上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

学士学位论文

THESIS OF BACHELOR

论文题目 Several Problems and Methods in Algebraic Combinat

学生姓名 夏嘉程

学生学号 5100309129

指导教师 Eiichi Bannai

专　　业 数学与应用数学(交大理科班)

学院（系） 致远学院

Several Problems and Methods in Algebraic Combinatorics

ABSTRACT

This paper has studied some problems in algebraic combinatorics. These are from magic squares, Hadamard matrix, Unit circles and rational spherical designs. Geometrically, these combinatorial problems are all related to curves, which is an important theme here. Several new conjecture are posed and several problems are solved through the methods, many of which are directly related to the quadratic aspect. It is pointed out in the paper that there are several kinds of methods in algebraic combinatorics which could be viewed as some kind of quadratic consideration, such as double counting, calculation of the modulus and consideration of the L^2 average of a system of objects. Also, a complete introduction to the rational spherical design is given. We give a sketch of the existence of rational spherical design from a general point of view which is called geometric design. At last, we study the picture of the zeroes of some polynomials and all of its higher order derivatives. A conjecture on the pattern of the pictures is made for the next few years' study.

KEY WORDS: rational spherical design, quadratic method, root of unity, unit circle

Content

Chapter 1

Introduction

1.1 Background: Important Problems in Algebraic Combinatorics

Enumeration, otherwise known as counting, is the oldest mathematical subject, while algebraic combinatorics is one of the youngest. algebraic combinatorics is in fact the synthesis of two opposing trends: abstraction of the concrete and concretization of the abstract.

The abstraction trend consists of the categorization, conceptualization, structuralization (in short, "bourbakization") of mathematics. Enumeration did not escape this trend, and in the hands of such giants as Gian-Carlo Rota[1] and Richard Stanley[2] in America and Marco Schützenberger and Dominique Foata[3] in France, it became more conceptual, structural, and algebraic[4]. For example, there are analogies[5] between the partially ordered set of all subsets of a finite set and the partially ordered set of all subspaces of a finite vector space which is natural in view of 'matroid design'.

The concrete trend is dominating contemporary mathematics[6], thanks to the omnipresence of the mighty Computer[7]. One of the results obtained by Ziqing Xiang and me, namely the existence for rational spherical designs, expects to see the future of finding by computer the explicit constructions. Also in a recent work on the complex zeros of polynomial and its derivatives, we saw a series of interesting pictures one of which is on the second picture below. As a deep result was obtained by Szegő in 1924 in that problem of the Taylor truncation of the exponential function, which is the zeros accumulate on the blue curve in the first picture below when the order goes to infinity, we expect such wonderful result will also appear under the combinatorial work.

It has been revealed that many algebraic structures have hidden combinatorial underpinnings; the attempts to unearth these have led to many fascinating discoveries and unsolved problems.

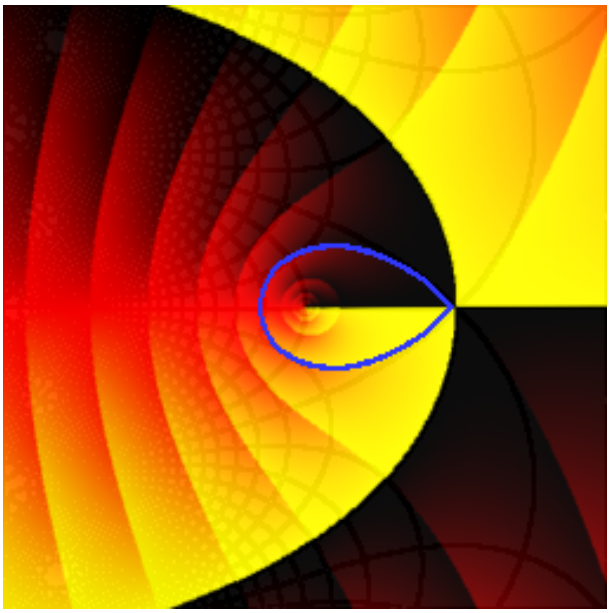

Figure 1–1 Accumulation of zeros of truncation of exp function

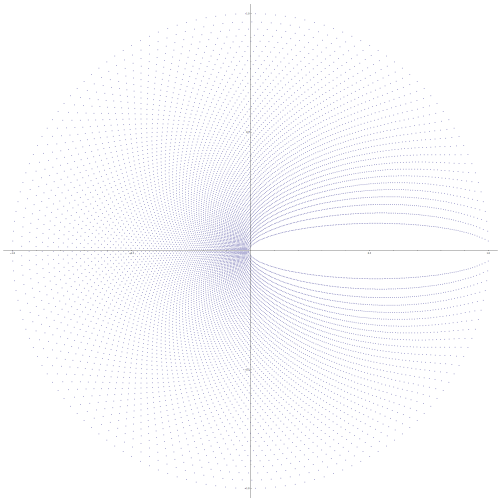

Figure 1–2 zeros of a normal polynomial and all of its derivatives

Therefore, it can be revealed that problems related with curves and distance[8] are really interesting and important for the author.

There are many different kinds of mathematics which could be called algebraic combinatorics. The content, as far as we would like to classify by a relatively normal discipline, can be designs(in the broadest meaning), algebraic graph theory, enumerative problems in the algebraic aspect, and sometimes more constructive things like Hadamard matrices and coding theory.

In doing several independent studies and cooperations with other people, I prefer to go further in those related to curves (also in a broader way). This theme can hardly be seen as one in algebraic combinatorics, while in the modest way, I try to keep on caring about problems from combinatorics and more related to algebra[9]. However this theme gives out a criterion on the scope I should be limited in which will concentrate the whole project on a mathematically interesting series of problems while several important problems in the usual meaning will not be neglected.

I did not mean to find out a particular method to tackle these problems[10]. However, in writing up the final paper and reviewing all the problems I have tackled in this series, it is surprisingly found out that to some extent all the important methods I have ever used are related to the 'quadratic calculation', which means when we meet a problem involved with modulo, we can calculate in the quadratic way adn when we are involved in enumerative problems, counting by two different ways in a modest idea is usually the best choice. This kind of idea is really a useful one and can be called a mathematical philosophy or a belief when we tackle difficult combinatorial problems.

In the following chapters, I will demonstrate this idea by several important problems and methods.

1.2 Background of Spherical Designs

Definition 1.1 (Delsarte-Goethals-Seidel)**.** We say a finite set $X \subsetneqq \mathbb{S}^{n-1}$ is a spherical t-design if

$$\frac{1}{|X|}\sum_{x\in X} f(x) = \frac{1}{|\mathbb{S}^{n-1}|}\int_{\mathbb{S}^{n-1}} f(x)d\sigma(x)$$

for all polynomials $f(\mathbf{x}) = f(x_1, \ldots, x_n)$ of degree not exceeding t.We can also define a toy model of it when $\mathbb{S}^{n-1}$ is replaced by the interval $[-1, 1]$, which is called an interval t-design.

The purpose of my work is to explore the existence of rational spherical multi $2e$-design on $\mathbb{S}^n$ and to give an effective method in analytic number theory to obtain the existence of rational interval $2e$-design and also design on $\mathbb{S}^1$. (The $\mathbb{S}^1$ case is however a little different where we get only one coordinate to be rational while the other is square root of a rational number).

We are most interested in this problem due to two simple ideas: First of all, many problems involving rational points on sphere $\mathbb{S}^n$ (say, the density problem for a sphere not necessarily centered at the origin, the approximation problem by rational points of given upper bound of height), more generally speaking, the problems of metric diophantine approximation on manifolds[11], are very fascinating themselves and our methods are related to the spirit of rational approximation. On the other hand, spherical t-design itself is a very important topic in combinatorics, especially in design theory[12].

It is not until the year 1984 that P. D. Seymour and T. Zaslavsky proved a theorem that in general solved the existence of spherical design : Let Ω be a path-connected topological space provided with a positive finite measure μ which makes use of the curve's property in the topological space. Therefore, we see the prototype of the importance of the curve's role in such existence problem in combinatorics. We will come back to that paper and state more detail on the corresponding result in it.

Moreover, the interesting result we get finally on $\mathbb{S}^2$ is related again to the quadratic form, since we can make sure that the square of each coordinates are rational numbers.

This is again related to our quadratic methods. However, the direct result which means the coordinates themselves are rational numbers is still a conjecture for us as fas as what the author know.

Chapter 2

Hadamard Matrices

2.1 enumerative problem of magic square

We begin by stating a result obtained by the author which fascinates him to the problem related with algebraic combinatorial problems on the finite matrix.

Theorem 2.1.

$$H_3(r) = \binom{r+4}{4} + \binom{r+3}{4} + \binom{r+2}{4}$$

where $H_3(r)$ is the number of all magic matrix of order 3 which has row sum and column sum r.

