y,q^j)} f(x)\chi(sx)\,dx \\ &= \chi(sy)\int_{B(0,q^j)} f(x+y)\chi(sx)\,dx\end{aligned}$$

We similarly get, for $|s'| < q^{-j}$:

$$\widehat{f}(s+s') = \chi((s+s')y)\int_{B(0,q^j)} f(x+y)\chi((s+s')x)\,dx$$

Now by the assumptions on s', we have that $s'x$ has absolute value at most 1; i.e., $s'x \in R$. This means that $\chi(s'x) = 1$, so we get

$$\widehat{f}(s+s') = \chi((s+s')y)\int_{B(0,q^j)} f(x+y)\chi(sx)\,dx$$

which is equal to $\chi(s'y)\widehat{f}(s)$. This is immediately seen to have absolute value $|\widehat{f}(s)|$, and, if $y = 0$, is exactly equal to $\widehat{f}(s)$. This establishes parts 1 and 2 of the theorem.

For part 3, assume $f(x)$ is constant on balls of radius q^j.

$$\begin{aligned}\widehat{f}(s) &= \int_K f(x)\chi(sx)\,dx \\ &= \sum_x f(x) \int_{B(x,q^j)} \chi(sx)\,dx\end{aligned}$$

Here the sum in contains one element of every ball of radius q^j in K (of which there are only countably many). Since $f(x)$ is in L^1 the sum is absolutely convergent and therefore well-defined. By Lemma 8.2.1, the integral of $\chi(sx)$ will vanish whenever s has absolute value greater than q^j, because in this instance the character χ is non-constant on the ball $B(x, q_j)$. Therefore, we have that $\widehat{f}(s) = 0$ if $|s| > q^j$. □

This uncertainty principle is an exact, explicit theorem that relates to the Euclidean uncertainty principle, quoted here [55, Chapter 5]:

> The uncertainty principle is the heuristic statement that if a measure μ is supported on [a rectangle] Q, then for many purposes $\widehat{\mu}$ may be regarded as being constant on any dual ellipsoid Q^*.

8.3 The Fourier Transform on Spaces Other than L^1

As is the case for the Euclidean setting, we have the Plancherel theorem [49].

Theorem 8.3.1 (Plancherel's Theorem)**.** *Let K be a non-archimedean local field, and Let $f \in L^1 \cap L^2(K)$. Then $||\widehat{f}||_{L^2(K)} = \|f\|_{L^2(K)}$ and thus the Fourier transform can be extended to an isometry on all of $L^2(K)$. By applying the Riesz-Thorin interpolation theorem, we see that the Fourier transform is bounded from $L^p(K)$ to $L^{p'}(K)$ for all $1 \leq p \leq 2$ with operator norm 1.*

Furthermore, we can extend the Fourier transform to a space of tempered distributions. We now define the Schwartz-Bruhat space $\mathcal{S}$, which is an analogue of the Schwartz space of functions in the Euclidean domain.

Definition 8.3.2. *A function $f(x)$ on K is said to be in the Schwartz-Bruhat space if there exists j such that:*

- *$f(x)$ is supported on a ball of radius q^j*
- *$f(x)$ is constant on balls of radius q^{-j}.*

By the Theorem 8.2.2, the Schwartz-Bruhat space maps to itself under the Fourier transform, and by the Fourier inversion theorem, the map is a bijection.

The dual of the Schwartz-Bruhat space is the space of distributions on K. Given a distribution f, we define the Fourier transform of f to be the distribution $\widehat{f}$ that satisfies the equation:

$$\left\langle \widehat{f}, \phi \right\rangle = \left\langle f, \widehat{\phi} \right\rangle$$

In particular, this definition is consistent with the usual definition of the Fourier transform of a measure:

$$\widehat{\mu}(s) = \int_K \chi(sx)\, d\mu(x).$$

Notice that, unlike the Euclidean setting, the indicator function $\mathbf{1}_{B(0,1)}$ for the ball $B(0,1)$ is smooth, because the set of points where $\mathbf{1}_{B(0,1)}$ is equal to 1 is separated from the set of points where $\mathbf{1}_{B(0,1)}$ is equal to 0 by a distance of 1. So the indicator function $\mathbf{1}_{B(0,1)}$ is in $\mathcal{S}$, and in fact satisfies the identity

$$\widehat{\mathbf{1}_{B(0,1)}} = \mathbf{1}_{B(0,1)}$$

This identity is of great value: unlike the Euclidean case, non-archimedean local fields admit compactly supported functions with compactly supported Fourier transforms. This often obviates the need for mollifiers, thereby greatly simplifying many of the standard arguments that are used in the Euclidean case, and making non-archimedean local fields a simplified model for the Euclidean setting.

8.4 The Case $K = \mathbb{Q}_p$

In the special case $K = \mathbb{Q}_p$, we have another way of defining the Fourier transform. If $x \in \mathbb{Q}_p$, x has an expansion of the form (4.3):

$$x = \sum_{j=M}^{\infty} x_j p^j.$$

If x is nonzero, we can assume that $x_M \neq 0$. The index M is nonnegative if and only if $x \in \mathbb{Z}_p$.

We will define the p**-adic integer part** $[x]_p$ and the p**-adic fractional part** $\{x\}_p$ of $x \in \mathbb{Q}_p$ as follows: if $x \in \mathbb{Z}_p$, then $[x]_p = x$ and $\{x\}_p = 0$. For $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ we define

$$[x]_p = \sum_{j=0}^{\infty} x_j p^j \tag{8.1}$$

and

$$\{x\}_p = \sum_{j=M}^{-1} x_j p^j \tag{8.2}$$

We now consider the function $e^{2\pi i \{x\}_p} =: e(\{x\}_p)$. We define this by reinterpreting the sum (8.2) as a rational number in $[0, 1]$. The p-adic fractional part is a locally constant (and hence continuous) function on $\mathbb{Q}_p$ that satisfies $\{x+y\}_p = \{x\}_p + \{y\}_p$. This implies that $e(\{x\}_p)$ is a unitary character on $\mathbb{Q}_p$. Thus we can select $\chi(x)$ to be this character. Every character on $\mathbb{Q}_p$ is of the form $e(\{xs\}_p)$ for some $s \in \mathbb{Q}_p$. Furthermore, every character on $\mathbb{Q}_p^n$ is of the form $e(\{x \cdot s\}_p)$ for some $s \in \mathbb{Q}_p^n$.

If f is an L^1 complex-valued function on $\mathbb{Q}_p^n$, the Fourier transform of f is the complex-valued function defined on $\mathbb{Q}_p^n$ by

$$\widehat{f}(s) = \int_{\mathbb{Q}_p} f(x) e(x \cdot s)\, dx.$$

This definition can be extended to distributions in the usual way. This definition specializes to Borel measures μ in the following way:

$$\widehat{\mu}(s) = \int_{\mathbb{Q}_p} e(x \cdot s)\, d\mu(x)$$

The character $e(\{x\}_p)$ is constant on $\mathbb{Z}_p$. In fact, for $x \in \mathbb{Z}_p$, the function $\{xs\}_p$ is equal to $\{xs'\}_p$ whenever $\{s\}_p = \{s'\}_p$. So the character associated to s is the same as the character associated to s' whenever $s - s' \in \mathbb{Z}_p$. Thus the character group on $\mathbb{Z}_p$ is isomorphic to the Prüfer group $\mathbb{Q}_p/\mathbb{Z}_p$. The Fourier series of a function $f : \mathbb{Z}_p \to \mathbb{C}$ is the function defined on $\mathbb{Q}_p/\mathbb{Z}_p$ defined by

$$\widehat{f}(s) = \int_{\mathbb{Z}_p} f(x) e(\{xs\}_p)\, dx.$$

We present some calculations of some Fourier transforms that will be useful in Chapter 9.

