From the holdings of the Department of Special Collections , Princeton University Library, Princeton, NJ

These documents are either in the public domain, or can only be used for educational and research purposes (Fair use) as per U.S. Copyright law (text below). By accessing this file, all users agree that their use falls in the public domain or within fair use as defined by the copyrightlaw. We do not charge any permission or usage fees for the publication of images of material inour collections, including those provided by Princeton University Library, via our website, catalog, or directly from staff.For more information regarding copyright, credit, and citation please review the information onthe Copyright, Credit and Citation Guidelines page of our website.
https://library.princeton.edu/special-collections/policies/copyright-credit-and-citation-guidelines. If you have any questions, including how to order higher-quality images from the collection, contact Special Collections Public Services via our Ask Us! Form. https://library.princeton.edu/special-collections/ask-us

---

Doctoral Dissertations, 2011-2026 Mathematics

2016

Optimal strong approximation for quadratic forms

Talebizadeh Sardari, Naser

Princeton, NJ : Princeton University

---

http://arks.princeton.edu/ark:/88435/dsp01zg64tp40m

U.S. Copyright law: The copyright law of the United States (Title 17, §108, United States Code) governs the making of photocopies or other reproductions of copyrighted material. Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be used for any purpose other than private study, scholarship, or research. If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of fair use that user may be liable for copyright infringement. This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve a violation of copyright law. https://www.copyright.gov/title17/title17.pdf

Optimal strong approximation for quadratic forms

Naser Talebizadeh Sardari

A Dissertation
Presented to the Faculty
of Princeton University
in Candidacy for the Degree
of Doctor of Philosophy

Recommended for Acceptance
by the Department of
Mathematics
Adviser: Peter Sarnak

September 2016

© Copyright by Naser Talebizadeh Sardari, 2016.

All Rights Reserved

Abstract

We study questions posed by Sarnak in his letter to S. Aaronson and A. Pollington, on "the Solovay-Kitaev Theorem and Golden Gates" [Sar15a]. We give the optimal exponent for the strong approximation problem for quadratic forms in 5 or more variables. We also give lower and upper bound for the exponent of approximation for quadratic forms in 4 variables which recovers the best upper bound, known previously under the Ramanujan conjecture, without any assumption. Our lower bound gives a nontrivial and numerically optimal bound on the diameter of LPS Ramanujan graphs. More generally, our numerical results suggests that our lower bound for the exponent is optimal for any quadratic forms in 4 variables. We consider the algorithmic aspect of the optimal strong approximation. As two applications of our algorithm, we develop and implement an algorithm in polynomial time in the size of digits of input integers for the navigation problem on LPS Ramanujan graphs and also the discrete log problem for the finite group $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ by assuming one can factor quickly and a standard conjecture in Number theory. Finally, our work fits into a more general framework of studying small scale equidistribution of measures coming from number theory in the optimal range. We give a definite answer to a conjecture of Lester and Rudnick on the small scale equidistribution of orthonormal basis of eigenfunctions restricted to an individual eigenspace on the flat torus $\mathbb{T}^d$ for $d \geq 5$ and find the optimal range for equidistribution.

Acknowledgements

It is with great pleasure to thank my advisor Peter Sarnak for his patience in discussing his ideas with me and being a source of energy during the PhD program. In fact the starting point of this work was his letter [Sar15a] and in particular the key observation of Bourgain noted there. His generosity, wisdom and Mathematics has been and continue to be an inspiration for me.

I would like to thank Professors Zeev Rudnick and Valentin Blomer for their generosity in discussing their ideas. I am also very thankful for Professor Tim Browning's comments on earlier versions of this work. In addition, I would like to thank Peter Selinger and Ori Parzanchevski for sharing their codes and answering my questions.

I am grateful to the mathematics departments at Princeton University and Institute for Advanced Study for the ideal environment they provide to learn mathematics. I would particularly like to thank Professors Manjul Bhargava, David Gabai, Nicholas Katz, Alex Kontorovich, Sophie Morel, Chris Skinner, Richard Taylor and Shou-Wu Zhang.

I am also very grateful to the mathematics department of Sharif University and University of Cambridge. I am indebted to Professors Mehrdad and Siavash Shahshahani for their generosity and endless support.

I would like to thank our kind graduate administrator Jill LeClair, for being super efficient. She brings life to Fine Hall by her sincere efforts to make sure every graduate student is doing well.

I would like to express my deepest gratitude to my dear friends both inside and outside of Princeton. I will not list their names here but rather stress that their company has enriched my life. I am privileged to have met every one of them.

Last but not the least, I would like to thank my father Hassan for his sincere love and dedication to support his family in the toughest time. I would like to thank my dear brothers Masood and Mansour and my dear sister Parvin and Homa, my sister in law Najmeh and my brothers in law Hamid and Sina for their love and endless support. Finally, I would like to thank my nephews Sohale, Armin, Soroush and Hamin for bringing joy and happiness to our family. I wish them the best and can not wait to see their success in the future.

To the memory of my mother, for her unconditional love and being my first Math teacher.

Zahrah Talebizadeh Sardari

Contents

Abstract . . . iii

Acknowledgements . . . iv

1 Introduction **1**

1.0.1 Trivial Lower bound on $N(r)$ . . . 1

1.0.2 Repulsion of integral points and Wright's lower bound on $N(r)$ . . . 2

1.0.3 Ramanujan Conjecture and upper bound on $N(r)$ . . . 2

1.1 Almost all exponent . . . 3

1.2 Algorithmic aspect of optimal strong approximation . . . 4

1.2.1 Discrete log problem . . . 4

1.2.2 Navigation on Ramanujan graphs . . . 5

1.3 Small scale equidistribution of measures coming from Number theory . . . 5

1.4 Outline of the Thesis . . . 6

2 Optimal strong approximation for quadratic forms **8**

2.1 Introduction . . . 8

2.1.1 Statement of results . . . 8

2.1.2 Further motivations and techniques . . . 14

2.1.3 Outline of the chapter . . . 20

2.2 Repulsion of integral points . . . 21

2.3 The delta method . . . 25

2.3.1 The properties of the function $h(x, y)$ . . . 28

2.4 Quadratic exponential sums $S_{mq}(c)$ . . . 29

2.5 The integral $I_{mq}(c)$ . . . 34

2.5.1 Upper bound on the integral $I_{mq}(c)$ for ordinary vectors . . . 36

2.5.2 Upper bound on the integrals $I_{mq}(c)$ for exceptional vectors . . . 42

2.5.3 Bounding the sum over the exceptional vectors 44
2.6 The main theorem 48
2.6.1 Singular integral 49
2.6.2 Singular series 50

3 Diameter of Ramanujan Graphs and Random Cayley Graphs 53
3.1 Introduction 53
3.1.1 Motivation 53
3.1.2 Statement of results 55
3.1.3 Outline of the chapter 57
3.2 Lower bound for the diameter of the Ramanujan graphs 58
3.3 Visiting almost all points after $(1+\epsilon)\log_{k-1}(n)$ steps 61
3.4 Numerical Results 63

4 Quadratic forms and semiclassical eigenfunction hypothesis for flat tori 67
4.1 Introduction 67
4.1.1 Semiclassical eigenfunction hypothesis for flat tori 67
4.1.2 Local statistics of integral points on sphere 69
4.1.3 Main theorem 72
4.1.4 Outline of the chapter 72
4.2 Proof of corollary (4.1.2) 73
4.3 Proof of the Main thoerem 77
4.4 Appendix 83

Chapter 1

Introduction

This thesis is primarily concerned with giving the best possible exponent for the rate of approximation of points on a quadrics by integral points lying on that quadric. In the following concrete example, we define this optimal exponent. We note that this exponent transforms easily to the covering exponent that is defined by Sarnak in his letter [Sar15a]. Let $F(x_1, \dots, x_4) := x_1^2 + \cdots + x_4^2$ and $V_N := \{X = (x_1, \dots, x_4) : F(X) = N\}$ be the quadric associated to F at level N. We note that $V_N(\mathbb{Z})$ is the set of integral points lying on the sphere of radius $\sqrt{N}$ in $\mathbb{R}^4$ and by a classical result of Jacobi when N is odd, $V_N(\mathbb{Z})$ has N elements up to a bounded constant scalar. We project points $X \in V_N(\mathbb{Z})$ onto the unit sphere $\frac{X}{\sqrt{N}} \in S^3$ and ask the following question.

Question 1.0.1 *Let $r > 0$. What is the minimal odd integer N such that for every point $y \in S^3$, there exists $X \in V_N(\mathbb{Z})$ such that*

$$\|\frac{X}{\sqrt{N}} - y\| \leq r.$$

We denote this value by $N(r)$.

1.0.1 Trivial Lower bound on $N(r)$

We have about $\approx r^{-3}$ disjoint boxes of size r on the unit sphere S^3. Since for odd integer N, $V_N(\mathbb{Z})$ have about $\approx N$ elements. Then

$$N(r) \gg r^{-3}.$$

1.0.2 Repulsion of integral points and Wright's lower bound on $N(r)$

Wright [Wri33, Wri37] observed that there exists a point $y \in S^3$ with almost equal coordinates which repels the projected integral points from $V_N(\mathbb{Z})$. From his example one can give the following lower bound on $N(r)$

$$N(r) \gg r^{-4}.$$

More generally, we can quantify this for every primitive integral point $v \in \mathbb{Z}^4$ with small norm (primitive means the gcd of all the coordinates is one and Wright example corresponds to $v = (1,1,1,1)$). In Chapter 2, by an elementary argument, we show that in a small neighborhood of the unit vector in the direction of v, they are points which repel the projected integral points from $V_N(\mathbb{Z})$. The size of these holes on the sphere of radius $\sqrt{N}$ is

$$\frac{N^{\frac{1}{4}}}{\sqrt{\|v\|}}.$$

1.0.3 Ramanujan Conjecture and upper bound on $N(r)$

For giving an upper bound on $N(r)$ in terms of r, we need to show that there exists points in every box of size r. One way of showing this is to count integral points inside a box of size r by circle method. In fact, Malyshev [Mal62] used Kloosterman's method and proved a result about the distribution of integral points of the quadric $F(X) = N$ with 4 or more variables in small boxes. His result shows that $N(r) \ll r^{-A}$ for some explicit power A. Sarnak in his letter [Sar15a] to Aaronson and Pollington, showed that

$$N(r) \ll r^{-6+\epsilon}.$$

To show this he appealed to the Ramanujan bound on the Fourier coefficients of weight k-modular forms. Furthermore, Sarnak states some open problems [Sar15a, Page 24]. The first problem is to show that $N(r) < r^{-\alpha}$ for some $\alpha < 6$ or even that $\alpha = 4$. In Chapter 2, we consider this problem for every quadratic from in 5 or more variables. In particular, we prove the following corollary:

Corollary 1.0.2 *Let $F(x_1, \ldots, x_d) := x_1^2 + \cdots + x_d^2$ where $d \geq 5$ and $V_N := \{X = (x_1, \ldots, x_d) : F(X) = N\}$. Let $N(r)$ be defined as in Question 1.0.1. Then*

$$N(r) \ll r^{-(4+\epsilon)},$$

and 4 is the optimal exponent.

We also consider the p-adic version of Question 1.0.1 and we prove the following corollary:

Corollary 1.0.3 *Let $F(x_1, \dots, x_d) := x_1^2 + \cdots + x_d^2$ where $d \geq 5$ and $V_N := \{X = (x_1, \dots, x_d) : F(X) = N\}$. If*

$$N \gg p^{4k+\epsilon}.$$

Then, for every $\lambda \in V_N(\frac{\mathbb{Z}}{p^k\mathbb{Z}})$, there exists $X \in V_N(\mathbb{Z})$ such that $X \equiv \lambda \bmod p^k$ and 4 is the optimal exponent.

1.1 Almost all exponent

One may ask the almost all version of Question 1.0.1.

Question 1.1.1 *Let $r > 0$. What is the minimal value of odd N such that for almost all points $y \in S^3$ with respect to natural measure on S^3, there exists $X \in V_N(\mathbb{Z})$ such that*

$$\|\frac{X}{\sqrt{N}} - y\| \leq r.$$

We denote this value by $N_\mu(r)$.

It turns out that the big holes (boxes of size $N^{-1/4}$ with no integral points inside) have a small total measure on the unit sphere. In fact, if we want to approximate almost all points on the unit sphere then the projection of integral points $V_N(\mathbb{Z})$ onto the unit sphere are very well distributed. They cover boxes as if we pick $\|V_N(\mathbb{Z})\|$ random points on the unit sphere. So, we have points in almost all boxes of size $N^{-1/3+\epsilon}$ and as a result

$$N_\mu(r) \leq r^{-(3+\epsilon)}.$$

Note that the exponent 3 is optimal and equals to the trivial lower bound given by the covering argument. By computing the variance of the number of points in random caps and using Chebyshev's inequality, Sarnak shows this in his letter [Sar15a] for Hecke orbits on S^2 and very recently for integral points on S^2 [BRS16] assuming the Lindelof Hypothesis. In the expository paper of Ghosh-Gorodnik and Nevo [GGN14], the more general problem of diophantine approximation for the homogeneous varieties has been discussed. We briefly describe their method here. Given a homogeneous variety $X := G/H$, the rational points or S-integral points of X are corresponded to the orbit of a lattice

$\Gamma \subset G$ acting on X. By the "Duality principle", the question about the density of an orbit Γ in X corresponds to the mixing property of an orbit H in $\Gamma\backslash G$. Now, the question is about the decay of the matrix coefficients of the representation of $L^2(\Gamma\backslash G)$ as a representation of H. In the cases where the restriction of the automorphic representation of $L^2(\Gamma\backslash G)$ to H is tempered (this is the representation theory interpretation of the Ramanujan bound on modular forms) as a representation of H, we have optimal diophantine approximation exponents for almost all points which matches with the trivial exponent given by a covering argument. In Chapter 3, we study the combinatorial version of this problem on k-regular Ramanujan graphs. We prove that the distance of almost all pair of vertices is asymptotically

$$\log_{k-1}(n). \tag{1.1}$$

We use the Ramanujan bound on the eigenvalues of the adjacency matrix of the graph to give an upper bound on the variance. We use Chebyshev's inequality to show that the almost all diameter of a k-regular Ramanujan graph equals the trivial lower bound given by a covering argument.

1.2 Algorithmic aspect of optimal strong approximation

A natural question after finding the optimal exponent for approximation is to develop an algorithm which gives us an integral point inside a given box. Sarnak asks essentially the same question in his letter for the existence of an algorithm for approximating $SU(2)$ elements by arithmetic quantum gates [Sar15a, Page 24]. Ross and Selinger develop and implement [RS14] an algorithm that, for any rotation in the z-axis, returns an optimal word in quantum gates that approximate it up to given ϵ by assuming one can factor quickly. We develop and implement the p-adic version of the Ross and Selinger algorithm which is of independent interest. In what follows we explain two applications of our algorithm.

1.2.1 Discrete log problem

Suppose we are given a prime p and a primitive root of unity g mod p. The discrete logarithm of a number x with respect to p and g is the integer r mod $(p-1)$ (the order of g in $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$) such that

$$g^r \equiv x \ (\bmod\ p).$$

Factorization problem and discrete log problem are generally thought to be computationally hard on a classical computer. They are the source of hardness for several proposed cryptosystems. Shor gave polynomial time algorithms in the number of digits of the input integers to factor integers and find discrete logarithms on a hypothetical quantum computer [Sho97]. We consider the discrete logarithm problem for the non-commutative group $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$. More precisely, for a specific family of generator set $S := \{s_1^{\pm}, \ldots, s_k^{\pm}\}$ (LPS generators) for $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ we develop and implement an algorithm for expressing a diagonal element x of $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ in a shortest possible word by the LPS generator set S. Note that since the Cayley graph of $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ with respect to the LPS generator set S is a Ramanujan graphs [LPS88] and as noted in 1.1 the almost diameter is optimally short for every Ramanujan graph, therefore, for a typical $g \in \mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ there exist a word in the LPS generator set with the optimal length $(1+\epsilon)\log_{2k-1} n$ which expresses it. This indicates that the LPS generators are natural choice as a symmetric generator set for $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$. One can use our algorithm and decompose a typical element x in $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ into three Euler rotations and as a result express it as a word with 3 times the optimal word length in LPS generators.

1.2.2 Navigation on Ramanujan graphs

We consider the problem of finding a shortest path between a given pair of vertices in the LPS Ramanujan graphs $X_{p,q}$ where p is a fixed prime number and q is an integer. We give a polynomial time algorithm in $\log(q)$ which returns a shortest path between two diagonal vertices under a standard conjecture on the distribution of integers representable as sum of two squares and assuming one can factor quickly. Numerically, for a typical pair of vertices corresponded to diagonal elements the minimal path has a length about $3\log(q) + O(1)$ while provably, there are pairs of points with distance at least $4\log(q) + O(1)$. For a general pair of vertices, we write it as a product of three Euler angles and as a result for a typical pair we find a path with distance $9\log(q) + O(1)$.

1.3 Small scale equidistribution of measures coming from Number theory

One can study the small scale behavior of other convergent sequence of measures coming form Number Theory. One natural sequence is the probability measures associated to the square of normalized Laplacian eigenfunctions as the eigenvalue goes to infinity. More precisely, given a compact Riemannian manifold M equipped with laplacian-Beltramin operator Δ, and $\{\psi_n\}$ an

orthonormal basis of $L^2(M, \mathrm{dvol})$ consisting of eigenfunctions of Δ. If the geodesic flow is ergodic then Quantum Unique Ergodicity says that for any orthonormal basis $\{\psi_n\}$, there is a density one subsequence of these eigenfunctions which are uniformly distributed in the unit cotangent bundle S^*M. In Chapter 4, we study the small scale equidistribution of eigenfunctions on flat tori. There is a trivial lower bound known as the Planck scale for the small scale equidistribution of eigenfunction. We show that there exists big holes where small scale equidistribution does not hold in that scale. The existence of big holes was noted by Bourgain independently [LR15]. We show the optimal exponent for the small scale equidistribution of eigenfunctions in the following corollary:

Corollary 1.3.1 *Let $\mathbb{T}^d := \frac{\mathbb{R}^d}{\mathbb{Z}^d}$ be a $d \geq 5$ dimensional flat torus and $\{\psi_i\}$ an orthonormal basis of eigenfunctions for the laplacian operator. Let E_n be the associated eigenspace for eigenvalue $n \in \mathbb{Z} \geq 0$ and $B_n := E_n \cap \{\psi_i\}$ be the restriction of the orthonormal basis $\{\psi_i\}$ to E_n. Then there exists a large subset $C_n \subset B_n$, which means $|C_n| = (1 - o(1))|B_n|$, such that along any sequence of $\{\psi_n : \psi_n \in C_n\}$*

$$\lim_{n\to\infty} \sup_{B(y,r)} \Big| \frac{1}{vol(B(y,r))} \int_{B(y,r)} |\psi_n(x)|^2 dvol(x) - 1 \Big| = o(1), \tag{1.2}$$

where $B(y,r)$ is any ball of radius $r > \lambda_n^{-\frac{1}{2(d-1)}+o(1)}$ centered at an arbitrary point $x \in \mathbb{T}^d$. The exponent $-\frac{1}{2(d-1)}$ is optimal. In fact there exists a sequence of balls with radius $r \approx \lambda_n^{-\frac{1}{2(d-1)}-o(1)}$ and an orthonormal basis $\{\psi_i\}$ where (1.2) does not hold for a positive proportion of eigenfunctions in B_n.

This corollary gives a definite answer to a conjecture of Lester and Rudnick on the small scale equidistribution of orthonormal basis of eigenfunctions restricted to an individual eigenspace on the flat torus $\mathbb{T}^d$ for $d \geq 5$ [LR15].

1.4 Outline of the Thesis

Chapter 2 is concerned with Question 1.0.1 for every integral quadratic form in 4 or more varables. For a non-degenerate integral quadratic form $F(x_1, \ldots, x_d)$ in 5 (or more) variables, we prove an optimal strong approximation theorem. Fix any compact subspace $\Omega \subset \mathbb{R}^d$ of the affine quadric $F(x_1, \ldots, x_d) = 1$. Suppose that we are given a small ball B of radius $0 < r < 1$ inside Ω, and an integer m. Further assume that N is a given integer which satisfies $N \gg (r^{-1}m)^{4+\epsilon}$ for any $\epsilon > 0$. Finally assume that we are given an integral vector $(\lambda_1, \ldots, \lambda_d)$ mod m. Then we show that there exists an integral solution $x = (x_1, \ldots, x_d)$ of $F(x) = N$ such that $x_i \equiv \lambda_i \bmod m$ and $\frac{x}{\sqrt{N}} \in B$,

provided that all the local conditions are satisfied. We also show that 4 is the best possible exponent. Moreover, for a non-degenerate integral quadratic form $F(x_1, \ldots, x_4)$ in 4 variables we prove the same result if $N \geq (r^{-1}m)^{6+\epsilon}$ and some non-singular local conditions for N are satisfied. Based on some numerical experiments on the diameter of LPS Ramanujan graphs, we conjecture that the optimal strong approximation theorem holds for any quadratic form $F(X)$ in 4 variables with the optimal exponent 4.

Chapter 3 is concerned with Ramanujan graphs. We show that, for an infinite family of $(p+1)$-regular LPS Ramanujan graphs, we show that the diameter of these graphs is greater than or equal to $\lfloor (\frac{4}{3}) \log_p(n) \rfloor$, where p is an odd prime number and n is the number of vertices. On the other hand, for any k-regular Ramanujan graph we show that the distance of only tiny fraction of all pairs of vertices is greater than $(1+\epsilon)\log_{k-1}(n)$. We also have some numerical experiments for LPS Ramanujan graphs and random Cayley graphs which suggest that the diameters are asymptotically $(\frac{4}{3})\log_{k-1}(n)$ and $\log_{k-1}(n)$, respectively. These are consistent with Sarnak's expectation on the covering exponent of universal quantum gates and our conjecture for the optimal strong approximation for quadratic forms in 4 variables.

Chapter 4 is concerned with small scale equidistribution of eigenfunctions on flat tori. Let $Q(X)$ be any integral primitive positive definite quadratic form with discriminant D and in k variables where $k \geq 4$. We give an upper bound on the number of integral solutions of $Q(X) = n$ for any integer n in terms of n, k and D. As a corollary, we give a definite answer to a conjecture of Lester and Rudnick on the small scale equidistribution of orthonormal basis of eigenfunctions restricted to an individual eigenspace on the flat torus $\mathbb{T}^d$ for $d \geq 5$. Another application of our main theorem gives a sharp upper bound on $A_d(n,t)$, the number of representation of the positive definite quadratic form $Q(x,y) = nx^2 + 2txy + ny^2$ as a sum of squares of $d \geq 5$ linear forms where $n - n^{\frac{1}{(d-1)} - o(1)} < t < n$. This upper bound allows us to study the local statistics of integral points on the sphere.

Chapter 2

Optimal strong approximation for quadratic forms

2.1 Introduction

2.1.1 Statement of results

Before stating our main theorem, we discuss three applications. The first addresses the question of approximating real matrices by integral matrices. More precisely, let A be a 2×2 matrix of determinant 1 and m be a positive integer. How well can one approximate A by $m^{-\frac{1}{2}}B$, where B is an integral matrix of determinant m? Tijdeman [Tij86], showed that there exists B such that

$$\max_{i,j} |m^{-\frac{1}{2}} b_{ij} - a_{ij}| < C m^{-\frac{1}{18}} (\log m)^{7/9}, \tag{2.1}$$

where C is a constant depending on $\max a_{ij}$. Later, Harman [Har90] improved the exponent $-\frac{1}{18}$ to $-\frac{1}{8}$ and showed this exponent cannot be smaller than $-\frac{1}{4}$. Harman remarked that if Hooley's R^* Conjecture were true, then the exponent drops to $-\frac{1}{6}$. Subsequently, Chiu [Chi95] remarked that an estimate of $|a(p)| < 2p^r$ for Maass cusp forms would yield an exponent of $[(r+1/2)-1]/3$. Therefore, if one assumes the Ramanujan Conjecture for $SL(2,\mathbb{Z})$ Maass cusp forms, then the exponent drops to $-\frac{1}{6}$. The best known bound toward the Ramanujan conjecture is $\frac{7}{64}$ [Kim03] and this yields $-\frac{1}{8} - \frac{1}{192}$, which slightly improves Harman's bound. It is interesting that under the most favorable conditions, the two different methods give the same exponent $-\frac{1}{6}$. Our theorem for the quadratic form $q(x_1, \ldots, x_4) = x_1x_4 - x_2x_3$ and the archimedean place ∞ shows that the matrix approximation

is possible with the exponent $-\frac{1}{6}$ without any assumptions.

Corollary 2.1.1 *Fix Ω a compact subset of $SL(2,\mathbb{R})$ and any $0 < \epsilon$. Then for every matrix $A \in \Omega$ and $m \in \mathbb{Z}$, there exists an integral matrix $B \in M_{2\times 2}[\mathbb{Z}]$ such that $\det(B) = m$ and*

$$\|A - \frac{1}{m}B\| \ll m^{-\frac{1}{6}+\epsilon}, \tag{2.2}$$

where $\ll$ only depends on ϵ and Ω. Moreover, we cannot replace $-\frac{1}{6}$ in the exponent with a number smaller than $-\frac{1}{4}$.

