

UCLA

UCLA Electronic Theses and Dissertations

Title

Rational function progressions and the density versions of the Diophantine equations

Permalink

<https://escholarship.org/uc/item/6b3990bn>

ISBN

9798244868678

Author

Lim, Zi Li

Publication Date

2026-05-18

Peer reviewed|Thesis/dissertation

UNIVERSITY OF CALIFORNIA

Los Angeles

Rational function progressions
and
the density versions of the Diophantine equations

A dissertation submitted in partial satisfaction
of the requirements for the degree
Doctor of Philosophy in Mathematics

by

Zi Li Lim

2026

© Copyright by

Zi Li Lim

2026

ABSTRACT OF THE DISSERTATION

Rational function progressions
and
the density versions of the Diophantine equations

by

Zi Li Lim

Doctor of Philosophy in Mathematics
University of California, Los Angeles, 2026
Professor Terence Chi-Shen Tao, Chair

In this thesis, we discuss Szemerédi type theorems for three term rational function progressions and two dimensional rational function corners. Moreover, we also consider the density versions of some Diophantine equations over finite fields, cyclic rings and primes. The methods and techniques in number theory and additive combinatorics for these two topics are presented in this dissertation.

The dissertation of Zi Li Lim is approved.

Romyar Thomas Sharifi

Raphaël Alexis Rouquier

Don Malcolm Blasius

Terence Chi-Shen Tao, Committee Chair

University of California, Los Angeles

2026

TABLE OF CONTENTS

1	Introduction	1
1.1	Introduction	1
1.2	Rational function progressions	2
1.3	Rational function corners	6
1.4	The density version of the Waring–Goldbach problem	8
1.5	The density version of Waring’s problem over cyclic rings	11
1.6	The density version of the generalized Fermat equations over finite fields and cyclic rings	13
1.7	Road map	16
2	Three term rational function progressions	17
2.1	Overview	17
2.2	Convention	22
2.2.1	Notation	22
2.2.2	Fourier analysis notation	23
2.2.3	Algebraic geometry terminology	23
2.3	Algebraic geometry PET induction	24
2.4	Dimension estimates	29
2.5	Final arguments	38
3	Two dimensional rational function corners	43
3.1	Overview	43

3.2	Convention	46
3.2.1	Gowers norm notation	46
3.3	Algebraic geometry PET induction	46
3.4	Dimension estimates	60
3.5	Degree lowering	75
3.6	Higher dimensions	83
4	The density version of quadratic Waring’s problem and the quadratic Waring–Goldbach problem	85
4.1	Overview	85
4.1.1	Sketch of the proofs	86
4.1.2	Future directions	86
4.1.3	Road map	87
4.2	Preliminaries	88
4.2.1	Squares in $\mathbb{Z}/W$	88
4.2.2	Other notation	89
4.3	Restriction estimates	90
4.4	Sumsets of dense subsets of $\mathbb{Z}/W$	99
4.5	Transference principle	102
4.6	Counterexamples	107
4.7	A combinatorial lemma	108
4.8	Extensions to small moduli	119
5	The density version of the generalized Fermat equations	124
5.1	Overview	124

5.2	Preliminaries	125
5.2.1	Wrappers	125
5.2.2	A popular Cauchy–Davenport lemma	127
5.2.3	Deligne’s bound	127
5.3	Semchankau’s wrapping lemma	128
5.4	Finite fields	133
5.4.1	Equidistribution of powers	133
5.4.2	Average Fourier decay	134
5.4.3	Dense Fermat over finite fields	136
5.5	Finite, cyclic rings	138
5.5.1	Equidistribution of powers in wrappers	139
5.5.2	Dense Fermat over finite, cyclic rings	144
6	Appendix	147
6.1	More discussions on the proof of Theorem 3.4.2	147
6.1.1	Smooth parts	147
6.1.2	Degenerate subvarieties of low dimension	148
6.1.3	A comparison of the techniques	148
6.2	Proof of Proposition 4.2.2	149
6.3	Proof of Proposition 4.8.3	151
	References	156

LIST OF TABLES

1.1	Comparison of Theorem 1.4.3 and previous record	11
-----	---	----

ACKNOWLEDGMENTS

I would like to thank my advisor Terence Tao for his guidance, support and kindness, especially during the times when I did not make much progress. He is literally the best advisor one can ask for. Because of him, I truly believe that doing mathematics is one of the most joyful and beautiful things in this infinite universe.

I would also like to thank Don Blasius, Raphaël Rouquier and Romyar Sharifi for being in my doctoral committee. Moreover, I benefit a lot from learning the knowledge in algebra and algebraic number theory in their amazing classes.

I want to thank my collaborators, Sam Chow, Guo-Dong Hong, Akshat Mudgal, Fang-Ting Tu and Jeng-Daw Yu. Any problem in mathematics, no matter how important and fundamental it is, would not be as much fun and exciting if there is no one to share with. (Our collaborations have been very fruitful, in particular, Chapter 2 is based on the joint work [HL25], and Chapter 5 is based on the joint work [CLM25].)

I am very grateful that I receive a lot of support from the mathematics community. Indeed, this support is one of the crucial ingredients that I can grow as a graduate student. I want to say thank you to David Conlon, Ernie Croot, Rui Han, Chandrashekhara Khare, Borys Kuca, Dominique Maldague, Sarah Peluse, Xuancheng Shao, Fan Yang, Tongou Yang.

Friends at UCLA bring so much fun to my grad school life. Special shout out to Jaume de Dios Pont, Ben Goldman, Ben Johnsrude, James Leng, Elias Manuelides, Siddharth Mulherkar, Arian Nadjimzadah, Hagen Papenburg, Rushil Raghavan for all those fun memories, in a deep sense, we are all connected by Cauchy–Schwarz inequality. I also had a lot of interesting conversations with Lisang Ding, Jiahua Du, Zhaobo Han, John Hopper, Fan-Yun Hung, Rohan Joshi, Eric Kim, Roman Krutovski, Jerry Luo, Advika Rajapakse, Daniel Rui, Jacob Swenberg, Hong Kiat Tan, Lunji Zhu.

Finally, my family has always been there for me. To my parents, even though we live so far away from each other, but love brings us so close anyway. To my brother, congratulations

on getting married and having a baby! To my late grandmother, I truly wish that you can see how I am doing now, and I really miss you.

VITA

2016–2020 B.S. in Mathematics, National Taiwan University.

2021–2023 M.A. in Mathematics, University of California, Los Angeles.

2021–present Ph.D. in Mathematics, University of California, Los Angeles (expected).

PUBLICATIONS

Generalised Fermat equations in dense variables over finite fields and rings, with Sam Chow and Akshat Mudgal, 2026, arXiv: 2601.00135

On the density version of quadratic Waring’s problem and the quadratic Waring–Goldbach problem, 2025, arXiv: 2508.14939

Uniform nonlinear Szemerédi theorem for corners in finite fields, 2025, arXiv: 2501.04887

Three term rational function progressions in finite fields, with Guo-Dong Hong, Int. Math. Res. Not. IMRN 10 (2025)

CHAPTER 1

Introduction

1.1 Introduction

In combinatorics, one often asks when a specific pattern can be found in a given set, meanwhile, in number theory, one often asks when a particular equation can be solved. It is extremely unlikely that there is a simple and clean solution to these questions, and our best guess would probably be when there is no obvious obstruction and there are sufficient “opportunities”, then the desired combinatorial or arithmetic structures would occur. This guess would suggest that the desired combinatorial patterns can be found in a given set, when the given set is sufficiently dense in the ambient space. Similarly, perhaps we can expect that an equation is solvable, when there are sufficiently many variables in the equation. These bold speculations, although imperfect, could be quite insightful while formulated properly.

For instance, Szemerédi’s theorem [Sze75] states that any subset of the positive integers $\mathbb{N}$ with positive *upper density* contains arbitrarily long arithmetic progressions. (Recall that for a subset A of the positive integers $\mathbb{N}$, the upper density of A is defined to be

$$\limsup_{N \rightarrow \infty} \frac{|A \cap [N]|}{N}$$

where $[N]$ denotes the first N positive integers $\{1, 2, \dots, N\}$.) Here, the desired combinatorial patterns, which are arithmetic progressions, can be found in a given subset as long as the given subset is sufficiently dense to occupy a positive proportion of the ambient space $\mathbb{N}$. Another example, coming from number theory, is Hardy and Littlewood’s result [HL22] on Waring’s problem: let $k \geq 2$ be an integer, then any sufficiently large integers can be written

as a sum of $(k-2)2^{k-1} + 5$ many k -powers. In other words, the equation

$$N = x_1^k + x_2^k + \dots + x_s^k \tag{1.1.1}$$

is solvable over positive integers when $s \geq (k-2)2^{k-1} + 5$ and N is sufficiently large. Here, despite the highly nonlinear nature of the equation (1.1.1), the solutions still exist as long as there are sufficiently many variables in the equation.

If we are being optimistic, then we probably would believe that an arithmetic progression is not the only combinatorial pattern that can be found in a subset of the positive integers with positive upper density. After all, what is to prevent other combinatorial patterns, ranging from complicated algebraic configurations to sophisticated geometric figures, to occur? In the same spirit, we might believe that the equation (1.1.1) is solvable over primes, or any reasonably dense subsets of the positive integers. Influenced by this line of thoughts, the main topics of this thesis are

- finding nonlinear combinatorial patterns that involve rational functions
- solving Waring/Fermat type equations over sufficiently dense subsets

1.2 Rational function progressions

Szemerédi's theorem [Sze75] reveals the existence of linear patterns—arithmetic progressions in dense subsets of the positive integers. It turns out that nonlinear patterns are also captured by the dense subsets of the positive integers; Bergelson and Leibman [BL96] proved the following polynomial version of Szemerédi's theorem.

Theorem 1.2.1 (Bergelson–Leibman). *Let $P_1, P_2, \dots, P_k \in \mathbb{Z}[t]$ be polynomials with zero constant terms, and A be a subset of the positive integers $\mathbb{N}$ with positive upper density. Then, there exist $x, y \in \mathbb{Z}$ with $y \neq 0$ such that*

$$x, x + P_1(y), x + P_2(y), \dots, x + P_k(y) \in A.$$

The Bergelson–Leibman theorem can be regarded as a nonlinear generalization of Szemerédi’s theorem, since one can recover Szemerédi’s theorem by setting $P_1, P_2, \dots, P_k$ in Theorem 1.2.1 to be linear polynomials $t, 2t, \dots, kt$ (the condition $y \neq 0$ in Theorem 1.2.1 corresponds to the nonzero common differences of the arithmetic progressions). The configurations $x, x + P_1(y), x + P_2(y), \dots, x + P_k(y)$ are called *polynomial progressions*, since the shifts of these combinatorial patterns are determined by polynomials. As a remark, the zero constant term assumption in Theorem 1.2.1 eliminates congruence obstructions—the set $3\mathbb{N}$ does not contain any polynomial progressions $x, x + y^2 + 1$ since $y^2 + 1$ is not divisible by 3 for any y , but the upper density of $3\mathbb{N}$ is $1/3$.

The Bergelson–Leibman theorem hints that there are far more nonlinear patterns that can be found in dense subsets of the positive integers. A natural next step would be extending polynomial shifts to rational function shifts. To consider *rational function progressions*, it is best to formulate the problem in the finite field setting, since one can freely divide nonzero elements in finite fields as opposed to the integer setting. Bourgain and Chang [BC17] initiated the research on rational function progressions, proving the following Szemerédi type theorem for the progressions $x, x + y, x + 1/y$.

Theorem 1.2.2 (Bourgain–Chang). *Let p be a prime, and A be a subset of $\mathbb{F}_p$. Then, the following asymptotic formula is true.*

$$\# \left\{ (x, y) \in \mathbb{F}_p^2 : y \neq 0 \text{ and } x, x + y, x + \frac{1}{y} \in A \right\} = \frac{|A|^3}{p} + O(p^{2/5}|A|^{3/2})$$

The main term in the Bourgain–Chang theorem has a heuristic interpretation. There are p^2 many progressions $x, x + y, x + 1/y$ since these progressions are parametrized by two variables x, y . The probability that x is in A is $|A|/p$. Similarly, the probability that $x + y$ is in A and the probability that $x + 1/y$ is in A are also $|A|/p$. Heuristically, these events are almost independent since y and $1/y$ probably behave quite differently, hence one might expect that the probability that $x, x + y, x + 1/y$ are all in A is roughly $(|A|/p)^3$. Thus, the number of the progressions $x, x + y, x + 1/y$ that are in A is approximately $p^2(|A|/p)^3 = |A|^3/p$.

In the Bourgain–Chang theorem, the main term dominates the error term when $|A| \geq Cp^{1-1/15}$ for some suitable constant $C > 0$. Hence, the progressions $x, x + y, x + 1/y$ can be found even in the subsets that have exponentially small density $p^{-1/15}$, not just the subsets with a fixed positive density. (A stronger result on density is in fact a new feature of finite fields setting, compared to the original integer setting.)

Bourgain and Chang proposed this question: is there an asymptotic formula for general three term rational function progressions $x, x + F(y), x + G(y)$, where $F, G \in \mathbb{Q}(t)$ are rational functions satisfying suitable linear independence conditions? Hong and the author answer this question in the affirmative, by proving the following theorem in [HL25].

Theorem 1.2.3. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$. Let p be a prime, and A be a subset of $\mathbb{F}_p$. Then, the following asymptotic formula is true.*

$$\begin{aligned} & \# \{ (x, y) \in \mathbb{F}_p^2 : y \text{ is not a pole of } F \text{ or } G, \text{ and } x, x + F(y), x + G(y) \in A \} \\ &= \frac{|A|^3}{p} + O_{F,G}(p^{2/5}|A|^{3/2}) \end{aligned}$$

Remark 1.2.4. In this thesis, we will frequently need to evaluate a $\mathbb{Q}$ -coefficients rational function over $\mathbb{F}_p$. Here, we use the natural interpretation. Let $F(t) \in \mathbb{Q}(t)$ be a rational function and write $F(t) = a(t)/b(t)$ with $a(t), b(t) \in \mathbb{Z}[t]$ and $\gcd(a(t), b(t)) = 1$. For any $y \in \mathbb{F}_p$ such that $b(y) \neq 0$, define $F(y) = a(y) \cdot (b(y))^{-1}$ where $(b(y))^{-1}$ is the multiplicative inverse of $b(y)$ in $\mathbb{F}_p^\times$.

Hong and the author in fact prove a functional version of Theorem 1.2.3. To state the results, we introduce some notation first. In this thesis, when there are rational functions involved, the notation $\mathbb{E}$ will be interpreted as averaging excluding the poles of the rational functions being averaged. For example, if $F(t), G(t) \in \mathbb{Q}(t)$ are rational functions and

$f_0, f_1, f_2 : \mathbb{F}_p \longrightarrow \mathbb{C}$ are functions, then

$$\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y)) = \frac{1}{p^2} \sum_{x,y \in \mathbb{F}_p \text{ and } y \neq \text{poles of } F \text{ or } G} f_0(x) f_1(x + F(y)) f_2(x + G(y)).$$

The notation $\|\cdot\|_2$ is the L^2 -norm with respect to the uniform probability measure on $\mathbb{F}_p$, that is, $\|f\|_2 = \left(\frac{1}{p} \sum_{x \in \mathbb{F}_p} |f(x)|^2\right)^{1/2}$.

Theorem 1.2.5. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$. Then, we have the asymptotic formula*

$$\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y)) = \prod_{i=0}^2 \mathbb{E}_z f_i(z) + O_{F,G}(p^{-1/10} \|f_0\|_2 \|f_1\|_2 \|f_2\|_2)$$

for all functions $f_0, f_1, f_2 : \mathbb{F}_p \longrightarrow \mathbb{C}$.

Specializing to $f_0 = f_1 = f_2 = 1_A$, where 1_A is the characteristic function of a subset A , Theorem 1.2.5 (functional version) recovers Theorem 1.2.3 (set theoretic version). As a remark, Bourgain and Chang also proved the functional version of the asymptotic formula for the progressions $x, x + y, x + 1/y$, and also for the progressions $x, x + y, x + y^2$.

Aside from being a generalization of Bourgain and Chang's results, Theorem 1.2.5 can also be viewed as a generalization of Peluse's results [Pel18] and Dong, Li and Sawin's results [DLS20] on three term polynomial progressions in finite fields.

As a remark, in Theorem 1.2.5, the linear independence assumption for $F(t), G(t)$ and the constant function 1 is reasonably natural; it includes the case that F, G are linearly independent polynomials with zero constant terms. This assumption also includes the formulation of the question of three term rational function progressions in Peluse's survey [Pel23, Question 3.13]. In fact, the linear independence assumption is necessary for the asymptotic formula to be valid. In the linear dependence case, the asymptotic formula is no longer true, but one can still formulate different statements for Szemerédi type theorems, however, this aspect will not be discussed in this thesis.

1.3 Rational function corners

It turns out that Szemerédi type phenomena occur not just in the one dimensional world. Furstenberg and Katznelson [FK78] generalized Szemerédi’s theorem to the multidimensional setting.

Theorem 1.3.1 (Furstenberg–Katznelson). *Let $d \geq 1$ and S be a finite subset of $\mathbb{Z}^d$. Then, any subset of $\mathbb{N}^d$ with positive upper density contains a homothetic copy of S , i.e., $v + a \cdot S$ where $v \in \mathbb{Z}^d$ and $a \in \mathbb{Z} \setminus \{0\}$.*

By setting $d = 1$ and $S = \{1, 2, \dots, k\}$, Theorem 1.3.1 recovers Szemerédi’s theorem on arithmetic progressions. Theorem 1.3.1 applies to a wide range of combinatorial patterns, since S can be any finite set, that is, one can even be creative and choose S to be an extremely sophisticated geometric configuration that consists of 1 billion points!

In the same spirit of the question of Bourgain and Chang regarding rational function progressions, one can pursue finding multidimensional configurations that involve rational functions. Among the infinitely rich class of multidimensional configurations, the first candidate to be considered would be *two dimensional corners*. To be more precise, a two dimensional corner is a three point configuration given by

$$(x_1, x_2), (x_1 + y, x_2), (x_1, x_2 + y)$$

for some x_1, x_2, y . The reason why two dimensional corners can serve as a first nontrivial example is that they are closely connected to three term arithmetic progressions. We would like to consider *two dimensional rational function corners*, i.e., the three point configurations given by

$$(x_1, x_2), (x_1 + F(y), x_2), (x_1, x_2 + G(y))$$

where F, G are rational functions. Intuitively, these configurations are corners with side length determined by rational functions in a highly nonlinear fashion.

The author proves an asymptotic formula for two dimensional rational function corners in [Lim25b].

Theorem 1.3.2. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$. Then we have the asymptotic formula*

$$\begin{aligned} \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O_{F, G} \left(p^{-\frac{1}{40960}} \right) \end{aligned}$$

for all 1-bounded functions $f_0, f_1, f_2 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$.

Remark 1.3.3. We have not attempted to optimize the power-saving exponent $1/40960$. The precise numerical value of the power-saving exponent can be ignored for a first reading.

Just like the one dimensional case, Theorem 1.3.2 can imply a set theoretic result on two dimensional rational function corners (but it is more complicated to state though). To see this, let f_0, f_1, f_2 be the characteristic function 1_A for some subset $A \subset \mathbb{F}_p^2$, and note that

$$\mathbb{E}_{x_1, x_2} \left(1_A(x_1, x_2) \mathbb{E}_a 1_A(a, x_2) \mathbb{E}_b 1_A(x_1, b) \right) \gg \left(\mathbb{E}_{x_1, x_2} 1_A(x_1, x_2) \right)^3$$

by the pigeonhole principle (see [HLY21, Lemma 3.1] for details). This leads to the following set theoretic version of Theorem 1.3.2.

Theorem 1.3.4. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$. There exist constants $c_1, c_2 > 0$ (at most depending on F, G) such that if p is a prime and A is a subset of $\mathbb{F}_p^2$ with $|A| \geq c_1 p^{2-1/122880}$, then*

$$\begin{aligned} \# \left\{ \begin{array}{l} (x_1, x_2, y) \in \mathbb{F}_p^3 : y \text{ is not a pole of } F \text{ or } G, \\ \text{and } (x_1, x_2), (x_1 + F(y), x_2), (x_1, x_2 + G(y)) \in A \end{array} \right\} \\ \geq c_2 \frac{|A|^3}{p^3} \end{aligned}$$

Theorem 1.3.2 generalizes Han, Lacey and Yang’s [HLY21] results and Kuca’s results [Kuc24b], [Kuc24a] on two dimensional *polynomial* corners in finite fields. Also, Theorem 1.3.2 can be viewed as a generalization of Theorem 1.2.5, thanks to the close connections between two dimensional rational function corners and one dimensional three term rational function progressions. To see this, let $g_0, g_1, g_2 : \mathbb{F}_p \rightarrow \mathbb{C}$ be 1-bounded functions, and define $f_i : \mathbb{F}_p^2 \rightarrow \mathbb{C}$ by setting $f_i(x_1, x_2) = g_i(x_1 + x_2)$ for $i = 0, 1, 2$. Then, we have

$$\begin{aligned} & \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ &= \mathbb{E}_{x_1, x_2, y} g_0(x_1 + x_2) g_1(x_1 + F(y) + x_2) g_2(x_1 + x_2 + G(y)) \\ &= \mathbb{E}_{x, y} g_0(x) g_1(x + F(y)) g_2(x + G(y)), \end{aligned}$$

meanwhile

$$\mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) = \mathbb{E}_{x_1, x_2} \left(g_0(x_1 + x_2) \mathbb{E}[g_1] \mathbb{E}[g_2] \right) = \mathbb{E}[g_0] \mathbb{E}[g_1] \mathbb{E}[g_2].$$

1.4 The density version of the Waring–Goldbach problem

Now, we turn our attention from finding combinatorial structures to finding arithmetic structures. The following famous theorem in analytic number theory is due to Vinogradov [Vin37].

Theorem 1.4.1 (Vinogradov). *Any sufficiently large odd integers can be written as a sum of three primes.*

If we take the viewpoint of Szemerédi type theorems, then we would believe that the informal reason why Vinogradov’s three primes theorem is true is that primes are sufficiently dense in the integers so that it is impossible to exclude the desired additive patterns. This heuristic would suggest that Vinogradov’s theorem is not only true for primes, but also any sufficiently dense subsets of the primes. This is where things get interesting and subtle, since positive density is no longer enough unlike the Szemerédi type theorems. To be more precise,

let

$$A = \{p : p \text{ is a prime and } p \equiv 1 \pmod{3}\}$$

then A consists of 50% of the primes by Dirichlet's theorem on primes in arithmetic progressions. However, any odd integer that is not divisible by 3 cannot be represented as a sum of three primes in A , due to the congruence obstruction. Perhaps this is an interesting twist in the story; one has to be more careful with the *density threshold* in the formulation of the density version of Vinogradov's three primes theorem. This rather mysterious density threshold was determined by Shao [Sha14]. Before stating Shao's results, we recall the definition of *relative lower density*. Denote the set of all prime numbers by $\mathcal{P}$. Let A be a subset of primes, the relative lower density $\delta_{\mathcal{P}}(A)$ is defined to be

$$\delta_{\mathcal{P}}(A) = \liminf_{N \rightarrow \infty} \frac{|A \cap [N]|}{|\mathcal{P} \cap [N]|}.$$

Theorem 1.4.2 (Shao). *Let A be a subset of the primes with relative lower density $\delta_{\mathcal{P}}(A) > 5/8$. Then, any sufficiently large odd integer can be written as a sum of three primes in A .*

Moreover, the density threshold $5/8$ is sharp. Let

$$B = \{p \in \mathcal{P} : p \equiv 1, 2, 4, 7, 13 \pmod{15}\}$$

then B has relative density $5/8$, but any integer that is $14 \pmod{15}$ cannot be written as a sum of three primes in B .

Prior to Shao's results, Li and Pan [LP10] obtained a density version of Vinogradov's three primes theorem with a density threshold $2/3$. Following Li and Pan's work and Shao's work, a lot of research has been done in understanding the density version of the Waring–Goldbach problem [Gao25], [Zha25], [Tan25] and Waring's problem [Sal21], however, the sharp density thresholds remain unknown.

In [Lim25a], the author obtains some new improvements on the density version of the quadratic Waring–Goldbach problem, i.e., the problem of representing large integers by sums

of squares of primes in dense subsets. For any integer $s \geq 5$, define

$$D_s := \begin{cases} \frac{59}{60} & \text{if } s = 5 \\ \frac{7}{8} & \text{if } s = 6 \\ \frac{3}{4} & \text{if } s = 7 \\ \frac{s+13}{4s} & \text{if } 8 \leq s \leq 12 \\ \frac{1}{2} & \text{if } s \geq 13 \end{cases}$$

Theorem 1.4.3. *Let $s \geq 5$ be an integer, and A be a subset of primes with relative lower density $\delta_{\mathcal{P}}(A) > \sqrt{D_s}$. Then, for all sufficiently large integers y that are congruent to $s \pmod{24}$, there exist primes $p_1, p_2, \dots, p_s \in A$ such that $y = p_1^2 + p_2^2 + \dots + p_s^2$.*

Remark 1.4.4. The congruence condition in Theorem 1.4.3 is necessary, since the square of any prime greater than 3 is congruent to 1 mod 24.

For comparison, Gao [Gao25] proved a density theorem for the quadratic Waring–Goldbach problem for $s \geq 44$ and density threshold $3/4$, and Zhao [Zha25] improved the result to $s \geq 8$ and density threshold $\sqrt{1 - \min\{s, 16\}/32}$. The density thresholds $\sqrt{D_s}$ given by Theorem 1.4.3 improve upon previous records when $s \geq 6$. However, when $s = 5$, our density threshold is not as good as the density threshold $\sqrt{4/5}$ obtained by Tan [Tan25]. (We still include the computations for Theorem 1.4.3 when $s = 5$ to demonstrate the method.) The table below is a detailed numerical comparison between the density thresholds in Theorem 1.4.3 and the previous records.

Comparison of Theorem 1.4.3 and previous record					
s	$\sqrt{D_s}$	Previous record	s	$\sqrt{D_s}$	Previous record
5	$\sqrt{\frac{59}{60}} \approx 0.9916$	$\sqrt{\frac{4}{5}} \approx 0.8944$	11	$\sqrt{\frac{6}{11}} \approx 0.7385$	$\sqrt{\frac{21}{32}} \approx 0.8101$
6	$\sqrt{\frac{7}{8}} \approx 0.9354$	unknown previously	12	$\sqrt{\frac{25}{48}} \approx 0.7217$	$\sqrt{\frac{5}{8}} \approx 0.7906$
7	$\sqrt{\frac{3}{4}} \approx 0.8660$	unknown previously	13	$\sqrt{\frac{1}{2}} \approx 0.7071$	$\sqrt{\frac{19}{32}} \approx 0.7706$
8	$\sqrt{\frac{21}{32}} \approx 0.8101$	$\sqrt{\frac{3}{4}} \approx 0.8660$	14	$\sqrt{\frac{1}{2}} \approx 0.7071$	$\sqrt{\frac{9}{16}} \approx 0.7500$
9	$\sqrt{\frac{11}{18}} \approx 0.7817$	$\sqrt{\frac{23}{32}} \approx 0.8478$	15	$\sqrt{\frac{1}{2}} \approx 0.7071$	$\sqrt{\frac{17}{32}} \approx 0.7289$
10	$\sqrt{\frac{23}{40}} \approx 0.7583$	$\sqrt{\frac{11}{16}} \approx 0.8292$	≥ 16	$\sqrt{\frac{1}{2}} \approx 0.7071$	$\sqrt{\frac{1}{2}} \approx 0.7071$

Table 1.1: Comparison of Theorem 1.4.3 and previous record

(In the table above, the previous records are obtained by Zhao when $s \geq 8$ and by Tan when $s = 5$.)

1.5 The density version of Waring's problem over cyclic rings

The density thresholds in Theorem 1.4.3 are not optimal. One of the reasons why obtaining sharp density thresholds in the density version of the Waring–Goldbach problem and Waring's problem is difficult is the complicated congruence obstruction, as shown by the extremal example in Shao's theorem. Perhaps a classical philosophy in number theory would suggest

that we should consider the density version of the local problems before solving the density version of the global problems. In the density version of the local problems, the congruence obstructions disappear and we can focus on other essential difficulties of the problems.

The author obtains a *sharp* density theorem for quadratic Waring's problem over cyclic rings in [Lim25a]. Informally, it gives a density threshold of $1/s$ of the Waring problem for sums of s squares in a cyclic ring, provided that the order of the ring is not divisible by small primes, and s is at least 5. For any positive integer W , denote the squares in $\mathbb{Z}/W$ by $(\mathbb{Z}/W)^{(2)}$.

Theorem 1.5.1. *Let $s \geq 5$ be an integer and $\theta \in (1/s, 1]$. There exists a constant $M(s, \theta)$ depending only on s and θ such that the following holds.*

Suppose $W = \prod_i p_i^{n_i}$ is an integer with $p_i \geq M(s, \theta)$ for all i , and A is a subset of the squares in $\mathbb{Z}/W$ with relative density greater than or equal to θ , i.e. $|A| \geq \theta |(\mathbb{Z}/W)^{(2)}|$. Then, for all $y \in \mathbb{Z}/W$, there exist $x_1, x_2, \dots, x_s \in A$ such that $y = x_1 + x_2 + \dots + x_s$. Moreover, one has the following quantitative estimate

$$|\{(x_1, x_2, \dots, x_s) \in A^s : y = x_1 + x_2 + \dots + x_s\}| \geq c(s, \theta) W^{-1} |(\mathbb{Z}/W)^{(2)}|^s$$

for some constant $c(s, \theta) > 0$ depending only on s and θ .

Remark 1.5.2. For Theorem 1.5.1, it is necessary to exclude small prime divisors. Let W be an integer coprime to 3, and $A = \{x \in (\mathbb{Z}/3W)^{(2)} : x \equiv 0 \pmod{3}\}$, then the relative density of A is $1/2$, but the s -fold sumset of A can only contain the elements congruent to $0 \pmod{3}$.

It might be worth to point out that the squares in $\mathbb{Z}/W$ are fairly sparse. Suppose $W = \prod_{1 \leq i \leq r} p_i$ is a product of r distinct odd primes, then the absolute density of $(\mathbb{Z}/W)^{(2)}$ in the ambient space $\mathbb{Z}/W$ is at most $\prod_{1 \leq i \leq r} (p_i + 1)/(2p_i) \leq (2/3)^r$, which tends to zero when $r \rightarrow \infty$. Hence, a subset of $(\mathbb{Z}/W)^{(2)}$ with relative density greater than $1/s$ can have absolute density arbitrarily close to zero.

The next theorem confirms that the density threshold $1/s$ is indeed sharp, except possibly at the endpoint.

Theorem 1.5.3. *Let $s \geq 5$ be an integer and $\tau \in [0, 1/s)$. For every sufficiently large (depending only on s and τ) prime p , there exists a subset A_p of the squares in $\mathbb{Z}/p$ with relative density greater than or equal to τ , i.e. $|A_p| \geq \tau |(\mathbb{Z}/p)^{(2)}|$, but the s -fold sumset sA_p is not equal to $\mathbb{Z}/p$.*

1.6 The density version of the generalized Fermat equations over finite fields and cyclic rings

Waring's problem concerns a very specific type of Diophantine equations. It is natural to wonder if the density type theorems hold for other equations as well? Chow, Mudgal and the author [CLM25] prove a *sharp* density theorem for a large class of Diophantine equations—*generalized Fermat equations*, over finite fields and cyclic rings.

Theorem 1.6.1. *Let r and $i_1 < \dots < i_r$ be positive integers, and let $s \geq 3$ be an integer. Let*

$$[s] = I_1 \cup \dots \cup I_r$$

be a partition of $[s]$ into discrete intervals $I_1, \dots, I_r$ such that $|I_j| = k_j$ for all j . Let $\kappa > 0$, and let $\varepsilon > 0$ be sufficiently small in terms of s, i_r, κ . Let p be a prime sufficiently large in terms of s, i_r, κ , and let $q = p^n$ for some $n \in \mathbb{N}$. Let $u \in \mathbb{F}_q$, let $c_1, \dots, c_s \in \mathbb{F}_q \setminus \{0\}$, and let $A \subseteq \mathbb{F}_q$ with

$$|A| \geq \left(\prod_{1 \leq j \leq r} \frac{1}{rk_j} + \kappa \right) q. \quad (1.6.1)$$

Then there are at least εq^{s-1} many solutions $\mathbf{x} \in A^s$ to

$$\sum_{1 \leq j \leq r} \sum_{m \in I_j} c_m x_m^{i_j} = u. \quad (1.6.2)$$

Specializing to the case that $r = 1$ and $i_1 = d$, Theorem 1.6.1 implies a density theorem for the Waring-type problem over $\mathbb{F}_q$.

Corollary 1.6.2. *Let $s \geq 3$ and $d \geq 1$ be integers. Let $\kappa > 0$, and let $\varepsilon > 0$ be sufficiently small in terms of s, d, κ . Let p be a prime sufficiently large in terms of s, d, κ , and let $q = p^n$ for some $n \in \mathbb{N}$. Let $u \in \mathbb{F}_q$, let $c_1, \dots, c_s \in \mathbb{F}_q \setminus \{0\}$, and let $A \subseteq \mathbb{F}_q$ with*

$$\frac{|A|}{q} \geq \frac{1}{s} + \kappa.$$

Then there are at least εq^{s-1} many solutions $\mathbf{x} \in A^s$ to

$$c_1 x_1^d + \dots + c_s x_s^d = u. \quad (1.6.3)$$

The next example confirms that the density threshold in Theorem 1.6.1 is optimal.

Example 1.6.3. *Given $\lambda_1, \dots, \lambda_r \in \mathbb{F}_p \setminus \{0\}$, we set $c_m = \lambda_j$ for every $1 \leq j \leq r$ and every $m \in I_j$, and let*

$$A = \left\{ x \in \mathbb{F}_p : \lambda_j x^{i_j} \in \left(0, \frac{p}{k_j r}\right) \ (1 \leq j \leq r) \right\}.$$

One may apply Lemma 5.4.1, along with the fact that $\|\widetilde{\mathbf{1}}_P\|_1 \ll \log p$ (see Section 2.2 for our Fourier analysis notation) for any arithmetic progression P in $\mathbb{F}_p$, to deduce that

$$|A| = (1 + o(1))p \prod_{1 \leq j \leq r} \frac{1}{k_j r}.$$

Moreover A has no solutions to (1.6.2) when $u = 0$, since for every $1 \leq j \leq r$ and every $\{a_m\}_{m \in I_j} \subseteq A$, one has

$$\lambda_j \sum_{m \in I_j} a_m^{i_j} \in \left(0, \frac{p}{r}\right), \quad \text{whence} \quad \sum_{j=1}^r \sum_{m \in I_j} c_m a_m^{i_j} \in (0, p).$$

Theorem 1.6.1 has a counterpart in another important local model, the cyclic ring $\mathbb{Z}/W$ model. (The finite field $\mathbb{F}_q$ model and the cyclic ring $\mathbb{Z}/W$ model have different behaviors, but they are equally useful.)

Theorem 1.6.4. *Let r and $i_1 < \dots < i_r$ be positive integers, and let $s \geq 3$ be an integer. Let $[s] = I_1 \cup \dots \cup I_r$ be a partition of $[s]$ into discrete intervals $I_1, \dots, I_r$ such that $|I_j| = k_j$ for all j . Let $\kappa > 0$, let $\Omega \geq 1$, and let $\varepsilon > 0$ be sufficiently small in terms of s, i_r, κ, Ω . Then there exists a large constant M depending only on s, i_r, κ, Ω such that the following is true.*

Let $W = p_1^{n_1} \dots p_t^{n_t}$ with

$$t, n_1, \dots, n_t \leq \Omega \quad \text{and} \quad p_1, \dots, p_t \geq M. \quad (1.6.4)$$

Let $u \in \mathbb{Z}/W$, let $c_1, \dots, c_s \in (\mathbb{Z}/W)^\times$, and let $A \subseteq \mathbb{Z}/W$ with

$$|A| \geq \left(\prod_{1 \leq j \leq r} \frac{1}{rk_j} + \kappa \right) W. \quad (1.6.5)$$

Then there are at least εW^{s-1} many solutions $\mathbf{x} \in A^s$ to (1.6.2).

As before, Theorem 1.6.4 implies a density theorem for the Waring-type problem over $\mathbb{Z}/W$.

Corollary 1.6.5. *Let $s \geq 3$ and $d \geq 1$ be integers. Let $\kappa > 0$, let $\Omega \geq 1$, and let $\varepsilon > 0$ be sufficiently small in terms of s, d, κ, Ω . Then, there exists a large constant M depending only on s, d, κ, Ω such that the following is true.*

Let $W = p_1^{n_1} \dots p_t^{n_t} \in \mathbb{N}$ with (1.6.4). Let $c_1, \dots, c_s \in (\mathbb{Z}/W)^\times$, let $u \in \mathbb{Z}/W$, and let $A \subseteq \mathbb{Z}/W$ with

$$\frac{|A|}{W} \geq \frac{1}{s} + \kappa.$$

Then there are at least εW^{s-1} many solutions $\mathbf{x} \in A^s$ to (1.6.3).

Compared to Theorem 1.5.1, Corollary 1.6.5 requires fewer variables but Theorem 1.5.1 allows stronger uniformity on the moduli W . Moreover, the proofs of them are fairly different—the proof of Theorem 1.5.1 is based on the transference principle while the proof of Theorem 1.6.4 (and hence Corollary 1.6.5) is based on the regularity lemma.

Remark 1.6.6. Similar to Remark 1.5.2, we note that it is necessary to exclude small prime divisors in Theorem 1.6.4. Let $d \in \mathbb{N}$, let $W = 3W'$ where W' is coprime to 3, and let

$$A = \{x \in \mathbb{Z}/W : x^d \equiv 1 \pmod{3}\}.$$

Then A has large density, which is $1/3$ when d is odd and $2/3$ when d is even. However, owing to the congruence obstruction, it is impossible to represent all elements in $\mathbb{Z}/W$ by $x_1^d + \cdots + x_s^d$ with $x_j \in A$ for all $1 \leq j \leq s$, no matter how large s is.

1.7 Road map

This thesis is organized as follows. We discuss three term rational function progressions in Chapter 2. In Chapter 3, we consider the two dimensional generalization of rational function progressions, i.e., two dimensional rational function corners. The topics of Chapter 4 are the density version of quadratic Waring's problem over cyclic rings and the quadratic Waring–Goldbach problem. The density version of the generalized Fermat equations over finite fields and cyclic rings is discussed in Chapter 5. We also include an appendix (Chapter 6) for completeness.

CHAPTER 2

Three term rational function progressions

2.1 Overview

In this chapter, we adapt the method developed in the joint work of Hong and the author [HL25] to reproduce a proof of Theorem 1.2.5.

Let $\mathcal{A}$ be a discrete interval $[N] = \{1, 2, \dots, N\}$ or a finite field, and $P_1, P_2, \dots, P_m \in \mathbb{Z}[t]$ be polynomials, define $r_{P_1, P_2, \dots, P_m}(\mathcal{A})$ to be the size of the largest subset of $\mathcal{A}$ that does not contain any nontrivial progression of the form

$$x, x + P_1(y), x + P_2(y), \dots, x + P_m(y).$$

Recall that Szemerédi [Sze75] proved that any subset of the positive integers of positive upper density contains an arbitrarily long nontrivial arithmetic progression, or equivalently,

$$r_{t, 2t, \dots, (k-1)t}([N]) = o_k(N)$$

for all $k \geq 2$ via combinatorial arguments. Shortly after Szemerédi's proof, Furstenberg [Fur77] found a new proof based on a completely different method, ergodic theory.

Bergelson and Leibman's theorem (Theorem 1.2.1) [BL96] can be rephrased as follows: let $P_1, P_2, \dots, P_m \in \mathbb{Z}[t]$ be polynomials with zero constant terms, then

$$r_{P_1, P_2, \dots, P_m}([N]) = o_{P_1, P_2, \dots, P_m}(N).$$

Bergelson and Leibman's proof is also based on ergodic theory.

Bergelson-Leibman's proof is qualitative in nature and Szemerédi's proof gives tower-type bounds. For sharper quantitative bounds, before Szemerédi, Roth [Rot53] already showed that

$$r_{t,2t}([N]) = O\left(\frac{N}{\log \log N}\right)$$

via Fourier analysis, but his arguments do not work for finding longer arithmetic progressions. In Gowers's celebrated papers [Gow98], [Gow01], he obtained quantitative bounds for the sets that do not contain arbitrarily long arithmetic progressions. More precisely, Gowers proved that for all $k \geq 2$, there exists a constant $c_k > 0$ such that

$$r_{t,2t,\dots,(k-1)t}([N]) = O_k\left(\frac{N}{(\log \log N)^{c_k}}\right)$$

via introducing higher order Fourier analysis. For quantitative bounds for general polynomial progressions, the general theory is not complete yet, but see Prendiville's [Pre17], Peluse and Prendiville's [PP24], Peluse's [Pel20], Peluse and Prendiville's [PP22], Bloom and Maynard's [BM22] and Peluse, Sah and Sawhney's [PSS23] results for the current state of the art.

Now, we turn our attention to finding progressions in finite fields, where new phenomena emerge. Here and throughout this chapter, let p be a prime and $\mathbb{F}_p$ be the finite field with p elements. One has the bound $r_{P_1,P_2,\dots,P_m}(\mathbb{F}_p) \leq r_{P_1,P_2,\dots,P_m}([p])$ *a priori*, but a much stronger bound is valid in many cases, since the images of polynomials are more densely distributed in $\mathbb{F}_p$. The case of two term polynomial progressions in finite fields is more straightforward and can be handled by a Fourier analytic calculation and Weil's bound. Hence, the first nontrivial polynomial progression in finite fields is the three term progression $x, x+y, x+y^2$. Bourgain and Chang [BC17] proved that $r_{t,t^2}(\mathbb{F}_p) \ll p^{1-1/15}$. In fact, Bourgain and Chang proved an asymptotic formula: if A is a subset of $\mathbb{F}_p$, then

$$\#\{(x, y) \in \mathbb{F}_p^2 : x, x+y, x+y^2 \in A\} = \frac{|A|^3}{p} + O(p^{2/5}|A|^{3/2}).$$

In the same paper, Bourgain and Chang posed the following three questions:

1. Let $P_1, P_2 \in \mathbb{Z}[t]$ be linearly independent polynomials with zero constant terms, is an

asymptotic formula for the number of the progressions $x, x + P_1(y), x + P_2(y)$ in subsets of $\mathbb{F}_p$ valid?

2. More generally, let $P_1, P_2, \dots, P_m \in \mathbb{Z}[t]$ be linearly independent polynomials with zero constant terms, is an asymptotic formula for the number of the progressions $x, x + P_1(y), x + P_2(y), \dots, x + P_m(y)$ in subsets of $\mathbb{F}_p$ valid?
3. In a different direction, can one replace the polynomials P_1, P_2 in the first question (1) by rational functions?

The first question (1) is answered by Peluse [Pel18] and independently by Dong, Li and Sawin [DLS20]. Peluse's theorem states that, if $P_1, P_2 \in \mathbb{Z}[t]$ are polynomials with zero constant terms such that P_1, P_2 are linearly independent over $\mathbb{Q}$, then

$$\#\{(x, y) \in \mathbb{F}_p^2 : x, x + P_1(y), x + P_2(y) \in A\} = \frac{|A|^3}{p} + O_{P_1, P_2}(p^{7/16}|A|^{3/2}).$$

for all subsets A of $\mathbb{F}_p$. This implies the bound $r_{P_1, P_2}(\mathbb{F}_p) \ll_{P_1, P_2} p^{1-1/24}$. Independently, Dong, Li and Sawin proved a similar result with the error term $O_{P_1, P_2}(p^{3/8}|A|^{3/2})$, implying $r_{P_1, P_2}(\mathbb{F}_p) \ll_{P_1, P_2} p^{1-1/12}$. As a side note, the linear independence assumption for P_1, P_2 is crucial, since one cannot hope for power saving bounds for progressions involving linearly dependent polynomials, even in the simplest case $x, x + y, x + 2y$ due to Behrend's example [Beh46]. Both Peluse's and Dong-Li-Sawin's methods applied deep results from algebraic geometry; Peluse's method used Deligne's proof of the Riemann hypothesis over finite fields while Dong-Li-Sawin's method used the Deligne-Katz theory.

The second question (2) is also answered by Peluse [Pel19]. By introducing the degree lowering method, Peluse proved that, if $P_1, P_2, \dots, P_m \in \mathbb{Z}[t]$ are polynomial with zero constant terms such that $P_1, P_2, \dots, P_m$ are linearly independent over $\mathbb{Q}$, then there exists a constant $\gamma > 0$ depending on $P_1, P_2, \dots, P_m$ such that

$$\#\{(x, y) \in \mathbb{F}_p^2 : x, x + P_1(y), x + P_2(y), \dots, x + P_m(y) \in A\} = \frac{|A|^{m+1}}{p^{m-1}} + O_{P_1, P_2, \dots, P_m}(p^{2-\gamma})$$

for all subsets A of $\mathbb{F}_p$. This implies the bound $r_{P_1, P_2, \dots, P_m}(\mathbb{F}_p) \ll_{P_1, P_2, \dots, P_m} p^{1-\gamma/(m+1)}$. Moreover, the degree lowering method only relies on Weil's bound for curves, as opposed to the heavy algebraic geometry machinery utilized in the methods [Pel18], [DLS20] for the three term polynomial progressions.

For the third question (3) of Bourgain and Chang, replacing the polynomials with rational functions presents new phenomena and difficulties. Unlike the case of polynomials, there is no obvious analogue of rational function progressions in integer setting, hence there is not any general bound *a priori*, not even a qualitative one. Bourgain and Chang's proof for the special progression $x, x + y, x + 1/y$ (Theorem 1.2.2) relies on the arithmetic geometry theorem that is specific to Kloosterman sums [FKM15]. All the previous methods [BC17], [Pel18], [DLS20], [Pel19] do not apply to the case of rational function progressions.