Lemma 8.4.1. *[Lemma 2.2.1 from [21]] For every $k \in \mathbb{Z}, a \in \mathbb{Q}_p^d$, and $s \in \mathbb{Q}_p^d$, we have*

$$\int_{B(a,p^{-k})} e(\{s \cdot x\}_p)\, dx = \begin{cases} p^{-dk} e(\{s \cdot a\}_p) & \text{if} |s|_p \leq p^k \\ 0 & \text{if} |s|_p > p^k \end{cases}$$

Proof. By a change of variable,

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

so it will suffice to prove the result when $a = 0$ and $k = 0$.

As the $d > 1$ case follows from the $d = 1$ case, we will also assume $d = 1$. If $|s|_p \leq 1$, then $\{sx\}_p = 0$ for all $x \in B(0,1)$, and so $\int_{B(0,1)} e(\{sx\}_p) dx = 1$.

Now suppose $|s|_p > 1$. By first making a change of variable and then using that $B(-1,1) = B(0,1)$, we get

$$\begin{aligned} \int_{B(0,1)} e(\{sx\}_p) dx &= e(\{s\}_p) \int_{B(-1,1)} e(\{sx\}_p) dx \\ &= e(\{s\}_p) \int_{B(0,1)} e(\{sx\}_p) dx. \end{aligned}$$

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

The Fourier transform on $\mathbb{Q}_p^d$ has the following property.

Lemma 8.4.2. *Let μ be a Borel measure on $\mathbb{Q}_p^d$ with support contained in $\mathbb{Z}_p^d$, and let ϕ be a positive, non-increasing function defined on $(0, \infty)$. If $|\widehat{\mu}(s)| \leq \phi(|s|_p)$ for all $s \in \mathbb{Q}_p$ with $[s]_p = 0$, then $|\widehat{\mu}(s)| \leq \phi(|s|_p)$ for all $s \in \mathbb{Q}_p^d$ with $|s|_p \geq 1$.*

Proof. If μ is an absolutely continuous measure supported on $\mathbb{Z}_p^d$, it immediately follows that $\widehat{\mu}$ is constant on balls of radius 1, which immediately shows the result. For more general Borel measures μ the result follows from an approximation argument. □

8.5 Hausdorff and Minkowski Dimension

The definitions of the Hausdorff dimension and Minkowski dimension of a Borel set E carry over with no modification to any metric space. However, we would like to discuss some of the analogues of the Euclidean theory of the behaviour of the Fourier transform on singular measures. These analogues appear in the Ph.D. thesis of Papadimitropoulos [38].

For example, we have the following theorem. The energy integral is defined in the same way as in the Euclidean setting:

Theorem 8.5.1 (Energy Integral Formulation of Frostman's Lemma for Local Fields, taken directly from Proposition 4.3.3 in [38])**.** *If $E \subset \Omega \subset K^n$ is a Borel set, where Ω is compact, then the Hausdorff dimension of E is the supremum value of t such that there exists a measure μ_t supported on E such that $I_t(\mu) < \infty$.*

There is a Fourier-analytic expression for the energy integral $I_s(\mu)$ [38, Lemma 4.3.4, part (ii)]:

Theorem 8.5.2 (Fourier-analytic expression for energy integrals)**.** *Let K be a non-archimedean local field with residue field $\mathbb{F}_q$. Let $E \subset K$ be a compact set and μ be a Borel probability measure supported on E. Then for $0 < t < 1$, t-energy $I_t(\mu)$ is given by the formula*

$$I_t(\mu) = \frac{1 - q^t}{1 - q^{t-1}} \int_K \frac{\widehat{\mu}(\xi)^2}{|\xi|^{1-t}}\, dx.$$

As is the case for singular measures in Euclidean space, this implies that the Hausdorff dimension of a bounded Borel set E is characterized by the L^2-averaged Fourier decay of Borel probability measures supported on E. We then define the Fourier dimension of such sets E in the following way [38, Discussion before Definition 4.3.5]:

Definition 8.5.3 (Definition of Fourier dimension)**.** *Let $E \subset \Omega \subset K^n$ be a Borel set, and let Ω be compact. Then the Fourier dimension of E is the supremum value of t such that E supports a measure μ_t satisfying*

$$|\widehat{\mu}_t(\xi)| \lesssim_{t,\mu} |\xi|^{-t/2}.$$

We way that E is a **Salem Set** if its Hausdorff dimension is equal to its Fourier dimension[38, Definition 4.3.5].

Chapter 9

An Explicit Salem Set

9.1 Introduction

We begin by discussing some properties of the sets $W(\tau)$ and $W(m,n,\tau)$ mentioned in Theorems 1.4.1 and 1.4.2. Recall the definition of this set

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

In Kaufman's example $E(\tau)$ replacing $\max(|q|,|r|)$ by q does not change the set $E(\tau)$. For the set $W(\tau)$ the bound $\max(|q|,|r|)^{-\tau}$ is of utmost importance; replacing this by $|q|^{-\tau}$ would give all of $\mathbb{Z}_p$ by the p-adic Dirichlet principle.

For $\tau\leq 2$, we also have that $W(\tau)=\mathbb{Z}_p$. This also follows from the Dirichlet principle. For $\tau>2$, Melničuk proved that $W(\tau)$ has Hausdorff dimension $2/\tau$ [37]. Together with Theorem 1.4.1, this shows that $W(\tau)$ is a Salem set.

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

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

We will first consider the Euclidean set of well-approximable vectors $E(m,n,\tau)$ defined by

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

It follows from Minkowski's theorem on linear forms that $E(m,n,\tau)=\mathbb{R}^{mn}$ whenever $\tau\leq n/m$. Bovey and Dodson showed that the Hausdorff dimension of $E(m,n,\tau)$ is equal to $m(n-1)+\frac{(m+n)}{1+\tau}$ whenever $\tau>n/m$. The $n=1$ case was done earlier by Jarník [25] and Eggleston [14].

Hambrook [24] generalized Kaufman's argument in order to obtain a lower bound on Fourier dimension of the sets $E(m,n,\tau)$. Hambrook constructs a measure on $E(m,n,\tau)$ with sufficient Fourier decay to guarantee that $E(m,n,\tau)$ has Fourier dimension at least $2n/(1+\tau)$. Theorem 1.4.2 is a p-adic version of this result.

Recall that we define $W(m,n,\tau)$ by

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

Unlike the case for $W(m,n,\tau)$, it is only necessary to use the Dirichlet pigeonhole principle in order to show that $W(m,n,\tau) = \mathbb{Z}_p^{mn}$ for $\tau \leq (m+n)/m$. Abercrombie [1] showed that $W(m,n,\tau)$ has Hausdorff dimension $m(n-1) + (m+n)/\tau$ whenever $\tau > (m+n)/n$.

9.2 A Salem Set in $\mathbb{Z}_p$

9.2.1 Setup

Let $\tau > 2$. For each $M \in \mathbb{N}$, define

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

We will assume that $M \geq 2$ in order to guarantee that Q_M is nonempty. For $q \in Q_M$ and $r \in R_M$, define the function $\phi_{q,r}$ on $\mathbb{Z}_p$ by

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

The function $\phi_{q,r}$ is a weighted indicator function for the ball of radius $p^{-\lceil \tau M \rceil}$ centered at $\frac{r}{q}$. For each $M \in \mathbb{N}$, we will define the function F_M on $\mathbb{Z}_p$ by

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

For any M, F_M has integral 1.