Proof. Let a, b, c, d be four numbers in a submatrix of order 2. We have the following three cases which give out a partition of all possible situations:

$$1.a+b+c, b+c+d \leq r$$

$$0 \leq a+b+c+d-r \leq a \leq a+b \leq a+b+c \leq r$$

$$2.b+c+d > r, a \leq d$$

$$0 \leq a < a+b+c+d-r \leq a+c \leq c+d \leq r$$

$$3.a+b+c > r, d < a$$

$$0 \leq d < a+b+c+d-r \leq c+d < a+c \leq r$$

which gives out respectively $\binom{r+4}{4}, \binom{r+3}{4}$ and $\binom{r+2}{4}$ possibilities to choose the construction. □

Remark 2.1. It is very interesting to find such a fascinating proof, since we know these three case itself is a combinatorial construction. And this is the charming property of algebraic combinatorics, which from the view of logic the proof itself is intrinsic. To find such a proof can sometimes be also a target to pursue for the author.

2.2 The Problem of Construction

Definition 2.1. An Hadamard matrix or order n is an $n \times n$ matrix H with entries $+1$and -1, such that

$$HH^\top = nI$$

Observation 1. *Of course, any two columns of H are also orthogonal. This property does not change if we permute rows and columns or if we multiply some rows or columns by -1. Two such matrices are called equivalent*[13].

Observation 2. *If $n \neq 1 or 2$ then n must be multiple of 4.*

For observation 2, one should operate the matrix into a normal one and the property of the size naturally comes out.

Theorem 2.2. *If H_m and H_n are Hadamard matrics of order m and n respectively, then $H_m \otimes H_n$ is also a Hadamard matrix of order mn.*

Proof. One sees that

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$$

$$(A \otimes B)^\top = A^\top \otimes B^\top$$

$$I_m \otimes I_n = I_{mn}$$

□

By this kind of product theorem, one can try to construct Hadamard Matrix of large size. When I practise the 'quadratic method' in a variable way, I found out that the idea of 'Paley construction' can be very useful. Last semester I once use the Paley

matrix to construct a kind of self-complementary graph. On the problem of the construction of Hadamard matrix, I also found it very helpful and natural to construct a three-term Kronecker product sum of matrices.

Definition 2.2. If we see the elements of $\mathbb{F}_q$ as numbers

$$0 = a_0, a_1, ..., a_{q-1}$$

we can define a matrix Q by

$$q_{ij} := \chi(a_i - a_j)$$

This is called Paley matrices. And we can easily obtain a symmetric of antisymmetric matrix C (conference matrix) which will be useful in the next construction of Hadamard matrics.

Definition 2.3. Let P_m be the matrix of size m with the asymmetric diag zero form where the submatrices have size $m/2$.

Proof. We need to define the conference matrix C. It should always meet the identity

$$CC^\top = (n-1)I$$

when all methods could be used to construct such matrix. Here we can construct it directly from Q. Let

$$C = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ \pm 1 & * & * & * & * \\ \pm 1 & * & * & * & * \\ \vdots & * & * & * & * \\ \pm 1 & * & * & * & * \\ & & & & \end{pmatrix} \tag{2–1}$$

where the star entry are that of Q. The signs of the terms ± 1 are chosen in such a way that C is symmetric or antisymmetric. □

Now we can state and prove our main result.

Theorem 2.3. *Let q be a prime number power $\equiv 1(mod 4)$. Let C be the matrix just constructed. Choose H and P as in the above construction. Then we have*

$$(H_m \otimes C_{q+1} \otimes Q_q) + (P_m H_m \otimes C_{q+1} \otimes I_q) + (H_m \otimes I_{q+1} \otimes J_q)$$

is also an Hadamard matrix of size $mq(q+1)$.

Hereby in this theorem we choose the positive sign on the first column.

Proof. Obviously we have the associativity of the Kronecker Product. And we also have

$$Q_q Q_q^T = qI_q - J_q$$

$$H_m H_m^T = mI_m$$

$$Q_q J_q = J_q Q_q = O$$

$$P_m P_m = -I_m$$

$$T = H_m \otimes C_{q+1} \otimes Q_q + P_m H_m \otimes C_{q+1} \otimes I_q + H_m \otimes I_{q+1} \otimes J_q$$

$$T^T = H_m^T \otimes C_{q+1}^T \otimes Q_q^T - H_m^T P_m \otimes C_{q+1}^T \otimes I_q + H_m^T \otimes I_{q+1} \otimes J_q$$

Hereby there are three main terms and six intersection terms of the product TT^T:

(1) main term

$$(H_m \otimes C_{q+1} \otimes Q_q)(H_m^T \otimes C_{q+1}^T \otimes Q_q^T) = (H_m H_m^T) \otimes (C_{q+1} C_{q+1}^T) \otimes (Q_q Q_q^T)$$

$$= mI_m \otimes qI_{q+1} \otimes (qI_q - J_q) = mqI_{m(q+1)} \otimes (qI_q - J_q)$$

(2) main term

$$(P_m H_m \otimes C_{q+1} \otimes I_q)(H_m^T P_m \otimes C_{q+1}^T \otimes I_q) = (P_m H_m H_m^T P_m) \otimes (C_{q+1} C_{q+1}^T) \otimes I_q$$

$$= mI_m \otimes qI_{q+1} \otimes I_q = mqI_{m(q+1)} \otimes I_q$$

(3) main term

$$(H_m \otimes I_{q+1} \otimes J_q)(H_m^T \otimes I_{q+1} \otimes J_q) = (H_m H_m^T) \otimes I_{q+1} \otimes J_q^2$$
$$= mI_m \otimes I_{q+1} \otimes qJ_q = mqI_{m(q+1)} \otimes J_q$$

(1)+(2)+(3) gives out the sum of main terms:

$$mqI_{m(q+1)} \otimes (q+1)I_q = mq(q+1)I_{mq(q+1)}$$

To complete the proof it suffices to show the six intersection terms cancel out. In fact we have

$$(H_m \otimes C_{q+1} \otimes Q_q)(H_m^T \otimes I_{q+1} \otimes J_q) = (H_m H_m^T) \otimes (C_{q+1} I_{q+1}) \otimes (Q_q J_q) = O_{mq(q+1)}$$

since we have at first

$$Q_q J_q = O_q$$

Similarly, we have

$$(H_m \otimes I_{q+1} \otimes J_q)(H_m^T \otimes C_{q+1}^T \otimes Q_q^T) = O_{mq(q+1)}$$

The other four terms cancel out two by two.

$$-(H_m \otimes C_{q+1} \otimes Q_q)(H_m^T P_m \otimes C_{q+1}^T \otimes I_q)$$

$$= -mP_m \otimes qI_{q+1} \otimes Q_q = -mqP_m \otimes I_{q+1} \otimes Q_q$$

while

$$(P_m H_m \otimes C_{q+1} \otimes I_q)(H_m^T \otimes C_{q+1}^T \otimes Q_q^T)$$

$$= mP_m \otimes qI_{q+1} \otimes Q_q^T = mqP_m \otimes I_{q+1} \otimes Q_q$$

These two terms thus annihilate.

$$(P_m H_m \otimes C_{q+1} \otimes I_q)(H_m^T \otimes I_{q+1} \otimes J_q)$$

$$= mP_m \otimes C_{q+1} \otimes J_q$$

while

$$(H_m \otimes I_{q+1} \otimes J_q)(-H_m^T P_m \otimes C_{q+1}^T \otimes I_q)$$

$$= -mP_m \otimes C_{q+1}^T \otimes J_q = -mP_m \otimes C_{q+1} \otimes J_q$$

and we are done for all the calculation.

□

2.3 The Problem of Entry Sum

After one has already constructed some Hadamard matrices, although the general problem of constructing all possible Hadamard matrices is still far from our ability,

one has also to consider another general problem:

What can we say about the total sum of all the entries?

This is formally posed under the existence of Hadamard matrix. However, it is independent of the existence of Hadamard matrix since this could be a criterion to look for the Hadamard matrix. In this paper, such problem is considered:

What is the asymptotic formula of the maximum absolute value of the sum of all the entries of Hadamard matrix of order n, when n goes to infinity?

We give out a quite accurate result on both the upper bound and lower bound of the asymptotic order here. It is really amazing that the upper order and the lower order are the same.

Theorem 2.4. *Suppose*

$$\beta(n) = \max |\sum_{i,j} a_{ij}|$$

where the the maximum value are chosen from all the Hadamard matrix of order n and a_{ij} are the entries.