The third question is answered affirmatively by Theorem 1.2.5, which implies the bound $r_{F,G}(\mathbb{F}_p) \ll_{F,G} p^{1-1/15}$. Our approach to Theorem 1.2.5 also provides a new solution to the first question (1) of Bourgain and Chang. Compared to previous methods, the exponent in the bound $r_{F,G}(\mathbb{F}_p) \ll_{F,G} p^{1-1/15}$ is slightly better than the exponent $1 - 1/24$ in Peluse's method, but slightly worse than the exponent $1 - 1/12$ in Dong-Li-Sawin's method. Moreover, our approach has less dependence on algebraic geometry; hence for the special progressions $x, x + y, x + y^2$ and $x, x + y, x + 1/y$, our proof would be an "elementary" algebra proof.

The main new difficulty for the rational function progression problem is that differentiating a rational function does not reduce its complexity. If one wishes to apply the degree lowering method [Pel19], then one requires Gowers norm control for the counting operator *a priori*. However, Gowers norm control is done by PET induction via Weyl's differencing, which is unhelpful for rational functions. Applying Peluse's previous method for three term polynomial progressions [Pel18] or Dong-Li-Sawin's method [DLS20] also does not work, since both methods would reduce the problem to estimating multidimensional exponential sums on varieties with rational function phases, which is highly nontrivial and unknown.

The main novelty in [HL25] is the development of an algebraic geometry version of PET

induction that bypasses Weyl's differencing. If we wanted to prove the power saving bounds directly, then we would need strong bounds for multidimensional exponential sums on varieties with rational function phases, which is out of reach of the current arithmetic geometry methods. However, if we only want to obtain the Gowers norm control, then it suffices to estimate the dimension of certain varieties, which is in the scope of classical algebraic geometry. We would decompose the varieties of interest into generic parts and special subvarieties. The generic parts can be dealt with complex analytic techniques, while the special subvarieties, which have extra constraints and special structures, can be handled by mod p point counting. After establishing Gowers norm control, we can immediately run the degree lowering arguments. In fact, since we obtain a U^2 -Gowers norm control, we could perform a Fourier level set decomposition of the functions to get a better power-saving exponent.

It is worth pointing out that in this chapter, the Gowers norms show up differently than they usually do in the related literature. Also, the algebraic geometry PET induction we use has the same end goal as traditional PET induction, but the mechanism is different. In fact, this chapter does not rely on any higher order Fourier analysis, in particular, it does not use neither inverse theorem of Gowers norms nor degree lowering (although degree lowering could be a different way to end the arguments with a weaker exponent). However, we use the terminology from higher order Fourier analysis in the overview to draw parallel comparisons with the existing literature and to highlight the analogy in certain concepts. In the rest of this chapter, we would write all theorems and proofs in the classical Fourier analytic language so that this chapter could be as self-contained as possible. We are hoping that the framework of higher order Fourier analysis could offer an easier and more conceptual way to think about the rational function progressions; and indeed this is how Hong and the author came up with the proof. We do apologize if this leads to any confusion. Additionally, in the case of two dimensional rational function corners, one needs Gowers box norms and the degree lowering method, and Fourier analysis is no longer sufficient.

A natural problem is to generalize algebraic geometry PET induction to longer rational

function progressions, which is a subject we intend to return to in the future. Given that all the previous methods generalize to finite fields $\mathbb{F}_q$ that may not have prime cardinality, we believe our approach also extends to all finite fields. Furthermore, it is natural to wonder about the quantitative bounds for polynomial progressions involving linearly dependent polynomials. This problem is still widely open; see Kuca's work [Kuc21] and Leng's works [Len22], [Len24] for the current status.

This chapter is organized as follows. In Section 2.2, we define the notation used in this chapter. The Section 2.3 is about the framework of the algebraic geometry PET induction and the Section 2.4 is about the key dimension estimates required for the algebraic geometry PET induction. In Section 2.5, we put everything together to finish the proof.

2.2 Convention

2.2.1 Notation

Throughout, let p be a prime and $\mathbb{F}_p$ be the finite field with p elements. For any finite set $\mathcal{A}$ and function $f : \mathcal{A} \rightarrow \mathbb{C}$, let $\mathbb{E}_{x \in \mathcal{A}} f(x) = \frac{1}{|\mathcal{A}|} \sum_{x \in \mathcal{A}} f(x)$ be the average of f over $\mathcal{A}$. When the summation variables are in $\mathbb{F}_p$, we would often omit the subscript $\mathbb{F}_p$ in the summation notation and write $\mathbb{E}_x$ instead. When there are rational functions involved, the notation $\mathbb{E}$ will be interpreted as averaging excluding the poles of the rational functions being averaged. For example, if $F(t), G(t) \in \mathbb{Q}(t)$ are rational functions and $f_0, f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$ are functions, then

$$\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y)) = \frac{1}{p^2} \sum_{x,y \in \mathbb{F}_p \text{ and } y \neq \text{poles of } F \text{ or } G} f_0(x) f_1(x + F(y)) f_2(x + G(y)).$$

Similarly, when there are rational functions involved, the notation $\sum$ will be interpreted as the summation excluding the poles.

Furthermore, we would often omit the subscript F, G in Vinogradov's notation $\ll, \gg$ and Landau's notation O, o since the implied constants would usually depend on the rational

functions F, G . Moreover, let $e(x) = e^{2\pi ix}$, and $e_W(x) = e^{2\pi ix/W}$ for any positive integer W .

2.2.2 Fourier analysis notation

Let G be a finite abelian group. Let $f : G \rightarrow \mathbb{C}$ be a function on G . Denote the L^r -norm with respect to the uniform probability measure on G by $\|f\|_r = \left(\frac{1}{|G|} \sum_{x \in G} |f(x)|^r\right)^{1/r}$ and the l^r -norm with respect to the counting measure on G by $\|f\|_{l^r} = \left(\sum_{x \in G} |f(x)|^r\right)^{1/r}$.

Denote the group of characters of G by $\widehat{G}$. Let $\widehat{f} : \widehat{G} \rightarrow \mathbb{C}$ be the Fourier transform of f with respect to the probability measure, that is,

$$\widehat{f}(\gamma) = \frac{1}{|G|} \sum_{x \in G} f(x) \overline{\gamma(x)}.$$

Let $\widetilde{f} : \widehat{G} \rightarrow \mathbb{C}$ be the Fourier transform of f with respect to the counting measure, that is,

$$\widetilde{f}(\gamma) = \sum_{x \in G} f(x) \overline{\gamma(x)}.$$

For example, let d be a positive integer, and $f : \mathbb{F}_p^d \rightarrow \mathbb{C}$ be a function on $\mathbb{F}_p^d$. Then, we have $\widehat{f}(\xi) = \mathbb{E}_x f(x) e_p(-x\xi)$ and $\widetilde{f}(\xi) = \sum_x f(x) e_p(-x\xi)$.

Let $g : G \rightarrow \mathbb{C}$ be another function on G . Then the convolution of f and g is defined to be

$$f * g(x) = \sum_{\substack{y, z \in G \\ y+z=x}} f(y)g(z)$$

2.2.3 Algebraic geometry terminology

By (classical) varieties, we mean any classical affine, quasi-affine, projective or quasi-projective varieties. We do not require the varieties to be irreducible, hence our affine varieties and projective varieties may be algebraic sets in some references. By abuse of terminology, we also refer to schemes that are separated and of finite type over $\text{Spec } k$ for some field k as a variety. We would often use $Y(\mathbb{C}), Z(\mathbb{F}_p), \dots$ to denote classical varieties and $Y, Z, \dots$ to

denote schemes. If X is a scheme over some field k , we also write $X(k)$ as k -valued points $\text{Hom}_k(\text{Spec } k, X)$.

If X is a variety or scheme, denote the dimension of X as a variety (or scheme) by $\dim_{\text{Var}} X$ (or $\dim_{\text{Sch}} X$), which is the supremum of the length of the chains of irreducible closed subsets in the underlying topological space.

2.3 Algebraic geometry PET induction

In this section, we establish the framework of algebraic geometry PET induction, bounding the counting operator for three term rational function progressions in terms of U^2 -Gowers norm (equivalently, the l^4 -norm of the Fourier transform) of some weight function, and the size of the $\mathbb{F}_p$ -points of certain varieties. This allows us to bypass Weyl's differencing, which is unhelpful for rational functions, to obtain Gowers norm control.

Definition 2.3.1. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$. Define the **Roth variety** associated to $F(t), G(t)$ to be the (quasi-affine) variety cut out by the following system of equations in eight variables $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$.*

$$F(y_1) - G(y_1) - F(y_2) + G(y_2) - F(y_3) + G(y_3) + F(y_4) - G(y_4) = 0 \quad (2.3.1)$$

$$F(y_5) - G(y_5) - F(y_6) + G(y_6) - F(y_7) + G(y_7) + F(y_8) - G(y_8) = 0 \quad (2.3.2)$$

$$F(y_1) - F(y_3) - F(y_5) + F(y_7) = 0 \quad (2.3.3)$$

$$F(y_2) - F(y_4) - F(y_6) + F(y_8) = 0 \quad (2.3.4)$$

$$G(y_3) - G(y_4) - G(y_7) + G(y_8) = 0 \quad (2.3.5)$$

The Roth variety could be regarded as a classical variety or a scheme over various fields, for example, the complex numbers $\mathbb{C}$ or finite fields $\mathbb{F}_p$. The Roth variety is quasi-affine since the poles of F and G are excluded.

Theorem 2.3.2. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ and $Y(\mathbb{F}_p)$ be $\mathbb{F}_p$ -points of the Roth variety associated to $F(t), G(t)$. For all functions $f_0, f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$, we have the following l^4 -Fourier norm control (equivalently, U^2 -Gowers norm control):*

$$|\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y))| \leq \|f_0\|_2^{1/2} \|\widehat{f_0}\|_{l^4}^{1/2} \|f_1\|_2 \|f_2\|_2 \left(\frac{1}{p^3} |Y(\mathbb{F}_p)| \right)^{1/8}.$$

The Roth variety $Y(\mathbb{F}_p) \subset \mathbb{F}_p^8$ is carved out by five equations in eight variables, hence we “naively believe” that the size $|Y(\mathbb{F}_p)|$ is around p^3 when F and G are sufficiently “independent”. This naive heuristic would be justified in Section 2.4. Therefore, the Theorem 2.3.2 is essentially saying that the counting operators for three term rational function progressions have l^4 -Fourier control. The first half of the proof of Theorem 2.3.2 is similar to the Fourier calculations in [BC17], [DLS20]. However, instead of dealing with difficult exponential sum estimates and pursuing the strongest cancellation, we transform the exponential sums into point counting on varieties, which is easier to handle.

Proof of Theorem 2.3.2. Fourier expand the functions f_0, f_1, f_2 to obtain

$$\begin{aligned} & |\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y))| \\ &= \left| \sum_{n_0, n_1, n_2} \widehat{f_0}(n_0) \widehat{f_1}(n_1) \widehat{f_2}(n_2) \mathbb{E}_x e_p(n_0 x + n_1 x + n_2 x) \mathbb{E}_y e_p(n_1 F(y) + n_2 G(y)) \right|. \end{aligned}$$

For convenience, denote $K(n_1, n_2) = \mathbb{E}_y e_p(n_1 F(y) + n_2 G(y))$. By orthogonality of the characters, we have

$$\begin{aligned} & \left| \sum_{n_0, n_1, n_2} \widehat{f_0}(n_0) \widehat{f_1}(n_1) \widehat{f_2}(n_2) \mathbb{E}_x e_p(n_0 x + n_1 x + n_2 x) \mathbb{E}_y e_p(n_1 F(y) + n_2 G(y)) \right| \\ &= \left| \sum_{n_1, n_2} \widehat{f_0}(-n_1 - n_2) \widehat{f_1}(n_1) \widehat{f_2}(n_2) K(n_1, n_2) \right|. \end{aligned}$$

Rearrange, apply Cauchy–Schwarz inequality in n_2 and apply Parseval’s identity to obtain

$$\begin{aligned}
& \left| \sum_{n_1, n_2} \widehat{f}_0(-n_1 - n_2) \widehat{f}_1(n_1) \widehat{f}_2(n_2) K(n_1, n_2) \right| \\
&= \left| \sum_{n_2} \widehat{f}_2(n_2) \sum_{n_1} \widehat{f}_0(-n_1 - n_2) \widehat{f}_1(n_1) K(n_1, n_2) \right| \\
&\leq \|f_2\|_2 \left(\sum_{n_2, n_1, m_1} \widehat{f}_0(-n_1 - n_2) \overline{\widehat{f}_0}(-m_1 - n_2) \widehat{f}_1(n_1) \overline{\widehat{f}_1}(m_1) K(n_1, n_2) \overline{K}(m_1, n_2) \right)^{1/2}.
\end{aligned}$$

Once again, rearrange, apply Cauchy–Schwarz inequality in n_1, m_1 and apply Parseval's identity to obtain

$$\begin{aligned}
& \|f_2\|_2 \left(\sum_{n_2, n_1, m_1} \widehat{f}_0(-n_1 - n_2) \overline{\widehat{f}_0}(-m_1 - n_2) \widehat{f}_1(n_1) \overline{\widehat{f}_1}(m_1) K(n_1, n_2) \overline{K}(m_1, n_2) \right)^{1/2} \\
&= \|f_2\|_2 \left(\sum_{n_1, m_1} \widehat{f}_1(n_1) \overline{\widehat{f}_1}(m_1) \sum_{n_2} \widehat{f}_0(-n_1 - n_2) \overline{\widehat{f}_0}(-m_1 - n_2) K(n_1, n_2) \overline{K}(m_1, n_2) \right)^{1/2} \\
&\leq \|f_2\|_2 \|f_1\|_2 \left(\sum_{n_1, m_1, n_2, m_2} \widehat{f}_0(-n_1 - n_2) \overline{\widehat{f}_0}(-m_1 - n_2) \overline{\widehat{f}_0}(-n_1 - m_2) \widehat{f}_0(-m_1 - m_2) \right. \\
&\quad \left. K(n_1, n_2) \overline{K}(m_1, n_2) \overline{K}(n_1, m_2) K(m_1, m_2) \right)^{1/4}.
\end{aligned} \tag{2.3.6}$$

Note that the variables in $\widehat{f}_0$ satisfy a linear relation $(-n_1 - n_2) + (-m_1 - m_2) = (-m_1 - n_2) + (-n_1 - m_2)$, hence they shall depend on three variables after suitable change of variables. By the change of variables $n_1 \leftrightarrow n_1 - n_2$, $m_1 \leftrightarrow m_1 - n_2$, the last line in the expression (2.3.6) is equal to

$$\begin{aligned}
& \|f_2\|_2 \|f_1\|_2 \left(\sum_{n_1, m_1, n_2, m_2} \widehat{f}_0(-n_1) \overline{\widehat{f}_0}(-m_1) \overline{\widehat{f}_0}(-n_1 + n_2 - m_2) \widehat{f}_0(-m_1 + n_2 - m_2) \right. \\
&\quad \left. K(n_1 - n_2, n_2) \overline{K}(m_1 - n_2, n_2) \overline{K}(n_1 - n_2, m_2) K(m_1 - n_2, m_2) \right)^{1/4}.
\end{aligned} \tag{2.3.7}$$

By the change of variables $a \leftrightarrow n_2 - m_2$, $b \leftrightarrow n_2$, the expression (2.3.7) is equal to

$$\begin{aligned}
& \|f_2\|_2 \|f_1\|_2 \left(\sum_{n_1, m_1, a, b} \widehat{f}_0(-n_1) \overline{\widehat{f}_0}(-m_1) \overline{\widehat{f}_0}(-n_1 + a) \widehat{f}_0(-m_1 + a) \right. \\
&\quad \left. K(n_1 - b, b) \overline{K}(m_1 - b, b) \overline{K}(n_1 - b, b - a) K(m_1 - b, b - a) \right)^{1/4}.
\end{aligned} \tag{2.3.8}$$

Rearranging and applying Cauchy–Schwarz inequality in n_1, m_1, a , the expression (2.3.8) is equal to

$$\begin{aligned}
& \|f_2\|_2 \|f_1\|_2 \left(\sum_{n_1, m_1, a} \widehat{f}_0(-n_1) \overline{\widehat{f}_0(-m_1)} \overline{\widehat{f}_0(-n_1 + a)} \widehat{f}_0(-m_1 + a) \right. \\
& \quad \left. \sum_b K(n_1 - b, b) \overline{K(m_1 - b, b)} \overline{K(n_1 - b, b - a)} K(m_1 - b, b - a) \right)^{1/4} \\
& \leq \|f_2\|_2 \|f_1\|_2 \left(\sum_{n_1, m_1, a} |\widehat{f}_0(-n_1) \overline{\widehat{f}_0(-m_1)} \overline{\widehat{f}_0(-n_1 + a)} \widehat{f}_0(-m_1 + a)|^2 \right)^{1/8} \\
& \quad \left(\sum_{n_1, m_1, a, b, b'} K(n_1 - b, b) \overline{K(m_1 - b, b)} \overline{K(n_1 - b, b - a)} K(m_1 - b, b - a) \right. \\
& \quad \left. \overline{K(n_1 - b', b')} K(m_1 - b', b') K(n_1 - b', b' - a) \overline{K(m_1 - b', b' - a)} \right)^{1/8}.
\end{aligned} \tag{2.3.9}$$

We estimate the two sums above separately. First, note that

$$\begin{aligned}
& \sum_{n_1, m_1, a} |\widehat{f}_0(-n_1) \overline{\widehat{f}_0(-m_1)} \overline{\widehat{f}_0(-n_1 + a)} \widehat{f}_0(-m_1 + a)|^2 \\
& = \sum_{n_1, m_1} |\widehat{f}_0(-n_1) \overline{\widehat{f}_0(-m_1)}|^2 \sum_a |\widehat{f}_0(-n_1 + a) \overline{\widehat{f}_0(-m_1 + a)}|^2 \\
& \leq \sum_{n_1, m_1} |\widehat{f}_0(-n_1) \overline{\widehat{f}_0(-m_1)}|^2 \|\widehat{f}_0\|_{l^4}^4 \\
& = \|f_0\|_2^4 \|\widehat{f}_0\|_{l^4}^4
\end{aligned} \tag{2.3.10}$$

where the second to last line follows from the Cauchy–Schwarz inequality. Next, note that

$$\begin{aligned}
& \sum_{n_1, m_1, a, b, b'} K(n_1 - b, b) \overline{K}(m_1 - b, b) \overline{K}(n_1 - b, b - a) K(m_1 - b, b - a) \\
& \quad \overline{K}(n_1 - b', b') K(m_1 - b', b') K(n_1 - b', b' - a) \overline{K}(m_1 - b', b' - a) \\
&= \frac{1}{p^8} \sum_{\substack{n_1, m_1, a \\ b, b'}} \sum_{\substack{y_1, y_2, y_3, y_4 \\ y_5, y_6, y_7, y_8}} \\
& \quad e_p(((n_1 - b)F(y_1) + bG(y_1)) - ((m_1 - b)F(y_2) + bG(y_2)) \\
& \quad - ((n_1 - b)F(y_3) + (b - a)G(y_3)) + ((m_1 - b)F(y_4) + (b - a)G(y_4)) \\
& \quad - ((n_1 - b')F(y_5) + b'G(y_5)) + ((m_1 - b')F(y_6) + b'G(y_6)) \\
& \quad + ((n_1 - b')F(y_7) + (b' - a)G(y_7)) - ((m_1 - b')F(y_8) + (b' - a)G(y_8))).
\end{aligned}$$

This is equal to

$$\begin{aligned}
& \frac{1}{p^8} \sum_{\substack{y_1, y_2, y_3, y_4 \\ y_5, y_6, y_7, y_8}} \sum_{\substack{n_1, m_1, a \\ b, b'}} \\
& \quad e_p(b(-F(y_1) + G(y_1) + F(y_2) - G(y_2) + F(y_3) - G(y_3) - F(y_4) + G(y_4)) \\
& \quad + b'(F(y_5) - G(y_5) - F(y_6) + G(y_6) - F(y_7) + G(y_7) + F(y_8) - G(y_8)) \\
& \quad + n_1(F(y_1) - F(y_3) - F(y_5) + F(y_7)) \\
& \quad + m_1(-F(y_2) + F(y_4) + F(y_6) - F(y_8)) \\
& \quad + a(G(y_3) - G(y_4) - G(y_7) + G(y_8))) \\
&= \frac{1}{p^8} \sum_{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in Y(\mathbb{F}_p)} p^5 \\
&= \frac{1}{p^3} |Y(\mathbb{F}_p)|
\end{aligned} \tag{2.3.11}$$

where the second to last equality follows from the orthogonality of the characters. Combining inequalities (2.3.9), (2.3.10) and (2.3.11) completes the proof. $\square$

Remark 2.3.3. In the proof of Theorem 2.3.2, if we were to only apply Cauchy–Schwarz inequality two times and stop at (2.3.8), then we could formulate an alternative approach

to Theorem 1.2.5, conditionally on the estimates of multidimensional exponential sums on varieties with rational function phases, which is highly nontrivial and out of reach of the current arithmetic geometry methods.

2.4 Dimension estimates

In Section 2.3, we establish a Gowers norm control, conditionally on estimating the size of the $\mathbb{F}_p$ -points of the Roth variety. We will prove the required estimates in Theorem 2.4.1, completing the algebraic geometry PET induction. The Roth variety is the solutions to five equations in eight-dimensional affine space, intuitively, when the five defining equations are “sufficiently independent”, the expected dimension of the Roth variety is $8 - 5 = 3$ and hence the size is around p^3 .

The proof of Theorem 2.4.1 is quite long and technical, hence we would like to briefly describe the strategy first. We would decompose the Roth variety Y into five pieces $Y = Y_{\text{gen}} \cup Y_{\text{low}} \cup Z_{\text{good}} \cup Z_{\text{bad}} \cup Z_{\text{low}}$ and estimate via different techniques. The variety Y_{gen} is a generic part of Y , which can be handled by complex analytic techniques. The variety Z_{good} is a generic component of a special subvariety of Y , which can be handled by complex analytic techniques too. On the other hand, the variety Z_{bad} is a special subvariety with extra constraints and special structures, hence we have extra inputs for mod p point counting. Finally, the varieties Y_{low} and Z_{low} are of lower dimension; therefore, we can control them more easily.

Theorem 2.4.1. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$, and $Y(\mathbb{F}_p)$ be the $\mathbb{F}_p$ -points of the Roth variety associated to $F(t), G(t)$. Then, we have the following point counting estimates:*

$$|Y(\mathbb{F}_p)| \ll p^3.$$

Proof. We would decompose $Y(\mathbb{F}_p)$ into various parts and estimate via different techniques accordingly. First, note that the first five columns of the Jacobian matrix of the defining equations (2.3.1), (2.3.2), (2.3.3), (2.3.4), (2.3.5) of the Roth variety are

$$\begin{bmatrix} F'(y_1) - G'(y_1) & -F'(y_2) + G'(y_2) & -F'(y_3) + G'(y_3) & F'(y_4) - G'(y_4) & 0 \\ 0 & 0 & 0 & 0 & F'(y_5) - G'(y_5) \\ F'(y_1) & 0 & -F'(y_3) & 0 & -F'(y_5) \\ 0 & F'(y_2) & 0 & -F'(y_4) & 0 \\ 0 & 0 & G'(y_3) & -G'(y_4) & 0 \end{bmatrix}.$$

Let $D(y_1, y_2, y_3, y_4, y_5)$ be the determinant of the matrix, that is,

$$(G'(y_5) - F'(y_5)) \begin{vmatrix} F'(y_1) - G'(y_1) & -F'(y_2) + G'(y_2) & -F'(y_3) + G'(y_3) & F'(y_4) - G'(y_4) \\ F'(y_1) & 0 & -F'(y_3) & 0 \\ 0 & F'(y_2) & 0 & -F'(y_4) \\ 0 & 0 & G'(y_3) & -G'(y_4) \end{vmatrix}$$

which is equal to

$$(G'(y_5) - F'(y_5)) \begin{vmatrix} -G'(y_1) & G'(y_2) & 0 & 0 \\ F'(y_1) & 0 & -F'(y_3) & 0 \\ 0 & F'(y_2) & 0 & -F'(y_4) \\ 0 & 0 & G'(y_3) & -G'(y_4) \end{vmatrix}.$$

Hence, we have

$$D(y_1, y_2, y_3, y_4, y_5) = (G'(y_5) - F'(y_5)) \left[G'(y_1)F'(y_2)F'(y_3)G'(y_4) - F'(y_1)G'(y_2)G'(y_3)F'(y_4) \right].$$

Define

$$Y_{\text{gen}} = Y \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : D(y_1, y_2, y_3, y_4, y_5) \neq 0\}$$

and

$$Y_{\text{sp}} = Y \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : D(y_1, y_2, y_3, y_4, y_5) = 0\}.$$

It makes sense to define Y_{gen} and Y_{sp} over any fields, hence the specific field is not mentioned in the definitions, and it would be convenient to work over various fields. Note that we have $Y(\mathbb{F}_p) = Y_{\text{gen}}(\mathbb{F}_p) \cup Y_{\text{sp}}(\mathbb{F}_p)$. Informally, the variety Y_{gen} is a generic part of Y which lies in the smooth component of Y , and Y_{sp} is a special subvariety of Y cut out by $D(y_1, y_2, y_3, y_4, y_5)$. As a side note, the variety Y_{gen} is empty when F, G and constant function 1 are linearly dependent.

The associated complex analytic space of $Y_{\text{gen}}(\mathbb{C})$ is a 3-dimensional complex manifold since the Jacobian matrices have full rank and we can apply the implicit function theorem. By Noether normalization, there exists a finite surjective map $Y_{\text{gen}}(\mathbb{C}) \longrightarrow \mathbb{A}^d(\mathbb{C})$ between varieties, where d is the dimension of $Y_{\text{gen}}(\mathbb{C})$ as a variety and $\mathbb{A}^d$ is the d -dimensional affine space. Regard the map $Y_{\text{gen}}(\mathbb{C}) \longrightarrow \mathbb{A}^d(\mathbb{C})$ as a finite holomorphic map between complex manifolds. By the first theorem in [GR84, Chapter 5, Section 4.1], we deduce that the dimension of $Y_{\text{gen}}(\mathbb{C})$ as a variety is 3. (We compare the dimension of a variety over $\mathbb{C}$ and the dimension of its associated complex analytic space via *ad hoc* argument here, for general dimension theory of complex analytic spaces, see [Har77, Appendix B] and [GR84, Chapter 5, Section 1].)

Consider an affine $\mathbb{Z}$ -model of $Y_{\text{gen}}(\mathbb{C})$ by clearing out the denominators in the defining equations of the Roth variety and adding one auxiliary variable z and one equation to require that the denominators are nonzero. To be more specific, write $F(t) = a(t)/b(t)$ and $G(t) = c(t)/d(t)$ with $a(t), b(t), c(t), d(t) \in \mathbb{Z}[t]$, let $I \subset \mathbb{Z}[y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, z]$ be the

ideal generated by the following polynomials:

$$\left(\prod_{i=1}^4 b(y_i)d(y_i)\right)\left(F(y_1) - G(y_1) - F(y_2) + G(y_2) - F(y_3) + G(y_3) + F(y_4) - G(y_4)\right) \quad (2.4.1)$$

$$\left(\prod_{i=5}^8 b(y_i)d(y_i)\right)\left(F(y_5) - G(y_5) - F(y_6) + G(y_6) - F(y_7) + G(y_7) + F(y_8) - G(y_8)\right) \quad (2.4.2)$$

$$\left(b(y_1)b(y_3)b(y_5)b(y_7)\right)\left(F(y_1) - F(y_3) - F(y_5) + F(y_7)\right) \quad (2.4.3)$$

$$\left(b(y_2)b(y_4)b(y_6)b(y_8)\right)\left(F(y_2) - F(y_4) - F(y_6) + F(y_8)\right) \quad (2.4.4)$$

$$\left(d(y_3)d(y_4)d(y_7)d(y_8)\right)\left(G(y_3) - G(y_4) - G(y_7) + G(y_8)\right) \quad (2.4.5)$$

$$z\left(\prod_{i=1}^8 b(y_i)d(y_i)\right)\left[\left(\prod_{i=1}^5 b(y_i)d(y_i)\right)^2 D(y_1, y_2, y_3, y_4, y_5)\right] - 1. \quad (2.4.6)$$

The polynomials (2.4.1), (2.4.2), (2.4.3), (2.4.4) and (2.4.5) are the denominator free version of the defining equations of the Roth variety. Including polynomial (2.4.6) is a localization trick in algebraic geometry; it ensures $D(y_1, y_2, y_3, y_4, y_5)$ and the denominators of F and G are nonzero, but it does not impose any unwanted constraints since the auxiliary variable z is uniquely determined by $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$.

Define affine $\mathbb{Z}$ -model $Y_{\text{gen}} = \text{Spec } \mathbb{Z}[y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, z]/I$. Note that the $\mathbb{C}$ -points of $Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{C}$ is isomorphic to $Y_{\text{gen}}(\mathbb{C})$, hence we have $\dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{C} = \dim_{\text{Var}} Y_{\text{gen}}(\mathbb{C}) = 3$. By [Har77, Chapter 2, Exercise 3.20.(f)], we have the invariance of dimension under base change, i.e., $\dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{Q} = \dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{C} = 3$. (Note that the integral assumption in [Har77, Chapter 2, Exercise 3.20.(f)] can be removed if one does not require the scheme after base change to be equidimensional.)

Note that the structure map $Y_{\text{gen}} = \text{Spec } \mathbb{Z}[y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, z]/I \longrightarrow \text{Spec } \mathbb{Z}$ is of finite type and the base $\text{Spec } \mathbb{Z}$ is irreducible, by [Sta23, Section 05F6, Lemma 37.30.1], we deduce that the dimension of the generic fiber is the same as mod p fibers for all but finitely many p , that is, $\dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{Q} = \dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{F}_p = 3$ for all but finitely many p . Once

again, by [Har77, Chapter 2, Exercise 3.20.(f)], we have $\dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \mathbb{F}_p = \dim_{\text{Sch}} Y_{\text{gen}} \times_{\mathbb{Z}} \overline{\mathbb{F}}_p$. Hence, we have $\dim_{\text{Var}} Y_{\text{gen}}(\overline{\mathbb{F}}_p) = 3$ for all but finitely many p . Now, the Lang-Weil bound [LW54] (also see [Tao23, Lemma 1]) implies that $|Y_{\text{gen}}(\mathbb{F}_p)| \ll p^3$. (Note that one does not need the irreducibility of the variety.)

(As a side note, we pass to complex numbers since it is convenient to work with algebraic geometry over characteristic zero and rational functions over complex numbers. That being said, the machinery of algebraic geometry is robust enough for one to only work over finite fields. Therefore, the approach we chose is just one possible way to proceed.)

Next, we would like to bound the size of $Y_{\text{sp}}(\mathbb{F}_p)$. Although Y_{sp} already has more constraints than Y , but we will further decompose Y_{sp} so that we have constraint which depends on sufficiently few variables. Let $\tilde{D}(y_1, y_2, y_3, y_4)$ denote the function

$$\frac{D(y_1, y_2, y_3, y_4, y_5)}{F'(y_1)F'(y_2)F'(y_3)F'(y_4)(G'(y_5) - F'(y_5))} = \frac{G'(y_1)G'(y_4)}{F'(y_1)F'(y_4)} - \frac{G'(y_2)G'(y_3)}{F'(y_2)F'(y_3)}.$$

Define

$$Y_{\text{low}} = Y_{\text{sp}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : F'(y_1)F'(y_2)F'(y_3)F'(y_4)(G'(y_5) - F'(y_5)) = 0\}$$

and

$$Z = Y_{\text{sp}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : \tilde{D}(y_1, y_2, y_3, y_4) = 0\}.$$

Note that we have $Y_{\text{sp}}(\mathbb{F}_p) = Y_{\text{low}}(\mathbb{F}_p) \cup Z(\mathbb{F}_p)$. Informally, the variety $Y_{\text{low}}(\mathbb{F}_p)$ has strong constraint $F'(y_1)F'(y_2)F'(y_3)F'(y_4)(G'(y_5) - F'(y_5)) = 0$, hence this lower dimensional contribution can be bounded more easily later. We would like to further decompose $Z(\mathbb{F}_p)$. To do so, consider the Jacobian matrix of the following equations:

$$\begin{aligned} F(y_1) - G(y_1) - F(y_2) + G(y_2) - F(y_3) + G(y_3) + F(y_4) - G(y_4) &= 0 \\ \tilde{D}(y_1, y_2, y_3, y_4) &= 0, \end{aligned}$$

which is

$$\begin{bmatrix} F'(y_1) - G'(y_1) & -F'(y_2) + G'(y_2) & -F'(y_3) + G'(y_3) & F'(y_4) - G'(y_4) \\ \frac{G'(y_4)}{F'(y_4)} \left(\frac{G'(y_1)}{F'(y_1)} \right)' & -\frac{G'(y_3)}{F'(y_3)} \left(\frac{G'(y_2)}{F'(y_2)} \right)' & -\frac{G'(y_2)}{F'(y_2)} \left(\frac{G'(y_3)}{F'(y_3)} \right)' & \frac{G'(y_1)}{F'(y_1)} \left(\frac{G'(y_4)}{F'(y_4)} \right)' \end{bmatrix}.$$

Let $E(y_1, y_4)$ be the determinant of the minor matrix of the Jacobian matrix consisting of the first column and fourth column, i.e.

$$E(y_1, y_4) = \begin{vmatrix} F'(y_1) - G'(y_1) & F'(y_4) - G'(y_4) \\ \frac{G'(y_4)}{F'(y_4)} \left(\frac{G'(y_1)}{F'(y_1)} \right)' & \frac{G'(y_1)}{F'(y_1)} \left(\frac{G'(y_4)}{F'(y_4)} \right)' \end{vmatrix}$$

which is

$$(F'(y_1) - G'(y_1)) \frac{G'(y_1)}{F'(y_1)} \left(\frac{G'(y_4)}{F'(y_4)} \right)' - (F'(y_4) - G'(y_4)) \frac{G'(y_4)}{F'(y_4)} \left(\frac{G'(y_1)}{F'(y_1)} \right)'.$$

Also, let $\tilde{E}(y_1, y_4)$ denote the function

$$\frac{E(y_1, y_4)}{\left(\frac{G'(y_1)}{F'(y_1)} \right)' \left(\frac{G'(y_4)}{F'(y_4)} \right)'} = \frac{(F'(y_1) - G'(y_1)) \frac{G'(y_1)}{F'(y_1)}}{\left(\frac{G'(y_1)}{F'(y_1)} \right)'} - \frac{(F'(y_4) - G'(y_4)) \frac{G'(y_4)}{F'(y_4)}}{\left(\frac{G'(y_4)}{F'(y_4)} \right)'}$$

Define

$$Z_{good} = Z \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : E(y_1, y_4) \neq 0\},$$

$$Z_{bad} = Z \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : \tilde{E}(y_1, y_4) = 0\}$$

and

$$Z_{low} = Z \cap \left\{ (y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : \left(\frac{G'(y_1)}{F'(y_1)} \right)' \left(\frac{G'(y_4)}{F'(y_4)} \right)' = 0 \right\}.$$

Note that we have $Z(\mathbb{F}_p) = Z_{good}(\mathbb{F}_p) \cup Z_{bad}(\mathbb{F}_p) \cup Z_{low}(\mathbb{F}_p)$. Informally, the variety $Z_{good}(\mathbb{F}_p)$ is a generic part of $Z(\mathbb{F}_p)$ which satisfies good property, the variety $Z_{bad}(\mathbb{F}_p)$ is a special subvariety cut out by $\tilde{E}(y_1, y_4) = 0$, and $Z_{low}(\mathbb{F}_p)$ is a lower dimensional contribution. It remains to bound $|Z_{good}(\mathbb{F}_p)|$, $|Z_{bad}(\mathbb{F}_p)|$, $|Z_{low}(\mathbb{F}_p)|$ and $|Y_{low}(\mathbb{F}_p)|$.

We start with bounding $|Z_{\text{good}}(\mathbb{F}_p)|$. Consider the auxiliary variety $X \subset \mathbb{A}^4$ defined by the following equations

$$F(y_1) - G(y_1) - F(y_2) + G(y_2) - F(y_3) + G(y_3) + F(y_4) - G(y_4) = 0 \quad (2.4.7)$$

$$\tilde{D}(y_1, y_2, y_3, y_4) = 0 \quad (2.4.8)$$

$$E(y_1, y_4) \neq 0. \quad (2.4.9)$$

The associated complex analytic space of $X(\mathbb{C})$ is a 2-dimensional complex manifold since the condition $E(y_1, y_4) \neq 0$ guarantees that the Jacobian matrices of the equations (2.4.7), (2.4.8) have full rank and we can apply the implicit function theorem. Similar to the dimension comparison between $Y_{\text{gen}}(\mathbb{C})$ and its associated complex analytic space, this implies that the dimension of $X(\mathbb{C})$ as a variety is 2. Moreover, similar to the previous arguments regarding Y_{gen} , we conclude that $|X(\mathbb{F}_p)| \ll p^2$.

For all points $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in Z_{\text{good}}(\mathbb{F}_p)$, the coordinates (y_1, y_2, y_3, y_4) lie on $X(\mathbb{F}_p)$, hence there are at most $O(p^2)$ choices of y_1, y_2, y_3, y_4 . Besides, there are at most p choices of y_5 , hence there are at most $O(p^3)$ choices of y_1, y_2, y_3, y_4, y_5 . For any given y_1, y_2, y_3, y_4, y_5 , there are only $O(1)$ choices of y_7 by equation (2.3.3). For any given $y_1, y_2, y_3, y_4, y_5, y_7$, there are only $O(1)$ choices of y_8 by equation (2.3.5). For any given $y_1, y_2, y_3, y_4, y_5, y_7, y_8$, there are only $O(1)$ choices of y_6 by equation (2.3.4). Therefore, we have $|Z_{\text{good}}(\mathbb{F}_p)| \ll p^3$. (Heuristically, the system of equations becomes "triangular" after choosing a certain subset of variables.)

Next, we turn our attention to bounding $|Z_{\text{bad}}(\mathbb{F}_p)|$. We would first show that the equation $\tilde{E}(y_1, y_4) = 0$ is a nontrivial constraint by showing

$$\frac{(F'(y_1) - G'(y_1)) \frac{G'(y_1)}{F'(y_1)}}{\left(\frac{G'(y_1)}{F'(y_1)}\right)'} \quad (2.4.10)$$

is nonconstant. Suppose the rational function (2.4.10) is a constant, then we have

$$c \left(\frac{G'(y_1)}{F'(y_1)} \right)' = (F'(y_1) - G'(y_1)) \frac{G'(y_1)}{F'(y_1)}$$

for some constant c . If $c = 0$, then we have $F'(y_1) - G'(y_1) = 0$ or $G'(y_1)/F'(y_1) = 0$, which both contradict the linear independence of F, G and the constant function 1. If $c \neq 0$, then we have

$$\left(\frac{G'(y_1)}{F'(y_1)} \right)' - \frac{F'(y_1) - G'(y_1)}{c} \frac{G'(y_1)}{F'(y_1)} = 0. \quad (2.4.11)$$

The equation (2.4.11) can be regarded as a first order linear ODE, where the unknown function is $G'(y_1)/F'(y_1)$. Multiplying integrating factor to equation (2.4.11), we have

$$\left[\exp \left(-\frac{F(y_1) - G(y_1)}{c} \right) \frac{G'(y_1)}{F'(y_1)} \right]' = 0. \quad (2.4.12)$$

Integrating the equation (2.4.12), we deduce that

$$\exp \left(-\frac{F(y_1) - G(y_1)}{c} \right) \frac{G'(y_1)}{F'(y_1)} = \tilde{c} \quad (2.4.13)$$

for some constant $\tilde{c}$. Since $G'(y_1)/F'(y_1)$ and $(F(y_1) - G(y_1))/c$ are both rational functions, the equation (2.4.13) implies that $G'(y_1)/F'(y_1) = 0$ or $(F(y_1) - G(y_1))/c$ is a constant. However, the conclusions that $G'(y_1)/F'(y_1) = 0$ or $(F(y_1) - G(y_1))/c$ is a constant contradict with the linear independence of F, G and the constant function 1. Hence, the rational function (2.4.10) is not a constant.

Now, for all points $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in Z_{\text{bad}}(\mathbb{F}_p)$, the coordinates y_2, y_4, y_5 have at most p^3 choices. For any given y_2, y_4, y_5 , there are at most $O(1)$ choices of y_1 by equation $\tilde{E}(y_1, y_4) = 0$. (Note that we use the fact that $\tilde{E}(y_1, y_4)$ is a difference of a nonconstant rational function in y_1 and a nonconstant rational function in y_4 , so it is crucial to have the linear independence of F, G and constant function 1 here.) For any given y_1, y_2, y_4, y_5 , there are at most $O(1)$ choices of y_3 by equation (2.3.1). For any given y_1, y_2, y_3, y_4, y_5 , there are at most $O(1)$ choices of y_7 by equation (2.3.3). For any given $y_1, y_2, y_3, y_4, y_5, y_7$, there are at most $O(1)$ choices of y_8 by equation (2.3.5). For any given $y_1, y_2, y_3, y_4, y_5, y_7, y_8$, there are

at most $O(1)$ choices of y_6 by equation (2.3.4). Therefore, we have $|Z_{\text{bad}}(\mathbb{F}_p)| \ll p^3$.

Finally, we estimate $|Y_{\text{low}}(\mathbb{F}_p)|$ and $|Z_{\text{low}}(\mathbb{F}_p)|$. These varieties have strong constraints which allow us to bound their cardinality more easily. We first decompose $Y_{\text{low}}(\mathbb{F}_p)$. Define

$$Y_{\text{low}}^{(1)} = Y_{\text{low}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : F'(y_1) = 0\},$$

$$Y_{\text{low}}^{(2)} = Y_{\text{low}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : F'(y_2) = 0\},$$

$$Y_{\text{low}}^{(3)} = Y_{\text{low}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : F'(y_3) = 0\},$$

$$Y_{\text{low}}^{(4)} = Y_{\text{low}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : F'(y_4) = 0\}$$

and

$$Y_{\text{low}}^{(5)} = Y_{\text{low}} \cap \{(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in \mathbb{A}^8 : (G'(y_5) - F'(y_5)) = 0\}.$$

When F is linear, the varieties $Y_{\text{low}}^{(1)}, Y_{\text{low}}^{(2)}, Y_{\text{low}}^{(3)}$ and $Y_{\text{low}}^{(4)}$ are empty, however, this situation would only help us since we are upper bounding the size of the varieties. Hence, without loss of generality, we may assume F is nonlinear.

Note that we have $Y_{\text{low}}(\mathbb{F}_p) = Y_{\text{low}}^{(1)}(\mathbb{F}_p) \cup Y_{\text{low}}^{(2)}(\mathbb{F}_p) \cup Y_{\text{low}}^{(3)}(\mathbb{F}_p) \cup Y_{\text{low}}^{(4)}(\mathbb{F}_p) \cup Y_{\text{low}}^{(5)}(\mathbb{F}_p)$. For all $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8) \in Y_{\text{low}}^{(1)}(\mathbb{F}_p)$, the coordinates y_2, y_4, y_5 have at most p^3 choices. For any given y_2, y_4, y_5 , there are at most $O(1)$ choices of y_1 by equation $F'(y_1) = 0$. For any given y_1, y_2, y_4, y_5 , there are at most $O(1)$ choices of y_3 by equation (2.3.1). For any given y_1, y_2, y_3, y_4, y_5 , there are at most $O(1)$ choices of y_7 by equation (2.3.3). For any given $y_1, y_2, y_3, y_4, y_5, y_7$, there are at most $O(1)$ choices of y_8 by equation (2.3.5). For any given $y_1, y_2, y_3, y_4, y_5, y_7, y_8$, there are at most $O(1)$ choices of y_6 by equation (2.3.4). Therefore, we have $|Y_{\text{low}}^{(1)}(\mathbb{F}_p)| \ll p^3$. Similarly, we have $|Y_{\text{low}}^{(2)}(\mathbb{F}_p)|, |Y_{\text{low}}^{(3)}(\mathbb{F}_p)|, |Y_{\text{low}}^{(4)}(\mathbb{F}_p)|, |Y_{\text{low}}^{(5)}(\mathbb{F}_p)| \ll p^3$ and hence $|Y_{\text{low}}(\mathbb{F}_p)| \ll p^3$. A similar decomposing and counting argument would show that $|Z_{\text{low}}(\mathbb{F}_p)| \ll p^3$ too. This completes the proof. $\square$

2.5 Final arguments

In this section, we would put everything together to complete the proof of Theorem 1.2.5. After establishing Gowers norm control, we could immediately run the degree lowering arguments [Pel19]. In fact, since we obtain a U^2 -Gowers norm control, we would perform a Fourier level set decomposition of the functions to get a better exponent.

We first start with the case of two term rational function progressions, which serves as the base case of the induction. As observed by Peluse [Pel19], one should consider the counting operator twisted by the characters for the purpose of induction. The proof of Proposition 2.5.1 is essentially the same as [Pel19, Lemma 3.2], except that we apply Bombieri's bound instead of Weil's bound. Denote the characteristic function by $1_{\xi=0}$, that is, $1_{\xi=0} = 1$ when $\xi = 0$ and $1_{\xi=0} = 0$ when $\xi \neq 0$.