Remark 2.1.2 *We conjecture that our theorem, which is optimal for 5 or more variables, holds with the same optimal exponent 4 for quadratic forms in 4 variables. As a result, the matrix approximation is possible with the optimal exponent $-\frac{1}{4}$.*

As the second application of our main theorem, we prove an asymptotic formula for the number of lattice points in a small cap on the sphere, i.e. the intersection of a ball with a small radius and the sphere. In the appendix of [BR12], an upper bound for the number of lattice points in such small caps is given. Following a suggestion of Bourgain [Sar15a, Page 23] we promote this to a lower bound and at the same time we prove this more general result, namely an asymptotic formula for the number of lattice points in a small cap. We illustrate our main theorem in the following application:

Corollary 2.1.3 *Let $S^d(R)$ be any d-dimensional sphere of radius R such that $N := R^2$ is an integer and $d \geq 4$. Suppose we are given a spherical cap of diameter Y where $Y \gg R^{1/2+\delta}$ for any $\delta > 0$. Then the number of integral lattice points inside this spherical cap is given by the following formula*

$$\sigma_\infty \mathfrak{S}(N)\frac{Y^d}{R} + O_{\epsilon,\delta}(\frac{Y^d}{R^{1+\epsilon}}), \tag{2.3}$$

where σ_∞ and $\sigma(N)$ are the singular integral and series (see below), and O and ϵ depend on δ not on the spherical cap or N. Moreover, $Y \gg R^{1/2+\delta}$ is necessary. For $d = 4$, if $Y \geq R^{2/3+\delta}$ for any $\delta > 0$ and N is not divisible by 2^k where $2^k \gg N^\epsilon$ for any ϵ, then we have the same formula.

Remark 2.1.4 *$\mathfrak{S}(N) = \prod_p \sigma_p(N)$ is the singular series. The singular series is nonzero if and only if $\sigma_p(N) \neq 0$ for every p. The condition $\sigma_p(N) \neq 0$ is equivalent to having local points over the p-adic integers $\mathbb{Z}_p$. If we have local points over every prime p we say that all the local conditions are satisfied. For $d \geq 5$, if $\mathfrak{S}(N) \neq 0$ then $\mathfrak{S}(N)$ is bounded form below and above by two positive*

constants c_1 and c_2 where do not depend on N. For $d = 4$, we require some non-singular local conditions on N which imply the following lower bound on the singular series $\mathfrak{S}(N)$

$$\mathfrak{S}(N) \gg N^{-\epsilon}.$$

for any $\epsilon > 0$. The singular integral σ_∞ is defined as

$$\sigma_\infty := \frac{Vol\ (spherical\ cap\ of\ size\ Y)}{Y^{d-1}}.$$

Therefore, the main term dominates the error term.

On the other hand, for every primitive integral vector $\vec{a}$, let $\tilde{a} = R\frac{\vec{a}}{|a|}$ be the parallel vector to $\vec{a}$ on the sphere $S^{d-1}(R)$. Then there is a cap of size $c_1\frac{R^{1/2}}{\sqrt{|a|}}$ with no integral points inside the cap centered at $\tilde{a}$ with size $c_2\frac{R^{1/2}}{\sqrt{|a|}}$, where c_1 and c_2 are universal constants. As a result, the covering exponent of integral points on the sphere, that is defined in [Sar15a], is

$$\begin{aligned} K &:= \limsup_{R\to\infty} \frac{\log\big(\text{Number of integral points on } S^{d-1}(R)\big)}{\log\big(\frac{\text{Volume of } S^{d-1}(R)}{\text{Volume of the largest empty spherical cap}}\big)} \\ &= \frac{\log(R^{d-2})}{\log(R^{\frac{d-1}{2}})} \\ &= 2 - \frac{2}{d-1}. \end{aligned} \tag{2.4}$$

for $d \geq 5$ and is

$$4/3 \leq K \leq 2$$

for $d = 4$.

Remark 2.1.5 *Sarnak in his letter [Sar15a] to Aaronson and Pollington, showed that $4/3 \leq K \leq 2$ for $d = 4$. To show that $K \leq 2$ he appealed to the Ramanujan bound on the Fourier coefficients of weight k-modular forms, while the lower bound $4/3 \leq K$ is a consequence of an elementary number theory argument. Furthermore, Sarnak states some open problems [Sar15a, Page 24]. The first one is to show that $K < 2$ or even that $K = 4/3$. We conjecture that the optimal strong approximation holds for quadratic forms in 4 variables which would imply that indeed $K = 4/3$.*

Another application of the theorem 4.1.4 recovers the best known upper bound for the diameter of the Ramanujan graphs constructed by Lubotzky, Phillips and Sarnak [LPS88] without appealing

to the Ramanujan bound on the Fourier coefficients of weight two modular forms [Eic54].

Corollary 2.1.6 *Let $q(x_1, \ldots, x_d) = \sum_{i=1}^{d} x_i^2$ where $5 \leq d$. Suppose m and N are given integers where $N \gg m^{4+\delta}$ for any $\delta > 0$, and assume that $(\lambda_1, \ldots, \lambda_d)$ is any integral vector where $q(\lambda_1, \ldots, \lambda_d) \equiv N \bmod m$. Then we have integral solutions for*

$$q(x_1, \ldots, x_d) = N \text{ with } x_i \equiv \lambda_i \bmod m,$$

provided that all the local conditions are satisfied. For $d = 4$, we prove the same result when $N \gg m^{6+\delta}$ and N is not divisible by 2^k where $2^k \gg N^{\epsilon}$ for any ϵ . In particular, we recover the best known upper bound on the diameter of LPS Ramanujan graphs $X_{p,q}$ by choosing $N = p^n$ and $m = q$ where $q^{6+\delta} \ll p^n$ for any $\delta > 0$.

Remark 2.1.7 *In [TS15] we demonstrated some numerical experiments on the diameter of the LPS Ramanujan graphs that the diameter is asymptotically*

$$diam \approx \frac{4}{3} \log_{k-1}(n).$$

The numerical experiments for the diameter of LPS Ramanujan graphs support our conjecture for the optimal strong approximation for quadratic forms in 4 variables.

The first form of our main theorem is the following.

Theorem 2.1.8 *Fix $F(X)$ a non-degenerate quadratic form in 5 or more variables and let Ω be a compact subset of the affine quadric $F(X) = 1$ over real numbers. Suppose that we are given any small ball B of radius $0 < r < 1$ inside Ω, and an integer m. Further assume that N is a given integer which satisfies*

$$N \gg (r^{-1}m)^{4+\delta},$$

for any $\delta > 0$ where the constant for $\gg$ only depends on Ω and δ. Finally assume that we are given an integral vector $(\lambda_1, \ldots, \lambda_d)$ mod m. Then there exists an integral solution $F(x_1, \ldots, x_d) = N$ such that

$$x_i \equiv \lambda_i \bmod m \text{ and } \frac{(x_1, \ldots, x_d)}{\sqrt{N}} \in B,$$

provided that all the local conditions are satisfied. The exponent 4 is optimal in $N \gg (r^{-1}m)^{4+\delta}$.

For a quadratic form $F(X)$ in 4 variables the same result holds provided that

$$N \gg (r^{-1}m)^{6+\delta},$$

and we require non-singular local conditions on N which imply the singular series $\mathfrak{S}(N) \gg N^{\epsilon}$ for any $\epsilon > 0$. We cannot replace 6 in the exponent with a number smaller than 4.

Based on our numerical experiments on the diameter of the Ramanujan graph [TS15] and the existence of the optimal lift for the case of $SL_2(\mathbb{Z}) \to SL_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ which is shown by an elementary method by Sarnak [Sar15b], we make the following conjecture.

Conjecture 2.1.9 *We conjecture that for a quadratic form with 4 variables the same result holds for*

$$N \gg (r^{-1}m)^{4+\delta}.$$

Therefore, the exponent 4 is the optimal exponent for every quadratic form with 4 or more variables.

In what follows, we state a stronger theorem and as a result deduce our main theorem. We give a formula for the number of integral points in an open neighborhood which is defined in the adelic topology. For every prime number p, there is a natural norm $\|.\|_p$ on the vector space $\mathbb{Q}_p^d$ given by

$$\|x - y\|_p := \max_{1 \leq i \leq n} |x_i - y_i|_p. \tag{2.5}$$

For the archimedean place ∞, we fix an arbitrary norm $\|.\|_\infty$ on $\mathbb{R}^d$. For a place v of $\mathbb{Q}$ and a point $b \in \mathbb{Q}_v^d$, we define the ball $B_v(b, r)$ centered at b and radius r as follows:

$$B_v(b, r) := \big\{x \in \mathbb{Q}_v^d : \|x - b\|_v \leq r\big\}. \tag{2.6}$$

Note that for a non-archimedean place v, the radius r takes discrete values q_v^n, where q_v is the order of the residue field and $n \in \mathbb{Z}$. We define the integral ring of adeles as the product

$$\mathbb{A}_{\mathbb{Z}}^d := \mathbb{R}^d \times \prod_p \mathbb{Z}_p^d, \tag{2.7}$$

and equip it with the product metric. We define a global ball B in $\mathbb{A}_{\mathbb{Z}}^d$ to be the product of local

ones such that the radius of local balls is 1 for almost all places, i.e.

$$B = B(b, r) \times \prod_p B(a(p), p^{-\nu_p}),$$

such that $\nu_p = 0$ for almost all primes. Note that $B(a(p), 1) = \mathbb{Z}_p^d$. We define the norm of the global ball B to be

$$|B| := r \prod_p p^{-\nu_p}.$$

Since $\nu_p = 0$ for almost all primes, the norm is well defined for global balls. The following theorem is the most general form of our main theorem.

Theorem 2.1.10 *Fix a non-degenerate quadratic form $F(X) = X^T AX$ in $d \geq 5$ variables and let V_N be the affine quadric $F(X) - N = 0$. Fix Ω a compact subset of the quadric $V_1(\mathbb{R})$ and consider the following compact topological space:*

$$\Theta := \Omega \times \prod_p V_N(\mathbb{Z}_p).$$

Suppose that we are given a global ball $B := B(b, r) \times \prod_p B(a(p), p^{-\nu_p})$ with the following lower bound on the norm

$$|B| \gg N^{-\frac{1}{4}+\delta},$$

where $b \times \prod_p a(p) \in \Theta$ and $\gcd(a(p), p) = 1$, i.e. $|a(p)|_p = 1$. Let $|V_N(\mathbb{Z}) \cap B|$ be the number of integral points inside B, then

$$|V_N(\mathbb{Z}) \cap B| = \sigma_\infty(F, b) \prod_p \sigma_p(a(p), N)|B|^{d-1} N^{\frac{d-2}{2}} + O(|B|^{d-1} N^{\frac{d-2}{2}} N^{-\epsilon}), \tag{2.8}$$

for some $\epsilon > 0$ where ϵ and O only depend on Ω and δ and not on the global ball B or N. For a non-degenerate quadratic form $F(X)$ in 4 variables the same formula holds provided that

$$|B| \gg N^{-\frac{1}{6}+\delta}.$$

and we require non-singular local conditions on N which imply the singular series $\mathfrak{S}(N) \gg N^{-\epsilon}$ for any $\epsilon > 0$. On the other hand, fix any primitive integral vector $q := (q_1, \ldots, q_d)$, i.e. $\gcd(q_1, \ldots, q_d) = 1$ where $F(q) > 0$. Let

$$B := B(a_\infty q, r) \times \prod_p B(a_p q, p^{-\nu_p}),$$

where $a_p \in \mathbb{Z}_p$ *and* $a_p q \in V_N(\mathbb{Z}_p)$ *if* $\nu_p \neq 0$ *and* $a_\infty = \frac{1}{\sqrt{F(q)}}$. *Note that there exists* $a_p \in \mathbb{Z}_p$ *such that* $a_p^2 = \frac{N}{F(q)}$ *if* $\left(\frac{N}{p}\right) = \left(\frac{F(q)}{p}\right)$, *where* $\left(\frac{\cdot}{\cdot}\right)$ *is the Legendre symbol. Hence, for the finite set of places where* $\nu_p \neq 0$, *we require that* $\left(\frac{N}{p}\right) = \left(\frac{F(q)}{p}\right)$. *Assume that*

$$|B| \geq c_1 \frac{N^{-\frac{1}{4}}}{\sqrt{|q|}}$$

then there exists a global B' *inside* B *with no integral points and a norm greater than*

$$|B'| > c_2 \frac{N^{-\frac{1}{4}}}{\sqrt{|q|}}$$

where c_1 *and* c_2 *are universal constants depends only on* Ω *and* $F(X)$.

Remark 2.1.11 *We have the following lower bounds on the product of local densities [Mal62, Remark 7 Page 73]*

$$c_\epsilon N^{-\epsilon} \leq \sigma_\infty(F, b) \prod_p \sigma_p(a(p), N).$$

where c_ϵ *only depends on* $F(x)$ *and* ϵ. *Therefore, the error term is smaller by a factor of* $N^{-\epsilon}$. *If* $\gcd(p^{\nu_p}, a_1(p), \ldots, a_d(p)) = p^{h_p} \neq 1$ *for some* p, *we can divide* N *by* p^{2h_p} *and replace the local balls at the place* p *by* $B(\frac{a(p)}{p^{h_p}}, p^{-(\nu_p - h_p)})$ *and use the above theorem. Since the power of* N *is* $\frac{d-2}{2}$ *and the power of* $|B|$ *is* $d-1$ *in the formula 2.8, the main term would be multiplied by* $\prod_p p^{h_p}$.

2.1.2 Further motivations and techniques

In several papers, Wright proved various results about the representation of a number N as a sum of squares "almost proportional" to assigned positive numbers $\lambda_1, \lambda_2, \ldots, \lambda_d$. For example in [Wri33], he improved his previous result and showed in the case of sum of five squares, if

$$\begin{aligned} \lambda_1 + \cdots + \lambda_5 = 1, \text{ where } 0 < \lambda_i, \\ \text{and } 0 < \epsilon, \end{aligned} \tag{2.9}$$

then a large enough integer N depending on ϵ is representable by a sum of five squares satisfying

the following conditions

$$\begin{aligned} N &= n_1^2 + \cdots + n_5^2, \\ |n_i^2 - \lambda_i N| &< U \\ N^{1-\frac{1}{8}+\epsilon} &\leq U. \end{aligned} \tag{2.10}$$

Note that the inequality $N^{1-\frac{1}{8}+\epsilon} \leq U$ is not sharp and can be improved to $N^{1-\frac{1}{4}+\epsilon} \leq U$. He also showed that the number of representation is

$$\asymp \frac{U^4}{\sqrt{N}}. \tag{2.11}$$

By an entirely elementary method Chowla and Auluck in [AC37] proved a sharp result for the special point $(\lambda_1, \ldots, \lambda_4) = (\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ and sum of four squares. They showed every positive integer $N \neq 0 \mod 8$ is expressible in the form

$$N = n_1^2 + \cdots + n_4^2,$$

where n_i are integers satisfying

$$\frac{N}{4} - n_i^2 = O(N^{\frac{3}{4}}).$$

It follows from Wright's result [Wri37] that the $O(N^{\frac{3}{4}})$ in this theorem cannot be replaced by $o(N^{\frac{3}{4}})$. More generally, he considered the sum of d kth powers and proved the diagonal point $(a, \ldots, a)$ repels the integral points. We will discuss this repulsion property in more detail in section 2.2.

In a recent paper [Dae10], Daemen gave a lower bound for the number of the integral points $(x_1, \ldots, x_d)$ close to the diagonal point $(a, \ldots, a)$ such that

$$x_1^k + \cdots + x_s^k = N.$$

He proved that for every k there exists s_k such that if $s \geq s_k$, if one takes a neighbourhood bigger by a large constant than the repulsion neighbourhood of Wright [Wri37], then one has a lower bound for the number of integral points which differs by a constant compared to the upper bound. For the sum of squares, his result implies that $s_2 = 9$. He remarked that by working a little harder, one can replace the number 9 for s_2 by 7. Our results show that this holds with 5 or more variables.

Our method is based on the Kloosterman circle method. This method has been developed by Kloosterman to prove the local to global principal for quadratic forms in 4 variables; see [Klo27]. For

the purpose of representation of integers by quadratic forms, if the number of variables is 5 or more the classical circle method of "major and minor " arcs works fine. However, for 4 variables it does not work. Kloosterman introduced a new method of dissection by Farey sequence (and no minor arcs) which deals with 4 variables. The problem of the distribution of integral points on quadrics between different residue classes to a fixed integer m has been studied by Malyshev; see [Mal62]. Malyshev used Kloosterman's method and proved a result about the distribution of integral points of the quadric $F(X) = N$ with 4 or more variables between residue class of an integer m. An application of our main theorem 4.1.4 significantly improves the exponents of m and N in his main theorem for $F(X)$ fixed. In our work, the method proves to be decisive in 5 or more variables as it gives the optimal exponent for lifting solutions. Our small sets optimal result for 5 variables depends crucially on the square root cancellation in the exponential sums and also relies on the refinement of the Kloosterman method developed by Duke, Friedlander and Iwaniec that is called delta method; see [DFI93]. In the delta method we use a smooth cut off function over the Farey dissections. The delta method allows us to use the rapid decay of the Fourier transform of the weight function and makes computations handier. For proving our main theorem 4.1.4, we are using a version of this method developed by Heath-Brown in [HB96]. In that method we first apply the delta method and then a Poisson summation over the sum of lattice points. We briefly describe the new method here and its advantages compared to the classical circle method.

Assume that we have a smooth bounded function $|F(x_1, \dots, x_d)| \leq T$ defined on a bounded region $U \subset \mathbb{R}^d$ and it takes integral values on the integral points. We are interested in counting the integral roots of F inside U. We write N for the weighted number of the integral roots counted by a smooth weight function w which is compactly supported on U. Since the function is bounded by T, we have the following formula for N:

$$N = \frac{1}{2T+1} \sum_{x \in \mathbb{Z}^d} w(x) \sum_{a=0}^{T-1} e(\frac{aF(x)}{2T+1}). \tag{2.12}$$

Following the classical circle method, we collect the fractions $\frac{a}{T}$ which are close to the $\frac{r}{q}$ where q is much smaller than T in to the major arcs and estimate this sum which gives us the main term. We give an upper bound for the complement of this set which is the minor arcs.

In the new circle method, the main idea is that we can expand the delta function on the integral interval $[-T, -(T-1), \dots, T-1, T]$ with smoother functions than $e(\frac{ax}{2T+1})$. The dimension of the

vector space of functions on this interval is $2T+1$. If we take the following set of function

$$\left\{e(\frac{ax}{q}) : \text{ where } \gcd(a,q)=1 \text{ and } q \le Q := 10\sqrt{T}\right\} \tag{2.13}$$

then this set spans the vector space of functions on the integral interval $[-T, -(T-1), \ldots, T-1, T]$. We can write the delta function as a linear combination of these functions and by an averaging argument we can assume without lost of generality that the coefficients $c_{q,n}$ don't depend on a mod q. Hence for $-T \le n \le T$,

$$\delta(n) = \sum_{q=1}^{Q} \sideset{}{^*}\sum_{a \bmod q} c_{q,n} e(\frac{an}{q}). \tag{2.14}$$

Note that q is now bounded by $10\sqrt{T}$ compared to $2T+1$ by the previous expansion, where we used $e(\frac{aF(x)}{2T+1})$. However, we need to control the smoothness of the coefficients $c_{q,n}$ as a function of n. Intuitively, we want to pay a higher cost for smaller value of q since it is multiplied by a smoother function $e(\frac{ax}{q})$ and we want the whole function $c_{q,n}e(\frac{an}{q})$ be smooth. In other words, we want $c_{k_1,n}$ be smoother than $c_{k_2,n}$ if $k_1 \ge k_2$. The existence of this expansion for the delta function has been established by Iwaniec and Kowalski; see [IK04, Chapter 20]. They proved that there exists an appropriate smooth function $h(x,y)$, such that

$$\begin{aligned} c_{q,n} &= \frac{C_Q}{Q^2} h(\frac{q}{Q}, \frac{n}{Q^2}), \text{ where } Q^2 \approx T \\ \delta(n) &= \frac{C_Q}{Q^2} \sum_{q=1}^{Q} \sideset{}{^*}\sum_{a \bmod q} e(\frac{an}{q}) h(\frac{q}{Q}, \frac{n}{Q^2}). \end{aligned} \tag{2.15}$$

We construct and state the main properties of $h(x,y)$ in Section 2.3.1. Using this expansion, we have the following formula for N

$$N = \sum_{x \in \mathbb{Z}^d} \frac{C_Q}{Q^2} \sum_{q=1}^{Q} \sideset{}{^*}\sum_{a \bmod q} e(\frac{aF(x)}{q}) h(\frac{q}{Q}, \frac{F(x)}{Q^2}) w(x). \tag{2.16}$$

We change the order of the summation and apply the Poisson summation on the sum over $x \in \mathbb{Z}^d$. We obtain

$$N = \frac{C_Q}{Q^2} \sum_{q=1}^{Q} \sideset{}{^*}\sum_{a \bmod q} q^{-d} \sum_{c \in \mathbb{Z}^d} S_q(a,c) I_q(c). \tag{2.17}$$

where

$$I_q(c) := \int_{\mathbb{R}^d} h(\frac{q}{Q}, \frac{F(x)}{Q^2}) w(x) e(-\frac{\langle c, x\rangle}{q}) dx$$
$$S_q(a,c) := \sideset{}{^*}\sum_{a \bmod q} e(\frac{aF(x) + \langle x, c\rangle}{q}).$$

From now on, we assume that the function $F(x_1, \ldots, x_d)$ is a non-degenerate quadratic form. We sum the Gaussian sums $S_q(a,c)$ over $\sum_{a \bmod q}$ and obtain

$$S_q(c) := \sum_{a \bmod q} S_q(a,c). \tag{2.18}$$

$S_q(c)$ is a Kloostermann's sum for even d or Salie's sum for odd d. In either cases, we have square root cancellation. Hence,

$$N = \frac{C_Q}{Q^2} \sum_{q=1}^{Q} q^{-d} \sum_{c \in \mathbb{Z}^d} S_q(c) I_q(c). \tag{2.19}$$

We separate the nonzero terms and write

$$N = \frac{C_Q}{Q^2} \sum_{q=1}^{Q} q^{-d} S_q(0) I_q(0) + \frac{C_Q}{Q^2} \sum_{q=1}^{Q} q^{-d} \sum_{c \neq 0 \in \mathbb{Z}^d} S_q(c) I_q(c). \tag{2.20}$$

We usually get the main term of the counting from the zero terms and bound the nonzero terms by putting absolute value inside the sum. We give upper bounds on

$$\frac{C_Q}{Q^2} \sum_{q=1}^{Q} q^{-d} \sum_{c \neq 0 \in \mathbb{Z}^d} |S_q(c)||I_q(c)| \tag{2.21}$$

Remark 2.1.12 *Note that in the sum (2.21), we are using different upper bounds by algebraic tools on $S_q(c)$ and from analysis on $I_q(c)$. The norm of c is not important in the sum $S_q(c)$, it only depends on the the congruence class of the integral vector c mod q. On the other hand, the fact that c is an integral vector is not important in $I_q(c)$, the absolute value of $I_q(c)$ depends on the position of this vector as a vector in $\mathbb{R}^d$ and the support of the weight function w.*

For the integral $I_q(c)$, we have

$$\begin{aligned} I_q(c) &= \int_{\mathbb{R}^d} h(\frac{q}{Q}, \frac{F(x)}{Q^2}) w(x) e(-\frac{\langle c, x\rangle}{q}) dx \\ &= \int_{\mathbb{R}} p_{\frac{q}{Q}}(\xi) \int_{\mathbb{R}^d} w(x) e(\xi \frac{F(x)}{Q^2} - \frac{\langle c, x\rangle}{q}) dx d\xi, \end{aligned} \tag{2.22}$$

where $p_r(\xi) := \int_{\mathbb{R}} h(r,x) e(-x\xi) dx$, is the Fourier transform of $h(r,x)$ in variable x. We consider the

function $I_q(kc)$ as a function of $k \in \mathbb{Z}$ in the direction of the vector c. We prove that, we have either an exponential decay or a polynomial decay in k. If we don't have a critical point in the oscillatory function $\xi \frac{F(x)}{Q^2} - \frac{\langle c,x \rangle}{q}$ on the support of $w(x)$, then we have exponential decay in k and this is the content of the Lemma 2.5.1. Otherwise, we have polynomial decay and this is the content of the Lemma 2.5.2. Following this strategy, we prove our main theorem 4.1.4 in section 2.6.

In a series of lectures and notes; see [Sar15a], Sarnak revisited the Solovay-Kitaev theorem. The general question comes from theoretical quantum computing. We briefly state the problem here and mention its relevance to our work. Assume that we have a compact group G, (for example $SL_2(\mathbb{Z}_p)$ or $PU(2)$). We want to find a finite set $\mathfrak{g} := \{s_1, s_2, \dots, s_v\}$ such that the group $\Gamma := \langle s_1, \dots, s_v \rangle$ generated by $\mathfrak{g}$ is topologically dense in G and covers G with a "fast mixing rate". Sarnak defined the covering exponent $K(\mathfrak{g})$ in [Sar15a] and proved for example the following special case:

Example 2.1.13 *Let $G = PU(2)$ and*

$$\mathfrak{g} = \{ \frac{1}{\sqrt{5}} \begin{bmatrix} 1+2i & 0 \\ 0 & 1-2i \end{bmatrix}^{\pm}, \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 2i \\ 2i & 1 \end{bmatrix}^{\pm}, \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 2 \\ -2 & 1 \end{bmatrix}^{\pm} \},$$

then we have the following bound for the covering exponent

$$\frac{4}{3} \leq K(\mathfrak{g}) \leq 2 \tag{2.23}$$

The inequalities (2.23) is another presentation of our main theorem 4.1.4 for the diophantine equation $x_1^2 + \cdots + x_4^2 = 5^h$. The lower bound $\frac{4}{3} \leq K(\mathfrak{g})$ comes from the repulsion of the integral points, in another words the fact that the lower bound $r^{-4} \ll 5^h$ is optimal in our main theorem 4.1.4. The upper bound $K(\mathfrak{g}) \leq 2$ comes from the special case $d = 4$ in our main theorem 4.1.4 and the lower bound $r^{-6} \ll 5^h$ in this case. In a letter to Scott Aaronson and Andy Pollington, Sarnak wrote [Sar15a, Page 23]:

" For $n \geq 3$ the determination of K (the covering exponent) for S-arithmetic points on S^n becomes easier. As pointed out to me by Bourgain, an application of the circle method as done in the Appendix [BR12], can be promoted to an asymptotic (and not just an upper bound) when one has this many variables, for counting these points in small caps. As a consequence we have together with the repulsion that for $n \geq 3$

$$K(S^n, \mathbb{Z}[\frac{1}{5}]) = 2 - \frac{2}{n}. \tag{2.24}$$

"

This was our main motivation to run the circle method which allowed us to prove our main theorem 4.1.4. We are very grateful for this suggestion.