We will choose a rapidly increasing sequence of positive integers $(M_k)_{k=0}^{\infty}$ such that for all $k \in \mathbb{N}$,

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

We will then define the measure μ_k on $\mathbb{Z}_p$ by

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

For convenience, we take $d\mu_0 = d\mu_{-1} = dx$ We will need the following lemmas in order to construct the desired measure μ.

Lemma 9.2.1 (Lemma 3.2.2 from [21]). *For all $M \in \mathbb{N}$ and $s \in \mathbb{Q}_p/\mathbb{Z}_p$,*

$$\begin{aligned}
\widehat{F}_M(s) &= 1 && \text{if} \quad s = 0 && (9.1)\\
\widehat{F}_M(s) &= 0 && \text{if} \quad 0 < |s|_p \leq p^M && (9.2)\\
|\widehat{F}_M(s)| &\lesssim |s|^{-1/\tau}\log^2(|s|_p) && \text{if} \quad p^M < |s|_p \leq p^{\lceil \tau M \rceil} && (9.3)\\
\widehat{F}_M(s) &= 0 && \text{if} \quad |s|_p > p^{\lceil \tau M \rceil} && (9.4)
\end{aligned}$$

Lemma 9.2.2 (Lemma 3.2.3 from [21]). *For all integers $k \geq 0$ and all $s \in \mathbb{Q}_p/\mathbb{Z}_p$,*

$$\begin{aligned}
\widehat{\mu}_k(s) &= 1 && \text{if} \quad s = 0 && (9.5)\\
\widehat{\mu}_k(s) &= \widehat{\mu}_{k-1}(s) && \text{if} \quad 0 < |s|_p \leq p^{M_k} && (9.6)\\
|\widehat{\mu}_k(s)| &\lesssim |s|^{-1/\tau}\log^2(|s|_p) && \text{if} \quad p^{M_k} < |s|_p \leq p^{\lceil \tau M_k \rceil} && (9.7)\\
\widehat{\mu}_k(s) &= 0 && \text{if} \quad |s|_p > p^{\lceil \tau M_k \rceil} && (9.8)
\end{aligned}$$

The equation (9.5) implies that each μ_k is a probability measure. By Prohorov's theorem, which can be found in [26, vol. 2, p. 202], the sequence of $(\mu_k)_{k=1}^{\infty}$ has a subsequence that converges weakly to a probability measure μ. Though μ is a measure on $\mathbb{Z}_p$, it extends to a measure on $\mathbb{Z}_p$ by defining $\mu(A) = \mu(A \cap \mathbb{Z}_p)$ for $A \subset \mathbb{Q}_p$. We have that supp(μ) is contained in $W(\tau)$: of course supp$(\mu) \subset$ supp(F_{M_k}). But every point x in supp(F_{M_k}) is within $p^{-\lceil \tau M_k \rceil}$ of a rational number $\frac{r}{q}$ where $(q, r) \in Q_{M_k} \times R_{M_k}$. But the growth rate of the M_k guarantees that the sets Q_{M_k} are disjoint for different values of k.

Furthermore, by the conditions in Lemma 9.2.2,

$$|\widehat{\mu}(s)| \leq \sup_{k \in \mathbb{N}} |\widehat{\mu}_k(s)| \lesssim |s|_p^{-1/\tau}\log^3(|s|_p) \quad \forall s \in \mathbb{Q}_p/\mathbb{Z}_p, s \neq 0.$$

The strategy of the proof is the following: we will first prove Lemma 9.2.1 using an exponential sum estimate. Then, we will use Lemma 9.2.1 together with a convolution estimate to prove Lemma 9.2.2.

9.2.2 Estimates on $\widehat{F}_M$

Proof. This is the part of the proof that differs the most from the Euclidean result in [27]. Let $M \in \mathbb{N}$ and let $s \in \mathbb{Q}_p/\mathbb{Z}_p$. For $|s|_p > p^{\lceil \tau M \rceil}$, we have (9.4) as a direct consequence of the formula (Lemma 8.4.1) for the Fourier transform of $\phi_{q,r}$. For $|s|_p \le p^{\lceil \tau M \rceil}$, we use the formula for the Fourier transform of $\phi_{q,r}$ to conclude that

$$\widehat{F}_M(s) = |Q_M|^{-1}|R_M|^{-1} \sum_{q \in Q_M} \sum_{0 \le r < p^M} e(\{rs/q\}_p). \tag{9.9}$$

If we set $s = 0$, then each exponential term $e(\{rs/q\}_p)$ is equal to 1. Thus $\widehat{F}_M(0) = 1$. This establishes (9.1). Now we need only compute $\widehat{F}_M(s)$ for $0 < |s|_p \le p^{\lceil \tau M \rceil}$. Therefore, $|s|_p = p^\ell$ for some $\ell \in \{1, \dots, \lceil \tau M \rceil\}$. We will consider the inside sum in r occurring in equation (9.9). Fix $q \in Q_M$. Since $|q|_p = 1$ (by the choice of Q_M) we have that $|s/q|_p = |s|_p = p^\ell$. Thus the p-adic expansion s/q has the form

$$\frac{s}{q} = \sum_{i=-\ell}^{\infty} c_i p^i, \quad c_i \in \{0, 1, \dots, p-1\},\ c_{-\ell} \ne 0. \tag{9.10}$$

Viewing $\{s/q\}_p$ as an element of $\mathbb{Q}$, we have that $0 < \{s/q\}_p < 1$, and so $e(\{s/q\}) \ne 1$. Thus we can apply the geometric series formula to conclude

$$\sum_{0 \le r < p^M} e(\{rs/q\}_p) = \frac{1 - e(\{sp^M/q\}_p)}{1 - e(\{s/q\}_p)}. \tag{9.11}$$

If $|s|_p \le p^M$, then $|p^M s| \le 1$ and we have $\{sp^M/q\}_p = 0$. In this case it follows that $e(\{sp^M/q\}_p) = 1$ and the sum in (9.11) is zero. This establishes (9.2).

Therefore only (9.3) needs to be shown. We will thus assume that $p^M < |s|_p = p^\ell \le p^{\lceil \tau M \rceil}$. For all $z \in \mathbb{R}$, $|1 - e(z)| = 2|\sin(\pi z)| = 2\sin(\pi \|z\|) \ge \pi \|z\|$, where $\|z\| := \min_{k \in \mathbb{Z}} |z - k|$ denotes the distance from z to the nearest integer. Thus the sum in (9.11) satisfies

$$\left| \sum_{0 \le r < p^M} e(\{rs/q\}_p) \right| \le \min\left\{ \frac{1}{\|\{s/q\}_p\|}, p^M \right\}. \tag{9.12}$$

We write $\frac{s}{q}$ as in (9.10), and conclude

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

Therefore, we get the estimate

$$|\widehat{F}_M(s)| \le |Q_M|^{-1}|R_M|^{-1} \sum_{k=1}^{\ell} \sum_{\substack{\frac{1}{2} \le q < p^M \\ |q|_p = 1,\, q \text{ prime} \\ p^{-k} \le \|\{s/q\}_p\| < p^{-k+1}}} \min\{p^k, p^M\} \tag{9.13}$$

In order to estimate this sum, we need to better understand the distribution of the fractional part $\{s/q\}_p$ modulo p^ℓ. If these fractional parts are well-distributed for every s, then the sum (9.13) should be controlled.