Proposition 2.5.1. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$. Then, we have the asymptotic formula*

$$\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) e_p(\xi G(y)) = 1_{\xi=0} \prod_{i=0}^1 \mathbb{E}_z f_i(z) + O_{F,G}(p^{-1/2} \|f_0\|_2 \|f_1\|_2)$$

for all functions $f_0, f_1 : \mathbb{F}_p \rightarrow \mathbb{C}$ and $\xi \in \mathbb{F}_p$.

Before we start the proof of Proposition 2.5.1, we recall the following Bombieri's bound on single variable exponential sums in finite fields with rational function phases [Bom66] (also see [BC17, Proposition 2.2]).

Lemma 2.5.2 (Bombieri [Bom66]). *Let $F(t) \in \mathbb{Q}(t)$ be a rational function such that it is nonconstant mod p , then we have*

$$|\mathbb{E}_y e_p(F(y))| \ll p^{-1/2},$$

where the implied constant only depends on the zeroes and poles of $F(t)$.

Proof of Proposition 2.5.1. Fourier expand the functions f_0, f_1 to obtain

$$\begin{aligned}
& \mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) e_p(\xi G(y)) \\
&= \mathbb{E}_{x,y} \sum_{n_0, n_1} \widehat{f}_0(n_0) \widehat{f}_1(n_1) e_p(n_0 x + n_1 x) e_p(n_1 F(y) + \xi G(y)) \\
&= \sum_{n_1} \widehat{f}_0(-n_1) \widehat{f}_1(n_1) \mathbb{E}_y e_p(n_1 F(y) + \xi G(y)).
\end{aligned}$$

By linear independence of F, G and the constant function 1, the function $n_1 F(y) + \xi G(y)$ is nonconstant unless $n_1 = \xi = 0$. When $n_1 \neq 0$ or $\xi \neq 0$, we have Lemma 2.5.2, i.e., Bombieri's bound on single variable exponential sums in finite fields with rational function phases, that is,

$$|\mathbb{E}_y e_p(n_1 F(y) + \xi G(y))| \ll p^{-1/2}.$$

Combining Bombieri's bound, the Cauchy–Schwarz inequality and Parseval's identity, we have

$$\left| \sum_{n_1 \neq 0} \widehat{f}_0(-n_1) \widehat{f}_1(n_1) \mathbb{E}_y e_p(n_1 F(y) + \xi G(y)) \right| \ll p^{-1/2} \|f_0\|_2 \|f_1\|_2.$$

Note that the main term comes from the term with $n_1 = 0$, that is,

$$\widehat{f}_0(0) \widehat{f}_1(0) \mathbb{E}_y e_p(\xi G(y)) = 1_{\xi=0} \prod_{i=0}^1 \mathbb{E}_z f_i(z) + O(p^{-1/2} \|f_0\|_2 \|f_1\|_2).$$

This completes the proof. □

Next, we show that the counting operator can be controlled by the dual function.

Proposition 2.5.3. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ and $f_0, f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$ be functions. Define the dual function $\mathcal{D} = \mathcal{D}_{f_1, f_2}$ by*

$$\mathcal{D}(x) = \mathbb{E}_y f_1(x + F(y)) f_2(x + G(y)).$$

Then, we have

$$|\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y))| \leq \|\widehat{f}_0\|_{l^1} \|\widehat{\mathcal{D}}\|_{l^\infty}.$$

Proof. By the definition of dual function and Parseval's identity, we have

$$|\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y))| = |\mathbb{E}_x f_0(x) \mathcal{D}(x)| = \left| \sum_m \widehat{f}_0(-m) \widehat{\mathcal{D}}(m) \right|,$$

which is bounded by $\|\widehat{f}_0\|_{l^1} \|\widehat{\mathcal{D}}\|_{l^\infty}$ by applying Hölder's inequality. $\square$

The following proposition says that the dual function is controlled by shorter progressions.

Proposition 2.5.4. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$, and $f_1, f_2 : \mathbb{F}_p \rightarrow \mathbb{C}$ be functions with $\mathbb{E}_z f_2(z) = 0$. Then, we have*

$$\|\widehat{\mathcal{D}}\|_{l^\infty} \ll p^{-1/2} \|f_1\|_2 \|f_2\|_2.$$

(Recall that the dual function $\mathcal{D}$ is defined in Proposition 2.5.3.)

Proof. Note that

$$\begin{aligned} \widehat{\mathcal{D}}(\xi) &= \mathbb{E}_x \mathbb{E}_y f_1(x + F(y)) f_2(x + G(y)) e_p(-x\xi) \\ &= \mathbb{E}_{x,y} f_1(x) e_p(-x\xi) f_2(x + G(y) - F(y)) e_p(\xi F(y)). \end{aligned}$$

To finish the proof, apply Proposition 2.5.1 and note that the main term is 0 due to the assumption $\mathbb{E}_z f_2(z) = 0$. $\square$

Finally, we have all the ingredients to finish the proof of Theorem 1.2.5.

Proof of Theorem 1.2.5. We will use convenient notation $\Lambda_{F,G}(f_0, f_1, f_2)$ to denote the counting operator $\mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) f_2(x + G(y))$. First, we start with a preliminary reduction. Let $f'_2 = f_2 - \mathbb{E}_z f_2(z)$ be the balanced version of the function f_2 , so that the mean of f'_2 is 0. Note that we have

$$\begin{aligned} \Lambda_{F,G}(f_0, f_1, f_2) &= \Lambda_{F,G}(f_0, f_1, \mathbb{E}_z f_2(z)) + \Lambda_{F,G}(f_0, f_1, f'_2) \\ &= \left(\mathbb{E}_z f_2(z) \right) \mathbb{E}_{x,y} f_0(x) f_1(x + F(y)) + \Lambda_{F,G}(f_0, f_1, f'_2) \\ &= \prod_{i=0}^2 \mathbb{E}_z f_i(z) + O(p^{-1/2} \|f_0\|_2 \|f_1\|_2 \|f_2\|_2) + \Lambda_{F,G}(f_0, f_1, f'_2), \end{aligned}$$

where the last equality follows from Proposition 2.5.1. It remains to bound $\Lambda_{F,G}(f_0, f_1, f'_2)$.

Next, we would construct a Fourier level set decomposition of f_0 . Let $\varepsilon > 0$ be a parameter to be chosen later, define g, h by setting their Fourier transforms

$$\widehat{g}(\xi) = \begin{cases} \widehat{f}_0(\xi), & |\widehat{f}_0(\xi)| > \frac{\|f_0\|_2}{\varepsilon p^{1/2}} \\ 0, & \text{otherwise} \end{cases}$$

and

$$\widehat{h}(\xi) = \begin{cases} \widehat{f}_0(\xi), & |\widehat{f}_0(\xi)| \leq \frac{\|f_0\|_2}{\varepsilon p^{1/2}} \\ 0, & \text{otherwise} \end{cases}.$$

Note that we have $\widehat{f}_0 = \widehat{g} + \widehat{h}$. By Parseval's identity, we have l^2 -bounds $\|\widehat{g}\|_{l^2} \leq \|f_0\|_2$ and $\|\widehat{h}\|_{l^2} \leq \|f_0\|_2$. Moreover, we have good l^1 -bound for $\widehat{g}$, that is,

$$\|\widehat{g}\|_{l^1} = \sum_{\xi} |\widehat{g}(\xi)| \leq \sum_{\xi} |\widehat{g}(\xi)| \cdot |\widehat{f}_0(\xi)| \left(\frac{\|f_0\|_2}{\varepsilon p^{1/2}} \right)^{-1} \leq \varepsilon p^{1/2} \|f_0\|_2.$$

Furthermore, we have good l^4 -bound for $\widehat{h}$, that is,

$$\|\widehat{h}\|_{l^4} \leq \|\widehat{h}\|_{l^\infty}^{1/2} \|\widehat{h}\|_{l^2}^{1/2} \leq \left(\frac{\|f_0\|_2}{\varepsilon p^{1/2}} \right)^{1/2} \|\widehat{h}\|_{l^2}^{1/2} \leq \varepsilon^{-1/2} p^{-1/4} \|f_0\|_2.$$

Note that we can decompose $f_0 = g + h$ by Fourier inversion.

To finish the proof, we would use dual function control to bound $\Lambda_{F,G}(g, f_1, f'_2)$ and algebraic geometry PET induction to bound $\Lambda_{F,G}(h, f_1, f'_2)$. By Proposition 2.5.3, Proposition 2.5.4 and the l^1 -bound for $\widehat{g}$, we have

$$|\Lambda_{F,G}(g, f_1, f'_2)| \leq \|\widehat{g}\|_{l^1} \|\widehat{\mathcal{D}}\|_{l^\infty} \ll p^{-1/2} \|\widehat{g}\|_{l^1} \|f_1\|_2 \|f_2\|_2 \leq \varepsilon \|f_0\|_2 \|f_1\|_2 \|f_2\|_2.$$

By Theorem 2.3.2, Theorem 2.4.1 and the l^4 -bound for $\widehat{h}$, we have

$$|\Lambda_{F,G}(h, f_1, f'_2)| \ll \|h\|_2^{1/2} \|\widehat{h}\|_{l^4}^{1/2} \|f_1\|_2 \|f_2\|_2 \leq \varepsilon^{-1/4} p^{-1/8} \|f_0\|_2 \|f_1\|_2 \|f_2\|_2.$$

Hence, we have

$$\begin{aligned}\Lambda_{F,G}(f_0, f_1, f'_2) &= \Lambda_{F,G}(g, f_1, f'_2) + \Lambda_{F,G}(h, f_1, f'_2) \\ &\ll \varepsilon \|f_0\|_2 \|f_1\|_2 \|f_2\|_2 + \varepsilon^{-1/4} p^{-1/8} \|f_0\|_2 \|f_1\|_2 \|f_2\|_2.\end{aligned}$$

Choosing $\varepsilon = p^{-1/10}$ will optimize the result and complete the proof. □

CHAPTER 3

Two dimensional rational function corners

3.1 Overview

In this chapter, we follow the strategy from [Lim25b] to reproduce a proof of Theorem 1.3.2.

Bergelson and Leibman's theorem (Theorem 1.2.1) provides a satisfactory qualitative understanding of the sets that do not contain polynomial progressions. Meanwhile, the quantitative understanding of this subject is still formative. Recent breakthroughs of Peluse [Pel19], [Pel20] and of Peluse and Prendiville [PP24] bring major progress on quantitative estimates for sets lacking one dimensional polynomial progressions, but the theory for higher dimensional polynomial progressions is far from complete.

There are significant new difficulties for higher dimensional progressions, which could be found in Peluse's paper on L-shaped configurations [Pel24]. Further evidence regarding high dimensional difficulties are recorded in Austin's work [Aus14].

In this chapter, we discuss the two dimensional rational function corners in $\mathbb{F}_p^2$. Let F, G be rational functions, to specific the dependency, we will call the two dimensional rational function corners $(x_1, x_2), (x_1 + F(y), x_2), (x_1, x_2 + G(y))$ *corners generated by F, G* .

Two dimensional rational function corners include a wide range of examples. For instance, two dimensional rational function corners include

$$(x_1, x_2), (x_1 + y, x_2), (x_1, x_2 + y^2)$$

and

$$(x_1, x_2), (x_1 + y^3, x_2), (x_1, x_2 + y^3 - y^2 + y)$$

and even strange examples like

$$(x_1, x_2), \left(x_1 + \frac{y^2}{y^7 - 5y^3}, x_2\right), \left(x_1, x_2 + y^{17} + \frac{1}{y^{13} + 19}\right).$$

Compared to previous results, Theorem 1.3.2 and Theorem 1.3.4 are new in the following two aspects.

- Qualitatively, Theorem 1.3.2 and Theorem 1.3.4 allow F, G to be rational functions while the previous results are only applicable to polynomials.
- Quantitatively, the power-saving exponent $1/122880$ is an improvement upon previous results when F, G are polynomials and their degrees are the same and greater than 2. Moreover, the power-saving exponent $1/122880$ is uniform in the degrees of F, G ; it does not decay exponentially as the degrees grow.

To be more specific, previously Han, Lacey and Yang [HLY21] proved that if F, G are linearly independent polynomials with zero constant terms and **distinct** degree or linearly independent quadratic polynomials with zero constant terms, and A is a subset of $\mathbb{F}_p^2$ with density $\delta \gg p^{-1/16}$, then

$$\#\{(x_1, x_2, y) \in \mathbb{F}_p^3 : \text{The corner } (x_1, x_2), (x_1 + F(y), x_2), (x_1, x_2 + G(y)) \text{ is in } A\} \gg p^3 \delta^3.$$

On the other hand, Kuca [Kuc24b], [Kuc24a] proved that if F, G are linearly independent polynomials with zero constant terms, then there exists a constant c depending on the degrees of F, G such that

$$\#\{(x_1, x_2, y) \in \mathbb{F}_p^3 : \text{The corner } (x_1, x_2), (x_1 + F(y), x_2), (x_1, x_2 + G(y)) \text{ is in } A\} \gg p^3 \delta^3$$

for all subsets $A \subset \mathbb{F}_p^2$ with density $\delta \gg p^{-c}$. The method of Han, Lacey and Yang is Fourier analytic while the method of Kuca is based on higher order Fourier analysis and degree

lowering. The power-saving exponent c in Kuca's results is unspecified in his papers, but it could be made explicit in principle, although it would be fairly small due to the astronomical amount of application of the Cauchy–Schwarz inequality in degree lowering. For this same reason, the power-saving exponent c would also decay quite quickly as the degrees of F, G grow. Therefore, our power-saving exponent $1/122880$ is a uniform numerical improvement only in the cases not covered by the results of Han, Lacey and Yang.

The approach of [Lim25b] comes from four different papers [HLY21, HL25, KW24, Kuc24a]. To generalize the algebraic geometry PET induction to the case of corners, we incorporate the method with the Fourier analytic approach due to Han, Lacey and Yang [HLY21]. However, the “naive” generalization of algebraic geometry PET induction does not work, since it would discard too much cancellation among exponential sums, and lead to degeneracy of certain varieties. Luckily, we could borrow an idea from the work of Kavrut and Wu [KW24] on improving the nonlinear Roth theorem to amplify the cancellation among exponential sums and hence obtain Gowers norm control. After obtaining Gowers norm control, it is natural to apply the degree lowering pioneered by Peluse [Pel19] to complete the proof. In fact, we need a different version of degree lowering that works for directional Gowers norms, and this version of degree lowering was developed by Kuca [Kuc24a].

Finally, we briefly review the existing literature related to this chapter. To draw parallel comparisons, for polynomial Szemerédi theorem for corners in integers, see work of Peluse, Prendiville and Shao [PPS24] and work of Kravitz, Kuca and Leng [KKL24].

This chapter is organized as follows. Section 3.2 contains the convention we use. The main Fourier analytic calculations and intermediate inequalities for algebraic geometry PET induction are in Section 3.3. Section 3.4 is about point-counting on certain varieties. In Section 3.5, we use the results in Section 3.3 and Section 3.4 and the degree lowering to prove Theorem 1.3.2. We touch upon some potential higher dimensional generalizations in Section 3.6. Appendix 6.1 includes some further discussions on the technical aspects of Section 3.4.

3.2 Convention

We will continue to use the convention listed in Section 2.2. Moreover, we would use boldface letters to denote vectors in $\mathbb{F}_p^2$, for example $\mathbf{h}, \mathbf{n}, \mathbf{m}$ would mean $(h_1, h_2), (n_1, n_2), (m_1, m_2)$ respectively.

3.2.1 Gowers norm notation

Let G be a finite abelian group. Denote the difference operator by Δ , that is $\Delta_h g(x) = g(x)\bar{g}(x+h)$ for any functions g on G and any elements $h \in G$. Let s be a positive integer and $f : G \rightarrow \mathbb{C}$ be a function, the $U^s(G)$ -Gowers norm is defined to be

$$\|f\|_{U^s(G)}^{2^s} = \mathbb{E}_{x \in G} \mathbb{E}_{h_1, h_2, \dots, h_s \in G} \Delta_{h_1} \Delta_{h_2} \dots \Delta_{h_s} f(x).$$

More generally, let $H_1, H_2, \dots, H_s$ be subgroups of G , the Gowers box norm with respect to $H_1, H_2, \dots, H_s$ is defined to be

$$\|f\|_{H_1, H_2, \dots, H_s}^{2^s} = \mathbb{E}_{x \in G} \mathbb{E}_{h_1 \in H_1, h_2 \in H_2, \dots, h_s \in H_s} \Delta_{h_1} \Delta_{h_2} \dots \Delta_{h_s} f(x).$$

When $H = H_1 = H_2 = \dots = H_s$, we would write $\|f\|_{U^s(H)}$ for $\|f\|_{H_1, H_2, \dots, H_s}$.

Suppose $K_1, K_2, \dots, K_s$ are subgroups of $H_1, H_2, \dots, H_s$ respectively, then we have

$$\|f\|_{H_1, H_2, \dots, H_s} \leq \|f\|_{K_1, K_2, \dots, K_s}$$

for all functions f .

3.3 Algebraic geometry PET induction

In this section, we will establish the framework of algebraic geometry PET induction for two dimensional rational function corners. The main purpose is to upper bound the counting operator for corners generated by rational functions $F(t), G(t)$ by a Gowers norm, modulo

the point-counting estimates for certain varieties. The precise statement is in Theorem 3.3.2, and the corresponding point-counting estimates will be handled in Section 3.4.

Definition 3.3.1. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$. Define the **Roth variety** for corners associated to $F(t), G(t)$ to be the (quasi-affine) variety cut out by the following ten equations in sixteen variables $y_1, y_2, \dots, y_{16}$.*

$$F(y_1) - F(y_3) - F(y_9) + F(y_{11}) = 0 \quad (3.3.1)$$

$$F(y_2) - F(y_4) - F(y_{10}) + F(y_{12}) = 0 \quad (3.3.2)$$

$$F(y_5) - F(y_7) - F(y_{13}) + F(y_{15}) = 0 \quad (3.3.3)$$

$$F(y_6) - F(y_8) - F(y_{14}) + F(y_{16}) = 0 \quad (3.3.4)$$

$$G(y_1) - G(y_2) - G(y_9) + G(y_{10}) = 0 \quad (3.3.5)$$

$$G(y_3) - G(y_7) - G(y_{11}) + G(y_{15}) = 0 \quad (3.3.6)$$

$$G(y_4) - G(y_8) - G(y_{12}) + G(y_{16}) = 0 \quad (3.3.7)$$

$$G(y_5) - G(y_6) - G(y_{13}) + G(y_{14}) = 0 \quad (3.3.8)$$

$$F(y_9) - F(y_{10}) - F(y_{11}) + F(y_{12}) - F(y_{13}) + F(y_{14}) + F(y_{15}) - F(y_{16}) = 0 \quad (3.3.9)$$

$$G(y_9) - G(y_{10}) - G(y_{11}) + G(y_{12}) - G(y_{13}) + G(y_{14}) + G(y_{15}) - G(y_{16}) = 0 \quad (3.3.10)$$

The Roth variety could be regarded as a classical variety or a scheme over various fields, for example, the complex numbers $\mathbb{C}$ or finite fields $\mathbb{F}_p$.

We will often abbreviate the Roth variety for corners associated to $F(t), G(t)$ as the Roth variety. In this chapter, when we use this abbreviation, the context will always be clear enough to see that we are referring to the Roth variety for corners, not the Roth variety for one dimensional progressions.

Theorem 3.3.2. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$, and $Y(\mathbb{F}_p)$ be the $\mathbb{F}_p$ -points of the Roth variety for corners associated to $F(t), G(t)$. Then, we have the following*

Gowers norm control

$$\left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right| \leq \|f_0\|_2 \|f_1\|_4 \|f_2\|_4^{\frac{1}{2}} \|f_2\|_{U^2(0 \times \mathbb{F}_p)}^{\frac{1}{4}} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{\frac{1}{16}}$$

for all 1-bounded functions $f_0, f_1, f_2 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$.

Remark 3.3.3. Theorem 3.3.2 is not the strongest form of Gowers norm control that we can have. In fact, we can control the counting operator with $\|f_2\|_{0 \times \mathbb{F}_p, \mathbb{F}_p^2}$ instead of $\|f_2\|_{U^2(0 \times \mathbb{F}_p)}$; see equation (3.3.33).

Remark 3.3.4. Even though Theorem 3.3.2 does not have any linear independence assumption, it would not be useful when F, G are linearly dependent. This is because if F, G are linearly dependent, then one of the equations (3.3.9), (3.3.10) is redundant, in which case the Roth variety does not have the expected dimension and $|Y(\mathbb{F}_p)|$ is too large for the inequality to be useful.

Heuristically, the Roth variety for corners is cut out by 10 constraints in 16 variables, hence the intuitive expectation suggests that the dimension of the Roth variety is $16 - 10 = 6$ and the size of $\mathbb{F}_p$ -points on the Roth variety is about p^6 when the 10 constraints are “sufficiently independent”. In this case, Theorem 3.3.2 would indeed be providing control by the Gowers norm.

The ingredients of the proof of Theorem 3.3.2 are divided into three propositions, namely Propositions 3.3.5, 3.3.7 and 3.3.8. The strategy is to generalize the algebraic geometry PET induction for one dimensional three term rational function progressions in Section 2.3 to two dimensional corners. We would proceed with Fourier analytic method, and transform the exponential sums into point-counting estimates for the corresponding Roth variety to avoid difficult multidimensional exponential sum estimates. The Fourier calculations in the first half (up until Equation (3.3.17)) of the proof of Proposition 3.3.5 are same as the

Fourier calculations in the work of Han, Lacey and Yang [HLY21] on corners generated by polynomials. It seems plausible that combining the ideas from Section 2.3 and [HLY21] would lead to the desired estimates, however, there is a new obstacle—the “naive” generalization of algebraic geometry PET induction produces varieties with wrong expected dimensions. Fortunately, this obstacle could be tackled by ideas in the work of Kavrut and Wu [KW24] on improving the nonlinear Roth theorem.

The Proposition 3.3.5 is an intermediate step for algebraic geometry PET induction; it has the correct geometric term $|Y(\mathbb{F}_p)|$ but messy Fourier terms T_1, T_2 . The Fourier terms would be simplified in Proposition 3.3.7 and 3.3.8. In the statement and proof of Proposition 3.3.5, we will frequently use boldface letters to denote vectors in $\mathbb{F}_p^2$, for example $\mathbf{h}, \mathbf{n}, \mathbf{m}$ will mean $(h_1, h_2), (n_1, n_2), (m_1, m_2)$ respectively. Also, recall that the difference operator Δ is defined as $\Delta_{\mathbf{h}}g(\mathbf{x}) = g(\mathbf{x})\bar{g}(\mathbf{x} + \mathbf{h})$ for any functions g . Moreover, we use subscripts in l^2 -norm to emphasize the variables, for example, for a two variable function $T(a, b)$ on $\mathbb{F}_p^2$, we denote $\left(\sum_{a,b}|T(a, b)|^2\right)^{1/2}$ by $\|T(a, b)\|_{l_{a,b}^2}$. In other words, the notation $\|T(a, b)\|_{l_{a,b}^2}$ is the same as $\|T\|_{l^2}$, but hopefully this notation would be clearer when there are a lot of variables.

Proposition 3.3.5. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$, and $Y(\mathbb{F}_p)$ be the $\mathbb{F}_p$ -points of the Roth variety for corners associated to $F(t), G(t)$. For any functions f_1, f_2 , define*

$$T_1(n_1, \mathbf{h}) := \sum_{n_2} \Delta_{-\mathbf{h}} \widehat{f_1}(n_1, n_2)$$

$$T_2(m_2, \mathbf{h}) := \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f_2}(m_1, m_2),$$

where the order of operators is taking Fourier transform first and then difference operator for $\Delta_{\mathbf{h}} \widehat{f}$. Then, we have

$$\left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right|$$

$$\leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l_{n_1, \mathbf{h}}^2}^{1/2} \|T_2(m_2, \mathbf{h})\|_{l_{m_2, \mathbf{h}}^2}^{1/4} \|\overline{T_2}(m'_2, \mathbf{h}) T_2(m''_2, \mathbf{h})\|_{l_{m'_2, m''_2, \mathbf{h}}^2}^{1/8} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{1/16}$$

for all functions $f_0, f_1, f_2 : \mathbb{F}_p^2 \longrightarrow \mathbb{C}$.

Proof. For notational convenience, denote

$$\Lambda_0 := \left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right|$$

to be the quantity we would like to estimate.

Applying Cauchy–Schwarz inequality in x_1, x_2 , we have

$$\begin{aligned} \Lambda_0 &= \left| \mathbb{E}_{x_1, x_2} f_0(x_1, x_2) \mathbb{E}_y f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right| \\ &\leq \|f_0\|_2 \left(\mathbb{E}_{x_1, x_2} \left| \mathbb{E}_y f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right|^2 \right)^{1/2}. \end{aligned}$$

Fourier expand the functions f_1, f_2 to obtain

$$\begin{aligned} &\mathbb{E}_y f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ &= \mathbb{E}_y \sum_{\mathbf{n}, \mathbf{m}} \widehat{f}_1(\mathbf{n}) e_p(\mathbf{n} \cdot \mathbf{x}) e_p(n_1 F(y)) \widehat{f}_2(\mathbf{m}) e_p(\mathbf{m} \cdot \mathbf{x}) e_p(m_2 G(y)) \\ &= \sum_{\mathbf{n}, \mathbf{m}} \widehat{f}_1(\mathbf{n}) \widehat{f}_2(\mathbf{m}) e_p((\mathbf{n} + \mathbf{m}) \cdot \mathbf{x}) \mathbb{E}_y e_p(n_1 F(y) + m_2 G(y)). \end{aligned} \tag{3.3.11}$$

Denote $K(a, b) = \mathbb{E}_y e_p(aF(y) + bG(y))$ and perform change of variables $\mathbf{n} \leftrightarrow \mathbf{n} - \mathbf{m}$, then the expression (3.3.11) is equal to

$$\begin{aligned} &\sum_{\mathbf{n}, \mathbf{m}} \widehat{f}_1(\mathbf{n}) \widehat{f}_2(\mathbf{m}) e_p((\mathbf{n} + \mathbf{m}) \cdot \mathbf{x}) K(n_1, m_2) \\ &= \sum_{\mathbf{n}, \mathbf{m}} \widehat{f}_1(\mathbf{n} - \mathbf{m}) \widehat{f}_2(\mathbf{m}) e_p(\mathbf{n} \cdot \mathbf{x}) K(n_1 - m_1, m_2) \\ &= \sum_{\mathbf{n}} \left(\sum_{\mathbf{m}} \widehat{f}_1(\mathbf{n} - \mathbf{m}) \widehat{f}_2(\mathbf{m}) K(n_1 - m_1, m_2) \right) e_p(\mathbf{n} \cdot \mathbf{x}) \end{aligned} \tag{3.3.12}$$

Combining (3.3.11) and (3.3.12), Parseval's identity says

$$\begin{aligned} &\mathbb{E}_{x_1, x_2} \left| \mathbb{E}_y f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right|^2 \\ &= \sum_{\mathbf{n}} \left| \sum_{\mathbf{m}} \widehat{f}_1(\mathbf{n} - \mathbf{m}) \widehat{f}_2(\mathbf{m}) K(n_1 - m_1, m_2) \right|^2. \end{aligned} \tag{3.3.13}$$

Expanding the squares and performing change of variables $\mathbf{n} \leftrightarrow \mathbf{n} + \mathbf{m}$, the expression (3.3.13) becomes

$$\begin{aligned}
& \sum_{\mathbf{n}} \sum_{\mathbf{m}, \mathbf{h}} \widehat{f}_1(\mathbf{n} - \mathbf{m}) \overline{\widehat{f}_1(\mathbf{n} - \mathbf{m} - \mathbf{h})} \widehat{f}_2(\mathbf{m}) \overline{\widehat{f}_2(\mathbf{m} + \mathbf{h})} K(n_1 - m_1, m_2) \overline{K}(n_1 - m_1 - h_1, m_2 + h_2) \\
&= \sum_{\mathbf{n}, \mathbf{m}, \mathbf{h}} \widehat{f}_1(\mathbf{n}) \overline{\widehat{f}_1(\mathbf{n} - \mathbf{h})} \widehat{f}_2(\mathbf{m}) \overline{\widehat{f}_2(\mathbf{m} + \mathbf{h})} K(n_1, m_2) \overline{K}(n_1 - h_1, m_2 + h_2) \\
&= \sum_{\mathbf{n}, \mathbf{m}, \mathbf{h}} \Delta_{-\mathbf{h}} \widehat{f}_1(\mathbf{n}) \Delta_{\mathbf{h}} \widehat{f}_2(\mathbf{m}) \Delta_{(-h_1, h_2)} K(n_1, m_2).
\end{aligned} \tag{3.3.14}$$

To clarify, for the notation $\Delta_{\mathbf{h}} \widehat{f}$, the order of operators is applying Fourier transform first and then difference operator.

Note that in the last line of (3.3.14), some variables decouple, hence we can write (3.3.14) as

$$\sum_{\mathbf{h}, n_1, m_2} \Delta_{(-h_1, h_2)} K(n_1, m_2) \left(\sum_{n_2} \Delta_{-\mathbf{h}} \widehat{f}_1(n_1, n_2) \right) \left(\sum_{m_1} \Delta_{\mathbf{h}} \widehat{f}_2(m_1, m_2) \right). \tag{3.3.15}$$

To ease the notations, define

$$\begin{aligned}
T_1(n_1, \mathbf{h}) &:= \sum_{n_2} \Delta_{-\mathbf{h}} \widehat{f}_1(n_1, n_2) \\
T_2(m_2, \mathbf{h}) &:= \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f}_2(m_1, m_2),
\end{aligned}$$

so that the expression (3.3.15) can be rewritten more succinctly as

$$\sum_{\mathbf{h}, n_1, m_2} T_1(n_1, \mathbf{h}) T_2(m_2, \mathbf{h}) \Delta_{(-h_1, h_2)} K(n_1, m_2). \tag{3.3.16}$$

Applying Cauchy–Schwarz inequality in variables $\mathbf{h}, n_1$, we deduce that

$$\begin{aligned}
(3.3.16) &= \sum_{\mathbf{h}, n_1} T_1(n_1, \mathbf{h}) \sum_{m_2} T_2(m_2, \mathbf{h}) \Delta_{(-h_1, h_2)} K(n_1, m_2) \\
&\leq \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}} \left(\sum_{\mathbf{h}, n_1} \sum_{m_2, m'_2} T_2(m_2, \mathbf{h}) \overline{T_2(m'_2, \mathbf{h})} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \right)^{1/2}.
\end{aligned}$$

For notational convenience, denote

$$\Lambda_1 := \sum_{\mathbf{h}, n_1} \sum_{m_2, m'_2} T_2(m_2, \mathbf{h}) \overline{T_2(m'_2, \mathbf{h})} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)}.$$

To sum up, so far we have obtained

$$\Lambda_0 \leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}}^{1/2} \Lambda_1^{1/4} \quad (3.3.17)$$

and we have Cauchy–Schwarz away the functions f_0, f_1 . It is tempting to apply Cauchy–Schwarz inequality to Λ_1 in variables $\mathbf{h}, m_2, m'_2$ to get rid of f_2 . However, in this way, we would discard too much cancellation and the resulting variety has degeneracy, that is, the variety is defined by six equations in eight variables, but its dimension is three. To fix this, we use a technique due to Kavrut and Wu [KW24] to iterate the exponential sums one more time in order to capture more cancellation. Hence, we apply Cauchy–Schwarz inequality to Λ_1 in variables $\mathbf{h}, m_2$ to obtain

$$\begin{aligned} \Lambda_1 &= \sum_{\mathbf{h}, m_2} T_2(m_2, \mathbf{h}) \sum_{n_1, m'_2} \overline{T_2(m'_2, \mathbf{h})} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \\ &\leq \|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}} \\ &\quad \times \left(\sum_{\mathbf{h}, m_2} \sum_{\substack{n_1, m'_2 \\ n'_1, m''_2}} \overline{T_2(m'_2, \mathbf{h})} T_2(m''_2, \mathbf{h}) \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n'_1, m_2)} \right. \\ &\quad \left. \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \Delta_{(-h_1, h_2)} K(n'_1, m''_2) \right)^{1/2}, \end{aligned} \quad (3.3.18)$$

where m''_2, n'_1 are the copies of m'_2, n_1 respectively.

Once again, for notational convenience, denote

$$\begin{aligned} \Lambda_2 &:= \sum_{\mathbf{h}, m_2} \sum_{\substack{n_1, m'_2 \\ n'_1, m''_2}} \overline{T_2(m'_2, \mathbf{h})} T_2(m''_2, \mathbf{h}) \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n'_1, m_2)} \\ &\quad \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \Delta_{(-h_1, h_2)} K(n'_1, m''_2) \end{aligned}$$

and (3.3.18) can be rewritten as

$$\Lambda_1 \leq \|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}} \Lambda_2^{1/2}. \quad (3.3.19)$$

Now, we have kept enough cancellation, and we can apply Cauchy–Schwarz inequality to Λ_2 in variables $\mathbf{h}, m'_2, m''_2$ to get rid of T_2 and transform exponential sums into point-counting on variety. Hence, we have

$$\begin{aligned} \Lambda_2 &= \sum_{\mathbf{h}, m'_2, m''_2} \overline{T_2(m'_2, \mathbf{h})} T_2(m''_2, \mathbf{h}) \sum_{n_1, n'_1, m_2} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n'_1, m_2)} \\ &\quad \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \Delta_{(-h_1, h_2)} K(n'_1, m''_2) \\ &\leq \| \overline{T_2(m'_2, \mathbf{h})} T_2(m''_2, \mathbf{h}) \|_{l^2_{m'_2, m''_2, \mathbf{h}}} \\ &\quad \times \left(\sum_{\mathbf{h}, m'_2, m''_2} \sum_{\substack{n_1, n'_1, m_2 \\ N_1, N'_1, M_2}} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n'_1, m_2)} \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \Delta_{(-h_1, h_2)} K(n'_1, m''_2) \right. \\ &\quad \left. \overline{\Delta_{(-h_1, h_2)} K(N_1, M_2)} \Delta_{(-h_1, h_2)} K(N'_1, M_2) \Delta_{(-h_1, h_2)} K(N_1, m'_2) \overline{\Delta_{(-h_1, h_2)} K(N'_1, m''_2)} \right)^{1/2}, \end{aligned} \quad (3.3.20)$$

where N_1, N'_1, M_2 are the copies of n_1, n'_1, m_2 respectively.

Finally, expanding the exponential sums, we have

$$\begin{aligned}
& \sum_{\mathbf{h}, m'_2, m''_2} \sum_{\substack{n_1, n'_1, m_2 \\ N_1, N'_1, M_2}} \Delta_{(-h_1, h_2)} K(n_1, m_2) \overline{\Delta_{(-h_1, h_2)} K(n'_1, m_2)} \overline{\Delta_{(-h_1, h_2)} K(n_1, m'_2)} \Delta_{(-h_1, h_2)} K(n'_1, m''_2) \\
& \quad \overline{\Delta_{(-h_1, h_2)} K(N_1, M_2)} \Delta_{(-h_1, h_2)} K(N'_1, M_2) \Delta_{(-h_1, h_2)} K(N_1, m'_2) \overline{\Delta_{(-h_1, h_2)} K(N'_1, m''_2)} \\
& = \mathbb{E}_{\substack{y_1, y_2, y_3, y_4 \\ y_5, y_6, y_7, y_8 \\ y_9, y_{10}, y_{11}, y_{12} \\ y_{13}, y_{14}, y_{15}, y_{16}}} \sum_{\substack{h_1, h_2 \\ n_1, n'_1, N_1, N'_1 \\ m_2, m'_2, m''_2, M_2}} \\
& \quad e_p \left(\begin{aligned}
& + n_1 F(y_1) + m_2 G(y_1) & - (n_1 - h_1) F(y_9) - (m_2 + h_2) G(y_9) \\
& - n'_1 F(y_2) - m_2 G(y_2) & + (n'_1 - h_1) F(y_{10}) + (m_2 + h_2) G(y_{10}) \\
& - n_1 F(y_3) - m'_2 G(y_3) & + (n_1 - h_1) F(y_{11}) + (m'_2 + h_2) G(y_{11}) \\
& + n'_1 F(y_4) + m''_2 G(y_4) & - (n'_1 - h_1) F(y_{12}) - (m''_2 + h_2) G(y_{12}) \\
& - N_1 F(y_5) - M_2 G(y_5) & + (N_1 - h_1) F(y_{13}) + (M_2 + h_2) G(y_{13}) \\
& + N'_1 F(y_6) + M_2 G(y_6) & - (N'_1 - h_1) F(y_{14}) - (M_2 + h_2) G(y_{14}) \\
& + N_1 F(y_7) + m'_2 G(y_7) & - (N_1 - h_1) F(y_{15}) - (m'_2 + h_2) G(y_{15}) \\
& - N'_1 F(y_8) - m''_2 G(y_8) & + (N'_1 - h_1) F(y_{16}) + (m''_2 + h_2) G(y_{16})
\end{aligned} \right)
\end{aligned} \tag{3.3.21}$$

which is equal to

$$\begin{aligned}
&= \sum_{\substack{y_1, y_2, y_3, y_4 \\ y_5, y_6, y_7, y_8 \\ y_9, y_{10}, y_{11}, y_{12} \\ y_{13}, y_{14}, y_{15}, y_{16}}} \mathbb{E}_{\substack{h_1, h_2 \\ n_1, n'_1, N_1, N'_1 \\ m_2, m'_2, m''_2, M_2}} \\
&\quad e_p \Big(n_1 (F(y_1) - F(y_3) - F(y_9) + F(y_{11})) \\
&\quad \quad + n'_1 (-F(y_2) + F(y_4) + F(y_{10}) - F(y_{12})) \\
&\quad \quad + N_1 (-F(y_5) + F(y_7) + F(y_{13}) - F(y_{15})) \\
&\quad \quad + N'_1 (F(y_6) - F(y_8) - F(y_{14}) + F(y_{16})) \\
&\quad \quad + m_2 (G(y_1) - G(y_2) - G(y_9) + G(y_{10})) \\
&\quad \quad + m'_2 (-G(y_3) + G(y_7) + G(y_{11}) - G(y_{15})) \\
&\quad \quad + m''_2 (G(y_4) - G(y_8) - G(y_{12}) + G(y_{16})) \\
&\quad \quad + M_2 (-G(y_5) + G(y_6) + G(y_{13}) - G(y_{14})) \\
&\quad \quad + h_1 (F(y_9) - F(y_{10}) - F(y_{11}) + F(y_{12}) - F(y_{13}) + F(y_{14}) + F(y_{15}) - F(y_{16})) \\
&\quad \quad + h_2 (-G(y_9) + G(y_{10}) + G(y_{11}) - G(y_{12}) + G(y_{13}) - G(y_{14}) - G(y_{15}) + G(y_{16})) \Big) \\
&= \frac{1}{p^6} |Y(\mathbb{F}_p)|
\end{aligned} \tag{3.3.22}$$

where the last line of (3.3.22) follows from the orthogonality of characters and the definition of the Roth variety.

To complete the proof, we combine (3.3.17), (3.3.19), (3.3.20), (3.3.21) and (3.3.22), and conclude

$$\begin{aligned}
\Lambda_0 &\leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}}^{1/2} \Lambda_1^{1/4} \\
&\leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}}^{1/2} \|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}}^{1/4} \Lambda_2^{1/8}. \\
&\leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}}^{1/2} \|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}}^{1/4} \|\overline{T_2}(m'_2, \mathbf{h}) T_2(m''_2, \mathbf{h})\|_{l^2_{m'_2, m''_2, \mathbf{h}}}^{1/8} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{1/16}.
\end{aligned}$$

□

Remark 3.3.6. Note that we do not consider summing over n_1 for Λ_1 to exploit the cancellation among exponential sums. If we were to do that, then we would run into some exponential sum of the form $\sum_{\mathbf{y} \in V(\mathbb{F}_p)} e_p(\varphi(\mathbf{y}))$ (with some variety V and rational function φ), which is rather difficult and complicated to understand. On the contrary, point-counting on the Roth variety is more tractable.

The next proposition is the first part of simplifications of Fourier coefficients in Proposition 3.3.5. Similar calculations also appear in [HLY21].

Proposition 3.3.7. *Let $f_1, f_2 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$ be functions, define*

$$T_1(n_1, \mathbf{h}) = \sum_{n_2} \Delta_{-\mathbf{h}} \widehat{f_1}(n_1, n_2), \quad T_2(m_2, \mathbf{h}) = \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f_2}(m_1, m_2),$$

then we have

$$\|T_1(n_1, \mathbf{h})\|_{l_{n_1, \mathbf{h}}^2} \leq \|f_1\|_4^2, \quad \|T_2(m_2, \mathbf{h})\|_{l_{m_2, \mathbf{h}}^2} \leq \|f_2\|_4^2.$$

Proof. We will prove the estimate for T_2 and the estimate for T_1 follows similarly by symmetry. By definition of T_2 and Fourier transform, we have

$$\begin{aligned} T_2(m_2, \mathbf{h}) &= \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f_2}(m_1, m_2) \\ &= \sum_{m_1} \widehat{f_2}(m_1, m_2) \overline{\widehat{f_2}(m_1 + h_1, m_2 + h_2)} \\ &= \sum_{m_1} \mathbb{E}_{\mathbf{x}, \mathbf{z}} f_2(\mathbf{x}) e_p(-\mathbf{m} \cdot \mathbf{x}) \overline{f_2(\mathbf{z})} e_p(\mathbf{m} \cdot \mathbf{z}) e_p(\mathbf{h} \cdot \mathbf{z}). \end{aligned} \tag{3.3.23}$$

Summing over variable m_1 to utilize the orthogonality of characters, the expression (3.3.23) becomes

$$\begin{aligned} &\mathbb{E}_{x_2, z_1, z_2} f_2(z_1, x_2) \overline{f_2(z_1, z_2)} e_p(m_2(z_2 - x_2)) e_p(\mathbf{h} \cdot \mathbf{z}) \\ &= \mathbb{E}_{x_2, z_1, z_2} f_2(z_1, x_2 + z_2) \overline{f_2(z_1, z_2)} e_p(\mathbf{h} \cdot \mathbf{z} - m_2 x_2) \end{aligned} \tag{3.3.24}$$

where the last line of (3.3.24) follows from change of variables $x_2 \leftrightarrow x_2 + z_2$.

Combining (3.3.23) and (3.3.24), Parseval's identity says

$$\|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}}^2 = \sum_{m_2, \mathbf{h}} |T_2(m_2, \mathbf{h})|^2 = \mathbb{E}_{x_2, z_1, z_2} |f_2(z_1, x_2 + z_2) \overline{f_2}(z_1, z_2)|^2. \quad (3.3.25)$$

Note that

$$\begin{aligned} \mathbb{E}_{x_2, z_1, z_2} |f_2(z_1, x_2 + z_2) \overline{f_2}(z_1, z_2)|^2 &= \mathbb{E}_{x_2, z_1, z_2} |f_2(z_1, x_2) f_2(z_1, z_2)|^2 \\ &= \mathbb{E}_{z_1} \left(\mathbb{E}_{x_2} |f_2(z_1, x_2)|^2 \right) \left(\mathbb{E}_{z_2} |f_2(z_1, z_2)|^2 \right) \\ &= \mathbb{E}_{z_1} \left(\mathbb{E}_{z_2} |f_2(z_1, z_2)|^2 \right)^2 \end{aligned} \quad (3.3.26)$$

Finally, applying Cauchy–Schwarz inequality to the inner sum of the last line of (3.3.26), we have

$$\mathbb{E}_{z_1} \left(\mathbb{E}_{z_2} |f_2(z_1, z_2)|^2 \right)^2 \leq \mathbb{E}_{z_1} \mathbb{E}_{z_2} |f_2(z_1, z_2)|^4 = \|f_2\|_4^4. \quad (3.3.27)$$

Combining (3.3.25), (3.3.26) and (3.3.27) would complete the proof. $\square$

The next proposition is the second part of simplifications of Fourier coefficients in Proposition 3.3.5. Compared to the Proposition 3.3.7, its proof is more complicated and involves Gowers norms.

Proposition 3.3.8. *Let $f_2 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$ be a 1-bounded function and define $T_2(m_2, \mathbf{h}) = \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f_2}(m_1, m_2)$. Then, we have*

$$\|\overline{T_2}(m_2, \mathbf{h}) T_2(m'_2, \mathbf{h})\|_{l^2_{m_2, m'_2, \mathbf{h}}} \leq \|f_2\|_{U^2(0 \times \mathbb{F}_p)}^2.$$

Proof. By definition of T_2 and Fourier transform, we have

$$\begin{aligned} T_2(m_2, \mathbf{h}) &= \sum_{m_1} \Delta_{\mathbf{h}} \widehat{f_2}(m_1, m_2) \\ &= \sum_{m_1} \widehat{f_2}(m_1, m_2) \widehat{\overline{f_2}}(m_1 + h_1, m_2 + h_2) \\ &= \sum_{m_1} \mathbb{E}_{\mathbf{x}, \mathbf{z}} f_2(\mathbf{x}) e_p(-\mathbf{m} \cdot \mathbf{x}) \overline{f_2}(\mathbf{z}) e_p(\mathbf{m} \cdot \mathbf{z}) e_p(\mathbf{h} \cdot \mathbf{z}). \end{aligned} \quad (3.3.28)$$

Summing over variable m_1 to utilize the orthogonality of characters, the expression (3.3.28) becomes

$$\begin{aligned} & \mathbb{E}_{x_2, z_1, z_2} f_2(z_1, x_2) \overline{f_2(z_1, z_2)} e_p(m_2(z_2 - x_2)) e_p(\mathbf{h} \cdot \mathbf{z}) \\ &= \mathbb{E}_{x_2} \left(\mathbb{E}_{z_1, z_2} f_2(z_1, x_2 + z_2) \overline{f_2(z_1, z_2)} e_p(\mathbf{h} \cdot \mathbf{z}) \right) e_p(-m_2 x_2) \end{aligned} \quad (3.3.29)$$

where the last line of (3.3.29) follows from change of variables $x_2 \leftrightarrow x_2 + z_2$.

