JOHANNES KEPLER
UNIVERSITY LINZ

Submitted by
Mehdi Makhul

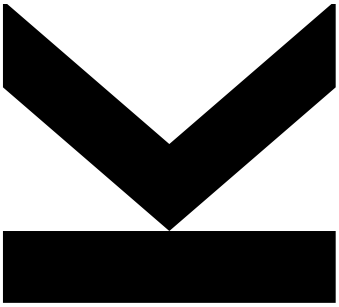
Submitted at
Radon Institute For Computational and Applied Mathematics
Doctoral Program Computational Mathematics

Supervisor and
First Examiner
Prof. Josef Schicho

Second Examiner
Prof. Herwig Hauser

November 2018

Algebraic geometry techniques in incidence geometry



Doctoral Thesis
to obtain the academic degree of
Doktor der technischen Wissenschaften
in the Doctoral Program
Technische Wissenschaften

JOHANNES KEPLER
UNIVERSITY LINZ
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe. Die vorliegende Dissertation ist mit dem elektronisch übermittelten Textdokument identisch.

Linz, 7. November 2018

Mehdi Makhul

Zusammenfassung

Inzidenzgeometrie untersucht das Verhalten endlicher Mengen von Objekten – Punkten, Geraden, oder Kreisen – bezüglich geometrischer Operationen wie Kolinearität, Durchschnitt oder Abstand. Arithmetische Kombinatorik untersucht das Verhalten endlicher Teilmengen von Gruppen oder Ringen bezüglich der arithmetischen Operationen, zum Beispiel Addition oder Multiplikation.

Diese Thesis versammelt neue Resultate in Inzidenzgeometrie und arithmetischer Kombinatorik. Die Schlüsseltechniken kommen aus der algebraischen Geometrie, der Distantgeometrie und der projektiven Geometrie.

Die Hauptresultate sind folgende. Für eine endliche Menge von Punkten definieren wir einen "gewöhnlichen Kreis" als einen Kreis, der genau drei der gegebenen Punkte enthält. Wir geben die minimale Anzahl von gewöhnlichen Kreisen für eine Menge von n Punkten an, falls n eine genügend große natürliche Zahl ist. Mit Hilfe eines Struktursatzes für Mengen mit wenig gewöhnlichen Kreisen stellen wir fest, wann die Schranke annähernd erreicht wird. Das *Obstgartenproblem* für Kreise fragt nach der maximalen Anzahl von Kreisen durch genau 4 von n gebenenen Punkten. In Kapitel 3 geben wir diese Anzahl an, und die Mengen bei denen das Maximum erreicht wird, falls n genügend groß ist.

Wir untersuchen die Wahrscheinlichkeit dafür, dass eine zufällige Gerade eine gegebene ebene Kurve über einem endlichen Körper in einer gegebenen Anzahl von Punkten schneidet. Insbesondere untersuchen wir in Kapitel 4 den Grenzwert dieser Wahrscheinlichkeiten unter einer Folge von Erweiterungen des endlichen Körpers. In Kapitel 5 geben wir eine zweite Lösung für dieses Problem basierend auf dem Dichtesatz von Chebotarev. Kapitel 6 enthält eine Verallgemeinerung auf höhere Dimensionen.

Eine n-stellige reelle Funktion f nennen wir einen Vervielfacher, wenn ein $\epsilon > 0$ existiert, sodass für jede endliche Menge A die Ungleichung $|f(A \times \dots A)| \geq |A|^{1+\epsilon}$ gilt. In Kapitel 7 untersuchen wir eine Familie von Vervielfachern mit quadratischem Wachstum. Teile der Thesis sind gemeinsamen Arbeiten mit Matteo Gallet, Aaron Lin, Hossein Nassajian Mojarrad, Josef Schicho, Konrad Swanepoel und Frank de Zeeuw entnommen.

Abstract

The basic objects of incidence geometry are arbitrary finite sets such as points, lines, curves, and we study the behaviours of these objects with respect to geometric operations such as collinearity, incidence or distance. In arithmetic combinatorics we study the behaviour of a finite set with respect to some algebraic operation such as addition or multiplications.

In recent years many mathematicians have used some algebraic geometry and algebraic topology techniques to solve some combinatorial problems. Among the most prominent of such problems, one can mention the *distinct distance problem*, the *Kakeya problem over finite fields* and the *Dirac-Motzkin conjecture*.

This thesis collects together new results related to the concept of incidence geometry and arithmetic combinatorics. The key tools throughout are from algebraic geometry, discrete geometry and projective geometry.

These are the main results of this thesis: For a given finite set P we define an *ordinary circle* to be a circle that contains exactly three of the given points. We will find the exact minimum number of ordinary circles, for sufficiently large n, and we will determine which configurations attain or come close to that minimum in Chapter 3, our proof being based on a structure theorem for the sets with few ordinary circles. The *orchard problem* for circles asks for the maximum number of circles passing through exactly four points from a set of n points. We determine the exact maximum and the extremal sets for all sufficiently large n in Chapter 3.

We study the probability for a random line to intersect a given plane curve, defined over a finite field, in a given number of points. In particular, we focus on the limits of these probabilities under successive finite field extensions in Chapter 4. We are using the Chebotarev density Theorem over finite fields to give another solution to this question in Chapter 5, and we generalise this to higher dimension in Chapter 6.

We say that an n-variable real function f is expander function if it is true that there is some $\epsilon > 0$ such that for every finite set $A \subset \mathbb{R}$, $|f(A \times \dots A)| \geq |A|^{1+\epsilon}$. In Chapter 7 we will study a family of four-variable expanders with quadratic growth. Parts of this thesis are taken from joint works with Matteo Gallet, Aaron Lin, Hossein Nassajian Mojarrad, Josef Schicho, Konrad Swanepoel and Frank de Zeeuw.

Acknowledgement

Firstly, I would like to express my sincere gratitude to my advisor Josef Schicho for his continuous support of my Ph.D study and related research, for his patience, motivation, and immense knowledge. Josef's expertise and kindness have been exceptionally important. He taught me many techniques from algebraic geometry in our numerous discussions together. I would also like to thank him for giving me the opportunity to consider my own problems, and to investigate areas in mathematics that appeal to me.

I am also indebted to my kind colleague Oliver Roche-Newton, who's assistance has been invaluable, particularly with results from Chapter 7.

I would like to thank Herwig Hauser and Arne Winterhof for their willingness to be referees of my thesis.

There are many friends and colleagues whose help made this thesis possible. I would like to thank some of these people.

I would like to thank my Italian academic brother Matteo Gallet, who deserved a very special mention for the mathematical, English and Latex help he has given me.

I would like to thank my other academic brother Niels Lubbes, who taught me many thing in Web-Geometry and with whom I have had many funny conversation.

I was very lucky to have two friendly and kind British colleagues Oliver Roche Newton and recently Audie Warren, who really changed my work atmosphere. I have learnt many thing in Mathematics and English from both of them. Audie also read some parts of this thesis and he corrected my English typos.

A special thanks to my family. Words cannot express how grateful I am to my mother and my sister for all of the sacrifices that you've made on my behalf.

It has been a pleasure to be part of the Research Institute for Symbolic Computation at Johannes Kepler University Linz and Radon Institute for Computation and Applied Mathematics. I'd also like to thank all of the administrative staff.

My PhD studied have been funded by DK9.

Contents

CHAPTER 1

Introduction

This thesis collects results in the field of additive combinatorics and discrete geometry. In recent years, the interplay between combinatorial problems and algebraic techniques has become more and more common, and has been revealing to be extremely fruitful. Here we refer in particular to the area called *combinatorial geometry*, which deals with, among others, distance or intersection relations between finite sets of geometric objects such as points, lines, or circles (see [**Tao14**]). In the last decade, algebraic geometry and algebraic topology helped solving several outstanding problems and conjectures in this area. Amongst the most prominent of such problems, one can mention the *distinct distance problem* (see [**GK15**]), the *Kakeya problem over finite fields* (see [**Dvi09**] and later improvements in [**SS08a**] and [**DKSS13**]) and the *Dirac-Motzkin conjecture* (see [**GT13**]). For a nice survey about these topics, see [**Tao14**].

1.1. Green-Tao results

Given a set P of n points in the plane, an *ordinary line* is a line containing exactly two points of P. The classical *Sylvester-Gallai* theorem, first posed as a problem by Sylvester in 1893, asserts that as long as the points of P are not all collinear, P defines at least one ordinary line.

Theorem 1.1.1 (Sylvester-Gallai)**.** *Suppose that P is a set of n non-collinear points in $\mathbb{R}^2$. Then there exists at least one line passing through exactly two points of P.*

It is natural to ask what the the minimum number of ordinary lines (denoted by t_2) a set of n non-collinear points in the plane defines. In 1940 Melchior [**Mel41**], using projective duality and the Euler formula $V - E + F = 2$ gave the first proof of the Sylvester-Gallai Theorem. Specifically he proved $t_2 \geq 3$. In 1951 Motzkin [**Mot51**] showed that $t_2 \geq \sqrt{n}$. Csima and Sawyer in 1993 [**CS93**], improved this bound to $\frac{6n}{13}$. In general the number of ordinary lines for a random set of n points is expected to be of the order n^2, so when we speak about a set with few ordinary lines we mean a non-collinear set of n points with at most the order of n ordinary lines. The following example was observed by Böröczky, for more details see [**GT13**]. For every natural number m, we define

$$X_{2m} = \{[cos\frac{2\pi j}{m} : sin\frac{2\pi j}{m} : 1], 0 \leq j < m\} \cup \{[-sin\frac{\pi j}{m} : cos\frac{\pi j}{m} : 0], 0 \leq j < m\}.$$

Proposition 1.1.2 (Böröczky example)**.** *For X_{2m} as defined above, we have*

(1) *The set X_{2m} contains $2m$ points and spans precisely m ordinary lines.*
(2) *The set X_{4m} together with the origin $[0:0:1]$ contains $4m+1$ points and spans precisely $3m$ ordinary lines.*
(3) *The set X_{4m} minus $[0:1:0]$ on the line at infinity contains $4m-1$ points and spans precisely $3m-3$ ordinary lines.*

(4) *The set X_{4m+2} minus any of the $2m+1$ points on the line at infinity contains $4m+1$ points and spans precisely $3m$ ordinary lines.*

In 2013 Green and Tao, [**GT13**] showed that these configurations are best possible for sufficiently large n:

Theorem 1.1.3 (Dirac-Motzkin conjecture)**.** *If n is sufficiently large, then any set of n non-collinear points in the plane will define at least $\lfloor n/2 \rfloor$ ordinary lines. Furthermore, if n is odd, at least $3\lfloor n/4 \rfloor$ ordinary lines are defined.*

The *Dirac-Motzkin conjecture* asserts that the first part of this conjecture holds for every n and not only for sufficiently large n. However, there are examples of sets with $(n-1)/2$ ordinary lines, one for $n = 7$ [**KM58**] and one for $n = 13$ [**CM68**].

Let t_k denote the number of lines that meet exactly k points of an n-point configuration (we say such line is a *k-rich line*), so that t_3 is the number of 3-rich lines and t_2 is the number of ordinary lines. Then we have the double counting identity:

$$\sum_{k=2}^{n} \binom{k}{2} t_k = \binom{n}{2}.$$

Sylvester's cubic curve examples: cubic curves (smooth and non-smooth) give us examples of finite sets with few ordinary lines. The smooth case was observed by Sylvester first time in 1863. These examples do not provide the best examples of sets with few ordinary lines. However, that consideration is essential in order to solve the Dirac-Motzkin conjecture in [**GT13**]. On the other hand they have a crucial role in the statement of the structure theorem 1.1.9. Since both smooth and non-smooth cubic curves provide examples of a finite set with few ordinary lines, we consider them separately in the following.

We first consider smooth cubic curve over complex plane. Let γ be a smooth cubic curve in $\mathbb{P}^2(\mathbb{C})$. The group structure is well defined, we know that every such curve has 9 inflection points once we have chosen one of the inflection points as a neutral element. For $p, q, r \in \gamma$, the sum $p + q + r = 0$, if and only if $\{p, q, r\}$ are collinear. The inflection points are the points with $3p = 0$. Let H_n be a finite subgroup of γ of order n. Consider the points of H_n, the n tangent to γ in points of H_n are ordinary lines, provided they are not tangents in inflection points. Therefore $t_2 = n - w$ where w is the number of inflection points contained in H_n. Since $t_r = 0$ for $r \geq 4$ and $\frac{n(n-1)}{2} = t_2 + 3t_3$ we have the following proposition.

Proposition 1.1.4 (smooth cubic curve)**.** *Let H_n be a subgroup of order n of a smooth cubic curve. For this set we have*

$$t_2 = n - w, \quad t_3 = \lfloor \frac{n(n-3)}{6} \rfloor + \frac{w}{3}, \quad t_r = 0 \quad \text{for } r \geq 4,$$

where w is the number of inflection points contained in H_n.

Cyclic groups H_n can be realized over the reals. Then $w = 1$ or $w = 3$ and $t_3 = \lfloor \frac{n(n-3)}{6} \rfloor + 1$. You can find this construction in [**BGS74**] and [**Hir83**]. The following example is established in Ref [**BGS74**].

Proposition 1.1.5. *Let H_n be a subgroup of γ of order n. If $x \in \gamma$ is such that $x \notin H_n$ and $x + x + x \in H_n$ then the coset $x + H_n$ has $n - 1$ ordinary lines and $\lfloor \frac{n(n-3)}{6} \rfloor$ 3-rich lines.*

Singular cubic curves: If γ has a singular point it may be transformed into one of the following three (affine) forms. For more details (see [**Bix06**, Theorem 8.3]).

- (nodal case) $y^2 = x^2(x+1)$
- (cuspidal case) $y^2 = x^3$
- (acnodal case) $y^2 = x^2(x-1)$.

We have seen that by using a subgroup of a smooth cubic curve (elliptic curves) γ we can construct a finite set with few ordinary lines. On the other hand if γ is a singular cubic curve and γ^* is the smooth part of γ, then it is still possible to define a group structure on γ^*, such that three points $a, b, c \in \gamma^*$ are collinear if and only if $a+b+c=0$ ($+$ is the group operation on γ^*). The Propositions 1.1.4 and 1.1.5 were observed for the first time for cubic curves with singularities in [**BGS74**].

Notice that if γ is an irreducible cubic curve over the complex numbers, then the following theorem guarantees that for every natural number $n \geq 1$ there exists a subgroup of order n. For more details (see [**Bix06**, Chap. 9]).

Theorem 1.1.6 (Classification of group structure)**.** *Let γ be an irreducible cubic curve, and let γ^* be the set of nonsingular points of γ. Then we have the following possibilities for γ^*, considered as a group:*

- *(elliptic curve case)* $\mathbb{R}/\mathbb{Z}$ *or* $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, depending on whether γ has one or two components*
- *(nodal case)* $\mathbb{R} \times \mathbb{Z}/2\mathbb{Z}$
- *(cuspidal case)* $\mathbb{R}$
- *(acnodal case)* $\mathbb{R}/\mathbb{Z}$.

The second main result of Green-Tao [**GT13**] concerns the 3-rich lines of an n-point set. A simple double counting argument (counting pairs of distinct points in the set in two different ways) shows that there are at most

$$\binom{n}{2} / \binom{3}{2} = \frac{1}{6}n^2 - \frac{1}{6}n$$

3-rich lines. On the other hand Propositions 1.1.4 and 1.1.5 can provide examples of n-point sets with a large number of 3-rich lines ($\lfloor \frac{1}{6}n^2 - \frac{1}{2}n + 1 \rfloor$, to be precise). Sylvester then formally posed [**Syl93**] the question of determining whether this was best possible. This problem was known as the *Orchard problem*, and nearly half a century prior to Sylvester was given a as puzzle by Jackson [**Jac21**] in 1821.

Theorem 1.1.7 (Orchard planting problem)**.** *If n is sufficiently large, then any set of n points in the plane will determine at most $\lfloor \frac{1}{6}n^2 - \frac{1}{2}n + 1 \rfloor$ 3-rich lines.*

The proof of Theorems 1.1.3 and 1.1.7 follows from the structure theorem 1.1.9. Rather than direct proof for the lower bound on the number of ordinary lines or upper bound for the number of 3-rich lines, in [**GT13**] they instead try to prove a structure theorem for the set with few ordinary lines (or with very many 3-rich lines).

Before we state the structure theorems, note that all examples of the set with few ordinary lines that we have seen involved cubic curves (Propositions 1.1.2 1.1.4 1.1.5); either irreducible examples such as elliptic curves or non-smooth cubic curves, or reducible examples such as the union of a circle (or more generally, a conic section) and a line. Conversely it turns out that they are essentially the only way to produce such lines. The first structure theorem is called the weak structure theorem, although this theorem is strong enough to resolve the orchard planting problem for large n.

Theorem 1.1.8 (Weak structure theorem [**GT13**])**.** *Suppose that P is a finite set of n points in the plane. Suppose that P spans at most Kn ordinary lines for*

some $K \geq 1$. Suppose that $K \geq \exp\exp(CK^C)$ for some sufficiently large absolute constant C. Then all but at most $O(K^{O(1)})$ points of P lie on an algebraic curve γ of degree 3.

For proving the Dirac-Motzkin conjecture one needs a more powerful structure theorem for controlling the configuration of sets with few ordinary planes, it is called the strong structure theorem.

Theorem 1.1.9. *(Strong structure Theorem [GT13]) Let $K > 0$ and let n be sufficiently large depending on K. If a set of n points in $\mathbb{P}^2(\mathbb{R})$ spans at most Kn ordinary lines, then P differs in at most $O(K)$ points from an example of the following type*

(1) *$n - O(K)$ points on a line.*
(2) *The set*
$$\{[cos\frac{2\pi j}{m} : sin\frac{2\pi j}{m} : 1], 1 \leq j < m\} \cup \{[-sin\frac{\pi j}{m} : cos\frac{\pi j}{m} : 1], 1 \leq j < m\}$$
consisting of m points on the unit circle and m points on the line at infinity, for some $m = \frac{n}{2} + O(K)$
(3) *A coset $H \oplus g$, $3g \in H$, of a finite subgroup H of the non-singular real points on an irreducible cubic curve, with H having cardinality $n + O(K)$.*

The proof of Theorems 1.1.8 and 1.1.9 are based on the Melchior's argument of the Sylvester-Gallai Theorem 1.1.1. In the following we give a copy of this proof that you can find in Ref [GT13] and [Mel41].

Melchior's Proof of the Sylvester-Gallai Theorem: Let P be a set of n non-collinear points in $\mathbb{P}^2(\mathbb{R})$. Consider the dual set $P = \{p^* : p \in P\}$ of n lines in $\mathbb{P}^2(\mathbb{R})$. These lines determine a graph Γ_P in the projective plane whose vertices are the intersections of pairs of lines p_1^*, p_2^* (or equivalently points l^*, where l is a line joining two or more points of P), and whose edges are (projective) line segments of lines in P^* connecting two vertices of Γ_P with no vertices interior. Note that as the points in P were assumed not to lie on one line, every line in P^* must meet at least two vertices of Γ_P; in particular, the graph Γ_P contains no loops. It is however possible for a line to meet exactly two vertices in Γ_P in which case those two vertices are joined by two edges, rather than one. Also, by construction, each vertex of Γ_P is incident to at least two lines in P^*. As such, the graph Γ_P partitions the projective plane $\mathbb{P}^2(\mathbb{R})$ into some number V of vertices, some number E of edges, and some number F of faces each of which is the projective image of a polygon. In particular, each face has at least three edges, and any edge is incident to two distinct faces.

By Euler' formula in the projective plane $\mathbb{P}^2(\mathbb{R})$ we have

$$V - E + F = 1. \tag{1}$$

To proceed further, suppose that for each $k = 2, 3, 4, \ldots$ the set P has t_k k-rich lines. Then we have,

$$V = \sum_{k=2}^{n} t_k. \tag{2}$$

Which by duality is the number of lines defined by pairs of points in P. Furthermore the degree $\deg(l^*)$ of a vertex l^* in our graph is twice the number of lines in P^* passing through l^*, which is $2|P \cap l|$. Thus summing over all lines l,

$$2E = \sum_{l} \deg(l^*) = 2\sum_{l} |P \cap l| = \sum_{k=2}^{n} 2kt_k. \tag{3}$$

Finally for $s = 3, 4, 5, \dots$ write M_s for the number of faces in Γ_P with s edges. Since each edge is incident to exactly two faces, we have

$$2E = \sum_{s=3}^{n} sM_s. \tag{4}$$

Combining 1,2,3 and 4 gives the following expression for t_2, the number of ordinary lines

$$t_2 = 3 + \sum_{k=4}^{n}(k-3)t_k + \sum_{s=4}^{n}(s-3)M_s, \tag{5}$$

which among other things gives Melchior's bound $t_2 \geq 3$, which implies the Sylvester-Gallai theorem. □

The last Equation 5 shows that when the number of ordinary lines t_2 is small, the number of faces with more than 3 sides is also small. In particular when there are at most $O(n)$ ordinary lines, all faces except $O(n)$ of them are triangles. Thus in such cases the lines P^* must form locally a triangular grid.

The idea of the Green-Tao paper [**GT13**] is based on following idea. Suppose that P is a set of n non-collinear points in $\mathbb{P}^2(\mathbb{R})$ with few ordinary lines, then by the Equation 5, the graph Γ_P in the dual plane $\mathbb{P}^2(\mathbb{R})$ contains many hexagons. In other words the lines in P^* must form locally a triangular grid. By applying Chasles' version of the Cayley-Bacharach theorem, we can convert dual triangular grids (produced by Melchior's argument) into cubic curves that meet many points of the original configuration P).

Theorem 1.1.10 (Chasles)**.** *Suppose that two triples of lines meet each other transversely in nine distinct points. Then any cubic curve that passes through eight of these points, also passes through the ninth.*

In the Appendix 8.4 we will consider a classical theorem in web geometry. Theorem A.2.3 concerns infinite sets, say P, in the plane which have no ordinary lines (more precisely every line passing through two points of P meets P in one more point).

On the sets with many k-rich lines for $k \geq 3$: Theorem 1.1.7 asserts that if you have a set of n points in the plane with at least $(\frac{1}{6}n^2 - O(n))$ three rich lines, then there exists an algebraic cubic curve γ such that almost every point of P lies on γ. On the other hand in a similar vein Elekes-Szabó [**GE13**] proved

Theorem 1.1.11. *If C is an irreducible curve of degree d in $\mathbb{R}^2$, and contains a set $\mathcal{H}$ of n points with cn^2 3-rich lines for some constant independent of n, then C is a cubic curve, provided that $n \geq n_0(c, d)$.*

The main ingredients in the proof of the above theorem are the Graf-Sauer Theorem A.2.3 and a theorem in incidence geometry that asserts that if some appropriate algebraicity conditions hold then (apart from being a cylinder) the only way for a surface $V := F(x, y, z) = 0$ to contain a near-quadratic number of points $cn^{2-\delta}$ (δ and c are independent of n) from a product set $X \times Y \times Z$ is that there are one-to-one analytic functions $f, g, h\colon (-1, 1) \longleftarrow \mathbb{R}$ with analytic inverses such that V contains the $f \times g \times h$-image of a part of the plane $x + y + z = 0$ near the origin:

$$\Big\{\big(f(x), g(y), h(z)\big) \in \mathbb{R}^3; \quad x, y, z \in (-1, 1); \quad x + y + z = 0\Big\} \subseteq V.$$

In the same circle of ideas, in the early 60s, Erdös asked the following question: is it possible for a set of points in the real plane to contain many collinear four-tuples, but to contain no five points on a line? Here by "many" we mean a number which

is quadratic in terms of the cardinality of the set of points. In [**SS13**], Solymosi pointed out that, if we weaken the quadratic condition, then the problem has a affirmative solution. Given a set P of points in the plane, a line is called *k-rich*, if it contains precisely k points of P. For example, a 2-rich line is an ordinary line. Then, Solymosi's theorem reads as:

Theorem (Solymosi)**.** *For any $k \geq 4$, there is a positive integer n_0 such that for all $n > n_0$ there exists $P \subseteq \mathbb{R}^2$ such that there are at least $n^{2-\frac{c}{\sqrt{\log n}}}$ k-rich lines, but no $k+1$-rich lines. Here, $c = 2\log(4k+1)$.*

Along similar lines: Elekes-Szabó [**GE13**] proved

Theorem 1.1.12. *In $\mathbb{R}^2$ no irreducible algebraic curve of degree d can accommodate n points with cn^2 4-rich lines if $n \geq n_0(c,d)$ (c is independent of n).*

Remark 1.1.13. In [**RSDZ16a**] it has been shown that the Theorems 1.1.11, 1.1.12 are valid when we replace $\mathbb{R}$ with $\mathbb{C}$.