Fix k such that $1 \le k \le \ell$. We will estimate the number of terms in the sum over q in (9.13). This estimate is similar to, and was inspired by, a similar argument from a work of Cilleruelo and Garaev [8, Theorem 1]. Consider any prime q with $\frac{1}{2}p^M \le q < p^M$, $|q|_p = 1$, and $p^{-k} \le \|\{s/q\}\| < p^{-k+1}$. Define $N = \|\{s/q\}_p\|\, p^\ell q$. Note that N is a positive integer that is at most $p^{M+\ell-k+1}$: $\|\{s/q\}_p\|$ is bounded above by p^{-k+1} and q is bounded above by p^M. If $\{s/q\}_p \le 1/2$, then $N = (s/q - [s/q]_p)\, p^\ell q \equiv sp^\ell \pmod{p^\ell}$. If $\{s/q\}_p > 1/2$, then $N = (1 - s/q + [s/q]_p)\, p^\ell q \equiv -sp^\ell \pmod{p^\ell}$. Therefore, q is a prime $\ge \frac{1}{2}p^M$ that divides a positive integer N with $N \le p^{M+\ell-k+1}$ and $N \equiv \pm sp^\ell \pmod{p^\ell}$. The number of positive integers N with $N \le p^{M+\ell-k+1}$ and $N \equiv \pm sp^\ell \pmod{p^\ell}$ is $\lesssim \max\{p^{M-k+1}, 1\}$, and the number of primes $q \ge \frac{1}{2}p^M$ that divide a specified positive integer N is at most a constant times $\frac{\log N}{\log p^M}$. Therefore, for a fixed k, the number of terms in the sum over q in (9.13) is

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

Therefore, (9.13) implies

$$|\widehat{F}_M(s)| \lesssim |Q_M|^{-1} |R_M|^{-1} \sum_{k=1}^{\ell} \min\{p^k, p^M\} \max\{p^{M-k+1}, 1\} \frac{\log p^{M+\ell-k+1}}{\log p^M}.$$

Because $|s|_p = p^\ell$ is between p^M and $p^{\lceil \tau M \rceil}$, $|Q_M| \gtrsim p^M / \log p^M$, and $|R_M| = p^M$, we have the desired estimate. □

9.2.3 Estimates on $\widehat{\mu_k}$

Proof. Let $s \in \mathbb{Q}_p/\mathbb{Z}_p$. The proof is by induction on k. The case $k = 0$ follows immediately from the choice of ψ_0 and the choice $d\mu_0 = d\mu_{-1} = \psi_0\, dx$.

So, we prove the inductive step. Assume $k \ge 1$. Then the inductive hypothesis is that the equations in 9.2.2 hold with k replaced by $k - 1$. By a standard argument we have

$$\widehat{\mu}_k(s) = \widehat{F_{M_k} \mu_{k-1}}(s) = \sum_{t \in \mathbb{Q}_p/\mathbb{Z}_p} \widehat{F}_{M_k}(s-t) \widehat{\mu}_{k-1}(t). \qquad (9.14)$$

If the summand $\widehat{F}_{M_k}(s-t)\widehat{\mu}_{k-1}(t)$ is nonzero, then $|t|_p \le p^{\lceil \tau M_{k-1}\rceil}$, which can be seen by applying the inductive hypothesis to $\widehat{\mu}_{k-1}(t)$. Furthermore, we must have that $F_{M_k}(s-t)$ is nonzero, so either $s=t$, or

$$p^{M_k} < |s-t|_p \le p^{\lceil \tau M_k\rceil}$$

by Lemma 9.2.1 and by the assumption that $\lceil \tau M_{k-1}\rceil < M_k$. Therefore, if $|s|_p > p^{\lceil \tau M_k\rceil}$, every term of the sum in (9.14) is zero (since at least one of $|s-t|_p$ and $|t|_p$ must be greater than $p^{\lceil \tau M_k\rceil}$). This proves (9.8).

If, instead, $|s|_p \le p^{M_k}$, then only the $t=s$ term contributes to the sum (since otherwise $|s-t|_p < p^{M_k}$) and thus $\widehat{\mu}_k(s) = \widehat{F}_{M_k}(0)\widehat{\mu}_{k-1}(s)$. This establishes (9.6), and also establishes (9.5) because the inductive hypothesis implies that $\widehat{\mu}_{k-1}(0) = 1$. Only (9.7) needs to be shown. Suppose that $p^{M_k} < |s|_p \le p^{\lceil \tau M_k\rceil}$ as in (9.7). For all $t \in \mathbb{Q}_p/\mathbb{Z}_p$ with $\widehat{F}_{M_k}(s-t)\widehat{\mu}_{k-1}(t) \ne 0$, we must have $|s|_p = |s-t|_p$ (since $|t|_p$ must be at most $p^{\lceil \tau M_{k-1}\rceil}$ or else $\widehat{\mu}_{k-1}(t)$ will vanish by the inductive assumption (9.8) applied to $k-1$) and so (9.3) gives that $|\widehat{F}_{M_k}(s-t)| \lesssim |s|^{-1/\tau}\log^2(|s|_p)$. By the inductive hypothesis and the fact that μ_{k-1} is a positive measure, $|\widehat{\mu}_{k-1}(t)| \le \widehat{\mu}_{k-1}(0) = 1$ for all $t \in \mathbb{Q}_p/\mathbb{Z}_p$. The number of $t \in \mathbb{Q}_p/\mathbb{Z}_p$ with $|t|_p \le p^{\lceil \tau M_{k-1}\rceil}$ is exactly $p^{\lceil \tau M_{k-1}\rceil}$; hence, the sum in (9.14) has at most $p^{\lceil \tau M_{k-1}\rceil}$ nonzero terms. Then we get

$$|\widehat{\mu}_k(s)| \lesssim p^{\lceil \tau M_{k-1}\rceil}|s|_p^{-1/\tau}\log^2(|s|_p)$$

We apply our assumption that $p^{\lceil \tau M_{k-1}\rceil} < \log(|s|_p)$ in order to complete the proof. □

9.3 Fourier Dimension of $W(m,n,\tau)$

The proof of this theorem is similar to the proof of Theorem 1.4.1.

General Setup

Let $\tau > (m+n)/m$. For each $M \in \mathbb{N}$ we define Q_M and R_M as in the proof of Theorem 1.4.1. Then

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

We will assume that $M > 1$ in order to guarantee that Q_M is nonempty. 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

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

and we 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 integers $(M_k)_{k=0}^{\infty}$ with $M_0 \geq 2$ such that for all $k \in \mathbb{N}$,

$$\lceil \tau M_{k-1} \rceil < M_k, \tag{9.15}$$

$$p^{mn\lceil \tau M_{k-1} \rceil} < \log(p^{M_k}) \tag{9.16}$$

As before, we take $d\mu_{-1}(x) = d\mu_0(x) = dx$ for notational convenience. For any $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$, define

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

Note that the set $D(s)$ will be empty unless the column space of $D(s)$ has dimension 1. The set $D(s)$ gives a family of q for which $\widehat{\phi}_{q,r}(s)$ may be nonzero:

Lemma 9.3.1. *For all $M \in \mathbb{N}$, $q \in Q_M^n$, $r \in R_M^m$, and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

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

We now state the multidimensional versions of Lemmas 9.2.1 and 9.2.2.