In the recent work of Kleinbock and Merrill [KM13], they proved the analogue of the Dirichlet's Theorem for the rational points on spheres. Their result implies that the covering exponent for the rational points on spheres is 2:

$$K(S^n, \mathbb{Q}) = 2. \tag{2.25}$$

Their method is quite interesting. It links the problem of the rational approximation to the following standard question in dynamical systems: whether the orbit of a point hits a "shrinking target". In the expository paper of Ghosh-Gorodnik and Nevo [GGN14], the more general problem of diophantine approximation for the homogeneous varieties has been discussed. We briefly describe their method here. Given a homogeneous variety $X := G/H$, the rational points or S-integral points of X are associated to the orbit of a lattice $\Gamma \subset G$ acting on X. The "Duality principle" links the question about the density of the orbit Γ in X to the mixing property of H acting on $\Gamma\backslash G$. Now, the question is about the decay of the matrix coefficients of the representation of $L^2(\Gamma\backslash G)$ as a representation of H. In the cases, where the restriction of the automorphic representation of $L^2(\Gamma\backslash G)$ to H is tempered as a representation of H, we have optimal diophantine approximation exponents.

2.1.3 Outline of the chapter

In section 2.2, we prove that the exponent 4 in the main theorem 4.1.4 is the best possible exponent, i.e., we construct an example where $N \gg r^{-4} \prod_p r_p^{-4}$ and for which we do not have any integral points on $F(x) = N$ in the corresponding local neighborhood. We explain briefly the main idea here. We take a point $a \in \{F(x) = N\}$, so that the tangent space of this point is defined by a hyperplane with integral coefficients. We consider those integral points which satisfy the mod m congruence condition $F(a_1, \ldots, a_d) \equiv l \bmod m$. Then if we slice our variety with the hyperplanes passing through these integral points and are parallel to this tangent space, the distance of those parallel hyperplanes is of order m. However, if we restrict our integral point to those on the variety $F(x) = N$, then the congruence condition $F(a_1, \ldots, a_d) \equiv l \bmod m$, impose a congruence condition mod m^2 and as a result, the distance of those parallel hyperplanes is of order m^2. Hence, we don't have any integral points with the given congruence condition between these slices and this gives us the repulsion that we need.

In section 2.3, we describe the delta method. We cite the main properties of the weight function $h(x, y)$ in lemma 2.3.3 and lemma 2.3.4. These are standard lemmas and can be found in the

literature [HB96]. Lemma 2.3.4 is crucial in the upper bound that we give on the integral $I_{mq}(c)$.

In section 2.4, we give an upper bound for the quadratic exponential sums $S_{mq}(c)$. First in Lemma 2.4.1, we show that this exponential sum is nonzero for certain congruence class c mod m. We reduce the sum $S_{mq}(c)$ to the Kloostermann's sum (Salie's sum) for even (odd) dimension. We use the well known bounds on the Kloostermann's sum (Salie's sum) to prove the main Lemma 2.4.4.

In section 2.5, we give an upper bound on the integral $I_{mq}(c)$. In the subsection 2.5.1, we prove an upper bound on the integral $I_{mq}(c)$ from the decay of the Fourier transform of $h(x, y)$ given in the lemma 2.3.4. In subsection 2.5.2, we use the stationary phase theorem to give an upper bound on the integral $I_{mq}(c)$. We improve the exponent $1 - \frac{n}{2}$ in the [HB96][Lemma 22; Page 39] of the Heath-Brown paper to $-\frac{n-1}{2}$. This improvement is essential in our treatment to get an optimal strong approximation result and this is the subject of Lemma 2.5.2. Finally, in the section 2.6 we prove our main theorem 2.1.10.

2.2 Repulsion of integral points

In this section we prove that the exponent 4 in our main theorem cannot be replaced by a smaller number. In fact we prove the second part of Theorem 2.1.10 which is a stronger result.

Let $F(X) = X^T AX$ be our non-degenerate quadratic form with 4 or more variables and discriminante $\Delta = \det(A)$. We recall that

$$\Theta := \Omega \times \prod_p V_N(\mathbb{Z}_p).$$

For every primitive integral vector q, a positive real number $0 < r < 1$ and an integer m where

$$\gcd(m, F(q)N\Delta) = 1,$$

and

$$\Big(\frac{N}{p}\Big) = \Big(\frac{F(q)}{p}\Big) \text{ for every prime } p|m \ ,$$

where $\Big(\frac{\cdot}{\cdot}\Big)$ is the Legendre symbol and $\Big(\frac{\cdot}{\infty}\Big)$ is the sign function. We define a global ball B inside Θ as

$$B := B(a_\infty q, r) \times \prod_p B(a_p q, p^{-\mathrm{ord}_p(m)}),$$

where $a_p \in \mathbb{Z}_p$ such that $a_p q \in V_N(\mathbb{Z}_p)$ if $p|m$ and $a_\infty = \frac{1}{\sqrt{F(q)}}$. Note that $|B| = rm^{-1}$.

Remark 2.2.1 *Note that $a_p q \in V_N(\mathbb{Z}_p)$ implies that $a_p^2 F(q) = N$ in $\mathbb{Z}_p$. Hence, $a_p^2 = \frac{N}{F(q)}$. Since $\left(\frac{N}{p}\right) = \left(\frac{F(q)}{p}\right)$, we have two solutions $\pm a_p$ for $a_p^2 = \frac{N}{F(q)}$ in $\mathbb{Z}_p$ and for every choice of square root at any prime divisor of m we have a different global ball B.*

Theorem 2.2.2 *Assume that*

$$|B| \geq c_1 \frac{N^{-\frac{1}{4}}}{\sqrt{|q|}},$$

then there exists a global B' inside B with no integral points and a norm greater than

$$|B'| > c_2 \frac{N^{-\frac{1}{4}}}{\sqrt{|q|}}$$

where c_1 and c_2 are universal constants and depend only on Ω and $F(X)$.

Proof: First, we consider the integral points inside B_f, the finite part of the global ball B, namely

$$B_f := \prod_p B(a_p q, p^{-\mathrm{ord}_p(m)}).$$

We assume that x is an integral point such that $x \in B_f$. Hence,

$$x \equiv a_p q \bmod p^{\mathrm{ord}_p(m)}, \text{ for every } p|m.$$

By the Chinese remainder theorem there exists α such that

$$x \equiv \alpha q \bmod m,$$

where $\alpha \equiv a_p \bmod p^{\mathrm{ord}_p(m)}$. Hence, $x = mt + \alpha q$ for some integral vector t. We write the Taylor expansion of $F(mt + \alpha q)$ at αq , i.e.

$$F(tm + \alpha q) = m^2 F(t) + 2mt^T A\alpha q + F(\alpha q) = N.$$

Since $\gcd(q\alpha, m) = 1$, we deduce that

$$t^T Aq \equiv \frac{N - F(\alpha q)}{2m\alpha} \bmod m.$$

Therefore, there exists a fixed number $l_0 \bmod m^2$ such that

$$\begin{aligned} \langle x, Aq\rangle &\equiv \langle mt + \alpha q, Aq\rangle \bmod m^2 \\ &\equiv l_0. \end{aligned} \tag{2.26}$$

Now consider the infinite part of the global ball B, namely

$$B_\infty := B(a_\infty q, r)$$

Our strategy is to find a shell inside this ball which avoids the integral points $V_N(\mathbb{Z})$. Inside B_∞ we let $\tilde{q}$ be a real point in $V_N(\mathbb{R})$ such that

$$\begin{aligned} \langle \tilde{q}, Aq\rangle = \frac{m^2}{2} + l_0 + km^2 \text{ for some } k \in \mathbb{Z}, \\ \text{and } |\tilde{q} - a_\infty q| \text{ is minimal.} \end{aligned} \tag{2.27}$$

Note that $\tilde{q}$ lies on the nearest parallel hyperplanes $\langle x, Aq\rangle = \frac{m^2}{2} + l_0 + km^2$, when we vary $k \in \mathbb{Z}$, to $a_\infty q$. Assume that $x = \tilde{q} + \xi$ is an integral point inside the global ball B with $F(x) = N$. We write the Taylor expansion of of $F(x)$ at $\tilde{q}$

$$F(\tilde{q} + \xi) = F(\tilde{q}) + 2\tilde{q}^T A\xi + F(\xi).$$

Since $F(x) = F(\tilde{q}) = N$, we deduce that

$$2\tilde{q}^T A\xi + F(\xi) = 0.$$

We give a lower bound on $|2\tilde{q}^T A\xi| = \langle 2\xi, A\tilde{q}\rangle$. Note that

$$|\,\langle 2\xi, A\tilde{q}\rangle\,| \geq |\,\langle 2\xi, a_\infty Aq\rangle\,| - |\,\langle 2\xi, A(\tilde{q} - a_\infty q)\rangle\,|.$$

By the definition of $\tilde{q}$ given in (2.27), we have $\langle 2\xi, Aq\rangle \geq m^2$ and we also use the Cauchy inequality to get $|\,\langle 2\xi, A(\tilde{q} - a_\infty q)\rangle\,| \leq 2|\xi||A||(\tilde{q} - a_\infty q)|$. Therefore,

$$|2\tilde{q}^T A\xi| \geq m^2 a_\infty - 2|\xi||A||(\tilde{q} - a_\infty q)|.$$

Therefore, $2\tilde{q}^T A\xi + F(\xi) = 0$ implies

$$|F(\xi)| \geq m^2 a_\infty - 2|\xi||A||(\tilde{q} - a_\infty q)|. \tag{2.28}$$

From the minimality condition in (2.27), we give an upper bound on $|\tilde{q} - a_\infty q|$. We have

$$F(\tilde{q}) = N,$$

$$[(\tilde{q} - a_\infty q) + q]^T A[(\tilde{q} - a_\infty q) + a_\infty q] = N.$$

Hence

$$(\tilde{q} - a_\infty q)^T A(\tilde{q} - a_\infty q) + 2(\tilde{q} - a_\infty q)^T A a_\infty q = 0.$$

From the minimality condition, one can check that $\tilde{q} - a_\infty q$ is the maximal eigenvector for A, hence

$$(\tilde{q} - a_\infty q)^T A(\tilde{q} - a_\infty q) = |A||(\tilde{q} - a_\infty q)|^2,$$

and moreover

$$|2(\tilde{q} - a_\infty q)^T A a_\infty q| \leq 2a_\infty m^2.$$

Therefore,

$$|A||(\tilde{q} - a_\infty q)|^2 \leq 2a_\infty m^2.$$

Hence,

$$|A||(\tilde{q} - a_\infty q)| \leq m a_\infty^{1/2} \sqrt{2|A|}. \tag{2.29}$$

We plug in this upper bound in the inequality (2.28), and obtain

$$|F(\xi)| \geq m^2 a_\infty - 2|\xi| m a_\infty^{1/2} \sqrt{2|A|}.$$

Since $|F(\xi)| \leq |\xi|^2 |A|$, we deduce that

$$|\xi|^2 \geq \frac{m^2 a_\infty}{|A|} - \frac{2\sqrt{2}|\xi| m a_\infty^{1/2}}{\sqrt{|A|}}. \tag{2.30}$$

From the above inequality, it is easy to check that

$$|\xi| > \frac{ma_\infty^{1/2}}{4\sqrt{|A|}}.$$

Since $\sqrt{N} = a_\infty |F(q)|^{1/2}$, there exists a constant c_2 depending on A such that

$$\frac{|\xi|}{\sqrt{N}} \geq c_2 \frac{m}{a_\infty^{1/2}|F(q)|^{1/2}}.$$

We deduce that we don't have any integral point inside the following global ball

$$B' := B(\frac{\tilde{q}}{\sqrt{N}}, \frac{|\xi|}{\sqrt{N}}) \prod_p B(a_p q, p^{-\mathrm{ord}_p(m)}). \tag{2.31}$$

We also note that

$$\begin{aligned} |B'| &= \frac{|\xi|}{\sqrt{N}} m^{-1} \\ &\geq c_2 a_\infty^{-1/2} |F(q)|^{-1/2} \\ &\geq c_2 N^{-1/4} |F(q)|^{-1/4} \\ &\geq \frac{c_2 N^{-1/4}}{|A|\sqrt{|q|}}. \end{aligned} \tag{2.32}$$

Therefore, we conclude the second part of our main theorem 2.1.10.□

2.3 The delta method

In this section, we give a formula for the weighted number of the integral points in a small neighborhood of a point b on the quadric $F(X) = N$. We use a smooth weight function w which is supported in a neighborhood of the point b with radius $r\sqrt{N}$. We also impose some congruence conditions mod m on the integral points. We use the additive character $e(\frac{2\pi i x}{m})$ to cut these congruence conditions. We begin with the following expansion of the delta function which is developed by Duke, Friedlander and Iwaniec. We cite this theorem from [HB96, Theorem 1 Page 3].

Theorem 2.3.1 *For any integer n let*

$$\delta_n = \begin{cases} 1 \text{ if } n = 0, \\ 0 \text{ otherwise.} \end{cases} \tag{2.33}$$

Then for any $Q > 1$ there is a positive constant C_Q, and an infinitely differentiable function $h(x, y)$ defined on the set $(0, \infty) \times \mathbb{R}$, such that

$$\delta_n = C_Q Q^{-2} \sum_{q=1}^{\infty} \sum_{a \in \left(\mathbb{Z}/q\mathbb{Z}\right)^*} e(\frac{an}{q}) h(\frac{q}{Q}, \frac{n}{Q^2}). \tag{2.34}$$

The constant C_Q satisfies

$$C_Q = 1 + O_N(Q^{-N}) \tag{2.35}$$

for any $N > 0$. Moreover $h(x, y) \ll x^{-1}$ for all y, and $h(x, y)$ is non-zero only for $x \leq \max(1, 2|y|)$.

We assume that $F(X) = X^T AX$ is a non-degenerate quadratic form and we impose the following congruence conditions mod m on the integral points $X = (x_1, \ldots, x_d)$ such that $F(X) = N$:

$$x_i \equiv \lambda_i \bmod m. \tag{2.36}$$

We let

$$x_i = t_i m + \lambda_i,$$

where $-\frac{m-1}{2} \leq \lambda_i \leq \frac{m-1}{2}$. Then,

$$F\big(t_1 m + \lambda_1, \ldots, t_d m + \lambda_d\big) = N,$$

$$m^2 F(t_1, \ldots, t_d) + 2m\lambda^T At = N - F(\lambda).$$

We define $km := N - F(\lambda)$. Then,

$$F(t_1, \ldots, t_d) + \frac{1}{m}(2\lambda^T At - k) = 0 \tag{2.37}$$

We also define

$$G(t_1, \ldots, t_d) := F(t_1, \ldots, t_d) + \frac{1}{m}(2\lambda^T At - k) = \frac{F(mt + \lambda) - N}{m^2}.$$

We let w be a smooth compactly supported weight function such that

$$w(x) = 0 \text{ if } |x - b| \geq r\sqrt{N}.$$

We write $N(a,w)$ for the weighted number of the integral points on the quadric $F(X)=N$ subjected to the the congruence condition (2.36). We have the following formal expansion for $N(a,w)$

$$N(a,w)=\sum_{t\in\mathbb{Z}^d}\omega(t)\delta_{(G(t))}. \tag{2.38}$$

$$N(a,w)=\frac{1}{m}\sum_{l \bmod m}\sum_{t\in\mathbb{Z}^d} e\big(\frac{l}{m}(2\lambda^T At-k)\big)w(t)\delta(G(t_1,\dots,t_d)) \tag{2.39}$$

Remark 2.3.2 *Note that the summation on l mod m is non-zero only if*

$$2\lambda^T At-k\equiv 0 \ mod\ m.$$

Hence, if $G(t_1,\dots,t_d)$ has non-integral values then this summation is zero. For the integral values of $G(t)$, we use the delta expansion (2.34) to cut out the non-zero integral values of $G(t)$.

From the assumption of the theorem 4.1.4, we have $N=(mr^{-1})^{4+2\delta}$ for some $\delta>0$. We take $Q=(mr^{-1})^{1+\delta}$ in the delta expansion (2.34). Therefore, from Remark 4.13, we have the following expression for $N(a,w)$

$$\begin{aligned} N(a,w)=\frac{C_Q}{mQ^2}\sum_l\sum_q\sideset{}{^*}\sum_a\sum_t e\Big(\frac{(lq+a)(2\lambda^T At-k)+amF(t)}{mq}\Big)\\ h(\frac{q}{Q},\frac{F(mt+\lambda)-N}{m^2Q^2})w(t)\end{aligned} \tag{2.40}$$

We apply the Poisson summation formula on the t variable to obtain

$$N(a,w)=\frac{C_Q}{mQ^2}\sum_l\sum_q\sideset{}{^*}\sum_a\sum_c (mq)^{-d}S_{mq}(a,l,c)I_{mq}(c), \tag{2.41}$$

where

$$I_{mq}(c)=\int h(\frac{q}{Q},\frac{F(t_1,\dots,t_d)-N}{m^2Q^2})w(t)e\big(-\frac{\langle c,t\rangle}{mq}\big)dt_1\dots dt_d, \tag{2.42}$$

$$S_{mq}(a,l,c)=\sum_{b\in\frac{\mathbb{Z}}{mq\mathbb{Z}}^d} e\Big(\frac{(lq+a)(2\lambda^T At-k)+amF(b)+\langle c,b\rangle}{mq}\Big). \tag{2.43}$$

We define the sum $S_{mq}(c)$, as :

$$S_{mq}(c) := \sum_{l \bmod m} \sideset{}{^*}\sum_{a \bmod q} S_{mq}(a, l; c). \tag{2.44}$$

From the assumption, $Q = (r^{-1}m)^{1+\delta}$. In the next section we prescribe a smooth compactly supported function w such that if $w(t) \neq 0$ then

$$\frac{F(X) - N}{m^2 Q^2} = \frac{G(t_1, \ldots, t_d)}{Q^2} \ll 1. \tag{2.45}$$

Since the support of the smooth function $h(x, y)$ is inside the interval $0 \leq x \leq \max(2y, 1)$. Hence, the summation on q is restricted to $1 \leq q \ll Q$.

2.3.1 The properties of the function $h(x, y)$

In this section we cite the basic properties of the smooth function $h(x, y)$ from [HB96]. The following lemma shows $h(x, y)$ converges to the delta function rapidly as $x \to 0$. For the proof we refer the reader to [HB96, Lemma 9].

Lemma 2.3.3 *Let f be a smooth function with compact support. Then if $x \ll 1$ we have*

$$\int f(y)h(x, y)dy = f(0) + O_M(x^M). \tag{2.46}$$

The following lemma shows the smooth property of the $h(x, y)$ in the y variable. Since, it converges to the delta function from the previous lemma, as $x \to 0$ the decay rate of the Fourier transform is slower as $x \to 0$. For the proof, we refer the reader to [HB96, Lemma 17]

Lemma 2.3.4 *Let ω be a smooth compactly supported weight function and $p(t)$ be the Fourier transform of $\omega(y)h(x, y)$, i.e.,*

$$p(t) = \int_{-\infty}^{\infty} \omega(y)h(r, y)e(-ty)dy. \tag{2.47}$$

Then, $p(t)$ decays faster than any polynomial in variable rt, i.e. for every $N \geq 0$

$$p(t) \ll_{\omega, N} (xt)^{-N}. \tag{2.48}$$

2.4 Quadratic exponential sums $S_{mq}(c)$

In this section, we give upper bounds for the quadratic exponential sums $S_{mq}(c)$. We show that this exponential sum is nonzero for certain congruence class c mod m. By Chinese remainder theorem, we write the sum $S_{mq}(c)$ as a product of two summation:

$$S_{mq}(c) = S_1 S_2$$

In Lemma 4.3.1, we give an upper bound on S_1 from the generalized Kloostermann's sum (Salie's sum) for even (odd) dimension . In Lemma 2.4.3, by applying a Cauchy inequality and next computing the square norm, we obtain an upper bound on S_2. Finally, we show in Lemma 2.4.4 that we have square root cancellation on average for the exponential sum $S_{mq}(c)$.

In the following lemma we show that $S_{mq}(a, l; c) = 0$ unless $c_i \equiv -2(lq + a)\lambda_i \bmod m$ for every $1 \leq i \leq d$.

Lemma 2.4.1 *We let $F(X) = X^T AX$ be a non degenerate quadratic form and*

$$S_{mq}(a, l; c) = \sum_{b \in \frac{\mathbb{Z}}{mq\mathbb{Z}}^d} e\Big(\frac{(lq + a)(2\lambda^T Ab - k) + amF(b) + \langle c, b\rangle}{mq}\Big).$$

Then

$$S_{mq}(a, l; c) = 0,$$

unless $c \equiv -2(lq + a)A\lambda \bmod m$. As a result $S_{mq}(c) = 0$, unless

$$c \equiv \alpha A\lambda \text{ for some scalar } \alpha \bmod m.$$

where $\lambda = (\lambda_1, \ldots, \lambda_d) \bmod m$.

Proof: We write vector b in the summation as

$$b = qb_1 + b_2,$$

where b_1 is a vector mod m and b_2 is a vector mod q. Then we write $S_{mq}(a, l; c)$ as a summation

over b_1 and b_2. We obtain

$$S_{mq}(a,l;c)=\sum_{b_2} e\Big(\frac{(lq+a)(2\lambda^T Ab_2-k)+amF(b_2)+\langle c,b_2\rangle}{mq}\Big)\sum_{b_1} e\Big(\frac{(lq+a)2\lambda^T Ab_1+\langle c,b_1\rangle}{m}\Big). \tag{2.49}$$

It is easy to check that the summation on b_1 is zero unless

$$c\equiv -2(lq+a)A\lambda \bmod m.$$

Since

$$S_{mq}(c):=\sum_{l \bmod m}\ \sideset{}{^*}\sum_{a \bmod q} S_{mq}(a,l;c),$$

if $S_{mq}(c)\neq 0$, then for some $a \bmod q$ and $l \bmod m$, $S_{mq}(a,l;c)\neq 0$. Therefore,

$$c\equiv -2(lq+a)A\lambda \bmod m.$$

Hence, we conclude the lemma $\square$.

In the rest of this section, we give an upper bound for $S_{mq}(c)$ when this summation is nonzero. We let

$$\Delta:=\det A$$

where A is the symmetric matrix corresponded to our non-degenerate quadratic form $F(X)=X^TAX$. We note that

$$S_{mq}(c)=\sum_{l \bmod m}\ \sideset{}{^*}\sum_{a \bmod q} S_{mq}(a,l;c),$$

since the summation over l is nonzero only if $m|2\lambda^T Ab-k$ and it is m when $m|2\lambda^T Ab-k$, then we have

$$S_{mq}(c)=m\sum_{b,a} e\Big(\frac{a(2\lambda^T Ab-k)+amF(b)+\langle c,b\rangle}{mq}\Big). \tag{2.50}$$

where the summation is over $a\in\big(\frac{\mathbb{Z}}{q\mathbb{Z}}\big)^*$ and vectors $b\in\big(\frac{\mathbb{Z}}{mq\mathbb{Z}}\big)^d$ such that

$$m|2\lambda^T Ab-k.$$

We assume that

$$q=q_1q_2,$$

where $\gcd(q_1, 2\Delta m) = 1$ and the set of primes which divide q_2 is a subset of primes in Δm. As a result $\gcd(q_1, mq_2) = 1$. Therefore, we can write $k = mq_2k_1 + q_1k_2$ for some integers k_1 and k_2, and also from the Chinese remainder theorem we obtain

$$b = mq_2b_1 + q_1b_2, \tag{2.51}$$

where $b_1 \in \left(\frac{\mathbb{Z}}{q_1\mathbb{Z}}\right)^d$ and moreover $b_2 \in \left(\frac{\mathbb{Z}}{mq_2\mathbb{Z}}\right)^d$ and $m|2\lambda^T Ab - k$. We can also write

$$a = q_2a_1 + q_1a_2, \tag{2.52}$$

where $a_1 \in \left(\frac{\mathbb{Z}}{q_1\mathbb{Z}}\right)^*$ and $a_2 \in \left(\frac{\mathbb{Z}}{q_2\mathbb{Z}}\right)^*$. We substitute these values of $k = mq_2k_1 + q_1k_2$, $a = q_2a_1 + q_1a_2$ and $b = mq_2b_1 + q_1b_2$ in the formula (2.50) for $S_{mq}(c)$ to obtain

$$\begin{aligned} S_{mq}(c) = &\sum_{a_1,b_1} e\Big(\frac{2q_2a_1\lambda^T Ab_1 + a_1(mq_2)^2F(b_1) + \langle c, b_1\rangle + q_2a_1k_1}{q_1}\Big) \\ &\times m\sum_{a_2,b_2} e\Big(\frac{2q_1a_2\lambda^T Ab_2 + a_2mq_1^2F(b_2) + \langle c, b_2\rangle + q_1a_2k_2}{mq_2}\Big), \end{aligned} \tag{2.53}$$

where $m|2\lambda^T Ab_2 - k_2$. We define

$$S_1 := \sum_{a_1,b_1} e\Big(\frac{2q_2a_1\lambda^T Ab_1 + a_1(mq_2)^2F(b_1) + \langle c, b_1\rangle + q_2a_1k_1}{q_1}\Big), \tag{2.54}$$

and

$$S_2 := m\sum_{a_2,b_2} e\Big(\frac{2q_1a_2\lambda^T Ab_2 + a_2mq_1^2F(b_2) + \langle c, b_2\rangle + q_1a_2k_2}{mq_2}\Big), \tag{2.55}$$

where $m|2\lambda^T Ab_2 - k_2$. In the following lemma we give upper bounds for S_1.