1.1.1. Sylvester-Gallai type problems over complex numbers. Here we have to mention that in the statement of the Sylvester-Gallai Theorem 1.1.1 if we replace $\mathbb{R}$ with $\mathbb{C}$, then the theorem does not hold. In the following paragraphs we state some result about Sylvester-Gallai problems over complex plane.

Definition 1.1.14. A Sylvester-Gallai (SG) configuration is a finite set S of points such that the line through any two points in S contains a third point of S.

Recall that a point p of an algebraic curve C is called an inflexion point if the tangent to C at p has triple contact with C. The following Sylvester-Gallai configuration was observed by Serre in [**Ser66**]. The cubic curve with homogeneous equation $x^3+y^3+z^3+xyz$ in the complex projective plane has nine inflection points given by homogeneous coordinates

$$S = \bigcup_{w^3=1} \Big\{(0:-1:w),(w:0:-1),(-1:w:0)\Big\}.$$

The following theorem shows that S has no ordinary lines [**BHW11**, Theorem 3.1].

Theorem 1.1.15. *Let C be a cubic curve defined over K. If p_1,p_2 are two distinct inflexion points of C lying in $\mathbb{P}^2(K)$, and the line $l = p_1p_2$ meets C again in p_3, then p_3 is also an inflexion point of C.*

Proof. Let l_i be the tangent line to C at the point p_i, $i = 1,2,3$, and let $C \cap l_3 = 2p_3 + r$. Define two cubics $D = l^3$ and $D' = l_1l_2l_3$. Then we have

$$C \cap D = 3p_1 + 3p_2 + 3p_3 \quad C \cap D' = 3p_1 + 3p_2 + 2p_3 + r.$$

So by the Chasles Theorem 1.1.10, $r = p_3$; that is $C \cap l_3 = 3p_3$ and so by definition p_3 is an inflexion point. □

On the other hand Hirzebruch in [**Hir83**] used deep results in algebraic geometry to show that for every n points in the complex plane such that no $n-2$ of them are collinear, either t_2 or t_3 must be non-zero. More precisely

Theorem 1.1.16 (Hirzebruch)**.** *Let P a set of n points in the complex plane such that $t_{n-2} = t_{n-1} = t_n = 0$. Then*

$$t_2 + \frac{3}{4}t_3 \geq n + \sum_{i\geq 5}(2i-9)t_i.$$

Similarly if not many points of a given finite set P are collinear we have the following theorem see [**Lan03**].

Theorem 1.1.17 (Langer). *Let P be a set of n points in $\mathbb{C}^2$, with at most $\frac{2n}{3}$ points collinear. Then*

$$\sum_{i\geq 2} it_i \geq \frac{n(n+3)}{3}. \tag{6}$$

Serre [**Ser66**] asked whether any SG configuration in $\mathbb{P}^n(\mathbb{C})$ must be coplanar. This was proved by Kelly [**Kel86**] using Hirzebruch's inequality. Twenty years later, in [**EPS06**] authors gave an elementary proof.

Theorem 1.1.18 (Kelly). *Every SG configuration in $\mathbb{P}^n(\mathbb{C})$ is coplanar.*

In the same circles of ideas, in [**SS08b**] the authors [1] used some elementary ideas to prove the following Sylvester-Gallai type theorems involving incidences between points and lines in the planes over the complex numbers.

Theorem 1.1.19 (Solymosi-Swanepoel 1). *Let S be a finite non-collinear subset of $\mathbb{C}^2$. Then there exists a line l such that $2 \leq |S \cap l| \leq 5$.*

Theorem 1.1.20 (Solymosi-Swanepoel 2). *Let $A, B \subset \mathbb{C}$ with $2 \leq |A|, |B| < \infty$. Then there exists a line l in $\mathbb{C}^2$ such that $|(A \times B) \cap l| = 2$.*

1.2. Circle version of the Sylvester-Gallai theorem

As we have seen in the previous section the classical Sylvester-Gallai theorem states any non-collinear finite set in the plane spans at least one ordinary line. A more sophisticated statement is the so-called Dirac-Motzkin conjecture, according to which every non-collinear set of $n > 13$ points in $\mathbb{R}^2$ determines at least $n/2$ ordinary lines. This conjecture was proved by Green and Tao [**GT13**] for all sufficiently large n. Their proof was based on a structure theorem, which roughly states that any point set with a linear number of ordinary lines must lie mostly on a cubic curve (see Theorem 3.3.3 for a precise statement).

It is natural to ask the corresponding question for *ordinary circles* (circles that contain exactly three of the given points); see for instance [**BMP05**, Section 7.2] or [**KW91**, Chapter 6]. Elliott [**Ell67**] introduced this question in 1967, and proved that any n points, not all on a line or a circle, determine at least $\frac{2}{63}n^2 - O(n)$ ordinary circles. He suggested, cautiously, that the optimal bound is $\frac{1}{6}n^2 - O(n)$. Elliott's result was improved by Bálintová and Bálint [**BB94**, Remark, p. 288] to $\frac{11}{247}n^2 - O(n)$, and Zhang [**Zha11**] obtained $\frac{1}{18}n^2 - O(n)$. Zhang also gave constructions of point sets on two concentric circles with $\frac{1}{4}n^2 - O(n)$ ordinary circles.

In this thesis we will use the results of Green and Tao (see Chapter 3) to prove that $\frac{1}{4}n^2 - O(n)$ is asymptotically the right answer, thus disproving the bound suggested by Elliott [**Ell67**].

We will find the exact minimum number of ordinary circles, for sufficiently large n, and we will determine which configurations attain or come close to that minimum. We make no attempt to specify the threshold implicit in the phrase 'for sufficiently large n'; any improvement would depend on an improvement of the threshold in

[1] In this paper authors considered the Sylvester-Gallai Theorem on the finite subset of complex numbers and quaternions $\mathbb{H}$.

the result of Green and Tao [**GT13**]. For small n, the bound $\frac{1}{9}\binom{n}{2}$ due to Zhang [**Zha11**] remains the best known lower bound on the number of ordinary circles.

As we mentioned in Section 1.1 Green and Tao [**GT13**] also solved (for large n) the even older orchard problem, which asks for the exact maximum number of lines passing through exactly three points of a set of n points in the plane. The analogous orchard problem for circles asks for the maximum number of circles passing through exactly four points from a set of n points. As far as we know, this question has not been asked before. We determine the exact maximum and the extremal sets for all sufficiently large n.

Our first main result concerns the minimum number of ordinary circles spanned by a set of n points, not all lying on a line or a circle, and the structure of sets of points that come close to the minimum. The first part of the theorem solves Problem 6 in [**BMP05**, Section 7.2].

Theorem 1.2.1 (Ordinary circles)**.**

(1) *If n is sufficiently large, the minimum number of ordinary circles determined by n points in $\mathbb{R}^2$, not all on a line or a circle, equals*

$$\begin{cases} \frac{1}{4}n^2 - \frac{3}{2}n & \text{if } n \equiv 0 \pmod 4, \\ \frac{1}{4}n^2 - \frac{3}{4}n + \frac{1}{2} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - n & \text{if } n \equiv 2 \pmod 4, \\ \frac{1}{4}n^2 - \frac{5}{4}n + \frac{3}{2} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines fewer than $\frac{1}{2}n^2 - Cn$ ordinary circles, then P lies on the disjoint union of two circles, or the disjoint union of a line and a circle.*

In Chapter 3, we will describe constructions that meet the lower bound in part 1 of Theorem 1.2.1. For even n, the bound in part 1 is attained by certain constructions on the disjoint union of two circles, while for odd n, the bound is attained by constructions on the disjoint union of a line and a circle. The main tools in our proof are circle inversion and the structure theorem of Green and Tao [**GT13**] for sets with few ordinary lines, together with some classical results about algebraic curves and their interaction with inversion.

Let us define a *generalised circle* to be either a circle or a line. Because inversion maps circles and lines to circles and lines, it turns out that in our proof it is more natural to work with generalised circles. Alternatively, we could phrase our results in terms of the *inversive plane* (or *Riemann sphere*) $\mathbb{R}^2 \cup \{\infty\}$, where ∞ is a single point that lies on all lines, which can then also be considered as circles. Yet another equivalent view would be to identify the inversive plane with the sphere $\mathbb{S}^2$ via stereographic projection, and consider circles on $\mathbb{S}^2$, which are in bijection with generalised circles. All our statements about generalised circles in $\mathbb{R}^2$ could thus be formulated in terms of circles in $\mathbb{R}^2 \cup \{\infty\}$ or on $\mathbb{S}^2$.

We define an *ordinary generalised circle* to be one that contains three points from a given set. Our proof of Theorem 3.4.6 proceeds via an analogous theorem for ordinary generalised circles, which turns out to be somewhat easier to obtain.

Theorem 1.2.2 (Ordinary generalised circles)**.**

(1) *If n is sufficiently large, the minimum number of ordinary generalised circles determined by n points in $\mathbb{R}^2$, not all on a generalised circle, equals*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines fewer than $\frac{1}{2}n^2 - Cn$ ordinary generalised circles, then P lies on two disjoint generalised circles.*

We also solve the analogue of the orchard problem for circles (for sufficiently large n). We define a 4-*point* (*generalised*) *circle* to be a (generalised) circle that passes through exactly four points of a given set of n points. The 'circular cubics' in part 2 will be defined in Section 2.2.

Theorem 1.2.3 (4-point generalised circles)**.**

(1) *If n is sufficiently large, the maximum number of 4-point generalised circles determined by a set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 2 & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3, 5, 7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2, 6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-point generalised circles, then up to inversions, P lies on an ellipse or a smooth circular cubic.*

Theorem 1.2.3 remains true if we replace 'generalised circles' by 'circles'. This is because we can apply an inversion to any set of n points with a maximum number of generalised circles in such a way that all straight-line generalised circles become circles. Therefore, the maximum is also attained by circles only.

The proofs of the above theorems are based on the following structure theorems in the style of Green and Tao [**GT13**]. The first gives a rough picture, by stating that a point set with relatively few ordinary generalised circles must lie on a bicircular quartic, a specific type of algebraic curve of degree four that we introduce in Section 2.2.

Theorem 1.2.4 (Weak structure theorem)**.** *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary generalised circles, then all but at most $O(K)$ points of P lie on a bicircular quartic.*

Ball [**Bal18**] concurrently obtained a similar result as a consequence of a structure theorem for ordinary planes in $\mathbb{R}^3$. He shows that n points with $O(n^{2+\frac{1}{6}})$ ordinary circles must lie mostly on a quartic curve.

We define bicircular quartics in Section 2.2; they can be reducible, so in Theorem 1.2.4 the set P may also lie mostly on a lower-degree curve contained in a bicircular quartic. Our proof actually gives a more precise list of possibilities. The curve that P mostly lies on can be: a line; a circle; an ellipse; a line and a disjoint circle; two disjoint circles; a circular cubic that is acnodal or smooth; or a bicircular quartic that is an inverse of an acnodal or smooth circular cubic.

A more precise characterisation of the possible configurations with few ordinary generalised circles is given in the following theorem. The group structures referred to in the theorem are defined in Section 3.1; the circular points at infinity (α and β) referred to in Case 3 are introduced in Section 2.2; and the 'aligned' and 'offset' double polygons are defined in Section 3.2.

Theorem 1.2.5 (Strong structure theorem)**.** *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary generalised circles, then up to inversions and similarities, P differs in at most $O(K)$ points from a configuration of one of the following types:*

(1) *A subset of a line;*
(2) *A subgroup of an ellipse;*
(3) *A coset $H \oplus x$ of a subgroup H of a smooth circular cubic, for some x such that $4x \in H \oplus \alpha \oplus \beta$, where α and β are the two circular points at infinity;*
(4) *A double polygon that is 'aligned' or 'offset'.*

Conversely, every set of these types defines at most $O(Kn^2)$ ordinary generalised circles.

1.3. Incidence between curves and lines in the finite plane

As we have seen the Sylvester-Gallai Theorem does not hold in complex plane. This is not too hard to construct a counterexample to show that this theorem does not hold over finite field too. For example consider all points in $\mathbb{F}_q^2$, where q is a prime power. However in this thesis we will study the behaviour of the number of k-rich lines determined by the set of points corresponding to the some algebraic plane curve in probability point of view. More formally, what is the probability that a random line in the (affine or projective) plane intersects a curve of given degree in a given number of points? More precisely, what happens if we consider a finite field with q elements as base field, and then we ask the same question for a field with $q^2, q^3, \ldots, q^N$ elements, analyzing how these probabilities behave as N goes to infinity? In this work we investigate this problem by means of algebro-geometric techniques.

Here, we consider an algebraic plane curve C of degree d over a finite field $\mathbb{F}_q$ with q elements, where q is a prime power, namely the set of points in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$ that are zeros of a homogeneous trivariate polynomial of degree d. Given such a curve, we can define the probability for a line in $\mathbb{P}^2(\mathbb{F}_q)$ to intersect it in exactly k points. Notice that here we consider the mere set-theoretic intersection: no multiplicities are taken into account. We can then consider the same kind of probability, keeping the same curve C — namely, the same trivariate polynomial — but changing the base field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and so on. In this way, for every $N \in \mathbb{N}$ we define the numbers $p_k^N(C)$, namely the probability for a line in $\mathbb{P}^2(\mathbb{F}_{q^N})$ to intersect C in exactly k points. If the limit as N goes to infinity of the sequence $\left(p_k^N(C)\right)_{N\in\mathbb{N}}$ exists, we denote this number by $p_k(C)$. The main tool we use to compute these numbers when the curve C is absolutely irreducible and with *simple tangency* is an effective version of the *Chebotarev theorem* for function fields. Here, by *absolutely irreducible* we mean that the curve is irreducible over the algebraic closure of its field of definition. By asking that the curve has *simple tangency* we require that there exists a line whose intersection with C consists of simple intersections except for one, which is a double intersection. These are the main results that we investigate about them in Chapter 4:

Theorem 1.3.1. *Let C be an absolutely irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Then the numbers $\{p_k(C)\}$ are well-defined, namely the corresponding limits exist.*

Theorem 1.3.2. *Let C be an absolutely irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \dots, d\}$ we have*

$$p_k(C) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

In particular, $p_{d-1}(C) = 0$ and $p_d(C) = 1/d!$.

A consequence of this theorem is that the question by Erdös we already mentioned — asking whether there exists a set of points in the plane containing many collinear four-tuples, but not containing any five points on a line — has a positive answer for the plane over a finite field.

Corollary 1.3.3. *Let C be an absolutely irreducible plane algebraic curve of degree 4 in the plane $\mathbb{P}^2(\mathbb{F}_q)$. By Theorem 2.1.35, the curve C has $cq+O(\sqrt{q})$ elements for some $c > 0$, and by Theorem 4.0.2 it has ϵq^2 4-rich lines for some $\epsilon > 0$, after possibly taking a finite extension of the base field, since $p_4(C) > 0$. Hence, if we take P as the set of points of C, then P spans a quadratic number of 4-rich lines, but no five points of P are collinear.*

We approached this problem using Galois theory techniques; during a revision of our work, we have been informed that some of the questions investigated in following thesis (or similar ones) have already appeared in the literature, though expressed in a different language and with different purposes (see [**BSJ12**] and [**Die12**]). Both the two cited paper use the Chebotarev theorem for function field as a key ingredient. After studying Chebotarev theorem, we realized that we could use it to provide a much shorter proof for our result than the one we initially used, and that our initial approach, although we were not aware of that, did not differ too much from the techniques that lead to Chebotarev theorem. Because of this, in Chapter 4 we report our initial approach to the problem, and then in Chapter 5 we explain how to use Chebotarev theorem to obtain Theorem 4.0.2. After that, we show how the same technique provides a formula for the probabilities of intersection between a given plane curve of degree d and a random plane curve of degree e.

Proposition 1.3.4. *Let C be an absolutely irreducible algebraic curve of degree d in $\mathbb{P}^2$ over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Let $e \in \mathbb{N}$ be a natural number. Then for every $k \in \{0, \dots, de\}$ we have*

$$p_k(C, e) = \sum_{s=k}^{de} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

We briefly summarize how the problem we investigate is discussed in the aforementioned literature. In [**BSJ12**], the focus is a variant of the so-called *Bateman-Horn conjecture* for polynomial rings of finite fields. The original Bateman-Horn conjecture concerns the frequency of prime numbers among the values of a system of polynomials at integer numbers. One of its consequences is *Schinzel conjecture*, which asks whether, given polynomials $f_1, \dots, f_r \in \mathbb{Z}[x]$, then for infinitely many $n \in \mathbb{Z}$ we have that $f_1(n), \dots, f_r(n)$ are all prime. Bary-Soroker and Jarden consider the situation in which $\mathbb{Z}$ is replaced by $\mathbb{F}_q[t]$ for some prime power q. More precisely, given polynomials $f_1, \dots, f_r \in \mathbb{F}_q[t][x]$, they want to compute the number

of polynomials $g \in \mathbb{F}_q[t]$ such that $f_1\big(t, g(t)\big), \dots, f_r\big(t, g(t)\big)$ are irreducible. In particular, they focus on the case when g is linear, namely on the computation of the pairs $(a_1, a_2) \in \mathbb{F}_q^2$ such that $f_1(t, a_1t + a_2), \dots f_r(t, a_1t + a_2)$ are irreducible. In our language, this is the number of lines in the plane such that the polynomial obtained by restricting a plane curve on such a line is irreducible. The authors improve a result by Bender and Wittenberg (see [**BW05**, Theorem 1.1 and Proposition 4.1]) and show that this number goes as q^2/d. To prove this, they make use of an effective version of the Chebotarev density theorem (see the appendix of [**ABSR15a**]). The number computed by Bary-Soroker and Jarden is similar to the quantity p_0 that we define, though it is not the same, since it can happen that a line does not intersect a curve at any point over $\mathbb{F}_q$, but the polynomial given by the restriction of the curve to the line can be reducible. Also the behaviour as $d \to \infty$ of these two quantities is different: the one by Bary-Soroker and Jarden goes to zero, while p_0 tends to $1/e$.

In [**Die12**], the author focuses on the complexity of computation of the so-called *discrete logarithm* in the group of divisors of degree 0 of a nonsingular curve. Given two elements a and b in a group G, the discrete logarithm $\log_b a$ is an integer k such that $b^k = a$. On a smooth curve C, one can consider formal integer sums of points of C, and define an equivalence relation on them in order to obtain the class group of C. One can therefore try to compute discrete logarithms in the class group of a curve, and in particular for those formal integer sums of points whose coefficients add up to zero, namely the ones of degree 0; this has important applications in cryptography. In [**Die12**, Theorem 2], Diem proves that computing the discrete logarithm has an expected time of $\tilde{O}(q^{2-\frac{2}{d-2}})$ for those curves defined over $\mathbb{F}_q$ that admit a birational plane model D of degree d such that there exists a line in the plane intersecting D in d distinct points over $\mathbb{F}_q$. Then the author computes the number of lines in the plane intersecting D in exactly d points over $\mathbb{F}_q$ (see [**Die12**, Theorem 3]), namely the quantity $p_d(D)$ in our language. As in the previous paper, this is done using an effective version of Chebotarev density theorem (see [**ABSR15b**]).

Recently, a new paper [**Ent18**] appeared dealing with the same problem we investigate in our work, but allowing the given curve to be constituted of several irreducible components.

CHAPTER 2

Preliminaries

The aim of this chapter is to introduce preliminary results that majority of them have been established elsewhere in the literature, however some of these result still are new.

2.1. Galois Group

Definition 2.1.1. Let E and F be two fields and suppose E/F is a field extension. Then we say that E is a *Galois extension* of F if the field fixed by the automorphism group $\mathrm{Aut}(E/F)$ is precisely the base field F.

Definition 2.1.2. Suppose F is a field and $\alpha \in F$. Suppose $p(x) \in F[x]$ is the minimal polynomial of α, then the roots of p is called the *conjugate* of α over F.

Definition 2.1.3. The algebraic field extension L/F is *normal* if $\alpha \in L$ then all conjugates of α over F belong to L

Definition 2.1.4. If E is an extension of F in which a polynomial $p(x) \in F[x]$ can be factored into linear factor, and if $p(x)$ can not be so factored in any intermediate field, then we call E a *splitting field* for $p(x)$. Thus, if E is a splitting field of $p(x)$, the roots of p generate E.

Definition 2.1.5. A *separable extension* is an algebraic field extension $E \supset F$ such that for every $\alpha \in E$, the minimal polynomial of α over F is a separable polynomial i.e., its formal derivative is not zero.

Theorem 2.1.6 (Artin Theorem)**.** *For a finite extension E/F, each of the following statements is equivalent to the statement that E/F is Galois*

(1) *E/F is a normal extension and a separable extension.*
(2) *E is a splitting field of a separable polynomial with coefficients in F.*
(3) *$|Aut(E/F)| = [E : F]$, that is, the number of automorphisms equals the degree of the extension.*

Definition 2.1.7. Let E/F be a field extension. An element $\alpha \in E$ is a *primitive element* when $E = F(\alpha)$.

Theorem 2.1.8 (Primitive element)**.** *Let E/F be a separable extension of finite degree. Then $E = F(\alpha)$ for some $\alpha \in E$; that is, the extension is simple and α is a primitive element.*

For more details you can see [[**Sha94**] Chapter 2]

Definition 2.1.9. Let X and Y be irreducible varieties of the same dimension and $f\colon X \longrightarrow Y$ a regular map such that $f(X) \subset Y$ is dense. The degree of the field extension $f^*(K(Y)) \subset K(X)$, which is finite under these assumption, is called the *degree* of f:

$$\deg f = [K(X) : f^*(K(Y))].$$

Definition 2.1.10. A domain R is called *normal* if it is integrally closed in its field of fractions. i.e for every $a \in K$ satisfying in an equation $a^n + t_{n-1}a^{n-1} + \dots a_0 = 0$ we have $a \in R$.

Definition 2.1.11. In algebraic geometry, an algebraic variety or scheme X is *normal variety* if it is normal at every point, meaning that the local ring at the point is an integrally closed domain. An affine variety X (understood to be irreducible) is normal if and only if the ring $O(X)$ of regular functions on X is an integrally closed domain.

Theorem 2.1.12. *If $f\colon X \longrightarrow Y$ is a finite map of irreducible varieties, and Y is normal, then the number of inverse image of any point $y \in Y$ is $\leq \deg f$.*

Definition 2.1.13. f is *unramified* over $y \in Y$ if the number of inverse image of y is equals the degree of the map. Otherwise, we say that f is *ramified* at y, or that y is a *ramification* point or a *branch* point of f.

Theorem 2.1.14. *The set of points at which a map is unramified is open, and is nonempty if $f^*(K(y)) \subset K(X)$ is a separable field extension.*

Corollary 2.1.15. *If X and Y are curves in the above theorem, then the number of ramification points are finite.*

2.1.1. Algebraic galois group of a plan curve. The aim of this section is to recall a construction (see [**Rat87**] [**MSG18**]) that associates a Galois group to a plane algebraic curve. We will see in the following sections that this group determines the irreducibility of certain surfaces; this will be the key to derive a formula for the probabilities we are interested in.