Lemma 9.3.2. *For all $M \in \mathbb{N}$ and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

$$\widehat{F}_M(s) = 1 \qquad \text{if} \quad s = 0 \tag{9.17}$$

$$\widehat{F}_M(s) = 0 \qquad \text{if} \quad 0 < |s|_p \leq p^M \tag{9.18}$$

$$|\widehat{F}_M(s)| \lesssim |s|^{-n/\tau} \log^{n+1}(|s|_p) \qquad \text{if} \quad p^M < |s|_p \leq p^{\lceil \tau M \rceil} \tag{9.19}$$

$$\widehat{F}_M(s) = 0 \qquad \text{if} \quad |s|_p > p^{\lceil \tau M \rceil} \tag{9.20}$$

Lemma 9.3.3. *For all integers $k \geq 0$ and all $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$,*

$$\widehat{\mu}_k(s) = 1 \qquad \text{if} \quad s = 0 \tag{9.21}$$

$$\widehat{\mu}_k(s) = \widehat{\mu}_{k-1}(s) \qquad \text{if} \quad 0 < |s|_p \leq p^{M_k} \tag{9.22}$$

$$|\widehat{\mu}_k(s)| \lesssim |s|^{-n/\tau} \log^{n+2}(|s|_p) \qquad \text{if} \quad p^{M_k} < |s|_p \leq p^{\lceil \tau M_k \rceil} \tag{9.23}$$

$$\widehat{\mu}_k(s) = 0 \qquad \text{if} \quad |s|_p > p^{\lceil \tau M_k \rceil} \tag{9.24}$$

We will not prove that these lemmas imply Theorem 1.4.2 because this follows in the same way as Theorem 1.4.1. We will also omit the proof of Lemma 9.3.3 because of the similarity to the proof of Lemma 9.2.2. We will prove Lemma 9.3.1 and Lemma 9.3.2.

9.3.1 Fourier Transform of $\phi_{q,r}$

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

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

ϕ_r is an m-dimensional tensor product of the weighted indicator function of the ball of radius $p^{-\lceil \tau M \rceil}$. Therefore, it is easy to compute $\widehat{\phi}_r$ using Lemma 8.4.1.

$$\widehat{\phi}_r(k) = \begin{cases} e(\{r \cdot k\}_p) & \text{if } |k|_p \leq p^{\lceil \tau M \rceil} \\ 0 & \text{if } |k|_p > p^{\lceil \tau M \rceil} \end{cases}.$$

By p-adic Fourier inversion [49, p. 120], we have

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

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

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

Here, the product xq denotes the usual matrix product of x and q, and the expression $k \cdot xq$ is the dot product of the vectors k and xq in $\mathbb{Z}_p^{mn}$. By Fubini's theorem:

$$\begin{aligned} \widehat{\phi}_{q,r}(s) &= \sum_{k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi}_r(k) \int_{\mathbb{Z}_p^{mn}} e(\{s \cdot x\}_p) e(-\{k \cdot xq\}_p) \, dx \\ &= \sum_{k \in (\mathbb{Q}_p/\mathbb{Z}_p)^m} \widehat{\phi}_r(k) \prod_{i=1}^{m} \prod_{j=1}^{n} \int_{\mathbb{Z}_p} e(\{x_{ij}(s_{ij} - k_i q_j)\}_p) \, dx_{ij}. \end{aligned}$$

Now, fix $k \in (\mathbb{Q}_p/\mathbb{Z}_p)$. By Lemma 8.4.1,

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

Note that, since $k_i \in \mathbb{Q}_p/\mathbb{Z}_p$ and $|q_j|_p = 1$, the condition that $|s_{ij} - k_i q_j|_p \leq 1$ is equivalent to the condition that $k_i = \{s_{ij}/q_j\}_p$. Therefore, we have that

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

The only thing that remains to be checked is that $\widehat{\phi}_{q,r}(s)=0$ if $|s|_p > p^{\lceil \tau M\rceil}$, in which case either one component $|\{s_{i1}/q_1\}_p|_p$ is larger than $p^{\lceil \tau M\rceil}$, or $|s_{i1}|_p \neq |s_{ij}|_p$ for some i,j, in which case $D(s)$ is empty. In either case, $\widehat{\phi}_{q,r}(s)$ vanishes. □

The only thing that remains to be shown is Lemma 9.3.2. This lemma relies on both Lemma 9.3.1 and on Lemma 9.2.1.

9.3.2 Estimate on $\widehat{F_M}$

Let $M \in \mathbb{N}$ and $s \in (\mathbb{Q}_p/\mathbb{Z}_p)^{mn}$. Choose $1 \leq i_0 \leq m$ and $1 \leq j_0 \leq n$ such that $|s_{i_0j_0}|_p = |s|_p$ (In the only nontrivial case, the one in which which $D(s)$ is nonempty, we can assume that $j_0 = 1$). For $|s|_p > p^{\lceil \tau M\rceil}$, Lemma 9.3.1 implies that $\widehat{F}_M(s) = 0$. This proves (9.20). For $|s|_p \leq p^{\lceil \tau M\rceil}$ it follows from Lemma 9.3.1 that

$$\widehat{F}_M(s) = |Q_M^n|^{-1}|R_M^m|^{-1} \sum_{q\in Q_M^m \cap D(s)} \left(\sum_{0\leq r_1<p^M} e(\{r_1 s_{1j_0}/q_{j_0}\}_p)\right)\cdots\left(\sum_{0\leq r_m<p^M} e(\{r_m s_{mj_0}/q_{j_0}\}_p)\right). \tag{9.25}$$

We get equation (9.1) by setting $s = 0$ and using the fact that $D(s) = Q_M^m$ when $s = 0$.

We will then assume instead that $0 \leq |s|_p \leq p^{\lceil \tau M\rceil}$. So $|s|_p = p^\ell$ for some $\ell \in \{1,\ldots,\lceil \tau M\rceil\}$. We will consider the sum over r_{i_0}. Fix $q \in Q_M^n \cap D(s)$. Since $|q_{j_0}|_p = 1$, we have that $|s_{i_0j_0}/q_{j_0}|_p = |s_{i_0j_0}|_p = |s|_p = p^\ell$. Therefore the p-adic expansion of $s_{i_0j_0}/q_{j_0}$ has the form

$$\frac{s_{i_0j_0}}{q_{j_0}} = \sum_{i=-\ell}^{\infty} c_i p^i, \quad c_i \in \{0,1,\ldots,p-1\}, c_{-\ell} \neq 0. \tag{9.26}$$

As a real number, we have that $0 < \{s_{i_0j_0}/q_{j_0}\}_p < 1$ and so $e(\{s_{i_0j_0}/q_{j_0}\}_p) \neq 1$. Therefore, we can use the geometric series formula

$$\sum_{0\leq r_{i_0}<p^M} e(\{r_{i_0} s_{i_0j_0}/q_{j_0}\}_p) = \frac{1-e(\{p^M s_{i_0j_0}/q_{j_0}\}_p)}{1-e(\{s_{i_0j_0}/q_{j_0}\}_p)}. \tag{9.27}$$

If $|s|_p \leq p^M$, we have $\{p^M s_{i_0j_0}/q_{j_0}\}_p = 0$; hence, the sum in (9.27) vanishes. Then one of the factors on the right hand side of (9.25) is zero, and $\widehat{F}_M(s) = 0$. This proves (9.18). So the only thing left to do is prove (9.19).