Lemma 2.4.2 *Let $F(X) := X^TAX$ be a quadratic form such that $\Delta := \det(A) \neq 0$. Assume that q is an odd integer such that $\gcd(q, 2\Delta) = 1$ and let*

$$S(F, c, c', k) := \sum_{a,b} e\Big(\frac{a[F(b) + \langle c', b\rangle + k] + \langle c, b\rangle}{q}\Big), \tag{2.56}$$

where a varies in units $\left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^*$ and b varies in $\left(\frac{\mathbb{Z}}{q\mathbb{Z}}\right)^d$. Then

$$S = \Big(\frac{\Delta}{q}\Big)\tau_q^d Kl(F, c, c', k) \tag{2.57}$$

where $\tau_q := \sum_x e\big(\frac{x^2}{q}\big)$ *is the Gauss sum,* $\Big(\frac{\cdot}{\cdot}\Big)$ *is the Legendre symbol and* $Kl(F, c, c', k)$ *is either a Kloosterman's sum or a Salie's sum. Therefore we have the following upper bound on* $S(F, c, c', k)$

$$S(F, c, c', k) \leq q^{\frac{d+1}{2}} \tau(q) \gcd(q, N)^{1/2}. \tag{2.58}$$

Proof: Since q is odd, we can diagonalize our quadratic form $F(x)$ mod q. Therefore, without loss of generality we assume that our quadratic form is a diagonal quadratic form

$$F(x) = \sum_{i=1}^{d} \alpha_i x_i^2$$

Hence,

$$S(F, c, c', k) := \sum_a \prod_{j=1}^{d} \sum_b e\Big(\frac{a[\alpha_j b^2 + c_j' b + k] + c_j b}{q}\Big).$$

We complete the square to obtain

$$S(F, c, c', k) := \sum_a \prod_{j=1}^{d} \sum_b e\Big(\frac{a\alpha_j\big(b + \frac{ac_j' + c_j}{2a\alpha_j}\big)^2 + ak - \frac{(ac_j' + c_j)^2}{4a\alpha_j}}{q}\Big)$$

$$= \tau_q^d\Big(\frac{\Delta}{q}\Big) e\big(\frac{\sum_j \frac{c_j c_j'}{\alpha_j}}{2q}\big) \sum_a \Big(\frac{a}{q}\Big)^d e\big(\frac{a(dk + \sum_j \frac{c_j'^2}{4\alpha_j}) + a^{-1}\sum_j (\frac{c_j^2}{\alpha_j})}{q}\big)$$

Note that for odd d we get the Salie's sum and for even d we have Kloosterman's sum. Therefore, we conclude the lemma.□

In this lemma we give an upper bound on S_2.

Lemma 2.4.3 *Let*

$$S_2 := m \sum_{a_2, b_2} e\Big(\frac{2q_1 a_2 \lambda^T A b_2 + a_2 m q_1^2 F(b_2) + \langle c, b_2\rangle + q_1 a_2 k_2}{m q_2}\Big) \tag{2.59}$$

where $m | 2\lambda^T A b_2 - k_2$. *Then,*

$$S_2 \ll_\Delta m^d q_2^{1+d/2}. \tag{2.60}$$

Proof: From the Cauchy inequality on a_2 variable we have

$$|S_2|^2 \leq m^2 \phi(q_2) \sum_{a_2} \Big| \sum_{b_2} e\Big(\frac{2q_1 a_2 \lambda^T A b_2 + a_2 m q_1^2 F(b_2) + \langle c, b_2\rangle + q_1 a_2 k_2}{m q_2}\Big)\Big|^2$$

$$\leq m^2\phi(q_2)^2\sum_{b_2,b_2'} e\Big(\frac{2q_1a_2\lambda^T A(b_2-b_2')+a_2mq_1^2(F(b_2)-F(b_2'))+\langle c,b_2-b_2'\rangle}{mq_2}\Big),$$

where $m|2\lambda^T Ab_2-k_2$ and $m|2\lambda^T Ab_2'-k_2$. We change the variables and write $u=b_2-b_2'$. Hence,

$$|S_2|^2\leq m^2\phi(q_2)^2\sum_{u,b_2} e\Big(\frac{2q_1a_2\lambda^T Au+a_2mq_1^2(2b_2Au+F(u))+\langle c,u\rangle}{mq_2}\Big).$$

where $m|2\lambda^T Ab_2-k_2$ and $m|2\lambda^T Au$. The summation over b_2 is unless $q_2|\Delta\gcd(u)$. Therefore,

$$|S_2|^2\ll_\Delta \phi(q_2)^2(m^2q_2)^d.$$

Hence,

$$|S_2|\ll_\Delta m^d q_2^{1+\frac{d}{2}}.$$

Therefore we conclude the lemma□.

In the last lemma of this section we prove an average result on the norm of the exponential sums $S_{qm}(c)$ with respect to q.

Lemma 2.4.4 *We have the following upper bound*

$$\sum_{q=1}^{X} m^{-d}q^{-\frac{d+1}{2}}|S_{qm}(c)|\ll_\Delta m^\epsilon X^{1+\epsilon}. \tag{2.61}$$

Proof: This is an easy consequence of Lemma 4.3.1 and Lemma 2.4.3. We factor

$$q=q_1q_2,$$

where $\gcd(q_1,2m\Delta)=1$ and prime factors of q_2 are subset of prime factors of $m\Delta$. From the formula (2.53), we deduce that

$$S_{mq}(c)|=|S_1||S_2|.$$

One can easily check that Lemma 4.3.1 implies

$$S_1\leq q_1^{\frac{d+1}{2}+\epsilon}.$$

Lemma 2.4.3 implies that

$$S_2\ll_\Delta m^d q_2^{1+d/2}.$$

Therefore, we have

$$\sum_{q=1}^{X} m^{-d} q^{-\frac{d+1}{2}} |S_{qm}(c)| \ll \sum_{q=1}^{X} q_1^{\epsilon} q_2^{1/2} \leq X^{\epsilon} \sum_{q=1}^{X} q_2^{1/2}.$$

Note that the prime factors of q_2 are subsets of prime factors of $m\Delta$, hence

$$\sum_{q=1}^{X} q_2^{1/2} \leq X^{1+\epsilon} m^{\epsilon}.$$

Therefore, we conclude the lemma.

2.5 The integral $I_{mq}(c)$

In this section we give upper bounds on the integral $I_{mq}(c)$ that appears in the expansion (2.42). We partition the integral vectors $c \neq 0 \in \mathbb{Z}^d$ into two sets. We call them by ordinary and exceptional vectors. In section 2.5.1, we give an upper bound on $I_{mq}(c)$ where c is an ordinary vector. We give a different upper bound on $I_{mq}(c)$ for the exceptional vectors in section 2.5.2. The definition of the ordinary and exceptional vectors is based on a choice of a point $b \in \mathbb{Z}^d$ where $F(b) = N$ and b is in the support of w.

Fix a point $b \in \mathbb{Z}^d$ such that $F(b) = N$ and $\omega(b) \neq 0$. In order to simplify the integral $I_{mq}(c)$. We change our standard basis to a new basis given by an orthonormal basis of the $d-1$ dimensional tangent space at b on the hyper-surface $F(x) = N$ and the normal vector at b.

We assume that $F(X)$ is a non-degenerate quadratic form with symmetric matrix A

$$F(x_1, \ldots, x_d) = X^T A X.$$

We assume that the smooth weight function w is compactly supported inside an open set given by fattening of the tangent space of the hyper-surface $F(X) = N$ at b. We give a precise description of the weight function $w(x)$ in what follows . The gradient of $F(x_1, \ldots, x_d) = X^T A X$ at point b is given by

$$\nabla F_{|b} = 2Ab. \tag{2.62}$$

We let e_d be the norm 1 vector in the direction of $\nabla F_{|b}$. The tangent space of the level set $F(X) = N$ at b is the orthogonal complement of e_d and we denote it by

$$T_b(F) := e_d^{\perp}$$

We restrict the quadratic from $F(X)$ to the $d-1$ dimensional subspace $T_b(F)$. By a standard theorem in linear algebra we can find an orthogonal basis $B := \{e_1, \ldots, e_{d-1}\}$ for $T_b(F)$ such that F is diagonal in this basis. Namely,

$$F\big(\sum_{i=1}^{d-1} u_i e_i\big) = \sum_{i=1}^{d-1} \lambda_i u_i^2 \tag{2.63}$$

We write the integral vectors c in the orthonormal basis

$$B_1 := \{e_1, \ldots, e_{d-1}, e_d\}. \tag{2.64}$$

We remark that c does not necessarily have integral coordinates anymore.

$$c = \sum_{i=1}^{d} c_i e_i \tag{2.65}$$

We define two types of the ordinary vectors. We call them ordinary of type I and type II. Type I ordinary vectors c are the integral vectors c such that their norm are large, more precisely

$$|c| \geq (mr^{-1})^{1+\epsilon}, \tag{2.66}$$

where $|.| = \max_i c_i$, and $\epsilon > 0$ is any positive number which is independent of δ. The type II vectors c are the integral vectors c such that there exist $1 \leq i \leq d-1$ where

$$\begin{aligned} c_i &\gg m(mr^{-1})^{\epsilon}. \\ |c| &< (mr^{-1})^{1+\epsilon}, \end{aligned} \tag{2.67}$$

We call the complement of these integral vectors the exceptional integral vectors.

We give a change of variable formula for the integral $I_{mq}(c)$ where we use in the subsequent subsections. Recall that

$$I_{mq}(c) = \int h(\frac{q}{Q}, \frac{F(mt+a)-N}{m^2Q^2}) w(t) e\big(-\frac{\langle c, t\rangle}{mq}\big) dt_1 \ldots . dt_d, \tag{2.68}$$

Since $F(b) = b^T A b = N \neq 0$, then $B_2 := \{e_1, \ldots, e_{d-1}, b\}$ is also a basis and we express the

vector $X - b$ in two basises B_1 and B_2 as follows:

$$X - b = \sum_{i=1}^{d-1} m u_i e_i + m\alpha e_d, \tag{2.69}$$

$$X - b = \sum_{i=1}^{d-1} m \tilde{u_i} e_i + m\beta b, \tag{2.70}$$

where if $b = \sum_{i=1}^{d} b_i e_i$ then

$$u_i = \tilde{u_i} + \beta b_i, \tag{2.71}$$

$$\alpha = \beta b_d. \tag{2.72}$$

We choose ω so that if $\omega(X) \neq 0$ then u_i are bounded by Q. Since $\{e_1, \ldots, e_d\}$ is an orthonormal basis then

$$dX = m^d du_1 \ldots du_{d-1} d\alpha.$$

Let $y := \frac{F(X)-N}{m^2Q^2}$, hence $\frac{\partial y}{\partial \alpha} = \frac{X^T A e_d}{mQ^2}$

$$du_1 \ldots du_{d-1} d\alpha = \frac{\partial y}{\partial \alpha}^{-1} du_1 \ldots du_{d-1} dy, \tag{2.73}$$

$$= \frac{mQ^2}{X^T A e_d} du_1 \ldots du_{d-1} dy. \tag{2.74}$$

Recall that $X = mt + a$, hence

$$dX = m^d dt.$$

Therefore,

$$dt = \frac{mQ^2}{X^T A e_d} du_1 \ldots du_{d-1} dy. \tag{2.75}$$

We substitute $b = mt_0 + a$ and also $dt_1 \ldots dt_d = \frac{mQ^2}{X^T A e_d} du_1 \ldots du_{d-1} dy$, hence

$$I_{mq}(c) = \int h(\frac{q}{Q}, \frac{F(mt+a)-N}{m^2Q^2}) w(t) e\big(-\frac{\langle c, t\rangle}{mq}\big) dt_1 \ldots . dt_d$$

$$= e\big(\frac{\langle c, t_0\rangle}{mq}\big) \frac{mQ^2}{R} \int \frac{R}{X^T A e_d} h(\frac{q}{Q}, y) w(t) e\big(\frac{\sum_{i=1}^{d} c_i u_i + \alpha c_d}{mq}\big) du_1 \ldots du_{d-1} dy. \tag{2.76}$$

2.5.1 Upper bound on the integral $I_{mq}(c)$ for ordinary vectors

In this section we prove a decay rate for $I_{mq}(c)$ when c is an ordinary vector. These are the integral vectors such that $I_{mq}(c)$ decays fast as $c \to \infty$. In the following lemma, we give an upper bound for the integral $I_{mq}(c)$, when c is an ordinary vector. Moreover, we show that their contribution in the delta method is bounded.

Lemma 2.5.1 *Let c be an ordinary type vector. Then for any $N > 0$, we have the following upper bounds on $I_{mq}(c)$ if c is an ordinary type I vector:*

$$I_{mq}(c) \ll_N \Big(|c| r^{-1} m\Big)^{-N}, \tag{2.77}$$

and if c is an ordinary type II vector we have

$$I_{mq}(c) \ll_N \Big(r^{-1} m\Big)^{-N}. \tag{2.78}$$

As a corollary, we show that their contribution is bounded in the delta method, namely

$$\frac{C_Q}{mQ^2} \sum_q \sum_c (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll_\epsilon 1. \tag{2.79}$$

Proof: Recall that

$$I_{mq}(c) = \int h(\frac{q}{Q}, \frac{F(mt+a)-N}{m^2Q^2}) w(t) e\big(-\frac{\langle c,t\rangle}{mq}\big) dt_1 \ldots . dt_d. \tag{2.80}$$

Without lost of generality, we assume that the weight function w is a product of two compactly supported weight function as follows:

$$w(t) = w_0(t) w_1(y), \tag{2.81}$$

where $y = \frac{F(mt+a)-N}{m^2Q^2}$. We let $p_{q/Q}(\xi)$ be the Fourier transform of $h(\frac{q}{Q}, x) w_1(x)$, i.e.,

$$p_{q/Q}(\xi) = \int_{-\infty}^{\infty} w_1(x) h(q/, x) e(-\xi x) dx. \tag{2.82}$$

Therefore,

$$I_{mq}(c) = \int_\xi p_{q/Q}(\xi) \int_t w_0(t) e\big(\xi y - \frac{\langle t,c\rangle}{mq}\big) dt. \tag{2.83}$$

Recall that $X = mt + a$.

$$X - b = \sum_{i=1}^{d-1} m u_i e_i + m\alpha e_d, \tag{2.84}$$

$$X - b = \sum_{i=1}^{d-1} m \tilde{u_i} e_i + m\beta b, \tag{2.85}$$

where if $b = \sum_{i=1}^{d} b_i e_i$ then

$$u_i = \tilde{u_i} + \beta b_i, \tag{2.86}$$

$$\alpha = \beta b_d. \tag{2.87}$$

We also have the following formula for the volume form

$$dt = \langle b, e_d \rangle \, d\tilde{u_i} d\beta$$

We express y in terms of $\tilde{u_i}$ and β

$$\begin{aligned} y &= \frac{F(X) - N}{m^2 Q^2} \\ &= \frac{\big(\sum m\tilde{u_i} e_i + (1 + m\beta)b\big)^T A\big(\sum m\tilde{u_i} e_i + (1 + m\beta)b\big) - N}{m^2 Q^2} \\ &= \frac{\sum_1^{d-1} \tilde{u_i}^2 m^2 \lambda_i + (1 + m\beta)^2 N - N}{m^2 Q^2}. \end{aligned} \tag{2.88}$$

Using the above expression for y, and also the following expansion for the inner product

$$\langle t, c \rangle = \langle t_0, c \rangle + \sum_{i=1}^{d} c_i u_i,$$

where $b = mt_0 + a$. We obtain

$$\begin{aligned} I_{mq}(c) = e\big(\frac{\langle c, t_0 \rangle}{mq}\big) \langle b, e_d \rangle \int_{\xi} p_{q/Q}(\xi) \\ \int_{\beta, \tilde{u}} w_0(\tilde{u_1}, \ldots, \tilde{u}_{d-1}, \beta) e\big(\frac{\xi\beta(2/m + \beta)N}{Q^2} + \frac{\beta \langle b, c \rangle}{mq}\big) \\ \times e\big(\sum_{i=1}^{d-1} [\frac{\xi \lambda_i \tilde{u_i}^2}{Q^2} + \frac{c_i \tilde{u_i}}{mq}]\big) d\beta d\tilde{u}_d \xi \end{aligned} \tag{2.89}$$

Since we are only concerned about the norm $|I_{mq}(c)|$, so we drop $e\big(\frac{\langle c, t_0 \rangle}{mq}\big)$. From the assumptions, we needed y to be bounded, so this restricts the range of $\tilde{u_i}$ and β . Hence, we let $\tilde{u_i}$ vary between

$-Q \leq \tilde{u_i} \leq Q$ and $-mQ^2/N \leq \beta \leq mQ^2/N$. We normalize the variables and write

$$x_i = \tilde{u_i}/Q, \tag{2.90}$$

$$x_d = \beta N/mQ^2. \tag{2.91}$$

The range of each integral is on the interval $[-1, 1]$ now. Therefore,

$$\begin{aligned} |I_{mq}(c)| = \frac{Q^{d+1}m\,\langle b, e_d\rangle}{N}\Big| \int_{\xi} p_{q/Q}(\xi) \\ \int_{-1}^{1}\dots\int_{-1}^{1} w_0(x) e\Big(x_d(2\xi + \frac{Q^2\,\langle b, c\rangle}{qN}) + \frac{\xi x_d^2 m^2 Q^2}{N}\Big) \\ e\big(\sum_{i=1}^{d-1}[\xi\lambda_i x_i^2 + \frac{c_i Q x_i}{mq}]\big) dx_1 \dots dx_d d\xi\Big|. \end{aligned} \tag{2.92}$$

At this point, we assume that c is an ordinary vector of type II, i.e., there exist $1 \leq i \leq d-1$ such that

$$c_i \gg m(mr^{-1})^{\epsilon}.$$

We split the integral $I_{mq}(c)$ as a sum of two.

$$I_{mq}(c) = I_{mq}(c)_1 + I_{mq}(c)_2,$$

where $I_{mq}(c)_1$ is the integral over ξ where $|\xi| < (r^{-1}m)^{\epsilon/2}\frac{Q}{q}$ and $I_{mq}(c)_2$ is the integral over the complement when $|\xi| > (r^{-1}m)^{\epsilon/2}\frac{Q}{q}$. First, we show that

$$|I_{mq}(c)_2| \ll (r^{-1}m)^{-N}. \tag{2.93}$$

This is a consequence of the Lemma 2.3.4. Recall that

$$p_{q/Q}(\xi) \ll (|\xi|q/Q)^{-N}.$$

Since $|\xi| > (r^{-1}m)^{\epsilon/2}\frac{Q}{q}$, we deduce the claimed upper bound on $|I_{qm}(c)_2|$. It remains to show that

$$|I_{mq}(c)_1| \ll (r^{-1}m)^{-N}.$$

Then by Fubini's theorem, we change the order of integration, and first take integration on the x_i

variable

$$
\begin{aligned}
|I_{mq}(c)| = \frac{Q^{d+1} m \langle b, e_d \rangle}{N} \Big| \int_{\xi} p_{q/Q}(\xi) \\
\int_{-1}^{1} \dots \int_{-1}^{1} w_0(x) e\Big(x_d (2\xi + \frac{Q^2 \langle b, c \rangle}{qN}) + \frac{\xi x_d^2 m^2 Q^2}{N} \Big) \\
e\big(\sum_{i=1}^{d-1} [\xi \lambda_i x_i^2 + \frac{c_i Q x_i}{mq}] \big) dx_1 \dots \hat{dx_i} \dots dx_d d\xi \\
\int_{-1}^{1} w_0(x_0, \dots, x_i, \dots, x_d) e\big(\xi \lambda_i x_i^2 + \frac{c_i Q x_i}{mq} \big) dx_i \Big|
\end{aligned}
\tag{2.94}
$$

Note that since $|\xi| < (r^{-1}m)^{\epsilon/2} \frac{Q}{q}$ and $c_i \gg m(mr^{-1})^{\epsilon}$ we deduce that following lower bound on the derivative of the oscillatory in the x_i variable

$$
\begin{aligned}
\frac{\partial(\xi \lambda_i x_i^2 + \frac{c_i Q x_i}{mq})}{\partial x_i} &\gg \frac{c_i Q x_i}{mq} \\
&\gg \frac{(mr^{-1})^{\epsilon} Q}{q} \\
&\gg (mr^{-1})^{\epsilon}.
\end{aligned}
\tag{2.95}
$$

By integrating by part multiple times in the x_i variable we have a fast decay for $I_{qm}(c)_1$. Because

$$
\int_{x_i} w(x_i) e\big(\xi \lambda_i x_i^2 + \frac{c_i Q x_i}{mq} \big) dx_i \ll_N (mr^{-1})^{-N\epsilon}, \tag{2.96}
$$

for every $N > 0$. Hence, if c is a type II vector, we proved the claimed upper bound on $I_{qm}(c)_1$ and therefore on $I_{qm}(c)$. In order to show that the contribution of the type II vectors is bounded in the delta method, namely

$$
\frac{C_Q}{mQ^2} \sum_{q=1}^{Q} \sum_{c} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll_{\epsilon} 1. \tag{2.97}
$$

Note that $Q = (r^{-1}m)$ and since $|c| \leq (r^{-1}m)^{1+\epsilon}$ the number of type II vectors is bounded by $(r^{-1}m)^{d(1+\epsilon)}$. Therefore if we choose $N > \epsilon^{-1} 2d$. We conclude the lemma for type II vectors.

It remain to prove the lemma for type I vectors c. We proceed as before and split the integral $I_{mq}(c)$ as a sum of two.

$$
I_{mq}(c) = I_{mq}(c)_1 + I_{mq}(c)_2,
$$

But this time, $I_{mq}(c)_1$ is the integral over ξ where $|\xi| < (|c| r^{-1}m)^{\epsilon/2} \frac{Q}{q}$ and $I_{mq}(c)_2$ is the integral

over $|\xi| > (|c|r^{-1}m)^{\epsilon/2}\frac{Q}{q}$. From the same line as in (2.93), we deduce

$$|I_{mq}(c)_2| \ll (|c|r^{-1}m)^{-N}. \tag{2.98}$$

It remains to prove $I_{mq}(c)_1 \leq (|c|mr^{-1})^{-N}$ for the type I vectors c. If $|c_d| \neq \max_i |c_i|$, we proceed as before. So, we assume the harder case where $c_d = |c|$, because our lower bound for the partial derivative in x_d variable is worse than other variables. We proceed the same strategy and use the Fubuni's theorem. We first take integration along the x_d variable and we give a lower bound for the partial derivative of the oscillatory function in x_d variable.

$$\frac{\partial(x_d(2\xi + \frac{Q^2\langle b,c\rangle}{qN}) + \frac{\xi x_d^2 m^2 Q^2}{N})}{\partial x_i} \gg \frac{Q^2\langle b,c\rangle}{qN} - |2\xi| - |\frac{2\xi m^2 Q^2}{N}|. \tag{2.99}$$

Recall that $N = Q^2m^2r^{-2}$, and $|\xi| < (|c|r^{-1}m)^{\epsilon/2}\frac{Q}{q}$, hence

$$\begin{aligned}\frac{\partial(x_d(2\xi + \frac{Q^2\langle b,c\rangle}{qN}) + \frac{\xi x_d^2 m^2 Q^2}{N})}{\partial x_d} &\gg \frac{Q^2\langle b,c\rangle}{qN} \\ &\gg (|c|mr^{-1})^{\epsilon}.\end{aligned} \tag{2.100}$$

By integrating by part multiple times in the x_d variable we deduce

$$I_{mq}(c)_1 \ll_N \Big(|c|r^{-1}m\Big)^{-N}. \tag{2.101}$$

Therefore we concluded the claimed upper bound (2.77) for the type I vectors. In order to prove the lemma it remains to show

$$\frac{C_Q}{mQ^2}\sum_{q=1}^{Q}\sum_{c}(mq)^{-d}S_{mq}(c)I_{mq}(c) \ll_\epsilon 1. \tag{2.102}$$

where the sum is over the ordinary type I vectors. We note that the following sum is bounded over $c \in \mathbb{Z}^d$ and as a result over the type I integral vectors.

$$\sum_{c\in\mathbb{Z}^d}\frac{1}{|c|^{d+1}} \ll 1. \tag{2.103}$$

Hence, by choosing $N > 2d$ in (2.101), we deduce the lemma. $\square$

2.5.2 Upper bound on the integrals $I_{mq}(c)$ for exceptional vectors

In this section we prove an upper bound for $I_{mq}(c)$ when c is an exceptional vector. These are the complement of the ordinary vectors, i.e. the integral vectors c with the following conditions

$$\begin{aligned} |c_i| &< m(mr^{-1})^{\epsilon}, \\ |c| &< (r^{-1}m)^{1+\epsilon}, \end{aligned} \tag{2.104}$$

where we used the basis B_1 defined in (2.64) to express $c = \sum_i c_i e_i$.

Lemma 2.5.2 *Let c be an exceptional integral vector then we have the following upper bound on $I_{mq}(c)$*

$$\frac{|I_{mq}(c)|}{mQ^2} \ll \frac{Q^{d-1}}{R} \min[\Big(\frac{Q|c|}{mr^{-1}q}\Big)^{-\frac{d-1}{2}}, 1]. \tag{2.105}$$

Recall that $R = \sqrt{N} = Qmr^{-1}$ and $Q = (mr^{-1})^{1+\delta}$.