Then one has

$$\beta(n) \leq n^{3/2}$$

Proof. From the definition of Hadamard matrix, two different rows have the inner product of their corresponding vectors 0. and the inner product by a vector with itself should be n, which means the double sum of the following form equals n^2:

$$n^2 = \sum_{i,j} \sum_{k=1}^{n} a_{ik} a_{j,k}$$

$$= \sum_{k=1}^{n} \sum_{i,j} a_{ik}a_{jk} = \sum_{k=1}^{n} (\sum_{i=1}^{n} a_{ik})^2 = \sum_{k=1}^{n} s_k^2$$

where s_k is the sum of the k th column.

By Cauchy inequality we have immediately that

$$(\sum_{k=1}^{n} s_k)^2 \leq (\sum_{k=1}^{n} 1^2)(\sum_{k=1}^{n} s_k^2)$$

which implies that

$$\sum_{k=1}^{n} s_k \leq n^{3/2}$$

.

Since the Hadamard matrix is chosen without restriction, we are done. □

Theorem 2.5.

$$\beta(n) \geq 2^{-n} \binom{n}{n/2} n^2$$

which is of order $n^{3/2}$

Proof. This is by direct calculation of Stirling formula that the order of the function on n is $n^{3/2}$. To prove the inequality, we need to find the whole structure of the some kind of average value. For this consideration, we should utilize the random vector, say $\mathbf{x} \in \{+1, -1\}^n$ and do the operation on an arbitary Hadamard matrix:

First of all, we transform each row vector $\mathbf{v}_j$ into $x_j\mathbf{v}_j$for each j.

Then we multiply -1 to some row vectors such that for each row, the sum of this row is nonnegative. Note that at this time the matrix transformed is still an Hadamard matrix since Hadamard matrix property will hold under the operation of changing rows

and columns and multiplication by ± 1.

We name the sum of entries of this Hadamard matrix by $s_{\mathbf{x}}$. One easily sees that in fact

$$s_{\mathbf{x}} = \sum_{i=1}^{n} |\mathbf{x} \cdot \mathbf{v}_i|$$

By the definition of $\beta(n)$, which is the maximum value, should be no smaller than $s_{\mathbf{x}}$ for every $\mathbf{x} \in \{+1, -1\}^n$.

In particular, one has the inequality

$$\begin{aligned}
\beta(n) &\geq \frac{1}{2^n} \sum_{\mathbf{x} \in \{+1,-1\}^n} s_{\mathbf{x}} \\
&= \frac{1}{2^n} \sum_{\mathbf{x} \in \{+1,-1\}^n} \sum_{i=1}^{n} |\mathbf{x} \cdot \mathbf{v}_i| \\
&= \frac{1}{2^n} \sum_{i=1}^{n} \sum_{d=0}^{n} \sum_{d(\mathbf{x}, \mathbf{v}_i)=d} |n - 2d|
\end{aligned}$$

Note that here d is the Hamming distance of two vectors, which is very common used in the coding theory. After looking at the right hand side of the calculation, we found that the summation by i is independent of the index i. The right hand side should be equal to

$$\begin{aligned}
&\frac{1}{2^n} \sum_{i=1}^{n} (\sum_{d=0}^{n} \binom{n}{d} |n - 2d|) \\
&= \frac{n}{2^n} \sum_{d=0}^{n} \binom{n}{d} |n - 2d|
\end{aligned}$$

To complete the proof, one should only examine the identity of binomial numbers:

$$\sum_{d=0}^{n} \binom{n}{d} |n - 2d| = n \binom{n}{n/2}$$

Note that here n is the order of an Hadamard matrix which is supposed to be an even number. Hence we can use technique to calculate by half:

$$\sum_{d=0}^{n/2-1} \binom{n}{d} |n-2d|$$

$$= \sum_{d=0}^{n/2-1} \frac{n!}{(n-d)!d!}((n-d)-d)$$

$$= n(\sum_{d=0}^{n/2-1} \binom{n-1}{d} - \sum_{d=1}^{n/2-1} \binom{n-1}{d-1}) = n\binom{n-1}{n/2-1}$$

Note that the other half part is the same with this part, we conclude by pointing out

$$2\binom{n-1}{n/2-1} = \binom{n}{n/2}$$

□

Remark 2.2. It is very interesting to note the order $3/2$. It is the mean value between that of a normal Hadamard matrix (of order 1) and of full entry matrix (of order 2). Basically speaking, this phenomenon is important when a random problem is involved. It is also very obvious for the physicists to understand such order, especially when a vector modulus is related to the essential inequality in Physics, due to professor Ye.X in Shanghai Jiaotong University. From a mathematical point of view, the author found the result not so surprising. Although the Hadamard matrices are far from understood, some of its combinatorial properties are very clear, like the conclusion made here. Again we see the 'quadratic' method fully used here, which is supposed to be the center of this article.

Chapter 3

Combinatorics on the Unit Circle

3.1 A Conjecture on the Unit Circle

The author has heard about this conjecture for many years: Consider several roots of unity which may not be different and the order of each root of unity may vary. Then what about the sum of these roots of unity? Mu.X.S. made such a beautiful conjecture which has many combinatorial and number theoretical implications: If the sum falls on a unit circle, then the sum itself is also a root of unity. Mu.X.S. is very good at number theory in even high school time, and he won the gold medal of IMO by a full score(together with Wei.D.Y and other foreign student in the participants of that year's IMO). He thought on it and asked this problem to some mathematicians, one of them is a French specialist on diophantine approximation and transcendental number theory. Everyone who heard about it found it both interesting and meaningful, while no proof has ever been found.

The author has been indulged in finding the key to the proof from three years ago and it was a coincidence that at that time Professor Feng.K.Q visited to Shanghai Jiaotong University to give a short course on algebraic curves. Professor Fend has advised the author to look up some results on the CM field. This is because the theory about algebraic integers on the unit circle would not necessarily be a root of unity, while in a CM field one can find much more to do with.However, until now there is no evidence that this theory could help on finding the combinatorial structure of the sum of roots of unity.

Then thanks to Professor Li.J.Y. who suggests me to think on Galois correspondence and some algebraic aspects on it. Although the Galois correspondence is not needed

finally, we tried to find the important thing successfully, which is related to the cyclotomic polynomial. It is really happy for the author to solve this conjecture just before he graduates from the University. He will continue to pursue his study on number theory related to combinatorics and algebraic theory.

It is important to point out that the author has met Professor W.Zudilin who is a specialist on transcendental number theory. And he told the author that it is not evident from the view of approximation theory to solve this problem although it is related to both the distance problem and algebraic problem.

Therefore, it is of first importance to state the proof in this paper. We expect to see more applications of it on algebraic combinatorics and other combinatorial problems.

Theorem 3.1. *Suppose the sum of several roots of unity is located on the unit circle, then it is a root of unity.*

Proof. To understand the key of the whole proof, we need first to state a lemma.

Lemma 3.2. *(Kronecker) If all the conjugate elements of an algebraic integer are located within the unit circle, then they are all roots of unity.*

One should note in particular that if all the conjugate elements are on the unit circle, the conclusion still holds.

Proof. This is a purely combinatorial proof. Suppose α is an algebraic integer with all the n conjugate elements $\alpha^{(i)}$ (including itself). Then

$$f_1(x) = \prod_{i=1}^{n}(x - \alpha^{(i)})$$

must be a irreducible polynomial with integer coefficient. Suppose the contrary of the assumption, if α is not a root of unity. One has for any two different integer $h < k$,

$$\alpha^h \neq \alpha^k$$

. This means that the two sets $\bigcup_{i=1}^{n}\{\alpha^{(i)h}\}$ and $\bigcup_{i=1}^{n}\{\alpha^{(i)k}\}$ can not be identical. Otherwise we can find a snake of the label of length no more then n which gives out the identity

$$\alpha^{h^t} = \alpha^{k^t}$$

where t is the length of the snake. One should note that we can safely forget about the special case where for some i and j, $\alpha^{(i)}$=$\alpha^{(j)}$ because that case could be easily reduced to the general case where all conjugate elements are different with each other. That means α is a root of unity, contrary to our supposition.

Therefore we get two different sets which means the series of polynomials $f_h(x) = \prod_{i=1}^{n}(x - \alpha^{(i)h})$ has no identical terms in the sense of polynomials. But these polynomials are all with integer coefficients from the number theoretic view. On the other hand, all the absolute values of the coefficients of them are bounded by n which is fixed since by our original assumption, $|\alpha^{(i)}|$ are all bounded by 1.

Combine these two aspects we immediately find the contradiction: the number of possible choices of all the different monomial polynomials of degree n with integer coefficients which are bounded by n in its absolute value is no more than $(2n+1)^n$, while on the other hand, there are infinitely many different polynomials in the series $\{f_h(x)\}$. This is a contradiction and we conclude here that α is a root of certainty. □

Now we come back to the proof of the theorem. Without loss of certainty, we may assume that these roots of certainty are ζ_n^h where h belongs to a subset of $[n]$ where ζ_n is a primitive root of unity of degree n. Let $\eta = \sum_h \zeta_n^h$, by the assumption $|\eta| = 1$,i.e.$|\eta|^2 = 1$.