Combining (3.3.28) and (3.3.29), Parseval's identity says

$$\begin{aligned} \sum_{m_2} |T_2(m_2, \mathbf{h})|^2 &= \mathbb{E}_{x_2} \left| \mathbb{E}_{\mathbf{z}} f_2(z_1, x_2 + z_2) \overline{f_2(z_1, z_2)} e_p(\mathbf{h} \cdot \mathbf{z}) \right|^2 \\ &= \mathbb{E}_{x_2} \mathbb{E}_{\mathbf{z}, \mathbf{z}'} \Delta_{\mathbf{z}'} f_2(z_1, x_2 + z_2) \overline{\Delta_{\mathbf{z}'} f_2(z_1, z_2)} e_p(-\mathbf{h} \cdot \mathbf{z}'). \end{aligned} \quad (3.3.30)$$

Note that the quantity we would like to upper bound for this proof has the following decomposition:

$$\begin{aligned} \|\overline{T_2}(m_2, \mathbf{h}) T_2(m'_2, \mathbf{h})\|_{l^2_{m_2, m'_2, \mathbf{h}}}^2 &= \sum_{m_2, m'_2, \mathbf{h}} |T_2(m_2, \mathbf{h}) T_2(m'_2, \mathbf{h})|^2 \\ &= \sum_{\mathbf{h}} \left(\sum_{m_2} |T_2(m_2, \mathbf{h})|^2 \right) \left(\sum_{m'_2} |T_2(m'_2, \mathbf{h})|^2 \right) \\ &= \sum_{\mathbf{h}} \left(\sum_{m_2} |T_2(m_2, \mathbf{h})|^2 \right)^2. \end{aligned} \quad (3.3.31)$$

By (3.3.31), (3.3.30) and Parseval's identity, we have

$$\|\overline{T_2}(m_2, \mathbf{h}) T_2(m'_2, \mathbf{h})\|_{l^2_{m_2, m'_2, \mathbf{h}}}^2 = \mathbb{E}_{\mathbf{z}'} \left| \mathbb{E}_{x_2, \mathbf{z}} \Delta_{\mathbf{z}'} f_2(z_1, x_2 + z_2) \overline{\Delta_{\mathbf{z}'} f_2(z_1, z_2)} \right|^2. \quad (3.3.32)$$

Note that the inner sum of (3.3.32) is nonnegative since

$$\begin{aligned} \mathbb{E}_{x_2, \mathbf{z}} \Delta_{\mathbf{z}'} f_2(z_1, x_2 + z_2) \overline{\Delta_{\mathbf{z}'} f_2(z_1, z_2)} &= \mathbb{E}_{x_2, \mathbf{z}} \Delta_{\mathbf{z}'} f_2(z_1, x_2) \overline{\Delta_{\mathbf{z}'} f_2(z_1, z_2)} \\ &= \mathbb{E}_{z_1} \left(\mathbb{E}_{x_2} \Delta_{\mathbf{z}'} f_2(z_1, x_2) \right) \left(\mathbb{E}_{z_2} \overline{\Delta_{\mathbf{z}'} f_2(z_1, z_2)} \right) \\ &= \mathbb{E}_{z_1} \left| \mathbb{E}_{x_2} \Delta_{\mathbf{z}'} f_2(z_1, x_2) \right|^2 \\ &\geq 0 \end{aligned}$$

Nonnegativity of the inner sum of (3.3.32) and the 1-boundedness of f_2 allow us to deduce that

$$\begin{aligned}
\|\overline{T_2}(m_2, \mathbf{h})T_2(m'_2, \mathbf{h})\|_{l^2_{m_2, m'_2, \mathbf{h}}}^2 &\leq \mathbb{E}_{\mathbf{z}'} \mathbb{E}_{x_2, \mathbf{z}} \overline{\Delta_{\mathbf{z}'} f_2}(z_1, x_2 + z_2) \Delta_{\mathbf{z}'} f_2(z_1, z_2) \\
&= \mathbb{E}_{\mathbf{z}} \mathbb{E}_{x_2, \mathbf{z}'} \Delta_{(0, x_2)} \Delta_{\mathbf{z}'} f_2(z_1, z_2) \\
&= \|f_2\|_{0 \times \mathbb{F}_p, \mathbb{F}_p^2}^4 \\
&\leq \|f_2\|_{U^2(0 \times \mathbb{F}_p)}^4.
\end{aligned} \tag{3.3.33}$$

For the first line of (3.3.33), we switch the complex conjugates so that it is easier to recognize the formula as a Gowers norm, and this is valid thanks to the nonnegativity again. For the last line of (3.3.33), we use the fact that restricting to subgroup will not decrease Gowers norms. $\square$

Now, we have enough ingredients to prove Theorem 3.3.2.

Proof of Theorem 3.3.2. We simply need to put Propositions 3.3.5, 3.3.7 and 3.3.8 together to obtain

$$\begin{aligned}
&\left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right| \\
&\leq \|f_0\|_2 \|T_1(n_1, \mathbf{h})\|_{l^2_{n_1, \mathbf{h}}}^{1/2} \|T_2(m_2, \mathbf{h})\|_{l^2_{m_2, \mathbf{h}}}^{1/4} \|\overline{T_2}(m'_2, \mathbf{h})T_2(m''_2, \mathbf{h})\|_{l^2_{m'_2, m''_2, \mathbf{h}}}^{1/8} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{1/16} \\
&\leq \|f_0\|_2 \|f_1\|_4 \|f_2\|_4^{\frac{1}{2}} \|f_2\|_{U^2(0 \times \mathbb{F}_p)}^{\frac{1}{4}} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{\frac{1}{16}}
\end{aligned}$$

$\square$

For the purpose of induction, we also need the following “dual version” of Theorem 3.3.2.

Theorem 3.3.9. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$, and $Y(\mathbb{F}_p)$ be the $\mathbb{F}_p$ -points of the Roth variety for corners associated to $F(t), G(t)$. Then, we have the following*

Gowers norm control

$$\left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right| \leq \|f_0\|_2 \|f_1\|_4^{\frac{1}{2}} \|f_1\|_{U^2(\mathbb{F}_p \times 0)}^{\frac{1}{4}} \|f_2\|_4 \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{\frac{1}{16}}$$

for all 1-bounded functions $f_0, f_1, f_2 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$.

Proof. One could repeat the proof of Theorem 3.3.2 and reverse the roles of f_1, f_2 in the order of applying Cauchy–Schwarz inequality. Alternatively, this theorem could be deduced from the Theorem 3.3.2 directly. Let $g_0(x_1, x_2) = f_0(x_2, x_1)$, $g_1(x_1, x_2) = f_1(x_2, x_1)$ and $g_2(x_1, x_2) = f_2(x_2, x_1)$, applying Theorem 3.3.2 to the functions g_0, g_2, g_1 , we have

$$\begin{aligned} & \left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right| \\ &= \left| \mathbb{E}_{x_1, x_2, y} g_0(x_2, x_1) g_2(x_2 + G(y), x_1) g_1(x_2, x_1 + F(y)) \right| \\ &\leq \|g_0\|_2 \|g_2\|_4 \|g_1\|_4^{\frac{1}{2}} \|g_1\|_{U^2(0 \times \mathbb{F}_p)}^{\frac{1}{4}} \left(\frac{1}{p^6} |Y(\mathbb{F}_p)| \right)^{\frac{1}{16}} \end{aligned}$$

Note that the Roth variety is symmetric in $F(t), G(t)$ and $\|g_1\|_{U^2(0 \times \mathbb{F}_p)} = \|f_1\|_{U^2(\mathbb{F}_p \times 0)}$. $\square$

3.4 Dimension estimates

In this section, we will prove the point-counting estimates for Roth variety in Theorem 3.4.2. Heuristically, while $F(t), G(t)$ and constant function 1 are linearly independent, the defining equations of the Roth variety for corners associated to $F(t), G(t)$ are essentially independent, hence the Roth variety has expected dimension 6.

We start with a preliminary proposition regarding certain determinant. For Proposition 3.4.1, we adopt the convention that a blank entry in a matrix is understood to be zero.

Proposition 3.4.1. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$, and Y be the Roth variety for corners associated to $F(t), G(t)$. Let J be the determinant of the first ten columns*

of the Jacobian matrix of the defining equations of Y , that is

$$\begin{vmatrix} F'(y_1) & & F'(y_3) & & & & & & -F'(y_9) & & \\ & F'(y_2) & & -F'(y_4) & & & & & & & -F'(y_{10}) \\ & & & & F'(y_5) & & -F'(y_7) & & & & \\ & & & & & F'(y_6) & & -F'(y_8) & & & \\ G'(y_1) & -G'(y_2) & & & & & & & -G'(y_9) & G'(y_{10}) & \\ & & G'(y_3) & & & & -G'(y_7) & & & & \\ & & & G'(y_4) & & & & -G'(y_8) & & & \\ & & & & G'(y_5) & -G'(y_6) & & & & & \\ & & & & & & & & F'(y_9) & -F'(y_{10}) & \\ & & & & & & & & G'(y_9) & -G'(y_{10}) & \end{vmatrix}.$$

Then, we have

$$\begin{aligned} J = & \left(F'(y_1)G'(y_2)G'(y_3)F'(y_4)G'(y_5)F'(y_6)F'(y_7)G'(y_8) \right. \\ & \left. - G'(y_1)F'(y_2)F'(y_3)G'(y_4)F'(y_5)G'(y_6)G'(y_7)F'(y_8) \right) \\ & \times \left(-F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) \right). \end{aligned}$$

Proof. Note that the first eight entries of the ninth and tenth rows of the Jacobian matrix

are entirely zeroes, hence we can expand J as

$$\begin{aligned}
& \begin{vmatrix} F'(y_1) & & -F'(y_3) & & & & & \\ & F'(y_2) & & -F'(y_4) & & & & \\ & & & & F'(y_5) & & -F'(y_7) & \\ F'(y_9) & -F'(y_{10}) & & & & F'(y_6) & & -F'(y_8) \\ G'(y_9) & -G'(y_{10}) & G'(y_1) & -G'(y_2) & & & & \\ & & & & G'(y_3) & & & -G'(y_7) \\ & & & & & G'(y_4) & & -G'(y_8) \\ & & & & & & G'(y_5) & -G'(y_6) \end{vmatrix} \\
&= \left(-F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) \right) J_1
\end{aligned} \tag{3.4.1}$$

where J_1 is defined to be the determinant of the 8×8 matrix in the first line of (3.4.1).

Next, expand J_1 with respect to the first column to obtain

$$J_1 = F'(y_1) \begin{vmatrix} F'(y_2) & & -F'(y_4) & & & & & \\ & & & F'(y_5) & & -F'(y_7) & & \\ & & & & F'(y_6) & & -F'(y_8) & \\ -G'(y_2) & & & & & & & \\ & G'(y_3) & & & & & -G'(y_7) & \\ & & G'(y_4) & & & & & -G'(y_8) \\ & & & G'(y_5) & -G'(y_6) & & & \end{vmatrix}$$

$$+ G'(y_1) \begin{vmatrix} & -F'(y_3) & & & & & \\ F'(y_2) & & -F'(y_4) & & & & \\ & & & F'(y_5) & & -F'(y_7) & \\ & & & & F'(y_6) & & -F'(y_8) \\ & G'(y_3) & & & & -G'(y_7) & \\ & & G'(y_4) & & & & -G'(y_8) \\ & & & G'(y_5) & -G'(y_6) & & \end{vmatrix}$$

$$=: A + B$$

where A, B are defined to be the two terms in the cofactor expansion of J_1 .

The 7×7 matrices in A, B are fairly sparse. For each of them, we could argue combinatorially that there is only one permutation of $\{1, 2, \dots, 7\}$ such that the product of entries is nonzero, and evaluate the determinant, but perhaps it would be clearer if we record the direct computations via repeated use of cofactor expansions of determinants as an alternative approach here.

We start with the quantity A . Expanding the determinant with respect to the fourth row, the expression simplifies to

$$F'(y_1)G'(y_2) \begin{vmatrix} & -F'(y_4) & & & & \\ & & F'(y_5) & & -F'(y_7) & \\ & & & F'(y_6) & & -F'(y_8) \\ G'(y_3) & & & & -G'(y_7) & \\ & G'(y_4) & & & & -G'(y_8) \\ & & G'(y_5) & -G'(y_6) & & \end{vmatrix}.$$

Expanding the determinant with respect to the first column, the expression simplifies to

$$-F'(y_1)G'(y_2)G'(y_3) \begin{vmatrix} -F'(y_4) & & \\ & F'(y_5) & -F'(y_7) \\ & & F'(y_6) & -F'(y_8) \\ G'(y_4) & & & -G'(y_8) \\ & G'(y_5) & -G'(y_6) & \end{vmatrix}.$$

Expanding the determinant with respect to the first row, the expression simplifies to

$$F'(y_1)G'(y_2)G'(y_3)F'(y_4) \begin{vmatrix} F'(y_5) & & -F'(y_7) \\ & F'(y_6) & -F'(y_8) \\ & & -G'(y_8) \\ G'(y_5) & -G'(y_6) & \end{vmatrix}.$$

Expanding the determinant with respect to the third column, the expression simplifies to

$$-F'(y_1)G'(y_2)G'(y_3)F'(y_4)F'(y_7) \begin{vmatrix} & F'(y_6) & -F'(y_8) \\ & & -G'(y_8) \\ G'(y_5) & -G'(y_6) & \end{vmatrix}.$$

Expanding the determinant with respect to the first column, the expression simplifies to

$$-F'(y_1)G'(y_2)G'(y_3)F'(y_4)G'(y_5)F'(y_7) \begin{vmatrix} F'(y_6) & -F'(y_8) \\ & -G'(y_8) \end{vmatrix}.$$

Expanding the 2×2 determinant, the expression simplifies to

$$F'(y_1)G'(y_2)G'(y_3)F'(y_4)G'(y_5)F'(y_6)F'(y_7)G'(y_8)$$

Next, we repeat the same process for B . Expanding the determinant with respect to the

first column, the expression simplifies to

$$-G'(y_1)F'(y_2) \begin{vmatrix} -F'(y_3) & & & & & & & \\ & F'(y_5) & & -F'(y_7) & & & & \\ & & F'(y_6) & & -F'(y_8) & & & \\ G'(y_3) & & & -G'(y_7) & & & & \\ & G'(y_4) & & & & & -G'(y_8) & \\ & & G'(y_5) & -G'(y_6) & & & & \end{vmatrix}.$$

Expanding the determinant with respect to the first row, the expression simplifies to

$$G'(y_1)F'(y_2)F'(y_3) \begin{vmatrix} & F'(y_5) & & -F'(y_7) & & \\ & & F'(y_6) & & -F'(y_8) & \\ & & & -G'(y_7) & & \\ G'(y_4) & & & & & -G'(y_8) \\ & G'(y_5) & -G'(y_6) & & & \end{vmatrix}.$$

Expanding the determinant with respect to the first column, the expression simplifies to

$$-G'(y_1)F'(y_2)F'(y_3)G'(y_4) \begin{vmatrix} F'(y_5) & & -F'(y_7) & \\ & F'(y_6) & & -F'(y_8) \\ & & -G'(y_7) & \\ G'(y_5) & -G'(y_6) & & \end{vmatrix}.$$

Expanding the determinant with respect to the last column, the expression simplifies to

$$G'(y_1)F'(y_2)F'(y_3)G'(y_4)F'(y_8) \begin{vmatrix} F'(y_5) & -F'(y_7) \\ & -G'(y_7) \\ G'(y_5) & -G'(y_6) \end{vmatrix}.$$

Expanding the determinant with respect to the second row, the expression simplifies to

$$G'(y_1)F'(y_2)F'(y_3)G'(y_4)G'(y_7)F'(y_8) \begin{vmatrix} F'(y_5) \\ G'(y_5) & -G'(y_6) \end{vmatrix}.$$

Expanding the 2×2 determinant, the expression simplifies to

$$-G'(y_1)F'(y_2)F'(y_3)G'(y_4)F'(y_5)G'(y_6)G'(y_7)F'(y_8),$$

this completes the proof. □

The main theorem in this section is Theorem 3.4.2.

Theorem 3.4.2. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and constant function 1 are linearly independent over $\mathbb{Q}$, and $Y(\mathbb{F}_p)$ be the $\mathbb{F}_p$ -points of the Roth variety for corners associated to $F(t), G(t)$. Then, we have the following point-counting estimate*

$$|Y(\mathbb{F}_p)| \ll p^6.$$

Proof.

High-level overview of the proof:

The method of the proof of Theorem 3.4.2 is similar to that of Theorem 2.4.1. The main idea is actually fairly intuitive and direct, but some long technical steps are needed in order to make the proof rigorous. These technical steps are similar to those used in the proof of Theorem 2.4.1 and they may not be very helpful for a first reading.

To improve readability, we decided to include a high-level overview of the proof, a working heuristic with sufficient details but omitting the technical steps, and an appendix (Appendix 6.1) which indicates how to modify the proof of Theorem 2.4.1 to fill in the missing technical steps in the working heuristic. Some key calculations are isolated as Lemma 3.4.3 so that the proof would be more modular.

The main idea is to decompose the Roth variety into smooth parts and singular parts repeatedly. Informally, the geometry of the smooth parts can be understood via machinery

in algebraic geometry, while the singular parts come with extra constraints. Repeating the decompositions will gradually amplify the constraints on singular parts. In fact, the Jacobian matrix of the Roth variety has nice structure, so the variables in the extra constraints on the singular parts often “decouple”, which is quite useful for the decomposition process. After sufficiently many decompositions, the singular parts will become simple enough for us to conclude the proof.

Working heuristic with details:

Our working heuristic is based on the following three principles.

Principle 1: A variety whose Jacobian matrix is full rank, is smooth, and hence has the expected dimension and $\mathbb{F}_p$ -point count. This is in line with our intuitions from geometry and implicit function theorem.

Principle 2: The number of $\mathbb{F}_p$ -points of a variety with “triangular” defining equations can be bounded easily. For example, let V be the variety cut out by the following three equations in six variables:

$$\begin{aligned} y_1 + 2y_2^3 - y_4^5 + 3y_5^7 + 100y_6^9 &= 0 \\ y_2^2 - y_4^3 + 5y_5^{11} &= 0 \\ y_3 - y_4^3 &= 0 \end{aligned}$$

Although the defining equations of V are fairly complicated and highly nonlinear, but we can still bound $|V(\mathbb{F}_p)|$ easily. Indeed, there are at most p^3 choices of y_1, y_2, y_3 ; for every fixed y_1, y_2, y_3 , there are at most $O(1)$ many choices of y_4, y_5, y_6 , therefore we have $|V(\mathbb{F}_p)| = O(p^3)$.

Principle 3: Constraints that look “strong” and “simple” often make a system of equations “triangular”. For example, let V be the variety cut out by the following two equations

in four variables:

$$\begin{aligned} y_1^5 - 2y_2^7 + 3y_3^{11} - 4y_4^{13} &= 0 \\ y_4^{10} - y_4^3 + y_4 &= 0 \end{aligned}$$

The constraint $y_4^{10} - y_4^3 + y_4 = 0$ is quite strong since it only involves one variable y_4 . As a result, the defining equations are "triangular" and we can easily deduce a good bound that $|V(\mathbb{F}_p)| = O(p^2)$.

Now, we can proceed with our argument.

Step 1: Preliminary decomposition

Let $J(y_1, y_2, \dots, y_{10})$ be the determinant of the first ten columns of the Jacobian matrix of the defining equations of the Roth variety Y , then by Proposition 3.4.1, we have

$$\begin{aligned} &J(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}) \\ &= \left(F'(y_1)G'(y_2)G'(y_3)F'(y_4)G'(y_5)F'(y_6)F'(y_7)G'(y_8) \right. \\ &\quad \left. - G'(y_1)F'(y_2)F'(y_3)G'(y_4)F'(y_5)G'(y_6)G'(y_7)F'(y_8) \right) \\ &\quad \times \left(-F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) \right). \end{aligned}$$

Define

$$Y_{\text{gen}} = Y \cap \{(y_1, y_2, \dots, y_{16}) \in \mathbb{A}^{16} : J(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}) \neq 0\}$$

and

$$Y_{\text{sp}} = Y \cap \{(y_1, y_2, \dots, y_{16}) \in \mathbb{A}^{16} : J(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{10}) = 0\}$$

where $\mathbb{A}$ is the affine space.

By construction, the variety Y_{gen} has a Jacobian matrix with full rank, thus Y_{gen} is smooth and hence has the expected dimension 6 and the expected $\mathbb{F}_p$ -point count that

$|Y_{\text{gen}}(\mathbb{F}_p)| = O(p^6)$. So, it remains to show that $|Y_{\text{sp}}(\mathbb{F}_p)| = O(p^6)$; we are in a better situation than where we started since we now get an extra constraint $J(y_1, y_2, \dots, y_{10}) = 0$ for free.

Next, we will further decompose Y_{sp} . Let

$$R(y) = \frac{F'(y)}{G'(y)} \quad (3.4.2)$$

and rewrite $J(y_1, y_2, \dots, y_{10})$ as

$$\begin{aligned} & \left(-F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) \right) \\ & \times \left(G'(y_1)G'(y_2)G'(y_3)G'(y_4)G'(y_5)G'(y_6)G'(y_7)G'(y_8) \right) \\ & \times \left(R(y_1)R(y_4)R(y_6)R(y_7) - R(y_2)R(y_3)R(y_5)R(y_8) \right). \end{aligned}$$

Define

$$Z = Y \cap \{(y_1, y_2, \dots, y_{16}) \in \mathbb{A}^{16} : R(y_1)R(y_4)R(y_6)R(y_7) - R(y_2)R(y_3)R(y_5)R(y_8) = 0\}$$

$$Y_i = Y \cap \{(y_1, y_2, \dots, y_{16}) \in \mathbb{A}^{16} : G'(y_i) = 0\} \quad \text{for } 1 \leq i \leq 8$$

$$Y_{9,10} = Y \cap \{(y_1, y_2, \dots, y_{16}) \in \mathbb{A}^{16} : -F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) = 0\}.$$

Note that $Y_{\text{sp}}(\mathbb{F}_p) = Z(\mathbb{F}_p) \cup Y_1(\mathbb{F}_p) \cup Y_2(\mathbb{F}_p) \cup \dots \cup Y_8(\mathbb{F}_p) \cup Y_{9,10}(\mathbb{F}_p)$. Informally, the varieties $Y_1, Y_2, \dots, Y_8, Y_{9,10}$ are “degenerate” subvarieties of low dimension due to the “strong” constraints $G'(y_i) = 0$ for $1 \leq i \leq 8$ and $-F'(y_9)G'(y_{10}) + G'(y_9)F'(y_{10}) = 0$, therefore we can safely ignore them for now to ease our mind. The main difficulty lies in the variety Z , and it remains to show that $|Z(\mathbb{F}_p)| = O(p^6)$.

Step 2: Auxiliary variety Z'

To bound the size of $Z(\mathbb{F}_p)$, we will define an auxiliary variety Z' . Let Z' be the variety

cut out by the following three equations in eight variables $y_1, y_2, \dots, y_8$.

$$F(y_1) - F(y_2) - F(y_3) + F(y_4) - F(y_5) + F(y_6) + F(y_7) - F(y_8) = 0 \quad (3.4.3)$$

$$G(y_1) - G(y_2) - G(y_3) + G(y_4) - G(y_5) + G(y_6) + G(y_7) - G(y_8) = 0 \quad (3.4.4)$$

$$R(y_1)R(y_4)R(y_6)R(y_7) - R(y_2)R(y_3)R(y_5)R(y_8) = 0 \quad (3.4.5)$$

Note that $Z'(\mathbb{F}_p)$ lives in $\mathbb{F}_p^8$. The first two defining equations of Z' do not come out of nowhere; the points on the Roth variety Y actually satisfy those two equations. To see this, we manipulate the defining equations of the Roth variety algebraically; consider adding the equations $(3.3.1) - (3.3.2) - (3.3.3) + (3.3.4) + (3.3.9)$ and $(3.3.5) - (3.3.6) + (3.3.7) - (3.3.8) + (3.3.10)$. Therefore, the varieties Z and Z' are closely related: for any $(y_1, y_2, \dots, y_{16}) \in Z(\mathbb{F}_p)$, we have $(y_1, y_2, \dots, y_8) \in Z'(\mathbb{F}_p)$.

We claim that it suffices to show that $|Z'(\mathbb{F}_p)| = O(p^5)$ in order to prove that $|Z(\mathbb{F}_p)| = O(p^6)$. Heuristically, this is because if $|Z'(\mathbb{F}_p)| = O(p^5)$, then we could pick a subset of variables so that the defining equations of Z become “triangular”. More precisely, we can argue as follows.

- For any $(y_1, y_2, \dots, y_{16}) \in Z(\mathbb{F}_p)$, we have $(y_1, y_2, \dots, y_8) \in Z'(\mathbb{F}_p)$ by construction of Z' , hence there are at most $O(p^5)$ choices of $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$.
- For any given $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$, there are p choices of y_9 .
- For any given $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9$, there are at most $O(1)$ choices of y_{11}, y_{10} by equations $(3.3.1), (3.3.5)$.
- For any given $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{11}, y_{10}$, there are at most $O(1)$ choices of y_{12}, y_{15} by equations $(3.3.2), (3.3.6)$.
- For any given $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{11}, y_{10}, y_{12}, y_{15}$, there are at most $O(1)$ choices of y_{13}, y_{16} by equations $(3.3.3), (3.3.7)$.

- For any given $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{11}, y_{10}, y_{12}, y_{15}, y_{13}, y_{16}$, there are at most $O(1)$ choices of y_{14} by equation (3.3.4).
- Thus, there are at most $O(p^5 p) = O(p^6)$ choices of $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8, y_9, y_{11}, y_{10}, y_{12}, y_{15}, y_{13}, y_{16}, y_{14}$. Therefore, we have $|Z(\mathbb{F}_p)| = O(p^6)$.

Hence, we have reduced our problem to point-counting on Z' , which is a much simpler variety compared to the Roth variety.

Step 3: Decomposing Z'

Now we decompose Z' into smooth part and singular parts just like how we decomposed the Roth variety Y before. Let $J_{Z'}(y_1, y_4, y_6)$ be the determinant of the first, fourth and sixth columns of the Jacobian matrix of the defining equations of Z' , that is

$$J_{Z'}(y_1, y_4, y_6) = \begin{vmatrix} F'(y_1) & F'(y_4) & F'(y_6) \\ G'(y_1) & G'(y_4) & G'(y_6) \\ R'(y_1)R(y_4)R(y_6)R(y_7) & R(y_1)R'(y_4)R(y_6)R(y_7) & R(y_1)R(y_4)R'(y_6)R(y_7) \end{vmatrix}.$$

Let $S(y)$ be the logarithmic derivative of $R(y)$, i.e.,

$$S(y) = \frac{R'(y)}{R(y)} \tag{3.4.6}$$

and

$$D(y_1, y_4, y_6) = \begin{vmatrix} F'(y_1) & F'(y_4) & F'(y_6) \\ G'(y_1) & G'(y_4) & G'(y_6) \\ S(y_1) & S(y_4) & S(y_6) \end{vmatrix} \tag{3.4.7}$$

so that we could rewrite

$$J_{Z'}(y_1, y_4, y_6) = R(y_1)R(y_4)R(y_6)R(y_7)D(y_1, y_4, y_6).$$

Define

$$\begin{aligned} Z'_{\text{gen}} &= Z' \cap \{(y_1, y_2, \dots, y_8) \in \mathbb{A}^8 : J_{Z'}(y_1, y_4, y_6) \neq 0\} \\ Z'_i &= Z' \cap \{(y_1, y_2, \dots, y_8) \in \mathbb{A}^8 : R(y_i) = 0\} \quad \text{for } i = 1, 4, 6, 7 \\ Z'_{\text{sp}} &= Z' \cap \{(y_1, y_2, \dots, y_8) \in \mathbb{A}^8 : D(y_1, y_4, y_6) = 0\}. \end{aligned}$$

Note that $Z'(\mathbb{F}_p) = Z'_{\text{gen}}(\mathbb{F}_p) \cup Z'_1(\mathbb{F}_p) \cup Z'_4(\mathbb{F}_p) \cup Z'_6(\mathbb{F}_p) \cup Z'_7(\mathbb{F}_p) \cup Z'_{\text{sp}}(\mathbb{F}_p)$.

The situation is somewhat similar to the decomposition of the Roth variety Y . By construction, the variety Z'_{gen} is smooth and hence has the desired number of $\mathbb{F}_p$ -points. Once again, the “degenerate” subvarieties Z'_1, Z'_4, Z'_6, Z'_7 are of low dimensions due to the strong constraints $R(y_i) = 0$ for $i = 1, 4, 6, 7$; they will not cause us much troubles and can be ignored for now. The main character in the play is Z'_{sp} , and it remains to show that $|Z'_{\text{sp}}(\mathbb{F}_p)| = O(p^5)$.

Step 4: Bounding $|Z'_{\text{sp}}(\mathbb{F}_p)|$

In this step, we will bound $|Z'_{\text{sp}}(\mathbb{F}_p)|$. The strategy is to use $D(y_1, y_4, y_6) = 0$ to constraint variables y_1, y_4, y_6 and the equations (3.4.3), (3.4.4) to constraint variables y_2, y_3, y_5, y_7, y_8 .

First, we will define auxiliary varieties $X_{a,b}$. For any $1 \leq a, b \leq p$, let $X_{a,b}$ be the variety cut out by the following two equations in five variables y_2, y_3, y_5, y_7, y_8 .

$$-F(y_2) - F(y_3) - F(y_5) + F(y_7) - F(y_8) = a \tag{3.4.8}$$

$$-G(y_2) - G(y_3) - G(y_5) + G(y_7) - G(y_8) = b \tag{3.4.9}$$

Note that $X_{a,b}(\mathbb{F}_p)$ live in $\mathbb{F}_p^5$. We claim that $|X_{a,b}(\mathbb{F}_p)| = O(p^3)$ where the implied constant does not depend on a, b .

To see why our claim is true, we will decompose $X_{a,b}$ into smooth part and singular part. Let $J_X(y_7, y_8)$ be the determinant of the last two columns of the Jacobian matrix of the

defining equations of $X_{a,b}$, that is

$$J_X(y_7, y_8) = \begin{vmatrix} F'(y_7) & -F'(y_8) \\ G'(y_7) & -G'(y_8) \end{vmatrix} = -F'(y_7)G'(y_8) + G'(y_7)F'(y_8).$$

Define

$$X_{a,b,\text{gen}} = X_{a,b} \cap \{(y_2, y_3, y_5, y_7, y_8) \in \mathbb{A}^5 : J_X(y_7, y_8) \neq 0\}$$

$$X_{a,b,\text{sp}} = X_{a,b} \cap \{(y_2, y_3, y_5, y_7, y_8) \in \mathbb{A}^5 : J_X(y_7, y_8) = 0\}$$

Note that $X_{a,b}(\mathbb{F}_p) = X_{a,b,\text{gen}}(\mathbb{F}_p) \cup X_{a,b,\text{sp}}(\mathbb{F}_p)$.

By construction, the variety $X_{a,b,\text{gen}}$ is smooth and hence has the expected $\mathbb{F}_p$ -point count, that is $|X_{a,b,\text{gen}}(\mathbb{F}_p)| = O(p^3)$. On the other hand, the defining equations of $X_{a,b,\text{sp}}$ are “triangular”, hence we can deduce that $|X_{a,b,\text{sp}}(\mathbb{F}_p)| = O(p^3)$ via a basic counting argument. Thus, we have $|X_{a,b}(\mathbb{F}_p)| = O(p^3)$.

Finally, for $(y_1, y_2, \dots, y_8) \in Z'_{\text{sp}}(\mathbb{F}_p)$, there are at most $O(p^2)$ choices of y_1, y_4, y_6 since $D(y_1, y_4, y_6)$ is a nonzero rational function by Lemma 3.4.3, and Lang–Weil bound [LW54] (or Schwartz–Zippel lemma) would imply the bounds. (*The calculations showing that $D(y_1, y_4, y_6)$ is nonzero are deferred to Lemma 3.4.3 to streamline the argument; it might be worth pointing out that we crucially use the linear independence of P, Q and constant function 1 in Lemma 3.4.3.*) Fix y_1, y_4, y_6 , for any $(y_1, y_2, \dots, y_8) \in Z'_{\text{sp}}(\mathbb{F}_p)$, the tuples $(y_2, y_3, y_5, y_7, y_8) \in X_{a,b}(\mathbb{F}_p)$ for some a, b by equations (3.4.3) and (3.4.4), hence we have at most $O(p^3)$ choices of y_2, y_3, y_5, y_7, y_8 . Therefore, we conclude that $|Z'_{\text{sp}}(\mathbb{F}_p)| = O(p^5)$.

This ends our hopefully not too long working heuristic. For the missing technical steps and more discussions, see Appendix 6.1. □

Lemma 3.4.3. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions over $\mathbb{Q}$ such that $F(t), G(t)$ and constant function 1 are linearly independent over $\mathbb{Q}$. Define $R(y), S(y)$ and $D(y_1, y_4, y_6)$*

as in (3.4.2), (3.4.6) and (3.4.7) respectively. Then, the rational function $D(y_1, y_4, y_6)$ is nonzero.

Proof. Expanding $D(y_1, y_4, y_6)$ with respect to the first column, we have

$$\begin{aligned} & D(y_1, y_4, y_6) \\ &= F'(y_1) \begin{vmatrix} G'(y_4) & G'(y_6) \\ S(y_4) & S(y_6) \end{vmatrix} - G'(y_1) \begin{vmatrix} F'(y_4) & F'(y_6) \\ S(y_4) & S(y_6) \end{vmatrix} + S(y_1) \begin{vmatrix} F'(y_4) & F'(y_6) \\ G'(y_4) & G'(y_6) \end{vmatrix}. \end{aligned} \quad (3.4.10)$$

Note that

$$\begin{aligned} S(y) &= \frac{R'(y)}{R(y)} \\ &= \frac{1}{R(y)} \left(\frac{F'(y)}{G'(y)} \right)' \\ &= \frac{G'(y)}{F'(y)} \frac{G'(y)F''(y) - F'(y)G''(y)}{(G'(y))^2} \\ &= \frac{F''(y)}{F'(y)} - \frac{G''(y)}{G'(y)} \end{aligned}$$

hence $S(y)$ is the difference of the logarithmic derivatives of $F'(y)$ and $G'(y)$.

If the poles of $F'(y_1)$ and $G'(y_1)$ are different, then $S(y_1)$ would at least have a simple pole since it is the difference of the logarithmic derivatives of $F'(y_1)$ and $G'(y_1)$. Meanwhile, the poles of $F'(y_1)$ and $G'(y_1)$ cannot be simple poles since they are derivatives of meromorphic functions. Therefore, in the expression (3.4.10), the poles of $S(y_1)$ could not be cancelled out by the poles of $F'(y_1)$ and $G'(y_1)$, and hence $D(y_1, y_4, y_6)$ is nonzero.

Similarly, if the zeroes of $F'(y_1)$ and $G'(y_1)$ are different, then $S(y_1)$ would at least have a simple pole since it is the difference of the logarithmic derivatives of $F'(y_1)$ and $G'(y_1)$. Once again, the poles of $S(y_1)$ could not be cancelled out by the poles of $F'(y_1)$ and $G'(y_1)$, and hence $D(y_1, y_4, y_6)$ is nonzero.

If the poles and zeroes of $F'(y_1)$ and $G'(y_1)$ are exactly the same, then F' and G' would only differ up to a scalar, and this would contradict the linear independence of F, G and constant function 1.

As an ending remark, we do have a little detail not checked yet, that is, we need to check that $\begin{vmatrix} F'(y_4) & F'(y_6) \\ G'(y_4) & G'(y_6) \end{vmatrix}$ is nonzero so that it could not cancel out the poles of $S(y_1)$. Suppose the said determinant is zero, then $F'(y_4)/G'(y_4) = F'(y_6)/G'(y_6)$, hence F'/G' would be a constant and this contradicts the linear independence of F, G and constant function 1. $\square$

3.5 Degree lowering

In this section, we will put everything together to prove Theorem 1.3.2. In Sections 3.3 and 3.4, we obtain Gowers norm control for counting operator for corners generated by $F(t), G(t)$, hence we could apply the degree lowering pioneered by Peluse [Pel19] to complete the proof of Theorem 1.3.2. Actually, we need a different version of degree lowering that works for directional Gowers norms, and this version of degree lowering is developed by Kuca [Kuc24a] in his work on multidimensional Szemerédi theorem in finite fields. However, we do not need full strength of Kuca’s work since we start degree lowering with U^2 -norm as opposed to general U^s -norm, for this reason, and for keeping track of the power-saving exponents and the sake of completeness, we reproduce Kuca’s arguments in this section. In this section, we closely follow Kuca’s paper [Kuc24a, Section 6].

Definition 3.5.1 (Eigenfunctions).

1. A function $\chi : \mathbb{F}_p^2 \longrightarrow \mathbb{C}$ is an eigenfunction with respect to the first coordinate if there exists a subset $E \subset \mathbb{F}_p$ and phase functions $\phi : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \psi : \mathbb{F}_p \longrightarrow \mathbb{R}$ such that

$$\chi(x_1, x_2) = 1_E(x_2)e_p(\phi(x_2)x_1)e(\psi(x_2))$$

for all $(x_1, x_2) \in \mathbb{F}_p^2$.

2. A function $\chi : \mathbb{F}_p^2 \longrightarrow \mathbb{C}$ is an eigenfunction with respect to the second coordinate if there exists a subset $E \subset \mathbb{F}_p$ and phase functions $\phi : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \psi : \mathbb{F}_p \longrightarrow \mathbb{R}$ such that

$$\chi(x_1, x_2) = 1_E(x_1)e_p(\phi(x_1)x_2)e(\psi(x_1))$$

for all $(x_1, x_2) \in \mathbb{F}_p^2$.

The following proposition could be regarded as an inverse theorem for $U^2(\mathbb{F}_p \times 0)$ -norm and $U^2(0 \times \mathbb{F}_p)$ -norm.

Proposition 3.5.2. *Let $f : \mathbb{F}_p^2 \rightarrow \mathbb{C}$ be a 1-bounded function.*

1. *Suppose $\|f\|_{U^2(\mathbb{F}_p \times 0)} \geq \delta$, then there exists an eigenfunction with respect to the first coordinate χ such that*

$$\mathbb{E}_{x_1, x_2} f(x_1, x_2) \chi(x_1, x_2) \geq \delta^4$$

and $\mathbb{E}_{x_1} f(x_1, x_2) \chi(x_1, x_2) \geq 0$ for all $x_2 \in \mathbb{F}_p$.

2. *Suppose $\|f\|_{U^2(0 \times \mathbb{F}_p)} \geq \delta$, then there exists an eigenfunction with respect to the second coordinate χ such that*

$$\mathbb{E}_{x_1, x_2} f(x_1, x_2) \chi(x_1, x_2) \geq \delta^4$$

and $\mathbb{E}_{x_2} f(x_1, x_2) \chi(x_1, x_2) \geq 0$ for all $x_1 \in \mathbb{F}_p$.

Proof. The proofs of Proposition 3.5.2.(1) and 3.5.2.(2) are similar, hence we will only prove 3.5.2.(2).

For any x_1 , let $g_{x_1}(x_2) = f(x_1, x_2)$. Note that

$$\begin{aligned} \delta^4 &\leq \|f\|_{U^2(0 \times \mathbb{F}_p)}^4 = \mathbb{E}_{x_1, x_2, h, k} f(x_1, x_2 + h + k) \bar{f}(x_1, x_2 + h) \bar{f}(x_1, x_2 + k) f(x_1, x_2) \\ &= \mathbb{E}_{x_1} \|g_{x_1}\|_{U^2}^4 \\ &= \mathbb{E}_{x_1} \|\widehat{g_{x_1}}\|_{l^4}^4. \end{aligned}$$

Observe that

$$\begin{aligned} \|\widehat{g_{x_1}}\|_{l^4}^4 &= \sum_{\xi} |\widehat{g_{x_1}}(\xi)|^4 \leq \|\widehat{g_{x_1}}\|_{\infty}^2 \sum_{\xi} |\widehat{g_{x_1}}(\xi)|^2 \\ &= \|\widehat{g_{x_1}}\|_{\infty}^2 \|g_{x_1}\|_2^2 \\ &\leq \|\widehat{g_{x_1}}\|_{\infty}^4. \end{aligned}$$

Hence, for every x_1 , there exists a frequency ξ_{x_1} such that

$$\delta^4 \leq \mathbb{E}_{x_1} |\widehat{g_{x_1}}(\xi_{x_1})| = \mathbb{E}_{x_1} \left| \mathbb{E}_{x_2} f(x_1, x_2) e_p(-\xi_{x_1} x_2) \right|.$$

Choosing phase functions $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_p, \psi : \mathbb{F}_p \rightarrow \mathbb{R}$ such that

$$\left| \mathbb{E}_{x_2} f(x_1, x_2) e_p(-\xi_{x_1} x_2) \right| = \mathbb{E}_{x_2} f(x_1, x_2) e_p(\phi(x_1) x_2) e(\psi(x_1))$$

completes the proof. (Note that in the definition of eigenfunctions, there is a characteristic function 1_E for some subset E , here we can choose $E = \mathbb{F}_p$.) $\square$

The following proposition is an asymptotic formula for two term progressions, which is needed for induction.

Proposition 3.5.3. *Let $F(t) \in \mathbb{Q}(t)$ be a rational function over $\mathbb{Q}$.*

1. *For all 1-bounded functions $f_0, f_1 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$, we have*

$$\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \right) + O(p^{-\frac{1}{2}}).$$

2. *For all 1-bounded functions $f_0, f_1 : \mathbb{F}_p^2 \rightarrow \mathbb{C}$, we have*

$$\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1, x_2 + F(y)) = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(x_1, a) \right) + O(p^{-\frac{1}{2}}).$$

Proof. The proofs of Proposition 3.5.3.(1) and 3.5.3.(2) are similar, hence we will only prove Proposition 3.5.3.(1).

Note that after fixing x_2 , the counting operator reduces to the one dimensional case, and we can invoke Proposition 2.5.1. Hence, we have

$$\begin{aligned} \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) &= \mathbb{E}_{x_2} \left(\mathbb{E}_{x_1, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) \right) \\ &= \mathbb{E}_{x_2} \left(\mathbb{E}_{x_1} f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) + O(p^{-\frac{1}{2}}) \right) \\ &= \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \right) + O(p^{-\frac{1}{2}}) \end{aligned}$$

$\square$

The following theorem contains the induction process for degree lowering. Essentially, we will induct on the number of the eigenfunctions in the counting operators. That being said, we choose to write the proof not in the exact format of an induction so that the notations could be less dense. Also, note that Theorem 3.5.4.(3) is same as Theorem 1.3.2.

Theorem 3.5.4. *Let $F(t), G(t) \in \mathbb{Q}(t)$ be rational functions such that $F(t), G(t)$ and the constant function 1 are linearly independent over $\mathbb{Q}$, and $f_0, f_1, f_2 : \mathbb{F}_p^2 \longrightarrow \mathbb{C}$ be 1-bounded functions.*

1. *Suppose f_1 is an eigenfunction with respect to the first coordinate and f_2 is an eigenfunction with respect to the second coordinate, then we have*

$$\begin{aligned} \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O_{P, Q}(p^{-\frac{1}{2}}). \end{aligned}$$

2. *Suppose f_2 is an eigenfunction with respect to the second coordinate, then we have*

$$\begin{aligned} \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O_{P, Q}(p^{-\frac{1}{640}}). \end{aligned}$$

3. *For all 1-bounded functions $f_0, f_1, f_2 : \mathbb{F}_p^2 \longrightarrow \mathbb{C}$, we have*

$$\begin{aligned} \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \\ = \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_1(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O_{P, Q}(p^{-\frac{1}{40960}}). \end{aligned}$$

Remark 3.5.5. In the proof of Theorem 3.5.4, we actually do not use the full power of the degree lowering since we only lower the norms from U^2 to U^1 . Indeed, we do not need the most essential part of the degree lowering because we are dealing with U^2 -norm as opposed to general U^s -norm.

Proof of Theorem 3.5.4.(1). This will be the base case for the induction for Theorem 3.5.4. Since f_1, f_2 are eigenfunctions, there exist subsets $E, E' \subset \mathbb{F}_p$, phase functions $\phi : \mathbb{F}_p \longrightarrow \mathbb{F}_p, \alpha : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ and $\psi : \mathbb{F}_p \longrightarrow \mathbb{R}, \beta : \mathbb{F}_p \longrightarrow \mathbb{R}$ such that

$$\begin{aligned} f_1(x_1, x_2) &= 1_E(x_2)e_p(\phi(x_2)x_1)e(\psi(x_2)) \\ f_2(x_1, x_2) &= 1_{E'}(x_1)e_p(\alpha(x_1)x_2)e(\beta(x_1)) \end{aligned}$$

for all $(x_1, x_2) \in \mathbb{F}_p^2$.

Expanding the counting operator, we have

$$\begin{aligned} &\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2)f_1(x_1 + F(y), x_2)f_2(x_1, x_2 + G(y)) \\ &= \mathbb{E}_{x_1, x_2} f_0(x_1, x_2)1_E(x_2)e_p(\phi(x_2)x_1)e(\psi(x_2))1_{E'}(x_1)e_p(\alpha(x_1)x_2)e(\beta(x_1)) \mathbb{E}_y e_p(\phi(x_2)F(y) + \alpha(x_1)G(y)) \end{aligned}$$

By Bombieri's bound on single variable exponential sums in finite fields with rational function phases (Lemma 2.5.2) we have

$$\left| \mathbb{E}_y e_p(\phi(x_2)F(y) + \alpha(x_1)G(y)) \right| \ll p^{-1/2}$$

when $\phi(x_2) \neq 0$ or $\alpha(x_1) \neq 0$.