Proof: We recall from the formula (2.76)

$$|I_{mq}(c)| = \frac{mQ^2}{R} \int \frac{R}{X^T A e_d} h(\frac{q}{Q}, y) w(t) e\big(\frac{\sum_{i=1}^{d} c_i u_i + \alpha c_d}{mq}\big) du_1 \dots du_{d-1} dy.$$

We want to separate the variables in the oscillatory function and write α in terms of $u_1, \dots, u_{d-1}$ and y. First, we give the taylor expansion of α in terms of $u_1, \dots u_{d-1}, y$. Recall that

$$y = \frac{F(X) - N}{m^2 Q^2}$$

$$= \frac{\big(\sum m\tilde{u}_i e_i + (1+m\beta)b\big)^T A\big(\sum m\tilde{u}_i e_i + (1+m\beta)b\big) - N}{m^2Q^2}.$$

Hence,

$$m^2Q^2y = \sum_{1}^{d-1} \tilde{u_i}^2 m^2 \lambda_i + (1+m\beta)^2 b^T A b - N.$$

Since $b^T A b = N$, then

$$(1+m\beta)^2 = \frac{N + m^2Q^2y - \sum_{i=1}^{d-1} m^2 \tilde{u_i}^2 \lambda_i}{N}.$$

Therefore,

$$m\beta = \sqrt{1 + \frac{m^2Q^2y}{N} - \sum_{i=1}^{d-1} \frac{m^2 \tilde{u_i}^2}{N} \lambda_i} - 1$$

From the taylor expansion, we obtain

$$m\beta = \sqrt{\frac{m^2Q^2y}{N}+1} - 1 + 1/2\Big[-\sum_{i=1}^{d-1}\frac{m^2\tilde{u_i}^2}{N}\lambda_i\Big] + O(r^{-4}\frac{\tilde{u}_i^2}{Q^2}) \tag{2.106}$$

Since, we are going to use the stationary phase theorem in variables $x_i := \frac{\tilde{u}_i}{Q}$ and outside a small neighborhood of the critical point the integration decay rapidly we can ignore the error term in the Tylor expansion and localize the integral around the critical point with radius of the squre root of the coefficient of x_i^2 . Therefore,

$$\alpha = \frac{b_d}{2}\Big[\frac{mQ^2y}{N} - \sum_{i=1}^{d-1}\frac{m\tilde{u_i}^2}{N}\lambda_i\Big] + O(Rr^{-4}m^{-1}) \tag{2.107}$$

We use the above expansion in the following formula for $|I_{mq}(c)|$

$$|I_{mq}(c)| = \frac{mQ^2}{R}\int \frac{R}{X^TAe_d}h(\frac{q}{Q},y)w(t)e\big(\frac{\sum_{i=1}^d c_iu_i + \alpha c_d}{mq}\big)du_1\dots du_{d-1}dy.$$

We use the Fubini's theorem and first take integration on $x_1,\dots,x_{d-1}$.

$$\begin{aligned}\frac{|I_{mq}(c)|}{mQ^2} = \frac{Q^{d-1}}{R}\prod_{i=1}^{d-1}\int \frac{R}{X^TAe_d}w(x,y)e\Big(\frac{Qxc_i + \langle c,b\rangle m^{-1}r^2\lambda_ix^2/2}{mq}\Big)dx \\ h(\frac{q}{Q},y)e\Big(\frac{\langle c,b\rangle y}{2(mr^{-1})^2q}\Big)dy,\end{aligned} \tag{2.108}$$

From the stationary phase theorem we obtain the following upper bound

$$G(y) := \int \frac{R}{X^TAe_d}w(x,y)e\Big(\frac{Qxc_i + \langle c,b\rangle m^{-1}r^2\lambda_ix^2/2}{mq}\Big)dx \ll \min\Big[\Big(\frac{\langle c,b\rangle m^{-1}r^2}{mq}\Big)^{-\frac{d-1}{2}},1\Big]. \tag{2.109}$$

We note that $|c| = c_d$ and $b_d \approx R$. Therefore,

$$\langle c,b\rangle \approx R|c|.$$

We also recall that $R = mr^{-1}Q$. Therefore after simplifying (2.109), we deduce

$$G(y) \le \min[\Big(\frac{Q|c|}{mr^{-1}q}\Big)^{-\frac{d-1}{2}},1].$$

Therefore,

$$\frac{|I_{mq}(c)|}{mQ^2} = \frac{Q^{d-1}}{R}\int G(y)h(\frac{q}{Q},y)e\Big(\frac{\langle c,b\rangle y}{2(mr^{-1})^2q}\Big)dy. \tag{2.110}$$

Assume that the test function $w(x,y)$ that we are using in equation 2.109 is the product of two test functions, namely

$$w(x,y) = w_1(x_1,\dots,x_{d-1})w_2(y)$$

From Fubini's theorem, we can separate the integral and write $g(y)$ as the product of the integral over y and $(x_1,...x_(d-1))$ coordinates. So we have

$$G(y) = G(0)\int_y w(y)h(q/Q,y)e(Ay)dy$$

Finally, we apply lemma 2.3.4 on $\int_y w(y)h(q/Q,y)e(Ay)dy$ for $N=0$ to obtain

$$\begin{aligned}\frac{|I_{mq}(c)|}{mQ^2} &= \frac{Q^{d-1}}{R}\int G(y)h(\frac{q}{Q},y)e\Big(\frac{\langle c,b\rangle\, y}{2(mr^{-1})^2q}\Big)dy \\ &\ll \frac{Q^{d-1}}{R}G(0). \\ &\ll \frac{Q^{d-1}}{R}\min[\Big(\frac{Q|c|}{mr^{-1}q}\Big)^{-\frac{d-1}{2}},1].\end{aligned} \tag{2.111}$$

Therefore, we conclude the lemma.□

2.5.3 Bounding the sum over the exceptional vectors

In this section we give an upper bound on the contribution of the exceptional integral vectors c in the delta method. First, we show the number of exceptional eigenvalues with a norm less than X is less than $X(r^{-1}m)^\epsilon$. This upper bound on the number of exceptional vectors and the upper bound on the integral $I_{qm}(c)$ allow us to bound the contribution of the exceptional integral vectors in the delta method.

Lemma 2.5.3 *The number of exceptional integral vectors c such that*

$$c \equiv \alpha a \ mod\ m,$$

for $\alpha \in \mathbb{Z}/m\mathbb{Z}$ *and* $a \in \mathbb{Z}/m\mathbb{Z}^d$, *and*

$$|c| \le X,$$

is bounded by $X(r^{-1}m)^\epsilon$.

Proof: The proof is based on the covering of $\mathbb{R}^d$ by boxes of volume m^{d-1} around the integral points with the following congruence condition

$$c \equiv \alpha a \bmod m.$$

From the definition of the exceptional vectors we know that

$$|c_i| < m(mr^{-1})^{\epsilon}. \tag{2.112}$$

Therefore, all the exceptional vectors with $|c| < X$ lies in a box with size

$$X \times m(mr^{-1})^{\epsilon} \times \cdots \times m(mr^{-1})^{\epsilon}$$

Therefore the number of exceptional vectors is less than

$$\frac{Xm^{d-1}(mr^{-1})^{(d-1)\epsilon}}{\text{Volume of the box}} = X(mr^{-1})^{(d-1)\epsilon}.$$

By choosing ϵ small enough in the definition of the exceptional vectors we conclude the lemma. $\square$.

We are ready to give an upper bound on the contribution of the exceptional vectors in the delta method. In order to do that we need two more auxiliary lemmas.

Lemma 2.5.4 *We have the following upper bound on the sum over the exceptional vectors with norm $|c| > Z$ and $1 \leq q \leq X$ for every $\epsilon > 0$*

$$\sum_{q=1}^{X} \sum_{|c| \geq Z} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} X(r^{-1}m)^{-\frac{\delta}{2}(d-1)+\epsilon} Z^{-\frac{d-3}{2}} \tag{2.113}$$

Proof: From Lemma 2.4.1 $S_{mq}(c) = 0$, unless $c \equiv \alpha a \bmod m$. So, without loss of generality, we assume that $c \equiv \alpha a \bmod m$. We use the upper bound on $I_{mq}(c)$ that is proved in Lamma 2.5.2 to derive,

$$\sum_{q=1}^{X} \sum_{|c| \geq Z} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} \sum_{q=1}^{X} \sum_{|c| \geq Z} q^{-d} m^{-d} |S_{mq}(c)| \Big(\frac{Q|c|}{r^{-1}mq} \Big)^{-\frac{d-1}{2}}$$

From Lemma 2.4.4, we have

$$\sum_{q=1}^{X} m^{-d} q^{-\frac{d+1}{2}} |S_{qm}(c)| \ll_{\Delta} m^{\epsilon} X^{1+\epsilon}.$$

Therefore,

$$\sum_{q=1}^{X} m^{-d} q^{-\frac{d+1}{2}} |S_{qm}(c)| \ll \frac{mQ^{d+1}}{R} X^{1+\epsilon} (r^{-1}m)^{-\frac{\delta}{2}(d-1)} \sum_{|c|\geq Z} \Big(\frac{1}{|c|}\Big)^{\frac{d-1}{2}}.$$

From the Lemma 2.5.3, we deduce that

$$\sum_{|c|\geq Z} \Big(\frac{1}{|c|}\Big)^{\frac{d-1}{2}} \leq (r^{-1}m)^{\epsilon} Z^{-\frac{d-3}{2}}. \tag{2.114}$$

Since $X < Q = (r^{-1}m)^{1+\delta}$, a small enough choice for ϵ in the definition of the exceptional vectors c concludes the lemma. $\square$

Lemma 2.5.5 *We have the following upper bound on the sum over $X \leq q \leq Q$ and exceptional vectors with $|c| < Z$*

$$\sum_{q=X}^{Q} \sum_{|c|<Z} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} Z R^{\epsilon} X^{-\frac{d-3}{2}}. \tag{2.115}$$

Proof: We use the trivial upper bound on $I_{mq}(c)$, i.e.

$$|I_{mq}(c)| \ll \frac{mQ^{d+1}}{R}. \tag{2.116}$$

Using this and Lemma 2.4.4, we have

$$\sum_{q=X}^{Q} \sum_{|c|<Z} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} Q^{\epsilon} X^{-\frac{d-3}{2}} \sum_{|c|<Z} 1. \tag{2.117}$$

From Lemma 2.5.3, we obtain

$$\sum_{|c|<Z} 1 \ll Z(mr^{-1})^{\epsilon}.$$

Hence,

$$\sum_{q=X}^{Q} \sum_{|c|<Z} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} Z Q^{\epsilon} X^{-\frac{d-3}{2}}. \tag{2.118}$$

Therefore, we conclude the lemma.$\square$

In the following lemma we apply the alternative use of the Lemma 2.5.4 and Lemma 2.5.5 to

improve an upper bound on the contribution of the exceptional vectors. We make an increasing sequence of (X_k, Z_k) of integers

$$X_k < X_{k+1} \text{ and } Z_k < Z_{k+1}.$$

such that the contribution of the exceptional vectors is negligible in the delta method if either $|c| < Z_k$ or $q < X_k$. Our strategy to bound the contribution of the exceptional vectors c is to find a k such that $Q < X_k$ or $(r^{-1}m)^{1+\epsilon} < Z_k$. We show such a k exists in the following lemma.

Lemma 2.5.6 *For every integer $k \geq 0$, there exists an $\eta > 0$ such that if $X_k = (r^{-1}m)^{\frac{\delta}{2}(d-1)\left[\sum_{i=0}^{k}(\frac{d-3}{2})^{2i}\right]-\eta}$ and $Z_k = (r^{-1}m)^{\frac{\delta}{2}(d-1)\left[\sum_{i=0}^{k}(\frac{d-3}{2})^{2i-1}\right]-\eta}$, then we have the following upper bound on the the sum over the exceptional integral vectors c*

$$\sum_{q=1}^{Q}\sum_{c}(mq)^{-d}S_{mq}(c)I_{mq}(c) - \sum_{q=X_k}^{Q}\sum_{|c|>Z_k}(mq)^{-d}S_{mq}(c)I_{mq}(c) \leq \frac{mQ^{d+1}}{R}Q^{-\epsilon} \tag{2.119}$$

Proof: We prove this lemma by induction on k. For $k = 0$, we let $X_0 = (r^{-1}m)^{\frac{\delta(d-1)}{2}-\eta}$ and $Z_0 = 1$. Hence, it suffices to show that

$$\sum_{q=1}^{X_0}\sum_{c}(mq)^{-d}S_{mq}(c)I_{mq}(c) \ll \frac{mQ^{d+1}}{R}Q^{-\epsilon}. \tag{2.120}$$

Note that this is implied from Lemma 2.5.4 for $X = (r^{-1}m)^{\frac{\delta}{2}(d-1)-\epsilon}$ and $Z = 1$. Next, we prove the inductive step. So, we assume the lemma holds for k. From the inductive hypothesis, we have

$$\sum_{q=1}^{Q}\sum_{c}(mq)^{-d}S_{mq}(c)I_{mq}(c) - \sum_{q=X_k}^{Q}\sum_{|c|>Z_k}(mq)^{-d}S_{mq}(c)I_{mq}(c) \leq \frac{mQ^{d+1}}{R}Q^{-\epsilon}$$

where $X_k = (r^{-1}m)^{\frac{\delta}{2}(d-1)\left[\sum_{i=0}^{k}(\frac{d-3}{2})^{2i}\right]-\eta}$ and $Z_k = (r^{-1}m)^{\frac{\delta}{2}(d-1)\left[\sum_{i=0}^{k}(\frac{d-3}{2})^{2i-1}\right]-\eta}$. Note that

$$\begin{aligned}
\sum_{q=X_k}^{Q}\sum_{|c|>Z_k}(mq)^{-d}S_{mq}(c)I_{mq}(c) &= \sum_{q=X_{k+1}}^{Q}\sum_{|c|>Z_{k+1}}(mq)^{-d}S_{mq}(c)I_{mq}(c) && (2.121)\\
&+ \sum_{q=X_k}^{X_{k+1}}\sum_{|c|>Z_{k+1}}(mq)^{-d}S_{mq}(c)I_{mq}(c) && (2.122)\\
&+ \sum_{q=X_k}^{Q}\sum_{Z_k<|c|<Z_{k+1}}(mq)^{-d}S_{mq}(c)I_{mq}(c). && (2.123)
\end{aligned}$$

From Lemma 2.5.4, the middle sum (2.122) is bounded above by

$$\sum_{q=X_k}^{X_{k+1}} \sum_{|c|>Z_{k+1}} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} X_{k+1} (r^{-1}m)^{-\frac{\delta}{2}(d-1)+\epsilon} Z_{k+1}^{-\frac{d-3}{2}} \ll \frac{mQ^{d+1}}{R} Q^{-\epsilon}. \tag{2.124}$$

From Lemma 2.5.5, the last sum (2.123) is also bounded above by

$$\sum_{q=X_k}^{Q} \sum_{Z_k<|c|<Z_{k+1}} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} Z_{k+1} Q^{\epsilon} X_k^{-\frac{d-3}{2}} \tag{2.125}$$

$$\ll \frac{mQ^{d+1}}{R} Q^{-\epsilon}. \tag{2.126}$$

Hence the lemma holds for $k+1$, and hence, we conclude the lemma $\square$.

Corollary 2.5.7 *Let $\delta > 0$ if the quadratic form $F(x)$ has $d \geq 5$ variables, and $\delta > 1$ if $d = 4$. Then there exists an $\epsilon > 0$ which only depends on d and δ such that*

$$\sum_{q=1}^{Q} \sum_{c\neq 0} (mq)^{-d} S_{mq}(c) I_{mq}(c) \ll \frac{mQ^{d+1}}{R} Q^{-\epsilon} \tag{2.127}$$

Proof: From the Lemma 2.5.6, it suffices to find a k such that $X_k > Q$ or $Z_k > (r^{-1}m)^{1+\epsilon}$. If $d \geq 5$, this is trivial, since $\frac{d-3}{2} \geq 1$ and in fact X_k and Z_k go to infinity as $k \to \infty$. For $d = 4$, It is easy to check there exists k such that $X_k > Q$ or $Z_k > (r^{-1}m)^{1+\epsilon}$.

2.6 The main theorem

In this section, we derive the main term of the smooth counting and as a result prove our optimal strong approximation theorem. The main term comes from $c = 0$ and summing over $1 \leq q \leq Q$. We estimate the integral $I_{mq}(0)$ it turns out that the main term of the integrals $I_{mq}(0)$ is independent of q if $1 \leq q \leq Q^{1-\epsilon}$, and the value is equal to the singular integral which appears in the circle method. On the other hand if $Q^{1-\epsilon} \leq q \leq Q$ the exponential sum is bounded by Lemma 2.4.4

$$\sum_{q=QR^{-\epsilon}}^{Q} (mq)^{-d} |S_q(0)| \ll Q^{\frac{3-d}{2}+\epsilon}. \tag{2.128}$$

Hence, their contributions are negligible in the main term. Therefore, the main term is the product of the singular integral with the sum of $S_{mq}(0)$ over $1 \leq q \leq Q^{1-\epsilon}$. This sum is converging to the

singular series. As claimed, we derive a smooth counting formula with a power saving error term which is the product of the singular series with the singular integral.

2.6.1 Singular integral

In the following lemma, we estimate the integral $I_{mq}(0)$ for $1 \leq q \leq Q^{1-\epsilon}$.

Lemma 2.6.1 *Suppose that* $1 \leq q \leq Q^{1-\epsilon}$. *Then*

$$I_{mq}(0) = \sigma_\infty(F, w)\frac{mQ^{d+1}}{R} + O_N(Q^{-N}) \tag{2.129}$$

for any $N > 0$, *where* $\sigma_\infty(F, w)$ *is the singular integral and equals to*

$$\begin{aligned} \sigma_\infty(F, w) &= \int_{y(x)=0} \frac{R}{X^T A e_d} w(x) dx_1 \dots dx_{d-1} \\ &= \lim_{\epsilon \to 0} \frac{\int_{0<y(x)<\epsilon} w(x) dx_1 \dots dx_d}{\epsilon} \end{aligned} \tag{2.130}$$

where we normalize the variable so that $-1 < x_i < 1$.

Proof: We change the variables from $(t_1, \dots t_d)$ to $(u_1, \dots, u_{d-1}, y)$. We recall the formula (2.76) and plug in $c = 0$ in the formula to obtain

$$\begin{aligned} I_{mq}(0) &= \int h(\frac{q}{Q}, \frac{F(mt+a)-N}{m^2Q^2}) w(t) dt_1 \dots . dt_d \\ &= \frac{mQ^2}{R} \int \frac{R}{X^T A e_d} h(\frac{q}{Q}, y) w(t) du_1 \dots du_{d-1} dy. \end{aligned} \tag{2.131}$$

We normalize variables again so that they lies in the interval $[-1, 1]$.

$$Qx_i = u_i,$$

$$\frac{mQ^2}{R} x_d = u_d.$$

Therefore, we obtain

$$I_{mq}(0) = \frac{mQ^{d+1}}{R} \int \frac{R}{X^T A e_d} h(\frac{q}{Q}, y) w(x, y) dx_1 \dots dx_{d-1} dy.$$

We apply the Fubini's theorem and first take integration over y

$$I_{mq}(0) = \frac{mQ^{d+1}}{R} \int \frac{R}{X^T A e_d} dx_1 \dots dx_{d-1} \int h(\frac{q}{Q}, y) w(x, y) dy.$$

We invoke Lemma 2.3.3 and estimate the integral over y

$$I_{mq}(0) = \frac{mQ^{d+1}}{R} \int \frac{R}{X^T A e_d} w(x, 0) dx_1 \dots dx_{d-1} + O_N(Q^{-N}).$$

By definition of $\sigma_\infty(w, F)$, we deduce that

$$I_{mq}(0) = \sigma_\infty(F, w) \frac{mQ^{d+1}}{R} + O_N(Q^{-N}).$$

Note that

$$\frac{\partial y}{\partial (x_d)}^{-1} = \frac{R}{X^T A e_d}.$$

Therefore, by change of variable formula we conclude

$$\begin{aligned} \sigma_\infty(F, w) &= \int_{y(x)=0} \frac{R}{X^T A e_d} w(x) dx_1 \dots dx_{d-1} \\ &= \lim_{\epsilon \to 0} \frac{\int_{0<y(x)<\epsilon} w(x) dx_1 \dots dx_d}{\epsilon}. \square \end{aligned} \tag{2.132}$$

2.6.2 Singular series

In this section, we show the sum $S_{mq}(0)$ over $1 \leq q \leq Q^{1-\epsilon}$ is convergent to the singular series $\mathfrak{S}(N, p)$. In the following lemma, we show the contribution of $Q^{1-\epsilon} \leq q \leq Q$ is negligible in the delta method.

Lemma 2.6.2 *We have the following upper bound on the sum over $Q^{1-\epsilon} \leq q \leq Q$*

$$\sum_{q=Q^{1-\epsilon}}^{Q} (mq)^{-d} S_{mq}(0) I_{mq}(0) \ll_\epsilon \frac{mQ^{d+1}}{R} Q^{\frac{3-d}{2}+\epsilon}. \tag{2.133}$$

Proof: We use the trivial bound on $I_{mq}(0)$ and we obtain

$$I_q(0) \ll \frac{mQ^{d+1}}{R}. \tag{2.134}$$

From Lemma 2.4.4, we have

$$\sum_{q=QR^{-\epsilon}}^{Q} (mq)^{-d}|S_q(0)| \ll Q^{\frac{3-d}{2}+\epsilon}. \tag{2.135}$$

Hence, we conclude the Lemma. □

We invoke the following lemma; see [HB96, Page 50; Lemma 31] which shows that the sum $S_{mq}(0)$ over $1 \leq q \leq Q^{1-\epsilon}$ is convergent to the singular series $\mathfrak{S}(N,p)$ and the singular series is the product of the local densities $\prod_p \sigma_p$.

Lemma 2.6.3 *Let $F(x)$ be a non-degenerate quadratic form in d variables where $d \geq 4$, then*

$$\sum_{1\leq q\leq X} (qm)^{-d} S_{mq}(0) = \prod_p \sigma_p + O_\epsilon(X^{3-d/2+\epsilon}Q^\epsilon) \tag{2.136}$$

As a result

$$\sum_{1\leq q\leq Q^{1-\epsilon}} (qm)^{-d} S_{mq}(0) = \prod_p \sigma_p + O_\epsilon(Q^{3-d/2+\epsilon}) \tag{2.137}$$

We can now state and prove our main theorem.

Theorem 2.6.4 *Let $F(X)$ be a non-degenerate quadratic form in d variables. Let m be an integer and $a \in \left(\frac{\mathbb{Z}}{m\mathbb{Z}}\right)^d$ is any mod m solution for $F(a) = l$ where $l \in \mathbb{Z}/m\mathbb{Z}$. Let b be a real point such that $F(b) = 1$ and let $B(b,r)$ be the r neighborhood of the point b on the variety $F(x) = 1$, i.e.*

$$B(b,r) := \{x : F(x) = 1 \text{ and } \ dist(x,b) \leq r\}.$$

Let $\delta > 0$ if $d > 4$ and $\delta > 1$ if $d = 4$. Assume that N is a positive integer such that

$$N := R^2 \text{ where } R \gg (mr^{-1})^{2+\delta},$$

and

$$Q := \frac{R}{mr^{-1}}.$$

We let $y(X) := \frac{F(X)-N}{m^2Q^2}$ and $w(x)$ be a compactly supported smooth weight function which is supported inside a convex region where y is bounded by a constant. Define

$$N(a,\omega) := \sum_{t\in\mathbb{Z}^d} \omega(mt+a)\delta_{F(mt+a)-N}. \tag{2.138}$$

Then we have the following formula:

$$N(a,\omega) = \sigma_\infty(F,w)\prod_p \sigma_p(a,N)\frac{Q^{d-1}}{R} + O_\epsilon(\frac{Q^{d-1}}{R}R^{-\epsilon}), \tag{2.139}$$

for some $\epsilon > 0$.

Proof: We write the smooth expansion of the delta function as stated in Lemma 2.3.1

$$N(a,\omega) = \frac{C_Q}{mQ^2}\sum_{q=1}^{Q}\sum_{c\in\mathbb{Z}^d}(mq)^{-d}S_{mq}(c)I_{mq}(c). \tag{2.140}$$

From Corollary 2.5.7 and Lemma 2.6.2, we can drop the nonzero integral vectors c and restrict the sum over q to $1 \le q \le Q^{1-\epsilon}$, hence

$$N(a,w) = \frac{C_Q}{mQ^2}\sum_{q=1}^{Q^{1-\epsilon}}(mq)^{-d}S_{mq}(0)I_{mq}(0) + O_\epsilon(\frac{Q^{d-1}}{R}R^{-\epsilon}). \tag{2.141}$$

From Lemma 2.6.1, we have

$$I_{mq}(0) = \sigma_\infty(F,w)\frac{mQ^{d+1}}{R} + O_\epsilon(\frac{Q^{d-1}}{R}R^{-\epsilon}).$$

Therefore,

$$N(a,w) = \sigma_\infty(F,w)\frac{Q^{d-1}}{R}\sum_{q=1}^{Q^{1-\epsilon}}(mq)^{-d}S_{mq}(0) + O_\epsilon(\frac{Q^{d-1}}{R}R^{-\epsilon}).$$

Finally, from Lemma 2.3.3, we obtain

$$N(a,\omega) = \sigma_\infty(F,w)\prod_p \sigma_p(a,N)\frac{Q^{d-1}}{R} + O_\epsilon(\frac{Q^{d-1}}{R}R^{-\epsilon}),$$

Therefore, we conclude our theorem.□

Since we derived a smooth counting formula for the number of integral points with a power saving error term. By a standard method in analysis we can find two smooth weight function $w_1(x)$ and $w_2(x)$ such that they approximate from below and above the characteristic function $\chi(x)$ of the open ball $B(b,r)$, i.e.

$$w_1(x) \le \chi(x) \le w_2(x). \tag{2.142}$$

Therefore we deduce our counting formula and Theorem 2.1.10.