We will assume $p^M < |s|_p = p^\ell \le p^{\lceil \tau M \rceil}$. For all $z \in \mathbb{R}$, $|1-e(z)| = 2|\sin(\pi z)| = 2\sin(\pi \|z\|) \ge \pi \|z\|$, where $\|z\| =: \min_{k\in\mathbb{Z}} |z-k|$ is the distance from z to the nearest integer. Then, as in the proof of Lemma 9.2.1:

$$\left| \sum_{0\le r_{i_0} < p^M} e(\{r_{i_0} s_{i_0 j_0}/q_{j_0}\}_p) \right| \le \min\left\{ \frac{1}{\|s_{i_0 j_0}/q_{j_0}\|}, p^M \right\}. \tag{9.28}$$

We also use the trivial bound

$$\left| \sum_{0\le r_i < p^M} e(\{r_i s_{i j_0}/q_{j_0}\}) \right| \le p^M \quad \forall\, 1 \le i \le m. \tag{9.29}$$

In the notation of (9.26), we have

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

As in the proof of Lemma 9.2.1:

$$|\widehat{F}_M(s)| \le |Q_M^n|^{-1} |R_M^m|^{-1} \sum_{k=1}^{\ell} \sum_{\substack{q\in Q_M^n \cap D(s) \\ p^{-k} \le \|\{s_{i_0 j_0}/q_{j_0}\}_p\| < p^{-k+1}}} p^{(m-1)M} \min\{p^k, p^M\}. \tag{9.30}$$

We will now claim that $(q_1, \ldots, q_n) \to q_{j_0}$ is an injection from $Q_M^n \cap D(s)$ into the set

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

This claim follows from the following two observations. First, for each $q \in Q_M^n$ and $1 \le j \le n$, we have $\{s_{i_0 j_0}/q_{j_0}\}_p = \{s_{i_0 j}/q_j\}_p$ if and only if $|s_{i_0 j_0} - s_{i_0 j}/q_j|_p$ (since $|q_j|_p = |q_{j_0}|_p = 1$), which happens if and only if $|q_j - q_{j_0} s_{i_0 j} s_{i_0 j_0}^{-1}|_p \le |s_{i_0 j_0}^{-1}|_p = p^{-\ell}$, which happens if and only if $q_j \equiv s_{i_0 j} s_{i_0 j_0}^{-1} \pmod{p^\ell}$. Second, for any given $b \in \mathbb{Q}_p$, there can be at most one integer satisfying $a \equiv b \pmod{p^\ell}$ and $\frac{1}{2}p^M \le a < p^M \le p^\ell$. This establishes that the map is an injection and thus

$$|\widehat{F}_M(s)| \le |Q_M^n|^{-1} |R_M^m|^{-1} \sum_{k=1}^{\ell} \sum_{\substack{\frac{1}{2}p^M \le q_{j_0} < p^M \\ |q_{j_0}|_p = 1, q_{j_0} \text{ prime} \\ p^{-k} \le \|\{s_{i_0 j_0}/q_{j_0}\}_p\| < p^{-k+1}}} p^{(m-1)M} \min\{p^k, p^M\}. \tag{9.31}$$

We make the same argument as in Lemma 9.2.1 to conclude that for each fixed k, the number of terms in the sum over q_{j_0} in (9.32) is

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

So we get a bound of

$$|Q_M^n|^{-1} |R_M^m|^{-1} \sum_{k=1}^{\ell} p^{(m-1)M} \min\{p^k, p^M\} \max\{p^{M-k+1}, 1\} \frac{\log p^{M+\ell-k+1}}{\log p^M}$$

on $|\widehat{F}_M(s)|$. Since $p^M < |s|_p = p^\ell \leq p^{\lceil \tau M \rceil}$, $|Q_M^n| \approx p^{nM}/(\log p^M)^n$, and because $|R_M^m| = p^{mM}$, we get (9.19).

9.3.3 Concluding Remarks Regarding $W(m, n, \tau)$

We elaborate a small amount on the gap between the Fourier dimension bound in Theorem 1.4.2 and the known Hausdorff dimension from Abercrombie's paper [1]. The Fourier transform $\widehat{F}_M(s)$ is supported on a small set: if the matrix s does not have column rank 1, then $D(s)$ is empty and $\widehat{F}_M(s)$ vanishes. The small support of $\widehat{F}_M(s)$ can be used to show that $\widehat{\mu}_k(s)$ cannot have good pointwise decay.

Heuristically, we should not expect the set $W(m, n, \tau)$ to be a Salem set: it is contained in small neighbourhoods of a relatively small number of hyperplanes. No upper bound is currently known on the upper Fourier dimension of $W(m, n, \tau)$ or its Euclidean analogue $E(m, n, \tau)$.

Chapter 10

Conclusion

The results of this thesis raise some interesting questions that warrant further study. We will provide a brief discussion of some of the research problems that are relevant to the work described in this thesis.

10.1 Configurations

10.1.1 Squares of Differences

Although the results in [19] apply to a very broad class of functions, there is no reason to believe that these results will be optimal when applied to a specific problem. For example, consider the specific function $f(x_1, x_2, x_3) = (x_3 - x_1)^2 - (x_2 - x_1)$. Theorem 1.1.1 and Theorem 3.1.4 can be applied to this configuration in order to locate a subset of $\mathbb{R}$ of Hausdorff dimension $\frac{1}{2}$ that does not contain 3 distinct points x_1, x_2, x_3 such that $f(x_1, x_2, x_3)$ vanishes.

However, in the discrete setting, certain additional results are available for this function. In fact, Ruzsa [43] constructs a subset S of $\{1, \ldots, N\}$ containing at least $c_1 x^{\frac{1}{2}\left(1+\frac{\log 7}{\log 65}\right)}$ points such that for any distinct $x, y \in S$, the value $x-y$ is not a perfect square. Of course, this implies that S does not contain any nontrivial solutions to the equation $f(x_1, x_2, x_3) = 0$. Unfortunately, there does not seem to be a simple way to use this result to construct a subset $E \subset \mathbb{R}$ that does not contain any solutions to $f(x_1, x_2, x_3) = 0$.

There is also a positive result for the function f on finite fields. Bourgain and Chang [6] show that there exists a constant $c_1 > 0$ such that if $A \subset |\mathbb{F}_p|$ contains at least $c_1 p^{14/15}$ elements, then A must contain three distinct points such that $f(x_1, x_2, x_3) = 0$. This gives some hope that a method similar to the one used by Łaba and Pramanik [32] will give some condition on a subset of $\mathbb{R}$ that guarantees the existence of 3 points x_1, x_2, x_3 such that $(x_2 - x_1) = (x_3 - x_1)^2$. Shaoming Guo, Malabika Pramanik, and I are interested in pursuing this question further.

10.1.2 Configurations and Fourier Dimension

The theorems presented in Chapter 3 concern the Hausdorff and Minkowski dimensions of subsets $E \subset \mathbb{R}^n$ that do not contain certain types of configurations. This leaves open the question of what can be said about the Fourier dimension of such sets E. This question is interesting because, in the case of 3-term arithmetic progressions, Łaba and Pramanik [32] provide a Fourier decay condition on a set E that guarantees that E contains a 3-term arithmetic progression:

Theorem 10.1.1 (Theorem 1.2 from [32])**.** *Assume that $E \subset [0,1]$ that supports a probability measure μ with the following properties:*

- $\mu([x, x+\epsilon]) \leq C_1\epsilon^\alpha$ *for all* $0 < \epsilon \leq 1$,
- $|\widehat{\mu}(k)| \leq C_2(1-\alpha)^{-B}|k|^{-\frac{\beta}{2}}$ *for all* $k \neq 0$.

where $0 < \alpha < 1$ and $2/3 < \beta \leq 1$. If $\alpha > 1 - \epsilon_0$, where ϵ_0 is a sufficiently small constant depending only on C_1, C_2, B, β, then E contains a nontrivial 3-term arithmetic progression.