By this quadratic method we can calculate with a polynomial:

$$(\sum_h \zeta_n^h)(\sum_h \zeta_n^{-h}) = 1$$

In view of $mod(x^n - 1)$ we can see the following function as a polynomial of x with

degree less than n which has one of its root ζ_n.

$$f(x) = (\sum_h \zeta_n^h)(\sum_h \zeta_n^{-h}) - 1$$

From the view of number theory we know that $f(x)$ is divisible by the cyclotomic polynomial of degree $\varphi(n)$, or say, ζ_n^m where $g.c.d.(n, m) = 1$ are root of $f(x)$.
Now we conclude by the lemma. For any $g \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, one has

$$g(\eta) = \sum_h g(\zeta_n)^h$$

while we have known from the discussion above that $g(\zeta_n)$ is a root of the $f(x)$.

This implies that $|g(\eta)|^2 = 1$ for any $g \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, we have then for any conjugate element of η, it will locates on the unit circle.

Note that η is an algebraic integer and it meets all the conditions of the lemma, hence it must be a root of unity. □

3.2 A Conjeture Transformed into Problems on the Unit Circle

A combinatorial problem naturally comes out when we do some 'crystallization' for a smooth curve or a continuous curve. This method is helpful for the famous discussion on the relation with area and the length, as well as other metric structure.

Usually people will use Fourier analysis when the corresponding problem of the distance that varies in a closed curve. Then the 'crystallization', or the approximation of the curve by a series of unit length polygons will be in the place when we try to tackle on the other hand.

We call it a problem on the unit circle since all the sides of the polygons can be moved to be a point on the unit circle. Then for the problem involved with distance, the quadratic method is the first one we would remind ourselves and sometimes it indeed works efficiently.

The problem stated here was totally posed by the author from a discussion of a proof in curve-shortening and mean curvature flow. In the page 19 of the paper[14], the author Mooney.Connor mentioned an important property without proof that 'At a spatial minimum, we must have $d/\psi \leq 1$, where equality holds if and only if our curve is a circle.' where d is the length of chord between two points on a closed curve and ψ is that of a circle with the same perimeter L.

At first looking, this problem seems obvious to be true. However, we can not find effective calculation to prove it. In fact, the problem considered is a kind of L_p average geometric inequality, particularly for $p = 1$. After our serious statement, we can even tackle a stronger result where $p = 2$. Thanks to the quadratic method and combinatorial calculation, this stronger version is even easier to handle with. One should think about this problem from the following statement, which is more general than that in the paper of Mooney.

Conjecture 3.1. Suppose C is any continuous closed curve in the Euclidean space $\mathbb{R}^2$ while C has a fixed perimeter L. Fix a real number l which is smaller then L, then we will have the following inequality

$$(\frac{1}{L}\int_0^L |X(s+l) - X(s)|^2 ds)^{1/2} \leq \frac{L}{\pi}\sin(\frac{\pi l}{L})$$

.

where $X(s)$ is a parameterization of the curve and s is the famous parameter of curve length.

Now we try to see the meaning of this conjecture. The right hand side of this inequality is nothing but the value of the left hand side when C is a circle. And the left hand side is the L^2 average of the chord length over the whole curve. Due to the fact that L^2 average is always no smaller than L^1 average, one can state that if we solve this conjecture finally, the problem from Mooney's paper would be a weaker conclusion.

Then we state here the geometric meaning of this inequality. In Mooney's paper, as

one can call ψ as the extrinsic distance between two points on the closed curve of the same length with the same intrinsic distance l between points. Such comparison could be read from at least two points of view: the geometric one and the combinatorial one.

As for the geometric aspect, this is a classical version of the comparison between two different important metrics in a manifold. The exterior distance is in the space where the manifold itself is embedded. And the interior distance is independent of the space, which is related only to the geometry of the manifold itself. Any inequality between these two different distances would be interesting for a geometer.

On the other hand, it is important to see it from a combinatorial view. Although the 'best curve' can be understood totally through an analytic way, such as obtaining several inequalities between derivatives and quadratic terms, sometimes it is also related to the 'best construction' in the combinatorial meaning, as well as the practical method to solve the problem itself.

The author has obtained one result on this conjecture independently, which could be called a partial proof of the conjeture. And the result followed is a local result while the conjeture it self can be seen as a global result.

Theorem 3.3. *Denote by* $c(s) = \max_{\cos<T(s),T(s+t(s))>>0} \{t(s)\}$ *and* $c = \min_{s\in[0,L]} c(s)$. *Then for any* $l < c$*, the conclusion of the conjecture is true. Here* $< T(s), T(s+t(s)) >$ *denotes the angle between the two tangent vectors at* $X(s)$ *and* $X(s+t(s))$ *respectively.*

Proof. This is mainly by the combinatorial and quadratic method.

Here we give a sketch of the proof which consists several important steps.

First of all, one can approximate the closed curve by a polygon whose side has the same length. We should prove the uniformity of such approximation due to compact property of the closed curve. This kind uniformity includes the aspect in distance between two points on the curve, and the 'label' distance between each vertex which can

be seen as the intrinsic distance.

The second step is suppose the polygon has length of 1 for each side. And the number of the vertices of the polygon,n, is a prime number. This is reasonable because without loss of certainty, as n goes to infinity, we can assume any number theoretical property of it as far as this property can be met by infinitely many number. In this case, prime numbers are infinite. And we can suppose any length of the polygon since the problem does not change after any dilation of the curve by the center of the origin.

The third step is to look up the problem on the unit circle, and we should do the 'translation' from the original problem to this unit circle problem. The chord length is translated into the modulus of the sum of the complex numbers on the unit circle with increasing label. and the curve length is translated into the difference of the label since each complex number here is of modulus 1.

The fourth step is to do concrete calculation and apply Jensen inequality with restriction of the angles difference which would be translated into the continuous version that our result is only a local result, which gives out the conclusion only when the chosen two points are close enough, such that $l < c$ where c is translated into a combinatorial restriction in our unit circle problem.

The important points that this method really works lie in the fact

$$|\sum_{k=j+1}^{j+m} e^{ix_k}|^2$$

$$= \sum_{k=j+1}^{j+m} e^{ix_k} \sum_{k=j+1}^{j+m} e^{-ix_k}$$

$$= \sum_{(k,k')} \cos(x_k - x'_k)$$

which means we have translated the L^2 average of chord length (continuous version)

into L^1 average of cosine of angles (discrete version)!

On the other hand, through a combinatorial point of view, the average of cosine of $x_k - x'_k$ can be precisely estimated. The method here is to regroup them according to $k - k'$.

For example by a series of Jensen inequality

$$\sum_k \cos(x_{k+1} - x_k) \leq n \cos(\frac{2\pi}{n})(m-1)$$

$$\sum_k \cos(x_{k+2} - x_k) \leq n \cos(\frac{4\pi}{n})(m-2)$$

$$\cdots$$

$$\sum_k \cos(x_{k+m-1} - x_k) \leq n \cos(\frac{2(m-1)\pi}{n})(m-(m-1))$$

since one has rigorous relation thanks to the fact that we have already chosen n to be a prime number.

$$\sum (x_{k+t} - x_k) = 2\pi t$$

However it is interesting to note that in the Euclidean space with dimension more than 3, this method does not work easily since the rigorous identity would be replaced by inequality and as t becomes large, the direction of the inequality would change mysteriously. However when $t = 1$ it is still workable and is related to the beautiful knot theory and combinatorial geometry. For the sake of the interested readers, please refer to the following more general conjecture and another theorem obtained by the author.

The last step is to sum up the inequality to get the inequality with left hand side $\sum_{(k,k')} \cos(x_k - x'_k)$ and then translated back to the continuous version. We will finally find that everything is perfectly done except that our result is only a local one while the conjecture needs a global estimate. So the problem is still there. □

Now we should state the general conjecture which is far from understood and proof. But it should be a real object of our studies.

Conjecture 3.2. Suppose C is any continuous closed curve in the Euclidean space $\mathbb{R}^n$ while C has a fixed perimeter L. Fix a real number l which is smaller then L, then the following function of curves

$$(\frac{1}{L}\int_0^L |X(s+l)-X(s)|^p ds)^{1/p}$$

attains its maximum value only when C is a circle in a plane if $p=2$ and an ellipse in a plane if $p>2$
where $X(s)$ is a parameterization of the curve and s is the famous parameter of curve length.

Now it is time to see the result mentioned above.