Therefore, the counting operator is equal to

$$\mathbb{E}_{x_1, x_2} f_0(x_1, x_2)1_E(x_2)e(\psi(x_2))1_{\phi(x_2)=0}1_{E'}(x_1)e(\beta(x_1))1_{\alpha(x_1)=0} + O(p^{-1/2}).$$

To complete the proof, note that the directional averages of eigenfunctions have a special form, i.e.,

$$\begin{aligned} \mathbb{E}_{x_1} f_1(x_1, x_2) &= \mathbb{E}_{x_1} 1_E(x_2)e_p(\phi(x_2)x_1)e(\psi(x_2)) = 1_E(x_2)e(\psi(x_2))1_{\phi(x_2)=0} \\ \mathbb{E}_{x_2} f_2(x_1, x_2) &= \mathbb{E}_{x_2} 1_{E'}(x_1)e_p(\alpha(x_1)x_2)e(\beta(x_1)) = 1_{E'}(x_1)e(\beta(x_1))1_{\alpha(x_1)=0}. \end{aligned}$$

□

Proof of Theorem 3.5.4.(2). First, we would like to de-mean f_2 with respect to variable x_2 by splitting $f_2(x_1, x_2) = (f_2(x_1, x_2) - \mathbb{E}_a f_2(x_1, a)) + \mathbb{E}_a f_2(x_1, a)$. The term $\mathbb{E}_a f_2(x_1, a)$ contributes to the main term since by Proposition 3.5.3.(1), we have

$$\begin{aligned}
& \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) \mathbb{E}_a f_2(x_1, a) \\
&= \mathbb{E}_{x_1, x_2, y} \left(f_0(x_1, x_2) \mathbb{E}_a f_2(x_1, a) \right) f_1(x_1 + F(y), x_2) \\
&= \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a f_2(x_1, a) \right) \mathbb{E}_b f_1(b, x_2) + O(p^{-1/2}) \\
&= \mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_b f_1(b, x_2) \mathbb{E}_a f_2(x_1, a) \right) + O(p^{-1/2}).
\end{aligned}$$

By replacing $f_2(x_1, x_2)$ by $f_2(x_1, x_2) - \mathbb{E}_a f_2(x_1, a)$, we can assume the directional average of f_2 with respect to x_2 is zero, that is $\mathbb{E}_{x_2} f_2(x_1, x_2) = 0$. (Also, note that $f_2(x_1, x_2) - \mathbb{E}_a f_2(x_1, a)$ is still an eigenfunction with respect to the second variable.)

Now, given 1-bounded functions f_0, f_1, f_2 where f_2 is an eigenfunction with respect to the second coordinate with $\mathbb{E}_{x_2} f_2(x_1, x_2) = 0$, let

$$\delta = \left| \mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) f_2(x_1, x_2 + G(y)) \right|$$

be the quantity that we would like to upper bound. Define the dual function

$$A_1(x_1, x_2) = \mathbb{E}_y f_0(x_1 - F(y), x_2) f_2(x_1 - F(y), x_2 + G(y)).$$

Note that

$$\delta = \left| \mathbb{E}_{x_1, x_2, y} f_1(x_1, x_2) A_1(x_1, x_2) \right| \leq \left(\mathbb{E}_{x_1, x_2} |A_1(x_1, x_2)|^2 \right)^{1/2}.$$

Expanding $|A_1(x_1, x_2)|^2$, we have

$$\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) \overline{A_1}(x_1 + P(y), x_2) f_2(x_1, x_2 + Q(y)) \geq \delta^2.$$

By algebraic geometry PET induction (Theorem 3.3.9) and the dimension estimates for the Roth variety (Theorem 3.4.2), we deduce that

$$\|A_1\|_{U^2(\mathbb{F}_p \times 0)}^{1/4} \gg \delta^2.$$

By inverse theorem for $U^2(\mathbb{F}_p \times 0)$ (Proposition 3.5.2), there exists an eigenfunction with respect to the first coordinate χ such that

$$\mathbb{E}_{x_1, x_2} A_1(x_1, x_2) \chi(x_1, x_2) \gg \delta^{32}$$

and $\mathbb{E}_{x_1} A_1(x_1, x_2) \chi(x_1, x_2) \geq 0$ for all $x_2 \in \mathbb{F}_p$.

Let

$$W = \{x_2 \in \mathbb{F}_p : \mathbb{E}_{x_1} A_1(x_1, x_2) \chi(x_1, x_2) \gg \delta^{32}/2\},$$

then by the pigeonhole principle, we have $\frac{|W|}{p} \gg \delta^{32}$. Hence, we deduce that

$$\mathbb{E}_{x_2} 1_W(x_2) \mathbb{E}_{x_1} A_1(x_1, x_2) \chi(x_1, x_2) \gg \delta^{64},$$

which is

$$\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) \chi(x_1 + F(y), x_2) 1_W(x_2) f_2(x_1, x_2 + G(y)) \gg \delta^{64}.$$

By induction on Theorem 3.5.4.(1) for the functions $f_0, \chi 1_W, f_2$, we have

$$\mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2) \mathbb{E}_a (\chi 1_W)(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O(p^{-1/2}) \gg \delta^{64}.$$

Note that the desired estimate in Theorem 3.5.4.(2) already holds when $p^{-1/2} \gg \delta^{64}$, since we are in the mean zero case. Thus, without loss of generality, we may eliminate the error term $O(p^{-1/2})$ in the above estimate. By Cauchy–Schwarz inequality in variable x_2 , we have

$$\mathbb{E}_{x_2} \left| \mathbb{E}_a (\chi 1_W)(a, x_2) \right|^2 \gg \delta^{128}.$$

Since χ is an eigenfunction with respect to the first coordinate, there exists a subset $E \subset \mathbb{F}_p$, phase functions $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_p, \psi : \mathbb{F}_p \rightarrow \mathbb{R}$ such that $\chi(x_1, x_2) = 1_E(x_2) e_p(\phi(x_2) x_1) e(\psi(x_2))$. Therefore, we have

$$\mathbb{E}_{x_2} \left| \mathbb{E}_a 1_E(x_2) e_p(\phi(x_2) a) e(\psi(x_2)) 1_W(x_2) \right|^2 \gg \delta^{128},$$

which is

$$\mathbb{E}_{x_2} \left| 1_E(x_2) 1_W(x_2) 1_{\phi(x_2)=0} \right|^2 \gg \delta^{128}.$$

By definition of W , we deduce that

$$\mathbb{E}_{x_2} 1_E(x_2) 1_W(x_2) 1_{\phi(x_2)=0} \mathbb{E}_{x_1} A_1(x_1, x_2) \chi(x_1, x_2) \gg \delta^{160},$$

which is

$$\mathbb{E}_{x_2} 1_E(x_2) 1_W(x_2) 1_{\phi(x_2)=0} e(\psi(x_2)) \mathbb{E}_{x_1} A_1(x_1, x_2) \gg \delta^{160}.$$

Applying Cauchy–Schwarz inequality in x_2 , we have successfully passed from $U^2(\mathbb{F}_p \times 0)$ -norm to $U^1(\mathbb{F}_p \times 0)$ -norm and lowered the degree, i.e.,

$$\delta^{320} \ll \mathbb{E}_{x_2} \left| \mathbb{E}_{x_1} A_1(x_1, x_2) \right|^2 = \|A_1\|_{U^1(\mathbb{F}_p \times 0)}^2$$

Finally, expanding the squares $|\mathbb{E}_{x_1} A_1(x_1, x_2)|^2$, we have

$$\mathbb{E}_{x_1, x_2, y} \left(f_0(x_1, x_2) f_2(x_1, x_2 + Q(y)) \mathbb{E}_a \overline{A_1}(a, x_2) \right) \gg \delta^{320},$$

By the asymptotic formula for two term progressions (Proposition 3.5.3.(2)) for the functions $f_0(x_1, x_2) \mathbb{E}_a \overline{A_1}(a, x_2)$ and $f_2(x_1, x_2)$, we conclude

$$\mathbb{E}_{x_1, x_2, y} \left(f_0(x_1, x_2) \mathbb{E}_a \overline{A_1}(a, x_2) \mathbb{E}_b f_2(x_1, b) \right) + O(p^{-1/2}) \gg \delta^{320}$$

The main term is zero since we already eliminated the mean of f_2 with respect to variable x_2 in the beginning of the argument, hence we have $\delta^{320} \ll p^{-1/2}$ which is equivalent to $\delta \ll p^{-1/640}$.

□

Proof of Theorem 3.5.4.(3) and Theorem 1.3.2. The proof of Theorem 3.5.4.(3) is similar to the proof of Theorem 3.5.4.(2), hence we would only briefly indicate the changes. Basically, we reverse the roles of x_1 and x_2 and induct on Theorem 3.5.4.(2). Here is a list of the changes.

- We would de-mean f_1 with respect to x_1 .
- The dual function would be $A_2(x_1, x_2) = \mathbb{E}_y f_0(x_1, x_2 - G(y)) f_1(x_1 + F(y), x_2 - G(y))$.
- We have $\|A_2\|_{U^2(0 \times \mathbb{F}_p)}$ instead of $\|A_1\|_{U^2(\mathbb{F}_p \times 0)}$ since we would invoke Theorem 3.3.2.
- We would invoke Proposition 3.5.2.(2) to get an eigenfunction with respect to the second coordinate χ .
- The definition of W would be $\{x_1 \in \mathbb{F}_p : \mathbb{E}_{x_2} A_2(x_1, x_2) \chi(x_1, x_2) \gg \delta^{32}/2\}$.
- We would induct on Theorem 3.5.4.(2) instead of Theorem 3.5.4.(1) for the averages

$$\mathbb{E}_{x_1, x_2, y} f_0(x_1, x_2) f_1(x_1 + F(y), x_2) \chi(x_1, x_2 + G(y)) 1_W(x_1) \gg \delta^{64},$$

hence we would get an error term $O(p^{-1/640})$ instead of $O(p^{-1/2})$, this would lead to the bound $\delta \ll p^{-1/(640 \cdot 64)} = p^{-1/40960}$.

□

3.6 Higher dimensions

A natural question is whether the method in this chapter can be extended to higher dimensional cases? We can obtain some results on “higher dimensional corners with two legs” by an immediate application of Theorem 1.3.2. Say, take “three dimensional corners with two legs”

$$(x_1, x_2, x_3), (x_1 + F(y), x_2, x_3), (x_1, x_2 + G(y), x_3)$$

as an example. Fixing x_3 and applying Theorem 1.3.2, we have

$$\begin{aligned} & \mathbb{E}_{x_1, x_2, x_3, y} f_0(x_1, x_2, x_3) f_1(x_1 + F(y), x_2, x_3) f_2(x_1, x_2 + G(y), x_3) \\ &= \mathbb{E}_{x_3} \left(\mathbb{E}_{x_1, x_2} \left(f_0(x_1, x_2, x_3) \mathbb{E}_a f_1(a, x_2, x_3) \mathbb{E}_b f_2(x_1, b, x_3) \right) + O_{F,G}(p^{-\frac{1}{40960}}) \right) \\ &= \mathbb{E}_{x_1, x_2, x_3} \left(f_0(x_1, x_2, x_3) \mathbb{E}_a f_1(a, x_2, x_3) \mathbb{E}_b f_2(x_1, b, x_3) \right) + O_{F,G}(p^{-\frac{1}{40960}}). \end{aligned}$$

More generally, we can deduce an asymptotic formula for “higher dimensional corners with two legs”

$$(x_1, x_2, \dots, x_n), (x_1, x_2, \dots, x_i + F(y), \dots, x_n), (x_1, x_2, \dots, x_j + G(y), \dots, x_n)$$

where $i \neq j$ similarly.

The more interesting cases are general higher dimensional corners, such as the three dimensional corners

$$(x_1, x_2, x_3), (x_1 + F(y), x_2, x_3), (x_1, x_2 + G(y), x_3), (x_1, x_2, x_3 + H(y)) \quad (3.6.1)$$

where F, G, H are rational functions with some linear independence assumption. Suppose one could generalize the method in this chapter to (3.6.1), then it would immediately imply a Szemerédi theorem on the one dimensional progressions

$$x, x + F(y), x + G(y), x + H(y)$$

and the proof would be Fourier analytically based. However, even in the case

$$x, x + y, x + y^2, x + y^3,$$

such a Fourier analytic proof is still unknown (but other approach is available, see [Pel19]). Hence, it is likely that one would need new ideas for such generalizations.

CHAPTER 4

The density version of quadratic Waring's problem and the quadratic Waring–Goldbach problem

4.1 Overview

In this chapter, we follow the framework of [Lim25a] to reproduce the proofs of Theorem 1.4.3, Theorem 1.5.1 and Theorem 1.5.3.

The key to Theorem 1.4.3 is the following local result. For any integer $s \geq 5$, define

$$d_s := \begin{cases} \frac{9}{10} & \text{if } s = 5 \\ \frac{5}{6} & \text{if } s = 6 \\ \frac{s+13}{4s} & \text{if } 7 \leq s \leq 12 \\ \frac{1}{2} & \text{if } s \geq 13 \end{cases}$$

Note that $D_s \geq d_s \geq 1/2$ and $d_s \geq (s+13)/(4s)$ for all s . Similar as before, for any positive integer W , denote the squares in $(\mathbb{Z}/W)^\times$ by $(\mathbb{Z}/W)^{\times(2)}$.

Theorem 4.1.1. *Let $s \geq 5$ be an integer, and W be a square free integer. Assume $(2 \cdot 3 \cdot 5, W) = 1$ when $s \geq 6$, and $(2 \cdot 3 \cdot 5 \cdot 7, W) = 1$ when $s = 5$. Let $f_j : (\mathbb{Z}/W)^{\times(2)} \rightarrow [0, 1]$ be functions for $1 \leq j \leq s$ with*

$$\frac{1}{s}(\mathbb{E}[f_1] + \mathbb{E}[f_2] + \dots + \mathbb{E}[f_s]) > d_s \text{ and } \mathbb{E}[f_j] \neq 0 \text{ for all } 1 \leq j \leq s.$$

Then, for all $y \in \mathbb{Z}/W$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/W)^{\times(2)}$ such that

$$\frac{1}{s}(f_1(x_1) + f_2(x_2) + \dots + f_s(x_s)) > d_s \text{ and } f_j(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

The essential distinction between Theorem 1.5.1 and Theorem 4.1.1 is Theorem 1.5.1 excludes considerably more amount of small primes. Due to this distinction, their proofs are fundamentally different.

4.1.1 Sketch of the proofs

All density type theorems, including ours, crucially rely on the transference principle pioneered by Green and Tao in their celebrated proof that primes contain arbitrarily long arithmetic progressions [Gre05], [GT08].

One of the key ingredients needed for the transference principle is restriction estimates. For Theorem 1.5.1, since we are working over cyclic rings $\mathbb{Z}/W$, we need restriction estimates for squares in $\mathbb{Z}/W$ instead of the classical Bourgain's restriction estimates for squares in $\mathbb{Z}$ [Bou89]. Surprisingly, the proofs are different in the cyclic ring setting and in the integer setting—the squares are denser in cyclic rings, but one has extra product structure of the groups.

For Theorem 1.4.3, our proof is based on a variant of the combinatorial inequalities developed by Shao [Sha14] and by Lacey, Mousavi, Rahimi and Vempati [LMR24]. The combinatorial inequality is inductive in nature, and the base cases are handled by linear programming with computer assistance.

4.1.2 Future directions

The main purpose of this chapter is demonstrating the methods as a proof of concept, rather than pursuing the best density that can be obtained by the methods. There are certainly

rooms for further improvements. First, we expect the density threshold $\sqrt{D_s}$ can be improved to D_s by not using certain smooth weights for majorants (see Appendix 6.3). Second, the numerical linear programming computations in Section 4.7 can be scaled up to lead to better density.

In another direction, we believe Theorem 1.5.1 and Theorem 1.4.3 can be generalized to higher powers. We also expect the techniques for Theorem 1.4.3 are applicable for the setting of Waring's problem.

Remark 4.1.2. To prove results like Theorem 4.1.1, in principle, one can use Theorem 1.5.1 to handle large primes, formulate the problem for medium primes in linear programming, and deal with small primes by hand. However, the number of "medium" primes here is astronomical, even for computers.

Remark 4.1.3. By classical estimates in number theory and union bounds, it is possible to prove Theorem 1.4.3 for density threshold extremely close to 1.

4.1.3 Road map

This chapter is organized as follows. We review some basic facts about the squares in $\mathbb{Z}/W$ in Section 4.2. Section 4.3 contains the restriction estimates for squares in $\mathbb{Z}/W$. Section 4.4 is about some auxiliary additive combinatorics results. We use the transference principle to prove Theorem 1.5.1 in Section 4.5. The examples for Theorem 1.5.3 are constructed in Section 4.6.

The key combinatorial inequality for Theorem 1.4.3 is established in Section 4.7. Section 4.8 extends Theorem 4.1.1 to all moduli. For self-containedness, we include two appendices. Appendix 6.2 contains some Gauss sum type results and Appendix 6.3 is about how to reduce Theorem 1.4.3 to Theorem 4.8.2.

4.2 Preliminaries

In this section, we will clarify our notation and review some basic facts about the squares in $\mathbb{Z}/W$. A comprehensive discussion on this subject can be found in the excellent book [IK04, Chapter 3].

4.2.1 Squares in $\mathbb{Z}/W$

Let W be a positive integer. Denote the squares in $\mathbb{Z}/W$ by $(\mathbb{Z}/W)^{(2)}$, more formally

$$(\mathbb{Z}/W)^{(2)} = \{x \in \mathbb{Z}/W : x = y^2 \text{ for some } y \in \mathbb{Z}/W\}$$

Similarly, we define

$$(\mathbb{Z}/W)^{\times(2)} = \{x \in \mathbb{Z}/W : x = y^2 \text{ for some } y \in (\mathbb{Z}/W)^\times\}$$

Let $S(W)$ be the number of squares in $\mathbb{Z}/W$, that is

$$S(W) = |(\mathbb{Z}/W)^{(2)}|.$$

We will use the convenient notation $\sum_{x=\square \bmod W}$ to denote the summation over the squares in $\mathbb{Z}/W$, so $\sum_{x=\square \bmod W}$ and $\sum_{x \in (\mathbb{Z}/W)^{(2)}}$ are interchangeable.

Now we recall some classical and well-known results regarding the squares. Here and throughout, p will always be a prime number. We start with the number of squares in $\mathbb{Z}/p^n$.

Proposition 4.2.1. *Let $p \geq 3$ and $n \geq 1$, then*

$$S(p^n) = \begin{cases} \frac{1}{2} \cdot \frac{p^{n+1} - 1}{p + 1} + 1 & \text{when } n \text{ is odd} \\ \frac{1}{2} \cdot \frac{p(p^n - 1)}{p + 1} + 1 & \text{when } n \text{ is even} \end{cases}$$

In particular, we have $S(p^n) \asymp p^n$.

Interested readers can find a proof of Proposition 4.2.1 in [Sta96]. In fact, instead of a closed form formula, we will only need $S(p^n) = \frac{1}{2}p^n + O(p^{n-1})$, which can be derived more straightforwardly by looking at the squares in $(\mathbb{Z}/p^n)^\times$. Intuitively, Proposition 4.2.1 says that roughly half of the elements of $\mathbb{Z}/p^n$ are squares. By Chinese remainder theorem, $(\mathbb{Z}/W_1W_2)^{(2)}$ can be identified with $(\mathbb{Z}/W_1)^{(2)} \times (\mathbb{Z}/W_2)^{(2)}$ if W_1 and W_2 are coprime, hence Proposition 4.2.1 also provides a formula for $S(W)$ for general modulus W . The next proposition is a Gauss sum type result.

Proposition 4.2.2. *Let $p \geq 3, n \geq 1$ and $t \in \mathbb{Z}$, then*

$$\left| \sum_{x=\square \bmod p^n} e_{p^n}(tx) \right| \ll (t, p^n) p^{1/2}$$

where the implied constant does not depend on p, n or t .

The formulation of Proposition 4.2.2 is slightly different than the Gauss sum type results in literature. To save readers' effort, we briefly explain how to derive Proposition 4.2.2 from standard references in Appendix 6.2. Intuitively, the term (t, p^n) corresponds to the repetition of some elements in the sum, and the term $p^{1/2}$ corresponds to the cancellation.

4.2.2 Other notation

In this chapter, the implied constants in the asymptotic notation $\ll, \gg, \asymp, O, o$ are allowed to depend on s, θ . We will continue to use the Fourier analysis notation listed in Section 2.2 for Fourier analysis on finite abelian groups.

We would also need Fourier analysis on $\mathbb{Z}$ and $\mathbb{R}/\mathbb{Z}$ in this chapter. For functions on $\mathbb{Z}$, the l^q -norms are taken with respect to counting measure. For functions on $\mathbb{R}/\mathbb{Z}$, the L^q -norms are taken with respect to Lebesgue measure. If f, g are finitely supported functions on $\mathbb{Z}$, then the Fourier transform is defined to be

$$\widehat{f}(\alpha) = \sum_{n \in \mathbb{Z}} f(n) e(n\alpha)$$

and the convolution is defined to be

$$f * g(x) = \sum_{\substack{y, z \in \mathbb{Z} \\ y+z=x}} f(y)g(z)$$

Finally, we will use $\|\cdot\|_{\mathbb{R}/\mathbb{Z}}$ to denote the distance to the nearest integer.

4.3 Restriction estimates

In this section, we formulate and prove restriction estimates for squares in $\mathbb{Z}/W$, which is an ingredient needed for the transference principle. It can be viewed as an analog of Bourgain's restriction estimates for squares in integers [Bou89] over $\mathbb{Z}/W$. However, the proof of the cases over $\mathbb{Z}/W$ and that of the cases over integers are somewhat different, since one can explore the product structure of $\mathbb{Z}/W$ via Chinese remainder theorem.

Recall that we denote the number of squares in $\mathbb{Z}/W$ by $S(W)$, and the notation $\sum_{x=\square \bmod W}$ means the summation over the squares in $\mathbb{Z}/W$. See Section 4.2 for more on our notation.

Definition 4.3.1. *Let W be a positive integer and $q \geq 2$ be a real number. Define $C_q(W)$ to be the best constant such that*

$$\left(\sum_{t \bmod W} \left\| \sum_{x=\square \bmod W} a_x e_W(tx) \right\|_H^q \right)^{1/q} \leq C_q(W) S(W)^{1/2} \left(\sum_{x=\square \bmod W} \|a_x\|_H^2 \right)^{1/2}$$

for all finite dimensional Hilbert space H with norm $\|\cdot\|_H$ and all vectors $a_x \in H$.

Remark 4.3.2. The constants $C_q(W)$ are defined for vector-valued restriction estimates.

When specializing to scalars, they give more “natural” inequalities:

$$\left(\sum_{t \bmod W} \left| \sum_{x=\square \bmod W} a_x e_W(tx) \right|^q \right)^{1/q} \leq C_q(W) S(W)^{1/2} \left(\sum_{x=\square \bmod W} |a_x|^2 \right)^{1/2}$$

for all complex numbers a_x . Indeed, only this form of restriction estimates would be needed for the proof of our main theorem. However, the vector-valued formulation is crucial for the multiplicativity of $C_q(W)$ (Lemma 4.3.4).

The purpose of this section is to prove the following theorem, which says that one has satisfactory restriction estimates for squares in $\mathbb{Z}/W$ for $q > 4$.

Theorem 4.3.3. *Let $q > 4$ be a real number. There exists a constant $M(q)$ depending only on q such that the following holds.*

Suppose $W = \prod_i p_i^{n_i}$ is a positive integer with $p_i \geq M(q)$ for all i , then

$$C_q(W) = O_q(1).$$

As a remark, the requirement that $s \geq 5$ in Theorem 1.5.1 and Theorem 1.4.3 is due to the critical exponent of restriction estimates for squares in $\mathbb{Z}/W$. The proof of Theorem 4.3.3 would be deferred to the end of the section. First, we need the following lemma to reduce to the cases of prime power moduli.

Lemma 4.3.4. *Let W_1, W_2 be two coprime positive integers, then $C_q(W_1 W_2) = C_q(W_1) C_q(W_2)$.*

Proof. First, we will show that $C_q(W_1 W_2) \leq C_q(W_1) C_q(W_2)$. Since W_1 and W_2 are coprime, we have $\beta_2 W_1 + \beta_1 W_2 = 1$ for some integers β_1, β_2 with $(\beta_1, W_1) = (\beta_2, W_2) = 1$. Hence, we have multiplicative property $e_W(u) = e_W((\beta_2 W_1 + \beta_1 W_2)u) = e_{W_1}(\beta_1 u) e_{W_2}(\beta_2 u)$ for all u .

Furthermore, by Chinese remainder theorem, we can identify $\mathbb{Z}/W$ with $\mathbb{Z}/W_1 \times \mathbb{Z}/W_2$ and $(\mathbb{Z}/W)^{(2)}$ with $(\mathbb{Z}/W_1)^{(2)} \times (\mathbb{Z}/W_2)^{(2)}$. Under these identifications, we will write $x = (x_1, x_2)$ for $x \in \mathbb{Z}/W$ as our notation. Thus, we have

$$\begin{aligned} & \left(\sum_{t \bmod W} \left\| \sum_{x = \square \bmod W} a_x e_W(tx) \right\|_H^q \right)^{1/q} \\ &= \left(\sum_{t_1 \bmod W_1} \sum_{t_2 \bmod W_2} \left\| \sum_{x_2 = \square \bmod W_2} \sum_{x_1 = \square \bmod W_1} a_{(x_1, x_2)} e_{W_1}(\beta_1 t_1 x_1) e_{W_2}(\beta_2 t_2 x_2) \right\|_H^q \right)^{1/q}. \end{aligned}$$

By definition of $C_q(W_2)$, the expression above is bounded by

$$C_q(W_2)S(W_2)^{1/2} \left(\sum_{t_1 \bmod W_1} \left(\sum_{x_2=\square \bmod W_2} \left\| \sum_{x_1=\square \bmod W_1} a_{(x_1, x_2)} e_{W_1}(t_1 x_1) \right\|_H^2 \right)^{q/2} \right)^{1/q}. \quad (4.3.1)$$

To proceed, we will work over the vector space $H^{(\mathbb{Z}/W_2)^{(2)}}$. Let $b_{x_1} = (a_{(x_1, x_2)})_{x_2 \in (\mathbb{Z}/W_2)^{(2)}} \in H^{(\mathbb{Z}/W_2)^{(2)}}$. Note that

$$\left\| \sum_{x_1=\square \bmod W_1} b_{x_1} e_{W_1}(t_1 x_1) \right\|_{H^{(\mathbb{Z}/W_2)^{(2)}}} = \left(\sum_{x_2=\square \bmod W_2} \left\| \sum_{x_1=\square \bmod W_1} a_{(x_1, x_2)} e_{W_1}(t_1 x_1) \right\|_H^2 \right)^{1/2}.$$

Hence, we deduce that (4.3.1) is bounded by

$$\begin{aligned} & C_q(W_2)S(W_2)^{1/2} C_q(W_1)S(W_1)^{1/2} \left(\sum_{x_1=\square \bmod W_1} \|b_{x_1}\|_{H^{(\mathbb{Z}/W_2)^{(2)}}}^2 \right)^{1/2} \\ &= C_q(W_1)C_q(W_2)S(W)^{1/2} \left(\sum_{x_1=\square \bmod W_1} \sum_{x_2=\square \bmod W_2} \|a_{(x_1, x_2)}\|_H^2 \right)^{1/2}, \end{aligned}$$

and this concludes that $C_q(W) \leq C_q(W_1)C_q(W_2)$.

Next, we will show that $C_q(W_1)C_q(W_2) \leq C_q(W)$. Suppose the worst examples for $C_q(W_1)$ and $C_q(W_2)$ are given by some vectors $a_{x_1}^{(1)}$ and $a_{x_2}^{(2)}$ in some vector spaces H_1 and H_2 respectively. Considering $a_{x_1}^{(1)} \otimes a_{x_2}^{(2)}$ in the tensor product $H_1 \otimes H_2$, we have

$$\begin{aligned} & \sum_{t_1 \bmod W_1} \sum_{t_2 \bmod W_2} \left\| \sum_{x_1=\square \bmod W_1} \sum_{x_2=\square \bmod W_2} a_{x_1}^{(1)} \otimes a_{x_2}^{(2)} e_{W_1}(t_1 x_1) e_{W_2}(t_2 x_2) \right\|_{H_1 \otimes H_2}^q \\ &= \left(\sum_{t_1 \bmod W_1} \left\| \sum_{x_1=\square \bmod W_1} a_{x_1}^{(1)} e_{W_1}(t_1 x_1) \right\|_{H_1}^q \right) \left(\sum_{t_2 \bmod W_2} \left\| \sum_{x_2=\square \bmod W_2} a_{x_2}^{(2)} e_{W_2}(t_2 x_2) \right\|_{H_2}^q \right) \end{aligned}$$

since $\|v_1 \otimes v_2\|_{H_1 \otimes H_2} = \|v_1\|_{H_1} \|v_2\|_{H_2}$ for all $v_1 \in H_1, v_2 \in H_2$. This implies that $C_q(W_1)C_q(W_2) \leq C_q(W)$.

□

The next proposition is the key to the proof of Theorem 4.3.3. It is about restriction estimates for squares in $\mathbb{Z}/p^n$.

Proposition 4.3.5. *Let $q \geq 4$ be a real number, we have*

$$C_q(p^n) \leq 1 + O_q \left(\frac{1}{p^{\frac{q}{2}-1}} \right)$$

for all sufficiently large (depending on q) primes p and all positive integers n . The implied constant for big O only depends on q but not p and n .

Proof of Proposition 4.3.5 for $q = 4$. Throughout the proof, we will assume p is sufficiently large. Expanding the powers, we have

$$\begin{aligned} \sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H^4 &= \sum_{t \bmod p^n} \sum_{x,y,z,w=\square \bmod p^n} \langle a_x, a_y \rangle_H \langle a_z, a_w \rangle_H e_{p^n}(t(x-y+z-w)) \\ &= p^n \sum_{\substack{x,y,z,w=\square \bmod p^n \\ x-y=w-z}} \langle a_x, a_y \rangle_H \langle a_z, a_w \rangle_H. \end{aligned}$$

Rewrite the expression above as

$$p^n \sum_{l \bmod p^n} \sum_{\substack{x,y,z,w=\square \bmod p^n \\ x-y=l=w-z}} \langle a_x, a_y \rangle_H \langle a_z, a_w \rangle_H = p^n \sum_{l \bmod p^n} \left| \sum_{\substack{x,y=\square \bmod p^n \\ x-y=l}} \langle a_x, a_y \rangle_H \right|^2,$$

and we will divide into two cases according to the invertibility of l .

First, we consider the summation over l that are not invertible in $\mathbb{Z}/p^n$. Note that

$$p^n \sum_{\substack{l \bmod p^n \\ l \notin (\mathbb{Z}/p^n)^\times}} \left| \sum_{\substack{x,y=\square \bmod p^n \\ x-y=l}} \langle a_x, a_y \rangle_H \right|^2 \leq p^n \sum_{\substack{l \bmod p^n \\ l \notin (\mathbb{Z}/p^n)^\times}} \left(\sum_{x=\square \bmod p^n} |\langle a_x, a_{x-l} \rangle_H| \right)^2$$

if we conveniently denote $a_u = 0$ for u that is not a square mod p^n .

Applying Cauchy–Schwarz inequality twice, the expression above is bounded by

$$\begin{aligned}
p^n \sum_{\substack{l \bmod p^n \\ l \notin (\mathbb{Z}/p^n)^\times}} \left(\sum_{x=\square \bmod p^n} \|a_x\|_H \|a_{x-l}\|_H \right)^2 &\leq p^n \sum_{\substack{l \bmod p^n \\ l \notin (\mathbb{Z}/p^n)^\times}} \left(\sum_{x=\square \bmod p^n} \|a_x\|_H^2 \right)^2 \\
&= p^{2n-1} \left(\sum_{x=\square \bmod p^n} \|a_x\|_H^2 \right)^2 \\
&\ll \frac{1}{p} S(p^n)^2 \left(\sum_{x=\square \bmod p^n} \|a_x\|_H^2 \right)^2
\end{aligned} \tag{4.3.2}$$

where the last line follows from Proposition 4.2.1.

Next, we consider the summation over l that are invertible in $\mathbb{Z}/p^n$. To proceed, we need a little digression on number of the solutions to certain equation over $\mathbb{Z}/p^n$. For any $l \in (\mathbb{Z}/p^n)^\times$, define

$$T(l, p^n) = \{(x, y) \in \mathbb{Z}/p^n \times \mathbb{Z}/p^n : x \text{ and } y \text{ are squares, and } x - y = l\}$$

We claim that $|T(l, p^n)| \leq \frac{p^n - p^{n-1}}{4} + 2$ for $p \geq 3$. To see this, let

$$\mathcal{A}(l, p^n) = \{(a, b) \in \mathbb{Z}/p^n \times \mathbb{Z}/p^n : a, b \neq 0 \text{ and } a^2 - b^2 = l\}$$

Note that for any $(a, b) \in \mathcal{A}(l, p^n)$, we have $(a + b)(a - b) = l$. Since $p \neq 2$, we can perform change of variables $u = a + b, v = a - b$ and rewrite the equation as $uv = l$. The assumption that l is invertible implies that u, v are invertible. Thus, there are at most $|(\mathbb{Z}/p^n)^\times| = p^n - p^{n-1}$ choices of (u, v) and hence $|\mathcal{A}(l, p^n)| \leq p^n - p^{n-1}$.

The relation between $\mathcal{A}(l, p^n)$ and $T(l, p^n)$ is not exactly one-to-one. For any $(x, y) \in T(l, p^n)$ with x and y both nonzero, there are at least four different elements in $\mathcal{A}(l, p^n)$ corresponding to it, since $(\pm a, \pm b)$ will correspond to the same (x, y) . Also, we need to consider the special case that $(l, 0)$ and $(0, -l)$ might belong to $T(l, p^n)$. Hence, we have

$$|T(l, p^n)| \leq \frac{|\mathcal{A}(l, p^n)|}{4} + 2 \leq \frac{p^n - p^{n-1}}{4} + 2.$$

Now, we can continue our previous estimates. Note that

$$p^n \sum_{\substack{l \bmod p^n \\ l \in (\mathbb{Z}/p^n)^\times}} \left| \sum_{\substack{x, y = \square \bmod p^n \\ x - y = l}} \langle a_x, a_y \rangle_H \right|^2 \leq p^n \sum_{\substack{l \bmod p^n \\ l \in (\mathbb{Z}/p^n)^\times}} |T(l, p^n)| \sum_{\substack{x, y = \square \bmod p^n \\ x - y = l}} |\langle a_x, a_y \rangle_H|^2$$

by Cauchy–Schwarz inequality.

Invoking the estimates for $|T(l, p^n)|$, the expression above is bounded by

$$\begin{aligned} & p^n \left(\frac{p^n - p^{n-1}}{4} + 2 \right) \sum_{\substack{l \bmod p^n \\ l \in (\mathbb{Z}/p^n)^\times}} \sum_{\substack{x, y = \square \bmod p^n \\ x - y = l}} |\langle a_x, a_y \rangle_H|^2 \\ & \leq p^n \left(\frac{p^n - p^{n-1}}{4} + 2 \right) \sum_{\substack{l \bmod p^n \\ l \in (\mathbb{Z}/p^n)^\times}} \sum_{\substack{x, y = \square \bmod p^n \\ x - y = l}} (\|a_x\|_H \|a_y\|_H)^2 \\ & \leq p^n \left(\frac{p^n - p^{n-1}}{4} + 2 \right) \sum_{x, y = \square \bmod p^n} (\|a_x\|_H \|a_y\|_H)^2 \\ & = p^n \left(\frac{p^n - p^{n-1}}{4} + 2 \right) \left(\sum_{x = \square \bmod p^n} \|a_x\|_H^2 \right)^2. \end{aligned} \tag{4.3.3}$$

Finally, by Proposition 4.2.1, we have

$$p^n \left(\frac{p^n - p^{n-1}}{4} + 2 \right) S(p^n)^{-2} \leq \frac{p^{2n+2} + O(p^{2n+1})}{p^{2n+2} - O(p^{2n+1})} \leq 1 + O\left(\frac{1}{p}\right). \tag{4.3.4}$$

Combining (4.3.2), (4.3.3) and (4.3.4), we conclude the desired inequality $C_4(p^n) \leq 1 + O(1/p)$ for sufficiently large p . $\square$

Proof of Proposition 4.3.5 for $q > 4$. Throughout the proof, we will assume p is sufficiently large depending on q , and all implied constants are allowed to depend on q . We may also assume $\sum_{x = \square \bmod p^n} \|a_x\|_H^2 = S(p^n)$ by normalization.

We would like to reduce to the case that

$$\left\| \sum_{x = \square \bmod p^n} a_x e_{p^n}(tx) \right\|_H \geq S(p^n) - O(p^{n-1}) \tag{4.3.5}$$

for some $t \in \mathbb{Z}/p^n$. To carry out the reduction, let A be a large constant (depending only on q) chosen later, and suppose

$$\left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H \leq S(p^n) - Ap^{n-1}$$

for all $t \in \mathbb{Z}/p^n$. Then, by restriction estimates for $q = 4$ (Proposition 4.3.5), we have

$$\begin{aligned} \sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H^q &\leq (S(p^n) - Ap^{n-1})^{q-4} \sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H^4 \\ &\leq (S(p^n) - Ap^{n-1})^{q-4} (1 + O(1/p)) S(p^n)^4 \\ &= S(p^n)^q (1 - Ap^{n-1}/S(p^n))^{q-4} (1 + O(1/p)). \end{aligned}$$

Since $p^{n-1}/S(p^n) \gg 1/p$, choosing sufficiently large A depending on q will make $(1 - Ap^{n-1}/S(p^n))^{q-4} (1 + O(1/p)) \leq 1$. Hence, we can reduce to that case that (4.3.5) holds for some $t \in \mathbb{Z}/p^n$. By multiplying $e_{p^n}(tx)$ to a_x , we may further assume that $t = 0$ and hence

$$\left\| \sum_{x=\square \bmod p^n} a_x \right\|_H \geq S(p^n) - O(p^{n-1}). \quad (4.3.6)$$

Now, let $c = \frac{1}{S(p^n)} \sum_{x=\square \bmod p^n} a_x$ be the average of a_x and decompose $a_x = b_x + c$, where the vectors b_x have mean zero. One has good lower and upper bounds for $\|c\|_H$, that is

$$1 - O(1/p) \leq \|c\|_H \leq 1$$

by (4.3.6) and Cauchy–Schwarz inequality respectively. Moreover, Pythagoras’s theorem says that $\sum_{x=\square \bmod p^n} \|a_x\|_H^2 = \sum_{x=\square \bmod p^n} \|b_x\|_H^2 + S(p^n) \|c\|_H^2$. Combining this and the lower bound for $\|c\|_H$, we deduce a good l^2 -bound for b_x , which is

$$\sum_{x=\square \bmod p^n} \|b_x\|_H^2 \ll \frac{1}{p} S(p^n). \quad (4.3.7)$$

Note that

$$\begin{aligned}
& \sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H^q \\
&= \sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} b_x e_{p^n}(tx) + \sum_{x=\square \bmod p^n} c e_{p^n}(tx) \right\|_H^q \\
&= \|S(p^n)c\|_H^q + \sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} b_x e_{p^n}(tx) + \sum_{x=\square \bmod p^n} c e_{p^n}(tx) \right\|_H^q \\
&\leq S(p^n)^q + \left\{ \left(\sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} b_x e_{p^n}(tx) \right\|_H^q \right)^{1/q} + \left(\sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} c e_{p^n}(tx) \right\|_H^q \right)^{1/q} \right\}^q
\end{aligned} \tag{4.3.8}$$

where the last line follows from Minkowski inequality. We will estimate the sums involving b_x and c separately.

For the sum involving b_x , we will use (4.3.7) and restriction estimates for $q = 4$. We have

$$\begin{aligned}
& \left(\sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} b_x e_{p^n}(tx) \right\|_H^q \right)^{1/q} \leq \left(\sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} b_x e_{p^n}(tx) \right\|_H^4 \right)^{1/4} \\
& \leq C_4(p^n) S(p^n)^{1/2} \left(\sum_{x=\square \bmod p^n} \|b_x\|_H^2 \right)^{1/2} \\
& \ll p^{n-1/2}.
\end{aligned} \tag{4.3.9}$$

For the sum involving c , we will use Gauss sum estimates (Proposition 4.2.2). We have

$$\sum_{\substack{t \bmod p^n \\ t \neq 0}} \left\| \sum_{x=\square \bmod p^n} c e_{p^n}(tx) \right\|_H^q \leq \sum_{\substack{t \bmod p^n \\ t \neq 0}} \left| \sum_{x=\square \bmod p^n} e_{p^n}(tx) \right|^q \ll \sum_{1 \leq t < p^n} (t, p^n)^q p^{q/2}, \tag{4.3.10}$$

which is

$$\begin{aligned}
& \sum_{0 \leq e \leq n-1} \sum_{\substack{1 \leq t < p^n \\ p^e \parallel t}} p^{qe} p^{q/2} \\
& \leq \sum_{0 \leq e \leq n-1} p^{n-e} p^{qe+q/2} \\
& = p^{n+q/2} \sum_{0 \leq e \leq n-1} p^{(q-1)e} \\
& \ll p^{n+q/2} p^{(n-1)(q-1)} \\
& = p^{qn+1-q/2}.
\end{aligned} \tag{4.3.11}$$

Combining (4.3.8), (4.3.9), (4.3.10) and (4.3.11), we obtain

$$\begin{aligned}
\sum_{t \bmod p^n} \left\| \sum_{x=\square \bmod p^n} a_x e_{p^n}(tx) \right\|_H^q & \leq S(p^n)^q + O(p^{qn-q/2} + p^{qn+1-q/2}) \\
& \leq S(p^n)^q (1 + O(p^{-\frac{q}{2}+1})).
\end{aligned}$$

This completes the proof. $\square$

Now, we have all the ingredients needed for the proof of Theorem 4.3.3.

Proof of Theorem 4.3.3. Let $q > 4$, by Proposition 4.3.5, there exists a constant $M = M(q)$ such that

$$C_q(p^n) \leq 1 + O_q \left(\frac{1}{p^{\frac{q}{2}-1}} \right)$$

for all $p \geq M$ and $n \geq 1$.

Let $W = \prod_i p_i^{n_i}$ be a modulus with $p_i \geq M$ for all i . By Lemma 4.3.4, we have

$$C_q(W) = \prod_i C_q(p_i^{n_i}) \leq \prod_{p \geq M} (1 + O_q(p^{-q/2+1})) \leq \exp \left(\sum_{p \geq M} O_q(p^{-q/2+1}) \right) \ll_q 1$$

since $q/2 - 1 > 1$ when $q > 4$. $\square$

4.4 Sumsets of dense subsets of $\mathbb{Z}/W$

With the transference principle, one can treat relatively dense subsets of squares in $\mathbb{Z}/W$ as if they are actually dense in $\mathbb{Z}/W$. Therefore, we would like a quantitative sumset estimates for dense subsets of $\mathbb{Z}/W$. Li and Pan [LP10, Lemma 3.3] proved the desired sumset estimates for prime moduli, and we will generalize their results to general moduli.

Theorem 4.4.1. *Let $0 < \theta_1, \theta_2, \dots, \theta_s \leq 1$ with $\theta_1 + \theta_2 + \dots + \theta_s > 1$. There exist positive constants $c(\theta_1, \theta_2, \dots, \theta_s)$ and $M(\theta_1, \theta_2, \dots, \theta_s)$ depending only on $\theta_1, \theta_2, \dots, \theta_s$ such that the following holds.*

Suppose $W = \prod_i p_i^{n_i}$ is an integer with $p_i \geq M(\theta_1, \theta_2, \dots, \theta_s)$ for all i , and $A_1, A_2, \dots, A_s$ are subsets of $\mathbb{Z}/W$ with $|A_j| \geq \theta_j W$ for all $1 \leq j \leq s$. Then,

$$1_{A_1} * 1_{A_2} * \dots * 1_{A_s}(x) \geq c(\theta_1, \theta_2, \dots, \theta_s) W^{s-1}$$

for all $x \in \mathbb{Z}/W$.

Our proof of Theorem 4.4.1 is similar to Li and Pan's proof of [LP10, Lemma 3.3], just that we need the following more general Pollard–Kneser type result due to Green and Ruzsa [GR05, Proposition 6.1].

Theorem 4.4.2 (Green–Ruzsa). *Let Z be a finite abelian group, and $D(Z)$ be the size of the largest proper subgroup of Z . Suppose A, B are subsets of Z , then, for any $1 \leq t \leq \min\{|A|, |B|\}$, we have*

$$\sum_{x \in Z} \min\{t, 1_A * 1_B(x)\} \geq t \min\{|Z|, |A| + |B| - t - D(Z)\}.$$

Proof of Theorem 4.4.1. We will induct on s , the number of the subsets. The base case

would be $s = 2$. Note that

$$\begin{aligned}
1_{A_1} * 1_{A_2}(x) &= \sum_{\substack{a_1 \in A_1, a_2 \in A_2 \\ a_1 + a_2 = x}} 1 \\
&= |A_1 \cap (x - A_2)| \\
&= |A_1| + |x - A_2| - |A_1 \cup (x - A_2)| \\
&\geq \theta_1 W + \theta_2 W - W \\
&= (\theta_1 + \theta_2 - 1)W
\end{aligned}$$

for all $x \in \mathbb{Z}/W$. This completes the proof for base case.