In light of this theorem, it seems reasonable to conjecture that any set E of Fourier dimension 1 should contain a 3-term arithmetic progression. In particular, the second condition of this theorem appears at first glance to be saying that E has Fourier dimension equal to β. However, the dependence of α on the constants C_1 and C_2 makes the theorem statement more complicated. In fact, Shmerkin [47] constructed a set of Fourier dimension 1 that does not contain any 3-term arithmetic progressions.

This raises the question of what can be said for arbitrary configurations. The case of linear configurations has been addressed by Körner [31]: Körner establishes that there is a set $E \subset \mathbb{R}^n$ of Fourier dimension $\frac{1}{v-1}$ that does not contain any v points $(x_1, \ldots, x_v)$ satisfying any nontrivial algebraic relation $\sum_{j=1}^{v} a_j x_j$ for integers x_j. This dimension $\frac{1}{v-1}$ is consistent with the statement of Theorem 1.1.1. Therefore, it is natural to ask whether the statement of Theorem 1.1.1 is true for Fourier dimension instead of Hausdorff dimension. If $\frac{1}{v-1}$ is replaced by $\frac{1}{v}$, a straightforward random Cantor set construction should give the desired set; the Euclidean equivalent of this result was also established by Körner [30] using a Baire category argument instead of a direct construction.

In a joint project with Pramanik, we will attempt to establish a result similar to that of Körner for arbitrary (not necessarily linear) configurations. The strategy is to adapt the proof of Körner's result [31] to this setting.

10.1.3 Local Fields

The discrepancy between the capset result [16] and Theorem 1.2.1 raises the following question: what conditions on a set are sufficient to guarantee that a set $E \subset K^n$ contains a 3-term arithmetic progression? The first place to look for an answer to this question is Theorem 10.1.1. I conjecture that a condition analogous to the conditions of this theorem will be enough to guarantee the existence of 3-term arithmetic progressions on K^n.

If K has finite characteristic, the situation might be somewhat different from the characteristic 0 case. There do not appear to be any obstructions to modifying Shmerkin's construction [47] to work in the p-adic setting. However, the capset result presents a real barrier to applying this construction on function fields $\mathbb{F}_q((t))$ because Shmerkin's construction relies on a construction of Behrend [2] of a subset of $\{1, \dots, N\}$ of size greater than $C_\epsilon N^{1-\epsilon}$ that does not contain any 3-term arithmetic progressions. The capset result implies that such sets cannot exist in $(\mathbb{F}_q)^n$.

In fact I will make the conjecture that any subset of $(\mathbb{F}_q)^n$ with Fourier dimension sufficiently close to 1 must contain an arithmetic progression. Such a result might follow from a modification of the proof of Theorem 10.1.1, but this has yet to be seriously pursued.

10.2 Besicovitch Sets on Local Fields

Two important problems related to Besicovitch sets are the Kakeya problem and the restriction problem. The Kakeya problem asks the following question: if $E \subset \mathbb{R}^n$ is a Kakeya set, must E have Hausdorff dimension n? This problem is connected to a large family of problems in Harmonic analysis. The Kakeya problem was solved in dimension 2 by Davies [10].

A related problem is the Fourier restriction problem. The restriction problem concerns questions of the following type: if S is a sufficiently curved surface in $\mathbb{R}^n$ and σ is the surface measure on S, for which values of p and q is the map from $\mathcal{S}^p(\mathbb{R}^n) \to L^q(\mathbb{R}^n)$ defined by $f \mapsto (\widehat{f})|_S$ bounded? Here, $\mathcal{S}^p(\mathbb{R}^n)$ is the Schwartz space of functions on $\mathbb{R}^n$ equipped with the L^p norm. Tomas [50] established an L^p-to-L^2 restriction estimate for the surface area measure on the sphere S^{d-1} for $1 \leq p < \frac{2(d+1)}{d+3}$; the endpoint estimate $p = \frac{2(n+1)}{n+3}$ was achieved by Elias Stein, as is mentioned in [48]. For $L^p \to L^2$ restriction estimates, this is the best possible result. The **Fourier restriction conjecture** concerns other values of q.

Conjecture 10.2.1 (Restriction Conjecture)**.** *The spherical surface measure σ satisfies an L^p-to-L^q restriction estimate for any pair (p, q) such that $p < \frac{2d}{d+1}$, $q \leq \frac{p(d-1)}{(p-1)(d+1)}$.*

By comparison to the Euclidean setting, the status of restriction and Kakeya-type results over local fields is less well-understood. Ellenberg, Oberlin, and Tao [17] proposed the discrete valuation ring $\mathbb{F}_p[[t]]$ as a model case for the study of Kakeya problems, with the hope of such Kakeya-type results as a stepping stone for translating the polynomial method and Dvir's finite field Kakeya result to the Euclidean setting, where little work on restriction has been done.

Dummit and Hablicsek [11] established that a Besicovitch set in $\mathbb{F}_q[[t]]^2$ must have Minkowski dimension 2. There does not appear to be an analogue of Davies' result [10] on the Hausdorff dimension of Kakeya sets. It is possible that such a result could be obtained via a sharpening of the methods in [11].

The restriction problem for the sphere does not make sense in the non-archimedean local field setting, because the unit sphere in K^n has positive Haar measure. Nonetheless, it is possible to consider parabolic versions of the restriction problem for such fields. Restriction problems for non-archimedean local fields are a subject of ongoing research, currently being pursued by Hickman and Wright.

10.3 Salem Sets

Although Theorem 1.4.1 is sufficient to precisely determine the Fourier dimension of $W(\tau)$, Theorem 1.4.2 is not sufficient to precisely determine the Fourier dimension of $W(m, n, \tau)$. Computing upper bounds on the Fourier dimension of a set E is typically a difficult problem because it requires a statement about the pointwise Fourier decay of all measures on E.

There does not appear to be a simple way to modify the argument of Theorem 1.4.1 to apply to local fields other than $\mathbb{Q}_p$ because of the difficulty of establishing the exponential sum estimate used to prove Lemma 9.2.1 in this setting. Together with Hambrook, we will aim to consider this problem. Some preliminary computations seem to indicate that a similar estimate should hold over arbitrary local fields.

The problem of computing explicit Salem sets of arbitrary Fourier dimension in $\mathbb{Q}_p^n$ for $n > 1$ is still open. Hambrook [23] has constructed explicit Salem sets of arbitrary Fourier dimension in $\mathbb{R}^2$, but no such sets are known in $\mathbb{R}^n$ for $n > 2$.

Hambrook and I are interested in constructing Salem sets in $\mathbb{R}^n$. As a prototype for this argument, we are exploring alternative matrix-based constructions for Salem sets in $\mathbb{R}^2$.

We are also interested in the problem of computing the Fourier dimension of a modified version of $E(\tau)$, so that the numerators r are restricted to lie in a subset of $\{0, \ldots, q\}$ such as the quadratic residues mod q.