Theorem 3.4. *The total curvature of a closed C^2 space curve is no less than 2π.*

Proof. If we do Gauss mapping and move the tangent vector of the close curve to the point on the sphere, it is easy to transform this theorem into the following result which the author called the 'traveller's theorem'. In fact, since the curve is closed, the average of these corresponding points on the sphere should be zero vector, and if the total curvature is less than 2π, it is obvious that the curve consisted by all the points on the sphere has length less than 2π. All we should prove is that this curve must be contained in a hemisphere which is contradictory to the average vector should be zeros vector. So we have the following interesting theorem and we conclude here for this important theorem. □

Theorem 3.5. *If a traveller has travelled to many places on the world and the total length is less than 2π times the radius of the earth, then one can conclude that he has always been in a hemisphere.*

Proof. Fix any point P on the trace. Let Q be another point on the trace such that the curve segments $\Gamma_1 = PQ$ and $\Gamma_2 = QP$ have equal length and $\Gamma = \Gamma_1 + \Gamma_2$. Rotate the sphere such that P and Q are located symmetrically to the north pole N (also fixed at first).So we have

$$P = Q = N$$

or P and Q have the same latitude, while have longitudes differing by angle π. If the trace Γ does not intersect the equator, we are already done.

If Γ intersects the equator at some point, then we can uniquely construct the curve Γ_3 such that it is symmetric to Γ_1 with respect to the north pole.

Now we conclude the proof by stating the fact that Γ_3 and Γ_1 have the same length, while the closed curve $\Gamma' = \Gamma_1 + \Gamma_3$ has the same length with Γ. Furthermore, there is a pair of antipodal equatorial points on Γ'. Join these points by geodesics on the sphere, we see that Γ' has length at least 2π which is a contradiction. □

Remark 3.1. We hope by the above result, one can finally find the way to tackle the general conjecture. It is a bit strange that the tuition tells us the problem is even more obvious in high dimension, while the effective calculation is hard to be applied and the inequalities are very difficult to control. However, we expect that this problem will be solved by someone who combines Fourier analysis and some important conclusions from combinatorics.

Chapter 4

Rational Spherical Design

This work has already been introduced in the first chapter. Here we study more details of it and show some important results related to it. A complete proof of each part will be recently published by Xiang.Z.Q and the author.

However, the interest to the existence of rational spherical t-design was originated in a much simpler problem, on rational design on the interval $[-1, 1]$ where the equation reads

$$\frac{1}{|X|}\sum_{x\in X} x^i = \begin{cases} 0, & i \text{ is odd}, \\ \frac{1}{i+1}, & i \text{ is even}, \end{cases}$$

for $0 \leq i \leq t$.

If we consider only the antipodal solution (i.e.$X = -X$) for the $t = 2e$ case, especially in the special form

$$\frac{1}{|X|}\sum_{x\in X} x^i = \frac{1}{i+1}$$

for $0 \leq i \leq t$.

4.1 Geometric Designs

A *strictly positive measure* on a topological space is a measure under which every non-empty open subset has strictly positive measure. A *probability measure* is a measure with total measure 1.

Let M be a topological space equipped with a strictly positive probability measure

μ on it, f be a continuous μ-integrable function into $\mathbb{R}^p$, c be a vector in $\mathbb{R}^p$. A subset Δ of M is an f, c-*design*, if it is a topological space (not necessarily to be topological subspace of M) equipped with a strictly positive probability measure δ, such that $f|_\Delta$ is a continuous δ-integrable function and

$$\int_\Delta f d\delta = c.$$

An f-*design* is an f, c-design Δ where c is the *centroid* of f, namely

$$\int_\Delta f d\delta = \int_M f d\mu.$$

Lemma 4.1. *For a finite family of f-designs, their topological union is also an f-design.*

Proof.

$$\delta(S) = \frac{1}{|Z|} \sum_{z \in Z} \delta_z(S \cap \Delta_z)$$

□

Theorem 4.2. *Suppose M is path-connected. Let $c \in relint(conv(Image f))$. Then for sufficiently large n, there exists a f, c-design of size n.*

This result was obtained in the paper of Seymour and Zaslavsky[15], where discussion is made on the most general case.

Lemma 4.3. *Let $c \in relint(conv(Image f))$[15], and S be a finite subset of M equipped with a strictly positive probability measure s. For sufficiently large n, there exists a finite f, c-design of size n containing S. In particular, f-designs give a cover of M.*

Proof. Let n be a sufficiently integer, and

$$c' = c - \frac{|S|}{n}(c - \int_S f ds) \in relint(conv(Image f)).$$

There exists an f, c'-design Δ. Hence $\Delta \cup S$ is an f, c-design. □

Lemma 4.4. *Let $c \in relint(conv(Image f))$. If f, c-designs give a cover of M, then every dense subset of M contains a finite f, c-design. In particular, if M is path-connected, then every dense subset of M contains a finite f-design.*

Proof. Suppose Y is a dense subset of M. Pick a set Z consisting of $\dim(Image f)$ points, such that $f(Z)$ is a basis of $(Image f)$. For each $z \in Z$, let Δ_z be a finite f, c-design containing point z. Their topological union Δ is also a finite f, c-design.

Since Y is dense in M, for every $x \in \Delta$, there exists a sequence x_i in Y whose limit is x. Take $\Delta_i = \{x_i \mid x \in \Delta\}$. For sufficiently large i, $f(\Delta_i)$ are linearly independent. Therefore, for sufficiently large i, we can find a strictly positive probability measure δ_i on Δ_i, which makes Δ_i an f, c-design. □

Theorem 4.5. *If M is path-connected, then every dense subset of M contains a finite f-design.*

Corollary 4.6. *There exists rational weight rational spherical designs.*

Corollary 4.7. *There exists rational weight rational interval designs.*

Lemma 4.8. *Let S be a countable dense subset of real interval $[0, 1]$, and T be a dense subset of $[0, 1]$. Then, there exists a continuous $f : [0, 1] \to [0, 1]$ where $f(S) \subseteq T$.*

Corollary 4.9. *Let C be a simple curve in a topological space and S be a dense subset with respect to the subtopology induced by C. The curve C can be parameterised as $f : [0, 1] \to C$ with $f(\mathbb{Q}) \subset S$.*

Proof. Let D be a dense subset of a topological space M. The topological space M is *p-D-path-connected* if every p points can be covered by a simple path, whose intersection with D is dense with respect to the subtopology induced by D. □

Theorem 4.10. *Let T be a topological space equipped with a strictly positive probability measure τ, and S be a dense subset of T. Suppose for every c such that f, c-designs in T exist, S contains a regular f, c-design in T.*

Proof. Choose $T = [0, 1]$.

Let D be a dense subset of M, and suppose furthermore that M is a p-M-path-connected topological space. Then, for c such that f, c-designs in M exist, the dense subset D contains a regular f, c-design in M. □

Lemma 4.11. *For a finite family of disjoint regular $\mathbb{F}$-designs, their topological union is also a regular $\mathbb{F}$-design.*

4.2 From Multi-Design to Design

Historically Hilbert-Kamke Problem is one of several meaningful generalizations of the Waring Problem in Number theory : For given $N_k \in \mathbb{N}$, solve the system of diophantine equations

$$\sum_{i=1}^{n} x_i^k = N_k$$

where $1 \leq k \leq t, x_i^k$ are non-negative integers.

Posed in 1900 by D. Hilbert,the problem was eventually solved by E. Kamke who proved the existence of the solution under some very ordinary compatible conditions for this Diophantine equation system. Later, the asymptotic formula for the number of solutions of this system using the Vinogradov method for estimating trigonometric sums was gained under the spirit of Vinogradov.

In fact,some useful results among them are accessible to us, which means to blow up the multi-set solution into the form we are looking for, i.e. a real set instead of a multi-set, one needs to get somehow explicit asymptotic formula for the number of solutions in terms of the number of variables in the equation. For the solution with multiplicity at least 2 at at least one point, one sees it is actually a solution to the equation with variables less than the original number, say n. Fortunately, one can find a classical result due to Arkhipov.

First we state the main theorem of this section.

Theorem 4.12. *$c_{n,k}$ is a constant which only depends on n, k and e. If for infinitely many n, Equation(1)has a solution, then there is a solution for Equation(2).*

$$\begin{aligned} \sum_{i=1}^{n} x_i^k = c_{n,k}, 0 \le k \le t \\ 0 < x_i < 1, 1 \le i \le n \\ x_i \in \mathbb{Q}, 1 \le i \le n \end{aligned} \tag{4–1}$$

$$\begin{aligned} \sum_{i=1}^{n} x_i^k = c_{n,k}, 0 \le k \le t \\ 0 < x_i < 1, 1 \le i \le n \\ x_i \in \mathbb{Q}, 1 \le i \le n \\ x_i \ne x_j, 1 \le i < j \le n \end{aligned} \tag{4–2}$$

Before proving the main theorem, one needs a routine rational-integral transformation in order to use the main result below from Arkhipov.