Chapter 3

Diameter of Ramanujan Graphs and Random Cayley Graphs

3.1 Introduction

3.1.1 Motivation

The diameter of any k-regular graph with n vertices is bounded from below by $\log_{k-1}(n)$ trivially. While the diameter of a general connected k-regular graph may be as large as a scalar multiple of the number of vertices n, it is known that the diameter of any k-regular Ramanujan graph is bounded from above by $2(1+\epsilon)\log_{k-1}(n)$ [LPS88]. Lubotzky, Phillips and Sarnak constructed a family of $(p+1)-$regular Ramanujan graphs $X^{p,q}$ [LPS88], where p and q are prime numbers. $X^{p,q}$ is the Cayley graph of $\mathrm{PGL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ with $p+1$ explicit generators. Their construction can be modified for every integer q; see [DSV03] or [Lub10]. It was expected that the diameter of the LPS Ramanujan graphs to be bounded from above by $(1+\epsilon)\log_{k-1}(n)$; see [Sar90, Chapter 3]. However, we show that the diameter of an infinite family of $p+1$-regular LPS Ramanujan graphs is greater than or equal to

$$\lfloor(\frac{4}{3})\log_p(n)\rfloor. \tag{3.1}$$

While there are points x and y whose distances is large in a LPS Ramanujan graph, we prove that the distance of almost all pairs of vertices in any k-regular Ramanujan graph G is less than $(1+\epsilon)\log_{k-1}(n)$. In other words, almost all diameter is asymptotic to

$$(1+\epsilon)\log_{k-1}(n).$$

In fact, we prove a stronger result, we show that for every vertex x in a k-regular Ramanujan graph G the number of points which can't visited by exactly l steps, where $l > (1+\epsilon)\log_{k-1}(n)$, is less than $n^{1-\epsilon}$. So the number is exponentially decaying. In particular, it also recovers $2(1+\epsilon)\log_{k-1}(n)$ as an upper bound on the diameter of k-regular Ramanujan graph. Furthermore, we give some numerical datas for two families of 6-regular graphs. The first family of graphs are the 6-regular LPS Ramanujan graphs and we denote them by $X^{5,q}$. The second family are the 6-regular random Cayley graphs $\mathrm{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$, i.e. the Cayley graphs that are constructed by 3 random generators of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ and their inverses $\{s_1^{\pm}, s_2^{\pm}, s_3^{\pm}\}$. We denote these graphs by Z^q. The numerical experiments suggest that the diameter of the (number theoretic) LPS Ramanujan Graphs is asymptotic to

$$(\frac{4}{3})\log_5(n). \tag{3.2}$$

This is consistent with our conjecture on the optimal strong approximation for quadratic forms in 4 variables [TS15]. On the other hand, the numerical data suggests that the diameter of the random Cayley graph equals that of a random 6-regular graph [BFdlV82], that is

$$\log_5(n). \tag{3.3}$$

These are consistent with Sarnak's expectation. Sarnak suggested that the covering exponent of a thin set of gates may achieve the trivial lower bound 1 and the covering exponent of arithmetic gates are $\frac{4}{3}$ [Sar15b]. The archimedean analog of our question has been discussed there; see [Sar15b]. For instance, the diameter of the LPS Ramanujan Graphs is bounded from above by $\frac{4}{3}(1+\epsilon)\log_{k-1}(n)$ is analogous to the covering exponent being bounded from above by $\frac{4}{3}$. This question is related to the theory of quadratic Diophantine equations; see [TS15]. Sarnak showed that the almost all covering exponent is 1; see [Sar15b, Page 28]. Our Theorem 4.16 is the p-adic analogue of Sarnak's theorem. In other words, these theorems state that the almost all diameter and the almost all covering exponent are equal to the trivial lower bound given by pigeonhole principle. In a recent paper [LP15], Peres and Lubetzky show the simple random walk exhibits cutoff on Ramanujan Graphs. As a result they give a more detailed version of our Theorem 4.16. In a similar work, for the family of LPS bipartite Ramanujan graphs, Biggs and Boshier determined the asymptotic

behavior of the girth of these graphs; see [BB90]. They showed that the girth is asymptotic to

$$(\frac{4}{3})\log_{k-1}(n).$$

3.1.2 Statement of results

We begin by the description of the LPS Ramanujan graphs. The idea of the construction comes from number theory, i.e. generalized Ramanujan conjecture. More precisely, we consider the symmetric space $\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ which can be identified with a regular $(p+1)$-infinite tree. We note that $\mathrm{PGL}_2(\mathbb{Z}[1/p])$ acts from the left on $\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$. The generalized Ramanujan conjecture, which is a theorem in this case, implies that the quotient of $\mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p)$ by any congruence subgroup of $\mathrm{PGL}_2(\mathbb{Z}[1/p])$ which is a $p+1$-regular graph is a Ramanujan graph. By considering an appropriate congruence subgroup of $\mathrm{PGL}_2(\mathbb{Z}[1/p])$ we can identify the quotient of this symmetric space with a Cayley graph of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$ with $p+1$ generators. These are LPS Ramanujan graphs. We show that the diameter of the LPS Ramanujan graphs is greater than

$$(\frac{4}{3})\log_p(n) - 4\log_p(\frac{m}{q}) - (\frac{2}{3})\log_p 2,$$

provided that $q|m$, where q is a prime power and $q \neq m$. Note that these graphs are congruence cover of the LPS Ramanujan graphs $X^{p,q}$.

In what follows, we give an explicit description of the LPS Ramanujan graphs in terms of the Cayley graphs of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$. Assume that q is a prime number and $q|m$ where m is an integer and -1 is quadratic residue mod m. Let p be a prime number such that $p \equiv 1 \bmod 4$ and p is quadratic residue mod m. We denote the representatives of square roots of -1 and p mod m by i and $\sqrt{p}$, respectively. We are looking at the integral solutions $\alpha = (x_0, x_1, x_2, x_3)$ of the following diophantine equation

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p, \tag{3.4}$$

where $x_0 > 0$ and is odd and x_1, x_2, x_3 are even numbers. There are exactly $p+1$ integral solutions with such properties . To each such integral solution α, we associates the following matrix α in $\mathrm{PSL}_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$:

$$\alpha := \frac{1}{\sqrt{p}} \begin{bmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & x_0 - ix_1 \end{bmatrix}. \tag{3.5}$$

This gives us $p+1$ matrices in $\mathrm{PSL}_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$. Lubotzky [Lub10, Theorem 7.4.3] showed that they

generate $\mathrm{PSL}_2(\frac{\mathbb{Z}}{m\mathbb{Z}})$ and the associated Cayley graph is a non-bipartite Ramanujan graph. We denote this graph by $X^{p,m}$. Furthermore, Lubotzky showed that

- diam $X^{p,m} \leq 2\log_p(n) + 2\log_p 2 + 1$.
- girth $X^{p,m} \geq \frac{2}{3}\log_p(n) - 2\log_p 2$.

Our first theorem shows that either the distance between the identity matrix I and $I' := \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix}$ or between I and $W := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ in $X^{p,m}$ is larger than

$$(\frac{4}{3})\log_p(n) - 4\log_p(\frac{m}{q}) - (\frac{2}{3})\log_p 2.$$

As a result,

$$(\frac{4}{3})\log_p(n) - 4\log_p(\frac{m}{q}) - (\frac{1}{3})\log_p 2 \leq \mathrm{diam}(X^{p,m}). \tag{3.6}$$

We state our first theorem which we prove in Section 4.1.2.

Theorem 3.1.1 *Let m be an integer such that -1 is quadratic residue mod m. Assume that q is an odd prime power such that $q|m$ and $q \neq m$. Let p be an odd prime number, such that p is quadratic residue mod m. Let $X^{p,m}$ be the LPS Ramanujan graph. Then we have the following lower bound on the diameter of the LPS graph $X^{p,m}$*

$$(\frac{4}{3})\log_p(n) - 4\log_p(\frac{m}{q}) - (\frac{2}{3})\log_p 2 \leq \mathit{diam}(X^{p,m}). \tag{3.7}$$

Corollary 3.1.2 *Let p and q be prime numbers that are congruent to 1 mod 4 and $p > 1250$. Then the diameter of the LPS Ramanujan graph $X^{p,5q^k}$ for any integer k is greater than or equal to*

$$\lfloor(\frac{4}{3})\log_p n\rfloor. \tag{3.8}$$

By contrast, we prove that the distance of almost all pairs of vertices in any k-regular Ramanujan graph G is less than $(1+\epsilon)\log_{k-1}(n)$. We use the Ramanujan bound on the nontrivial eigenvalues of the adjacency matrix to prove the distance of almost all pairs of vertices is less than $(1+\epsilon)\log_k(n)$. The archimedean version of this problem has been discussed in Sarnak's letter to Scott Aaronson and Andy Pollington [Sar15b, Page 28]. More precisely, we prove the following stronger result in Section 3.3:

Theorem 3.1.3 *Let G be a k-regular Ramanujan graph and fix a vertex $x \in V(G)$. Let R be an integer such that $R > (1+\epsilon)\log_{k-1}(n)$. Define $M(x,R)$ to be the set of all vertices $y \in G$ such that there is no path from x to y with length R (we allow to pass from an edge multiple times but not immediately after). Then,*

$$|M(x,l)| \leq n^{1-\epsilon}(1+R)^2. \tag{3.9}$$

3.1.3 Outline of the chapter

In Section 4.1.2, we prove Theorem 3.1.1. The proof uses some elementary facts in Number Theory and is short. In Section 3.3, we prove Theorem 4.16. As a corollary, we prove that the distance of almost all pair of vertices is less than

$$(1+\epsilon)\log_{k-1}(n).$$

We use the Chebyshev's inequality by giving an upper bound for the variance. We use the Ramanujan bound on the eigenvalues of the adjacency matrix of the graph to give an upper bound on the variance. Finally in Section 3.4, we compute the diameter of two families of 6-regular graphs. From our numerical experiments, we expect that the diameter of the LPS Ramanujan graphs [Sar15a] is asymptotic to

$$(\frac{4}{3})\log_p(n). \tag{3.10}$$

We define a random 6 regular Cayley graph Z^q , by considering the Cayley graph of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ relative to the generating set $S = \{s_1^{\pm}, s_2^{\pm}, s_3^{\pm}\}$, where s_1, s_2, s_3 are random elements of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$. From the numerical experiments , we show that in fact the random Cayley graph has a shorter diameter and break the $\frac{4}{3}\log_5 n$ lower bound for the LPS Ramanujan graphs. For example, We obtained a sample from the random Cayley graph of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{229\mathbb{Z}})$, such that

$$\text{diam } (Z^{229}) < 1.23\log_5 n. \tag{3.11}$$

We expect that the diameter of the random Cayley graph would be as small as possible. More precisely, for $\epsilon > 0$

$$\text{diam}(Z^q) \leq (1+\epsilon)\log_5(n) + c_\epsilon, \text{ almost surely as } q \to \infty. \tag{3.12}$$

3.2 Lower bound for the diameter of the Ramanujan graphs

In the rest of this section, we give a proof of Theorem 3.1.1.

Recall that $W := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $I' := \begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix}$. We show that

$$\max(\text{ dist }(I, I'),\ \text{dist }(I, W)) \geq (\frac{4}{3}) \log_p(n) - 4 \log_p(\frac{m}{q}) - (\frac{2}{3}) \log_p 2. \tag{3.13}$$

Assume the contrary that

$$\max(\text{ dist }(I, I'),\ \text{dist }(I, W)) < (\frac{4}{3}) \log_p(n) - 4 \log_p(\frac{m}{q}) - (\frac{2}{3}) \log_p 2. \tag{3.14}$$

Since $n = \frac{(m-1)m(m+1)}{2}$, the above assumption is equivalent to

$$\max(\text{ dist }(I, I'),\ \text{dist }(I, W)) < \log_p \frac{q^4}{4} \tag{3.15}$$

$dist(I, I') < \log_p \frac{q^4}{4}$ gives us a solution to the following diophantine equation

$$a^2 + b^2 + c^2 + d^2 = p^k, \tag{3.16}$$

where $b \equiv c \equiv d \equiv 0 \bmod 2q$ and $a \equiv 1 \bmod 2$. At least one of b, c, d is nonzero. From this we deduce that

$$a^2 \equiv p^k \bmod q^2 \text{ and } 4q^2 \leq p^k. \tag{3.17}$$

We consider two cases: k even and k odd.

If k is even and $k = 2t$. From 3.17 we deduce that

$$a \equiv \pm p^t \bmod q^2. \tag{3.18}$$

If $p^t \geq \frac{q^2}{2}$,

$$dist(I, I') = 2t \geq \log_p \frac{q^4}{4}, \tag{3.19}$$

a contradiction. Consequently, $p^t < \frac{q^2}{2}$. Since $a \neq \pm p^t$, we deduce that

$$a = p^t + lq^2 \text{ for } l \neq 0. \tag{3.20}$$

Therefore

$$\|a\| \geq \frac{1}{2}q^2. \tag{3.21}$$

Hence,

$$\begin{aligned} p^{2t} &\geq \frac{q^4}{4}, \text{ and so} \\ \text{dist } (I, I') = 2t &\geq \log_p \frac{q^4}{4}. \end{aligned} \tag{3.22}$$

a contradiction. Hence k is odd and $k = 2t + 1$.

We want to use a similar argument to show that dist $(I, W) = 2t_0 + 1$ is an odd number. dist $(I, W) < \frac{4}{3}\log_p(n)$ gives us a solution to the following diophantine equation

$$a^2 + b^2 + c^2 + d^2 = p^k. \tag{3.23}$$

Where $b \equiv a \equiv d \equiv 0 \bmod q$ and $c \equiv 0 \bmod 2$. Since a is odd, then $q \leq \|a\|$. We deduce that

$$c^2 \equiv p^k \bmod q^2 \text{ and } q^2 \leq p^k. \tag{3.24}$$

We consider two cases: k even and k odd.

If k is even and $k = 2t$, from 3.24 we deduce that

$$c \equiv \pm p^t \bmod q^2. \tag{3.25}$$

If $p^t \geq \frac{q^2}{2}$,

$$dist(I, W) = 2t \geq \log_p \frac{q^4}{4}, \tag{3.26}$$

a contradiction. Consequently, $p^t < \frac{q^2}{2}$. Since c is even, then $c \neq \pm p^t$. We deduce that

$$c = \pm p^t + lq^2 \text{ for } l \neq 0. \tag{3.27}$$

Therefore,

$$c \geq \frac{1}{2}q^2. \tag{3.28}$$

Hence,

$$\begin{aligned} p^{2t} &\geq \frac{1}{4}q^4, \\ dist(I, W) = 2t &\geq \log_p \frac{q^4}{4}. \end{aligned} \tag{3.29}$$

This is a contradiction. Therefore $k = 2t_0 + 1$ for some t_0.

We now investigate the case where

$$\text{dist } (I, I') = 2t + 1 < \log_p \frac{q^4}{4}$$

and

$$\text{dist } (I, W) = 2t_0 + 1 < \log_p \frac{q^4}{4}.$$

dist $(I, I') = 2t + 1$ gives us a solution to the following diophantine equation

$$a^2 + b^2 + c^2 + d^2 = p^{2t+1} < \frac{q^4}{4}. \tag{3.30}$$

Where $b \equiv c \equiv d \equiv 0 \mod 2q$ and $a \equiv 1 \mod 2$. At least one of b, c, d is nonzero. Hence

$$4q^2 < p^{2t+1} < q^4. \tag{3.31}$$

dist $(I, W) = 2t_0 + 1 < \log_p \frac{q^4}{4}$, gives us a solution to the following diophantine equation

$$a_0^2 + b_0^2 + c_0^2 + d_0^2 = p^{2t_0+1} < q^4/4. \tag{3.32}$$

Where $b_0 \equiv a_0 \equiv d_0 \equiv 0 \mod$ q and $a_0 \equiv 1 \mod 2$. From 3.30 and 3.32 we deduce that

$$\begin{aligned} a^2 \equiv p^{2t+1} \mod q^2 \text{ and } a \text{ is odd } a < p^{t+1/2} < q^2/2, \\ c^2 \equiv p^{2t_0+1} \mod q^2 \text{ and } c \text{ is even } c < p^{t_0+1/2} < q^2/2. \end{aligned} \tag{3.33}$$

Without loss of generality we assume that $t_0 > t$, from 4.1.4 we deduce that

$$\pm a p^{t_0 - t} = c. \tag{3.34}$$

However, this is incompatible with the parities of a and c. Hence, we conclude Theorem 3.1.1.

3.3 Visiting almost all points after $(1+\epsilon)\log_{k-1}(n)$ steps

In this section, we show that if we pick two random points from a k-regular Ramanujan graph G, then almost surely they have a distance less than

$$(1+\epsilon)\log_{k-1}(n). \tag{3.35}$$

The idea is to use the spectral gap of the adjacency matrix of the Ramanujan graphs to prove an upper bound on the variance. A similar strategy has been implemented by Sarnak ; see [Sar15b, Page 28].

Let $A(x,y)$ be the adjacency matrix of the Ramanujan graph G, i.e.

$$A(x,y) := \begin{cases} 1 \text{ if } x \equiv y \\ \\ 0 \text{ otherwise} \end{cases}. \tag{3.36}$$

Since $A(x,y)$ is a symmetric matrix, so it is diagonalizable. We can write the spectral expansion of this matrix by the set of its eigenfunctions. Namely,

$$A(x,y) = \frac{k}{\|G\|} + \sum_j \lambda_j \phi_j(x)\phi_j(y), \tag{3.37}$$

where $\{\phi_j\}$ is the orthonormal basis of the nontrivial eigenfunctions with eigenvalues $\{\lambda_j\}$ for the adjacency matrix $A(x,y)$. Since we assumed that G is a Ramanujan graph, then $|\lambda_j| \leq 2\sqrt{k-1}$. We change the variables and write

$$\lambda_j = 2\sqrt{k-1}\cos\theta_j. \tag{3.38}$$

We define $S(R) := (k-1)^{\frac{R}{2}} U_R(\frac{A}{2\sqrt{k-1}})$, where $U_R(x)$ is the Chebyshev polynomial of the second kind, i.e.

$$U_R(x) := \frac{\sin((R+1)\arccos x)}{\sin(\arccos x)}. \tag{3.39}$$

The following is the spectral expansion of $S(R)$:

$$S(R)(x,y) := \frac{(k-1)^{\frac{R}{2}} U_R(\frac{k}{2\sqrt{k-1}})}{\|G\|} + \sum_j (k-1)^{\frac{R}{2}} U_R(\frac{\lambda_j}{2\sqrt{k-1}})\phi_j(x)\phi_j(y), \tag{3.40}$$

Remark 3.3.1 *Note that if we lift the linear operator $S(R)$ to the universal covering space of the*

k-regular graph G, (which is an infinite k-regular tree), then S(R) is the linear operator, which takes the average of a function on a sphere with radius R. Namely,

$$S(R)f(x) := \sum_{y, dist(x,y)=R} f(y). \tag{3.41}$$

From the formula for the kernel of $S(R)$ given in 3.40, we obtain

$$S(R)(x,y) = \frac{k(k-1)^{R-1}}{\|G\|} + \sum_j (k-1)^{\frac{R}{2}} \frac{\sin((R+1)\theta_j)}{\sin\theta_j} \phi_j(x)\phi_j(y). \tag{3.42}$$

We calculate the variance over y. For $i \neq j$, we have $\sum_{y\in G} \phi_i(y)\phi_j(y) = 0$ and $\sum_{y\in G} \phi_i(y)^2 = 1$, So only the diagonal terms remain in the following summation:

$$\begin{aligned} \text{Var } (x) &:= \sum_{y\in G} \|S(R)(x,y) - \frac{k(k-1)^{R-1}}{\|G\|}\|^2 \\ &= \sum_j (k-1)^R \frac{(\sin(R+1)\theta_j)^2}{(\sin\theta_j)^2} \phi_j(x)^2. \end{aligned} \tag{3.43}$$

Since $\{\phi_j\}$ is an orthonormal basis, we have

$$1 = \sum_{y\in G} \delta(x,y)dy = \frac{1}{\|G\|} + \sum_j \phi_j(x)^2. \tag{3.44}$$

We also have the following trivial trigonometric inequality, which is derived from the geometric series summation formula :

$$|\frac{\sin(R+1)\theta}{\sin\theta}| = |\sum_{j=0}^{R} e^{i\theta}| \leq R+1. \tag{3.45}$$

From 3.44 and 3.45, we obtain

$$\text{Var } \leq (R+1)^2(k-1)^R. \tag{3.46}$$

We define

$$M := \{y : S(R)(x,y) = 0\}. \tag{3.47}$$

Note that M is the set of all vertices $y \in G$, such that there is no path from x to y with length R. Therefore, this is exactly the set $M(x,R)$ as defined in the Theorem 4.16. By the definition of the Var given in 3.43,

$$\|M\||\frac{k(k-1)^{R-1}}{\|G\|}|^2 \leq \text{ Var.} \tag{3.48}$$

From 3.48 and 3.46, we have

$$\|M\|\|(k-1)^R\| < \|G\|^2(R+1)^2. \tag{3.49}$$

If we choose $R > (1+\epsilon)\log_{k-1}(n)$, Hence

$$\|M\| \leq n^{1-\epsilon}(1+R)^2. \tag{3.50}$$

Therefore, we conclude the Theorem 4.16.

3.4 Numerical Results

In this section, we present our numerical experiments for the diameter of a family of 6-regular LPS Ramanujan graphs $X^{5,q}$ and compare it with the diameter of a family of 6-regular random Cayley graphs Z^q. Our numerical experiments show that the ratio of the diameter by the logarithm of the number of vertices $\frac{\text{diam}}{\log_5|X^{5,q}|}$ converges to 4/3 as $q \to \infty$ for the LPS Ramanujan graphs $X^{5,q}$. On the other hand $\frac{\text{diam}}{\log_5|Z^q|}$ converges to 1 as $q \to \infty$ for the random Cayley graphs Z^q .

We give the detailed construction of the LPS Ramanujan graphs $X^{5,29}$ in what follows. The construction of LPS Ramanujan graphs $X^{5,q}$ requires that 5 and -1 to be quadratic residues mod q. From the reciprocity law we deduce that all the prime factors of q are congruent to 1 or 9 mod 20. The least q with such properties is 29. We take the integral solutions $\alpha = (x_0, x_1, x_2, x_3)$ of the following diophantine equation

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = 5, \tag{3.51}$$

where $x_0 > 0$ is odd and x_1, x_2, x_3 are even numbers. There are exactly 6 integral solutions with such properties which are listed below:

$$\big\{(1, \pm 2, 0, 0), (1, 0, \pm 2, 0), (1, 0, 0, \pm 2)\big\}.$$

To each such integral solution $\alpha = (x_0, x_1, x_2, x_3)$, we associates the following matrix in $\text{PSL}_2(\frac{\mathbb{Z}}{29\mathbb{Z}})$:

$$\frac{1}{\sqrt{5}}\begin{bmatrix} x_0 + ix_1 & x_2 + ix_3 \\ -x_2 + ix_3 & x_0 - ix_1 \end{bmatrix}, \tag{3.52}$$

where $\sqrt{5}$ and i are the square root of 5 and -1 mod 29 respectively. We obtain the following 6 matrices in $\mathrm{PSL}_2(\frac{\mathbb{Z}}{29\mathbb{Z}})$

$$S := \left\{ \begin{bmatrix} 10 & 0 \\ 0 & 3 \end{bmatrix}, \begin{bmatrix} 3 & 0 \\ 0 & 10 \end{bmatrix}, \begin{bmatrix} 8 & 16 \\ 13 & 8 \end{bmatrix}, \begin{bmatrix} 21 & 16 \\ 13 & 21 \end{bmatrix}, \begin{bmatrix} 21 & 11 \\ 11 & 21 \end{bmatrix}, \begin{bmatrix} 8 & 11 \\ 11 & 8 \end{bmatrix} \right\},$$

which generate $\mathrm{PSL}_2(\frac{\mathbb{Z}}{29\mathbb{Z}})$. The LPS Ramanujan graph $X^{5,29}$ is the Cayley graph of $\mathrm{PSL}_2(\frac{\mathbb{Z}}{29\mathbb{Z}})$ with the generator set S. The Ramanujan graph $X^{5,29}$ has 12180 vertices with diameter 8. We note that

$$\lceil \frac{4}{3} \log_5(12180) \rceil = 8.$$

We show the level structure of $X^{5,29}$ with root $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in table 3.1. We note that the girth of this graph is 8

$$\mathrm{girth}(X^{5,29}) = 8.$$

and this means a ball of radius 4 in the graph $X^{5,29}$ is a tree as illustrated in Figure 3.1. For the family of LPS bipartite Ramanujan graphs, Biggs and Boshier determined the asymptotic behavior of the girth of these graphs; see [BB90]. They showed that the girth is asymptotic to

$$(\frac{4}{3}) \log_{k-1}(n).$$

r (Distance from $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$)	$N(r)$ (Number of vertices of $X^{5,29}$ with distance r from $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$)
0	1
1	6
2	30
3	150
4	750
5	3026
6	5970
7	2195
8	52

Table 3.1: Level structure of the LPS Ramanujan graphs $X^{5,29}$

We give the diameter of the LPS Ramanujan graphs $X^{5,q}$ for $1 \leq q \leq 229$ in Table 3.2.

We note that $\frac{\mathrm{diam}}{\log_5 n}$ are close to $\frac{4}{3}$. These numerical experiments are consistent with our conjectures on optimal strong approximation for quadratic forms in 4 variables [TS15]. The conjec-

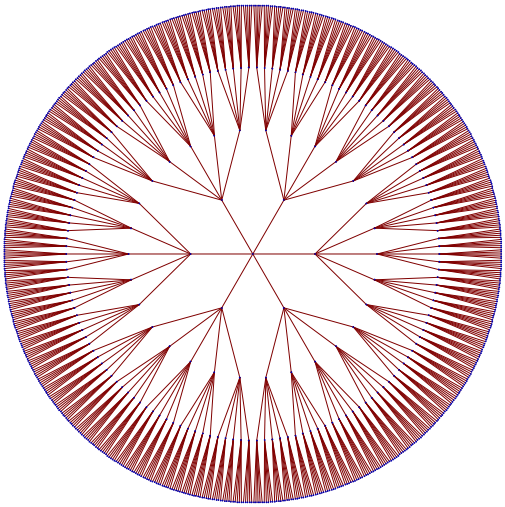


Figure 3.1: A ball of radius 4 in the LPS Ramanujan graphs $X^{5,29}$.

q	number of vertices of $X^{5,q}$	Diameter	$\frac{\text{diam}}{\log_5 n}$
29	12180	8	1.36
41	34440	9	1.38
61	113460	9	1.24
89	352440	11	1.38
101	515100	11	1.34
109	647460	11	1.32
149	1653900	12	1.34
181	3375540	14	1.51
229	6004380	13	1.34

Table 3.2: LPS Ramanujan graphs $X^{5,q}$

ture implies that for the LPS Ramanujan graphs $X^{p,q}$ where p is a fixed prime number, the ratio $\frac{\text{diam}(X^{p,q})}{\log_{p-1}|X^{p,q}|}$ converges to $\frac{4}{3}$ as $q \to \infty$.