Assume the Theorem 4.4.1 holds for $s - 1$ subsets. Let ϵ be a small parameter and M' be a large parameter chosen later. We will assume that we are working with moduli $W = \prod_i p_i^{n_i}$ with $p_i \geq M'$ for all i , in particular, W will be sufficiently large. Let $A_1, A_2, \dots, A_s$ be subsets of $\mathbb{Z}/W$ with $|A_j| \geq \theta_j W$ for all $1 \leq j \leq s$. Due to Theorem 4.4.2, we have

$$\sum_{x \in \mathbb{Z}/W} \min\{\lceil \epsilon W \rceil, 1_{A_1} * 1_{A_2}(x)\} \geq \lceil \epsilon W \rceil \min\left\{W, \theta_1 W + \theta_2 W - \lceil \epsilon W \rceil - \frac{1}{\min_i p_i} W\right\}$$

by noting that $D(\mathbb{Z}/W) \leq \frac{1}{\min_i p_i} W$ since $D(\mathbb{Z}/W)$ divides W .

Hence, we have

$$\begin{aligned}
&\sum_{\substack{x \in \mathbb{Z}/W \\ 1_{A_1} * 1_{A_2}(x) > \lceil \epsilon^2 W \rceil}} \min\{\lceil \epsilon W \rceil, 1_{A_1} * 1_{A_2}(x)\} \\
&\geq \lceil \epsilon W \rceil \min\left\{W, \theta_1 W + \theta_2 W - \lceil \epsilon W \rceil - \frac{1}{\min_i p_i} W\right\} - \lceil \epsilon^2 W \rceil W \\
&\geq \min\left\{(\epsilon - 2\epsilon^2)W^2, \epsilon\left(\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'}\right)W^2\right\}
\end{aligned}$$

where the last line follows from assuming M' is sufficiently large so W is sufficiently large and hence $\lceil \epsilon W \rceil \leq 2\epsilon W$ and $\lceil \epsilon^2 W \rceil \leq 2\epsilon^2 W$ for notational convenience.

Denote $B = \{x \in \mathbb{Z}/W : 1_{A_1} * 1_{A_2}(x) > \lceil \epsilon^2 W \rceil\}$, then we conclude that

$$\begin{aligned} |B| &\geq \min \left\{ \frac{\epsilon - 2\epsilon^2}{\lceil \epsilon W \rceil} W^2, \frac{\epsilon (\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'})}{\lceil \epsilon W \rceil} W^2 \right\} \\ &\geq \min \left\{ \frac{\epsilon - 2\epsilon^2}{\epsilon W + \epsilon^2 W} W^2, \frac{\epsilon (\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'})}{\epsilon W + \epsilon^2 W} W^2 \right\} \end{aligned} \quad (4.4.1)$$

(Assuming W is large enough so $\lceil \epsilon W \rceil \leq \epsilon W + \epsilon^2 W$)

$$= \min \left\{ \frac{1 - 2\epsilon}{1 + \epsilon} W, \frac{\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'}}{1 + \epsilon} W \right\}.$$

Now, we will choose our parameters carefully. We will choose sufficiently small ϵ depending on $\theta_1, \theta_2, \dots, \theta_s$ and sufficiently large M' depending on $\epsilon, \theta_1, \theta_2, \dots, \theta_s$ so that we have the followings:

- $\lceil \epsilon W \rceil \leq \min\{\theta_1 W, \theta_2 W\}$ so that the assumption of Theorem 4.4.2 is met.
- $\lceil \epsilon W \rceil \leq 2\epsilon W$, $\lceil \epsilon^2 W \rceil \leq 2\epsilon^2 W$ and $\lceil \epsilon W \rceil \leq \epsilon W + \epsilon^2 W$ for notational convenience.
- $\frac{1-2\epsilon}{1+\epsilon}$ is close enough to 1 and $\frac{\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'}}{1+\epsilon}$ is close enough to $\theta_1 + \theta_2$ so that

$$\min \left\{ \frac{1 - 2\epsilon}{1 + \epsilon}, \frac{\theta_1 + \theta_2 - 4\epsilon - \frac{1}{M'}}{1 + \epsilon} \right\} + \theta_3 + \dots + \theta_s > 1.$$

- Thus, by (4.4.1), we have $|B| \geq \eta W$ for some η depending on $M', \epsilon, \theta_1, \theta_2, \dots, \theta_s$ with $0 < \eta \leq 1$ and $\eta + \theta_3 + \dots + \theta_s > 1$.
- By induction hypothesis, we may apply Theorem 4.4.1 for $s - 1$ densities $\eta, \theta_3, \dots, \theta_s$ to obtain two constants $c(\eta, \theta_3, \dots, \theta_s) > 0$ and $M(\eta, \theta_3, \dots, \theta_s)$. We claim that for s densities $\theta_1, \theta_2, \dots, \theta_s$, we can pick $c(\theta_1, \theta_2, \dots, \theta_s) = \epsilon^2 c(\eta, \theta_3, \dots, \theta_s)$ and $M(\theta_1, \theta_2, \dots, \theta_s) = \max\{M', M(\eta, \theta_3, \dots, \theta_s)\}$.

To finish the proof, note that for all $x \in \mathbb{Z}/W$, we have

$$\begin{aligned}
1_{A_1} * 1_{A_2} * \dots * 1_{A_s}(x) &\geq (1_{A_1} * 1_{A_2})|_B * (1_{A_3} \dots * 1_{A_s})(x) \\
&\geq \epsilon^2 W(1_B * 1_{A_3} \dots * 1_{A_s})(x) \\
&\geq \epsilon^2 W c(\eta, \theta_3, \dots, \theta_s) W^{s-2} \quad (\text{By induction hypothesis}) \\
&= \epsilon^2 c(\eta, \theta_3, \dots, \theta_s) W^{s-1}.
\end{aligned}$$

□

4.5 Transference principle

In this section, we will use the transference principle pioneered by Green and Tao [Gre05], [GT08] to prove Theorem 1.5.1. We will closely follow the arguments in Section 6 in [Gre05]. As a remark, one can view the assumption of Theorem 1.5.1 that W does not have small prime divisors as an analog of the W -trick.

Let $s \geq 5$ be an integer and $\theta \in (1/s, 1]$. Let M be a large constant chosen later, and we will be working with moduli $W = \prod_i p_i^{n_i}$ with $\min_i p_i \geq M$ so that we can freely apply Gauss sum estimates, restriction theorem, quantitative sumset estimates, etc. Let A be a subset of the squares in $\mathbb{Z}/W$ with $|A| \geq \theta S(W)$.

We define the following objects for the transference principle:

- Let $\nu = \frac{1}{S(W)} 1_{(\mathbb{Z}/W)^{(2)}}$ be a probability measure supported on the squares in $\mathbb{Z}/W$.
- Define the normalized indicator function of A by setting $a = 1_A \nu$. Note that the l^1 -norm of a is the relative density of A .
- Let $\delta, \epsilon > 0$ be small parameters chosen later. Let

$$R = \{\xi \in \mathbb{Z}/W : |\tilde{a}(\xi)| > \delta\}$$

be the large spectrum of a and

$$B = \left\{ x \in \mathbb{Z}/W : \left\| \frac{x\xi}{W} \right\|_{\mathbb{R}/\mathbb{Z}} < \epsilon \text{ for all } \xi \in R \right\}$$

be the Bohr neighborhood of R .

- Let $\beta = \frac{1}{|B|}1_B$ and $a' = a * \beta * \beta$. The function a' can be thought of as the “transferred” version of a . Note that a' and a have the same l^1 -norm.

First, we show that A and the transferred version of A are close in finding certain additive configurations.

Proposition 4.5.1. *For all $y \in \mathbb{Z}/W$, we have*

$$\sum_{\substack{x_1, x_2, \dots, x_s \in \mathbb{Z}/W \\ y = x_1 + x_2 + \dots + x_s}} a(x_1)a(x_2)\dots a(x_s) = \sum_{\substack{x_1, x_2, \dots, x_s \in \mathbb{Z}/W \\ y = x_1 + x_2 + \dots + x_s}} a'(x_1)a'(x_2)\dots a'(x_s) + O\left(\frac{1}{W}(\epsilon\delta^{-4.5} + \delta^{1/2})\right)$$

Proof. By Fourier expansions, we obtain

$$\begin{aligned} & \sum_{\substack{x_1, x_2, \dots, x_s \in \mathbb{Z}/W \\ y = x_1 + x_2 + \dots + x_s}} a(x_1)a(x_2)\dots a(x_s) - \sum_{\substack{x_1, x_2, \dots, x_s \in \mathbb{Z}/W \\ y = x_1 + x_2 + \dots + x_s}} a'(x_1)a'(x_2)\dots a'(x_s) \\ &= \frac{1}{W} \sum_{\xi \in \mathbb{Z}/W} \tilde{a}(\xi)^s e_W(\xi y) - \frac{1}{W} \sum_{\xi \in \mathbb{Z}/W} \tilde{a}'(\xi)^s e_W(\xi y) \\ &= \frac{1}{W} \sum_{\xi \in \mathbb{Z}/W} \tilde{a}(\xi)^s e_W(\xi y) (1 - \tilde{\beta}(\xi)^{2s}). \end{aligned}$$

We will divide the sum above into two cases, according to whether ξ is in the large spectrum R .

Note that by construction of B , we have $\tilde{\beta}(\xi) = 1 + O(\epsilon)$ if $\xi \in R$. Also, by restriction estimates (Theorem 4.3.3), we obtain $\|\tilde{a}\|_{l^q} = O_q(1)$ when all the prime factors of W are sufficiently large depending on q . In particular, we have $\|\tilde{a}\|_{l^{4.5}} = O(1)$ and hence $|R| = O(\delta^{-4.5})$. Therefore, we deduce

$$\left| \sum_{\xi \in R} \tilde{a}(\xi)^s e_W(\xi y) (1 - \tilde{\beta}(\xi)^{2s}) \right| \ll \epsilon |R| \ll \epsilon \delta^{-4.5}.$$

On the other hand, we have

$$\left| \sum_{\xi \notin R} \tilde{a}(\xi)^s e_W(\xi y) (1 - \tilde{\beta}(\xi)^{2s}) \right| \ll \delta^{1/2} \sum_{\xi \notin R} |\tilde{a}(\xi)|^{s-1/2} \ll \delta^{1/2}$$

by applying the restriction estimates for $q = s - 1/2$ or $q = 4.5$. $\square$

The next proposition is about the pseudorandomness of the measure ν .

Proposition 4.5.2. *For all $\xi \neq 0$, we have*

$$|\tilde{\nu}(\xi)| \ll \frac{1}{(\min_i p_i)^{1/2}}.$$

Recall that the minimum is taken among all prime factors of W .

Proof. First, we recall the multiplicativity of Gauss sums. Let $W = W_1 W_2$ with $(W_1, W_2) = 1$, then $\lambda_2 W_1 + \lambda_1 W_2 = 1$ for some integers λ_1, λ_2 with $(\lambda_1, W_1) = (\lambda_2, W_2) = 1$. We can decompose

$$\sum_{x=\square \bmod W} e_W(\xi x) = \left(\sum_{x_1=\square \bmod W_1} e_{W_1}(\lambda_1 \xi x_1) \right) \left(\sum_{x_2=\square \bmod W_2} e_{W_2}(\lambda_2 \xi x_2) \right).$$

Now, if we write $W = \prod_i p_i^{n_i}$, then there exists a prime p_j such that $p_j^{n_j} \nmid \xi$ since $\xi \neq 0$. By Gauss sum estimates (Proposition 4.2.2) and the multiplicativity of Gauss sums, we have

$$\begin{aligned} |\tilde{\nu}(\xi)| &= \frac{1}{S(W)} \left| \sum_{x=\square \bmod W} e_W(\xi x) \right| \ll \frac{1}{S(W)} p_j^{n_j-1} p_j^{1/2} \prod_{\substack{i \\ i \neq j}} S(p_i^{n_i}) \\ &= \frac{1}{S(p_j^{n_j})} p_j^{n_j-1/2} \\ &\ll \frac{1}{p_j^{1/2}} \\ &\leq \frac{1}{(\min_i p_i)^{1/2}}. \end{aligned}$$

$\square$

Next, we show that a' is set-like in the following proposition.

Proposition 4.5.3. *For all $x \in \mathbb{Z}/W$, we have*

$$a'(x) \leq \frac{1}{W} \left(1 + O \left(\frac{1}{\epsilon^{O(\delta^{-4.5})} (\min_i p_i)^{1/2}} \right) \right)$$

Proof. Note that

$$\begin{aligned} a'(x) &\leq \nu * \beta * \beta(x) \\ &= \frac{1}{W} \sum_{\xi \in \mathbb{Z}/W} (\nu * \beta * \beta)^\sim(\xi) e_W(\xi x) \quad \text{by Fourier expansion} \\ &= \frac{1}{W} \sum_{\xi \in \mathbb{Z}/W} \tilde{\nu}(\xi) \tilde{\beta}(\xi)^2 e_W(\xi x) \\ &\leq \frac{1}{W} + \frac{1}{W} \sum_{\substack{\xi \in \mathbb{Z}/W \\ \xi \neq 0}} |\tilde{\nu}(\xi)| |\tilde{\beta}(\xi)|^2 \end{aligned}$$

By Proposition 4.5.2 and Parseval's identity, we have

$$\sum_{\substack{\xi \in \mathbb{Z}/W \\ \xi \neq 0}} |\tilde{\nu}(\xi)| |\tilde{\beta}(\xi)|^2 \ll \frac{W}{(\min_i p_i)^{1/2} |B|}.$$

The classical lower bound for the size of Bohr sets [TV06, Lemma 4.20] states that $|B| \geq \epsilon^{|R|} W$. To complete the proof, we observe that $|R| = O(\delta^{-4.5})$ since $\|\tilde{a}\|_{l^{4.5}} = O(1)$ due to restriction estimates (Theorem 4.3.3) for $q = 4.5$. $\square$

Now, we have all the ingredients to prove our main theorem.

Proof of Theorem 1.5.1. Let $s \geq 5$ be an integer and $\theta \in (1/s, 1]$. We will choose a list of parameters carefully depending on s, θ as follow:

- Choose $\gamma > 0$ sufficiently small such that $\frac{1-\gamma}{1+\gamma} \theta s > 1$.
- Let $c' = c'(\frac{1-\gamma}{1+\gamma} \theta, \frac{1-\gamma}{1+\gamma} \theta, \dots, \frac{1-\gamma}{1+\gamma} \theta) > 0$ and $M' = M'(\frac{1-\gamma}{1+\gamma} \theta, \frac{1-\gamma}{1+\gamma} \theta, \dots, \frac{1-\gamma}{1+\gamma} \theta)$ be the constants from the quantitative sumset estimates for dense subsets of cyclic rings (Theorem 4.4.1) for the density $\frac{1-\gamma}{1+\gamma} \theta$.

- Let M'' be the constant from the restriction estimates (Theorem 4.3.3) for $q = 4.5$.
- Choose δ and then ϵ sufficiently small such that the error term in Proposition 4.5.1 is less than $\frac{\gamma^s \theta^s c'}{2W}$.
- By Proposition 4.5.3, we can choose sufficiently large M''' such that $\|a'\|_\infty \leq \frac{1}{W}(1 + \gamma)$ when $\min_i p_i \geq M'''$.
- For the proof of main theorem (Theorem 1.5.1), we claim that we can choose $c = \frac{\gamma^s \theta^s c'}{2} > 0$ and $M = \max\{M', M'', M'''\}$.

Let

$$A' = \left\{ x \in \mathbb{Z}/W : a'(x) \geq \frac{\gamma\theta}{W} \right\}$$

Since $\|a'\|_\infty \leq \frac{1}{W}(1 + \gamma)$ and $\|a'\|_1 \geq \theta$, by pigeonhole principle, we have $|A'| \geq \frac{1-\gamma}{1+\gamma}\theta W$.

By the quantitative sumset estimates for dense subsets of $\mathbb{Z}/W$ (Theorem 4.4.1), we have

$$\begin{aligned} \underbrace{a' * a' * \dots * a'}_{s\text{-times}}(y) &\geq \left(\frac{\gamma\theta}{W} 1_{A'} \right) * \left(\frac{\gamma\theta}{W} 1_{A'} \right) * \dots * \left(\frac{\gamma\theta}{W} 1_{A'} \right)(y) \\ &= \left(\frac{\gamma\theta}{W} \right)^s (1_{A'} * 1_{A'} * \dots * 1_{A'})(y) \\ &\geq \left(\frac{\gamma\theta}{W} \right)^s c' W^{s-1} \\ &= \frac{\gamma^s \theta^s c'}{W} \end{aligned}$$

for all $y \in \mathbb{Z}/W$. Combining this and Proposition 4.5.1, we conclude that

$$\sum_{\substack{x_1, x_2, \dots, x_s \in \mathbb{Z}/W \\ y = x_1 + x_2 + \dots + x_s}} a(x_1) a(x_2) \dots a(x_s) \geq \frac{\gamma^s \theta^s c'}{2W}$$

and complete the proof. □

4.6 Counterexamples

In this section, we prove Theorem 1.5.3 to complement Theorem 1.5.1. By identifying the representatives of the elements of $\mathbb{Z}/p$ with the integers in $[1, p]$, we can speak of “intervals” in $\mathbb{Z}/p$. We will use squares in intervals in $\mathbb{Z}/p$ to construct subsets of squares with relative density close to $1/s$, but their s -fold sumsets are not entire $\mathbb{Z}/p$.

The next proposition, which states that the quadratic residues are equidistributed among intervals, is a classical result that can be proved in many different ways, say, by Polya-Vinogradov inequality. For self-containedness, we still include a short proof based on Gauss sums.

Proposition 4.6.1. *Let $0 < \eta < 1$, then*

$$\#\{x \in \mathbb{Z} : 1 \leq x \leq \eta p \text{ and } x \text{ is a square mod } p\} = \eta \frac{p+1}{2} + O(\sqrt{p} \log p)$$

for all primes p .

Proof. By abuse of notation, we will denote the characteristic function of the interval $[1, \eta p]$ in $\mathbb{Z}/p$ by $1_{[1, \eta p]}$. By Fourier expansion, we have

$$\begin{aligned} & \sum_{x=\square \bmod p} 1_{[1, \eta p]}(x) \\ &= \frac{1}{p} \sum_{x=\square \bmod p} \sum_{\xi \bmod p} \tilde{1}_{[1, \eta p]}(\xi) e_p(\xi x) \\ &= \frac{[\eta p]}{p} \cdot \frac{p+1}{2} + \frac{1}{p} \sum_{\substack{\xi \bmod p \\ \xi \neq 0}} \tilde{1}_{[1, \eta p]}(\xi) \sum_{x=\square \bmod p} e_p(\xi x) \\ &= \eta \frac{p+1}{2} + O(1) + \frac{1}{p} \sum_{\substack{\xi \bmod p \\ \xi \neq 0}} \tilde{1}_{[1, \eta p]}(\xi) \sum_{x=\square \bmod p} e_p(\xi x). \end{aligned}$$

To bound the error term, we calculate the Fourier coefficients

$$|\tilde{1}_{[1, \eta p]}(\xi)| = \left| \sum_{1 \leq x \leq [\eta p]} e_p(-x\xi) \right| \ll \left\| \frac{\xi}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^{-1}$$

for all $\xi \neq 0$. Combining this and the Gauss sum estimates (Proposition 4.2.2), we deduce that

$$\begin{aligned} \left| \frac{1}{p} \sum_{\substack{\xi \bmod p \\ \xi \neq 0}} \tilde{1}_{[1, \eta p]}(\xi) \sum_{x=\square \bmod p} e_p(\xi x) \right| &\ll \frac{1}{\sqrt{p}} \sum_{\substack{\xi \bmod p \\ \xi \neq 0}} \left\| \frac{\xi}{p} \right\|_{\mathbb{R}/\mathbb{Z}}^{-1} \\ &\ll \sqrt{p} \log p. \end{aligned}$$

□

Now, we will apply Proposition 4.6.1 to prove Theorem 1.5.3.

Proof of Theorem 1.5.3. Let $s \geq 5$ be an integer, and $\tau \in [0, 1/s)$. Choose η with $\tau < \eta < 1/s$, by Proposition 4.6.1, we have

$$\#\{x \in \mathbb{Z} : 1 \leq x \leq \eta p \text{ and } x \text{ is a square mod } p\} \geq \tau \frac{p+1}{2}$$

for sufficiently large p . However, the s -fold sumset of $\{x \in \mathbb{Z} : 1 \leq x \leq \eta p \text{ and } x \text{ is a square mod } p\}$ cannot be $\mathbb{Z}/p$ since $\eta s < 1$. □

4.7 A combinatorial lemma

One of the key ingredients in Shao's [Sha14] proof of the sharp density version of Vinogradov three primes theorem is a combinatorial inequality. Subsequently, Lacey, Mousavi, Rahimi and Vempati [LMR24] developed a variant of Shao's inequality to generalize the density version of Vinogradov theorem to sum of more primes. In this section, we will use variants of Shao's and Lacey, Mousavi, Rahimi and Vempati's ideas to prove a combinatorial inequality that suits our purpose.

The combinatorial inequality is inductive in nature, but our base cases are more complicated, hence we handled them by linear programming with computer assistance. As a remark, Shao also used linear programming techniques in his proof, but the linear programming problems we dealt with are different due to different formulations of the combinatorial inequalities.

Lemma 4.7.1. *Let $s \geq 6, n \geq 3$ or $s = 5, n \geq 5$. For each integer $1 \leq j \leq s$, let $\{a_{i,j}\}_{0 \leq i < n}$ be a decreasing sequence in interval $[0, 1]$. Suppose*

$$\frac{1}{ns} \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j} > d_s \text{ and } a_{0,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

Then, there exist indices $0 \leq i_1, i_2, \dots, i_s < n$ with $i_1 + i_2 + \dots + i_s \geq 2n$ such that

$$\frac{1}{s} \sum_{1 \leq j \leq s} a_{i_j,j} > d_s \text{ and } a_{i_j,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

The proof of Lemma 4.7.1 is a bit long, so we separate it into inductive step and base cases. Along the proof, we will see explanations for the somewhat awkward definition of d_s . The reason why we choose d_s to be greater than or equal to $(s + 13)/4s$ is to make the inductive step work.

Proof of Lemma 4.7.1 assuming the base cases. We will prove Lemma 4.7.1 by induction on n . Let $s \geq 6, n \geq 4$ or $s = 5, n \geq 6$. Suppose the lemma holds for $n - 1$.

There are at least two nonzero elements among $a_{1,j}$ where $1 \leq j \leq s$, otherwise the total average is not large enough, that is

$$\frac{1}{ns} \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j} \leq \frac{1}{ns} (n + (s - 1)) \leq \frac{s + 3}{4s}$$

since $n \geq 4$. However, the total average is assumed to be greater than d_s , which is at least $(s + 13)/(4s)$. Thus, by relabeling if needed, we may assume $a_{1,1}, a_{1,2} \neq 0$.

Suppose we have

$$\frac{1}{s} (a_{0,1} + a_{0,2} + a_{i_3,3} + a_{i_4,4} + \dots + a_{i_s,s}) \leq d_s \text{ for some indices } 0 \leq i_3, i_4, \dots, i_s < n.$$

By monotonicity of $a_{i,j}$ in i , we may further assume

$$\frac{1}{s} (a_{0,1} + a_{0,2} + a_{i_3,3} + a_{i_4,4} + \dots + a_{i_s,s}) \leq d_s \text{ for some indices } 1 \leq i_3, i_4, \dots, i_s < n.$$

Remove the elements $a_{0,1}, a_{0,2}, a_{i_3,3}, a_{i_4,4}, \dots, a_{i_s,s}$ from the sequences $\{a_{i,j}\}_{0 \leq i < n, 1 \leq j \leq s}$ and denote the new sequences after removal by $\{b_{i,j}\}_{0 \leq i < n-1, 1 \leq j \leq s}$. Note that by construction, we have

$$\begin{aligned} b_{i,j} &= a_{i+1,j} \text{ if } j = 1, 2 \\ b_{i,j} &\leq a_{i,j} \text{ if } j \geq 3. \end{aligned} \tag{4.7.1}$$

Observe that the total average of $b_{i,j}$ is greater than or equal to the total average of $a_{i,j}$ since the average of the removed elements is less than the total average of $a_{i,j}$, that is

$$\frac{1}{(n-1)s} \sum_{\substack{0 \leq i < n-1 \\ 1 \leq j \leq s}} b_{i,j} \geq \frac{1}{ns} \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j} > d_s.$$

Also, the elements $b_{0,j}$ are nonzero for $1 \leq j \leq s$ because $b_{0,j} = a_{1,j} \neq 0$ for $j = 1, 2$ and $b_{0,j} = a_{0,j} \neq 0$ for $j \geq 3$. In short, the sequences $\{b_{i,j}\}_{0 \leq i < n-1, 1 \leq j \leq s}$ satisfy all assumptions in Lemma 4.7.1 for $n-1$. By induction hypothesis, there exist indices $i_1, i_2, \dots, i_s$ with $i_1 + i_2 + \dots + i_s \geq 2(n-1)$ such that

$$\frac{1}{s} \sum_{1 \leq j \leq s} b_{i_j,j} > d_s \text{ and } b_{i_j,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

Note that by equations (4.7.1), we conclude that

$$\frac{1}{s}(a_{i_1+1,1} + a_{i_2+1,2} + a_{i_3,3} + \dots + a_{i_s,s}) > d_s.$$

Furthermore, the sum of indices is $(i_1 + 1) + (i_2 + 1) + i_3 + \dots + i_s \geq 2(n-1) + 2 = 2n$, hence the elements $a_{i_1+1,1}, a_{i_2+1,2}, a_{i_3,3}, \dots, a_{i_s,s}$ are the desired collection of the elements for Lemma 4.7.1.

Now, we consider the other possibility, namely

$$\frac{1}{s}(a_{0,1} + a_{0,2} + a_{i_3,3} + a_{i_4,4} + \dots + a_{i_s,s}) > d_s \text{ for all indices } 0 \leq i_3, i_4, \dots, i_s < n.$$

For each $1 \leq j \leq s$, let t_j be the number of nonzero elements among $\{a_{i,j}\}_{0 \leq i < n}$. In particular, we have

$$\frac{1}{s}(a_{0,1} + a_{0,2} + a_{t_3-1,3} + a_{t_4-1,4} + \dots + a_{t_s-1,s}) > d_s.$$

It remains to check that the sum of indices is large enough. Since $a_{i,j}$ are all bounded by 1, we have

$$2n + (t_3 + t_4 + \dots + t_s) \geq \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j} > nsd_s$$

Hence, we deduce that

$$\begin{aligned} (t_3 - 1) + (t_4 - 1) + \dots + (t_s - 1) &> n(sd_s - 2) - (s - 2) \\ &\geq n \left(\frac{s + 13}{4} - 2 \right) - (s - 2) \quad \left(\text{since } d_s \geq \frac{s + 13}{4s} \text{ for all } s \right) \\ &= n \left(\frac{s + 5}{4} \right) - (s - 2). \end{aligned}$$

Note that $n(s + 5)/4 - (s - 2) \geq 2n - 1$ when $n \geq 4$, thus we have

$$(t_3 - 1) + (t_4 - 1) + \dots + (t_s - 1) > 2n - 1.$$

Since $(t_3 - 1) + (t_4 - 1) + \dots + (t_s - 1)$ is an integer, we conclude that

$$(t_3 - 1) + (t_4 - 1) + \dots + (t_s - 1) \geq 2n$$

and this completes the inductive step. □

For the base cases of Lemma 4.7.1 when $5 \leq s \leq 11$, we will handle them via linear programming with computer assistance. For certain linear programming problems to have expected optimal values, we choose $d_s = 5/6$ instead of $(s + 13)/4s$ when $s = 6$. This is also the reason why the base case for $s = 5$ corresponds to $n = 5$ as opposed to $n = 3$.

Proof of base cases of Lemma 4.7.1 when $5 \leq s \leq 11$. The crucial observation is for any fixed s, n , the Lemma 4.7.1 can be approached by linear programming. Let s, n be fixed, for any integral indices $1 \leq t_1, t_2, \dots, t_s \leq n$, we can define the following linear programming problem $\mathbf{LP}(t_1, t_2, \dots, t_s)$.

$\mathbf{LP}(t_1, t_2, \dots, t_s)$:

Variables: $a_{i,j}$ for $0 \leq i < n, 1 \leq j \leq s$

Constraints:

1. For all $0 \leq i < n, 1 \leq j \leq s$, we require that $0 \leq a_{i,j} \leq 1$.
2. For all $1 \leq j \leq s$ and $i \geq t_j$, we require that $a_{i,j} = 0$.
3. For all $0 \leq i < n - 1, 1 \leq j \leq s$, we require that $a_{i,j} \geq a_{i+1,j}$.
4. For all indices $0 \leq i_1, i_2, \dots, i_s < n$ with $i_1 + i_2 + \dots + i_s \geq 2n$ and $i_1 < t_1, i_2 < t_2, \dots, i_s < t_s$, we require that

$$\frac{1}{s}(a_{i_1,1} + a_{i_2,2} + \dots + a_{i_s,s}) \leq d_s.$$

Objective: Maximize

$$\frac{1}{ns} \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j}$$

We claim that if the maxima for linear programming problems $\mathbf{LP}(t_1, t_2, \dots, t_s)$ are upper bounded by d_s for all indices $1 \leq t_1, t_2, \dots, t_s \leq n$, then Lemma 4.7.1 is true for the parameters s, n .

To see why the claim is true, we suppose the contrary, that is, the maxima for linear programming problems $\mathbf{LP}(t_1, t_2, \dots, t_s)$ are upper bounded by d_s for all indices $1 \leq t_1, t_2, \dots, t_s \leq n$, but Lemma 4.7.1 is false for the parameters s, n . Let $\{a_{i,j}\}_{0 \leq i < n, 1 \leq j \leq s}$ be the hypothetical counterexample and T_j be the number of nonzero elements among $\{a_{i,j}\}_{0 \leq i < n}$ for every $1 \leq j \leq s$. Note that the numbers $\{a_{i,j}\}_{0 \leq i < n, 1 \leq j \leq s}$ satisfy all constraints of the linear programming problem $\mathbf{LP}(T_1, T_2, \dots, T_s)$, hence the total average of $\{a_{i,j}\}_{0 \leq i < n, 1 \leq j \leq s}$ is upper bounded by the maximum for this linear programming problem, which is less than or equal to d_s . This leads to a contradiction.

Now, the coefficients involved in the linear programming problems $\mathbf{LP}(t_1, t_2, \dots, t_s)$ are rational numbers, hence the maxima will be rational numbers. Therefore, these linear programming problems can be solved by computers without numerical errors in finitely many

steps. We used a computer program to verify that in the cases

$$(s, n) = (5, 5), (6, 3), (7, 3), (8, 3), (9, 3), (10, 3), (11, 3),$$

the maxima for linear programming problems $\mathbf{LP}(t_1, t_2, \dots, t_s)$ are indeed upper bounded by d_s . For those (s, n) , there are 126, 28, 36, 45, 55, 66, 78 linear programming problems for each (s, n) respectively. The codes we used were initially generated by ChatGPT and then modified by the author. The codes run in Sage and took about one hour to run on a personal computer. $\square$

For the base cases of Lemma 4.7.1 when $s \geq 12$, the linear programming problems become quite demanding for a personal computer. Fortunately, in this range, we have enough variables to handle them by hand. The reason why we choose $d_s = 1/2$ but not $(s + 13)/4s$ when $s \geq 14$ is because it is impossible to prove Theorem 1.4.3 for threshold lower than $1/2$, since the set $\{p \in \mathcal{P} : p \equiv 1, 4 \pmod{5}\}$ has relative lower density $1/2$, but the squares of its elements are always congruent to $1 \pmod{5}$.

We separate the proof of base cases of Lemma 4.7.1 when $s \geq 12$ into the following lemma.

Lemma 4.7.2. *Let $s \geq 12$ be an integer, and $D \geq \frac{1}{2}$ be a real number. For each integer $1 \leq j \leq s$, let $\{a_{i,j}\}_{0 \leq i < 3}$ be a decreasing sequence in interval $[0, 1]$. Suppose*

$$\frac{1}{3s} \sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} > D \text{ and } a_{0,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

Then, there exist indices $0 \leq i_1, i_2, \dots, i_s < 3$ with $i_1 + i_2 + \dots + i_s \geq 6$ such that

$$\frac{1}{s} \sum_{1 \leq j \leq s} a_{i_j,j} > D \text{ and } a_{i_j,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

Proof of Lemma 4.7.2 and bases cases of Lemma 4.7.1 when $s \geq 12$. Let R be the number of nonzero elements among $a_{2,j}$ where $1 \leq j \leq s$. We will prove Lemma 4.7.2 via cases-by-cases analysis based on the values of R . Note that the number of nonzero elements among

$a_{i,j}$ where $i = 1, 2$ and $1 \leq j \leq s$ is ≥ 7 , because this number is greater than $s/2$.

Case 0: $R = 0$

There are at least 7 nonzero elements among $a_{i,j}$ where $i = 1, 2$ and $1 \leq j \leq s$. By relabeling, we may assume $a_{1,j} \neq 0$ for $1 \leq j \leq 7$. Suppose Lemma 4.7.2 is false, then

$$(a_{1,1} + a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5} + a_{1,6}) + (a_{0,7} + a_{0,8} + \dots + a_{0,s}) \leq sD,$$

$$a_{0,1} + (a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5} + a_{1,6} + a_{1,7}) + (a_{0,8} + a_{0,9} + \dots + a_{0,s}) \leq sD.$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 0$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,2} + a_{0,3} + a_{0,4} + a_{0,5} + a_{0,6}) \leq 2sD.$$

This implies $3sD - 5 < 2sD$, which leads to a contradiction.

The strategies for the remaining cases are similar to Case 0.

Case 1: $R = 1$

There are at least 7 nonzero elements among $a_{i,j}$ where $i = 1, 2$ and $1 \leq j \leq s$. By relabeling, we may assume $a_{1,j} \neq 0$ for $1 \leq j \leq 6$ and $a_{2,1} \neq 0$. Suppose Lemma 4.7.2 is false, then

$$a_{2,1} + (a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5}) + (a_{0,6} + a_{0,7} + \dots + a_{0,s}) \leq sD,$$

$$(a_{1,1} + a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5} + a_{1,6}) + (a_{0,7} + a_{0,8} + \dots + a_{0,s}) \leq sD.$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 1$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,1} + a_{0,2} + a_{0,3} + a_{0,4} + a_{0,5}) \leq 2sD.$$

This implies $3sD - 5 < 2sD$, which leads to a contradiction.

Case 2: $R = 2$

There are at least 7 nonzero elements among $a_{i,j}$ where $i = 1, 2$ and $1 \leq j \leq s$. By relabeling, we may assume $a_{1,j} \neq 0$ for $1 \leq j \leq 5$ and $a_{2,1}, a_{2,2} \neq 0$. Suppose Lemma 4.7.2 is false, then

$$\begin{aligned} (a_{2,1} + a_{2,2}) + (a_{1,3} + a_{1,4}) + (a_{0,5} + a_{0,6} + \dots + a_{0,s}) &\leq sD, \\ a_{2,1} + (a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5}) + (a_{0,6} + a_{0,7} + \dots + a_{0,s}) &\leq sD. \end{aligned}$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 2$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,1} + a_{1,1} + a_{0,2} + a_{0,3} + a_{0,4}) \leq 2sD.$$

This implies $3sD - 5 < 2sD$, which leads to a contradiction.

Case 3: $R = 3$

There are at least 7 nonzero elements among $a_{i,j}$ where $i = 1, 2$ and $1 \leq j \leq s$. By relabeling, we may assume $a_{1,j} \neq 0$ for $1 \leq j \leq 4$ and $a_{2,1}, a_{2,2}, a_{2,3} \neq 0$. Suppose Lemma 4.7.2 is false, then

$$\begin{aligned} (a_{2,1} + a_{2,2} + a_{2,3}) + (a_{0,4} + a_{0,5} + a_{0,6} + a_{0,7} + \dots + a_{0,s}) &\leq sD, \\ (a_{2,1} + a_{2,2}) + (a_{1,3} + a_{1,4}) + (a_{0,5} + a_{0,6} + \dots + a_{0,s}) &\leq sD. \end{aligned}$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 3$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,1} + a_{1,1} + a_{0,2} + a_{1,2} + a_{0,3}) \leq 2sD.$$

This implies $3sD - 5 < 2sD$, which leads to a contradiction.

Case 4: $R = 4$

By relabeling, we may assume $a_{i,j} \neq 0$ for $1 \leq i \leq 2, 1 \leq j \leq 4$. Suppose Lemma 4.7.2 is false, then

$$\begin{aligned}(a_{2,1} + a_{2,2}) + (a_{1,3} + a_{1,4}) + (a_{0,5} + a_{0,6} + \dots + a_{0,s}) &\leq sD, \\ (a_{1,1} + a_{1,2}) + (a_{2,3} + a_{2,4}) + (a_{0,5} + a_{0,6} + \dots + a_{0,s}) &\leq sD.\end{aligned}$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 4$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,1} + a_{0,2} + a_{0,3} + a_{0,4}) \leq 2sD.$$

This implies $3sD - 4 < 2sD$, which leads to a contradiction.

Case 5: $R = 5$

By relabeling, we may assume $a_{i,j} \neq 0$ for $1 \leq i \leq 2, 1 \leq j \leq 5$. Suppose Lemma 4.7.2 is false, then

$$\begin{aligned}(a_{2,1} + a_{2,2}) + (a_{1,3} + a_{1,4} + a_{1,5}) + (a_{0,6} + a_{0,7} + \dots + a_{0,s}) &\leq sD, \\ (a_{1,1} + a_{1,2}) + (a_{2,3} + a_{2,4} + a_{2,5}) + (a_{0,6} + a_{0,7} + \dots + a_{0,s}) &\leq sD.\end{aligned}$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i and $R = 5$, we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} - (a_{0,1} + a_{0,2} + a_{0,3} + a_{0,4} + a_{0,5}) \leq 2sD.$$

This implies $3sD - 5 < 2sD$, which leads to a contradiction.

Case 6: $R \geq 6$

By relabeling, we may assume $a_{i,j} \neq 0$ for $1 \leq i \leq 2, 1 \leq j \leq 6$. Suppose Lemma 4.7.2 is

false, then

$$(a_{0,1} + a_{0,2} + a_{0,3}) + (a_{2,4} + a_{2,5} + a_{2,6}) + (a_{0,7} + a_{0,8} + \dots + a_{0,s}) \leq sD,$$

$$(a_{1,1} + a_{1,2} + a_{1,3} + a_{1,4} + a_{1,5} + a_{1,6}) + (a_{0,7} + a_{0,8} + \dots + a_{0,s}) \leq sD,$$

$$(a_{2,1} + a_{2,2} + a_{2,3}) + (a_{0,4} + a_{0,5} + a_{0,6}) + (a_{0,7} + a_{0,8} + \dots + a_{0,s}) \leq sD.$$

Summing the inequalities above and using the facts that $a_{i,j}$ is decreasing in i , we have

$$\sum_{\substack{0 \leq i < 3 \\ 1 \leq j \leq s}} a_{i,j} \leq 3sD.$$

This implies $3sD < 3sD$, which leads to a contradiction.

□

Now, we will apply Lemma 4.7.1 to prove Theorem 4.1.1. The method is similar to that of Shao [Sha14, Proposition 3.1] and Li and Pan [LP10, Theorem 1.2].

Proof of Theorem 4.1.1. We will prove Theorem 4.1.1 by induction on the number of prime divisors of W . The base case is W being a single prime p . Note that by coprime assumptions in Theorem 4.1.1, we have $p \geq 7$ when $s \geq 6$ and $p \geq 11$ when $s = 5$.

For every $1 \leq j \leq s$, write the image of f_j as a decreasing sequence $a_{0,j} \geq a_{1,j} \geq a_{2,j} \geq \dots \geq a_{n-1,j}$ in interval $[0, 1]$, where $n = (p-1)/2$. Note that by lower bounds for p , we have $n \geq 3$ when $s \geq 6$ and $n \geq 5$ when $s = 5$. Moreover, we have lower bound for the total average of $a_{i,j}$, that is

$$\frac{1}{ns} \sum_{\substack{0 \leq i < n \\ 1 \leq j \leq s}} a_{i,j} = \frac{1}{s} (\mathbb{E}[f_1] + \mathbb{E}[f_2] + \dots + \mathbb{E}[f_s]) > d_s.$$

Also, the leading terms $a_{0,j}$ are nonzero since $\mathbb{E}[f_j] \neq 0$ for $1 \leq j \leq s$. Therefore, we can apply Lemma 4.7.1 and conclude that there exist indices $i_1, i_2, \dots, i_s$ with $i_1 + i_2 + \dots + i_s \geq 2n$ such that

$$\frac{1}{s} (a_{i_1,1} + a_{i_2,2} + \dots + a_{i_s,s}) > d_s \text{ and } a_{i_j,j} \neq 0 \text{ for all } 1 \leq j \leq s.$$

Let $I_j = \{x \in (\mathbb{Z}/p)^{\times(2)} : f_j(x) \geq a_{i_j,j}\}$ for $1 \leq j \leq s$. The size of I_j is at least $i_j + 1$ for $1 \leq j \leq s$. By the Cauchy–Davenport inequality, we have

$$\begin{aligned} |I_1 + I_2 + \dots + I_s| &\geq \min\{p, |I_1| + |I_2| + \dots + |I_s| - (s-1)\} \\ &\geq \min\{p, i_1 + i_2 + \dots + i_s + 1\} \\ &\geq \min\{p, 2n + 1\} \\ &= p \end{aligned}$$

hence the sumset $I_1 + I_2 + \dots + I_s$ is $\mathbb{Z}/p$. Thus, for all $y \in \mathbb{Z}/p$, there exist $x_j \in I_j$ for $1 \leq j \leq s$ such that $y = x_1 + x_2 + \dots + x_s$. By constructions, we have $f_j(x_j) \geq a_{i_j,j} > 0$ for all $1 \leq j \leq s$ and

$$\frac{1}{s}(f_1(x_1) + f_2(x_2) + \dots + f_s(x_s)) \geq \frac{1}{s}(a_{i_1,1} + a_{i_2,2} + \dots + a_{i_s,s}) > d_s.$$

This completes the proof of base case.

Now, for general modulus W , suppose Theorem 4.1.1 is true for all moduli whose numbers of prime divisors are strictly less than the number of prime divisors of W . Write $W = pW'$ for some prime p and square free integer W' , where W' has one less prime divisors than W . By Chinese remainder theorem, we can identify $(\mathbb{Z}/W)^{\times(2)}$ with $(\mathbb{Z}/p)^{\times(2)} \times (\mathbb{Z}/W')^{\times(2)}$. The elements in $(\mathbb{Z}/W)^{\times(2)}$ can be conveniently written as (x, x') where $x \in (\mathbb{Z}/p)^{\times(2)}$, $x' \in (\mathbb{Z}/W')^{\times(2)}$.

For each $1 \leq j \leq s$, define $g_j : (\mathbb{Z}/p)^{\times(2)} \longrightarrow [0, 1]$ by setting

$$g_j(x) = \mathbb{E}_{x' \in (\mathbb{Z}/W')^{\times(2)}} f_j(x, x')$$

for all $x \in (\mathbb{Z}/p)^{\times(2)}$. Note that we have $\mathbb{E}[g_j] = \mathbb{E}[f_j] \neq 0$ for all $1 \leq j \leq s$ and

$$\frac{1}{s}(\mathbb{E}[g_1] + \mathbb{E}[g_2] + \dots + \mathbb{E}[g_s]) = \frac{1}{s}(\mathbb{E}[f_1] + \mathbb{E}[f_2] + \dots + \mathbb{E}[f_s]) > d_s.$$

Since we know that the base case is true, for all $(y, y') \in \mathbb{Z}/W$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/p)^{\times(2)}$ such that

$$\frac{1}{s}(g_1(x_1) + g_2(x_2) + \dots + g_s(x_s)) > d_s \text{ and } g_j(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

For each $1 \leq j \leq s$, define $h_j : (\mathbb{Z}/W')^{\times(2)} \longrightarrow [0, 1]$ by setting

$$h_j(x') = f_j(x_j, x')$$

for all $x' \in (\mathbb{Z}/W')^{\times(2)}$. Note that we have $\mathbb{E}[h_j] = g_j(x_j) \neq 0$ for all $1 \leq j \leq s$ and

$$\frac{1}{s}(\mathbb{E}[h_1] + \mathbb{E}[h_2] + \dots + \mathbb{E}[h_s]) = \frac{1}{s}(g_1(x_1) + g_2(x_2) + \dots + g_s(x_s)) > d_s.$$

By induction hypothesis, we have $y' = x'_1 + x'_2 + \dots + x'_s$ for some $x'_1, x'_2, \dots, x'_s \in (\mathbb{Z}/W')^{\times(2)}$ such that

$$\frac{1}{s}(h_1(x'_1) + h_2(x'_2) + \dots + h_s(x'_s)) > d_s \text{ and } h_j(x'_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

which is the same as

$$\frac{1}{s}(f_1(x_1, x'_1) + f_2(x_2, x'_2) + \dots + f_s(x_s, x'_s)) > d_s \text{ and } f_j(x_j, x'_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

Hence, $(y, y') = (x_1, x'_1) + (x_2, x'_2) + \dots + (x_s, x'_s)$ is the desired decomposition. $\square$

4.8 Extensions to small moduli

In this section, we will extend Theorem 4.1.1 to cover the small moduli. Extensions to small moduli cause the density threshold to go up from d_s to D_s .

Proposition 4.8.1. *Let $s \geq 6, m = 5$ or $s = 5, m = 35$. Let $f : (\mathbb{Z}/m)^{\times(2)} \longrightarrow [0, 1]$ be a function with $\mathbb{E}[f] > D_s$. For all $y \in \mathbb{Z}/m$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/m)^{\times(2)}$ such that*

$$\frac{1}{s}(f(x_1) + f(x_2) + \dots + f(x_s)) > d_s \text{ and } f(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

Proof. We will divide into four different cases according to the values of s .