Theorem 4.13. *We state here the Hilbert-Kamke problem in number theory.*

Hilbert-Kamke problem[16]

$$\begin{aligned} x_1 + x_2 + \cdots + x_s = N_1 \\ x_1^2 + x_2^2 + \cdots + x_s^2 = N_2 \\ \cdots \\ x_1^k + x_2^k + \cdots + x_s^k = N_k. \end{aligned} \tag{4–3}$$

However there are obviously some necessary conditions:

$$N_k^{j/k} \le N_j \le s^{1-j/k} N_k^{j/k} (1 \le j \le k) \tag{4–4}$$

for the system of equations (3) to be solvable.

Denote by J the number of solutions of equation (1) in positive integers. Let $s_0 = \min\{k^2 2^{2k-1}, 3k^2 2^k - k\}$ and $P = N_k^{1/k}$. Then for $s \geq k^2(4\log k + 2\log\log k + 9)$, the following asymptotic formula is valid:

$$J = J(N_1, \ldots, N_k) = \sigma\gamma P^{s-k(k+1)/2} + \theta k^{30k^3} P^{s-k(k+1)/2-1/30(2+\log k)}.$$

If the necessary conditions (4) hold and $s \geq s_0$, then $\sigma \geq \sigma_0 > 0$ and $\gamma \geq \gamma_0 > 0$, then

$$J \sim P^{s-k(k+1)/2}.$$

where the common notations among analytic number-theorists are defined as follows, while they are not essentially related to our main theorem:

$$\sigma = \sum_{q_1=1}^{\infty} \cdots \sum_{q_k=1}^{\infty} \sum_{\substack{0 \leq a_1 < q_1 \\ (a_1, q_1)=1}} \cdots \sum_{\substack{0 \leq a_k < q_k \\ (a_k, q_k)=1}} q^{-s} V^s e^{-2\pi i A},$$

$$\gamma = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} W^s e^{-2\pi i B} d\beta_1 \cdots d\beta_s,$$

$$q = q_1 \cdots q_k$$

$$V = \sum_{x=1}^{q} e^{2\pi i (a_1 x/q_1 + \cdots + a_k x^k/q_k)}$$

$$A = \frac{a_1 N_1}{q_1} + \cdots + \frac{a_k N_k}{q_k}$$

$$W = \int_0^1 e^{2\pi i (\beta_1 x + \cdots + \beta_k x^k)} dx$$

$$B = \frac{\beta_1 N_1}{P} + \cdots + \frac{\beta_k N_k}{P}.$$

Arkhipov's proof[17] also works if we restrict the integral variables $x_j \in [1, Y]$. The final result turns out to be:

$$J(Y) \sim Y^{s-k(k+1)/2}.$$

More precisely, one has the following proposition

Proposition 4.14. *For large Y, denote by $J(Y)$ the number of solutions of equation (3) in positive integers with $x_j \in [1, Y](1 \leq j \leq k)$. Then for $s \geq s_0$, the following asymptotic formula is valid:*

$$J(Y) = \sigma\gamma' Y^{s-k(k+1)/2} + \theta k^{30k^3} Y^{s-k(k+1)/2-1/30(2+\log k)}.$$

Here θ and the singular series σ are as above, while the new singular integral γ' is defined as

$$\gamma' = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} W^s e^{-2\pi i B'} d\beta_1 \cdots d\beta_s,$$

where

$$B' = \beta_1 s/2 + \cdots + \beta_k s Y^{k-1}/(k+1).$$

Further more, $\gamma' \geq \gamma_0' > 0$.

Having this theorem, we now consider the following special case in the theorem, which is just our problem:

$$\begin{aligned} x_1 + x_2 + \cdots + x_s &= N_1 \\ x_1^2 + x_2^2 + \cdots + x_s^2 &= sY^2/3 \\ &\cdots \\ x_1^k + x_2^k + \cdots + x_s^k &= sY^k/(k+1). \end{aligned} \tag{4–5}$$

Arkhipov's proof also works if we restrict the integral variables $x_j \in [1, Y]$. The final result turns out to be:

$$J(Y) \sim Y^{s-k(k+1)/2}.$$

Proposition 4.15. *For large enough Y, Denote by $J'(Y)$ the number of solutions of equation (5) in positive integers with $x_j \in [1, Y](1 \leq j \leq k)$ and $x_i \neq x_j (i \neq j)$. Then for $s \geq s_0 + 2$, the following holds:*

$$J'(Y) \gg Y^{s-k(k+1)/2}.$$

Proof. One easily sees the total number of solutions $J''(Y)$ with $x_i = x_j$ for some $i \neq j$ is

$$\leq \binom{s}{2} \sum_{x=1}^{Y} J_{s-2}(\frac{sY}{2} - 2x, \ldots, \frac{sY^k}{k+1} - 2x^k) \leq \binom{s}{2} Y k^{30k^3} Y^{s-2-k(k+1)/2}$$

by the asymptotic formula. So

$$J'(Y) \geq J(Y) - J''(Y) \gg Y^{s-k(k+1)/2}.$$

□

Now we have come to the final proof of the main theorem.

Proof. of the main theorem. Suppose Equation (1) has a solution. Let Y be a multiple of each denominator in the rational number x_i, we get a solution to the system of diophantine equations:

$$\sum_{i=1}^{n} x_i^k = c_{n,k} Y^k, 0 \leq k \leq t$$

$$0 < x_i < Y, 1 \leq i \leq n$$

$$x_i \in \mathbb{Z}, 1 \leq i \leq n.$$

Then one applied the above result to get the integer solution with mutually different property. After we divide the integer solution by the denominator, again we obtain a rational solution of Equation (2), which has mutually different rational coordinates. □

Chapter 5

Far Beyond the Unit Circle

In this section I will state a breaktaking studying program starting from one concrete problem.
We begin by considering the zeros of the following polynomial

$$f(x) = \frac{x^{n+1} - 1}{x - 1}$$

.

One can easily find out that the zeros of it are distributed on the unit circle by equidistance. And by the old theorem, we know that all the roots of the derivative of $f(x)$ are also located within the unit circle. But how on the earth is the distribution? Is there an obvious pattern, even describable pattern of its distribution?

In fact, this question is more clear to ask when we consider even more: How about the zeros of the second order derivative and the higher order ones?

This time I drew all the zeros of each order derivative of $f(x)$ and the first few ones met the author's expectation. The following picture reveals the distribution of zeros of the first 6 consecutive derivatives (including $f(x)$ itself) when $n = 45$.

There is clearly an effect of draging all the points to the right half plane. We call it 'effect of derivative'. In fact, we have a more precise result in the discrete version to understand this effect:

Theorem 5.1. *If all the zeros of a polynomial $f(x)$ are located on a line $\Re z = a$, then the finite difference of it with step length h will have all the zeros located on the line $\Re z = a - h/2$.*

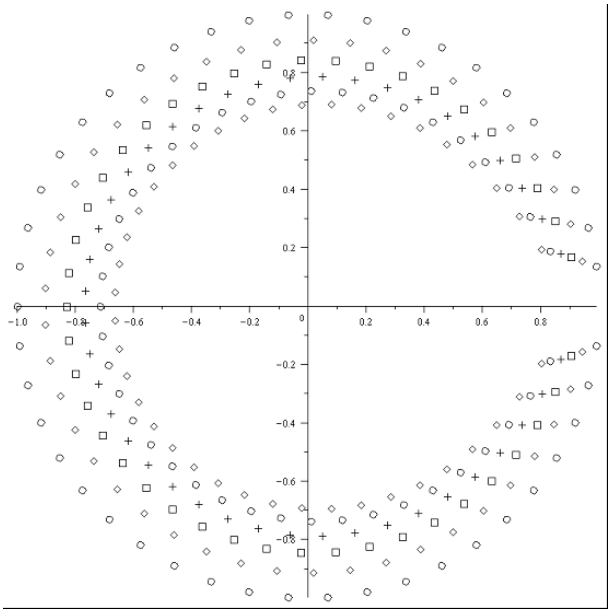

Figure 5–1 zeros of the first 6 sheafs

Proof. We use again the quadratic method. suppose

$$f(x) = \prod_{k=1}^{n} (x - a - ib_k)$$

then we have the finite difference of it with step h is

$$f_h(x) = \prod_{k=1}^{n} (x + h - a - ib_k) - \prod_{k=1}^{n} (x - a - ib_k)$$

.

Suppose $\xi = \mu + i\tau$ is a root of $f_h(x)$,

$$\prod_{k=1}^{n} (\mu + i\tau + h - a - ib_k) = \prod_{k=1}^{n} (\mu + i\tau - a - ib_k)$$

.