Let q be a prime power, namely $q = p^r$ for some prime number p. We denote by $\mathbb{F}_q$ the finite field with q elements. Let C be an absolutely irreducible algebraic curve in $\mathbb{P}^2(\mathbb{F}_q)$. Define

$$X_1 := \big\{(w, [\ell]) \in C \times \check{\mathbb{P}}^2(\mathbb{F}_q) : w \in \ell\big\} \quad \text{and} \quad X_0 := \check{\mathbb{P}}^2(\mathbb{F}_q).$$

Here $\check{\mathbb{P}}^2(\mathbb{F}_q)$ denotes the *dual* projective plane, namely the projective plane whose points are in bijection with the lines in $\mathbb{P}^2\big(\mathbb{F}_q\big)$. For a line $\ell \subset \mathbb{P}^2(\mathbb{F}_q)$, we write $[\ell]$ for the corresponding point in $\check{\mathbb{P}}^2(\mathbb{F}_q)$. The correspondence is given by

$$\check{\mathbb{P}}^2(\mathbb{F}_q) \ni (a : b : c) \quad \longleftrightarrow \quad \big\{(x : y : z) \in \mathbb{P}^2(\mathbb{F}_q) \,:\, ax + by + cz = 0\big\}.$$

Definition 2.1.16. Using the notation we have already introduced, we define the map $\pi\colon X_1 \longrightarrow X_0$ to be the projection onto the second component.

Since X_0 is irreducible, we can define its *function field*, denoted $K(X_0)$. This is the field of equivalence classes of morphisms $\varphi\colon U \longrightarrow \mathbb{F}_q$, where U is any (Zariski) open subset of X_0; two morphisms are considered equivalent if they agree on a non-empty open subset. Consider the projection $\rho\colon X_1 \longrightarrow C$ on the first component: its fibers are lines in $\check{\mathbb{P}}^2\big(\mathbb{F}_q\big)$, because the elements in the fiber over a point $w \in C$ correspond to the lines in $\mathbb{P}^2\big(\mathbb{F}_q\big)$ through w. Hence all these fibers are irreducible varieties of the same dimension. This implies that X_1 is irreducible by [**Sha94**, Chapter 1, Section 6.3, Theorem 1.26]; its function field is denoted $K(X_1)$.

Lemma 2.1.17 (see [**Rat87**, Definition 1.3])**.** *The projection $\pi\colon X_1 \longrightarrow X_0$ is a quasi-finite dominant separable morphism of degree d.*

Because of Lemma 2.1.17, the induced map $\pi^*\colon K(X_0) \longrightarrow K(X_1)$ between fields of rational functions realizes $K(X_1)$ as a finite separable extension of $K(X_0)$ of degree d. By the primitive element theorem, the field $K(X_1)$ is generated over $K(X_0)$

by a single rational function $h \in K(X_1)$ satisfying $P(h) = 0$ for an irreducible monic polynomial P over $K(X_0)$ of degree d.

Definition 2.1.18 (Galois group, see [**Rat87**, Definition 1.3])**.** Using the notation just introduced, we define the *Galois group* $\mathrm{Gal}(C)$ of C to be the Galois group of a splitting field of the polynomial P over $K(X_0)$. In other words, $\mathrm{Gal}(C)$ is the Galois group of a Galois closure (see [**Row06**, Remark 4.77]) of the field extension $K(X_0) \hookrightarrow K(X_1)$. The group $\mathrm{Gal}(C)$ is independent of the choice of h and it can be regarded as a subgroup of the permutation group S_d of the roots of P.

Definition 2.1.19 (Simple tangency [**MSG18**])**.** Let C be an absolutely irreducible curve of degree d in $\mathbb{P}^2(\overline{\mathbb{F}_q})$. We say that C has *simple tangency* if there exists a line $\ell \subseteq \mathbb{P}^2(\overline{\mathbb{F}_q})$ intersecting C in $d-1$ smooth points of C such that ℓ intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point.

Remark 2.1.20. A general curve $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ of degree d has simple tangency. In fact, notice that having simple tangency is an open condition, therefore it is enough to exhibit a single example in order to obtain the claim. To do that, consider the curve of equation

$$x^2\, P(x,y) + z\, Q(x,y,z) = 0,$$

where P is a homogeneous polynomial with $d-2$ distinct roots in $\overline{\mathbb{F}}_a$ and Q is a homogeneous polynomial of degree $d-1$.

In the following we give tw examples of curves without simple tangency. More precisely, we will show that there exist a curve of degree $q+1$ in $\mathbb{F}_q$ (to simplify the calculation we assume q is odd) such that tangent line at each point intersects the curve in only two points, one with multiplicity q and the other with multiplicity 1

Example 2.1.21. *Consider the curve C given by*

$$x^q y + y^q z + z^q x = 0. \tag{7}$$

This is a curve of degree $q+1$; the equation of tangent line at an arbitrary point (x_0, y_0, z_0) on the curve is given by $z_0^q x + x_0^q y + y_0^q z = 0$.

Consider the affine part corresponding to $z = 1$, then the equations of curve and tangent line at $(x_0, y_0, 1)$ are $x^q y + y^q + x = 0$ and $x_0^q y + x + y_0^q = 0$, respectively.

To obtain the intersection points of C and its tangent line we substitute $x = -(x_0^q y + y_0^q)$ in the affine equation of C

$$-(x_0^q y + y_0^q)^q y + y^q - x_0^q y - y_0^q = 0, \tag{8}$$

hence

$$-x_o^{q^2} y^{q+1} + y^q - (x_o^q + y_0^{q^2}) y - y_0^q = 0. \tag{9}$$

Claim: y_0 is a root of multiplicity q of Equation 9:

If $(y-y_0)^q$ is a factor of the Equation 9, then it means there exist $A, B \in \mathbb{F}_q$ such that:

$$(y-y_0)^q (Ay + B) = -x_o^{q^2} y^{q+1} + y^q - (x_o^q + y_0^{q^2}) y - y_0^q. \tag{10}$$

Notice that $(y-y_0)^q = y^q - y_0^q$, and we obtain

$$Ay^{q+1} - Ay_0^q y + By^q - By_0^q = -x_o^{q^2} y^{q+1} + y^q - (x_o^q + y_0^{q^2}) y - y_0^q. \tag{11}$$

It implies $A = -x_0^{q^2}$ and $B = 1$. However, we need the coefficients of y to be equal in both side of the Equation 11 this holds, in fact if we compare the coefficients of y

on both sides of the Equation 11, we have $x_o^q + y_0^{q^2} = Ay_0^q$. *Now substitute* $A = x_0^{q^2}$, *thus*

$$x_0^q + y_0^{q^2} = -x_o^{q^2} y_0^q \quad \textit{equivalently we must have} \quad x_0^q + y_0^{q^2} + x_0^{q^2} y_0^q = 0.$$

By applying the inverse of Frobenius map on the last equation, we get that $x_0 + y_0^q + x_0^q y_0^q$ *must be zero. But this is a consequence of this fact that* (x_o, y_0) *is a point on the curve 7* C *and this completes the proof.*

Actually, we have shown that the tangent line at $(x_0, y_0, 1)$ *intersects the affine part of* $x^q y + y^q z + z^q x = 0$ *corresponding to* $z = 1$ *in two points. Hence if we suppose* $q \geq 2$, C *cannot have simple tangency.*

As another example consider the curve given by $x^{q+1} + y^{q+1} + z^{q+1} = 0$, this is also is a curve of degree $q+1$ over $\mathbb{F}_q$ such that every tangent line intersects this curve in only two points.

Proposition 2.1.22 ([**Rat87**, Proposition 2.1])**.** *Let* $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ *be an absolutely irreducible plane curve of degree* d *with simple tangency. Then the Galois group* $\mathrm{Gal}(C)$ *of* C *is the whole symmetric group* S_d.

2.1.2. Geometry Galois group and Galois theory for étale maps. In the preceding section we associated a Galois group to any planer curves, namely algebraic Galois group. In this section we associate a *geometry Galois group* to an algebraic planer curve and latter on we will see the algebraic Galois group and geometry Galois group associated to an algebraic curves are isomorphic [see [**MSG18**]].

For doing this we first associate a Galois group to a morphism (satisfying certain conditions) between two irreducible smooth varieties.

Note. All varieties considered in this section are supposed to be defined over an algebraically closed field.

For technical reasons, we develop the theory for a special class of morphisms, namely the one of *étale* maps. They model, in the algebraic setting, the notion of "local isomorphism" for the analytic topology. Recall that, in differential geometry, a smooth map between two smooth manifolds is a *local diffeomorphism* if it induces an isomorphism at the level of tangent spaces. For an affine variety X cut out by polynomials $P_1, \ldots, P_r$, one defines the *tangent cone* $C_x(X)$ of X at the origin as the variety defined by the homogeneous parts of minimal degree of each of the polynomials $P_1, \ldots, P_r$; the tangent cone at any other point is obtained by translating it to the origin and by applying the previous definition. The tangent cone plays for étale morphisms the role played by the tangent space for local diffeomorphisms:

Definition 2.1.23 (Étale map)**.** A morphism $f\colon X \longrightarrow Y$ between irreducible varieties is *étale at a point* $x \in X$ if f induces an isomorphism between the tangent cones $C_x(X)$ and $C_{f(x)}(Y)$. A map is called *étale* if it is étale at every point.

Definition 2.1.24. Let $f\colon X \longrightarrow Y$ be a finite separable dominant étale map of degree d between two irreducible smooth varieties. We define the *Galois scheme* (see [**Vak06**, Section 3]) of f as

$$\mathrm{GS}(f) := \big\{(x_1, \ldots, x_d) \in X^d \,:\, f(x_1) = \cdots = f(x_d),\ x_i \neq x_j \text{ for all } i \neq j\big\}.$$

Notice that the Galois scheme is the fiber product of d copies of the map f minus the big diagonal. Because of this, and since f is a finite map, we have

$$\dim \mathrm{GS}(f) \;=\; \dim X \;=\; \dim Y. \tag{12}$$

There is an induced map $F\colon \mathrm{GS}(f) \longrightarrow Y$, sending $(x_1, \dots, x_d)$ to $f(x_1)$, which is dominant of degree $d!$.

Because of Definition 2.1.24, in the following we will consider often morphisms between varieties satisfying the following condition:

$(*)$ the morphism is a finite separable dominant étale map of degree d between smooth absolutely irreducible varieties.

We have a natural action of the symmetric group S_d on $\mathrm{GS}(f)$ given by

$$\sigma \cdot (x_1, \dots, x_d) := \left(x_{\sigma(1)}, \dots, x_{\sigma(d)}\right) \quad \text{for evey } \sigma \in S_d.$$

Lemma 2.1.25. *Let $f\colon X \longrightarrow Y$ be a morphism satisfying $(*)$. Then, for any pair of irreducible components Z and Z' of $\mathrm{GS}(f)$ there exists an element $\tau \in S_d$ such that $\tau \cdot Z = Z'$. Namely, the action of S_d on $\mathrm{GS}(f)$ is transitive on irreducible components.*

Proof. Since fiber products of étale maps are étale (see [**Sta17**, Tag 03PA, Proposition 53.26.2]), the morphism F is étale. Moreover, by construction F is dominant, and it is finite, since the fiber product of finite morphisms is finite. Hence F is surjective. Since Y is irreducible and smooth and F is étale, then $\mathrm{GS}(f)$ is smooth (see [**Sta17**, Tag 03PA, Proposition 53.26.2]) and equidimensional (namely, all of its irreducible components have the same dimension, see [**Har77**, Corollary 9.6] and [**Har77**, Theorem 10.2] taking into account that an étale morphism is smooth of relative dimension 0). For any two irreducible components Z and Z', consider the restriction maps

$$F_{|_Z}\colon Z \longrightarrow Y \quad \text{and} \quad F_{|_{Z'}}\colon Z' \longrightarrow Y.$$

These maps are also étale, in fact open immersions are étale, and the composition of étale maps is étale. Moreover, both restrictions are dominant. In fact, since $\mathrm{GS}(f)$ is equidimensional, it follows $\dim Z = \dim \mathrm{GS}(f)$, and since F is finite, we get $\dim F(Z) = \dim(Z) = \dim(Y)$ because of Equation (12).

Since f is finite and étale, then for every $y \in Y$ the fiber $f^{-1}(y)$ is constituted of d distinct points (see [**GW10**, Equation 12.6.2] Hence, for all $y \in Y$ we have $|F^{-1}(y)| = d!$. Fix $y \in Y$ and write $f^{-1}(y) = \{x_1, \dots, x_d\}$. Therefore

$$F^{-1}(y) = \left\{(x_{\sigma(1)}, \dots, x_{\sigma(d)}) \,:\, \sigma \in S_d\right\},$$

where S_d is the symmetric group. Suppose that $F^{-1}(y)$ intersects nontrivially both Z and Z'. It follows that there exists $a \in Z$ and $a' \in Z'$ and an element $\tau \in S_d$ such that $\tau \cdot a = a'$. Since the action of S_d on $\mathrm{GS}(f)$ is algebraic, then the action of any element $\sigma \in S_d$ determines an automorphism of $\mathrm{GS}(f)$; in particular, such an action sends irreducible components to irreducible components. It follows that $\tau \cdot Z = Z'$. Hence, we are left to show that such an element $y \in Y$ exists. This is the case because of the following argument. Define

$$\tilde{Y}_Z = \left\{y \in Y \,:\, F^{-1}(y) \cap Z \neq \emptyset\right\} \quad \text{and} \quad \tilde{Y}_{Z'} = \left\{y \in Y \,:\, F^{-1}(y) \cap Z' \neq \emptyset\right\}.$$

These two sets are open, and since the restrictions $F_{|_Z}$ and $F_{|_{Z'}}$ are dominant, they are non-empty. Since Y is irreducible, then $\tilde{Y}_Z \cap \tilde{Y}_{Z'}$ is open and non-empty. Any point in $\tilde{Y}_Z \cap \tilde{Y}_{Z'}$ satisfies the desired requirement.

□

Lemma 2.1.25 shows that the action of the symmetric group S_d on the Galois scheme is transitive on irreducible components. Because of this, the stabilizers of these components are conjugate subgroups of S_d.

Definition 2.1.26 (geometry Galois group)**.** We define the *geometric Galois group* $\mathrm{Gal}_g(f)$ of a morphism $f\colon X \longrightarrow Y$ of degree d satisfying $(*)$ to be the stabilizer of any irreducible component of $\mathrm{GS}(f)$ with respect to the action of the symmetric group S_d. This definition is well-posed up to conjugacy in S_d.

Now suppose that the Galois scheme $\mathrm{GS}(f)$ has b distinct irreducible components say $X = \{Z_1, Z_2, \dots Z_b\}$ be the set of all irreducible components of $\mathrm{GS}(f)$, S_d acts on X and by a theorem in group action theory we have:

$$b = |X| = [S_d : \mathrm{Gal}_g(f)].$$

It follows that the number of irreducible components of the Galois scheme $\mathrm{GS}(f)$ coincides with the number of cosets of the geometric Galois group $\mathrm{Gal}_g(f)$ in S_d.

Definition 2.1.27. Let $f\colon X \longrightarrow Y$ be a morphism satisfying $(*)$. Since f is dominant, it determines a field extension $K(Y) \hookrightarrow K(X)$. We define the *algebraic Galois group* $\mathrm{Gal}_a(f)$ of f to be the Galois group of the extension $K(Y) \hookrightarrow E$, where E is a Galois closure (see [**Row06**, Remark 4.77]) of $K(Y) \hookrightarrow K(X)$.

Proposition 2.1.28. *For every morphism $f\colon X \longrightarrow Y$ of degree d satisfying $(*)$, the two groups $\mathrm{Gal}_g(f)$ and $\mathrm{Gal}_a(f)$ are isomorphic.*

Proof. Let Z be any component of $\mathrm{GS}(f)$ and realize $\mathrm{Gal}_g(f)$ as the stabilizer of Z. Since the restriction $F_{|_Z}\colon Z \longrightarrow Y$ is dominant (see Lemma 2.1.25) we have a field inclusion $K(Y) \hookrightarrow K(Z)$.

Claim. $\mathrm{Gal}_g(f) \cong \mathrm{Gal}\big(K(Z)/K(Y)\big)$.
Proof of the claim. Since $\mathrm{Gal}_g(f)$ is the stabilizer of Z, then for every $\sigma \in \mathrm{Gal}_g(f)$ we have an automorphism $\varphi_\sigma\colon Z \longrightarrow Z$, which induces an automorphism $\psi_\sigma\colon K(Z) \longrightarrow K(Z)$ fixing $K(Y)$. We define a group homomorphism

$$\begin{array}{rccc} \Psi\colon & \underset{\sigma}{\mathrm{Gal}_g(f)} & \longrightarrow & \underset{\psi_\sigma}{\mathrm{Gal}\big(K(Z)/K(Y)\big)} \\ & & \mapsto & \end{array} \tag{13}$$

Let b be the number of components of $\mathrm{GS}(f)$. Notice that the field extension $K(Y) \hookrightarrow K(Z)$ has degree $d!/b$, since $K(Y) \hookrightarrow K(\mathrm{GS}(f))$ has degree $d!$ and all components of $\mathrm{GS}(f)$ differ by the action of an element of S_d. In particular, $|\,\mathrm{Gal}\big(K(Z)/K(Y)\big)| \leq d!/b$. The group homomorphism Ψ is injective because any automorphism which is the identity on an open subset is the identity everywhere. Hence the set $\Psi\big(\mathrm{Gal}_g(f)\big)$ has cardinality $|\,\mathrm{Gal}_g(f)|$. By what we noticed before, the number $|\,\mathrm{Gal}_g(f)|$ equals $|S_d|/b = d!/b$ because the number of components of $\mathrm{GS}(f)$ equals the number of cosets of $\mathrm{Gal}_g(f)$. Hence, Ψ is an isomorphism and $K(Y) \hookrightarrow K(Z)$ is a Galois extension (see [**CL05**, Definition 3.2.5]).

Claim. $K(Z)$ is a Galois closure of $K(Y) \hookrightarrow K(X)$.

Proof of the claim. We know already that $K(Y) \hookrightarrow K(Z)$ is a Galois extension. Moreover, the latter factors via $K(Y) \hookrightarrow K(X)$ by considering the projection $Z \longrightarrow X$ on the first factor. The only thing left to prove is that $K(Y) \hookrightarrow K(Z)$ is minimal among Galois extensions of $K(Y) \hookrightarrow K(X)$. Namely, we have to show that if $E \subset K(Z)$ is a field such that the image of the inclusion $K(X) \hookrightarrow K(Z)$ is contained

in E, and $K(Y) \hookrightarrow E$ is Galois, then $E = K(Z)$. Define $G := \mathrm{Gal}\big(K(Z)/K(Y)\big)$. By the Galois correspondence, and recalling that the inclusion $K(X) \hookrightarrow K(Z)$ is given by the projection on the first factor, we have

$$\begin{array}{ccccc} G & \supset & \mathrm{Stab}_G(1) & \supset & \{\mathrm{id}\} \\ \updownarrow & & \updownarrow & & \updownarrow \\ K(Y) & \hookrightarrow & K(X) & \hookrightarrow & K(Z) \end{array} \tag{14}$$

where $\mathrm{Stab}_G(1) = \big\{\sigma \in G \,:\, \sigma(1) = 1\big\}$ is the stabilizer of 1 under the action of G on $\{1, \dots, d\}$. This action is given by the identification of G with $\mathrm{Gal}_g(f)$ provided by the map Ψ in Equation (13). Under this correspondence, the field E is associated to a subgroup $H \subset G$, which is normal since $K(Y) \hookrightarrow E$ is Galois, and which is contained in $\mathrm{Stab}_G(1)$. To conclude, we prove that $H = \{\mathrm{id}\}$, which implies $E = K(Z)$. We start by showing that G acts transitively on $\{1, \dots, d\}$. If we denote by $G \cdot 1$ the orbit of 1 under G, then by standard results in Galois theory and taking into account Equation (14), we have

$$|G \cdot 1| = [G : \mathrm{Stab}_G(1)] = [K(X) : K(Y)] = d.$$

This implies that $G \cdot 1 = \{1, \dots, d\}$, showing that the action is transitive. By normality, $H \subset \sigma\, \mathrm{Stab}_G(1)\, \sigma^{-1}$ for any $\sigma \in G$. Since G is transitive on $\{1, \dots, d\}$, it follows

$$H \;\subset\; \mathrm{Stab}_G(1) \cap \mathrm{Stab}_G(2) \cap \cdots \cap \mathrm{Stab}_G(d). \tag{15}$$

The right hand side of Equation (15) equals $\{\mathrm{id}\}$, so the claim is proved.

Summing up, the first claim says that $\mathrm{Gal}_g(f) \cong \mathrm{Gal}\big(K(Z)/K(Y)\big)$, and the second claim implies that the latter group is isomorphic to $\mathrm{Gal}_a(f)$. This concludes the proof of the proposition. □

Now we cast the notions defined so far into the framework of Galois schemes of morphisms (Corollary 2.1.32). After that, we recall the notion of simple tangency for a curve and highlight its consequences on Galois groups.

Definition 2.1.29. For an absolutely irreducible curve $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ of degree d, define $\mathcal{V}_C$ to be the set of points in $X_0(\overline{\mathbb{F}}_q) = \check{\mathbb{P}}^2\big(\overline{\mathbb{F}}_q\big)$ such that the restriction of the map $\pi\colon X_1(\overline{\mathbb{F}}_q) \longrightarrow X_0(\overline{\mathbb{F}}_q)$ from Definition 2.1.16 to $\mathcal{U}_C := \pi^{-1}\big(\mathcal{V}_C\big)$ is étale.

Remark 2.1.30. Notice that the set $\mathcal{V}_C$ is open and non-empty. In fact, since the map $\pi\colon X_1(\overline{\mathbb{F}}_q) \longrightarrow X_0(\overline{\mathbb{F}}_q)$ is separable, it is enough to ensure that $\pi\colon \mathcal{U}_C \longrightarrow \mathcal{V}_C$ is flat. Now, the locus in the domain where a map is flat is open (see [**Sta17**, Tag 0398, Theorem 36.15.1,]), and flat maps are open morphisms (see [**Sta17**, Tag 01U2, Lemma 28.24.9]), so this shows that $\mathcal{V}_C$ is open. The fact that $\mathcal{V}_C$ is non-empty is ensured by the generic flatness result (see [**Sta17**, Tag 0529, Proposition 28.26.1]).

Lemma 2.1.31. *Let C be an absolutely irreducible curve of degree d defined over $\mathbb{F}_q$. Then the restriction to $\mathcal{U}_C := \pi^{-1}\big(\mathcal{V}_C\big)$ of the map $\pi\colon X_1\big(\overline{\mathbb{F}}_q\big) \longrightarrow X_0\big(\overline{\mathbb{F}}_q\big)$ from Definition 2.1.16 is a finite separable dominant étale morphism between smooth absolutely irreducible varieties, namely it satisfies condition $(*)$.*

Proof. From the explanation after Definition 2 we know that both X_0 and X_1 are smooth and absolutely irreducible. Since $\mathcal{V}_C$ and $\mathcal{U}_C$ are open and non-empty, the same is true for them. Moreover, π is a quasi-finite separable dominant morphism between projective varieties (Lemma 2.1.17) and so it is finite. Hence,

the same holds for its restriction $\pi_{|\mathcal{U}_C}$. By Remark 2.1.30, the map is étale, and this concludes the proof. □

By unravelling the definition, in the light of Lemma 2.1.31 we obtain:

Corollary 2.1.32. *For an absolutely irreducible curve C defined over $\mathbb{F}_q$, we have* $\mathrm{Gal}(C) \cong \mathrm{Gal}_a\big(\pi_{|\mathcal{U}_C}\big)$.