When $s \geq 8$:

There are two elements in $(\mathbb{Z}/5)^{\times(2)}$, which are 1 and 4. Note that $f(1)$ and $f(4)$ are nonzero since $\mathbb{E}[f] > D_s \geq 1/2$.

Observe that for all $y \in \mathbb{Z}/5$, there are two ways to write y as a sum of 1's and 4's, so that the number of 1's is not less than the number of 4's in one way, and the number of 4's is not less than the number of 1's in the other way. This is because we can consider

$$\underbrace{1 + 1 + \dots + 1}_{r \text{ times}} + \underbrace{4 + 4 + \dots + 4}_{s-r \text{ times}} = r + 4(s-r) = 4s - 3r$$

for $0 \leq r \leq 4$ and $s-4 \leq r \leq s$. Note that $4s - 3r$ ranges through all congruence classes mod 5 when r ranges through all congruence classes mod 5.

Thus, for all $y \in \mathbb{Z}/5$, we can pick a way to write $y = x_1 + x_2 + \dots + x_s$ where $x_1, x_2, \dots, x_s \in (\mathbb{Z}/5)^{\times(2)}$ so that

$$\frac{1}{s}(f(x_1) + f(x_2) + \dots + f(x_s)) \geq \mathbb{E}[f] > D_s \geq d_s.$$

When $s = 7$:

By enumerating all possibilities, we observe that for $0, 2, 3 \in \mathbb{Z}/5$, there are two ways to write them as a sum of 1's and 4's, so that the number of 1's is not less than the number of 4's in one way, and the number of 4's is not less than the number of 1's in the other way. Hence, the elements $0, 2, 3$ can be handled by the same reasoning in previous case ($s \geq 8$).

For $1, 4 \in \mathbb{Z}/5$, we have $1 = 1+1+1+1+4+4+4 \pmod{5}$ and $4 = 1+1+1+4+4+4+4 \pmod{5}$. The analysis for elements 1 and 4 is similar and we will demonstrate it for the element 1. First, note that $f(1), f(4) > 2D_7 - 1$ since $\mathbb{E}[f] = (f(1) + f(4))/2 > D_7$. To proceed, we compute

$$\frac{1}{7}(4f(1) + 3f(4)) > \frac{1}{7}(6D_7 + (2D_7 - 1)) = \frac{5}{7} = d_7.$$

When $s = 6$:

By enumerating all possibilities, we observe that for $0, 1, 4 \in \mathbb{Z}/5$, there are two ways to write them as a sum of 1's and 4's, so that the number of 1's is not less than the number of 4's in one way, and the number of 4's is not less than the number of 1's in the other way. Hence, the elements $0, 1, 4$ can be handled by the same reasoning in previous cases.

For $2, 3 \in \mathbb{Z}/5$, we have $2 = 1 + 1 + 1 + 1 + 4 + 4 \pmod{5}$ and $3 = 1 + 1 + 4 + 4 + 4 + 4 \pmod{5}$. The analysis for elements 2 and 3 is similar and we will demonstrate it for the element 2. First, note that $f(1), f(4) > 2D_6 - 1$ since $\mathbb{E}[f] = (f(1) + f(4))/2 > D_6$. To proceed, we compute

$$\frac{1}{6}(4f(1) + 2f(4)) > \frac{1}{7}(4D_6 + 2(2D_6 - 1)) = \frac{5}{6} = d_6.$$

When $s = 5$:

Since the size of $(\mathbb{Z}/35)^{\times(2)}$ is 6 and $\mathbb{E}[f] > D_5$, we have $f(x) > 6D_5 - 5$ for any $x \in (\mathbb{Z}/35)^{\times(2)}$. Note that the 5-fold sumset of $(\mathbb{Z}/35)^{\times(2)}$ is $\mathbb{Z}/35$, hence, for all $y \in \mathbb{Z}/35$, we can write $y = x_1 + x_2 + x_3 + x_4 + x_5$ for some $x_1, x_2, x_3, x_4, x_5 \in (\mathbb{Z}/35)^{\times(2)}$. To complete the proof, we compute

$$\frac{1}{5}(f(x_1) + f(x_2) + f(x_3) + f(x_4) + f(x_5)) > \frac{1}{5}(5(6D_5 - 5)) = \frac{9}{10} = d_5.$$

□

The following theorem combines Theorem 4.1.1 and Proposition 4.8.1. The method for Theorem 4.8.2 is similar to that of Shao [Sha14, Proposition 3.1] and Li and Pan [LP10, Theorem 1.2]. It might be worth to point out that the proof of Theorem 4.8.2 is similar to the inductive step of the proof of Theorem 4.1.1.

Theorem 4.8.2. *Let $s \geq 5$ be an integer, and W be a square free integer with $(24, W) = 1$. Let $f : (\mathbb{Z}/24W)^{\times(2)} \rightarrow [0, 1]$ be a function with $\mathbb{E}[f] > D_s$. For all $y \in \mathbb{Z}/24W$ with $y \equiv s \pmod{24}$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/24W)^{\times(2)}$ such that*

$$\frac{1}{s}(f(x_1) + f(x_2) + \dots + f(x_s)) > d_s \text{ and } f(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

Proof. Without loss of generality, we may assume $5|W$ when $s \geq 6$ and $35|W$ when $s = 5$. This is because if $W_1|W_2$ and Theorem 4.8.2 holds for modulus W_2 , then Theorem 4.8.2 is also true for modulus W_1 .

Write $W = mW'$ where $m = 5$ if $s \geq 6$, and $m = 35$ if $s = 5$. By Chinese remainder theorem, we can identify $(\mathbb{Z}/24W)^{\times(2)}$ with $(\mathbb{Z}/24)^{\times(2)} \times (\mathbb{Z}/m)^{\times(2)} \times (\mathbb{Z}/W')^{\times(2)}$. The elements in $(\mathbb{Z}/24W)^{\times(2)}$ can be conveniently written as $(1, x, x')$ where $x \in (\mathbb{Z}/m)^{\times(2)}$, $x' \in (\mathbb{Z}/W')^{\times(2)}$, since 1 is the only element in $(\mathbb{Z}/24)^{\times(2)}$.

Define $g : (\mathbb{Z}/m)^{\times(2)} \rightarrow [0, 1]$ by setting

$$g(x) = \mathbb{E}_{x' \in (\mathbb{Z}/W')^{\times(2)}} f(1, x, x')$$

for all $x \in (\mathbb{Z}/m)^{\times(2)}$. Note that we have $\mathbb{E}[g] = \mathbb{E}[f] > D_s$. By applying Proposition 4.8.1, for all $(s, y, y') \in \mathbb{Z}/24W$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/m)^{\times(2)}$ such that

$$\frac{1}{s}(g(x_1) + g(x_2) + \dots + g(x_s)) > d_s \text{ and } g(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

For each $1 \leq j \leq s$, define $h_j : (\mathbb{Z}/W')^{\times(2)} \rightarrow [0, 1]$ by setting

$$h_j(x') = f(1, x_j, x')$$

for all $x' \in (\mathbb{Z}/W')^{\times(2)}$. Note that we have $\mathbb{E}[h_j] = g(x_j) \neq 0$ for all $1 \leq j \leq s$ and

$$\frac{1}{s}(\mathbb{E}[h_1] + \mathbb{E}[h_2] + \dots + \mathbb{E}[h_s]) = \frac{1}{s}(g(x_1) + g(x_2) + \dots + g(x_s)) > d_s.$$

By applying Theorem 4.1.1, we have $y' = x'_1 + x'_2 + \dots + x'_s$ for some $x'_1, x'_2, \dots, x'_s \in (\mathbb{Z}/W')^{\times(2)}$ such that

$$\frac{1}{s}(h_1(x'_1) + h_2(x'_2) + \dots + h_s(x'_s)) > d_s \text{ and } h_j(x'_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

which is the same as

$$\frac{1}{s}(f(1, x_1, x'_1) + f(1, x_2, x'_2) + \dots + f(1, x_s, x'_s)) > d_s \text{ and } f(1, x_j, x'_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

Hence, $(s, y, y') = (1, x_1, x'_1) + (1, x_2, x'_2) + \dots + (1, x_s, x'_s)$ is the desired decomposition. $\square$

Now, we have all ingredients needed to deduce Theorem 1.4.3 from the transference principle. Roughly speaking, Theorem 4.8.2 is essential for completing the W -trick. We state the general transference mechanism as follow.

Hypothesis (s, μ) : *Let W be a square free integer with $(24, W) = 1$, and $f : (\mathbb{Z}/24W)^{\times(2)} \rightarrow [0, 1]$ be a function with $\mathbb{E}[f] > \mu$. For all $y \in \mathbb{Z}/24W$ with $y \equiv s \pmod{24}$, we have $y = x_1 + x_2 + \dots + x_s$ for some $x_1, x_2, \dots, x_s \in (\mathbb{Z}/24W)^{\times(2)}$ such that*

$$\frac{1}{s}(f(x_1) + f(x_2) + \dots + f(x_s)) \geq \frac{1}{2} \text{ and } f(x_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

Proposition 4.8.3. *Let $s \geq 5$ be an integer, $0 < \mu < 1$ be a real number, and A be a subset of primes with relative lower density $\delta_{\mathcal{P}}(A) > \sqrt{\mu}$. Suppose the Hypothesis (s, μ) is true, then, for all sufficiently large integers y that are congruent to $s \pmod{24}$, there exist primes $p_1, p_2, \dots, p_s \in A$ such that $y = p_1^2 + p_2^2 + \dots + p_s^2$.*

Theorem 1.4.3 indeed follows from Proposition 4.8.3 since Theorem 4.8.2 implies that Hypothesis (s, D_s) is true for $s \geq 5$. Proposition 4.8.3 is quite close to Section 3 in [LP10], where Li and Pan applied the transference principle to deduce their density version of Vinogradov three primes theorem from local results. Hence, the proof of Proposition 4.8.3 only requires slight modifications to the proof in Section 3 in [LP10], and it will be deferred to Appendix 6.3.

CHAPTER 5

The density version of the generalized Fermat equations

5.1 Overview

In this chapter, we adapt the ideas in the joint work of Chow, Mudgal and the author [CLM25] to reproduce the proofs of Theorem 1.6.1 and Theorem 1.6.4.

We would like to provide a heuristic for the proofs of Theorem 1.6.1 and Theorem 1.6.4. For simplicity, let us consider the equation

$$x_1^2 + x_2^2 + \dots + x_s^2 = 0 \tag{5.1.1}$$

over $\mathbb{F}_p$ for large p and $s \geq 3$. Let A be a subset of $\mathbb{F}_p$ with

$$|A| \geq \left(\frac{1}{s} + \kappa\right)p$$

where κ is some small parameter greater than zero.

The goal is to show that there exists a solution $\mathbf{x} \in A^s$ to the equation (5.1.1). Suppose that this is false, then we would like to reach a contradiction by showing that the cardinality of A is small.

Let

$$A' = \{x^2 : x \in A\}$$

then the s -fold sumset sA' is not $\mathbb{F}_p$, since the equation (5.1.1) is not solvable in A . By the intuition of Cauchy–Davenport inequality, we may assume that we have $s|A'| \leq p$. Note that we have trivial bound $|A'| \geq |A|/2$ since the number of square roots of an element in $\mathbb{F}_p$ is at most 2. This gives us $|A| \leq 2p/s$, which misses the threshold by a factor of 2.

For the sake of the heuristic, let us pretend that since sA' is not the entire $\mathbb{F}_p$, then A' must be close to the extremal example we have in mind—an interval. (This is in line with the intuition of Semchankau’s wrapping lemma [Sem25].) Let’s say that there exists an interval I containing A' and sI is not the entire $\mathbb{F}_p$. Once again, the intuition of Cauchy–Davenport inequality suggests that we may further assume that $s|I| \leq p$.

The interval I is much more structured than the set A' . In particular, it is not unreasonable to assume that the squares are equidistributed among intervals, that is

$$\#\{x \in \mathbb{F}_p : x^2 \in I\} \approx |I|.$$

Hence, we have $|A| \leq |I|$, which saves us a factor of 2. Combining this and the inequality $s|I| \leq p$, we deduce that $|A| \leq p/s$, leading to a contradiction.

Remark 5.1.1. Prior to [CLM25], the other combinatorial aspects of the generalized Fermat equations, such as coloring problem, have been investigated by Csikvári–Gyarmati–Sárközy [CGS12] and Lindqvist [Lin18].

This chapter is organized as follows. We record some preliminary results in Section 5.2. Section 5.3 is about a variation of Semchankau’s wrapping lemma [Sem25]. We prove Theorem 1.6.1 in Section 5.4, and we prove some equidistribution results along with Theorem 1.6.4 in Section 5.5.

5.2 Preliminaries

In this chapter, we will continue to use the Fourier analysis notation listed in Section 2.2.

5.2.1 Wrappers

We now record the notion of wrappers. These were introduced and employed by Semchankau [Sem25] to analyze various sum–product-type problems in $\mathbb{F}_p$. Let $\tau \in (0, 1)$ be a real number,

and let

$$\mathbb{S}^1 = S_1 \cup S_2 \cup \cdots \cup S_r \quad (5.2.1)$$

be a partition of $\mathbb{S}^1$ into arcs such that $\mu(S_1) = \cdots = \mu(S_{r-1}) = \tau$ and $0 < \mu(S_r) \leq \tau$. Let $\gamma_1, \dots, \gamma_d$ be pairwise distinct characters in $\widehat{G}$. For any $\mathbf{v} = (v_1, \dots, v_d) \in [r]^d$, we define the inhomogeneous Bohr set

$$B_{\mathbf{v}} = B_{\mathbf{v}, \gamma_1, \dots, \gamma_d, S_1, \dots, S_r} = \{x \in G : \gamma_i(x) \in S_{v_i} \ (1 \leq i \leq d)\}. \quad (5.2.2)$$

For ease of notation, we omit the dependence of $B_{\mathbf{v}}$ on the parameters $\gamma_1, \dots, \gamma_d, S_1, \dots, S_r$. Note that

$$G = \cup_{\mathbf{v} \in [r]^d} B_{\mathbf{v}}.$$

Given any set $X \subseteq [r]^d$, we call the set $V = \cup_{\mathbf{v} \in X} B_{\mathbf{v}}$ a (τ, d) -wrapper.

These are essentially the wrappers introduced by Semchankau [Sem25], but our definition is very slightly more general. We will use wrappers to contain — i.e. wrap — certain sets, up to a small number of elements. The advantage of using wrappers is that they have considerable average Fourier decay.

Given real numbers $0 \leq \ell_1 < \ell_2$ and any function $f : G \rightarrow [0, \infty)$, we define

$$\Delta_f(\ell_1, \ell_2) = \{x \in G : \ell_1 \leq f(x) \leq \ell_2\}.$$

The following is essentially [Sem25, Corollary 1], and can be deduced by combining elementary combinatorial arguments with a result of Croot–Łaba–Sisask [CLS13, Corollary 3.3].

Lemma 5.2.1. *Let $f : G \rightarrow [0, \infty)$, let $\tau \in (0, 1)$, and let $q > 2$ be a real number. Then there exists a positive integer $d \ll q/\tau^2$, pairwise distinct, non-trivial characters $\gamma_1, \dots, \gamma_d \in \widehat{G}$, a partition of $\mathbb{S}^1$ as in (5.2.1), and a set $Z \subseteq G$ with $|Z| \leq e^{-q}|G|$ such that the following holds. For any real numbers $0 \leq \ell_1 < \ell_2$, there exists $X \subseteq [r]^d$ such that*

$$\Delta_f(\ell_1 + \delta, \ell_2 - \delta) \setminus Z \subseteq (\cup_{\mathbf{v} \in X} B_{\mathbf{v}}) \setminus Z \subseteq \Delta_f(\ell_1 - \delta, \ell_2 + \delta) \setminus Z,$$

where $\delta = 20\|\tilde{f}\|_1\tau$.

We remark that for certain choices of ℓ_1, ℓ_2 , one could have $X = \emptyset$.

5.2.2 A popular Cauchy–Davenport lemma

The general Pollard–Kneser-type result due to Green–Ruzsa (Theorem 4.4.2) can be used to establish the following popular Kneser-type inequality, see the proof of Theorem 4.4.1.

Lemma 5.2.2. *For each $s \in \mathbb{N}$ and each $\delta, \kappa > 0$, there exist $c, M > 0$ such that the following holds. Let $\theta_1, \dots, \theta_s > \delta$ with*

$$\theta_1 + \dots + \theta_s \geq 1 + \kappa.$$

Let G be a finite abelian group G such that its largest proper subgroup H satisfies $|H| \leq |G|/M$. Then, for any $x \in G$ and any $A_1, \dots, A_s \subseteq G$ satisfying $|A_i| \geq \theta_i |G|$ for all $1 \leq i \leq s$,

$$\sum_{a_1 \in A_1, \dots, a_s \in A_s} 1_{a_1 + \dots + a_s = x} \geq c |G|^{s-1}.$$

5.2.3 Deligne’s bound

The following estimate was demonstrated by Deligne. This formulation can be found in the introduction of [Kat08], and is a special case of [Del74, Theorem 8.4].

Lemma 5.2.3. *Let $k \in \mathbb{N}$, and let p be a prime such that $p \nmid k$. Let $\mathbb{F}_q$ be a field of characteristic p , and let $\psi : \mathbb{F}_q \rightarrow \mathbb{S}^1$ be a non-trivial additive character. Let $P(x) \in \mathbb{F}_q[x]$ be a polynomial of degree k . Then*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(P(x)) \right| \leq (k-1)\sqrt{q}.$$

For the rings $\mathbb{Z}/p^n$, there are also power-saving exponential sum bounds. The following estimate follows from [Vau97, Equation 7.9] and Lemma 5.2.3.

Lemma 5.2.4. *Let $k, n \in \mathbb{N}$, and let p be a prime such that $p > k$. Let $P(x) \in (\mathbb{Z}/p^n)[x]$ be a polynomial of degree k . Then*

$$\sum_{x \in \mathbb{Z}/p^n} e_{p^n}(P(x)) \ll_k p^{n-1/k}.$$

5.3 Semchankau's wrapping lemma

Our aim in this section is to record the proof of the following variation of a result due to Semchankau [Sem25].

Theorem 5.3.1. *Let $\varepsilon, \delta \in (0, 1]$, let $s \geq 3$ be an integer, and let $A_1, \dots, A_s \subseteq G$ satisfy $|A_i| \geq \delta|G|$ for every $1 \leq i \leq s$. Suppose there exists $a \in G$ such that*

$$\sum_{a_1 \in A_1, \dots, a_s \in A_s} 1_{a_1 + \dots + a_s = a} < \varepsilon |G|^{s-1}.$$

Then, for every $1 \leq i \leq s$, there exist $\tau_i > 0$ and $d_i \in \mathbb{N}$, as well as $U_i, Y_i \subseteq G$ such that U_i is a (τ_i, d_i) -wrapper,

$$\tau_i \gg \varepsilon^{1/(2s)} \delta^{1/2} \varepsilon^{\lceil \varepsilon^{-2} \rceil}, \quad d_i \ll \tau_i^{-2} \log(10/\varepsilon)$$

and

$$|Y_i| \ll \varepsilon^{1/(2s)} |G|, \quad A_i \setminus Y_i \subseteq U_i.$$

Moreover, there exists $b \in G$ such that

$$\sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = b} \ll_s \delta^{-s} \varepsilon^{1/2} |G|^{s-1}.$$

We now present the proof of Theorem 5.3.1. We may assume that $a = 0$ by translating A_1 appropriately. Let $n \geq 2$ be an integer to be chosen later, and let

$$\Gamma = \{\gamma \in \widetilde{G} : |\widetilde{1_{A_1}}(\gamma)| > |G|/n^{1/2}\}.$$

Since $s \geq 3$,

$$\begin{aligned}
|G|^{-1} \sum_{\gamma \in \tilde{G} \setminus \Gamma} |\widetilde{1_{A_1}}(\gamma) \cdots \widetilde{1_{A_s}}(\gamma)| &\leq |G|^{s-4} \sum_{\gamma \in \tilde{G} \setminus \Gamma} |\widetilde{1_{A_1}}(\gamma) \widetilde{1_{A_2}}(\gamma) \widetilde{1_{A_3}}(\gamma)| \\
&\leq |G|^{s-4} \left(\sum_{\gamma \in \tilde{G}} |\widetilde{1_{A_2}}(\gamma)|^2 \right)^{1/2} \left(\sum_{\gamma \in \tilde{G}} |\widetilde{1_{A_3}}(\gamma)|^2 \right)^{1/2} \max_{\gamma \in \tilde{G} \setminus \Gamma} |\widetilde{1_{A_1}}(\gamma)| \\
&\leq |G|^{s-1} / n^{1/2}.
\end{aligned} \tag{5.3.1}$$

By orthogonality, one has

$$\#\Gamma |G|^2 / n \leq \sum_{\gamma \in \tilde{G}} |\widetilde{1_{A_1}}(\gamma)|^2 = |G| \#A_1 \leq |G|^2,$$

whence $\#\Gamma \leq n$.

Let $\sigma \in (0, 1)$ be a parameter to be chosen later, let S_σ be an arc of length 2σ centred at $1 \in \mathbb{S}^1$, and let B be the Bohr set

$$B = \{x \in G : \gamma(x) \in S_\sigma \text{ for all } \gamma \in \Gamma\}.$$

The Bohr set B has rank $|\Gamma| \leq n$, and so

$$|B| \geq \sigma^{|\Gamma|} |G| \geq \sigma^n |G|, \tag{5.3.2}$$

see [TV06, Lemma 4.20]. Moreover, for any $\gamma \in \Gamma$,

$$\widetilde{1_B}(\gamma) = \sum_{b \in B} \gamma(b) = |B|(1 + O(\sigma)). \tag{5.3.3}$$

Now for every $1 \leq i \leq s$, define

$$f_i(x) = |B|^{-1} (1_{A_i} * 1_B)(x) = |B|^{-1} \sum_{y \in G} 1_{A_i}(y) 1_B(x - y)$$

for all $x \in G$. These functions approximate the additive structure of 1_{A_i} on the physical side while having smoother Fourier L^1 norm, see (5.3.4) and (5.3.5) respectively. We first prove the former statement, and so, note that

$$\widetilde{f_i}(\gamma) = |B|^{-1} \widetilde{1_{A_i}}(\gamma) \widetilde{1_B}(\gamma).$$

This, in turn, implies that $|\widetilde{f}_i(\gamma)| \leq |G|/n^{1/2}$ for all $\gamma \notin \Gamma$, while $\widetilde{f}_i(\gamma) = \widetilde{1}_{A_i}(\gamma)(1 + O(\sigma))$ for all $\gamma \in \Gamma$, with the latter equality following from (5.3.3). Furthermore, (5.3.1) implies that

$$\begin{aligned} |G|^{-1} \sum_{\gamma \notin \Gamma} |\widetilde{f}_1(\gamma) \cdots \widetilde{f}_s(\gamma)| &\leq |G|^{-1} \sum_{\gamma \notin \Gamma} |\widetilde{1}_{A_1}(\gamma) \cdots \widetilde{1}_{A_s}(\gamma)| \\ &\leq |G|^{s-1}/n^{1/2}. \end{aligned}$$

Consequently,

$$\begin{aligned} \sum_{x_1, \dots, x_s} f_1(x_1) \cdots f_s(x_s) 1_{x_1 + \dots + x_s = 0} &= |G|^{-1} \sum_{\gamma} \widetilde{f}_1(\gamma) \cdots \widetilde{f}_s(\gamma) \\ &= |G|^{-1} \sum_{\gamma \in \Gamma} \widetilde{1}_{A_1}(\gamma) \cdots \widetilde{1}_{A_s}(\gamma) (1 + O(\sigma))^s + O(|G|^{s-1}/n^{1/2}) \\ &= |G|^{-1} \sum_{\gamma \in \Gamma} \widetilde{1}_{A_1}(\gamma) \cdots \widetilde{1}_{A_s}(\gamma) + O_s(|G|^{s-1}(n^{-1/2} + \sigma)) \\ &= \sum_{x_1, \dots, x_s} 1_{A_1}(x_1) \cdots 1_{A_s}(x_s) 1_{x_1 + \dots + x_s = 0} + O_s(|G|^{s-1}(n^{-1/2} + \sigma)) \\ &< \varepsilon |G|^{s-1} + O_s(|G|^{s-1} n^{-1/2} + \sigma), \end{aligned} \tag{5.3.4}$$

where the penultimate step follows from (5.3.1) and orthogonality. As for the Fourier properties of f_i , note by a straightforward application of the Cauchy–Schwarz inequality and orthogonality that

$$\|\widetilde{f}_i\|_1 = |G|^{-1} |B|^{-1} \sum_{\gamma \in \widetilde{G}} |\widetilde{1}_{A_i}(\gamma) \widetilde{1}_B(\gamma)| \leq |A_i|^{1/2} |B|^{-1/2}. \tag{5.3.5}$$

Now let $q > 2$ and $\alpha \in (0, 1)$ be parameters and, for every $1 \leq i \leq s$, let

$$\eta_i = \frac{\alpha |A_i|}{20 |G|} \quad \text{and} \quad \tau_i = \frac{\alpha |A_i|^{1/2} |B|^{1/2}}{800 |G|} \tag{5.3.6}$$

be reals lying in $(0, 1)$. For each $1 \leq i \leq s$, we apply Lemma 5.2.1 to obtain a positive integer $d_i \ll q/\tau_i^2$ and a set $Z_i \subseteq G$ with $|Z_i| \leq e^{-q} |G|$ such that, upon setting $\ell_1 = \eta_i$ and

$\ell_2 = 1 + 40\|\tilde{f}_i\|_1\tau_i$, we obtain a (τ_i, d_i) -wrapper V_i such that

$$\begin{aligned}\Delta_{f_i}(\eta_i + 20\|\tilde{f}_i\|_1\tau_i, 1 + 20\|\tilde{f}_i\|_1\tau_i) \setminus Z_i &\subseteq V_i \setminus Z_i \\ &\subseteq \Delta_{f_i}(\eta_i - 20\|\tilde{f}_i\|_1\tau_i, 1 + 60\|\tilde{f}_i\|_1\tau_i) \setminus Z_i.\end{aligned}\quad (5.3.7)$$

Let us also record some useful properties that we will need later. By (5.3.5),

$$20\|\tilde{f}_i\|_1\tau_i \leq \eta_i/2. \quad (5.3.8)$$

This, along with our choice of η_i, τ_i , implies that

$$\begin{aligned}\sum_{x \in G: f_i(x) < \eta_i + 20\|\tilde{f}_i\|_1\tau_i} f_i(x) &< (\eta_i + 20\|\tilde{f}_i\|_1\tau_i)|G| < 2\eta_i|G| \\ &= \alpha|A_i|/10 < |A_i| = \sum_{x \in G} f_i(x),\end{aligned}\quad (5.3.9)$$

whence $\Delta_{f_i}(\eta_i + 20\|\tilde{f}_i\|_1\tau_i, 1) \neq \emptyset$. Finally, the second inclusion in (5.3.7) combines with (5.3.8) to furnish

$$1_{V_i} \leq \frac{f_i}{\eta_i - 20\|\tilde{f}_i\|_1\tau_i} + 1_{Z_i} \leq \frac{2f_i}{\eta_i} + 1_{Z_i} \leq 2\eta_i^{-1}(f_i + 1_{Z_i}). \quad (5.3.10)$$

We now establish some desirable additive properties of $V_1, \dots, V_s$. Inequality (5.3.10) gives us

$$\begin{aligned}&\sum_{v_1 \in V_1, \dots, v_s \in V_s} 1_{v_1 + \dots + v_s = 0} \\ &\leq \sum_{x_1, \dots, x_s \in G} \prod_{i=1}^s 2\eta_i^{-1}(f_i(x_i) + 1_{Z_i}(x_i)) 1_{x_1 + \dots + x_s = 0} \\ &\ll_s (\eta_1 \cdots \eta_s)^{-1} \left(\sum_{x_1, \dots, x_s \in G} f_1(x_1) \cdots f_s(x_s) 1_{x_1 + \dots + x_s = 0} + e^{-q}|G|^{s-1} \right).\end{aligned}$$

The assumption that $|A_i| \geq \delta|G|$ along with the definition of η_i in (5.3.6) imply that $\eta_i \gg \alpha\delta$ for every $1 \leq i \leq s$. This in turn combines with the preceding inequality and (5.3.4) to deliver the estimate

$$\sum_{v_1 \in V_1, \dots, v_s \in V_s} 1_{v_1 + \dots + v_s = 0} \ll_s \alpha^{-s} \delta^{-s} |G|^{s-1} (\varepsilon + n^{-1/2} + \sigma + e^{-q}).$$

Setting

$$n = \lceil \varepsilon^{-2} \rceil, \quad \sigma = \varepsilon \quad \text{and} \quad q = \log(10/\varepsilon) \quad (5.3.11)$$

yields

$$\sum_{v_1 \in V_1, \dots, v_s \in V_s} 1_{v_1 + \dots + v_s = 0} \ll_s \varepsilon \alpha^{-s} \delta^{-s} |G|^{s-1}. \quad (5.3.12)$$

Given $1 \leq i \leq s$ and $b \in B$, define

$$A_{i,b} = \{a \in A_i : f_i(a+b) < \eta_i + 20\|\tilde{f}_i\|_1 \tau_i\}.$$

Let $b_i \in B$ satisfy $|A_{i,b_i}| \leq |A_{i,b}|$ for all $b \in B$. A standard averaging argument, together with (5.3.9), gives

$$|A_{i,b_i}| \leq |B|^{-1} \sum_{b \in B} |A_{i,b}| = \sum_{x \in G : f_i(x) < \eta_i + 20\|\tilde{f}_i\|_1 \tau_i} f_i(x) < \alpha |A_i|/10.$$

Now, if $a \in A_i \setminus A_{i,b_i}$, then $f_i(a+b_i) \geq \eta_i + 20\|\tilde{f}_i\|_1 \tau_i$, which in turn combines with the first inclusion in (5.3.7) to tell us that either $a+b_i \in Z_i$ or $a+b_i \in V_i$. For every $1 \leq i \leq s$, we set

$$U_i = V_i - b_i \quad \text{and} \quad Y_i = A_{i,b_i} \cup (Z_i - b_i).$$

Then

$$|Y_i| \leq \alpha |A_i|/10 + e^{-q} |G| \ll \alpha |G| + \varepsilon |G|.$$

Setting $\alpha = \varepsilon^{1/(2s)}$ delivers the desired upper bound for $|Y_i|$. Moreover, note that $A_i \setminus Y_i \subseteq U_i$ and

$$\begin{aligned} \sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = -b_1 - \dots - b_s} &= \sum_{v_1 \in V_1, \dots, v_s \in V_s} 1_{v_1 + \dots + v_s = 0} \\ &\ll \varepsilon^{1/2} \delta^{-s} |G|^{s-1}, \end{aligned}$$

using (5.3.12) and the fact that $\alpha = \varepsilon^{1/(2s)}$.

The simple observation that translates of (τ_i, d_i) -wrappers are also (τ_i, d_i) -wrappers ensures that U_i is a (τ_i, d_i) -wrapper. Our choice of τ_i in (5.3.6) along with (5.3.2) and (5.3.11)

implies that

$$\tau_i \gg \alpha \delta^{1/2} \sigma^{n/2} \gg \varepsilon^{1/(2s)} \delta^{1/2} \varepsilon^{\lceil \varepsilon^{-2} \rceil}.$$

Finally, since $d_i \ll q/\tau_i^2$, our choice of q dispenses the estimate

$$d_i \ll \tau_i^{-2} \log(10/\varepsilon).$$

This concludes the proof of Theorem 5.3.1.

5.4 Finite fields

This section will culminate in a proof of Theorem 1.6.1. Here $q = p^n$, for some prime p and some $n \in \mathbb{N}$. For $\alpha, x \in \mathbb{F}_q$, let

$$\psi_\alpha(x) = e_p(\text{Tr}(\alpha x)) = \psi_1(\alpha x).$$

5.4.1 Equidistribution of powers

Lemma 5.4.1. *Let r be a positive integer, let $X_1, \dots, X_r$ be non-empty subsets of $\mathbb{F}_q$, and let $1 \leq i_1 < i_2 < \dots < i_r < p$ be integers. Then*

$$\begin{aligned} & \#\{m \in \mathbb{F}_q : m^{i_j} \in X_j \ (1 \leq j \leq r)\} - \frac{|X_1| \cdots |X_r|}{q^{r-1}} \\ & \ll_{i_r} \|\widetilde{\mathbf{1}_{X_1}}\|_1 \cdots \|\widetilde{\mathbf{1}_{X_r}}\|_1 \sqrt{q}. \end{aligned}$$

Proof. Put $X = X_1 \times \dots \times X_r$. By orthogonality,

$$\begin{aligned} & \#\{m \in \mathbb{F}_q : m^{i_j} \in X_j \ (1 \leq j \leq r)\} \\ &= \sum_{m \in \mathbb{F}_q} \sum_{\mathbf{x} \in X} \mathbf{1}_{m^{i_1}=x_1} \cdots \mathbf{1}_{m^{i_r}=x_r} \\ &= q^{-r} \sum_{\alpha \in \mathbb{F}_q^r} \sum_{\mathbf{x} \in X} \psi_1(-\alpha \cdot \mathbf{x}) \sum_{m \in \mathbb{F}_q} \psi_1(\alpha_1 m^{i_1} + \dots + \alpha_r m^{i_r}) \\ &= q^{-r} \sum_{\alpha \in \mathbb{F}_q^r} \widetilde{\mathbf{1}_{X_1}}(\psi_{\alpha_1}) \cdots \widetilde{\mathbf{1}_{X_r}}(\psi_{\alpha_r}) \sum_{m \in \mathbb{F}_q} \psi_1(\alpha_1 m^{i_1} + \dots + \alpha_r m^{i_r}). \end{aligned}$$

Thus, by Lemma 5.2.3,

$$\begin{aligned}
& \left| \#\{m \in \mathbb{F}_q : m^{i_j} \in X_j \ (1 \leq j \leq r)\} - \frac{|X_1| \cdots |X_r|}{q^{r-1}} \right| \\
& \leq q^{-r} \sum_{\mathbf{0} \neq \boldsymbol{\alpha} \in \mathbb{F}_q^r} |\widetilde{1_{X_1}}(\alpha_1) \cdots \widetilde{1_{X_r}}(\alpha_r)| \sum_{m \in \mathbb{F}_q} \psi_1(\alpha_1 m^{i_1} + \cdots + \alpha_r m^{i_r})| \\
& \leq \|\widetilde{1_{X_1}}\|_1 \cdots \|\widetilde{1_{X_r}}\|_1 i_r \sqrt{q}.
\end{aligned}
\tag*{$\square$}$$

5.4.2 Average Fourier decay

As an additive group, we can identify $\mathbb{F}_q$ with $G = \mathbb{F}_p^n$. In this subsection, we use $\langle \cdot, \cdot \rangle$ interchangeably with the dot product on G . Let $\mathbf{r} \in G$ and

$$\psi_{\mathbf{r}}(\mathbf{x}) = e_p(\mathbf{r} \cdot \mathbf{x}).$$

Bohr sets of rank 1 for this additive character have the form

$$B = \left\{ \mathbf{x} \in G : \left\| \frac{\mathbf{r} \cdot \mathbf{x} - c}{p} \right\| \leq \delta \right\},$$

where $c \in \mathbb{Z}$ and $0 < \delta \leq 1/2$.

In the case $m = 1$, it follows from [Sem25, Proposition 3.2] and the proof of [Sem25, Proposition 3.3] that

$$\|\widetilde{1_B}\|_1 \ll \log p. \tag{5.4.1}$$

We now extend this to the case of general m .

Lemma 5.4.2. *We have (5.4.1).*

Proof. First suppose $\mathbf{r} = \mathbf{0}$. Then B is either empty or G . If B is empty, then $\|\widetilde{1_B}\|_1 = 0$. If $B = G$, then

$$\|\widetilde{1_B}\|_1 = |G|^{-1} |\widetilde{1_G}(\mathbf{0})| = 1.$$

It suffices to consider two other cases for $\mathbf{r}$, namely:

1. $\mathbf{r} \cdot \mathbf{r} \neq 0$

2. $\mathbf{r} \cdot \mathbf{r} = 0$.

Let $\ell \in G \setminus H$, where

$$H = \{\mathbf{x} \in G : \mathbf{r} \cdot \mathbf{x} = 0\}.$$

In Case I, we choose $\ell = \mathbf{r}$ for simplicity.

We decompose

$$G = H \oplus \mathbb{F}_p \ell.$$

This restricts to a decomposition

$$B = H + U\ell,$$

where

$$U = \left\{ u \in \mathbb{F}_p : \left\| \frac{u\ell \cdot \mathbf{r} - c}{p} \right\| \leq \delta \right\},$$

and each element of B is $\mathbf{h} + u\ell$ for some unique pair $(\mathbf{h}, u) \in H \times U$. Now

$$\widetilde{1}_B(\boldsymbol{\xi}) = \sum_{\mathbf{x} \in B} e_p(-\mathbf{x} \cdot \boldsymbol{\xi}),$$

so

$$\begin{aligned} \|\widetilde{1}_B\|_1 &= p^{-m} \sum_{\substack{\boldsymbol{\xi}_0 \in H \\ v \in \mathbb{F}_p}} \left| \sum_{u \in U} \sum_{\mathbf{h} \in H} e_p(\langle \mathbf{h} + u\ell, \boldsymbol{\xi}_0 + v\ell \rangle) \right| \\ &= p^{-m} \sum_{\substack{\boldsymbol{\xi}_0 \in H \\ v \in \mathbb{F}_p}} \left| \sum_{u \in U} e_p(u\langle \ell, \boldsymbol{\xi}_0 + v\ell \rangle) \sum_{\mathbf{h} \in H} e_p(\langle \mathbf{h}, \boldsymbol{\xi}_0 + v\ell \rangle) \right|. \end{aligned}$$

The inner sum vanishes unless $\boldsymbol{\xi}_0 + v\ell = \lambda \mathbf{r}$ for some $\lambda \in \mathbb{F}_p$.

Case 1

In this case $\ell = \mathbf{r}$. For the inner sum not to vanish, we must have $\boldsymbol{\xi}_0 \parallel \mathbf{r}$ and hence $\boldsymbol{\xi}_0 = \mathbf{0}$, since $\mathbf{r} \cdot \boldsymbol{\xi}_0 = 0$ and $\mathbf{r} \cdot \mathbf{r} \neq 0$. Consequently,

$$\|\widetilde{1}_B\|_1 = p^{-1} \sum_{v \in \mathbb{F}_p} \left| \sum_{u \in U} e_p(uvr \cdot \mathbf{r}) \right| = p^{-1} \sum_{v \in \mathbb{F}_p} \left| \sum_{u \in U} e_p(uv) \right|.$$

This is $O(\log p)$, as we saw in the case $m = 1$.

Case 2

As $\ell \notin H$ and $\xi_0, \mathbf{r} \in H$, we cannot have $\xi_0 + v\ell = \lambda\mathbf{r}$ unless $v = 0$ and $\xi_0 = \lambda\mathbf{r}$.

Therefore

$$\|\widetilde{1_B}\|_1 = p^{-1} \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{u \in U} e_p(u\lambda\ell \cdot \mathbf{r}) \right| = p^{-1} \sum_{\lambda \in \mathbb{F}_p} \left| \sum_{u \in U} e_p(u\lambda) \right|.$$

This is $O(\log p)$, as in Case 1. □

We can bootstrap this to infer average Fourier decay for wrappers.

Lemma 5.4.3. *Let U be a (τ, d) -wrapper in $\mathbb{F}_q$. Then*

$$\|\widetilde{1_U}\|_1 \ll_{\tau, d} (\log p)^d.$$

Proof. By definition, the wrapper U is a disjoint union of $O_{\tau, d}(1)$ many sets $B = B_{\mathbf{v}}$ as given by (5.2.2), and so, by a simple application of triangle inequality, it suffices to prove the desired result for the set $B_{\mathbf{v}}$. In this case, note that we can write

$$B = B_1 \cap \cdots \cap B_d,$$

for some Bohr sets $B_1, \dots, B_d$ of rank 1. Finally, Young's convolution inequality and Lemma 5.4.1 deliver

$$\begin{aligned} \|\widetilde{1_B}\|_1 &= \|\widetilde{1_{B_1} \cdots 1_{B_d}}\|_1 = \|\widetilde{1_{B_1}} * \cdots * \widetilde{1_{B_d}}\|_1 \\ &\leq \|\widetilde{1_{B_1}}\|_1 \cdots \|\widetilde{1_{B_d}}\|_1 \ll (\log p)^d. \end{aligned} \quad \square$$

5.4.3 Dense Fermat over finite fields

We now establish Theorem 1.6.1. Assume for a contradiction that there are fewer than εq^{s-1} many solutions $\mathbf{x} \in A^s$ to (1.6.2). Define

$$A_m = \{c_m a^{i_j} : a \in A\}$$

for all $m \in I_j$ and all $1 \leq j \leq r$. Note that $|A_m| \geq |A|/i_r \gg_{i_r, s} q$. We may now apply Theorem 5.3.1 to find, for every $1 \leq i \leq s$, a (τ_i, d_i) -wrapper U_i with $\tau_i \gg_{\varepsilon, s, i_r} 1$ and $d_i \ll_{\varepsilon, s, i_r} 1$ such that

$$|A_i \setminus U_i| \ll \varepsilon^{1/(2s)} q$$

and

$$\sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = b} \ll_{s, i_r} \varepsilon^{1/2} q^{s-1}, \quad (5.4.2)$$

for some $b \in \mathbb{F}_q$.

We now claim that

$$|U_1| + \dots + |U_s| < \left(1 + \frac{\kappa}{10}\right) q. \quad (5.4.3)$$

We prove this claim via contradiction, so let us assume that it does not hold. Let C be a large, positive constant. As ε is sufficiently small, we have

$$|U_i| \geq |A_i| - C\varepsilon^{1/(2s)} q \gg_{i_r, s} q$$

for all $1 \leq i \leq s$. We may now apply Lemma 5.2.2, giving

$$\sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = b} \gg_{s, i_r, \kappa} q^{s-1}.$$

As ε is sufficiently small in terms of s, i_r, κ , this contradicts (5.4.2).

We may therefore assume that (5.4.3) holds. For every $\mathbf{m} \in I_1 \times \dots \times I_r$, let

$$X_{\mathbf{m}} = \{x \in \mathbb{F}_q : c_{m_j} x^{i_j} \in U_{m_j} \ (1 \leq j \leq r)\}.$$

By Lemma 5.4.3 and a change of variables, we note that if U is a (τ, d) -wrapper in $\mathbb{F}_q$ and $c \in \mathbb{F}_q^\times$ then

$$\|\widetilde{1_{cU}}\|_1 \ll_{\tau, d} (\log p)^d.$$

Combining this with Lemma 5.4.1 yields

$$|X_{\mathbf{m}}| - \frac{|U_{m_1}| \dots |U_{m_r}|}{q^{r-1}} \ll_{s, i_r, \varepsilon} (\log p)^{O_{\varepsilon, s, i_r}(1)} q^{1/2}.$$

Since $|A_i \setminus U_i| \ll \varepsilon^{1/(2s)} q$ for all $1 \leq i \leq s$,

$$|A| \leq |X_{\mathbf{m}}| + O_{i_r, s}(\varepsilon^{1/(2s)} q).$$

Coupling this with the preceding bound, and then averaging over all $\mathbf{m} \in I_1 \times \cdots \times I_r$, gives

$$\begin{aligned} \frac{|A|}{q} &\leq \frac{1}{k_1 \cdots k_r} \sum_{\mathbf{m} \in I_1 \times \cdots \times I_r} \frac{|U_{m_1}| \cdots |U_{m_r}|}{q^r} \\ &\quad + O_{s, i_r}(\varepsilon^{1/(2s)}) + O_{\varepsilon, i_r, s}((\log p)^{O_{\varepsilon, s, i_r}(1)} q^{-1/2}). \end{aligned} \quad (5.4.4)$$

Clearly, we may assume that κ is sufficiently small in terms of r . We may also assume that ε is a function of s, i_r, κ , as the result would then follow for all smaller values of ε . This enables us to subsume any dependence on ε into the dependence on s, i_r, κ .

By the AM–GM inequality and (5.4.3), the first term on the right-hand side of (5.4.4) is bounded above by

$$\begin{aligned} \frac{1}{q^r k_1 \cdots k_r} \left(r^{-1} \sum_{j=1}^r \sum_{m_j \in I_j} |U_{m_j}| \right)^r &\leq \frac{(1 + \kappa/10)^r}{k_1 \cdots k_r r^r} \\ &\leq \frac{1 + r\kappa/5}{k_1 \cdots k_r r^r} \leq \prod_{1 \leq j \leq r} \frac{1}{rk_j} + \frac{\kappa}{5}. \end{aligned}$$

The other terms on the right-hand side of (5.4.4) are smaller than $\kappa/5$. Therefore

$$|A| < \left(\prod_{1 \leq j \leq r} \frac{1}{rk_j} + \frac{3\kappa}{5} \right) q,$$

contradicting the hypothesis (1.6.1). Hence, we must have at least εq^{s-1} many solutions to (1.6.2) with $x_1, \dots, x_s \in A$.

5.5 Finite, cyclic rings

In this section, we will first prove that the wrappers are nicely additively structured, in the sense that the powers are equidistributed among them. Then we will use this property to deduce Theorem 1.6.4.