Bibliography

[1] A. G. Abercrombie. The Hausdorff dimension of some exceptional sets of p-adic integer matrices. *J. Number Theory*, 53(2):311–341, 1995.

[2] F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U. S. A.*, 32:331–332, 1946.

[3] A. S. Besicovitch. On Kakeya's problem and a similar one. *Math. Z.*, 27(1):312–320, 1928.

[4] C. Bluhm. Random recursive construction of Salem sets. *Ark. Mat.*, 34(1):51–63, 1996.

[5] C. Bluhm. On a theorem of Kaufman: Cantor-type construction of linear fractal Salem sets. *Ark. Mat.*, 36(2):307–316, 1998.

[6] J. Bourgain and M.-C. Chang. Nonlinear Roth type theorems in finite fields. *Israel J. Math.*, 221(2):853–867, 2017.

[7] X. Caruso. Almost all non-archimedean Kakeya sets have measure zero. Manuscript. Available at `https://arxiv.org/abs/1608.02720`. Online; accessed January 19, 2018.

[8] J. Cilleruelo and M. Z. Garaev. Concentration of points on two and three dimensional modular hyperbolas and applications. *Geom. Funct. Anal.*, 21(4):892–904, 2011.

[9] E. Croot, V. F. Lev, and P. P. Pach. Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. *Ann. of Math. (2)*, 185(1):331–337, 2017.

[10] R. O. Davies. Some remarks on the Kakeya problem. *Proc. Cambridge Philos. Soc.*, 69:417–421, 1971.

[11] E. P. Dummit and M. Hablicsek. Kakeya sets over non-Archimedean local rings. *Mathematika*, 59(2):257–266, 2013.

[12] Z. Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009.

[13] Y. Edel. Extensions of generalized product caps. *Des. Codes Cryptogr.*, 31(1):5–14, 2004.

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

[15] F. Ekström, T. Persson, and J. Schmeling. On the Fourier dimension and a modification. *J. Fractal Geom.*, 2(3):309–337, 2015.

[16] J. S. Ellenberg and D. Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Ann. of Math. (2)*, 185(1):339–343, 2017.

[17] J. S. Ellenberg, R. Oberlin, and T. Tao. The Kakeya set and maximal conjectures for algebraic varieties over finite fields. *Mathematika*, 56(1):1–25, 2010.

[18] R. Fraser. Large subsets of local fields not containing configurations. Submitted. Available at `https://arxiv.org/abs/1612.08231`. Online; accessed January 19, 2018.

[19] R. Fraser and M. Pramanik. Large sets avoiding patterns. Submitted.

[20] R. Fraser. Kakeya-type sets in local fields with finite residue field. *Mathematika*, 62(2):614–629, 2016.

[21] R. Fraser and K. Hambrook. Explicit salem sets, Fourier restriction, and metric diophantine approximation in the p-adic numbers. Submitted. Available at `https://arxiv.org/abs/1708.05770`. Online; accessed January 19, 2018.

[22] O. Frostman. Potentiel déquilibre et capacité des ensembles avec quelques applications à la théorie des fonctions. *Lunds Univ. Math Sem.*, 3:1–118, 1935.

[23] K. Hambrook. Explicit Salem sets in $\mathbb{R}^2$. *Adv. Math.*, 311:634–648, 2017.

[24] K. Hambrook. Explicit salem sets and applications to metrical diophantine approximation. To Appear in Tran. Amer. Math. Soc.

[25] V. Jarník. über die simultanen diophantischen Approximationen. *Math. Z.*, 33(1):505–543, 1931.

[26] J.-P. Kahane. *Some random series of functions*, volume 5 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 1985.

[27] R. Kaufman. On the theorem of Jarník and Besicovitch. *Acta Arith.*, 39(3):265–267, 1981.

[28] T. Keleti. A 1-dimensional subset of the reals that intersects each of its translates in at most a single point. *Real Anal. Exchange*, 24(2):843–844, 1998/99.

[29] T. Keleti. Construction of one-dimensional subsets of the reals not containing similar copies of given patterns. *Anal. PDE*, 1(1):29–33, 2008.

[30] T. W. Körner. Measures on independent sets, a quantitative version of Rudin's theorem. *Proc. Amer. Math. Soc.*, 135(12):3823–3832, 2007.

[31] T. W. Körner. Fourier transforms of measures and algebraic relations on their supports. *Ann. Inst. Fourier (Grenoble)*, 59(4):1291–1319, 2009.

[32] I. Łaba and M. Pramanik. Arithmetic progressions in sets of fractional dimension. *Geom. Funct. Anal.*, 19(2):429–456, 2009.

[33] P. Maga. Full dimensional sets without given patterns. *Real Anal. Exchange*, 36(1):79–90, 2010/11.

[34] A. Máthé. Sets of large dimension not containing polynomial configurations. *Adv. Math.*, 316:691–709, 2017.

[35] P. Mattila. *Geometry of sets and measures in Euclidean spaces*, volume 44 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1995. Fractals and rectifiability.

[36] P. Mattila. *Fourier analysis and Hausdorff dimension*, volume 150 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2015.

[37] J. V. Melničuk. Hausdorff dimension in Diophantine approximations of p-adic numbers. *Ukrain. Mat. Zh.*, 32(1):118–124, 144, 1980.

[38] C. Papadimitropoulos. *Fourier Restriction Phenomenon in Thin Sets.* PhD thesis, University of Edinburgh, 2010.

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

[40] C. Papadimitropoulos. Salem sets in the p-adics, the Fourier restriction phenomenon and optimal extension of the Hausdorff-Young inequality. In *Vector measures, integration and related topics*, volume 201 of *Oper. Theory Adv. Appl.*, pages 327–338. Birkhäuser Verlag, Basel, 2010.

[41] A. M. Robert. *A course in p-adic analysis*, volume 198 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2000.

[42] K. Roth. Sur quelques ensembles d'entiers. *C. R. Acad. Sci. Paris*, 234:388–390, 1952.

[43] I. Z. Ruzsa. Difference sets without squares. *Period. Math. Hungar.*, 15(3):205–209, 1984.

[44] R. Salem. On singular monotonic functions whose spectrum has a given Hausdorff dimension. *Ark. Mat.*, 1:353–365, 1951.

[45] E. Sawyer. Families of plane curves having translates in a set of measure zero. *Mathematika*, 34(1):69–76, 1987.

[46] J.-P. Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics.* Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[47] P. Shmerkin. Salem Sets with No Arithmetic Progressions. *Int. Math. Res. Not. IMRN*, (7):1929–1941, 2017.

[48] E. M. Stein and S. Wainger. Problems in harmonic analysis related to curvature. *Bull. Amer. Math. Soc.*, 84(6):1239–1295, 1978.

[49] M. H. Taibleson. *Fourier analysis on local fields.* Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1975.

[50] P. A. Tomas. A restriction theorem for the Fourier transform. *Bull. Amer. Math. Soc.*, 81:477–478, 1975.

[51] A. Weil. *Basic number theory.* Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

[52] L. Wisewell. Families of surfaces lying in a null set. *Mathematika*, 51(1-2):155–162 (2005), 2004.

[53] J. Wolf. Finite field models in arithmetic combinatorics—ten years on. *Finite Fields Appl.*, 32:233–274, 2015.

[54] T. Wolff. Recent work connected with the Kakeya problem. In *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162. Amer. Math. Soc., Providence, RI, 1999.

[55] T. Wolff. *Lecture Notes on Harmonic Analysis*, volume 29 of *University Lecture Series*. AMS, 2003.