The interpretation of the Galois group of a curve provided by Corollary 2.1.32 allows to use Proposition 2.1.28 and hence to deduce the irreducibility of the Galois scheme when the Galois group is the full symmetric group.

2.1.3. Lang-Weil Theorem. One of the main tools we will use in Chapter 4 is the so-called *Lang-Weil bound* for the number of points of a variety over a finite field (see [**LW54**, Theorem 1]). For a nice exposition of this result, see Terence Tao's blog[1]. Let $\mathbb{F}$ be a field and consider an affine algebraic variety V defined over $\mathbb{F}$. This means that V is the set of common zeros in $\mathbb{F}^n$ of finitely many polynomials $P_1, \dots, P_r \in \mathbb{F}[x_1, \dots, x_n]$. To a variety V defined over $\mathbb{F}$ we can then associate the ideal $I(V)$ of all polynomials $P \in \mathbb{F}[x_1, \dots, x_n]$ that vanish at all points of V. For any extension of fields $\mathbb{F} \subseteq \mathbb{K}$, we denote by $V(\mathbb{K})$ the set of common zeros in $\mathbb{K}^n$ of the polynomials in the ideal $I(V)$, considered now as an ideal in $\mathbb{K}[x_1, \dots, x_n]$. One says that a variety $V \subseteq \mathbb{F}^n$ is *irreducible* if $I(V)$ is prime in $\mathbb{F}[x_1, \dots, x_n]$. For our considerations we will need a stronger notion of irreducibility, which we introduce in the following definition.

Definition 2.1.33. We say that an affine variety V over a field $\mathbb{F}$ is *absolutely irreducible* if the ideal $I(V)$ is prime in $\overline{\mathbb{F}}[x_1, \dots, x_n]$, where $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$. This is equivalent to the fact that $V(\overline{\mathbb{F}})$ is irreducible.

Definition 2.1.34. We say that an affine variety $V \subseteq \mathbb{F}^n$ defined by polynomials $P_1, \dots, P_r$ has *complexity* M if $n, r \leq M$ and $\deg(P_i) \leq M$ for all $i \in \{1, \dots r\}$.

Theorem 2.1.35 (Lang-Weil bound)**.** *Let V be an absolutely irreducible variety over a finite field $\mathbb{F}$ of complexity at most M. Then*

$$|V(\mathbb{F})| = \big(1 + O_M(|\mathbb{F}|^{-\frac{1}{2}})\big)\, |\mathbb{F}|^{\dim(V)}\,.$$

By writing $O_M(|\mathbb{F}|^{-\frac{1}{2}})$ we mean that there exists a nonnegative constant δ_M depending on M, but not on V, such that

$$\big(1 - \delta_M|\mathbb{F}|^{-\frac{1}{2}})\big)\, |\mathbb{F}|^{\dim(V)} \leq |V(\mathbb{F})| \leq \big(1 + \delta_M|\mathbb{F}|^{-\frac{1}{2}})\big)\, |\mathbb{F}|^{\dim(V)}\,.$$

Using an inclusion-exclusion argument, one obtains by induction on the dimension:

Corollary 2.1.36. *Let V be a variety over a finite field $\mathbb{F}$ of complexity at most M. Then*

$$|V(\mathbb{F})| = \big(c + O_M(|\mathbb{F}|^{-\frac{1}{2}})\big)\, |\mathbb{F}|^{\dim(V)}\,,$$

where c is the number of irreducible components of $V(\overline{\mathbb{F}})$.

All the considerations and results we stated so far hold also for projective varieties defined over finite fields. By a *projective variety* defined over a field $\mathbb{F}$ we mean the set of common zeros in the projective space $\mathbb{P}^n(\mathbb{F})$ of finitely many *homogeneous* polynomials $P_1, \dots, P_r \in \mathbb{F}[x_0, \dots, x_n]$. From now on, all the varieties we consider are projective, or are open subsets of projective varieties.

[1] https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/

2.2. Circular Curves

This chapter is devoted to *circular curves* and projective geometry, they play a crucial roll to find a structure theorem for a set with few ordinary circles i.e a circle through exactly three points of a given finite set and we will use this in the forthcoming thesis. For an appropriate introduction to projective geometry see [[**ST92**], App. A]. We use the homogeneous coordinates $[x : y : z]$ for points in $\mathbb{P}^2(\mathbb{R})$ or $\mathbb{P}^2(\mathbb{C})$, and we think of the line with equation $z = 0$ as the line at infinity. An affine algebraic curve in $\mathbb{R}^2$, defined by a polynomial $f \in \mathbb{R}[x, y]$, can be naturally extended to a projective algebraic curve, by taking the zero set of the homogenisation of f. This curve in $\mathbb{P}^2(\mathbb{R})$ then extends to $\mathbb{P}^2(\mathbb{C})$, by taking the complex zero set of the homogenised polynomial. A reference for this section please see [**LMM+18**].

Definition 2.2.1. We define the *circular points* to be the points

$$\alpha = [i : 1 : 0], \beta = [-i : 1 : 0]$$

on the line at infinity in $\mathbb{P}^2(\mathbb{C})$.

We notice that every circle contains both circular points. Moreover, any real conic containing α and β is either a circle, or a union of a line with the line at infinity. We could thus consider a *generalised circle* to be a conic that contains both circular points.

A more general definition of circularity is following. Suppose that $\mathbb{P}^n(\mathbb{R})$ is the projective space over the real numbers and $x_0, \dots x_n$ are the coordinates. The absolute quadratic hyper-surface is corresponding to the solutions of

$$x_0 = 0,\ x_1^2 + \dots x_n^2 = 0. \tag{16}$$

Obviously when $n = 2$ these equations give the cyclic points in the Definition 2.2.1

Definition 2.2.2. An algebraic curve in $\mathbb{P}^2(\mathbb{R})$ is *circular* if it contains α and β. For $k \geq 2$, an algebraic curve in $\mathbb{P}^2(\mathbb{R})$ is *k-circular* if it has singularity of multiplicity at least k at both α and β.

Definition 2.2.3. A *generalised circle* is an algebraic curve of degree two that contains α and β.

Equivalently, A *generalized circle* is an algebraic curves of degree two that contains α and β; in fact suppose that

$$ax^2 + by^2 + cxy + dxz + eyz + fz^2$$

is a quadric curve containing α and β, by replacing cyclic points we obtain $a = b$ and $c = 0$, so

$$t(x^2 + y^2) + l(x, y, z)z,$$

where $t \in \mathbb{R}$ and $l \in \mathbb{R}[x, y, z]$ is a non-trivial linear form. If $t \neq 0$, then the curve is a circle, while if $t = 0$, the curve is the union of a line with the line at infinity.

Example 2.2.4. *A* circular cubic *is an algebraic curve of degree three that contains α and β; equivalently let*

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2z + fxz^2 + gy^2z + hyz^2 + kz^3$$

by replacing α and β we obtain $a = d$ and $b = c$. This implies any circular cubic curve in $\mathbb{P}^2(\mathbb{R})$ defined by a homogeneous polynomials of the form

$$(ax + by)(x^2 + y^2) + q(x, y, z)z, \tag{17}$$

where $a, b \in \mathbb{R}$ and $q \in \mathbb{R}[x, y, z]$ is a non-zero quadratic homogeneous polynomial.

Note that this is not necessary that a circular cubic to be irreducible or smooth. For instance, the union of a circle and a line is a circular cubic, and so is the union of any conic with the line at infinity (take $a = b = 0$) in 17.

Example 2.2.5. *A* bicircular quartic *is an algebraic curve of degree four that is* 2*-circular, equivalently, it is any curve in* $\mathbb{P}^2(\mathbb{R})$ *defined by a homogeneous polynomial of the form*

$$t(x^2 + y^2)^2 + (ux + vy)(x^2 + y^2)z + q(x, y, z)z^2, \tag{18}$$

where $t, u, v \in \mathbb{R}$ *and* $q \in \mathbb{R}[x, y, z]$ *is a non-trivial homogeneous quadratic polynomial (see* [**Wer12**, 24, Sect 8.2] *for a proof that a quartic is* 2*-circular if and only if its equation has the form (18)). A reducible bicircular quartic curve is the union of two circles, for which it is easy to see that the curve has double points at* α *and* β*, since both circle contain those points.*

Every circular cubic is contained in a bicircular quartic, since for $t = 0$ in 18 we get a union of a circular cubic and the line at infinity. A non-circular conic is also contained in a bicircular quartic, since for $t = u = v = 0$ in 18 we get a union of a conic and $z^2 = 0$, which is a double line at infinity.

Definition 2.2.6. The *circular degree* of an algebraic curve γ in $\mathbb{P}^2(\mathbb{R})$ is the smallest k such that γ is contained in a k-circular curve of degree $2k$.

The circular degree is well-defined, since given any curve γ of degree k, we can add k copies of the line at infinity, to get a k-circular curve of degree $2k$.

For example, a line has circular degree one, since its union with the line at infinity is a 1-circular curve of degree two. A conic that is not a circle has circular degree two, since its union with two copies of the line at infinity is a 2-circular curve of degree four. Similarly, a circular cubic has circular degree two, since its union with the line at infinity is a 2-circular curve of degree four. We can thus classify curves of low circular degree as follows:

- Circular degree one : lines and circles (that is, generalised circles).
- Circular degree two : non-circular conics, circular cubics, and bicircular quartics.
- Circular degree three : non-circular cubics, circular quartics, 2-circular quintics, and 3-circular sextics.

This classification is important to us, because we will see that circular degree is invariant under inversion.

We have defined circular curves and circular degrees in the projective plane, because that is their most natural setting. In the rest of the paper, to avoid confusion between the projective and inversive planes, we will use these notions for curves in $|R^2$, with the understanding that to inspect the definitions we should consider $\mathbb{P}^2(\mathbb{R})$ and $\mathbb{P}^2(\mathbb{C})$

2.2.1. Inversion. Circular curves are intimately related to circle inversion, which we now introduce. A general reference is [**Bla00**]

Definition 2.2.7. Let $C(p, r)$ be the circle with centre $p = (x_p, y_p) \in \mathbb{R}^2$ and radius $r > 0$. The *circle inversion* with respect to $C(p, r)$ is the mapping $I_{p,r} \colon \mathbb{R}^2 \setminus \{p\} \longrightarrow \mathbb{R}^2 \setminus \{p\}$ defined by

$$I_{p,r}(x, y) = \Big(\frac{r^2(x - x_p)}{(x - x_p)^2 + (y - y_p)^2} + x_p, \frac{r^2(y - y_p)}{(x - x_p)^2 + (y - y_p)^2} + y_p \Big)$$

for $(x, y) \neq p$. We write I_p for $I_{p,1}$. We call p the *center* of the inversion $I_{p,r}$.

In the inversion plane $\mathbb{R}^2 \cup \{\infty\}$, the inversion map can be completed by setting $I_{p,r}(p) = \infty$ and $I_{p,r}(\infty) = p$, so that inversions take generalised circles to generalised circles. The group of transformations of the inversive plane generated by the inversions and the similarities is called the inversive group. It is known that a bijection of the inversive plane that takes generalised circles to generalised circles has to be an element of this group, and that any element of this group is either a similarity or an inversion followed by an isometry [[**Cox69**], Thm. 6.71].

The image of an algebraic curve in $\mathbb{R}^2$ under an inversion is also an algebraic curve, in the following sense.

Definition 2.2.8. For any algebraic curve γ there is an algebraic curve γ' such that

$$I_{p,r}(\gamma \setminus \{p\}) = \gamma' \setminus \{p\}.$$

We refer to γ' as the *inverse* of γ with respect to the circle $C(p, r)$, and abuse notation slightly by writing $\gamma' = I_{p,r}(\gamma)$. Also, since for different choices of radius $r, I_{p,r}(\gamma)$ differs only by a dilatation in p, we will often only consider the inverse $I_p(\gamma) = I_{p,1}(\gamma)$ and refer to it as the inverse of γ in the point p.

If a curve has degree d, then its inverse has degree at most $2d$ [**Wer12**, Thm 24, Sect 8.2] If γ is irreducible, then its inverse is also irreducible. Note that inverses of algebraic curves can behave somewhat unintuitively; for instance, Proposition 2.2.11 states that the inverse of an ellipse has an isolated point, which is surprising if one thinks of an ellipse as just a closed continuous curve.

It is well known that the inverses of generalised circles are again generalised circles. It turns out that, more generally, circular degree is preserved under inversion. We now make precise what this means for curves of low circular degree. A proof can be found in the classical paper [**Joh77**], for a more modern reference, see [**Wer12**].

Lemma 2.2.9 (Inversion and circular degree)**.** *Let C_k be a curve of circular degree k. Then:*

(1) *The inverse of C_1 in a point on C_1 is a line; the inverse of C_1 in a point not on $C_1$is a circle.*
(2) *The inverse of C_2 in a singular point on C_2 is a non-circular conic; the inverse of C_2 in a regular point on C_2 is a circular cubic; the inverse of C_2 in a point not on C_2 is a bicircular quartic.*
(3) *The inverse of C_3 in a singularity of multiplicity three is a non-circular cubic; the inverse of C_3 in a singularity of multiplicity two is a circular quartic; the inverse of C_3 in a regular point on C_3 is a 2-circular quintic; the inverse of C_3 in a point not on C_3 is a 3-circular sextic.*

One particular subcase of Case (ii) will play an important role in our result in the Section 3.3, and we state it separately in Proposition 2.2.11 A proof can be found in [**Hil20**, p,202].

Definition 2.2.10. (acnodal cubic) Let C be a cubic curve, we say that C is an acnodal cubic curve if it is a singular cubic curve with a singularity that is an isolated point.

For example,$(2x-1)(x^2+y^2)-y^2 = 0$ is an acnodal circular cubic with a singularity at the origin.

Proposition 2.2.11. *The inverse of an ellipse in a point on the ellipse is an acnodal circular cubic with the centre of inversion as its singularity ;the inverse of an acnodal circular cubic in its singularity is an ellipse through the singularity.*

Example 2.2.12. *Compute the inverse of* $(2x-1)(x^2+y^2)-y^2=0$ *at its singularity at the origin. The inverse of a curve* $f(X,Y)=0$ *under an inversion with centre at the origin and radius one is given by*

$$(x^2+y^2)^k f\big(\frac{x}{x^2+y^2},\frac{y}{x^2+y^2}\big)=0,$$

where k *is the smallest integer such that it became a polynomial. In our situation we know that its circular degree is one and so* $k=2$*. By replacing we have*

$$(x^2+y^2)^2\Big[\big(\frac{2x}{x^2+y^2}-1\big)\big(\frac{x^2}{(X^2+y^2)^2}+\frac{y^2}{(x^2+y^2)^2}\big)-\frac{y^2}{(x^2+y^2)^2}\big)\Big]=0.$$

After a simplification we obtain $(x-1)^2+2y^2=1$*, and this is an ellipse.*

CHAPTER 3

On sets defining few ordinary circles

The results of this Chapter is based on a collaboration with Aaron Lin, Hossein Nassajian Mojarrad, Josef Schicho, Konrad Swanepoel and Frank De Zeeuw [**LMM+18**].

3.1. Groups on circular curves

3.1.1. Groups on irreducible circular cubics. The extremal configurations in our main theorems are all based on group laws on certain circular curves. It is well-known that irreducible smooth cubics (elliptic curves) have a group law (see for instance [**ST92**]). These groups play a crucial role in the work of Green and Tao [**GT13**]. The reason that these groups are relevant to ordinary lines is the following collinearity property of this group (when defined in the standard way). Three points on the curve are collinear if and only if in the group they sum to the identity element. For this property to hold, the identity element must be an inflection point. It is known that every smooth irreducible cubic curve over complex numbers has 9 inflection points, while either 1 or 3 of them have real coordinates.

Here we will define a group in a slightly different way (described for instance in [**ST92**]*Section 1.2), in which the identity element is not necessarily an inflection point, and the same collinearity property does not hold. However, for circular cubics, we show that we can choose the identity element so that we get a similar property for concyclicity.

First let γ be any irreducible cubic, write γ^* for its set of regular points, and pick an arbitrary point $o \in \gamma^*$. We describe an additive group operation $\oplus$ on the set γ^* for which o is the identity element. The construction is depicted in Figure 1.

Given $a, b \in \gamma^*$, let $a * b$ be the third intersection point of γ and the line ab, and define $a \oplus b$ to be $(a * b) * o$, the third intersection point of γ and the line through $a * b$ and o. When $a = b$, the line ab should be interpreted as the tangent line at a; when $a * b = o$, the line through $a * b$ and o should be interpreted as the tangent line to γ at o. We refer to [**ST92**] for a more careful definition and a proof that this operation really does give a group.

Now consider a circular cubic γ. Since the circular points α and β lying on it are conjugate, γ has a unique real point on the line at infinity, which we choose as our identity element o. We define the point ω to be the third intersection point of the tangent line to γ at o (if there is no third intersection point, then o is an inflection point, and we consider o itself to be the third point). Throughout this paper we will use ω to denote this special point on a circular cubic; note that ω is not fixed like α and β, but depends on γ. Also note that ω is real, since it corresponds to the third root of a real cubic polynomial whose other two roots correspond to the real point o. Observe that

$$\omega = \alpha \oplus \beta,$$

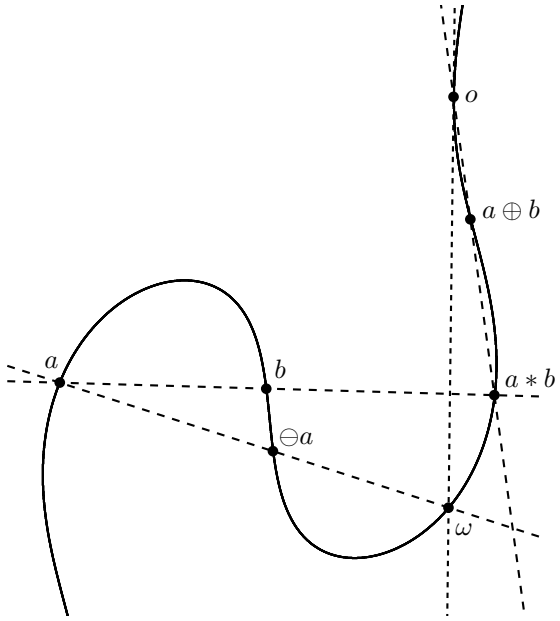


FIGURE 1. Group law on a smooth circular cubic curve

since $\alpha * \beta = o$, and by definition $o * o = \omega$.

With this group law, we no longer have the property that three points are collinear if and only if they sum to o (unless o happens to be an inflection point). Nevertheless, one can check that three points $a, b, c \in \gamma^*$ are collinear if and only if $a \oplus b \oplus c = \omega$. More important for us, four points of γ^* lie on a generalised circle if and only if they sum to ω.

This amounts to a classical fact (see [**Bas01**]Article 225 for an equivalent statement), but we include a proof for completeness. We use the following version of the Cayley-Bacharach Theorem, due to Chasles (see [**EGH96**]).

Theorem 3.1.1 (Chasles)**.** *Suppose two cubic curves in $\mathbb{P}^2(\mathbb{C})$ with no common component intersect in nine points, counting multiplicities. If γ is another cubic curve containing eight of these intersection points, counting multiplicities, then γ also contains the ninth.*

Recall from Section 2.2 that a generalised circle, viewed projectively, is either a circle, or the union a line with the line at infinity.

Proposition 3.1.2. *Let γ be an irreducible circular cubic in $\mathbb{P}^2(\mathbb{R})$, and let $a, b, c, d \in \gamma^*$ be points that are not necessarily distinct. A generalised circle intersects γ in the points a, b, c, d (taking into account multiplicity) if and only if $a \oplus b \oplus c \oplus d = \omega$.*

PROOF. We consider the cubic γ extended to $\mathbb{P}^2(\mathbb{C})$. We first show the forward direction. All statements in the proof should be considered with multiplicity.

If the generalised circle is the union of a line ℓ and the line at infinity ℓ_∞, then $\ell \cup \ell_\infty$ intersects γ in $a, b, c, d, \alpha, \beta$. Since ℓ intersects γ in at most three points, one of the points a, b, c, d must equal o, say $d = o$. Since ℓ_∞ also intersects γ in at most three points, we must have $a, b, c \in \ell$. Thus a, b, c are collinear, and we have $a \oplus b \oplus c = \omega$, by the definition of the group law. It then follows from $d = o$ that $a \oplus b \oplus c \oplus d = \omega$.

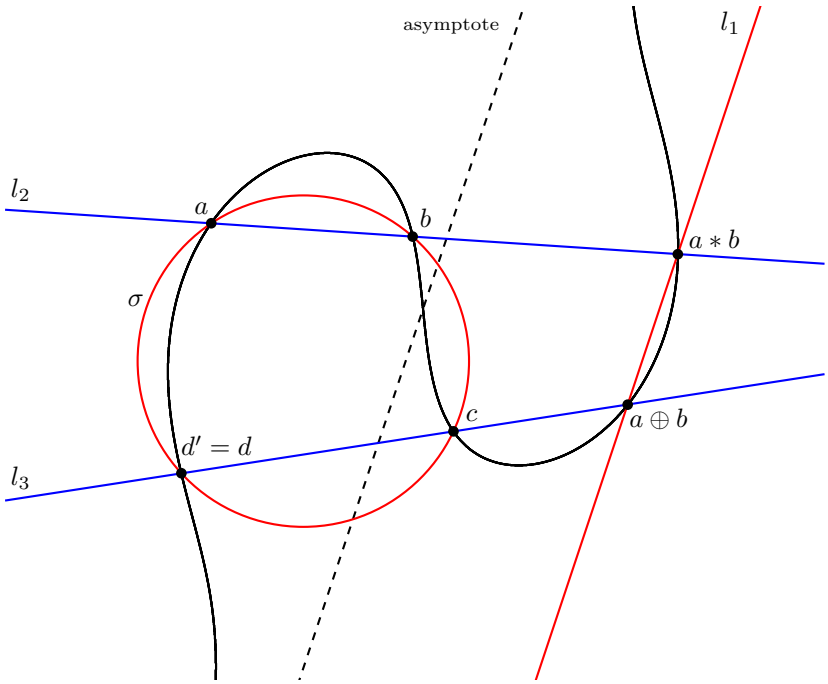


FIGURE 2. Concyclicity of four regular points on a circular cubic

Suppose next that the generalised circle is a circle σ, and intersects γ in $a, b, c, d, \alpha, \beta$. The construction that follows is depicted in Figure 2 Let l_1 be the line through o and $a * b$ (and thus through $a \oplus b$), l_2 the line through a and b (and thus through $a * b$), and l_3 the line through c and $a \oplus b$. Note that σ and l_∞ intersect in α and β. Then $\gamma_1 = \sigma \cup l_1$ and $\gamma_2 = l_2 \cup l_3 \cup l_\infty$ are two cubic curves that intersect in nine points, of which the eight points a, b, c, $a * b$, $a \oplus b$, o, α, and β certainly lie on γ; the remaining point is the third intersection point of γ_1 and ℓ_3 beside c and $a \oplus b$, which we denote by d'. By Theorem 3.1.1, γ contains d'. By the group law on γ, we have $d' = (a \oplus b) * c$. Moreover, d' must be the sixth intersection point of γ and σ beside a, b, c, α, β, which is d, so $d = d' = (a \oplus b) * c$. By the definition of the group law, this implies $a \oplus b \oplus c = o * d$, so $(a \oplus b \oplus c) * d = (o * d) * d = o$, and finally $a \oplus b \oplus c \oplus d = o * o = \omega$.