5.5.1 Equidistribution of powers in wrappers

Let W be a positive integer, let $\beta_1, \beta_2, \dots, \beta_d \in \mathbb{Z}/W$ be frequencies, and let $\mathbb{I}_1, \mathbb{I}_2, \dots, \mathbb{I}_d$ be real intervals. The inhomogeneous Bohr set

$$B = B(\beta_1, \beta_2, \dots, \beta_d; \mathbb{I}_1, \mathbb{I}_2, \dots, \mathbb{I}_d)$$

is defined to be

$$= \left\{ x \in \mathbb{Z}/W : \frac{\beta_j x}{W} \in \mathbb{I}_j \bmod 1 \text{ for all } 1 \leq j \leq d \right\}.$$

We refer to d as the *rank* of B . (Strictly speaking, the rank is a property of the Bohr set data, rather than a property of the set.)

The following lemma, which is in the same spirit as Lemma 5.4.2, asserts that the inhomogeneous Bohr sets in $\mathbb{Z}/p^n$ have considerable average Fourier decay.

Lemma 5.5.1. *Let p be a prime, let $n \in \mathbb{N}$, and let B be an inhomogeneous Bohr set of rank d in $\mathbb{Z}/p^n$. Then*

$$\|\widetilde{1_B}\|_1 \leq (C \log p^n)^d,$$

where C is some absolute constant.

Proof. First, we consider the case where the Bohr set B has rank 1. Say $B = B(p^\ell \beta; \mathbb{I})$, where β is not divisible by p and $\ell < n$.

Note that for $x \in \mathbb{Z}/p^n$, whether $p^\ell \beta x / p^n = \beta x / p^{n-\ell}$ is in $\mathbb{I}$ depends only on the residue class of $x \bmod p^{n-\ell}$. Thus, the Bohr set B is of the form $Q + H$, where Q is an arithmetic progression mod $p^{n-\ell}$ with common difference z not divisible by p , and H is the subgroup of $\mathbb{Z}/p^n$ generated by the element $p^{n-\ell}$. With this description, we can compute $\widetilde{1_B}$ explicitly.

Indeed,

$$\begin{aligned}
\widetilde{1}_B(\xi) &= \sum_{q \in Q} \sum_{0 \leq x < p^\ell} e_{p^n}((q + xp^{n-\ell})\xi) = \sum_{q \in Q} e_{p^n}(q\xi) \sum_{0 \leq x < p^\ell} e_{p^\ell}(x\xi) \\
&= \begin{cases} 0, & \text{if } p^\ell \nmid \xi \\ p^\ell \sum_{q \in Q} e_{p^n}(q\xi), & \text{if } p^\ell \mid \xi \end{cases} \\
&\ll \begin{cases} 0, & \text{if } p^\ell \nmid \xi \\ p^\ell \left\| \frac{\xi z}{p^n} \right\|_{\mathbb{R}/\mathbb{Z}}^{-1}, & \text{if } p^\ell \mid \xi. \end{cases}
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\sum_{\xi \in \mathbb{Z}/p^n} |\widetilde{1}_B(\xi)| &\ll p^n + p^\ell \sum_{1 \leq \eta < p^{n-\ell}} \left\| \frac{\eta z}{p^{n-\ell}} \right\|_{\mathbb{R}/\mathbb{Z}}^{-1} \\
&\ll p^n + p^\ell \sum_{1 \leq \eta < p^{n-\ell}} \frac{p^{n-\ell}}{\eta} \ll p^n \log(p^n),
\end{aligned}$$

which gives the desired bound.

For higher-rank Bohr sets, we observe that $\|\widetilde{1}_B \widetilde{1}_{B'}\|_1 \leq \|\widetilde{1}_B\|_1 \|\widetilde{1}_{B'}\|_1$ for any Bohr sets B, B' by Young's inequality. Hence, combining this inequality and the fact that higher-rank Bohr sets are intersections of rank 1 Bohr sets completes the proof. $\square$

Next, we will prove that the powers are equidistributed among the inhomogeneous Bohr sets in $\mathbb{Z}/p^n$.

Proposition 5.5.2. *Let $i_1 < \dots < i_r$ be positive integers. Let $p > i_r$ be prime, let $n \in \mathbb{N}$, and let $B_1, \dots, B_r$ be inhomogeneous Bohr sets of rank d in $\mathbb{Z}/p^n$. Let $c_1, \dots, c_r \in (\mathbb{Z}/p^n)^\times$. Then*

$$\begin{aligned}
\sum_{x \in \mathbb{Z}/p^n} 1_{B_1}(c_1 x^{i_1}) \cdots 1_{B_r}(c_r x^{i_r}) &= |B_1| \cdots |B_r| p^{-n(r-1)} \\
&\quad + O_{i_r, d}(p^{n-1/i_r} \log^{dr} p^n).
\end{aligned}$$

Proof. By Fourier expansion and Lemma 5.2.4,

$$\begin{aligned}
& \sum_{x \in \mathbb{Z}/p^n} 1_{B_1}(c_1 x^{i_1}) \cdots 1_{B_r}(c_r x^{i_r}) \\
&= p^{-nr} \sum_{x \in \mathbb{Z}/p^n} \sum_{\xi_1, \dots, \xi_r \in \mathbb{Z}/p^n} \widetilde{1_{B_1}}(\xi_1) \cdots \widetilde{1_{B_r}}(\xi_r) \\
&\quad \cdot e_{p^n}(-\xi_1 c_1 x^{i_1} - \cdots - \xi_r c_r x^{i_r}) \\
&= |B_1| \cdots |B_r| p^{-n(r-1)} + O_{i_r}(p^{n-1/i_r} \|\widetilde{1_{B_1}}\|_1 \cdots \|\widetilde{1_{B_r}}\|_1).
\end{aligned}$$

Thus, applying Lemma 5.5.1 gives the desired error term. $\square$

To extend Proposition 5.5.2 to general moduli $W = p_1^{n_1} \cdots p_t^{n_t}$, such Fourier-analytic arguments are — perhaps surprisingly — less effective. The reason is that the analysis of Hardy–Littlewood major arcs in $\mathbb{Z}/W$ is more delicate; on some non-zero major arcs we only save $\sqrt{p_1}$ over the trivial exponential sum bound, but p_1 might be considerably smaller than other prime factors, rendering this saving not as large as we would like. To overcome this issue, we argue in the physical space and utilize the product structure of $\mathbb{Z}/W$ to deduce the following proposition.

Proposition 5.5.3. *Let $i_1 < \cdots < i_r$ be positive integers. Let*

$$W = p_1^{n_1} \cdots p_t^{n_t} \quad \text{with} \quad p_1, \dots, p_t > i_r,$$

and let $B_1, B_2, \dots, B_r$ be inhomogeneous Bohr sets of rank d in $\mathbb{Z}/W$. Let $c_1, \dots, c_r \in (\mathbb{Z}/W)^\times$. Then

$$\begin{aligned}
\sum_{x \in \mathbb{Z}/W} 1_{B_1}(c_1 x^{i_1}) \cdots 1_{B_r}(c_r x^{i_r}) &= |B_1| \cdots |B_r| W^{-(r-1)} \\
&\quad + O_{i_r, d} \left(W \sum_{1 \leq j \leq t} \frac{\log^{dr} p_j^{n_j}}{p_j^{1/i_r}} \right).
\end{aligned}$$

Proof. We will prove Proposition 5.5.3 by induction on the number of prime factors t . The base case $t = 1$ is given by Proposition 5.5.2.

When $t > 1$, write $W = p_1^{n_1} W'$. Let $f_j = 1_{B_j}$ for $1 \leq j \leq r$. We can regard f_j as functions on $\mathbb{Z}/p_1^{n_1} \times \mathbb{Z}/W'$, by the Chinese remainder theorem. Note that

$$\begin{aligned} & \sum_{x \in \mathbb{Z}/W} 1_{B_1}(c_1 x^{i_1}) \cdots 1_{B_r}(c_r x^{i_r}) \\ &= \sum_{z \in \mathbb{Z}/W'} \sum_{y \in \mathbb{Z}/p_1^{n_1}} f_1(c_1 y^{i_1}, c_1 z^{i_1}) \cdots f_r(c_r y^{i_r}, c_r z^{i_r}). \end{aligned} \quad (5.5.1)$$

The key observation is that a slice of a Bohr set is still a Bohr set of the same rank, that is, we can regard $f_j(\cdot, v)$ as the characteristic function of a Bohr set in $\mathbb{Z}/p_1^{n_1}$, for $v \in \mathbb{Z}/W'$ and $1 \leq j \leq r$. To justify this observation, note that the canonical isomorphism

$$\mathbb{Z}/p_1^{n_1} \times \mathbb{Z}/W' \simeq \mathbb{Z}/W$$

is given by $(u, v) \mapsto uW'\Gamma + vp_1^{n_1}\gamma$, where Γ is the multiplicative inverse of W' in $\mathbb{Z}/p_1^{n_1}$ and γ is the multiplicative inverse of $p_1^{n_1}$ in $\mathbb{Z}/W'$. Now, for any $\beta \in \mathbb{Z}/W$ and interval $\mathbb{I}$, we have

$$\frac{\beta(uW'\Gamma + vp_1^{n_1}\gamma)}{W} \in \mathbb{I} \iff \frac{\beta\Gamma u}{p_1^{n_1}} \in \mathbb{I} - \frac{\beta v \gamma}{W'},$$

hence $f_j(\cdot, v)$ is the characteristic function of a Bohr set of the same rank as B_j in $\mathbb{Z}/p_1^{n_1}$.

By Proposition 5.5.2, the expression (5.5.1) is equal to

$$\begin{aligned} & \sum_{z \in \mathbb{Z}/W'} \left(p_1^{-n_1(r-1)} \prod_{1 \leq j \leq r} \sum_{\eta_j \in \mathbb{Z}/p_1^{n_1}} f_j(\eta_j, c_j z^{i_j}) \right. \\ & \quad \left. + O_{i_r, d}(p_1^{n_1-1/i_r} \log^{dr} p_1^{n_1}) \right). \end{aligned} \quad (5.5.2)$$

Summing over $\mathbb{Z}/W'$, the error term in (5.5.2) is $O_{i_r, d}(W p_1^{-1/i_r} \log^{dr} p_1^{n_1})$. For the main term, we apply the induction hypothesis for each $\eta_1, \dots, \eta_r$ — once again, we use the fact that the

slicing of a Bohr set is still a Bohr set of the same rank — to obtain

$$\begin{aligned}
& p_1^{-n_1(r-1)} \sum_{\mathfrak{y}_1, \dots, \mathfrak{y}_r \in \mathbb{Z}/p_1^{n_1}} \sum_{z \in \mathbb{Z}/W'} f_1(\mathfrak{y}_1, c_1 z^{i_1}) \cdots f_r(\mathfrak{y}_r, c_r z^{i_r}) \\
&= p_1^{-n_1(r-1)} \sum_{\mathfrak{y}_1, \dots, \mathfrak{y}_r \in \mathbb{Z}/p_1^{n_1}} \left((W')^{-(r-1)} \prod_{1 \leq j \leq r} \sum_{\mathfrak{z}_j \in \mathbb{Z}/W'} f_j(\mathfrak{y}_j, \mathfrak{z}_j) \right. \\
&\quad \left. + O_{i_r, d} \left(W' \sum_{2 \leq j \leq t} p_j^{-1/i_r} \log^{dr} p_j^{n_j} \right) \right). \tag{5.5.3}
\end{aligned}$$

Summing over $\mathfrak{y}_1, \dots, \mathfrak{y}_r$ and multiplying by $p_1^{-n_1(r-1)}$, the error term in (5.5.3) is

$$O_{i_r, d} \left(W \sum_{2 \leq j \leq t} p_j^{-1/i_r} \log^{dr} p_j^{n_j} \right),$$

while the main term is

$$\begin{aligned}
& W^{-(r-1)} \sum_{\mathfrak{y}_1, \dots, \mathfrak{y}_r \in \mathbb{Z}/p_1^{n_1}} \sum_{\mathfrak{z}_1, \dots, \mathfrak{z}_r \in \mathbb{Z}/W'} f_1(\mathfrak{y}_1, \mathfrak{z}_1) \cdots f_r(\mathfrak{y}_r, \mathfrak{z}_r) \\
&= W^{-(r-1)} |B_1| \cdots |B_r|. \quad \square
\end{aligned}$$

Since wrappers are disjoint unions of Bohr sets, we can write the characteristic functions of wrappers as sums of characteristic functions of Bohr sets to obtain the following corollary.

Corollary 5.5.4. *Let $i_1 < \cdots < i_r$ and D be positive integers. Let*

$$W = p_1^{n_1} \cdots p_t^{n_t} \quad \text{with} \quad p_1, \dots, p_t > i_r,$$

and let U_j be a (τ_j, d_j) -wrapper in $\mathbb{Z}/W$, with $\tau_j \geq D^{-1}$ and $d_j \leq D$ for $1 \leq j \leq r$. Let $c_1, \dots, c_r \in (\mathbb{Z}/W)^\times$. Then

$$\begin{aligned}
& \sum_{x \in \mathbb{Z}/W} 1_{U_1}(c_1 x^{i_1}) \cdots 1_{U_r}(c_r x^{i_r}) = |U_1| \cdots |U_r| W^{-(r-1)} \\
&\quad + O_{i_r, D} \left(W \sum_{1 \leq j \leq t} \frac{\log^{Dr} p_j^{n_j}}{p_j^{1/i_r}} \right).
\end{aligned}$$

5.5.2 Dense Fermat over finite, cyclic rings

We now establish Theorem 1.6.4. Recall that ε is sufficiently small depending on s, i_r, κ, Ω , and that M is sufficiently large depending on s, i_r, κ, Ω . Over the course of the proof, we will explain how small ε has to be and how large M has to be, albeit implicitly. We will work in $\mathbb{Z}/W$, where $W = p_1^{n_1} \cdots p_t^{n_t}$ with (1.6.4). Without loss of generality, we may assume that $A \subseteq (\mathbb{Z}/W)^\times$, at the cost of changing (1.6.5) to

$$|A| \geq \left(\prod_{1 \leq j \leq r} \frac{1}{rk_j} + \frac{9}{10}\kappa \right) W, \quad (5.5.4)$$

since there are at most $O_\Omega(W/M)$ many elements that are not invertible.

Assume for a contradiction that there are fewer than εW^{s-1} many solutions $\mathbf{x} \in A^s$ to (1.6.2). Define

$$A_m = \{c_m a^{i_j} : a \in A\}$$

for all $m \in I_j$ and all $1 \leq j \leq r$. Note that $|A_m| \geq |A|/i_r^\Omega \gg_{i_r, s, \Omega} W$ since $A \subseteq (\mathbb{Z}/W)^\times$. We may now apply Theorem 5.3.1 to find — for every $1 \leq i \leq s$ — a (τ_i, d_i) -wrapper U_i with $\tau_i \gg_{\varepsilon, s, i_r, \Omega} 1$ and $d_i \ll_{\varepsilon, s, i_r, \Omega} 1$ such that

$$|A_i \setminus U_i| \ll \varepsilon^{1/(2s)} W$$

and

$$\sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = b} \ll_{s, i_r, \Omega} \varepsilon^{1/2} W^{s-1}, \quad (5.5.5)$$

for some $b \in \mathbb{Z}/W$.

We now claim that

$$|U_1| + \dots + |U_s| < \left(1 + \frac{\kappa}{10}\right) W. \quad (5.5.6)$$

We prove this claim via contradiction, so let us assume that it does not hold. Let C be a large, positive constant. As ε is sufficiently small, we have

$$|U_i| \geq |A_i| - C\varepsilon^{1/(2s)} W \gg_{i_r, s, \Omega} W$$

for all $1 \leq i \leq s$. We may now apply Lemma 5.2.2, giving

$$\sum_{w_1 \in U_1, \dots, w_s \in U_s} 1_{w_1 + \dots + w_s = b} \gg_{s, i_r, \kappa, \Omega} W^{s-1}.$$

As ε is sufficiently small, this contradicts (5.5.5).

We may therefore assume that (5.5.6) holds. For every $\mathbf{m} \in I_1 \times \dots \times I_r$, let

$$X_{\mathbf{m}} = \{x \in \mathbb{Z}/W : c_{m_j} x^{i_j} \in U_{m_j} \ (1 \leq j \leq r)\}.$$

By Corollary 5.5.4,

$$\begin{aligned} |X_{\mathbf{m}}| &= |U_{m_1}| \dots |U_{m_r}| W^{-(r-1)} \\ &\quad + O_{\varepsilon, s, i_r, \Omega} \left(W \sum_{1 \leq j \leq t} p_j^{-1/i_r} \log^{O_{\varepsilon, s, i_r, \Omega}(1)} p_j \right). \end{aligned} \quad (5.5.7)$$

Since $|A_i \setminus U_i| \ll \varepsilon^{1/(2s)} W$ for all $1 \leq i \leq s$,

$$|A| \leq |X_{\mathbf{m}}| + O_{s, i_r, \Omega}(\varepsilon^{1/(2s)} W).$$

Coupling this with the preceding bound, and then averaging over all $\mathbf{m} \in I_1 \times \dots \times I_r$, gives

$$\begin{aligned} \frac{|A|}{W} &\leq \frac{1}{k_1 \dots k_r} \sum_{\mathbf{m} \in I_1 \times \dots \times I_r} \frac{|U_{m_1}| \dots |U_{m_r}|}{W^r} \\ &\quad + O_{s, i_r, \Omega}(\varepsilon^{1/(2s)}) + O_{\varepsilon, s, i_r, \Omega} \left(\sum_{1 \leq j \leq t} p_j^{-1/i_r} \log^{O_{\varepsilon, s, i_r, \Omega}(1)} p_j \right). \end{aligned} \quad (5.5.8)$$

Clearly, we may assume that κ is sufficiently small in terms of r . Also, like in the previous section, we may assume that ε is a function of s, i_r, κ, Ω , so that the dependence of the implied constants on ε can be subsumed into their dependence on s, i_r, κ, Ω .

By the AM–GM inequality and (5.5.6), the first term on the right-hand side of (5.5.8) is bounded above by

$$\begin{aligned} \frac{1}{W^r k_1 \dots k_r} \left(r^{-1} \sum_{j=1}^r \sum_{m_j \in I_j} |U_{m_j}| \right)^r &\leq \frac{(1 + \kappa/10)^r}{k_1 \dots k_r r^r} \\ &\leq \frac{1 + r\kappa/5}{k_1 \dots k_r r^r} \leq \prod_{1 \leq j \leq r} \frac{1}{r k_j} + \frac{\kappa}{5}. \end{aligned}$$

Now choose ε small enough to ensure that the first error term on the right-hand side of (5.5.8) is less than $\kappa/5$, and then choose M large enough to ensure that the second error term on the right-hand side of (5.5.8) is less than $\kappa/5$. Thus,

$$|A| < \left(\prod_{1 \leq j \leq r} \frac{1}{rk_j} + \frac{3\kappa}{5} \right) W,$$

contradicting the hypothesis (5.5.4). Hence, we must have at least εW^{s-1} many solutions to (1.6.2) with $x_1, \dots, x_s \in A$.

CHAPTER 6

Appendix

6.1 More discussions on the proof of Theorem 3.4.2

In this appendix, we provide more details on the missing technical steps in the proof of Theorem 3.4.2. We also compare our treatment for the Roth variety for one dimensional progressions and the Roth variety for corners.

6.1.1 Smooth parts

In the proof of Theorem 3.4.2, we assume the smooth parts from the decompositions have expected dimensions and expected $\mathbb{F}_p$ -point counts. We would need some machinery in algebraic geometry to justify this. In this subsection, we will indicate how to modify the proof of Theorem 2.4.1 to produce a justification. Take Y_{gen} as a prototypical example, the goal is to show that $|Y_{\text{gen}}(\mathbb{F}_p)| = O(p^6)$.

- The associated complex analytic space of $Y_{\text{gen}}(\mathbb{C})$ would be a 6-dimensional complex manifold.
- One can still use a dimension comparison argument to deduce that the dimension of $Y_{\text{gen}}(\mathbb{C})$ as a variety is 6.
- Similarly, one can define an affine $\mathbb{Z}$ -model of $Y_{\text{gen}}(\mathbb{C})$ by changing the generators of the ideal accordingly.

- The argument that compares the dimension of the generic fiber and the dimensions of mod p fibers still works, thus one has $\dim_{\text{var}} Y_{\text{gen}}(\overline{\mathbb{F}}_p) = 6$ for all but finitely many p .
- Finally, one invokes Lang–Weil bound [LW54] to conclude that $|Y_{\text{gen}}(\mathbb{F}_p)| = O(p^6)$.

6.1.2 Degenerate subvarieties of low dimension

In the proof of Theorem 3.4.2, we also omit the point-counting on several “degenerate” subvarieties of low dimension. They are not the most essential difficulties in the proof. Here we would like to take Z'_1 as an example to demonstrate how we can deal with them; the goal is to show that $|Z'_1(\mathbb{F}_p)| = O(p^5)$.

- For any $(y_1, y_2, \dots, y_8) \in Z'_1(\mathbb{F}_p)$, there are at most $O(1)$ choices of y_1 by equation $R(y_1) = 0$.
- By equation (3.4.5) and $R(y_1) = 0$, we have $R(y_2)R(y_3)R(y_5)R(y_8) = 0$, hence for any given y_1 , there are at most $O(p^3)$ choices of y_2, y_3, y_5, y_8 .
- For any given y_1, y_2, y_3, y_5, y_8 , there are p^2 choices of y_4, y_6 .
- For any given $y_1, y_2, y_3, y_5, y_8, y_4, y_6$, there are at most $O(1)$ choices of y_7 by equation (3.4.3).
- Thus, there are at most $O(p^3 p^2) = O(p^5)$ choices of $y_1, y_2, y_3, y_5, y_8, y_4, y_6, y_7$.
- Therefore, we have $|Z'_1(\mathbb{F}_p)| = O(p^5)$.

6.1.3 A comparison of the techniques

In Section 2.4, to deal with the Roth variety for one dimensional progressions, one of the key steps is showing that

$$(G'(y_1) - F'(y_1)) \frac{R(y_1)}{R'(y_1)} - (G'(y_4) - F'(y_4)) \frac{R(y_4)}{R'(y_4)}$$

is nonzero, where F, G are rational functions such that F, G and constant function 1 are linearly independent, and $R = F'/G'$. This is just like we need to show that $D(y_1, y_4, y_6)$ is nonzero in Lemma 3.4.3 in order to deal with the Roth variety for two dimensional progressions.

The approach in Section 2.4.1 is to show that $(G'(y_1) - F'(y_1))R(y_1)/R'(y_1)$ is not a constant by solving a first order linear ODE via integrating factor. Alternatively, as in the proof of Lemma 3.4.3, we can regard R'/R as the difference of the logarithmic derivatives of F' and G' , and analyze the poles and zeroes of F' and G' , to give a different proof that $(G' - F')R/R'$ is not a constant.

6.2 Proof of Proposition 4.2.2

For any odd prime p , let

$$\epsilon_p = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ i & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

First, we recall the following result on Gauss sums with reduced residue classes.

Lemma 6.2.1. *Let $p \geq 3, n \geq 1$ and $t \in \mathbb{Z}$ with $(t, p) = 1$, then*

$$\sum_{y \in (\mathbb{Z}/p^n)^\times} e_{p^n}(ty^2) = \begin{cases} \left(\frac{t}{p}\right) \epsilon_p \sqrt{p} - 1 & \text{when } n = 1 \\ 0 & \text{when } n \geq 2 \end{cases}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Proof. The case that $n = 1$ is more well-known, see [IK04, Chapter 3, Section 3.5, Theorem 3.3]. The cases that $n \geq 2$ can be derived from [IK04, Chapter 3, Section 3.4,

Lemma 3.1]. Alternatively, one can calculate directly

$$\begin{aligned}
\sum_{y \in (\mathbb{Z}/p^n)^\times} e_{p^n}(ty^2) &= \sum_{\substack{z \in (\mathbb{Z}/p^{n-1})^\times \\ w \in \mathbb{Z}/p}} e_{p^n}(t(z + p^{n-1}w)^2) \\
&= \sum_{z \in (\mathbb{Z}/p^{n-1})^\times} e_{p^n}(tz^2) \sum_{w \in \mathbb{Z}/p} e_{p^n}(2tp^{n-1}zw) \\
&= 0
\end{aligned}$$

since z, t are coprime to p . □

Proof of Proposition 4.2.2. We will partition the squares in $\mathbb{Z}/p^n$ according to the divisibility of p powers. Let $0 \leq e < n$, if $x \in (\mathbb{Z}/p^n)^{(2)}$ and $p^e \parallel x$, then e must be even and we can write $x = p^e x'$ for some $x' \in (\mathbb{Z}/p^{n-e})^{\times(2)}$.

Write $t = p^v t'$ with $(t', p) = 1$. We may assume $v < n$ otherwise the results are trivial. When $e < n - v$, we have

$$\begin{aligned}
\sum_{x' \in (\mathbb{Z}/p^{n-e})^{\times(2)}} e_{p^n}(tp^e x') &= \sum_{x' \in (\mathbb{Z}/p^{n-e})^{\times(2)}} e_{p^{n-v-e}}(t' x') \\
&= p^v \sum_{x' \in (\mathbb{Z}/p^{n-v-e})^{\times(2)}} e_{p^{n-v-e}}(t' x') \\
&= p^v \cdot \frac{1}{2} \sum_{y \in (\mathbb{Z}/p^{n-v-e})^\times} e_{p^{n-v-e}}(t' y^2) \\
&= \begin{cases} O(p^{v+1/2}) & \text{when } n - v - e = 1 \\ 0 & \text{when } n - v - e \geq 2 \end{cases}
\end{aligned}$$

by Lemma 6.2.1. When $e \geq n - v$, we have

$$\left| \sum_{x' \in (\mathbb{Z}/p^{n-e})^{\times(2)}} e_{p^n}(tp^e x') \right| \leq p^{n-e}.$$

Ranging through all e such that $e \geq n - v$, the contribution is at most

$$p^v + p^{v-1} + \dots + p + 1 = O(p^v)$$

Combining the contributions from $e < n - v$ and $e \geq n - v$ completes the proof. □

6.3 Proof of Proposition 4.8.3

In this appendix, we will closely follow Section 3 in [LP10] to prove Proposition 4.8.3.

First, we will define majorants that parametrize prime squares. These majorants have appeared in [Cho18], [Gao25], [Zha25] and [Tan25]. Let $N, W \geq 2$ be integers with $W \leq \log N$, and $b \in (\mathbb{Z}/W)^{\times(2)}$. Denote the number of square roots of b by $\sigma_W(b)$, that is

$$\sigma_W(b) = |\{x \in (\mathbb{Z}/W)^\times : x^2 = b\}|$$

In fact, the value of $\sigma_W(b)$ is independent of b and equal to $\varphi(W)/|(\mathbb{Z}/W)^{\times(2)}|$, so we will often abbreviate it as σ_W . Define a function $\nu_b : [N] \rightarrow \mathbb{R}_{\geq 0}$ by setting

$$\nu_b(n) = \begin{cases} \frac{\varphi(W)}{W\sigma_W(b)}(2p \log p) & \text{if } Wn + b = p^2 \text{ for some prime } p \\ 0 & \text{otherwise} \end{cases}$$

for all $n \in [N]$. Roughly speaking, the majorant ν_b parametrizes weighted prime squares that are $b \pmod W$ in $[WN]$.

Before proceeding further, we record the following well-known asymptotic formulae which would be useful later:

$$\sum_{x \leq X} x\Lambda(x) = \frac{X^2}{2} + O(X^2 \exp(-c\sqrt{\log X})) \quad (6.3.1)$$

where Λ is von Mangoldt function and c is a positive absolute constant. Also, let $Q > 0$, $X \geq 1$, and a, r be positive integers with $r \leq (\log X)^Q$ and $(a, r) = 1$, then

$$\sum_{\substack{x \leq X \\ x \equiv a \pmod r}} x\Lambda(x) = \frac{X^2}{2\varphi(r)} + O(X^2 \exp(-c_Q \sqrt{\log X})) \quad (6.3.2)$$

where c_Q is a positive absolute constant depending on Q . These asymptotic formulae can be proved by Siegel-Walfisz theorem and summation by parts.

By applying formula (6.3.2), one can show that

$$\sum_{n \in [N]} \nu_b(n) = N + O(N \exp(-c\sqrt{\log N}))$$

where $c > 0$ is a constant. (The constant c here might be different from the constant c in formula (6.3.1), however, we will abuse the notation here and throughout.)

Now, let A be a subset of primes with relative lower density $\delta_{\mathcal{P}}(A) > \sqrt{\mu}$. Let $N, W \geq 2$ be integers with $W \leq \log N$, and $b \in (\mathbb{Z}/W)^{\times(2)}$, we will define a function $f_{A,b} : [N] \rightarrow \mathbb{R}_{\geq 0}$ by setting

$$f_{A,b}(n) = \begin{cases} \frac{\varphi(W)}{W\sigma_W}(2p \log p) 1_A(p) & \text{if } Wn + b = p^2 \text{ for some prime } p \\ 0 & \text{otherwise} \end{cases}$$

for all $n \in [N]$. Roughly speaking, the function $f_{A,b}$ can be thought as a weighted, W -tricked version of characteristic function of A .

Let y be a sufficiently large (depending on A and s) integer such that $y \equiv s \pmod{24}$. Let

$$w = \log \log \log y, \quad W = 8 \prod_{3 \leq p < w} p, \quad N = \left\lfloor \frac{2y}{sW} \right\rfloor.$$

Note that we have $w = O(\log \log \log N)$ and hence $W \leq \log N$. We will work with $\nu_b, f_{A,b}$ defined as before based on this choice of N, W .

Let $\kappa > 0$ be a sufficiently small parameter depending on A , for the sake of the definiteness, say $\kappa = (\delta_{\mathcal{P}}(A) - \sqrt{\mu})^2/10^{10}$. Define a function $f : (\mathbb{Z}/W)^{\times(2)} \rightarrow [0, 1]$ by setting

$$f(b) = \max \left\{ 0, \mathbb{E}_{n \in [N]} f_{A,b}(n) - \kappa \right\}$$

for all $b \in (\mathbb{Z}/W)^{\times(2)}$. Note that

$$\begin{aligned}
& \sum_{b \in (\mathbb{Z}/W)^{\times(2)}} \sum_{n \in [N]} f_{A,b}(n) \\
&= \frac{2\varphi(W)}{W\sigma_W} \sum_{\substack{p \in A \\ W \leq p^2 \leq W(N+1) \\ p^2 \in (\mathbb{Z}/W)^{\times(2)}}} p \log p \\
&\geq \frac{2\varphi(W)}{W\sigma_W} \left(\sum_{\substack{p \in A \\ p \leq \sqrt{W(N+1)}}} p \log p - O(W) \right) \\
&\geq \frac{2\varphi(W)}{W\sigma_W} \left(\sum_{p \leq (\sqrt{\mu} + 2\sqrt{\kappa})\sqrt{W(N+1)}} p \log p - O(W) \right) \quad (\text{since } \delta_{\mathcal{P}}(A) > \sqrt{\mu}) \\
&\geq \frac{2\varphi(W)}{W\sigma_W} \left(\frac{(\sqrt{\mu} + 2\sqrt{\kappa})^2 W N}{2} - O(W N \exp(-c\sqrt{\log N})) \right) \quad (\text{by formula (6.3.1)}) \\
&\geq \frac{\varphi(W)}{\sigma_W} \left((\sqrt{\mu} + 2\sqrt{\kappa})^2 N - O(N \exp(-c\sqrt{\log N})) \right)
\end{aligned}$$

Thus, we have

$$\mathbb{E}_{b \in (\mathbb{Z}/W)^{\times(2)}} f(b) \geq \mu + \kappa$$

Even though the relative lower density of A is greater than $\sqrt{\mu}$, the ν -weighted density of A is only greater than μ , and this is the reason why the threshold in Theorem 1.4.3 is $\sqrt{D_s}$ instead of D_s .

By Hypothesis (s, μ) , we have $y = b_1 + b_2 + \dots + b_s \pmod{W}$ for some $b_1, b_2, \dots, b_s \in (\mathbb{Z}/W)^{\times(2)}$ such that

$$\frac{1}{s}(f(b_1) + f(b_2) + \dots + f(b_s)) \geq \frac{1}{2} \text{ and } f(b_j) \neq 0 \text{ for all } 1 \leq j \leq s.$$

In particular, this implies that

$$\mathbb{E}[f_{A,b_1}] + \mathbb{E}[f_{A,b_2}] + \dots + \mathbb{E}[f_{A,b_s}] > \frac{s}{2}(1 + \kappa) \text{ and } \mathbb{E}[f_{A,b_j}] > \frac{\kappa}{2} \text{ for all } 1 \leq j \leq s.$$

Let $y' = (y - b_1 - b_2 - \dots - b_s)/W$. The goal is to find $n_1, n_2, \dots, n_s \in [N]$ such that

$$y' = n_1 + n_2 + \dots + n_s \text{ and } f_{A,b_j}(n_j) > 0 \text{ for all } 1 \leq j \leq s$$

since $Wn_j + b_j$ will be a square of prime in A when $f_{A,b_j}(n_j) > 0$ for all $1 \leq j \leq s$.

Now that we have completed the W -trick, for the rest of the details of the transference principle, we are able to find a well-formulated proposition in literature to cover them. The following proposition due to Salmensuu [Sal21, Proposition 3.9] is what we need.

Proposition 6.3.1. *Let $N \geq 1, s \geq 2$ be integers and $\epsilon \in (0, 1)$. Let $f_j : [N] \rightarrow \mathbb{R}_{\geq 0}, \nu_j : [N] \rightarrow \mathbb{R}_{\geq 0}$ be functions with $f_j \leq \nu_j$ for $1 \leq j \leq s$. Assume the following are true.*

1. (Pseudorandomness) $\|\widehat{\nu}_j - \widehat{1}_{[N]}\|_\infty \leq \eta N$ for some $\eta > 0$ and all $1 \leq j \leq s$
2. (Restriction at q) $\|\widehat{f}_j\|_{l^q} \leq KN^{1-1/q}$ for some $K > 0, s-1 < q < s$ and all $1 \leq j \leq s$
3. $\mathbb{E}[f_1] + \mathbb{E}[f_2] + \dots + \mathbb{E}[f_s] > \frac{s}{2}(1 + \epsilon)$
4. $\mathbb{E}[f_j] > \frac{\epsilon}{2}$ for all $1 \leq j \leq s$

Suppose η is sufficiently small depending on s, ϵ, K, q . Then, for any integers y with

$$y \in \left((1 - (\epsilon/32)^2) \frac{sN}{2}, (1 + (\epsilon/32)^2) \frac{sN}{2} \right)$$

we have

$$f_1 * f_2 * \dots * f_s(y) \geq c(\epsilon, s) N^{s-1}$$

where $c(\epsilon, s) > 0$ is a constant that only depends on ϵ, s .

The proof of Proposition 6.3.1 essentially involves embedding $[N]$ in $\mathbb{Z}/N'$ for some prime $N' \in [(1 + (\kappa^2/100)) \frac{y}{W}, (1 + (2\kappa^2/100)) \frac{y}{W}]$. Passing from N to N' loses density by a factor of $2/s$, and this is why the lower bound $1/2$ appears in Hypothesis (s, μ) .

To apply Proposition 6.3.1 to f_{A,b_j}, ν_{b_j} for $1 \leq j \leq s$ and complete the proof, it remains to verify the pseudorandomness and restriction at q . These types of estimates have been proved by Chow [Cho18], Gao [Gao25] and Zhao [Zha25]. The version we need is in [Zha25, Proposition 3.2, 3.3], which states that

$$\|\widehat{\nu}_b - \widehat{1}_{[N]}\|_\infty \ll_\epsilon \frac{N}{w^{1/2-\epsilon}}$$

for all $\epsilon > 0$, and

$$\|\widehat{f}_{A,b}\|_{l^q} \ll_q N^{1-1/q}$$

for all $q > 4$.

REFERENCES

- [Aus14] Tim Austin. “Partial difference equations over compact Abelian groups, I: modules of solutions.” arXiv 1305.7269, 2014.
- [BC17] Jean Bourgain and Mei-Chu Chang. “Nonlinear Roth type theorems in finite fields.” *Israel J. Math.*, **221**(2):853–867, 2017.
- [Beh46] 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.
- [BL96] Vitaly Bergelson and Alexander Leibman. “Polynomial extensions of van der Waerden’s and Szemerédi’s theorems.” *J. Amer. Math. Soc.*, **9**(3):725–753, 1996.
- [BM22] Thomas F. Bloom and James Maynard. “A new upper bound for sets with no square differences.” *Compositio Mathematica*, **158**(8):1777–1798, 2022.
- [Bom66] Enrico Bombieri. “On exponential sums in finite fields.” *Amer. J. Math.*, **88**:71–105, 1966.
- [Bou89] J. Bourgain. “On $\Lambda(p)$ -subsets of squares.” *Israel J. Math.*, **67**(3):291–311, 1989.
- [CGS12] Péter Csikvári, Katalin Gyarmati, and András Sárközy. “Density and Ramsey type results on algebraic equations with restricted solution sets.” *Combinatorica*, **32**(4):425–449, 2012.
- [Cho18] Sam Chow. “Roth-Waring-Goldbach.” *Int. Math. Res. Not. IMRN*, (8):2341–2374, 2018.
- [CLM25] Sam Chow, Zi Li Lim, and Akshat Mudgal. “Generalised Fermat equations in dense variables over finite fields and rings.” arXiv 2601.00135, 2025.
- [CLS13] Ernie Croot, Izabella Łaba, and Olof Sisask. “Arithmetic progressions in sumsets and L^p -almost-periodicity.” *Combin. Probab. Comput.*, **22**(3):351–365, 2013.
- [Del74] Pierre Deligne. “La conjecture de Weil. I.” *Inst. Hautes Études Sci. Publ. Math.*, (43):273–307, 1974.
- [DLS20] Dong Dong, Xiaochun Li, and Will Sawin. “Improved estimates for polynomial Roth type theorems in finite fields.” *J. Anal. Math.*, **141**(2):689–705, 2020.
- [FK78] H. Furstenberg and Y. Katznelson. “An ergodic Szemerédi theorem for commuting transformations.” *J. Analyse Math.*, **34**:275–291, 1978.
- [FKM15] Étienne Fouvry, Emmanuel Kowalski, and Philippe Michel. “A study in sums of products.” *Philos. Trans. Roy. Soc. A*, **373**(2040):20140309, 26, 2015.

- [Fur77] Harry Furstenberg. “Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions.” *J. Analyse Math.*, **31**:204–256, 1977.
- [Gao25] Meng Gao. “A density version of Waring-Goldbach problem.” *Int. J. Number Theory*, **21**(6):1417–1436, 2025.
- [Gow98] W. T. Gowers. “A new proof of Szemerédi’s theorem for arithmetic progressions of length four.” *Geom. Funct. Anal.*, **8**(3):529–551, 1998.
- [Gow01] W. T. Gowers. “A new proof of Szemerédi’s theorem.” *Geom. Funct. Anal.*, **11**(3):465–588, 2001.
- [GR84] Hans Grauert and Reinhold Remmert. *Coherent analytic sheaves*, volume 265 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1984.
- [GR05] Ben Green and Imre Z. Ruzsa. “Sum-free sets in abelian groups.” *Israel J. Math.*, **147**:157–188, 2005.
- [Gre05] Ben Green. “Roth’s theorem in the primes.” *Ann. of Math. (2)*, **161**(3):1609–1636, 2005.
- [GT08] Ben Green and Terence Tao. “The primes contain arbitrarily long arithmetic progressions.” *Ann. of Math. (2)*, **167**(2):481–547, 2008.
- [Har77] Robin Hartshorne. *Algebraic geometry*, volume No. 52 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1977.
- [HL22] G. H. Hardy and J. E. Littlewood. “Some problems of ‘Partitio Numerorum’: IV. The singular series in Waring’s Problem and the value of the number $G(k)$.” *Math. Z.*, **12**(1):161–188, 1922.
- [HL25] Guo-Dong Hong and Zi Li Lim. “Three term rational function progressions in finite fields.” *Int. Math. Res. Not. IMRN*, (10):Paper No. rnaf118, 16, 2025.
- [HLY21] Rui Han, Michael T. Lacey, and Fan Yang. “A polynomial Roth theorem for corners in finite fields.” *Mathematika*, **67**(4):885–896, 2021.
- [IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.
- [Kat08] Nicholas M. Katz. “Estimates for mixed character sums.” *Geom. Funct. Anal.*, **18**(4):1251–1269, 2008.
- [KKL24] Noah Kravitz, Borys Kuca, and James Leng. “Corners with polynomial side length.” arXiv 2407.08637, 2024.

- [Kuc21] Borys Kuca. “Further bounds in the polynomial Szemerédi theorem over finite fields.” *Acta Arith.*, **198**(1):77–108, 2021.
- [Kuc24a] Borys Kuca. “Multidimensional polynomial patterns over finite fields: bounds, counting estimates and Gowers norm control.” *Adv. Math.*, **448**:Paper No. 109700, 61, 2024.
- [Kuc24b] Borys Kuca. “Multidimensional polynomial Szemerédi theorem in finite fields for polynomials of distinct degrees.” *Israel J. Math.*, **259**(2):589–620, 2024.
- [KW24] Necef Kavrut and Shukun Wu. “A bilinear estimate in $\mathbb{F}_p$.” arXiv 2401.07925, 2024.
- [Len22] James Leng. “A Quantitative Bound For Szemerédi’s Theorem for a Complexity One Polynomial Progression over $\mathbb{Z}/N\mathbb{Z}$.” arXiv 2205.05540, 2022.
- [Len24] James Leng. “Efficient equidistribution of periodic nilsequences and applications.” arXiv 2306.13820, 2024.
- [Lim25a] Zi Li Lim. “On the density version of quadratic Waring’s problem and the quadratic Waring–Goldbach problem.” arXiv 2508.14939, 2025.
- [Lim25b] Zi Li Lim. “Uniform nonlinear Szemerédi theorem for corners in finite fields.” arXiv 2501.04887, 2025.
- [Lin18] Sofia Lindqvist. “Partition regularity of generalised Fermat equations.” *Combinatorica*, **38**(6):1457–1483, 2018.
- [LMR24] Michael T. Lacey, Hamed Mousavi, Yaghoub Rahimi, and Manasa N. Vempati. “A Density Theorem for Higher Order Sums of Prime Numbers.” arXiv 2411.01296, 2024.
- [LP10] Hongze Li and Hao Pan. “A density version of Vinogradov’s three primes theorem.” *Forum Math.*, **22**(4):699–714, 2010.
- [LW54] Serge Lang and André Weil. “Number of points of varieties in finite fields.” *Amer. J. Math.*, **76**:819–827, 1954.
- [Pel18] Sarah Peluse. “Three-term polynomial progressions in subsets of finite fields.” *Israel J. Math.*, **228**(1):379–405, 2018.
- [Pel19] Sarah Peluse. “On the polynomial Szemerédi theorem in finite fields.” *Duke Math. J.*, **168**(5):749–774, 2019.
- [Pel20] Sarah Peluse. “Bounds for sets with no polynomial progressions.” *Forum Math. Pi*, **8**:e16, 55, 2020.

- [Pel23] Sarah Peluse. “Finite field models in arithmetic combinatorics – twenty years on.” arXiv 2312.08100, 2023.
- [Pel24] Sarah Peluse. “Subsets of $\mathbb{F}_p^n \times \mathbb{F}_p^n$ without L -shaped configurations.” *Compos. Math.*, **160**(1):176–236, 2024.
- [PP22] Sarah Peluse and Sean Prendiville. “A polylogarithmic bound in the nonlinear Roth theorem.” *Int. Math. Res. Not. IMRN*, (8):5658–5684, 2022.
- [PP24] Sarah Peluse and Sean Prendiville. “Quantitative bounds in the nonlinear Roth theorem.” *Invent. math.*, **238**:865–903, 2024.
- [PPS24] Sarah Peluse, Sean Prendiville, and Xuancheng Shao. “Bounds in a popular multidimensional nonlinear Roth theorem.” arXiv 2407.08338, 2024.
- [Pre17] Sean Prendiville. “Quantitative bounds in the polynomial Szemerédi theorem: the homogeneous case.” *Discrete Analysis*, 2 2017.
- [PSS23] Sarah Peluse, Ashwin Sah, and Mehtaab Sawhney. “Effective bounds for Roth’s theorem with shifted square common difference.” arXiv 2309.08359, 2023.
- [Rot53] K. F. Roth. “On Certain Sets of Integers.” *Journal of the London Mathematical Society*, **s1-28**(1):104–109, 1953.
- [Sal21] Juho Salmensuu. “A density version of Waring’s problem.” *Acta Arith.*, **199**(4):383–412, 2021.
- [Sem25] Aliaksei Semchankau. “A new bound for $A(A + A)$ for large sets.” *J. Number Theory*, **268**:142–162, 2025.
- [Sha14] Xuancheng Shao. “A density version of the Vinogradov three primes theorem.” *Duke Math. J.*, **163**(3):489–512, 2014.
- [Sta96] Walter D. Stangl. “Counting squares in Z_n .” *Math. Mag.*, **69**(4):285–289, 1996.
- [Sta23] The Stacks project authors. “The Stacks project.” <https://stacks.math.columbia.edu>, 2023.
- [Sze75] E. Szemerédi. “On sets of integers containing k elements in arithmetic progression.” *Acta Arithmetica*, **27**(1):199–245, 1975.
- [Tan25] Maoru Tan. “A density version of Hua’s theorem.” *Forum Mathematicum*, 2025.
- [Tao23] Terence Tao. “The Lang-Weil Bound.” <https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/>, 2023.
- [TV06] Terence Tao and Van Vu. *Additive combinatorics*, volume 105 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2006.

- [Vau97] R. C. Vaughan. *The Hardy-Littlewood method*, volume 125 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, second edition, 1997.
- [Vin37] Ivan Matveevich Vinogradov. “Representation of an odd number as the sum of three primes.” *Proceedings of the USSR Academy of Sciences*, **15**:129–132, 1937.
- [Zha25] Genheng Zhao. “A density theorem for prime squares.” arXiv 2502.20322, 2025.