Taking modulus square on each side, one has the identity

$$\prod_{k=1}^{n} ((\mu + h - a)^2 + (\tau - b_k)^2) = \prod_{k=1}^{n} ((\mu - a)^2 + (\tau - b_k)^2)$$

which from the obvious inequalities implies that

$$|\mu + h - a| = |\mu - a|$$

hence

$$\mu = a - h/2$$

□

Now we are glad to see the whole pictures on the full zeros, of each derivatives with order $n = 500$ and different pixels.

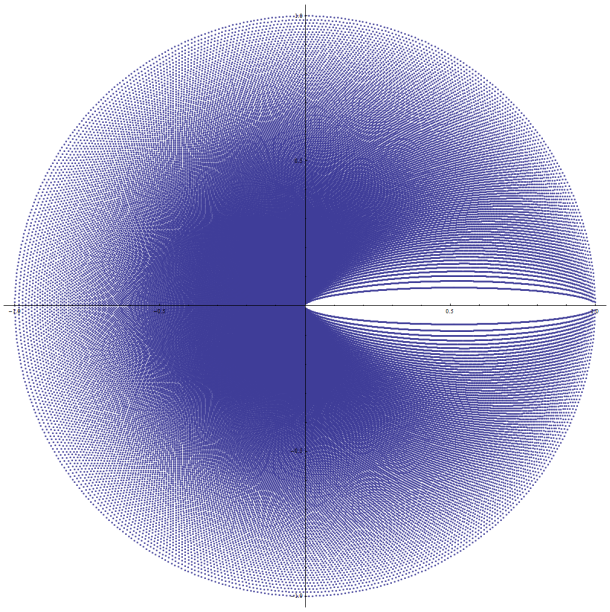

Figure 5–2 1000px

It is mysterious to see the pattern of curves because of the difference of pixels.

However, the distribution itself is the essential thing of our studies. We make a conjecture here that such graph has a limit pattern under some meaningful distance between

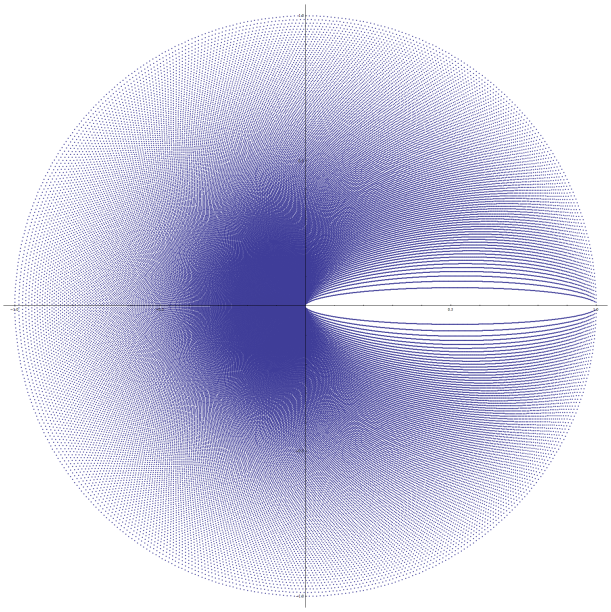

Figure 5–3 1500px

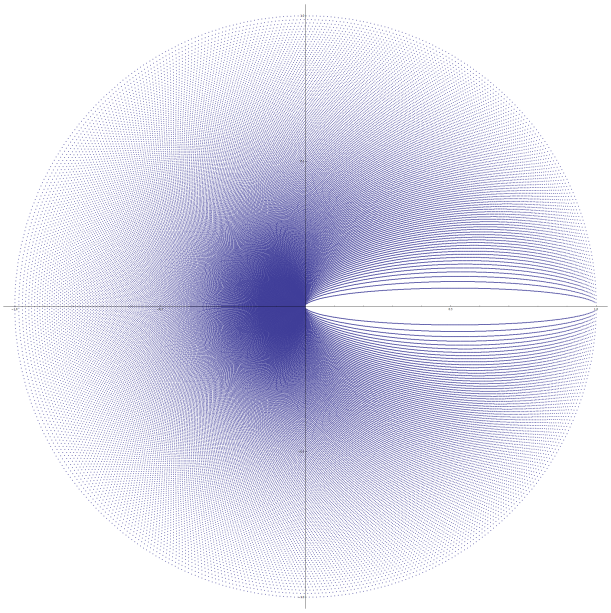

Figure 5–4 2000px

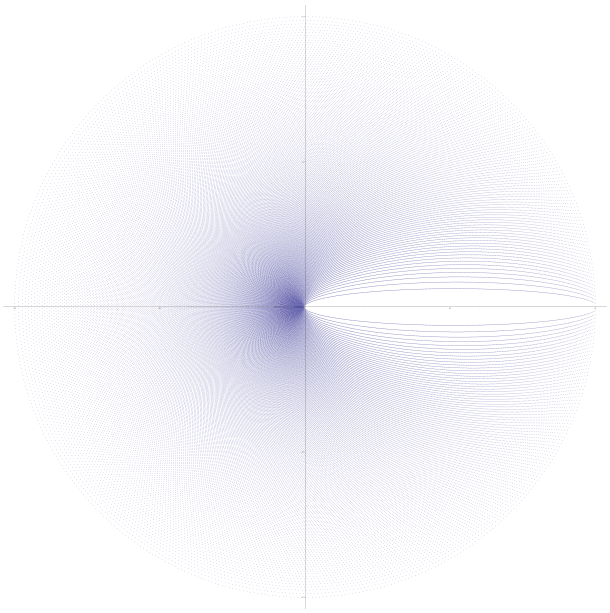

Figure 5–5 4000px

two pictures. Limit means when n goes to infinity, there is a picture which will be close enough to the pictures drawn under large enough n.
From the view of algebraic combinatorics, such kind of pattern is very closed to combinatorial 2=design because as we observe the picture, each point has always located at the intersection of two beautiful curves which are imagined by us from connecting the natural neighbour points.

However, neighbour points are still not defined very well just from observing the picture. More precise conjecture is to be posed.

From the view of prime number theory, these graphs are even more interesting. Please compare the following two graphs, which give out the similarity of the pattern of the two graphs. It would be very surprising to point out what they really are:

The first one is our known picture of roots of all derivatives up to degree of 150, which is totally algebraic and combinatorial.

While the second one is nothing but the famous picture of the distribution of primes numbers on the spiral obeying basic equations in the plane.

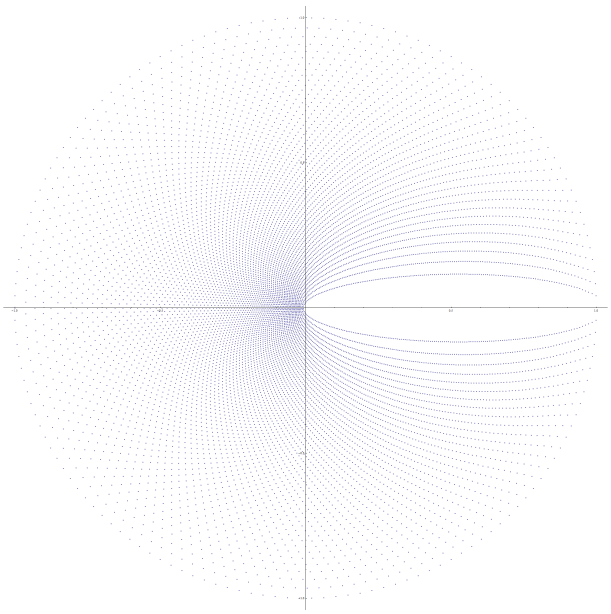

Figure 5–6 basic zeros picture

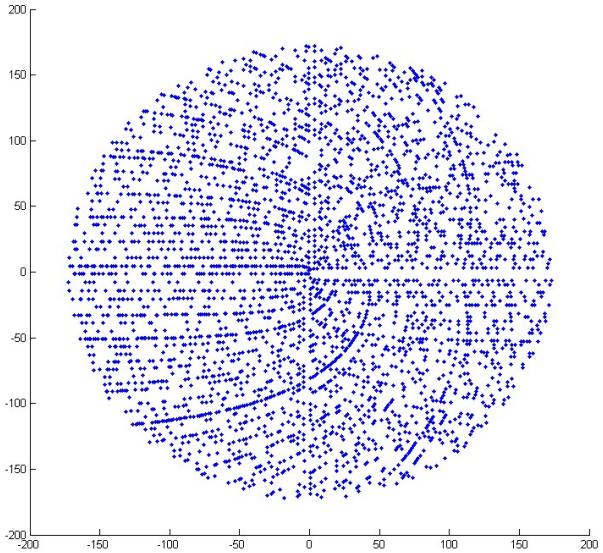

Figure 5–7 primes on the spiral

The author also stuied the corresponding picture of the polynomial whose zeros

are located with equidistance on the unit square and unit hexagone with high degree. The pictures are also surprisingly beautiful and the author expects to get some remarkable properties of it. Please see these two patterns as belowed.