For the converse, suppose that $a \oplus b \oplus c \oplus d = \omega$, and let d' be the fourth point where the generalised circle σ through a, b, c intersects γ. Then, by what we have just shown, $a \oplus b \oplus c \oplus d' = \omega$, and it follows that $d = d'$, and a, b, c, d lie on σ. □

We also are able to define a group structure on a circular cubic C in another way such that four points $p, q, r, s \in C$ are cocircular if and only if $p+q+r+s = 0$, where 0 is the identity element of the group structure. The proof proceeds as follows:

Lemma 3.1.3. *Suppose that C is a cubic curve and $+$ is a group operation on C. Then $p + q + r + s + t + u = 0$ if and only if p, q, r, s, t, u are* coconicular*, for all p, q, r, s, t, u in C. Here coconicular means are on a common conic*

PROOF. for both directions, we observe that the linear system of cubics passing through the nine points $p, q, r, s, t, u, (-p - q), (-r - s), (-t - u)$ contains at least two cubics, namely C and the union of the three lines $(pq), (rs), (tu)$. By linear combination of the two equations, we may find a cubic passing through the nine

points and any pre-assigned point in the plane. The proof proceeds by finding reducible curves in the linear system.

If $p+q+r+s+t+u=0$, then $(-p-q),(-r-s),(-t-u)$ are collinear, say on a line L. Then there is a cubic passing through the nine pints and a fourth point of L. Then L must be a component, and the remaining 6 points are coconicular.

If $p,q,r,s,t,u \in C$ are coconicular, say on a conic Q, then there is a cubic through the nine points and a seventh point of Q. Then Q must be a component, and $(-p-q),(-r-s),(-t-u)$ are collinear, hence $p+q+r+s+t+u=0$.

□

Now suppose that C is a cubic curve passing through the two cyclic points α and β. We define the group law $\oplus : C^2 \longrightarrow C$ by

$$p \oplus q := p+q+x,$$

where x in C has to fulfil the condition $3x = \alpha+\beta$. Such points always exist (one can show that there are 1 or 3 solutions for x).

Theorem 3.1.4. *$p \oplus q \oplus r \oplus s = 0$ if and only if p,q,r,s are cocircular, for all p,q,r,s in C.*

Proof. $p \oplus q \oplus r \oplus s = 0$ if and only if $p+q+r+s+3x=0$ if and only if $p+q+r+s+\alpha+\beta=0$ if and only if p,q,r,s are cocircular. □

This proposition is a consequence of the more general fact that six points on a circular cubic lie on a conic if and only if they sum to 2ω. (In the standard group structure on a cubic, where the identity o is chosen as an inflection point, they would sum to o; see [**Wal78**]*Theorem 9.2.) Since a generalised circle in $\mathbb{P}^2(\mathbb{R})$ is a conic containing α and β, and $\alpha \oplus \beta = \omega$, it follows that four points a,b,c,d (possibly including o) lie on a generalised circle if and only if they sum to ω.

Theorem 3.1.5. *Let γ be an irreducible circular cubic, and let $\oplus$ be the group operation defined in Section 3.1.1. Then the group $(\gamma^*,\oplus)$ is isomorphic to the circle $\mathbb{R}/\mathbb{Z}$ if γ is acnodal or if γ is smooth and has one connected component, and is isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$ if γ is smooth and has two connected components.*

Proof. It is well known (see for instance [**GT13**]). □

3.1.2. Group structure on ellipse and two cocenter circles. We now define group laws on two other types of curves of circular degree two, and observe that they satisfy similar concyclicity properties. Let us note at this point that most bicircular quartics can also be given a group structure (if an irreducible bicircular quartic has no singularities besides α and β, then it is a curve of genus one, and thus has a group law by [**Sil09**, Section III.3]). However, in our proofs we will handle bicircular quartics by inverting in a point on the curve, which by Lemma 2.2.9 transforms a bicircular quartic into a circular cubic. For that reason, we do not need to study the group law on bicircular quartics separately.

Ellipses

We discuss a group law on ellipses, although we do not actually need it, because for proving our result for the sets with few ordinary circles in the Section 3.3.3 inversion lets us transform an ellipse into an acnodal cubic (Proposition 2.2.11), which we have already given a group structure in the previous section. Nevertheless, we treat

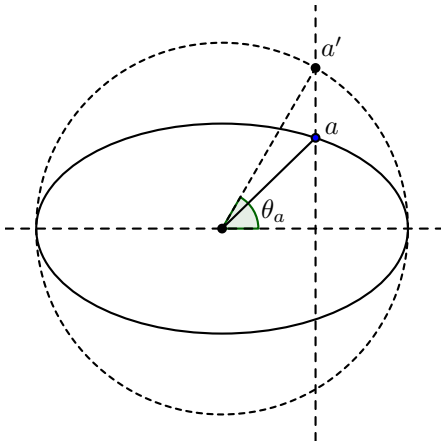


FIGURE 3. Eccentric angle of a point on an ellipse

the group law on ellipses here because it is especially elementary, and it would be strange not to mention it.

Consider the ellipse σ given by the equation $x^2 + (y/s)^2 = 1$, with $s \neq 0, 1$. For any point $a \in \sigma$, we project a vertically to the point a' on the unit circle around the origin, as in Figure 3, and call the angle θ_a the *eccentric angle* of a. We define the sum of two points $a, b \in \sigma$ to be the point $c = a \oplus b$ whose eccentric angle is $\theta_c = \theta_a + \theta_b$. This gives σ a group structure isomorphic to $\mathbb{R}/\mathbb{Z}$. The identity element is $o = (1, 0)$, and the inverse of a point is its reflection in the x-axis. We have the following classical fact that describes when four points on an ellipse are concyclic (see [**Joa48**] for the oldest reference we could find, and [**BPBSR84**, Problem 17.2] for two detailed proofs).

Proposition 3.1.6. *Four points $a, b, c, d \in \sigma$ are concyclic if and only if $a \oplus b \oplus c \oplus d = o$. We may allow two of the points to be equal, in which case the circle through the three distinct points is tangent to the ellipse at the repeated point.*

Another way to look at this group law is that we are parametrising the ellipse using lines through $o = (1, 0)$ (see for instance [**ST92**, Section 1.1]. More precisely, each point $a \in \sigma$ corresponds to the line oa; oa makes an angle $\pi - \theta_a/2$ with the x-axis, and the set of lines through o thus has a group structure equivalent to the one above. This view lets us relate the group on the ellipse to the group on the acnodal cubic. By Proposition 2.2.11, inverting in o maps the ellipse to an acnodal circular cubic γ, with o becoming the isolated point of the cubic. The lines through o now parametrise the cubic, and this parametrisation gives the same group on γ as the line construction that we gave in Section 3.1.1 (see [**ST92**, Section 3.7].

Concentric circles.

We now define a group on the union of two disjoint circles. For notational convenience, we identify $\mathbb{R}^2$ with $\mathbb{C}$. After an appropriate inversion, we can assume the circles to be

$$\sigma_1 = \{e^{2\pi i t} : t \in [0, 1)\}, \quad \sigma_2 = \{re^{-2\pi i t} : t \in [0, 1)\},$$

with $r > 1$, and we represent each element of $\sigma_1 \cup \sigma_2$ as $r^\epsilon e^{2\pi i t}$ with $\epsilon \in \mathbb{Z}_2$ (with the obvious convention $r^0 = 1$ and $r^1 = r$). We define a group operation on $\sigma_1 \cup \sigma_2$ by

$$r^{\epsilon_1} e^{2\pi i t_1} \oplus r^{\epsilon_2} e^{2\pi i t_2} = r^{(\epsilon_1 + \epsilon_2) \bmod 2} e^{2\pi i (t_1 + t_2)},$$

which turns $\sigma_1 \cup \sigma_2$ into a group isomorphic to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}_2$, with identity element $o = 1 = r^0 e^{2\pi i \cdot 0}$. We again have the following concyclicity property, which is easily seen using symmetry.

Proposition 3.1.7. *Points $a, b \in \sigma_1$ and $c, d \in \sigma_2$ lie on a generalised circle if and only if $a \oplus b \oplus c \oplus d = o$. If $a = b$ or $c = d$, then the generalised circle is tangent at that point.*

3.2. Constructions of Sets with few Ordinary Circles

As we mentioned in Section 2.2 an *ordinary circle* is a circle contains exactly three points from a given set. Since each circle is determined by 3 points, so we expect for a random set of n points we get $\Omega(n^3)$ ordinary circles. In this subsection, we have a plan to give several examples with at most $O(n^2)$ ordinary circles and $\Omega(n^3)$ 4-*rich circles* . More less our constructions are coming from a group structure on some algebraic curves.

Proposition 3.2.1. *Let σ be an ellipse, with the group structure introduced in Section 3.1.2. Then for every positive integer n there exists a subgroup say H_n of σ of order n such that*

- *H_n spans $\frac{n^2}{2} - O(n)$ ordinary circles.*
- *The number of 4-rich circles of H_n is given by:*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - 1 & \text{if } n \equiv 0 \pmod 4, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3 \pmod 4, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. Let σ be the ellipse defined by $x^2 + (y/s)^2 = 1$. Let $n \geq 5$. We have a finite subgroup of size n given by

$$S = \left\{ \left(\cos\left(\frac{2\pi k}{n}\right), s \sin\left(\frac{2\pi k}{n}\right) \right) : k = 0, \ldots, n-1 \right\} \subset \sigma.$$

By Proposition 3.1.6, the circle through any three points $a, b, c \in S$ passes through the point $d = \ominus a \ominus b \ominus c \in S$. Therefore, the only way S spans an ordinary circle is when d coincides with one of the points a, b, c (which occurs if the circle is tangent to σ at that point). It follows that the number of ordinary circles is equal to

$$\frac{1}{2} \left| \left\{ (k_1, k_2, k_3) \in \mathbb{Z}_{n^3} : 2k_1 + k_2 + k_3 \equiv 0 \pmod n, \quad k_1, k_2, k_3 \text{ distinct} \right\} \right|,$$

which is $\frac{1}{2}n^2 - O(n)$.

Similarly, the number of 4-point circles is equal to

$$\frac{1}{4!} \left| \left\{ (k_1, k_2, k_3, k_4) \in \mathbb{Z}_{n^4} : k_1 + k_2 + k_3 + k_4 \equiv 0 \pmod n, \quad k_1, k_2, k_3, k_4 \text{ distinct} \right\} \right|,$$

which is, by inclusion-exclusion, equal to $\frac{1}{24}(n^3 - 6n^2 + (8 + 3\delta_n)n - 6\epsilon_n)$, where δ_n is the number of solutions in $\mathbb{Z}_n$ to the equation $2k = 0$ and ϵ_n is the number of solutions in $\mathbb{Z}_n$ to the equation $4k = 0$. This works out to

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - 1 & \text{if } n \equiv 0 \pmod 4, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1, 3 \pmod 4, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

□

Notice that if γ^* is the set of smooth points of γ, then by Theorem 3.1.5 we know that for each $n \in \mathbb{N}$ there exists a subgroup of order n in γ^*.

Proposition 3.2.2. *Let γ be an irreducible circular cubic, and let $\oplus$ be the group operation defined in Section 3.1.1. Let H_n be a subgroup of order n of γ^*, and let $x \in \gamma^*$ be such that $4x = \omega \ominus h$ for some $h \in H_n$. Then:*

- *The number of ordinary generalised circles in the coset $S = H_n \oplus x$ equals $\frac{n^2}{2} - O(n)$*
- *The number of ordinary circles in the coset $S = H_n \oplus x$ equals $\frac{n^2}{2} - O(n)$*
- *If $o \notin S$ (equivalently, $x \notin H_n$) then the number of 4-point circles is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 2 & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8, \end{cases}$$

Proof. Let H_n be a subgroup of order n of γ^*, and let $x \in \gamma^*$ be such that $4x = \omega \ominus h$ for some $h \in H_n$. By Proposition 3.1.2, the number of ordinary generalised circles in the coset $S = H_n \oplus x$ equals

$$\frac{1}{2}\left|\left\{(a,b,c) \in H_n^3 : 2a \oplus b \oplus c = h, \quad a,b,c \text{ distinct}\right\}\right|,$$

which is easily seen to equal $\frac{1}{2}n^2 - O(n)$.

Similarly, the number of ordinary circles in $S = H_n \oplus x$ equals

$$\frac{1}{2}\left|\left\{(a,b,c) \in H_n^3 : 2a \oplus b \oplus c = h, \quad a,b,c \neq \ominus x \text{ and distinct}\right\}\right|,$$

which also equals $\frac{1}{2}n^2 - O(n)$.

As in the previous proposition, if $o \notin S$ (equivalently, $x \notin H_n$) then the number of 4-point circles is equal to $\frac{1}{24}(n^3 - 6n^2 + (8 + 3\delta_n)n - 6\epsilon_n)$, where δ_n is the number of solutions in H_n to the equation $2k = h$ and ϵ_n is the number of solutions in H_n to the equation $4k = h$. If H_n is cyclic, then we get the same numbers as in the previous construction. Otherwise, $n = 0 \pmod 4$, $H_n \cong \mathbb{Z}_{n/2} \times \mathbb{Z}_2$, and the number of 4-point circles equals

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 2 & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8, \end{cases}$$

which is greater than the corresponding number in the previous construction.

□

Proposition 3.2.3. *Let σ_1 and σ_2 be two cocenter circles and radius 1 and $r > 1$ respectively. Assume $S_1 \subset \sigma_1$ and $S_2 \subset \sigma_2$ are two subset corresponding to the set of vertices of two regular m-gon that are aligned for $m \geq 3$. Let $S = S_1 \cup S_2$ be a subset of $2m$ points where $m = \frac{n}{2}$, then*

- *S determines $\frac{n^2}{4} - O(n)$ ordinary generalised circles.*
- *S determines $\frac{n^2}{4} - O(n)$ ordinary circles.*
- *S determines $\frac{n^3}{32} - O(n^2)$ 4-rich circles.*

PROOF. We identify $\mathbb{R}^2$ with $\mathbb{C}$. Let σ_1 be the circle with centre the origin and radius one, and σ_2 the circle with centre the origin and radius $r > 1$. By the definition S_1 and S_2 are

$$S_1 = \left\{e^{2\pi ik/m} : k = 0, \dots, m-1\right\} \subset \sigma_1$$

and

$$S_2 = \left\{re^{2\pi ik/m} : k = 0, \dots, m-1\right\} \subset \sigma_2.$$

(see Figure 4). Let $S = S_1 \cup S_2$. By Proposition 3.1.7, the points $a, b \in \sigma_1$, $c, d \in \sigma_2$ are collinear or concyclic if and only if $a \oplus b \oplus c \oplus d = o$. In particular, if $a = b$, then the generalised circle through the three points is tangent to σ_1. It follows that if $n \geq 8$, the ordinary generalised circles of S are exactly those through $e^{2\pi ik_1/m}, re^{-2\pi ik_2/m}, re^{-2\pi ik_3/m}$ or through $re^{-2\pi ik_1/m}, e^{2\pi ik_2/m}, e^{2\pi ik_3/m}$ where $2k_1 + k_2 + k_3 \equiv 0 \pmod m$, with $k_2 \not\equiv k_3 \pmod m$.

For generic $r > 1$, we then obtain that the number of ordinary generalised circles equals

$$\left|\left\{(k_1, k_2, k_3) \in \mathbb{Z}_{m^3} : 2k_1 + k_2 + k_3 \equiv 0 \pmod m, \quad k_2, k_3 \text{ distinct}\right\}\right|$$

(although k_2 and k_3 are not ordered, we either have two points on σ_1 or two points on σ_2). This equals $m(m-2)$ if m is even and $m(m-1)$ if m is odd. That is, for generic r, we obtain $\frac{1}{4}n^2 - n$ ordinary generalised circles if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - \frac{1}{2}n$ ordinary generalised circles if $n \equiv 2 \pmod 4$.

If we choose $r = (\cos(2\pi k/m))^{-1}$ (there are $\lfloor m/4 \rfloor$ choices for r), then the tangent lines at points of S_1 pass through two points of S_2, so are ordinary generalised circles. Thus, for these choices of r we lose m ordinary circles, and obtain $\frac{1}{4}n^2 - \frac{3}{2}n$ ordinary circles if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - n$ ordinary circles if $n \equiv 2 \pmod 4$. Note that this is much less than the number of ordinary circles given by Proposition 3.2.1 and 3.2.2.

Similarly, the number of 4-point generalised circles spanned by S equals

$$\frac{1}{4}\left|\left\{(k_1, k_2, k_3, k_4) \in \mathbb{Z}_{m^4} : k_1 + k_2 + k_3 + k_4 \equiv 0 \pmod m, \quad k_1 \neq k_2 \text{ and } k_3 \neq k_4\right\}\right|,$$

which is $\frac{1}{4}m^3 - O(m^2) = \frac{1}{32}n^3 - O(n^2)$, also much less than the number in Proposition 3.2.1 and 3.2.2. □

Proposition 3.2.4. *Let σ_1, σ_2, S_1 and m be as in Proposition 3.2.3. Suppose that S_2' is the rotating of S_2 around the origin by an angle of $\frac{k\pi}{m}$. If $S' = S_1 \cup S_2'$, then*

- *S' determines m^2 ordinary generalized circles if m is even. Otherwise $m(m-1)$*
- *S' determines $\frac{n^2}{4} - O(n)$ ordinary circles.*
- *S' determines $\frac{n^3}{32} - O(n^2)$.*

PROOF. By the definition we have:

$$S_2' = \left\{re^{-i\pi(2k-1)/m} : k = 0, \dots, m-1\right\},$$

and $S' = S_1 \cup S_2'$ (see Figure 5). As before, if $n \geq 8$, the ordinary circles (including straight lines through exactly three points) of S' are exactly those through

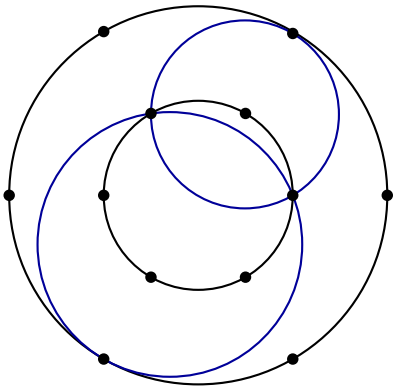


FIGURE 4. 'Aligned' double hexagon

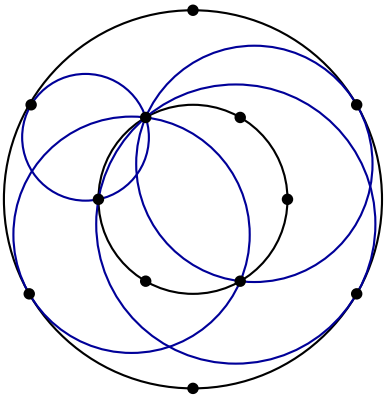


FIGURE 5. 'Offset' double hexagon

$e^{2\pi ik_1/m}, re^{-i\pi(2k_2-1)/m}, re^{-i\pi(2k_3-1)/m}$ or through $re^{-i\pi(2k_1-1)/m}, e^{2\pi ik_2/m}, e^{2\pi ik_3/m}$, where $2k_1 + k_2 + k_3 \equiv 1 \pmod m$ with $k_2 \not\equiv k_3 \pmod m$.

For generic $r > 1$, we now have to count the number of ordered triples in the set

$$\left\{(k_1, k_2, k_3) \in \mathbb{Z}_{m^3} : 2k_1 + k_2 + k_3 \equiv 1 \pmod m, \quad k_2, k_3 \text{ distinct}\right\}.$$

This equals m^2 if m is even and $m(m-1)$ if m is odd. That is, for generic r, we obtain $\frac{1}{4}n^2$ ordinary generalised circles if $n \equiv 0 \pmod 4$, worse than Proposition 3.2.3, and $\frac{1}{4}n^2 - \frac{1}{2}n$ ordinary generalised circles if $n \equiv 2 \pmod 4$, the same number as in Proposition 3.2.3.

Again, if we choose $r = (\cos(2\pi k/m))^{-1}$ (there are $\lfloor m/4 \rfloor$ choices for r), we lose m ordinary circles. Thus, we obtain $\frac{1}{4}n^2 - n$ ordinary circles if $n \equiv 2 \pmod 4$, the same number as in Proposition 3.2.3.

As in Proposition 3.2.3, we get $\frac{1}{32}n^3 - O(n^2)$ 4-point circles. □

Proposition 3.2.5. *Let σ_1, σ_2, S_1 and S_2 be as in Proposition 3.2.3. Assume that $n = 2m - 1 \geq 11$ is odd, and remove an arbitrary $p \in S_1$. Then*

- *$S \setminus \{p\}$ determines $\frac{3n^2}{8} - O(n)$ ordinary generalised circles.*
- *$S \setminus \{p\}$ determines $\frac{n^3}{32} - O(n^2)$ 4-rich generalised circles.*

PROOF. First assume that m is odd. Before we remove p, there are $m(m-1)$ ordinary generalised circles. Of these, there are $(m-1)/2$ tangent at p. There are also $m-1$ ordinary generalised circles through p tangent at some point of S_2. Thus, by removing p, we destroy $3(m-1)/2$ ordinary generalised circles and create $\binom{m}{2} - (m-1)/2$ new ones. Therefore, $S \setminus \{p\}$ has

$$m(m-1) - \frac{3}{2}(m-1) + \binom{m}{2} - \frac{1}{2}(m-1) = \frac{3}{2}m^2 - \frac{7}{2}m + 2$$

ordinary generalised circles. That is, there are $\frac{3}{8}n^2 - n + \frac{5}{8}$ ordinary generalised circles if $n \equiv 1 \pmod 4$.

Next assume that m is even. Before we remove p, there are $m(m-2)$ ordinary generalised circles, of which there are $(m-2)/2$ through two different points of S_2 tangent at p, and there are also $m-2$ ordinary generalised circles through p tangent at a point of S_2. As before, we obtain

$$m(m-2) - \frac{3}{2}(m-2) + \binom{m}{2} - \frac{1}{2}(m-2) = \frac{3}{2}m^2 - \frac{9}{2}m + 4$$

ordinary generalised circles. Thus, we obtain $\frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8}$ ordinary generalised circles if $n \equiv 3 \pmod 4$.

Instead of starting with Construction 3.2.3, we can take the 'offset' Construction 3.2.4 and remove a point. It is easy to see that when $n \equiv 1 \pmod 4$ we obtain the same number of ordinary generalised circles, while if $n \equiv 3 \pmod 4$ we obtain more.

Since there are no 5-point circles in Propositions 3.2.3 and 3.2.4 when $m \geq 6$, removing a point does not add any 4-point circle, but destroys $O(n^2)$ of them. We thus get $\frac{1}{32}n^3 - O(n^2)$ 4-point generalised circles, which is asymptotically the same as in Propositions 3.2.3 and 3.2.4. □

Now in the following example by applying an inversion to the example of Proposition 3.2.5 we obtain an example with few ordinary circles. More precisely,

Corollary 3.2.6. *Suppose that $\sigma_1, \sigma_2, \setminus\{p\}$ and m are as in the Proposition 3.2.5. Assume I_p is an inversion with centre at p (removed point from S). The resulting point set has m points on a circle and $m-1$ points on a line disjoint from the circle. Then*

- *$I_p(\setminus\{p\})$ determines $\frac{(m-1)(2m-3)}{2}$ ordinary circles when m is odd.*
- *$I_p(\setminus\{p\})$ determines $\frac{(m-2)(2m-3)}{2}$ ordinary circles when m is even.*

Proof. Every ordinary circle after the inversion corresponds to an ordinary generalised circle not passing through p before the inversion. If m is odd, there are $(m-1)/2$ ordinary generalised circles tangent at p and a further $m-1$ ordinary generalised circles through p tangent to σ_2, so we obtain $m(m-1) - 3(m-1)/2 = \frac{1}{2}(m-1)(2m-3)$ ordinary circles. For even m we similarly obtain $m(m-2) - 3(m-2)/2 = \frac{1}{2}(m-2)(2m-3)$ ordinary circles. That is, we have $\frac{1}{4}(n-1)(n-2) = \frac{1}{4}n^2 - \frac{3}{4}n + \frac{1}{2}$ ordinary circles when $n \equiv 1 \pmod 4$ and $\frac{1}{4}(n-3)(n-2) = \frac{1}{4}n^2 - \frac{5}{4}n + \frac{3}{2}$ ordinary circles when $n \equiv 3 \pmod 4$.