Finally, we give our numerical experiments for the diameter of the 6-regular random Cayley graphs $\text{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$. To compare the diameter of the random Cayley graphs with that of the LPS Ramanujan graphs given above, we choose the same set of integers q. We generate 8 random samples for each q, and we give the averaged ratio $\frac{\text{diam}}{\log_5 n}$ in the last column of Table 3.3.

($8^{\times 6}9^{\times 2}$ means that 6 of our random samples are 8 and 2 of them are 9). We note that the

q	number of vertices of Z^q	Diameter	$\frac{\text{diam}}{\log_5 n}$
29	12180	$8^{\times 6}9^{\times 2}$	1.50
41	34440	$9^{\times 4}8^{\times 4}$	1.30
61	113460	$9^{\times 5}10^{\times 3}$	1.29
89	352440	$10^{\times 5}11^{\times 3}$	1.30
101	515100	$10^{\times 5}11^{\times 3}$	1.26
109	647460	$10^{\times 4}11^{\times 4}$	1.26
149	1653900	$11^{\times 6}12^{\times 2}$	1.25
181	3375540	$11^{\times 3}12^{\times 5}$	1.24
229	6004380	$12^{\times 8}$	1.23

Table 3.3: Random Cayley graphs $\text{PSL}_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$ with 6 generators

empirical mean of the ratio $\frac{\text{diam}(Z_q)}{\log_5 |Z_q|}$ is decreasing in q and one can easily show that

$$\frac{\text{diam}(Z_q)}{\log_5 |Z_q|} \geq 1.$$

Based on our numerical experiments, we expect that $\frac{\text{diam}(Z_q)}{\log_5 |Z_q|}$ converges to 1 in probability as $q \to \infty$ for random Cayley graphs Z^q .

Chapter 4

Quadratic forms and semiclassical eigenfunction hypothesis for flat tori

4.1 Introduction

4.1.1 Semiclassical eigenfunction hypothesis for flat tori

We begin by describing the main application of this Chapter. Let $\mathbb{T}^d := \frac{\mathbb{R}^d}{\mathbb{Z}^d}$ be the flat torus of dimension $d \geq 2$ with the laplacian operator $\Delta := \frac{1}{(2\pi)^2}(\frac{\partial^2}{\partial\theta_1} + \cdots + \frac{\partial^2}{\partial\theta_d})$, and $\{\psi_i\}$ an orthonormal basis of eigenfunctions. Marklof and Rudnick [MR12] showed that for flat torus $\mathbb{T}^d$ there is a density one subsequence of any orthonormal basis $\{\psi_i\}$ such that $|\psi_i|^2$ converges weakly to the uniform distribution in $\mathbb{T}^d$, i.e. for any continuous function f on $\mathbb{T}^d$

$$\int_{\mathbb{T}^d} |\psi_n(x)|^2 f(x) d\text{vol}(x) \to \int_{\mathbb{T}^d} f(x) d\text{vol}(x) \text{ as } n \to \infty.$$

M.V. Berry [Ber77, Ber83] in his work on the " Semiclassical Eigenfunction Hypothesis" suggested to go beyond this weak convergence, and study the equidistribution of $|\psi_n|^2$ on small scale. Recently, Lester and Rudnick [LR15] prove the equidistribution of a density one subsequence of $\{\psi_i\}$ in an optimal small scale on the flat torus $\mathbb{T}^d$ for $d \geq 2$. Density one means if we order the eigenfunctions by their eigenvalue then the subsequence contains a density one subset of the basis. More precisely,

they show that along a density one subsequence of the orthonormal basis $\{\psi_n\}$,

$$\lim_{n\to\infty} \sup_{B(y,r)} \Big| \frac{1}{\mathrm{vol}(B(y,r))} \int_{B(y,r)} |\psi_n(x)|^2 d\mathrm{vol}(x) - 1 \Big| = 0, \tag{4.1}$$

where ψ_n is an eigenfunction with eigenvalue λ_n and $B(y,r)$ is any ball of radius $r > \lambda_n^{-\frac{1}{2(d-1)}+o(1)}$ centered at an arbitrary point $x \in \mathbb{T}^d$. The exponent $-\frac{1}{2(d-1)}$, for the size of the ball, is optimal. Moreover, for dimension 3 and 4, they prove a stronger result. They prove the small scale equidistribution holds for almost every eigenfunction in individual eigenspace with the optimal exponent $-\frac{1}{2(d-1)}$ and they conjecture that the same result holds for every $d \geq 5$. The main application of this Chapter is to resolve this conjecture. In what follows, we explain their result and conjecture in detail and how it is reduced to counting pairs of integral points with small distance on sphere.

We note that if $d \geq 4$ then the set of eigenvalues of the laplacian Δ on $\mathbb{T}^d$ are given by the set of non-negative integers $\{n \in \mathbb{Z} : n \geq 0\}$. We denote the associated eigenspace by E_n. It is well-known that the dimension of this space is equal to the number of integral points on sphere of radius $\sqrt{n}$ in $\mathbb{R}^d$. Therefore, for $d \geq 5$, the multiplicity of each eigenvalue n is large and grow like a scalar multiple of $n^{\frac{d-2}{2}}$. The intersection of the orthonormal basis of eigenfunctions $\{\psi_i\}$ with E_n gives us an orthonormal basis of eigenfunctions for E_n. We denote this orthonormal basis of E_n by $B_n := E_n \cap B$. Lester and Rudnick [LR15] prove that there exists a large subset $C_n \subset B_n$, which means $|C_n| = (1 - o(1))|B_n|$, such that along any sequence of $\{\psi_n : \psi_n \in C_n\}$

$$\lim_{n\to\infty} \sup_{B(y,r)} \Big| \frac{1}{\mathrm{vol}(B(y,r))} \int_{B(y,r)} |\psi_n(x)|^2 d\mathrm{vol}(x) - 1 \Big| = o(1), \tag{4.2}$$

where $B(y,r)$ is any ball of radius $r > \lambda_n^{-\frac{1}{2(d-1)}+o(1)}$ centered at an arbitrary point $x \in \mathbb{T}^d$. This means that we can choose our density one subsequence so that it contains a large proportion of the basis restricted to each eigenspace. In this thesis we prove the analogue of this result for $d \geq 5$.

Corollary 4.1.1 *Let $\mathbb{T}^d := \mathbb{R}^d/\mathbb{Z}^d$ be a $d \geq 5$ dimensional flat torus and $\{\psi_i\}$ an orthonormal basis of eigenfunctions for the laplacian operator. Let E_n be the associated eigenspace for eigenvalue $n \in \mathbb{Z} \geq 0$ and $B_n := E_n \cap \{\psi_i\}$ be the restriction of the orthonormal basis $\{\psi_i\}$ to E_n. Then there exists a large subset $C_n \subset B_n$, which means $|C_n| = (1 - o(1))|B_n|$, such that along any sequence of $\{\psi_n : \psi_n \in C_n\}$*

$$\lim_{n\to\infty} \sup_{B(y,r)} \Big| \frac{1}{vol(B(y,r))} \int_{B(y,r)} |\psi_n(x)|^2 dvol(x) - 1 \Big| = o(1), \tag{4.3}$$

where $B(y,r)$ is any ball of radius $r > \lambda_n^{-\frac{1}{2(d-1)}+o(1)}$ centered at an arbitrary point $x \in \mathbb{T}^d$. The

exponent $-\frac{1}{2(d-1)}$ *is optimal. In fact there exists a sequence of balls with radius* $r \approx \lambda_n^{-\frac{1}{2(d-1)}-o(1)}$ *and an orthonormal basis* $\{\psi_i\}$ *where (4.3) does not hold for a positive proportion of eigenfunctions in* B_n.

4.1.2 Local statistics of integral points on sphere

In this section we explain Lester and Rudnick's [LR15][Remark 5.4] observation that the small scale equidistribution for individual eigenspace on flat tori is related to counting pairs of integral points with small distance on sphere.

Let $\psi \in B_n$ be an orthonormal function in our basis then we can write

$$\psi(\theta) = \sum_{\lambda \in \mathbb{Z}^d, \|\lambda\|^2 = n} c_\lambda(\psi) e(\langle \lambda, \theta \rangle), \tag{4.4}$$

where

$$\sum_{\lambda \in \mathbb{Z}^d, \|\lambda\|^2 = n} \|c_\lambda(\psi)\|^2 = 1. \tag{4.5}$$

Since B_n is an orthonormal basis for E_n, similarly if we fix $\lambda \in \mathbb{Z}^d$ we also obtain

$$\sum_{\psi \in B_n} \|c_\lambda(\psi)\|^2 = 1. \tag{4.6}$$

Lester and Rudnick estimate the indicator function of the ball $B(x,r)$ by the majorant and minorant Beurling-Selberg trigonometric polynomials $a^{\pm}(\theta)$ on the flat torus $\mathbb{T}^d$ such that

$$\begin{aligned} a(\theta)^{\pm} &= \sum_{\xi \in \mathbb{Z}^d} a(\xi) e(\langle \theta, \xi \rangle), \\ a^{\pm}(0)^{\pm} &= \mathrm{vol}(B(x,r)) + O(r^{d-o(1)}), \\ \hat{a}(\xi)^{\pm} &= 0 \text{ if } |\xi| > n^{\frac{1}{2(d-1)}-o(1)}, \\ \left|\hat{a}(\xi)^{\pm}\right| &\leq r^d. \end{aligned}$$

Then one can estimate from below and above the local integral (4.3) by using the trigonometric polynomials $a^{\pm}$ and reduce the problem into counting pairs of integral points with small distance

on the sphere. We include a brief exposition of this reduction in what follows

$$\begin{aligned}\frac{\int_{\mathbb{T}^d}\|\psi\|^2 a^{\pm}(\theta)d\theta}{a^{\pm}(0)}-1 &= \int\big|\sum_{\lambda}c_\lambda(\psi)e(\langle\lambda,\theta\rangle)\big|^2\big(\sum_{\xi}\frac{\hat{a}^{\pm}(\xi)}{\hat{a}^{\pm}(0)}e(\langle\xi,\theta\rangle)\big)d\theta\\ &= \sum_{\lambda-\lambda'=\xi}c_\lambda(\psi)\bar{c}_{\lambda'}\frac{\hat{a}^{\pm}(\xi)}{\hat{a}^{\pm}(0)}\\ &\ll \sum_{0<\|\lambda-\lambda'\|\leq n^{\frac{1}{2(d-1)}-o(1)}}\|c_\lambda(\psi)\|^2+\|c_{\lambda'}(\psi)\|^2.\end{aligned}$$

Average this inequality over $\psi\in B_n$ and use the identity (4.6) to obtain

$$\begin{aligned}\sum_{\psi\in B_n}\Big[\sup_{B(y,r)}\Big|\frac{1}{\mathrm{vol}(B(y,r))}\int_{B(y,r)}|\psi(x)|^2 d\mathrm{vol}(x)-1\Big|\Big]&\\ \leq \frac{1}{|B(n)|}\sum_{0<\|\lambda-\lambda'\|\leq n^{\frac{1}{2(d-1)}-o(1)}}1.&\end{aligned}$$

Note that the right hand side of the above inequality is the average over the pair of integral points $\lambda\neq\lambda'$ on the sphere of radius $\sqrt{n}$ where their distance is less than $n^{\frac{1}{2(d-1)}-o(1)}$. For a large integer n, let

$$E(n)=E_d(n)=\{x\in\mathbb{Z}^d:|x|^2=n\},$$

be the set of integral lattice points on the sphere $\sqrt{n}S^{d-1}$ of radius $\sqrt{n}$. For any $Y\ll\sqrt{n}$, and $|x|^2=n$, let

$$\mathrm{cap}(x;n,Y):=\{y\in\sqrt{n}S^{d-1},|x-y|\leq Y\},$$

be the spherical cap of size Y around the point x on the sphere $\sqrt{n}S^{d-1}$. Given a point $x\in E(n)$, let

$$\mu(x;n,Y):=|\mathrm{cap}(x;n,Y)\cap\mathbb{Z}^d|-1,$$

be the number of other lattice points in the cap around x. The mean of $\mu(x;n,Y)$, averaged over all lattice points $E(n)$ is:

$$\langle\mu(\bullet;n,Y)\rangle:=\frac{1}{|E(n)|}\sum_{x\in E(n)}\big(|\mathrm{cap}(x;n,Y)\cap\mathbb{Z}^d|-1\big).$$

We note that $|E(n)|\approx n^{\frac{d-2}{2}}$ when $d\geq 5$ and the volume of $\sqrt{n}S^{d-1}$ is $\approx n^{\frac{d-1}{2}}$. Heuristically, if

we assume that the integral points are uniformly distributed, then we expect to have $\frac{Y^{d-1}}{n^{\frac{1}{2}}}$ integral points inside a cap of size Y. So, if $Y \ll n^{\frac{1}{2(d-1)}-o(1)}$ then we expect to have no integral points inside a cap of size Y. On the other hand, if $n^{\frac{1}{2(d-1)}+o(1)} \ll Y$ then we expect to have many points. In fact, we have the following corollary of our main theorem that makes this heuristic rigorous.

Corollary 4.1.2 *Let $d \geq 5$. Assume that Y, the size of the caps, satisfies*

$$n^{\frac{1}{2(d-1)}+o(1)} \ll Y \ll n^{1/2}.$$

Then the probability that a cap of size Y centered at integral point has more than $\log(n)$ points is greater than $1/2$

$$\mathbb{P}\big[\mu(\bullet; n, Y) > \log(n)\big] > 1/2,$$

as a result

$$\langle \mu(\bullet; n, Y) \rangle \to \infty \text{ as } n \to \infty.$$

On the other hand, if $Y \ll n^{\frac{1}{2(d-1)}-o(1)}$, then

$$\langle \mu(\bullet; n, Y) \rangle \to 0 \text{ as } n \to \infty.$$

Remark 4.1.3 *Lester and Rudnick [LR15][Remark 5.4] remarked that the small scale equidistributin for individual eigenspace as stated in Corollary 4.1.1 is implied from*

$$\langle \mu(\bullet; n, Y) \rangle \to 0 \text{ as } n \to \infty,$$

where $Y \ll n^{\frac{1}{2(d-1)}-o(1)}$. Bourgain [LR15][Theorem 4.1] show that the exponent $-\frac{1}{2(d-1)}$ is optimal by using the fact that

$$\mathbb{P}\big[\mu(\bullet; n, Y) > 2\big] > 1/2.$$

Therefore corollary 4.1.2 implies the corollary 4.1.1.

4.1.3 Main theorem

In our main Theorem (4.1.4), we give an uniform upper bound on the number of integral points on a quadric that is defined by any positive definite integral primitive quadratic form with discriminant D in $k \geq 4$ variables. First, we state our main theorem.

Theorem 4.1.4 *Let n be any integer, and let $Q(X)$ be any primitive positive definite integral quadratic form of discriminant D in $k \geq 4$ variables. If $D \ll n^{\frac{k-3}{2(k-2)}}$, then the number of integral solutions of $Q(X) = n$ is bounded from above by*

$$c_\epsilon \frac{n^{\frac{k-2}{2}}}{\sqrt{D}} \gcd(D, n)^{1/2} n^\epsilon, \tag{4.7}$$

where c_ϵ is a constant which depends only on ϵ and not on $Q(X)$ or n.

4.1.4 Outline of the chapter

We give a brief outline of this chapter. In section (4.2), we show that corollary (4.1.2) is a consequence of our main Theorem (4.1.4). Next, we give a proof of our main Theorem (4.1.4). In the proof of Theorem (4.1.4), we use an improved version of a lemma in Blomer's papers [Blo04, Lemma 4.2] or [Blo08, Lemma 3]. Professor Blomer provided us a proof for this improved version of his previous lemma.We include his proof in our appendix. We are responsible for any gap or typo in the appendix.

We begin by introducing some notations. We write $r(Q, n)$ for the number of integral solutions of

$$Q(X) = n.$$

We consider the Theta series associated to this quadratic form

$$\Theta(z) = \sum_n r(Q, n) e(nz).$$

This is a modular form of weight $k/2$ and level N, where N is the smallest integer such that NL^{-1} is an integral matrix where L is the symmetric matrix associated to the quadratic form Q . From the theory of modular forms we can write $\Theta(z)$ uniquely as a sum of standard Eisenstein series $E(z, Q)$ (the Eisenstein series of the form Q) and a cusp form $F(z, Q)$

$$\Theta(z) = E(z, Q) + F(z, Q).$$

From this decomposition

$$r(Q, n) = \rho(n, Q) + \tau(n, Q).$$

where, $\rho(n, Q)$ and $\tau(n, Q)$ are the n-th Fourier coefficients of $E(z, Q)$ and $F(z, Q)$ respectively. In Lemma (4.3.1), we use the Siegel product formula (The main term of the Hardy-Littlewood formula) to give an upper bound on $\rho(n, Q)$. In Lemma (4.3.3), we invoke the upper bound of Blomer [Blo04, Lemma 4.2] on $\|F(z, Q)\|^2$ and then we apply the Petersson trace formula to give an upper bound on $\tau(n, Q)$. The theorem is a consequence of lemma (4.3.1) and lemma (4.3.3).

4.2 Proof of corollary (4.1.2)

We begin by proving the first part of Corollary (4.1.2) when the size of the caps is large, i.e.

$$n^{\frac{1}{2(d-1)}+o(1)} \ll Y \ll n^{1/2}.$$

This part is elementary; we use a covering argument in combination with a pigeonhole argument. We assume that $n^{\frac{1}{2(d-1)}+o(1)} \ll Y$. Call an integral point $p \in E(n)$ *bad* if

$$\mu(p; n, Y) \leq \log(n).$$

We denote the number of bad points by B. Assume to the contrary that $B \geq \frac{1}{2}|E(n)|$. Hence, using $|E(n)| \approx n^{\frac{d-2}{2}}$, $B \gg n^{\frac{d-2}{2}}$. Consider balls of radius $\frac{Y}{2}$ centered at each bad point. Each point of the sphere is covered by at most $\log(n)$ of these balls; otherwise, there are more than $\log(n)$ bad points with distance at most Y, contradicting the definition of a bad point. Therefore, we have the following inequality from a covering argument

$$B(Y/2)^{d-1} \ll n^{\frac{d-1}{2}} \log(n).$$

Hence,

$$Y^{d-1} \ll n^{1/2} \log(n).$$

This is a contradiction to $Y \gg n^{\frac{1}{2(d-1)}+o(1)}$. Therefore, $B < \frac{1}{2}|E(n)|$. Consequently,

$$\mathbb{P}[\langle \mu(\bullet; n, Y)\rangle > \log(n)] > 1/2,$$

Therefore,

$$\langle \mu(\bullet; n, Y)\rangle \to \infty \text{ as } n \to \infty.$$

This concludes the proof of the first part.

Lemma 4.2.1 *The second part of the Corollary (4.1.2) is a consequence of the inequality*

$$A_d(n,t) \ll n^{\frac{d-3}{2}+\varepsilon} \gcd(n,t)^{1/2}(n-t)^{\frac{d-3}{2}},$$

where $n - n^{\frac{1}{(d-1)}-o(1)} < t < n$ *and* $5 \leq d$.

Proof 4.2.2 *For the second part of Corollary (4.1.2), when the size of caps is small, i.e.*

$$Y \ll n^{\frac{1}{2(d-1)}-o(1)},$$

we follow the technique in the argument for [LR15, lemma 11] to prove lemma (4.2.1). Let $A_d(n,t)$ *be the number of ordered pairs of distinct integral lattice points* $(p,q) \in \mathbb{Z}^d \times \mathbb{Z}^d$ *such that* $|p|^2 = |q|^2 = n$ *and* $|p-q|^2 = 2(n-t)$. *Note that a change of summation argument gives us the equality*

$$\langle \mu(\bullet; n, Y)\rangle = \frac{1}{|E(n)|} \sum_{n-\frac{Y^2}{2}<t<n} A_d(n,t).$$

Since $Y \ll n^{\frac{1}{2(d-1)}-o(1)}$ *and* $n - \frac{Y^2}{2} < t < n$, *so* $n - n^{\frac{1}{(d-1)}-o(1)} < t < n$ *and we can apply the inequality*

$$A_d(n,t) \ll n^{\frac{d-3}{2}+\varepsilon} \gcd(n,t)^{1/2}(n-t)^{\frac{d-3}{2}},$$

and we obtain

$$\begin{aligned}
\langle \mu(\bullet; n, Y) \rangle &\ll \frac{1}{|E(n)|} \sum_{n-\frac{Y^2}{2}<t<n} n^{\frac{d-3}{2}+\varepsilon} \gcd(n,t)^{1/2} (n-t)^{\frac{d-3}{2}} \\
&\ll \frac{n^{\frac{d-3}{2}+\varepsilon}}{|E(n)|} \sum_{n-\frac{Y^2}{2}<t<n} \gcd(n,t)^{1/2} (n-t)^{\frac{d-3}{2}} \\
&\ll \frac{n^{\frac{d-3}{2}+\varepsilon}}{|E(n)|} \sum_{1<s<\frac{Y^2}{2}} \gcd(n,s)^{1/2} s^{\frac{d-3}{2}} \ (\textit{where } s := n-t) \\
&\ll \frac{n^{\frac{d-3}{2}+\varepsilon} Y^{d-1} n^{\varepsilon}}{|E(n)|}.
\end{aligned}$$

Using $|E(n)| \approx n^{\frac{d-2}{2}}$ *and* $Y \ll n^{\frac{1}{2(d-1)}-o(1)}$*, we get*

$$\langle \mu(\bullet; n, Y) \rangle \ll n^{\varepsilon - o(1)} \to 0 \ \textit{as} \ n \to \infty.$$

Lemma (4.2.3) is devoted to showing that the following inequality in lemma (4.2.1) is true:

$$A_d(n,t) \ll n^{\frac{d-3}{2}+\varepsilon} \gcd(n,t)^{1/2} (n-t)^{\frac{d-3}{2}}$$

for $n - n^{\frac{1}{(d-1)}-o(1)} < t < n$ and $5 \leq d$.

Lemma 4.2.3 *Theorem (4.1.4) implies that*

$$A_d(n,t) \ll n^{\frac{d-3}{2}+\varepsilon} \gcd(n,t)^{1/2} (n-t)^{\frac{d-3}{2}}$$

where $n - n^{\frac{1}{(d-1)}-o(1)} < t < n$ *and* $5 \leq d$.

Proof 4.2.4 *Recall that* $A_d(n,t)$ *is the number of ordered pairs of distinct integral lattice points* $(p,q) \in \mathbb{Z}^d \times \mathbb{Z}^d$ *such that* $|p|^2 = |q|^2 = n$ *and* $|p-q|^2 = 2(n-t)$*. Let* $v := p - q$*. Note that* v *is an integral vector of length* $\sqrt{2(n-t)}$ *and so, up to a constant, we have at most*

$$(n-t)^{\frac{d-2}{2}} \tag{4.8}$$

choices for v, because $d \geq 5$. Note that

$$\langle p+q, v\rangle = 0,$$

and

$$|p+q|^2 = 2(n+t).$$

Let L be the $(d-1)$-dimensional lattice that is given by the intersection of $\mathbb{Z}^d$ and the hyperplane orthogonal to v. Therefore, $p+q$ lies inside the lattice L and the sphere of radius $\sqrt{2(n+t)}$. The fundamental domain of the lattice L has volume $|v'|$ where v' is the primitive integral vector in the direction of v. We take an integral basis for the lattice L and denote it by

$$\{e_1, \ldots, e_{d-1}\}.$$

We define the symmetric matrix A by

$$A := \left[\langle e_i, e_j \rangle_{1 \leq i,j \leq d-1} \right].$$

We define the quadratic form $Q(X)$ by

$$Q(X) := X^T A X.$$

This quadratic from is a primitive quadratic form in $(d-1) \geq 4$ variables with discriminant $D := |v'|^2$. We have the following upper bound on the discriminant of Q

$$D = |v'|^2 \leq n^{\frac{1}{(d-1)} - o(1)}.$$

Since $\frac{1}{(d-1)} \leq \frac{d-4}{2(d-3)}$ when $d \geq 5$ we also have

$$D \ll n^{\frac{d-3}{2(d-2)}}.$$

We can apply theorem 4.1.4, and as a consequence we have the following bound on the number of lattice points of L with norm $2(n+t)$

$$c_\epsilon \frac{(2(n+t))^{\frac{d-3}{2}}}{|v'|} \gcd(2(n-t), 2(n+t))^{1/2} (2(n+t))^{\epsilon} \ll \frac{n^{\frac{d-3}{2}}}{|v'|} \gcd(n,t)^{1/2} n^{\epsilon}.$$

Recall that $|v|^2 = |p-q|^2 = 2(n-t)$ *and the number of integral points* v *where* $\frac{|v|}{|v'|} = l$ *is less than* $\left(\frac{n-t}{l^2}\right)^{\frac{d-2}{2}+\epsilon}$ *up to a constant. We give an upper bound on* $A_d(n,t)$ *by first choosing* $v = p-q$ *and then* $p+q$

$$A_d(n,t) \ll \sum_{l^2|2(n-t)} (\frac{n-t}{l^2})^{\frac{d-2}{2}} \frac{n^{\frac{d-3}{2}}}{\frac{\sqrt{n-t}}{l}} \gcd(n,t)^{1/2} n^{\epsilon}.$$

Therefore,

$$A_d(n,t) \ll n^{\frac{d-3}{2}+\epsilon} \gcd(n,t)^{1/2} (n-t)^{\frac{d-3}{2}}.$$

4.3 Proof of the Main thoerem

We write $r(Q,n)$ for the number of integral solutions of

$$Q(X) = n.$$

We consider the theta series associated to this quadratic form

$$\Theta(z) = \sum_n r(Q,n) e(nz),$$

This is a modular form of weight $\frac{k}{2}$ and level N, where N is the smallest integer such that NL^{-1} is an integral matrix . From the theory of modular forms we can write $\Theta(z)$ uniquely as a sum of standard Eisenstein series $E(z,Q)$ (the Eisenstein series of the form Q) and a cusp form $F(z,Q)$

$$\Theta(z) = E(z,Q) + F(z,Q).$$

From this decomposition

$$r(Q,n) = \rho(n,Q) + \tau(n,Q).$$

where, $\rho(n,Q)$ and $\tau(n,Q)$ are the n-th Fourier coefficients of $E(z,Q)$ and $F(z,Q)$ respectively. In Lemma 4.3.1, we use the Siegel product formula (The main term of the Hardy-Littlewood formula) to give an upper bound on $\rho(n,Q)$. In Lemma 4.3.3, we invoke the upper bound of Blomer on $\|F(z,Q)\|^2$ in Lemma (4.3.5) that is proved in our appendix. Finally we apply the Petersson trace formula together with a Cauchy inequality to give an upper bound on the n-th Fourier coefficient $\tau(n,Q)$ of $F(z,Q)$. Theorem (4.1.4) is a consequence of lemma (4.3.1) and lemma (4.3.3).