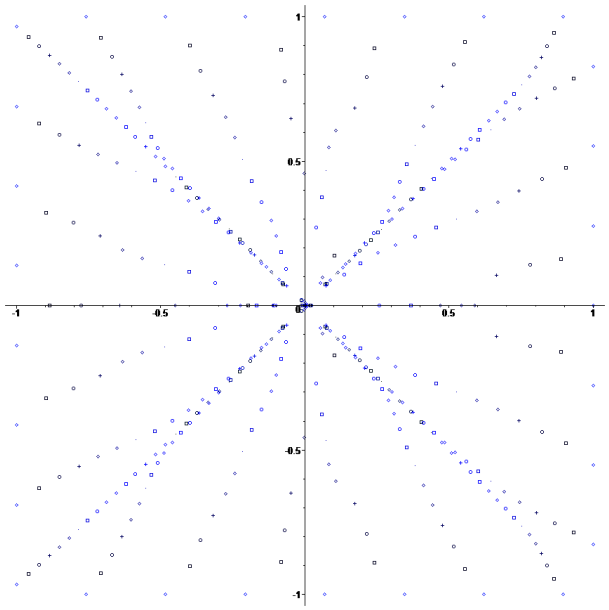

Figure 5–8 square1

Remark 5.1. It is important to note this remarkable phenomenon of higher order derivatives. In fact, only that of the exponential truncation functions are well studied till now. In that case, the famous result is by Szegő in 1924 which is stated in the introduction part. From this view, one would like to conclude that the hidden power of combinatorics, behind these deep problems, are really infinite.

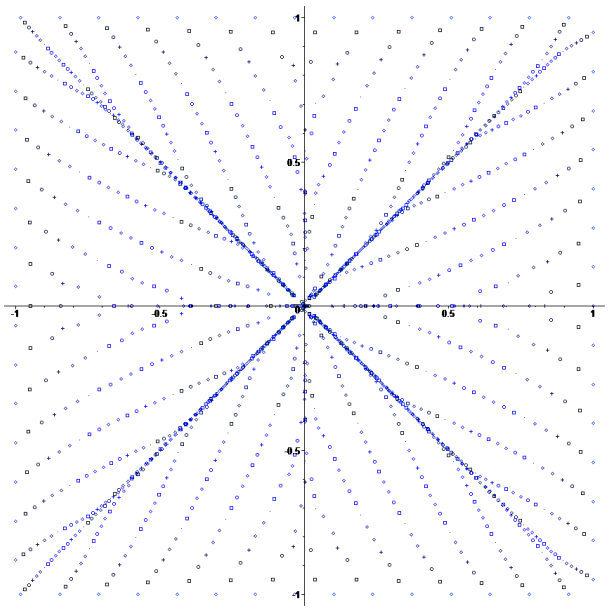

Figure 5–9 square2

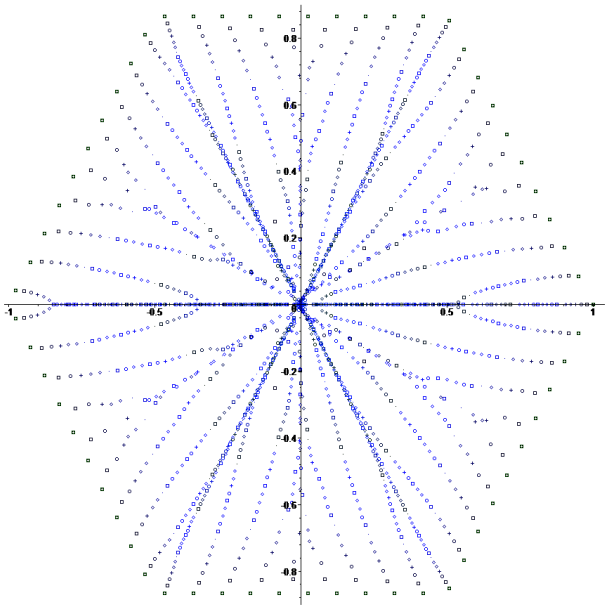

Figure 5–10 hexagon

Conclusion

In this paper we have stated several important theorems on the existence of Hadamard matrices and the so called rational spherical design and rational interval design. We have studied some combinatorial aspects of the zeroes of all order derivatives of a polynomial. An enumerative problem has been totally solved about the three order magic square. An interesting conjecture on the root of unity posed by Mu.X.S is proved by combinatorial facts. Besides, the most important conjecture posed by the author on the comparison inequality of two different metrics are also locally solved by the author using purely combinatorial method. In solving these problems, it is remarkable that sometimes the calculation by quadratic terms are more helpful. These problems themselves and the proofs are related by many geometric common views, for example, curves play the main role in the whole paper. From this view, one would like to conclude that the hidden power of combinatorics, behind these deep problems, are really infinite.

Bibliography

[1] Crapo H, Rota G. On the Foundations of Combinatorial Theory: Combinatorial Geometries, 1970[缺文献类型标志代码].[S.l.]: MIT Press, Cambridge, MA.

[2] Stanley R P. Enumerative combinatorics[M].[S.l.]: Cambridge university press, 2011.

[3] Hall M. The theory of groups[M], Vol. 288.[S.l.]: American Mathematical Soc., 1976.

[4] Bannai E, Ito T. Algebraic combinatorics[M].[S.l.]: Benjamin/Cummings Menlo Park, 1984.

[5] Tits J. Sur les systèmes de Steiner associés aux trois ¡°grands¡± groupes de Mathieu[J]. Rendic. Math, 1964, 23:166–184.

[6] Brouwer A, Cohen A, Neumaier A. Distance-Regular Graphs, ser. A Series of Modern Surveys in Mathematics[缺文献类型标志代码].[S.l.]: Springer-Verlag.

[7] de Bruijn N G. Pólya¡¯s theory of counting[J]. Applied Combinatorial Mathematics, 1964:144–184.

[8] Grunbaum B, Klee V, Perles M A, et al. Convex polytopes[M].[S.l.]: Springer, 1967.

[9] Whitney H. Non-Separable and Planar Graphs*[M]//Classic Papers in Combinatorics.[S.l.]: Springer, 1987:25–48.

[10] Tutte W T. Graph theory, volume 21 of Encyclopedia of Mathematics and its Applications[缺文献类型标志代码].[S.l.]: Addison-Wesley Publishing Company Advanced Book Program, Reading, MA.

[11] Bernik V. Metric Diophantine approximation on manifolds[M].[S.l.]: [s.n.] .

[12] Veblen O, Young J W. Projective geometry[M], Vol. 2.[S.l.]: Ginn, 1918.

[13] Dénes J, Keedwell A. Latin squares: New developments in the theory and applications[M], Vol. 46.[S.l.]: Elsevier, 1991.

[14] Mooney C. An Introduction to Curve-Shortening and the Ricci Flow[J]. 2011.

[15] Seymour P, Zaslavsky T. Averaging sets: a generalization of mean values and spherical designs[J]. Advances in Mathematics, 1984, 52(3):213–240.

[16] Hilbert D. Beweis für die Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem)[M]//Gesammelte Abhandlungen.[S.l.]: Springer, 1932:510–527.

[17] Arkhipov G. On the Hilbert-Kamke problem[J]. Izv. Akad. Nauk SSSR Ser. Mat, 1984, 48(1):3–52.

Acknowledgements

In the four years undergraduate study I should first express my gratitude to professor Eiichi.Bannai who is also my advisor, not only in the undergraduate paper, but in many occasions and many studying activities. I should also say many thanks to him for his recommendation for me to the best program in learning mathematics, especially in the aspect of algebra, geometry and number theory. He has hosted a lot of seminar and courses in algebraic combinatorics as well as topics in graph theory and other combinatorial theories. I have learnt a lot from not only his knowledge of mathematics, but also his altitude to do mathematics, his method to understand problems and his interesting way to introduce a lot of new problems. He is a real Master of mathematics.

My gratitude should also been expressed to professor Wu.Y.K who is my first year teacher on algebra. He is a real specialist on combinatorics, especially on algorithm and graph theory. I learnt a lot from him both in combinatorics and in algebra, and his philosophy of mathematics impressed and will always influence me a lot.

I have also learnt a lot in algebra from professor Zhang.P and professor Li.J.Y. who have also given me a lot of precious advice and problems to think about.

On the aspect of geometry, I have to say thanks a lot to professor Xu.Y.Z and professor Yang.Y.H. who taught me and influenced me a lot in differential geometry and one chapter of my thesis is related to that aspect.

Finally I have not enough space here to thanks to everybody who gave me advices on learning mathematics, especially to Tyaglov.M. who is my collaborator and also taught me a lot on analysis.