If we remove another point from this inverted construction, we obtain a set of n points where n is even, with $\frac{3}{8}n^2 - O(n)$ ordinary circles. □

Remark 3.2.7. If we invert Proposition 3.2.1 in a point on the ellipse that is not in the set S, then by Proposition 2.2.11, we obtain points on an acnodal circular cubic (without its acnode) as in proposition 3.2.2, with the same number of ordinary and 4-point generalised circles.

If we invert a circular cubic in a point not on the curve, then we obtain a bicircular quartic by Lemma 2.2.9. There will again be $\frac{1}{2}n^2 - O(n)$ ordinary circles (or ordinary generalised circles) and $\frac{1}{24}n^3 - O(n^2)$ 4-point circles among the inverted points.

3.3. The structure theorems

In This section we will proof several structure theorems for the finite sets in the plane that determines few ordinary circles. In the next Section 3.4 by using strong structure theorem 3.3.3 We are proving the minimum number of ordinary circles determined by a set of n points.

3.3.1. Proof of the weak structure theorem. In this section we will proof the fist structure theorem for the set with few ordinary circles, namely

Theorem 3.3.1 (Weak structure theorem)**.** *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary generalised circles, then all but at most $O(K)$ points of P lie on a bicircular quartic.*

The proofs of our structure theorems for sets with few ordinary circles crucially rely on the following structure theorem for sets with few ordinary lines due to Green and Tao [**GT13**]. Recall that an *ordinary line* is a line containing exactly two points of the given point set.

Theorem 3.3.2 (Green–Tao)**.** *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn ordinary lines, then P differs in at most $O(K)$ points from an example of one of the following types:*

(1) *$n - O(K)$ points on a line;*
(2) *m points each on a line and a disjoint conic, for some $m = \frac{n}{2} \pm O(K)$*
(3) *$n \pm O(K)$ points on an acnodal or smooth cubic.*

Proof. Let P be a set of n points spanning at most Kn^2 ordinary generalised circles. We wish to show that P lies mostly on a bicircular quartic (we will repeatedly use 'mostly' to mean 'for all but $O(K)$ points').

Note that for at least $2n/3$ points p of P, there are at most $9Kn$ ordinary circles through p, hence the set $I_p(P\backslash\{p\})$ spans at most $9Kn$ ordinary lines. Let P' be the set of such points. For n sufficiently large depending on K, applying Theorem 3.3.2 to $I_p(P \setminus \{p\})$ for any $p \in P'$ gives that $I_p(P \setminus \{p\})$ lies mostly on a line, a line and a conic, an acnodal cubic, or a smooth cubic.

If there exists $p \in P'$ such that $I_p(P \setminus \{p\})$ lies mostly on a line, then inverting again in p, we see that P must lie mostly on a line or a circle.

If there exists $p \in P'$ such that $I_p(P \setminus \{p\})$ lies mostly on a line l and a disjoint conic σ, we have two cases, depending on whether p lies on l or not.

If $p \in l$, we invert again in p to find that P lies mostly on the union of l and $I_p(\sigma)$. By Lemma 2.2.9, $I_p(\sigma)$ is either a circle (if σ is a circle) or an irreducible bicircular quartic (if σ is a non-circular conic). Furthermore, p is the only point that could possibly lie on both l and $I_p(\sigma)$. Since roughly $n/2$ points of P lie on l, there must be another point $q \in l \cap P'$ that does not lie on $I_p(\sigma)$. In $I_q(P \setminus \{q\})$, the line l remains a line, and by definition of P' the set $I_q(P \setminus \{q\})$ spans few ordinary lines, so Theorem 3.3.2 tells us $I_q(I_p(\sigma))$ is a conic. It follows from Lemma 2.2.9 that $I_p(\sigma)$ cannot be a quartic, since we inverted in the point q outside $I_p(\sigma)$ and did not obtain a quartic. That means $I_p(\sigma)$ has to be a circle, and it is disjoint from l. Thus, P lies mostly on the union of a line and a disjoint circle.

If $p \notin l$, we invert in p to see that P lies mostly on the union of the circle $I_p(l)$ and the curve $I_p(\sigma)$, which is either a circle or a quartic. Again p is the only point that

can lie on both curves. Inverting in another point $q \in I_p(l) \cap P'$, $I_q(I_p(l))$ becomes a line, so Theorem 3.3.2 tells us that $I_q(I_p(\sigma))$ is a conic, so that $I_p(\sigma)$ must be a circle disjoint from $I_p(l)$ as before. Thus, P lies mostly on the union of two disjoint circles.

The case that remains is when for all $p \in P'$, the set $I_p(P \setminus \{p\})$ lies mostly on an acnodal or smooth cubic γ. Fix such a p, and consider $I_p(\gamma)$, which mostly contains P. If γ is not a circular cubic, then by the classification in Section 2.2 it has circular degree three, so $I_p(\gamma)$ has circular degree three as well. For any $q \in I_p(\gamma) \cap P'$ other than p, the curve $I_q(I_p(\gamma))$ is also a cubic curve, by the definition of P' and Theorem 3.3.2. By Case 3 of Lemma 2.2.9, this can only happen if q is a singularity of $I_p(\gamma)$. But $I_p(\gamma)$ is an irreducible curve of degree at most six, and so has at most 10 singularities by [**Wal78**, Theorem 4.4], which is a contradiction. So γ must be a circular cubic that is acnodal or smooth. If γ is acnodal, then $I_p(\gamma)$ is either a bicircular quartic (if $p \notin \gamma$), an acnodal circular cubic (if p is a regular point of γ), or a non-circular conic (if p is the singularity of γ). In the last case, the conic is an ellipse by Proposition 2.2.11. If γ is smooth, then $I_p(\gamma)$ is either a bicircular quartic or a smooth circular cubic.

We have encountered the following curves that P could mostly lie on: a line, a circle, an ellipse, a disjoint union of a line and a circle, a disjoint union of two circles, a circular cubic, or a bicircular quartic. All of these are subsets of bicircular quartics, which proves the statement of Theorem 3.3.1. □

3.3.2. Proof of the strong structure theorem.

Theorem 3.3.3 (Strong structure theorem)**.** *Let $K > 0$ and let n be sufficiently large depending on K. If a set P of n points in $\mathbb{R}^2$ spans at most Kn^2 ordinary generalised circles, then up to inversions and similarities, P differs in at most $O(K)$ points from a configuration of one of the following types:*

1. *A subset of a line;*
2. *A subgroup of an ellipse;*
3. *A coset $H \oplus x$ of a subgroup H of a smooth circular cubic, for some x such that $4x \in H \oplus \alpha \oplus \beta$, where α and β are the two circular points at infinity;*
4. *A double polygon that is 'aligned' or 'offset'.*

Conversely, every set of these types defines at most $O(Kn^2)$ ordinary generalised circles.

First of all, as explained in Section 3.2, a subgroup of an ellipse and an appropriate coset of a subgroup of a smooth circular cubic both have at most $\frac{1}{2}n^2$ ordinary generalised circles, and a double polygon has at most $\frac{1}{4}n^2$ ordinary generalised circles. It follows from Lemma 3.3.4 below that if we add and/or remove $O(K)$ points, then there will be at most $O(Kn^2)$ ordinary generalised circles.

Lemma 3.3.4. *Let S be a set of n points in $\mathbb{R}^2$ with s ordinary generalised circles. Let T be a set that differs from S in at most K points: $|S \triangle T| \leq K$. Then T has at most $s + O(Kn^2 + K^2n + K^3)$ ordinary generalised circles.*

Proof. First note that if we add a point to any set of n points, we create at most $\binom{n}{2}$ ordinary generalised circles. Secondly, since two circles intersect in at most two points, the number of 4-point circles through a fixed point in a set of n points is at most $\frac{1}{3}\binom{n-1}{2}$, so by removing a point we create at most $\frac{1}{3}\binom{n-1}{2} < \binom{n}{2}$

ordinary generalised circles. It follows that by adding and removing $O(K)$ points, we create at most

$$\binom{n}{2} + \binom{n+1}{2} + \cdots + \binom{n+K-1}{2} = O(Kn^2 + K^2 n + K^3)$$

ordinary generalised circles. □

Next, let P be a set of n points with at most Kn^2 ordinary generalised circles. From the proof of Theorem 3.3.1 above, we see that P differs in at most $O(K)$ points from a line, a circle, an ellipse, a disjoint union of a line and a circle, a disjoint union of two circles, a circular cubic, or a bicircular quartic. Moreover, in the proof we saw that the circular cubic must be acnodal or smooth, and that the bicircular quartic has the property that if we invert in a point on the curve, the resulting circular cubic is acnodal or smooth.

Using inversions, we can reduce the number of types of curves that we need to analyse further.

- If P lies mostly on a line, then we are in Case 1 of Theorem 3.3.3, so we are done.
- If P lies mostly on a circle, then inverting in a point on the circle puts us in Case 1 again.
- If P lies mostly on an ellipse, then inverting in a point of the ellipse places P mostly on an acnodal circular cubic.
- If P lies mostly on a bicircular quartic, then inverting in any regular point on the curve gives us a circular cubic. As mentioned above, this cubic is acnodal or smooth.
- If P lies mostly on a line and a disjoint circle, then an inversion in a point not on the line or circle places P mostly on two disjoint circles.
- If P lies mostly on the disjoint union of two circles, we can apply an inversion that maps the two disjoint circles to two concentric circles [**Bla00**, Theorem 1.7].

So, up to inversions, we need only consider the cases when P lies mostly on an acnodal or smooth circular cubic, or on two concentric circles. We do this in Lemmas 3.3.7 and 3.3.8 below, which will complete the proof of Theorem 3.3.3.

To determine the structure of P, we use a variant of a lemma from additive combinatorics that was used by Green and Tao [**GT13**]. It captures the principle that if a finite subset of a group is almost closed under addition, then it is close to a subgroup. The following statement is Proposition A.5 in [**GT13**].

Proposition 3.3.5. *Let $K > 0$ and let n be sufficiently large depending on K. Let A, B, C be three subsets of some abelian group $(G, \oplus)$, all of cardinality within K of n. Suppose there are at most Kn pairs $(a, b) \in A \times B$ for which $a \oplus b \notin C$. Then there is a subgroup $H \leq G$ and cosets $H \oplus x$, $H \oplus y$ such that*

$$|A \triangle (H \oplus x)|, |B \triangle (H \oplus y)|, |C \triangle (H \oplus x \oplus y)| = O(K).$$

The variant that we need is a simple corollary of Proposition 3.3.5.

Corollary 3.3.6. *Let $K > 0$ and let n be sufficiently large depending on K. Let A, B, C, D be four subsets of some abelian group $(G, \oplus)$, all of cardinality within K of n. Suppose there are at most Kn^2 triples $(a, b, c) \in A \times B \times C$ for which $a \oplus b \oplus c \notin D$. Then there is a subgroup $H \leq G$ and cosets $H \oplus x$, $H \oplus y$, $H \oplus z$ such that*

$$|A \triangle (H \oplus x)|, |B \triangle (H \oplus y)|, |C \triangle (H \oplus z)|, |D \triangle (H \oplus x \oplus y \oplus z)| = O(K).$$

PROOF. By the pigeonhole principle, there exists an $a_0 \in A$ such that there are at most $K'n$ (where $K' = O(K)$) pairs $(b,c) \in B \times C$ for which $a_0 \oplus b \oplus c \notin D$, or equivalently $b \oplus c \notin D \ominus a_0$. Applying Proposition 3.3.5, we have a subgroup $H \leq G$ and cosets $H \oplus y$, $H \oplus z$ such that

$$|B \triangle (H \oplus y)|, |C \triangle (H \oplus z)|, |(D \ominus a_0) \triangle (H \oplus y \oplus z)| = O(K).$$

Since $|B \cap (H \oplus y)| \geq n - O(K)$, we repeat the argument above to obtain $b_0 \in B \cap (H \oplus y)$ such that there are at most $O(Kn)$ pairs $(a,c) \in A \times C$ with $a \oplus b_0 \oplus c \notin D$, and Proposition 3.3.5 gives a subgroup $H' \leq G$ and cosets $H' \oplus x$, $H' \oplus z'$ such that

$$|A \triangle (H' \oplus x)|, |C \triangle (H' \oplus z')|, |(D \ominus b_0) \triangle (H' \oplus x \oplus z')| = O(K).$$

From this, it follows that $|(H \oplus z) \triangle (H' \oplus z')| = O(K)$, hence $|(H \oplus z) \cap (H' \oplus z')| \geq n - O(K)$. Since $(H \oplus z) \cap (H' \oplus z')$ is not empty, it has to be a coset of $H' \cap H$. If $H' \neq H$, then $|H' \cap H| \leq n/2 + O(K)$, a contradiction. Therefore, $H = H'$ and $H \oplus z = H' \oplus z'$. So we have $|A \triangle (H \oplus x)|, |B \triangle (H \oplus y)|, |C \triangle (H \oplus z)|, |D \triangle (H \oplus x \oplus b_0 \oplus z)| = O(K)$. Since $b_0 \in H \oplus y$, we obtain $|D \triangle (H \oplus x \oplus y \oplus z)| = O(K)$ as well. □

Lemma 3.3.7 (Circular cubic)**.** *Let $K > 0$ and let n be sufficiently large depending on K. Suppose P is a set of n points in $\mathbb{R}^2$ spanning at most Kn^2 ordinary generalised circles, and all but at most K points of P lie on an acnodal or smooth circular cubic γ. Then there is a coset $H \oplus x$ of a subgroup $H \leq \gamma^*$, with $4x \in H \oplus \omega$, such that $|P \triangle (H \oplus x)| = O(K)$.*

PROOF. Let $P' = P \cap \gamma^*$. Then $|P \triangle P'| = O(K)$, and by Lemma 3.3.4, P' spans at most $O(Kn^2)$ ordinary circles. If a, b, $c \in \gamma$ are distinct, then by Proposition 3.1.2, the generalised circle through a, b, c meets γ again in the unique point $d = \omega \ominus (a \oplus b \oplus c)$. This implies that $d \in P'$ for all but at most $O(Kn^2)$ triples a, b, $c \in P'$, or equivalently $a \oplus b \oplus c \in \omega \ominus P'$. Applying Corollary 3.3.6 with $A = B = C = P'$ and $D = \omega \ominus P'$, we obtain $H \leq \gamma^*$ and a coset $H \oplus x$ such that $|P \triangle (H \oplus x)| = O(K)$ and $|(\omega \ominus P') \triangle (H \oplus 3x)| = O(K)$, which is equivalent to $|P \triangle (H \ominus 3x \oplus \omega)| = O(K)$. Thus we have $|(H \oplus x) \triangle (H \ominus 3x \oplus \omega)| = O(K)$, which implies $4x \in H \oplus \omega$. □

Lemma 3.3.8 (Concentric circles)**.** *Let $K > 0$ and let n be sufficiently large depending on K. Suppose P is a set of n points in $\mathbb{R}^2$ spanning at most Kn^2 ordinary generalised circles. Suppose all but at most K of the points of P lie on two concentric circles, and that P has $n/2 \pm O(K)$ points on each. Then, up to similarity, P differs in at most $O(K)$ points from an 'aligned' or 'offset' double polygon.*

PROOF. By scaling and rotating, we can assume that P lies mostly on the two concentric circles $\sigma_1 = \{e^{2\pi it} : t \in [0,1)\}$ and $\sigma_2 = \{re^{-2\pi it} : t \in [0,1)\}$, $r > 1$, which we gave a group structure in Section 3.1.2.

Let $P_1 = P \cap \sigma_1$ and $P_2 = P \cap \sigma_2$. Then $|P \triangle (P_1 \cup P_2)| = O(K)$, and by Lemma 3.3.4, $P_1 \cup P_2$ spans at most $O(Kn^2)$ ordinary circles. If $a, b \in \sigma_1$ and $c \in \sigma_2$ with $a \neq b$, then by Lemma 3.1.7, the generalised circle through a, b, c meets $\sigma_1 \cup \sigma_2$ again in the unique point $d = \ominus(a \oplus b \oplus c)$. This implies $d \in P_2$ for all but at most $O(Kn^2)$ triples (a,b,c) with $a, b \in P_1$ and $c \in P_2$. Applying Corollary 3.3.6 with $A = B = P_1$, $C = P_2$ and $D = \ominus P_2$, we get cosets $H \oplus x$ and $H \oplus y$ of $\sigma_1 \cup \sigma_2$ such that $|P_1 \triangle (H \oplus x)|, |P_2 \triangle (H \oplus y)| = O(K)$ and $2x \oplus 2y \in H$, where $x \in \sigma_1$ and $y \in \sigma_2$. It follows that $H \leq \sigma_1$, hence H is a cyclic group of order $m = n/2 \pm O(K)$,

and $H \oplus x$ and $H \oplus y$ are the vertex sets of regular m-gons inscribed in σ_1 and σ_2, respectively, either 'aligned' or 'offset' depending on whether $x \oplus y \in H$ or not. □

Together these lemmas prove Theorem 3.3.3. It just remains to remark that if P differs in $O(K)$ points from a coset on an acnodal circular cubic, then we apply inversion in its singularity. By Proposition 2.2.11, we obtain that P differs in $O(K)$ points from a coset $H \oplus x$ of a finite subgroup H of an ellipse, where $4x = o$. Thus, x is a point of the ellipse with eccentric angle a multiple of $\pi/2$. After a rotation, we can assume that $x = o$, which is Case 2 of Theorem 3.3.3. □

3.4. Extremal configurations

In this section we prove Theorems 3.4.6, 3.4.1, and 3.4.8. The prove of these theorems are consequences of the structure theorems have proven in previous section. We first consider generalised circles.

3.4.1. Ordinary generalised circles.

Theorem 3.4.1 (Ordinary generalised circles)**.**

(1) *If n is sufficiently large, the minimum number of ordinary generalised circles determined by n points in $\mathbb{R}^2$, not all on a generalised circle, equals*

$$\begin{cases} \frac{1}{4}n^2 - n & \text{if } n \equiv 0 \pmod 4, \\ \frac{3}{8}n^2 - n + \frac{5}{8} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - \frac{1}{2}n & \text{if } n \equiv 2 \pmod 4, \\ \frac{3}{8}n^2 - \frac{3}{2}n + \frac{17}{8} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines fewer than $\frac{1}{2}n^2 - Cn$ ordinary generalised circles, then P lies on two disjoint generalised circles.*

Suppose P is an n-point set in $\mathbb{R}^2$ spanning fewer than $\frac{1}{2}n^2$ ordinary generalised circles, and that P is not contained in a generalised circle. Applying Theorem 3.3.3, we can conclude that, up to inversions, P differs in $O(1)$ points from one of the following examples: points on a line, a coset of a subgroup of an acnodal or smooth circular cubic, or a double polygon.

The first type of set is very easy to handle. Note that the lower bound is on the number of ordinary circles, not counting 3-point lines.

Lemma 3.4.2. *Let $K \geq 1$ and $n \geq 2K + 4$. If all except K points of a set $P \subset \mathbb{R}^2$ of n points lie on a line, then P spans at least $\binom{n-1}{2}$ ordinary circles.*

Proof. Let ℓ be a line such that $|P \cap \ell| = n - K$. For any $p \in P \cap \ell$ and $q \in P \setminus \ell$ there are at most $K - 1$ non-ordinary circles through p, q, another point on $P \cap \ell$, and another point in $P \setminus \ell$. Therefore, there are at least $K(n - 2K)$ ordinary circles through p. This holds for any of the $n - K$ points $p \in P \cap \ell$, and we obtain at least $\frac{1}{2}K(n-2K)(n-K)$ ordinary circles. It is easy to see that when $1 \leq K \leq (n-4)/2$, $\frac{1}{2}K(n-2K)(n-K)$ is minimised when $K = 1$. □

Cosets on cubics are also relatively easy to handle. We again obtain a lower bound on the number of ordinary circles, not including 3-point lines.

Lemma 3.4.3. *Suppose $P \subset \mathbb{R}^2$ differs in K points from a coset $H \oplus x$ of an acnodal or smooth circular cubic, where $|H| = n \pm O(K)$ and $4x \ominus \omega \in H$. Then P spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary circles.*

PROOF. Suppose that P differs in K points from $H \oplus x$. We know from Construction 3.2.2 that $H \oplus x$ spans $\frac{1}{2}n^2 - O(n)$ ordinary circles, all of which are tangent to γ. We show that adding or removing K points destroys no more than $O(Kn)$ of these ordinary circles, so that the resulting set P still spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary circles.

Suppose we add a point $q \notin H \oplus x$. For $p \in H \oplus x$, at most one circle tangent to γ at p can pass through q. Thus, adding q destroys at most n ordinary circles. Now suppose we remove a point $p \in H \oplus x$. Since ordinary circles of $H \oplus x$ correspond to solutions of $2p \oplus q \oplus r = \omega$ or $p \oplus 2q \oplus r = \omega$, there are at most $O(n)$ solutions for a fixed p. Thus removing p destroys at most $O(n)$ ordinary circles.

Repeating K times, we see that adding or removing K points to or from $H \oplus x$ destroys at most $O(Kn)$ ordinary generalised circles out of the $\frac{1}{2}n^2 - O(n)$ spanned by $H \oplus x$. This proves that P spans at least $\frac{1}{2}n^2 - O(Kn)$ ordinary circles. □

From the two lemmas above we know that there is an absolute constant C such that a set of n points, not all collinear or concyclic, spanning at most $\frac{1}{2}n^2 - Cn$ ordinary generalised circles, differs in $O(1)$ points from Case 4 in Theorem 3.3.3. This case, where P is close to the vertex set of a double polygon, requires a more careful analysis of the effect of adding or removing points.

We use the following special case of a result due to Raz, Sharir, and De Zeeuw [**RSDZ16b**].

Proposition 3.4.4. *If $P \subset \mathbb{R}^2$ is a set of n points contained in two circles, then the number of lines with at least three points of P is at most $O(n^{11/6})$.*

PROOF. Denote the two circles by σ_1 and σ_2. We use [**RSDZ16b**, Theorem 6.1], which states that for (not necessarily distinct) algebraic curves C_1, C_2, C_3 of constant degree, and finite sets $S_i \subset C_i$, the number of collinear triples $(p_1, p_2, p_3) \in S_1 \times S_2 \times S_3$, with p_1, p_2, p_3 distinct, is bounded by $O(|S_1|^{1/2}|S_2|^{2/3}|S_3|^{2/3} + |S_1| + |S_1|^{1/2}|S_2| + |S_1|^{1/2}|S_3|)$, unless $C_1 \cup C_2 \cup C_3$ is a line or a cubic. Let $C_1 = \sigma_1$ and $C_2 = C_3 = \sigma_2$. Set $S_i = P \cap C_i$ for $i = 1, 2, 3$. Every line with at least one point of S_1 and two points of $S_2 = S_3$ corresponds to a collinear triple in $S_1 \times S_2 \times S_3$. Since the union of two circles is not a line or a cubic, we can apply the theorem to get the bound $O(n^{11/6})$ for the number of collinear triples in P with one point in σ_1 and two points in σ_2. Similarly, the number of collinear triples in P with one point in σ_2 and two points in σ_1 is also $O(n^{11/6})$. Since a line intersects $\sigma_1 \cup \sigma_2$ in at most four points, we also obtain the bound $O(n^{11/6})$ for the number of lines with at least three points. □

Lemma 3.4.5. *Let S be a double polygon with m points on each circle. Let $P = (S \setminus A) \cup B$ be a set of n points, where A is a subset of S with $a = O(1)$ points and B is a set disjoint from S with $b = O(1)$ points. Then P spans at least $\frac{1}{8}(2 + a + 4b)n^2 - O(n^{11/6})$ ordinary generalised circles.*

PROOF. We know from Propositions 3.2.3 and 3.2.4 that S spans $\frac{1}{4}n^2 - O(n)$ ordinary generalised circles.