The following lemma proved by Blomer [Blo08, page 6] for $k = 3$. We follow his strategy and

give a proof for every $k \geq 4$.

Lemma 4.3.1 *We have the following upper bound on the n-th Fourier coefficient of the Eisenstein series of the form Q*

$$\rho(n, Q) \leq c_\epsilon \frac{n^{\frac{k-2}{2}}}{\sqrt{D}} \gcd(N, n)^{1/2} (nN)^\epsilon,$$

where N is the level of the quadratic from Q.

Proof 4.3.2 *$\rho(n, Q)$, the n-th Fourier coefficient of the Eisenstein series, coincides with the main term of the Hardy-Littlewood formula. The main term of the Hardy-Littlewood formula, is given by the product of local densities*

$$\rho(n, Q) := n^{\frac{k-2}{2}} \sigma_\infty \prod_p \sigma_p.$$

We have the following formula for the local densities:

$$\sigma_p = \sum_{t=0}^{\infty} S(p^t),$$

where

$$S(p^t) := \frac{1}{p^{tk}} \sum_a^* \sum_b e\Big(\frac{a(Q(b) - n)}{p^t}\Big)$$

($\sum_a^*$ means $\gcd(a, p) = 1$ and that a varies mod p^t, b is a vector that varies mod $p^t\mathbb{Z}$, and S(1)=1).

We give an upper bound for each place. First, we start with ∞. The density at ∞ is given by

$$\sigma_\infty = \lim_{\epsilon \to 0} \frac{\int_{1<Q(X)<1+\epsilon} 1 dx_1 \dots dx_k}{\epsilon}.$$

We diagonalize $Q(X)$ in an orthonormal coordinates $Y := (y_1, \dots, y_k)$ such that

$$Q(Y) := n_1 y_1^2 + \dots + n_k y_k^2.$$

where $n_1, \dots, n_k$ are the eigenvalues of the symmetric matrix A. We change the variables to $(y_1, \dots, y_k)$ to get

$$\sigma_\infty = \frac{1}{\sqrt{detA}} vol(S^{k-1}).$$

Next, we give an upper bound on the local densities σ_p where $p \neq 2$. Since p is an odd prime number, we can diagonalize our quadratic form $Q(X)$ over the local ring $\mathbb{Z}_p$. Without loss of generality we

assume that

$$Q(x_1,\dots,x_k)=\sum_{i=1}^{k}a_ip^{\alpha_i}x_i^2,$$

where $\gcd(a_i,p)=1$ *and* $a_i\in\mathbb{Z}_p$. *We substitute the diagonal expansion of* $Q(x_1,\dots,x_k)$ *to compute* $S(p^t)$

$$\begin{aligned}S(p^t)&:=\frac{1}{p^{tk}}\sum_{a}^{*}\sum_{b\in(\frac{\mathbb{Z}}{p^t\mathbb{Z}})^k}e\Big(\frac{a(Q(b)-n)}{p^t}\Big)\\&=\frac{1}{p^{tk}}\sum_{a}^{*}\sum_{b\in(\frac{\mathbb{Z}}{p^t\mathbb{Z}})^k}e\Big(\frac{a(\sum_{i=1}^{k}a_ip^{\alpha_i}b_i^2-n)}{p^t}\Big)\\&=\frac{1}{p^{tk}}\sum_{a}^{*}e\Big(\frac{-an}{p^t}\Big)\prod_{i=1}^{k}\sum_{b\ mod\ p^t}e\Big(\frac{aa_ip^{\alpha_i}b^2}{p^t}\Big).\end{aligned}$$

We note that the last summation is a Gauss sum. Let $G(h,m):=\sum_{x\ mod\ m}e(\frac{hx^2}{m})$ *be the Gauss sum, and let* $\epsilon_m=1$ *if* $m\equiv 1(\ mod\ 4)$ *and* $\epsilon_m=i$ *if* $m\equiv 3(\ mod\ 4)$. *Then if* $\gcd(h,m)=1$ *we have*

$$G(h,m):=\begin{cases}\epsilon_m\Big(\frac{h}{m}\Big)m^{1/2} & \text{if } m \text{ is odd},\\ (1+\chi_{-4}(h))m^{1/2} & \text{if } m=4^{\alpha},\\ (\chi_8(h)+i\chi_{-8}(h))m^{1/2} & \text{if } m=2.4^{\alpha},\alpha\geq 1.\end{cases}$$

where $\Big(\frac{h}{m}\Big)$ *is the Jacobi symbol. We have*

$$S(p^t)=\frac{1}{p^{tk}}\sum_{a}^{*}e\Big(\frac{-an}{p^t}\Big)\prod_{i=1}^{k}p^{\min(\alpha_i,t)}G(aa_i,p^{t-\alpha_i}).$$

We define $G(\bullet,p^{t-\alpha_i}):=1$ *when* $t<\alpha_i$. *We substitute the values of* G *and obtain,*

$$|S(p^t)|=\frac{\prod_{i=1}^{k}p^{\min(\frac{\alpha_i+t}{2},t)}}{p^{tk}}\Big|\sum_{a}^{*}e\Big(\frac{-an}{p^t}\Big)\Big(\frac{a}{p}\Big)^{k'}\Big|,$$

where k' *is the number of integers* i *such that* $1\leq i\leq k$ *and* $t-\alpha_i$ *is a positive odd integer. Assume that* $n=p^{\beta}n'$, *where* $\gcd(n',p)=1$. *If* k' *is an odd number then the inner sum is a Gaussian sum, and we obtain*

$$\Big|\sum_{a\ mod\ p^t}^{*}e\Big(\frac{-ap^{\beta}n'}{p^t}\Big)\Big(\frac{a}{p}\Big)\Big|=\begin{cases}p^{t-\frac{1}{2}} & \text{if } \beta=t-1,\\ 0 & \text{otherwise}.\end{cases}$$

Hence, if k' is odd we deduce that

$$|S(p^t)| = \begin{cases} \frac{\prod_{i=1}^{k} p^{\min(\frac{\alpha_i+t}{2},t)}}{p^{tk}} p^{t-\frac{1}{2}} & \text{if } \beta = t-1, \\ 0 & \text{otherwise.} \end{cases} \tag{4.9}$$

On the other hand, if k' is even then the inner sum is a Ramanujan sum $c_{p^t}(n)$,

$$c_{p^t}(n) = \sideset{}{^*}\sum_{a} e\Big(\frac{-an}{p^t}\Big) = \begin{cases} 0 & \text{if } \beta < t-1, \\ -p^{t-1} & \text{if } \beta = t-1, \\ \phi(p^t) & \text{if } \beta \geq t. \end{cases}$$

Hence, if k' is even we deduce that

$$|S(p^t)| = \begin{cases} 0 & \text{if } \beta < t-1, \\ -\frac{\prod_{i=1}^{k} p^{\min(\frac{\alpha_i+t}{2},t)}}{p^{tk}} p^{t-1} & \text{if } \beta = t-1, \\ \phi(p^t)\frac{\prod_{i=1}^{k} p^{\min(\frac{\alpha_i+t}{2},t)}}{p^{tk}} & \text{if } \beta \geq t. \end{cases} \tag{4.10}$$

Without loss of generality suppose that $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_k$. Since $Q(X)$ is primitive we deduce that $\alpha_1 = 0$. If k' is odd (4.9) and if k' is even (4.10), we deduce that

$$\begin{aligned} |\sigma_p| &\leq \sum_{t=0}^{\beta+1} p^{t/2} \frac{\prod_{i=2}^{k} p^{\min(\frac{\alpha_i+t}{2},t)}}{p^{tk}} p^{\min(t,\frac{t+\beta}{2})} \\ &\leq \sum_{t=0}^{\beta+1} \frac{p^{t/2} p^{(k-1)\min(\frac{\alpha_k+t}{2},t)} p^{\min(t,\frac{t+\beta}{2})}}{p^{tk}} \end{aligned} \tag{4.11}$$

From the above inequality and the condition that $k \geq 4$, we give an upper bound on the product of local densities $\prod_{p\nmid 2nN} \sigma_p$ as follows.

$$\begin{aligned} \prod_{p\nmid 2nN} \sigma_p &\leq \prod_{p\nmid 2nN} (1 + p^{-\frac{k-1}{2}}) \\ &\leq \sum_{n=1}^{\infty} \frac{1}{n^{3/2}} = O(1) \end{aligned} \tag{4.12}$$

If p is an odd prime number from the inequality (4.11), we obtain

$$\sigma_p \ll p^{\frac{\min(\alpha_k,\beta)}{2}}$$

Hence, for odd prime numbers where $p|nN$ we have

$$\prod_{p|nN} \sigma_p \leq (nN)^{\epsilon} \gcd(n,N)^{1/2} \tag{4.13}$$

Finally, we assume that $p = 2$. One can write any quadratic form $Q(X)$, after a change of variables over the 2-adic integers $\mathbb{Z}_2$, as a direct sum of scalar multiples of $q_0(x) := x^2$, $q_1(x_1, x_2) := x_1x_2$ and $q_2(x_1, x_2) := x_1^2 + x_1x_2 + x_2^2$. The corresponding Gauss sums can be evaluated for odd h:

$$\sum_{b_1,b_2 \ mod \ 2^t} e\big(\frac{2^{\alpha_1}x_1x_2h}{2^t}\big) = 2^{\min(t+\alpha_1,2t)},$$

and

$$\sum_{b_1,b_2 \ mod \ 2^t} e\big(\frac{2^{\alpha_1}(x^2+x_1x_2+x^2)h}{2^t}\big) = 2^{\min(t+\alpha_1,2t)}.$$

We substitute the values of these Gauss sums and obtain

$$\begin{aligned} \sigma_2(Q,n) &\leq \sum_{t=0}^{\beta+1} 2^{t/2} \frac{\prod_{i=2}^{k} 2^{\min(\frac{\alpha_i+t}{2},t)}}{2^{tk}} 2^{\min(t,\frac{t+\beta}{2})} \\ &\leq \sum_{t=0}^{\beta+1} \frac{2^{t/2} 2^{(k-1)\min(\frac{\alpha_k+t}{2},t)} 2^{\min(t,\frac{t+\beta}{2})}}{2^{tk}} \end{aligned} \tag{4.14}$$

From the inequality (4.14), we obtain

$$\sigma_2(Q,n) \ll 2^{\frac{\min(\alpha_k,\beta)}{2}}$$

This inequality together with inequality (4.13) for odd primes p implies

$$\prod_{p|\gcd(D,N)} \sigma_p \leq \gcd(N,D)^{1/2}.$$

Therefore, we conclude the lemma.

In Lemma 4.3.3, we invoke a result of Blomer, proved in Appendix 1, and then we apply the Petersson trace formula together with a Cauchy inequality to give an upper bound on $\tau(n,Q)$. Theorem (4.1.4) is a consequence of lemma (4.3.1) and lemma (4.3.3).

Lemma 4.3.3 *Let $Q(X)$ be a quadratic form in $k \geq 4$ variables and discriminant $D < n^{\frac{k-3}{2(k-2)}}$. Then we have the following upper bound on the n-th Fourier coefficient of the cusp form part of the*

theta series associated to Q

$$|\tau(n,Q)| \ll_{d,\epsilon} D^{\frac{(k-3)}{2}} n^{(k-1)/4} \gcd(n,D)^{1/4} n^{\epsilon}.$$

In particular

$$|\tau(n,Q)| \ll c_{\epsilon} \frac{n^{\frac{k-2}{2}}}{\sqrt{D}} \gcd(D,n)^{1/4} n^{\epsilon}.$$

Proof 4.3.4 *We take an orthonormal basis $\{f_i\}$ for the space of cusp forms of weight $k/2$ and level N. We write $F(z,Q)$ as a linear combination of them*

$$F(Q,z) = \sum_{f_i} C(Q,f_i) f_i(z).$$

We obtain

$$\tau(n,Q) = \sum_{f_i} C(Q,f) \rho_{f_i}(n).$$

We apply Cauchy inequality to obtain

$$|\tau(n,Q)|^2 \leq \big(\sum_{f_i} |C(Q,f)|^2\big)\big(\sum_{f_i} |\rho_{f_i}(n)|^2\big) \tag{4.15}$$

Since we take an orthonormal basis for the space of cusp forms we deduce that

$$||F||^2 = \sum_{f_i} |C(Q,f_i)|^2.$$

We invoke a result of Blomer. The proof is included in Appendix 1.

Lemma 4.3.5 *We have*

$$\|F\|^2 \ll N^{\epsilon}(N^{k-2} + N^{\frac{k-3}{2}} D^{1/2} + D^{1-1/k}).$$

for $k \geq 4$. As a corollary,

$$\|F\|^2 \ll N D^{k-3+\epsilon}. \tag{4.16}$$

Next, we give an upper bound on the sum over the square norm of the n-th Fourier coefficients of $\{f_i\}$

$$\big(\sum_{f_i} |\rho_{f_i}(n)|^2\big).$$

We apply the Petersson formula for the modular forms of weight $k/2$. See [Iwa87, Lemma 1]

$$\frac{\Gamma(k/2-1)}{(4\pi n)^{k/2-1}} \sum_{f_i} |\rho_{f_i}(n)|^2 = 1 + 2\pi i^{-k/2} \sum_{c\equiv 0 \ mod \ N} c^{-1} J_{k/2-1}\big(\frac{4\pi n}{c}\big) K(n,n;c).$$

In order to give an upper bound on $K(n,n;c)$, we apply the bound on Salie's sum for odd dimensions k and Weil's bound on the Kloosterman's sum for even dimensions k. We invoke the following formula [IK04, Corollary 14.24]

$$\frac{\Gamma(l-1)}{(4\pi n)^{l-1}} \sum_{f_i} |\rho_{f_i}(n)|^2 = 1 + O\Big(\tau_3(n) \gcd(n,N)^{1/2} n^{1/2} \frac{\tau(N)}{N\sqrt{l}} \log\big(1 + \frac{n^{1/2}}{\sqrt{Nl}}\big)\Big),$$

where $l = k/2$. Since the discriminant $D < n^{\frac{k-3}{2(k-2)}}$ and $N|D$ then

$$\sum_{f_i} |\rho_{f_i}(n)|^2 \ll_\epsilon \frac{n^{(k-1)/2}}{N} n^\epsilon \gcd(n,D)^{1/2} \tag{4.17}$$

From the inequalities (4.15), (4.16) and (4.17) we deduce that

$$|\tau(n,Q)|^2 \ll_{d,\epsilon} D^{k-3} n^{(k-1)/2} \gcd(n,D)^{1/2} n^\epsilon.$$

This concludes the first part of the lemma. For the second part, $D \ll n^{\frac{k-3}{2(k-2)}}$ implies that

$$D^{\frac{k-3}{2}} n^{\frac{k-1}{4}} \leq \frac{n^{\frac{k-2}{2}}}{\sqrt{D}}$$

Hence,

$$|\tau(n,Q)| \ll c_\epsilon \frac{n^{\frac{k-2}{2}}}{\sqrt{D}} \gcd(D,n)^{1/4} n^\epsilon,$$

The main theorem (4.1.4) is a consequence of lemma (4.3.5) and lemma (4.3.1).

4.4 Appendix

In this appendix, we include Valentin Blomer's paper to us. We are responsible for any gap or typo in this section.

Let

$$Q(X) = \frac{1}{2}X^T AX$$

be a primitive positive definite integral k-dimensional quadratic form ($k \geq 3$) of discriminant D and level N. For $n \in \mathbb{N}$ let $r(n, Q)$ denote the number of representations of n by Q and let $\rho(n, Q)$ be the main term given by a formal application of the circle method. Denote by $\mu_1, \dots \mu_k$ the successive minima (see [Cas78, Chapter 12]) of $Q(X)$. We can write

$$Q(X) := h_1(x_1 + c_{12}x_2 + \cdots + c_{1n}x_k)^2 + \cdots + h_k x_k^2$$

with $c_j, h_j \in \mathbb{Q}$ such that

$$h_j \asymp \mu_j.$$

Let $\Theta(Q, z)$ denote the corresponding theta-series and $F(z, Q)$ the orthogonal projection onto the space of cusp forms. The following lemma uses only reduction theory and the Lipschitz principle.

Lemma 4.4.1 *We have*

$$r(Q, n) \ll \Big(1 + \frac{n^{1/2}}{\mu_3} + \frac{n}{(\mu_3\mu_4)^{1/2}} + \cdots + \frac{n^{\frac{k-2}{2}}}{(\mu_3 \dots \mu_k)^{1/2}}\Big)n^{\epsilon}$$

and

$$\sum_{n \leq x} r(Q, n) \ll \max_{j \leq k} \frac{x^{\frac{j}{2}}}{(\mu_1 \dots \mu_j)^{1/2}}.$$

Proof 4.4.2 *We choose $x_k, x_{k-1}, \dots, x_3$ in*

$$\ll \big(1 + \frac{n}{\mu_k}\big)^{1/2} \dots \big(1 + \frac{n}{\mu_3}\big)^{1/2}$$

ways. Then we are left with an inhomogeneous binary problem that has $O(n^{\epsilon})$ solutions (see [BM13, Lemma 3a]), uniformly for all choices of $x_k, \dots, x_3$. To prove the second part, we choose $x_k, \dots, x_1$ in

$$\ll (1 + \frac{x}{\mu_k})^{1/2} \dots (1 + \frac{x}{\mu_1})^{1/2}$$

ways.

Corollary 4.4.3 *We have*

$$\sum_{n \leq x} r(Q, n)^2 \ll x^{\epsilon}\Big(x^{k-2} + \frac{x^{k-\frac{3}{2}}}{D^{1/2}} + \frac{x^{k-1}}{D^{1-1/k}}\Big).$$

Finally, we give a proof of Lemma (4.3.5). It suffices to show that

$$\|F(z,Q)\|^2 \ll N^{\epsilon}(N^{k-2} + N^{\frac{k-3}{2}}D^{1/2} + D^{1-1/k}).$$

Note that if $k \geq 4$, then the right hand side is $\ll ND^{k-3+\epsilon}$.

Proof 4.4.4 *We follow the argument of [Blo04, Lemma 4.2] or [Blo08, Lemma 3]. This gives*

$$\|F(z,Q)\|^2 \ll N^{\epsilon}\Big(\frac{1}{N} + \int_{1/2}^{\infty}\sum_{n=1}^{\infty}\big(r(\hat{Q},n)^2 + r_{Eis}(\hat{Q},n)^2\big)e^{\frac{-4\pi ny}{N}}y^{k/2-2}dy\Big)$$

where $\hat{Q}(X) = \frac{1}{2}X^T(NA^{-1})X$ *has determinant* N^kD^{-1} *and level* N*. Inserting Lemma 4.3.1 and Corollary 4.4.3, we obtain after a short computation the desired bound.*

Bibliography

[AC37] F. C. Auluck and S. Chowla. The representation of a large number as a sum of almost equal squares,. *Proc. Indian Acad. Sci.*, 6:8182., 1937.

[BB90] N. L. Biggs and A. G. Boshier. Note on the girth of Ramanujan graphs. *J. Combin. Theory Ser. B*, 49(2):190–194, 1990.

[Ber77] M.V. Berry. Regular and irregular semiclassical wave functions . *J.Phys.A*, (10), 1977.

[Ber83] Michael Berry. Semiclassical mechanics of regular and irregular motion. In *Chaotic behavior of deterministic systems (Les Houches, 1981)*, pages 171–271. North-Holland, Amsterdam, 1983.

[BFdlV82] B. Bollobás and W. Fernandez de la Vega. The diameter of random regular graphs. *Combinatorica*, 2(2):125–134, 1982.

[Blo04] Valentin Blomer. Uniform bounds for Fourier coefficients of theta-series with arithmetic applications. *Acta Arith.*, 114(1):1–21, 2004.

[Blo08] Valentin Blomer. Ternary quadratic forms, and sums of three squares with restricted variables. In *Anatomy of integers*, volume 46 of *CRM Proc. Lecture Notes*, pages 1–17. Amer. Math. Soc., Providence, RI, 2008.

[BM13] Valentin Blomer and Philippe Michel. Hybrid bounds for automorphic forms on ellipsoids over number fields. *J. Inst. Math. Jussieu*, 12(4):727–758, 2013.

[BR12] Jean Bourgain and Zeév Rudnick. Restriction of toral eigenfunctions to hypersurfaces and nodal sets. *Geom. Funct. Anal.*, 22(4):878–937, 2012.

[BRS16] J. Bourgain, Z. Rudnick, and P. Sarnak. Spatial statistics for lattice points on the sphere I: Individual results. *ArXiv e-prints*, June 2016.

[Cas78] J. W. S. Cassels. *Rational quadratic forms*, volume 13 of *London Mathematical Society Monographs*. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[Chi95] Patrick Chiu. Covering with Hecke points. *J. Number Theory*, 53(1):25–44, 1995.

[Dae10] Dirk Daemen. Localized solutions in Waring's problem: the lower bound. *Acta Arith.*, 142(2):129–143, 2010.

[DFI93] W. Duke, J. Friedlander, and H. Iwaniec. Bounds for automorphic L-functions. *Invent. Math.*, 112(1):1–8, 1993.

[DSV03] Giuliana Davidoff, Peter Sarnak, and Alain Valette. *Elementary number theory, group theory, and Ramanujan graphs*, volume 55 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.

[Eic54] Martin Eichler. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[GGN14] A. Ghosh, A. Gorodnik, and A. Nevo. Diophantine approximation exponents on homogeneous varieties. *ArXiv e-prints*, January 2014.

[Har90] Glyn Harman. Approximation of real matrices by integral matrices. *J. Number Theory*, 34(1):63–81, 1990.

[HB96] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[Iwa87] Henryk Iwaniec. Fourier coefficients of modular forms of half-integral weight. *Invent. Math.*, 87(2):385–401, 1987.

[Kim03] Henry H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. *J. Amer. Math. Soc.*, 16(1):139–183, 2003. With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.

[Klo27] H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Math.*, 49(3-4):407–464, 1927.

[KM13] D. Kleinbock and K. Merrill. Rational Approximation on Spheres. *ArXiv e-prints*, January 2013.

[LP15] E. Lubetzky and Y. Peres. Cutoff on all Ramanujan graphs. *ArXiv e-prints*, July 2015.

[LPS88] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[LR15] S. Lester and Z. Rudnick. Small scale equidistribution of eigenfunctions on the torus. *ArXiv e-prints*, August 2015.

[Lub10] Alexander Lubotzky. *Discrete groups, expanding graphs and invariant measures*. Modern Birkhäuser Classics. Birkhäuser Verlag, Basel, 2010. With an appendix by Jonathan D. Rogawski, Reprint of the 1994 edition.

[Mal62] A. V. Malyšev. On the representation of integers by positive quadratic forms. *Trudy Mat. Inst. Steklov*, 65:212, 1962.

[MR12] Jens Marklof and Zeév Rudnick. Almost all eigenfunctions of a rational polygon are uniformly distributed. *J. Spectr. Theory*, 2(1):107–113, 2012.

[RS14] N. J. Ross and P. Selinger. Optimal ancilla-free Clifford+T approximation of z-rotations. *ArXiv e-prints*, March 2014.

[Sar90] Peter Sarnak. *Some applications of modular forms*, volume 99 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1990.

[Sar15a] Peter Sarnak. *Letter to Scott Aaronson and Andy Pollington on the Solovay-Kitaev Theorem*, February 2015.

[Sar15b] Peter Sarnak. *Letter to Stephen D. Miller and Naser Talebizadeh Sardari on optimal strong approximation by integral points on quadrics; the case:* $SL_2(\mathbb{Z}) \to SL_2(\frac{\mathbb{Z}}{q\mathbb{Z}})$, August 2015.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Tij86] R. Tijdeman. Approximation of real matrices by integral matrices. *J. Number Theory*, 24(1):65–69, 1986.

[TS15] Naser Talebizadeh Sardari. *Diameter of Ramanujan graphs and random Cayley graphs with numerics* , 2015.

[Wri33] E. M. Wright. The representation of a number as a sum of five or more squares (ii). *Quart. J. Math. Oxford*, 4:37–51 ; 228–232., 1933.

[Wri37] E. M. Wright. The representation of a number as a sum of four almost equal squares. *Quart. J. Math. Oxford*, 8:278–279., 1937.