Consider first the number of ordinary generalised circles spanned by $S \setminus A$. As we saw in Proposition 3.2.5, removing a point $p \in S$ destroys at most $3m/2$ ordinary generalised circles spanned by S, and adds $\frac{1}{2}m^2 - O(m) = \frac{1}{8}n^2 - O(n)$ ordinary generalised circles. Noting that there are at most m 4-point generalised circles spanned by S that go through any two given points of A, we thus have by inclusion-exclusion that $S \setminus A$ determines at least $(\frac{1}{4}+\frac{a}{8})n^2 - O(n)$ ordinary generalised circles.

Now consider adding $q \in B$ to S. For any pair of points from $S \setminus A$, adding $q \in B$ creates a new ordinary generalised circle, unless the generalised circle through the pair and q contains three or four points of $S \setminus A$. We already saw that the number of ordinary generalised circles hitting a fixed point is $O(n)$, so it remains to bound the number of 4-point generalised circles of S that hit q. If q lies on one of the concentric circles, then no 4-point generalised circles hit q, so we can assume that q does not. Applying inversion in q reduces the problem to bounding the number of 4-point lines determined by a subset of two circles. By Proposition 3.4.4, this number is bounded by $O(n^{11/6})$, so p lies on at most $O(n^{11/6})$ of the 4-point generalised circles spanned by S. Adding q to S thus creates at least $\binom{n}{2} - O(n^{11/6})$ ordinary generalised circles. Note that each $p \in A$ that was removed destroys at most n of these circles.

Adding q to $S \setminus A$ also destroys at most $O(n)$ ordinary circles, since for each $p \in S$ there is only one circle tangent at p and going through q, and for each $p \in A$, at most m ordinary circles spanned by $S \setminus A$ go through p. Finally, since there are at most $2m$ circles through two points of B that also go through two points of $S \setminus A$, $P = (S \setminus A) \cup B$ spans at least $(\frac{1}{4} + \frac{a}{8} + \frac{b}{2})n^2 - O(n^{11/6})$ ordinary generalised circles. □

Theorem 3.4.1 then follows easily from the lemmas above.

Proof of Theorem 3.4.1. Suppose that P is a set of n points in $\mathbb{R}^2$ with fewer than $\frac{1}{2}n^2 - Cn$ ordinary generalised circles, where C is sufficiently large. Without loss of generality, n is also sufficiently large. By Lemmas 3.4.2 and 3.4.3, we need only consider the case where P differs by $O(1)$ points from a double polygon. In the notation of Lemma 3.4.5, we have $P = (S \setminus A) \cup B$ and $\frac{1}{8}(2 + a + 4b) < \frac{1}{2}$, which implies that $a \leq 1$ and $b = 0$. So P is either equal to S, or is obtained from S by removing one point, which are exactly the cases in propositions 3.2.3, 3.2.4, and 3.2.5. In particular, the minimum number of ordinary generalised circles occurs in Propositions 3.2.3 when $n \equiv 0 \pmod 4$, in Propositions 3.2.5 when $n \equiv 1, 3 \pmod 4$, and in propositions 3.2.3 and 3.2.4 when $n \equiv 2 \pmod 4$. □

3.4.2. Ordinary circles. We now consider what happens if we do not count generalised circles that are lines, and prove Theorem 3.4.6.

Theorem 3.4.6 (Ordinary circles)**.**

(1) *If n is sufficiently large, the minimum number of ordinary circles determined by n points in $\mathbb{R}^2$, not all on a line or a circle, equals*

$$\begin{cases} \frac{1}{4}n^2 - \frac{3}{2}n & \text{if } n \equiv 0 \pmod 4, \\ \frac{1}{4}n^2 - \frac{3}{4}n + \frac{1}{2} & \text{if } n \equiv 1 \pmod 4, \\ \frac{1}{4}n^2 - n & \text{if } n \equiv 2 \pmod 4, \\ \frac{1}{4}n^2 - \frac{5}{4}n + \frac{3}{2} & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines fewer than $\frac{1}{2}n^2 - Cn$ ordinary circles, then P lies on the disjoint union of two circles, or the disjoint union of a line and a circle.*

Proof of Theorem 3.4.6. Let P be a set of n points not all on a line or a circle, with at most $\frac{1}{2}n^2 - Cn$ ordinary circles, for a sufficiently large C. By a simple double counting argument, there are at most $\frac{1}{6}n^2$ 3-point lines, so there are at most $\frac{2}{3}n^2 - O(n)$ ordinary generalised circles. By Theorem 3.3.3, up to inversions and up to $O(1)$ points, P lies on a line, an ellipse, a smooth circular cubic, or two concentric circles. By Lemmas 3.4.2 and 3.4.3, the first three cases give us at least $\frac{1}{2}n^2 - O(n)$ ordinary circles, contrary to assumption. Therefore, we only need to consider the case where, when P is transformed by an inversion to P', we have $P' = (S \setminus A) \cup B$, where S is a double polygon ('aligned' or 'offset'), and $|A| = a$, $|B| = b$.

By Lemma 3.4.5, P' has at least $\frac{1}{8}(2 + a + 4b)n^2 - O(n^{11/6})$ ordinary generalised circles, which gives us the inequality $\frac{1}{8}(2+a+4b) < \frac{2}{3}$, which in turn gives us $a \leq 3$ and $b = 0$. Therefore, P' lies on two concentric circles, and P lies on the disjoint union of two circles or the disjoint union of a line and a circle.

Suppose that $a = 3$ (and $b = 0$). Then P' has $\frac{5}{8}n^2 - O(n)$ ordinary generalised circles. Those passing through the centre of the inversion that transforms P to P', are inverted back to straight lines passing through three points of P. As in the proof of Lemma 3.4.5, there are $\frac{1}{8}n^2 - O(n)$ ordinary generalised circles that pass through any point of A. Also, we can use Lemma 3.4.7 below to show that there are at most $O(n)$ ordinary generalised circles spanned by $S \setminus A$ that intersect in the same point not in S. Indeed, by Lemma 3.4.7, there are at most $n/2$ ordinary generalised circles of S that intersect in the same point $p \notin S$. Furthermore, for each point $q \in A$ there are $O(n)$ generalised circles through p, q, and two more points of S. It follows that there are $O(n)$ ordinary generalised circles spanned by $S \setminus A$ through p.

Thus, if the centre of inversion is in A, P has $\frac{1}{2}n^2 - O(n)$ ordinary circles, which is a contradiction if C is chosen large enough. On the other hand, if the centre of inversion is not in A, then P has $\frac{5}{8}n^2 - O(n)$ ordinary circles, also a contradiction.

Therefore, we have $a \leq 2$, which means that P' is a set of n points as in Propositions 3.2.3, 3.2.4, 3.2.5, or 3.2.6.

Next, suppose that n is even. If $a = 2$, then there are $\frac{1}{2}n^2 - O(n)$ ordinary generalised circles and through both points of A there are $\frac{1}{8}n^2 - O(n)$ ordinary generalised circles. If we invert in one of these points in A, we obtain a set with $\frac{3}{8}n^2 - O(n)$ ordinary circles (as in proposition 3.2.6), which is not extremal. Otherwise, $a = 0$, P' is as in Propositions 3.2.3 or 3.2.4, and there are at least $\frac{1}{4}n^2 - n$ ordinary generalised circles if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - \frac{1}{2}n$ if $n \equiv 2 \pmod 4$. Let p be the centre of the inversion that transforms P to P'. Then all the 3-point lines of P are inverted to ordinary circles in the double polygon P', all passing through p. By Lemma 3.4.7 below, there are at most $n/2$ ordinary circles that intersect in the same point not in P'. Thus, in P there at most $n/2$ 3-point lines, and the number of ordinary circles (not including lines) is at least $\frac{1}{4}n^2 - \frac{3}{2}n$ if $n \equiv 0 \pmod 4$ and $\frac{1}{4}n^2 - n$ if $n \equiv 2 \pmod 4$, which match Proposition 3.2.3 (and Proposition 3.2.4 if $n \equiv 2 \pmod 4$), if the radii are chosen so that each vertex of the inner polygon has an ordinary generalised circle that is a straight line tangent to it.

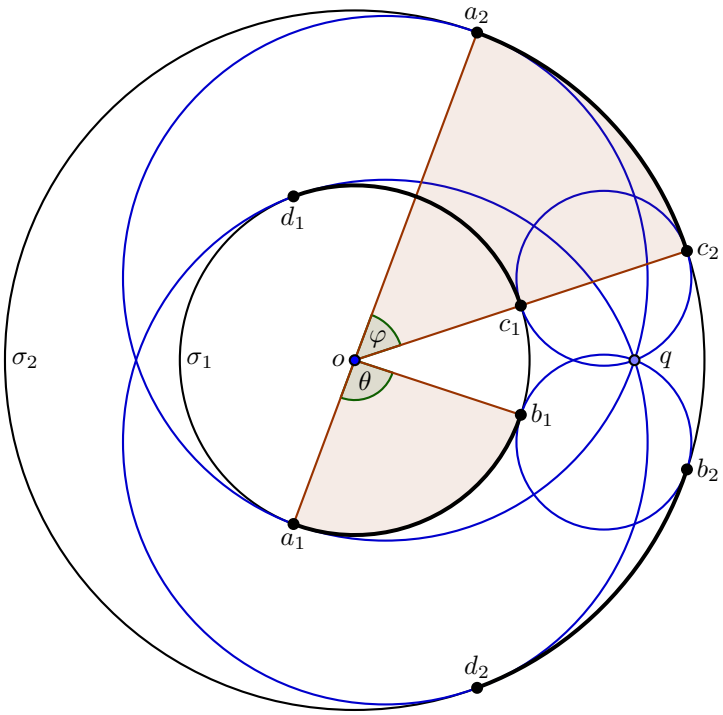


FIGURE 6. Bitangent circles through q

Finally, suppose that n is odd. Then $a = 1$ and P' is as in Proposition 3.2.5, with $\frac{3}{8}n^2 - O(n)$ ordinary generalised circles. It follows that P must be as in Proposition 3.2.6, with $\frac{1}{4}n^2 - \frac{3}{4}n + \frac{1}{2}$ ordinary circles if $n \equiv 1 \pmod 4$ and $\frac{1}{4}n^2 - \frac{5}{4}n + \frac{3}{2}$ ordinary circles if $n \equiv 3 \pmod 4$. This finishes the proof. □

Lemma 3.4.7. *Let S be a double polygon ('aligned' or 'offset') with m points on each circle. Then a point $q \notin S$ lies on at most m ordinary generalised circles spanned by S.*

PROOF. Denote the inner circle by σ_1 and the outer circle by σ_2, both with centre o. We proceed by case analysis on the position of q with respect to σ_1 and σ_2. Note that for each point $p \in S$, at most one of the ordinary generalised circles tangent at p can go through q.

If q lies on either σ_1 or σ_2, then q does not lie on any ordinary generalised circle spanned by S.

If q lies inside σ_1, then q lies on at most m ordinary generalised circles spanned by S, since ordinary generalised circles tangent to σ_1 cannot pass through q. Similarly, if q lies outside σ_2, it lies on at most m ordinary generalised circles, since ordinary generalised circles tangent to σ_2 lie inside σ_2.

The remaining case to consider is when q lies in the annulus bounded by σ_1 and σ_2. Consider the subset $S' \subset S$ of points p such that there exists an ordinary generalised circle tangent at p going through q. Consider the four circles passing through q and tangent to both σ_1 and σ_2. They touch σ_1 at a_1, b_1, c_1, d_1 and σ_2 at a_2, b_2, c_2, d_2 as in Figure 6.

Any circle through q tangent to σ_1 and intersecting σ_2 in two points, must touch σ_1 on one of the open arcs a_1b_1 or c_1d_1. Similarly, any circle through q tangent to σ_2 and intersecting σ_1 in two points, must touch σ_2 on one of the open arcs a_2c_2 or b_2d_2. It follows that S' must be contained in the relative interiors of one of these four arcs. Since S consists of m equally spaced points on each of σ_1 and σ_2,

$$|S'| < \left\lceil \frac{2m(\angle a_1ob_1 + \angle c_1od_1 + \angle b_2od_2 + \angle a_2oc_2)}{4\pi} \right\rceil = \left\lceil \frac{m(\theta+\phi)}{\pi} \right\rceil,$$

where θ and ϕ are as indicated in Figure 6. In order to show that $|S'| \leq m$, it suffices to show that the angle sum $\theta + \phi$ is strictly less than π. This is clear from Figure 6 (note that a_1, o, a_2 are collinear with a_1 and a_2 on opposite sides of o). □

3.4.3. Four-point circles.

Theorem 3.4.8 (4-point generalised circles)**.**

(1) *If n is sufficiently large, the maximum number of 4-point generalised circles determined by a set of n points in $\mathbb{R}^2$ is equal to*

$$\begin{cases} \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 2 & \text{if } n \equiv 0 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{11}{24}n - \frac{1}{4} & \text{if } n \equiv 1,3,5,7 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{7}{12}n - \frac{1}{2} & \text{if } n \equiv 2,6 \pmod 8, \\ \frac{1}{24}n^3 - \frac{1}{4}n^2 + \frac{5}{6}n - 1 & \text{if } n \equiv 4 \pmod 8. \end{cases}$$

(2) *Let C be sufficiently large. If a set P of n points in $\mathbb{R}^2$ determines more than $\frac{1}{24}n^3 - \frac{7}{24}n^2 + Cn$ 4-point generalised circles, then up to inversions, P lies on an ellipse or a smooth circular cubic.*

Proof of Theorem 3.4.8. Let P be a set of n points in $\mathbb{R}^2$ with at least $\frac{1}{24}n^3 - \frac{7}{24}n^2 + O(n)$ 4-point generalised circles. Let t_i denote the number of i-point lines ($i \geq 2$) and s_i the number of i-point circles ($i \geq 3$) in P. By counting unordered triples of points, we have

$$\binom{n}{3} = \sum_{i \geq 3} \binom{i}{3}(t_i + s_i) \geq t_3 + s_3 + 4(t_4 + s_4),$$

hence

$$\frac{1}{6}n^3 - O(n^2) \geq t_3 + s_3 + 4\left(\frac{1}{24}n^3 - O(n^2)\right)$$

and $t_3 + s_3 = O(n^2)$, so we can apply Theorem 3.3.3. We next consider each of the cases of that theorem in turn.

If all except $O(1)$ points of P lie on a straight line, it is easy to see that P determines only $O(n^2)$ generalised circles, contrary to assumption.

If all except $O(1)$ are vertices of two regular m-gons on concentric circles where $m = n/2 \pm O(1)$, then we know from Propositions 3.2.3, 3.2.4, and 3.2.5 that P determines at most $\frac{1}{32}n^3 + O(n^2)$ 4-point generalised circles, again contrary to assumption.

Suppose next that $P = ((H \oplus x) \setminus A) \cup B$, where H is a finite subgroup of order $m = n \pm O(1)$ of a smooth circular cubic, A is a subset of $H \oplus x$ with $a = O(1)$ points, and B is a set disjoint from $H \oplus x$ with $b = O(1)$ points. Then $n = m - a + b$. The number of 4-point generalised circles in $H \oplus x$ is $\frac{1}{24}m^3 - \frac{1}{4}m^2 + O(m)$. We next determine an upper bound for the number of 4-point generalised circles in P.

For each $p \in A$, let C_p be the set of 4-point generalised circles of $H \oplus x$ that pass through p. Then $|C_p| = \frac{1}{6}m^2 - O(m)$ and $|C_p \cap C_q| = O(m)$ for distinct $p, q \in A$. By inclusion-exclusion, we destroy at least $|\bigcup_{p\in A} C_p| \geq \frac{1}{6}am^2 - O(m)$ 4-point generalised circles by removing A, and we still have at most $\frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m)$ 4-point generalised circles in $(H \oplus x) \setminus A$.

For each $p \in B$, the number of ordinary generalised circles spanned by $H \oplus x$ passing through p is at most $O(m)$. This is because each such generalised circle is tangent to the cubic at one of the points of $H \oplus x$, and there is only one generalised circle through p and tangent at a given point of $H \oplus x$. Also, for each pair of distinct $p, q \in B$, there are at most $O(m)$ generalised circles through p and q and two points of $H \oplus x$; and for any three $p, q, r \in B$ there are at most $O(1)$ generalised circles through p, q, r and one point of $H \oplus x$. Therefore, again by inclusion-exclusion, by adding B we gain at most $O(m)$ 4-point generalised circles.

It follows that the number of 4-point generalised circles determined by P is

$$t_4 + s_4 \leq \frac{1}{24}m^3 - \frac{1}{4}m^2 - \frac{1}{6}am^2 + O(m) = \frac{n^3 - (a + 3b + 6)n^2 + O(n)}{24}.$$

Since we assumed that

$$t_4 + s_4 \geq \frac{n^3 - 7n^2 + O(n)}{24},$$

we obtain $a + 3b < 1$. Therefore, $a = b = 0$ and $P = H \oplus x$. The maximum number of 4-point circles in a coset has been determined in Propositions 3.2.1 and 3.2.2.

The final case, when all but $O(1)$ points of P lie on an ellipse, can be reduced to the previous case. Indeed, by Lemma 2.2.11, if we invert the ellipse in a point on the ellipse, we obtain an acnodal circular cubic, and then the above analysis holds verbatim for the group of regular points on this cubic.

□

CHAPTER 4

Probabilities of incidence between lines and a plane curve

The results of this Chapter is based on a collaboration with Matteo Gallet and Josef Schicho [**MSG18**].

In this chapter, we consider an algebraic plane curve C of degree d over a finite field $\mathbb{F}_q$ with q elements, where q is a prime power, namely the set of points in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$ that are zeros of a homogeneous trivariate polynomial of degree d. Given such a curve, we can define the probability for a line in $\mathbb{P}^2(\mathbb{F}_q)$ to intersect it in exactly k points. Notice that here we consider the mere set-theoretic intersection: no multiplicities are taken into account. We can then consider the same kind of probability, keeping the same curve C — namely, the same trivariate polynomial — but changing the base field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and so on. In this way, for every $N \in \mathbb{N}$ we define the numbers $p_k^N(C)$, namely the probability for a line in $\mathbb{P}^2(\mathbb{F}_{q^N})$ to intersect C in exactly k points. If the limit as N goes to infinity of the sequence $\left(p_k^N(C)\right)_{N\in\mathbb{N}}$ exists, we denote this number by $p_k(C)$. The main tool we use to compute these numbers when the curve C is absolutely irreducible (see Definition 2.1.33) and with *simple tangency* is an effective version of the *Chebotarev theorem* (see Chapter 5) for function fields. By asking that the curve has *simple tangency* we require that there exists a line whose intersection with C consists of simple intersections except for one, which is a double intersection. Namely in this section we will prove

Theorem 4.0.1. *Let C be an absolutely irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Then the numbers $\{p_k(C)\}$ are well-defined, namely the corresponding limits exist.*

Theorem 4.0.2. *Let C be an absolutely irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \dots, d\}$ we have*

$$p_k(C) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

In particular, $p_{d-1}(C) = 0$ and $p_d(C) = 1/d!$.

Finally, the concept of simple tangency (see 2.1.19) is applicable to curves in arbitrary projective space: an absolutely irreducible curve C in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ for $n \in \mathbb{N}$ has simple tangency if there exists a hyperplane $H \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ intersecting C in $d-1$ smooth points of C such that H intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point. Also the concepts of Galois group of a curve and probabilities of intersections generalize similarly by considering hyperplanes instead of lines. By applying a *Veronese map* and using Chebotarev Theorem we derive the following proposition:

Proposition 4.0.3. *Let C be an absolutely irreducible algebraic curve of degree d in $\mathbb{P}^2$ over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Let $e \in \mathbb{N}$ be a natural number. Then for every $k \in \{0, \dots, de\}$ we have*

$$p_k(C, e) = \sum_{s=k}^{de} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

First let we make more precise the definition of the probabilities of intersection between a random line and a given curve in the projective plane over a finite field (Definition 4.0.4). We then prove the Theorems 4.0.1 and 4.0.2, by showing that its counterpart for morphisms hold (Theorems 4.0.8 and 4.0.10). We will re-prove these results in Section 5.1.1 by using Chebotarev density theorem.

Definition 4.0.4 (Probabilities of intersection)**.** Let q be a prime power and let $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve of degree d defined over $\mathbb{F}_q$. For every $N \in \mathbb{N}$ and for every $k \in \{0, \dots, d\}$, the *k-th probability of intersection* $p_k^N(C)$ of lines with C over $\mathbb{F}_{q^N}$ is

$$p_k^N(C) := \frac{\left|\left\{\text{lines } \ell \subseteq \mathbb{P}^2(\mathbb{F}_{q^N}) \,:\, |\ell(\mathbb{F}_{q^N}) \cap C(\mathbb{F}_{q^N})| = k\right\}\right|}{q^{2N} + q^N + 1}.$$

Notice that $q^{2N} + q^N + 1$ is the number of lines in $\mathbb{P}^2(\mathbb{F}_{q^N})$.

The aim of this chapter is to prove that the limit as N goes to infinity of the quantities $p_k^N(C)$ exists for every k, and to give a formula for these limits, provided that some conditions on the curve C are fulfilled.

The following result is a direct consequence of Definitions 4.0.4 and 2.1.16.

Lemma 4.0.5. *Let $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve of degree d defined over $\mathbb{F}_q$. For every $k \in \{0, \dots, d\}$ we have*

$$p_k^N(C) = \frac{\left|\left\{[\ell] \in \check{\mathbb{P}}^2(\mathbb{F}_{q^N}) \,:\, |\pi^{-1}([\ell])(\mathbb{F}_{q^N})| = k\right\}\right|}{q^{2N} + q^N + 1}.$$

Via Lemma 4.0.6 and Definition 4.0.7 we reduce the problem of computing intersection probabilities for curves to the analogous problem for morphisms.

Lemma 4.0.6. *Let $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve of degree d defined over $\mathbb{F}_q$. Let $\mathcal{V}_C \subseteq \check{\mathbb{P}}^2(\overline{\mathbb{F}}_q)$ be as in Definition 2.1.29. For every $N \in \mathbb{N}$ and for every $k \in \{0, \dots, d\}$, define*

$$\tilde{p}_k^N(C) := \frac{\left|\left\{[\ell] \in \mathcal{V}_C(\mathbb{F}_{q^N}) \,:\, |\pi^{-1}([\ell])(\mathbb{F}_{q^N})| = k\right\}\right|}{|\mathcal{V}_C(\mathbb{F}_{q^N})|}.$$

Then $\lim_{N\to\infty} p_k^N(C)$ exists if and only if $\lim_{N\to\infty} \tilde{p}_k^N(C)$ exists, in which case the two numbers coincide.

Proof. It is enough to show that the probability for a point to lie in $\mathbb{P}^2(\mathbb{F}_{q^N}) \setminus \mathcal{V}_C(\mathbb{F}_{q^N})$ goes to zero as N goes to infinity. This is a consequence of the Lang-Weil bound (Theorem 2.1.35). In fact, since $\mathbb{P}^2(\mathbb{F}_{q^N}) \setminus \mathcal{V}_C(\mathbb{F}_{q^N})$ has dimension at most 1:

$$\frac{\left|\mathbb{P}^2(\mathbb{F}_{q^N}) \setminus \mathcal{V}_C(\mathbb{F}_{q^N})\right|}{q^{2N} + q^N + 1} \sim \frac{a\, q^N}{q^{2N}} \to 0,$$

where the constant a is the number of irreducible components of $\mathbb{P}^2(\overline{\mathbb{F}}_q) \setminus \mathcal{V}_C(\overline{\mathbb{F}}_q)$. □

Definition 4.0.7. Let $f\colon X \longrightarrow Y$ be a morphism of degree d defined over $\mathbb{F}_q$, where q is a prime power, satisfying $(*)$. For every $N \in \mathbb{N}$ and for every $k \in \{0,\dots,d\}$, we define the *k-th preimage probability* $p_k^N(f)$ to be

$$p_k^N(f) := \frac{\left|\left\{y \in Y(\mathbb{F}_{q^N}) \,:\, |f^{-1}(y)(\mathbb{F}_{q^N})| = k\right\}\right|}{|Y(\mathbb{F}_{q^N})|}\,.$$

Notice that if C is an absolutely irreducible algebraic plane curve of degree d, then for every $N \in \mathbb{N}$ and for every $k \in \{0,\dots,d\}$ we have $\tilde{p}_k^N(C) = p_k^N\big(\pi_{|_{\mathcal{U}_C}}\big)$. Hence, by Lemma 4.0.6, in order to show the existence of the limits of k-th probabilities of intersections for a curve, it is enough to show the existence of k-th preimage probabilities for morphisms over $\mathbb{F}_q$ satisfying $(*)$.

Theorem 4.0.8. *Let $f\colon X \longrightarrow Y$ be a morphism of degree d defined over $\mathbb{F}_q$, where q is a prime power, satisfying $(*)$. Then for every $k \in \{0,\dots,d\}$ the limit as N goes to infinity of the sequence $\big(p_k^N(f)\big)_{N\in\mathbb{N}}$ exists.*

Proof. We generalize the construction of the Galois scheme of the morphism f. For every $k \in \{0,\dots,d\}$, define

$$G_k(f) := \big\{(x_1,\dots,x_k) \in X^k \,:\, f(x_1) = \dots = f(x_k),\ x_i \neq x_j \text{ for all } i \neq j\big\}.$$

In particular $G_d(f) = \mathrm{GS}(f)$. As we showed for the Galois scheme, see Equation (12), for every k the variety $G_k(f)$ has the same dimension of X and Y. There is a natural finite morphism $F_k\colon G_k(f) \longrightarrow Y$, the fiber product of f with itself k times. This map has degree $d(d-1)\cdots(d-k+1)$. The main idea of the proof is to compute, in two different ways, the expected cardinality $\mu_k^N(f)$ of a fiber $F_k^{-1}(y)$ over $\mathbb{F}_{q^N}$, where y is a random element in Y. On one hand,

$$\mu_k^N(f) = \frac{\big|G_k(f)(\mathbb{F}_{q^N})\big|}{\big|Y(\mathbb{F}_{q^N})\big|}\,.$$

On the other hand, we can express $\mu_k^N(f)$ in terms of the preimage probabilities:

$$\mu_k^N(f) = \sum_{s=k}^{d} s(s-1)\cdots(s-k+1)\, p_s^N(f)\,. \tag{19}$$

In matrix form:

$$\begin{pmatrix} \mu_0^N(f) \\ \vdots \\ \mu_d^N(f) \end{pmatrix} = \begin{pmatrix} 1 & * & \cdots & & \cdots & * \\ 0 & 1 & * & & & \vdots \\ \vdots & & \ddots & & & \vdots \\ 0 & \cdots & 0 & k! & * & * \\ \vdots & & & & \ddots & \vdots \\ 0 & \cdots & & & \cdots & d! \end{pmatrix} \begin{pmatrix} p_0^N(f) \\ \vdots \\ p_d^N(f) \end{pmatrix}. \tag{20}$$

Since the matrix in Equation (20) has non-zero determinant, we can write

$$p_k^N(f) = \sum_{s=0}^{d} \alpha_{k,s}\, \mu_s^N \tag{21}$$

for some numbers $(\alpha_{k,s})_{k,s}$. Using the Lang-Weil bound on Equation (19), we have

$$\mu_k^N \;\sim\; \frac{\delta_k\, q^{N\cdot\dim G_k(f)}}{q^{N\cdot\dim Y}} \qquad \text{as } N \to \infty\,, \tag{22}$$

where δ_k is the number of irreducible components of $G_k(f)(\overline{\mathbb{F}}_q)$. Since $\dim G_k(f) = \dim Y$, we conclude that the limit in Equation (22) exists, and so by Equation (21) also $\lim_{N\to\infty} p_k^N(f)$ exists. □

Corollary 4.0.9. *Theorem 4.0.1 holds. In fact, the map $\pi_{|_{\mathcal{U}_C}}$ satisfies the hypotheses of Theorem 4.0.8, so the numbers $p_k(\pi_{|_{\mathcal{U}_C}})$ exist, and we have already proved that this implies that the limits $p_k(C)$ exist.*

Theorem 4.0.10. *Let $f\colon X \longrightarrow Y$ be a morphism of degree d defined over $\mathbb{F}_q$, where q is a prime power, satisfying (∗). Suppose that $\mathrm{Gal}_g(f) \cong \mathrm{Gal}_a(f)$ is the full symmetric group S_d. Then for every $k \in \{0,\dots,d\}$ we have*

$$p_k(f) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

In particular, $p_{d-1}(f) = 0$ and $p_d(f) = 1/d!$.

Proof. Since $\mathrm{Gal}_g(f)$ is the full symmetric group, the Galois scheme $\mathrm{GS}(f)$ is absolutely irreducible. Hence, using the notation of the proof of Theorem 4.0.8, for all $k \in \{0,\dots,d\}$ we have

$$\lim_{N\to\infty} \mu_k^N(f) = \lim_{N\to\infty} \frac{q^{N\cdot\dim G_k(f)}}{q^{N\cdot\dim Y}} = 1. \tag{23}$$

In fact, every variety $G_k(f)$ is an image (under a projection) of $\mathrm{GS}(f) = G_d(f)$, thus is absolutely irreducible and so Equation (23) follows from Equation (22). Again using the notation as in Theorem 4.0.8, we get

$$\lim_{N\to\infty} p_k^N(f) = \sum_{s=0}^{d} \alpha_{k,s}. \tag{24}$$

Therefore, the statement is proved once we are able to explicitly compute the coefficients $(\alpha_{k,s})_{k,s}$. Recall that $\alpha_{k,s}$ is the (k,s)-entry of the inverse of the matrix M_d appearing in Equation (20). A direct inspection of the matrices M_d shows that they admit the following structure:

$$M_d = \left(\begin{array}{ccc|c} & & & 1 \\ & M_{d-1} & & \vdots \\ & & & d!/1! \\ \hline 0 & \cdots & 0 & d!/0! \end{array}\right).$$

A direct computation shows that

$$M_d^{-1} = \left(\begin{array}{ccc|c} & & & \frac{(-1)^d}{d!}\cdot\binom{d}{0} \\ & M_{d-1}^{-1} & & \vdots \\ & & & \frac{(-1)}{d!}\cdot\binom{d}{d-1} \\ \hline 0 & \cdots & 0 & \frac{1}{d!}\cdot\binom{d}{d} \end{array}\right).$$

Hence

$$\alpha_{k,s} = \frac{(-1)^{k+s}}{s!}\binom{s}{k} \quad \text{for all } k,s \in \{0,\dots,d\}.$$

It follows from Equation (24) that for all $k \in \{0,\dots,d\}$,

$$p_k(f) = \sum_{s=0}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k} = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}$$

and so the statement is proved. □

As a consequence of Proposition 2.1.22 and Theorem 4.0.10, we obtain:

Corollary 4.0.11. *Theorem 4.0.2 holds.*

As we pointed out in the Introduction, one of the consequences of Theorem 4.0.2 is that a question raised by Erdös concerning 4- and 5-rich lines has a positive answer over finite fields.

Corollary 4.0.12. *Let C be an absolutely irreducible plane algebraic curve of degree 4 in the plane $\mathbb{P}^2(\mathbb{F}_q)$. By Theorem 2.1.35, the curve C has $cq+O(\sqrt{q})$ elements for some $c > 0$, and by Theorem 4.0.2 it has ϵq^2 4-rich lines for some $\epsilon > 0$, after possibly taking a finite extension of the base field, since $p_4(C) > 0$. Hence, if we take P as the set of points of C, then P spans a quadratic number of 4-rich lines, but no five points of P are collinear.*

CHAPTER 5

Probabilities of intersection via Chebotarev theorem

The results of this Chapter is based on a collaboration with Matteo Gallet and Josef Schicho [**MSG18**].

In this Chapter, we show how to use an effective version of Chebotarev density theorem for function fields as exposed in [**ABSR15a**, Appendix A], and used in [**BSJ12**] and [**Die12**] to prove the results reported in the Introduction, to prove Theorems 4.0.1 and 4.0.2. We recall the setting of the paper and specialize Chebotarev theorem to our case; we refer to the cited appendix for the proofs of the claims we make in this section regarding the objects introduced to state Chebotarev theorem.

In this Chapter we first explain Chebotarev Theorem 5.1.2 in the first section, then we will see how Theorems 4.0.1 and 4.0.2 are derived by Chebotarev Theorem.

5.1. Chebotarev Theorem

5.1.1. Frobenius elements. Let $\mathbb{F}_q$ be a finite field with q elements, where q ia a prim power and algebraic closure $\mathbb{F}$. We denote $\mathrm{Fr_q}$ the *Frobenius* automorphism $x \mapsto x^q$.

Let R be an integrally closed finitely generated $\mathbb{F}_q$-algebra with fraction field K, and let $\mathcal{F} \in R[T]$ be a monic separable polynomial of degree m such that the discriminant of $\mathcal{F}$ is a invertible in R^*. Suppose that $\{y_1, \dots, y_m\}$ are the roots of $\mathcal{F}$ and put

$$S = R[y_1, \dots, y_m], \quad L = K[y_1, \dots, y_m] \quad \text{and} \quad G = \mathrm{Gal}(\frac{L}{K}).$$

We can identify the Galois group G with a subgroup of S_m via the natural action on indices $y_1, \dots y_m$:

$$g(y_i) = y_{g(i)}, \quad g \in G \geq S_m.$$

Since the discriminant of $\mathcal{F}$ is invertible in R and Cramer rule, S is the integral closure of R in L and S/R is unramified. In particular, the relative algebraic closure (the relative algebraic closure of A in B is the set of all elements of B which satisfy an algebraic equation with coefficient in A) $\mathbb{F}_{q^\nu}$ of $\mathbb{F}_q$ in L is contained in S.

For each $\nu \geq 0$ we let

$$G_\nu = \left\{ g \in G : g(x) = x^{q^\nu}, \forall x \in \mathbb{F}_{q^\nu} \right\},$$

the preimage of $\mathrm{Fr}_{\mathrm{q}}^{\nu}$ in G under the restriction map. Since $\mathrm{Gal}(\mathbb{F}_{q^\nu}/\mathbb{F}_q)$ is commutative, G_ν is stable under conjugation. This is known that G_ν are the cosets of G_0 for each $\nu \geq 1$.

Definition 5.1.1. For every $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ with $\phi(R) = \mathbb{F}_{q^\nu}$ there exists a unique element in G, which we call the *Frobenius element* and denote by

$$\left[\frac{S/R}{\Phi}\right] \in G,$$

such that

$$\phi\left(\left[\frac{S/R}{\Phi}\right] x\right) = \phi(x)^{q^\nu}, \quad \forall x \in S. \tag{25}$$

In the diagram language the Frobenius element means that the following diagram is commutative:

$$\begin{array}{ccc} S & \xrightarrow{\left[\frac{S/R}{\Phi}\right]} & S \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ \mathbb{F} & \xrightarrow{\alpha \mapsto \alpha^{q^\nu}} & \mathbb{F} \end{array} \tag{26}$$

Since S is generated by $\{y_1, \ldots, y_m\}$ over R, it suffices to consider $x \in \{y_1, \ldots y_m\}$ in Equation 25. If we further assume that $\phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$, then Equation 25 gives that $[S/R/\phi]x = x^{q^{nu}}$ for all $x \in \mathbb{F}_{q^\nu}$, hence

$$\phi(R) = \mathbb{F}_{q^\nu} \Longrightarrow \left[\frac{S/R}{\Phi}\right] \in G_\nu. \tag{27}$$

For $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$, we set

$$\left(\frac{S/R}{\varphi}\right) := \left\{ \left[\frac{S/R}{\Phi}\right] \,:\, \Phi \in \mathrm{Hom}_{\mathbb{F}_q^\nu}(S, \mathbb{F})\ \Phi \text{ prolongs } \varphi \right\}.$$

Let $Z \subseteq G$ be an orbit, i.e $Z = C_g = \{hgh^{-1} \colon\ h \in G_o\}$, $g \in G_\nu$. Then $Z \subseteq G_\nu$, since the latter is stable under conjugation. The explicit *Chebotarev theorem* gives the asympotic probability that $((S/R/\phi)) = Z$:

$$P_{\nu,Z} := \frac{\left|\left\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\varphi}\right) = Z\right\}\right|}{\left|\left\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu}\right\}\right|}.$$

Now we are ready to state Chebotarev theorem (see [**ABSR15a**, Theorem A.4]).

Theorem 5.1.2 (Chebotarev Theorem)**.** *Let $Z \subseteq G$ be a conjugacy class and let $\nu \geq 1$. Then there exists a constant δ independent of q such that*

$$P_{\nu,Z} = \frac{|Z|}{|G|} + \frac{\delta}{\sqrt{q}}.$$

Now we give another prove for our results in the Section 4, by using the Chebotarev Theorem 5.1.2. For doing this we should first translate every things to the language of Chebotarev Theorem.

We start by considering an integrally closed finitely generated $\mathbb{F}_q$-algebra R and a monic polynomial $\mathcal{F} \in R[T]$ such that the discriminant of $\mathcal{F}$ is invertible in R. In our case, we take R to be the $\mathbb{F}_q$-algebra

$$R := \frac{\mathbb{F}_q[a, b, u]}{\mathrm{Disc}_x\big(F(x, ax + b)\big) \cdot u - 1} \cong \mathbb{F}_q[a, b]_{(f)} \quad \text{with } f := \mathrm{Disc}_x\big(F(x, ax + b)\big),$$

where the last ring is the localization of the polynomial ring $\mathbb{F}_q[a, b]$ at the element f. In geometric terms, R is the coordinate ring of the open subset of the dual projective plane parametrizing lines in the plane that intersect the curve $\{F = 0\}$ in d distinct

points over the algebraic closure of $\mathbb{F}_q$. We then take the polynomial $\mathcal{F}$ to be $F(T, aT + b)$. Then by construction, its discriminant is invertible in R.

Starting from R and $\mathcal{F}$, we consider K, the quotient field of R, and we define L to be the splitting field of $\mathcal{F}$ over K. In other words, if $\{y_1, \dots, y_d\}$ are the roots of $\mathcal{F}$, we set $L := K(y_1, \dots, y_d)$. In our situation, we have

$$L = \frac{K[t_1, \dots, t_d]}{\big(F(t_i, at_i + b) \text{ for } i \in \{1, \dots, d\}\big)}\,.$$

Then we define S to be the integral closure of R in L, namely $S = R[y_1, \dots, y_d]$. Geometrically, S is the coordinate ring of an open subset of the variety

$$X_d := \big\{(x_1, \dots, x_d, [\ell]) \in C^d \times \check{\mathbb{P}}^2 : \, x_i \in \ell\big\}\,.$$

The strategy we adopt to compute probabilities of intersections is the following: our goal is to count the number of lines ℓ in $\mathbb{P}^2$ such that the intersection $\ell \cap C$ is constituted of exactly k points over $\mathbb{F}_{q^N}$, and we interpret this as the number of lines such that the univariate polynomial $F_{|\ell}$ has exactly k linear factors over $\mathbb{F}_{q^N}$. Notice that every univariate polynomial H of degree d over $\mathbb{F}_q^N$ determines a partition π_H of d, namely a tuple $\pi_H = (\alpha_1, \dots, \alpha_s)$ such that $\alpha_1 + \cdots + \alpha_s = d$ and $\alpha_1 \leq \cdots \leq \alpha_s$. Such partition is obtained by factoring H over $\mathbb{F}_{q^N}$ into irreducible factors $H_1, \dots, H_s$ and then setting $\alpha_i = \deg(H_i)$. Then, the number of lines we are interested in can be computed as the sum, over the set of partitions π of d with exactly k ones, of the number of lines ℓ such that the partition associated to $F_{|\ell}$ is π. Chebotarev theorem provides a formula for the probability for a line to determine a given partition.

We set G to be the Galois group of the field extension $K \subseteq L$. By definition, this coincides with the Galois group of the curve C as in Definition 2.1.18. Notice that, in our situation, the intersection $L \cap \mathbb{F}$, where $\mathbb{F}$ is an algebraic closure of $\mathbb{F}_q$, coincides with $\mathbb{F}_q$. This implies that the subgroup

$$G_0 := \big\{g \in G : \, g_{|\mathbb{F}_q}(x) = x \text{ for all } x \in \mathbb{F}_q\big\}$$

coincides with G. Similarly, if for every $\nu \geq 1$ we set

$$G_\nu := \big\{g \in G : \, g_{|\mathbb{F}_q}(x) = x^{q^\nu} \text{ for all } x \in \mathbb{F}_q\big\}\,,$$

then G_ν, which in general is a coset of G_0 in G, coincides with G.

As one can see from the definition of X_d, its points are intimately related to the probabilities we are interested in. From an algebraic point of view (see [**Mum99**, Section II.6]) these points correspond to $\mathbb{F}_q$-homomorphisms from S to $\mathbb{F}$. Moreover, a homomorphism $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ such that $\Phi(R) = \mathbb{F}_{q^\nu}$ corresponds to a point $(x_1, \dots, x_d, [\ell])$ in X_d such that the line ℓ is defined over $\mathbb{F}_{q^\nu}$. Given such a homomorphism Φ by Definition 5.1.1 there always exists an element in G denoted by $\left[\frac{S/R}{\Phi}\right]$, that

$$\begin{array}{ccc} S & \xrightarrow{\left[\frac{S/R}{\Phi}\right]} & S \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ \mathbb{F} & \xrightarrow{\alpha \mapsto \alpha^{q^\nu}} & \mathbb{F} \end{array}$$

In other words, we have the relation

$$\Phi\left(\left[\frac{S/R}{\Phi}\right] x\right) = \Phi(x)^{q^\nu}\,.$$

One then can show that $\left[\frac{S/R}{\Phi}\right] \in G_\nu$. If we fix a line in $\mathbb{P}^2$, namely, if we fix an $\mathbb{F}_q$-homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$, we can consider all points in X_d "lying over" this line. In other terms, we can consider all homomorphisms $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ prolonging φ. Their corresponding Frobenius elements form one key object in the statement of the Chebotarev theorem. For $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$, we set

$$\left(\frac{S/R}{\varphi}\right) := \left\{ \left[\frac{S/R}{\Phi}\right] \,:\, \Phi \text{ prolongs } \varphi \right\}.$$

In our setting, since $G_0 = G$ one can show that $\left(\frac{S/R}{\varphi}\right)$ is a conjugacy class in G.

Now we are in the situation of the Chebotarev Theorem 5.1.2, namely, let $Z \subseteq G$ be a conjugacy class and let $\nu \geq 1$; define

$$P_{\nu,Z} := \frac{\left|\left\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\varphi}\right) = Z\right\}\right|}{\left|\left\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu}\right\}\right|}.$$

Then there exists a constant δ independent of q such that

$$P_{\nu,Z} = \frac{|Z|}{|G|} + \frac{\delta}{\sqrt{q}}.$$

In order to use Chebotarev theorem for our purposes, we have to understand what does the condition $\left(\frac{S/R}{\varphi}\right) = Z$ correspond to in our setting. Suppose that C has simple tangency. then we know by Proposition 2.1.22 that G is the symmetric group S_d. Notice that to every conjugacy class Z of S_d we can associate a partition π_Z of d, obtained from the cycle structure of permutations belonging to Z. On the other hand, given a line $\ell = \{y = ax + b\}$, we can consider the restriction of the equation F of C to ℓ, namely the univariate polynomial $F_\ell = F(x, ax + b)$. This polynomial defines a partition π_ℓ of d by considering its factorization over $\mathbb{F}_{q^\nu}$: the partition π_ℓ has as many 1 as the linear factors of F_ℓ, as many 2 as the quadratic factors of F_ℓ, and so on.

Lemma 5.1.3. *If $Z \subseteq S_d$ is a conjugacy class of permutations, then the set*

$$I_{\nu,Z} := \left\{\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\varphi}\right) = Z\right\}$$

corresponds to the set of lines in $\mathbb{P}^2$ defined over $\mathbb{F}_{q^\nu}$ such that $\pi_\ell = \pi_Z$.

Proof. Let $\varphi \in I_{\nu,Z}$ and let $\Phi \in \mathrm{Hom}(S, \mathbb{F})$ be a homomorphism prolonging φ. Let $\ell = \{y = \bar{a}x + \bar{b}\}$ be the line in $\mathbb{P}^2_{\mathbb{F}_{q^\nu}}$ corresponding to φ. Then from the explicit description of K and L we provided at the beginning of the section, it follows that $M := \Phi(S)$ is a splitting field of the polynomial $F_\ell = F(x, \bar{a}x + \bar{b})$. By definition of the Frobenius element, we have the commutative diagram

$$\begin{array}{ccc} L = \frac{K[t_1,\dots,t_d]}{\left(F(t_i, at_i+b) \text{ for } i\in\{1,\dots,d\}\right)} & \xrightarrow{\left[\frac{S/R}{\Phi}\right]} & L = \frac{K[t_1,\dots,t_d]}{\left(F(t_i, at_i+b) \text{ for } i\in\{1,\dots,d\}\right)} \\ \downarrow & & \downarrow \\ M = \frac{K[u_1,\dots,u_d]}{\left(F(u_i, \bar{a}u_i+\bar{b}) \text{ for } i\in\{1,\dots,d\}\right)} & \xrightarrow{\alpha\mapsto\alpha^{q^\nu}} & M = \frac{K[u_1,\dots,u_d]}{\left(F(u_i, \bar{a}u_i+\bar{b}) \text{ for } i\in\{1,\dots,d\}\right)} \end{array}$$

which is just the extension to L of the diagram in Equation (26). From the commutativity of this diagram, we see that the permutation action of $\left[\frac{S/R}{\Phi}\right]$ on the classes $[t_1], \dots, [t_d]$ is the same as the action of the map $\alpha \mapsto \alpha^{q^\nu}$ on the classes

$[u_1], \dots, [u_d]$. Since the $\{[u_i]\}$ are the roots of $F(x, \bar{a}x + \bar{b})$, and the latter is a polynomial with coefficients in $\mathbb{F}_{q^\nu}$, which are hence preserved by the map $\alpha \mapsto \alpha^{q^\nu}$, it follows that the structure of factors of F_ℓ over $\mathbb{F}_{q^{nu}}$ is the same as the cycle structure of $\left[\frac{S/R}{\Phi}\right]$. This concludes the proof. □

As a corollary, we obtain that the set of lines in $\mathbb{P}^2$ over $\mathbb{F}_{q^\nu}$ intersecting C in exactly k points corresponds to the set

$$\bigcup_{Z \text{ has exactly } k \text{ fixed points}} I_{\nu,Z}\,.$$

The cardinality of this set is given by the so-called *rencontres numbers*, see [**Rio02**]. We have hence:

$$\left|\bigcup_{Z \text{ has exactly } k \text{ fixed points}} I_{\nu,Z}\right| = d! \sum_s = k^d \frac{(-1)^{k+s}}{s!}\binom{s}{k}\,.$$

Using Chebotarev theorem we then conclude the proof of Theorem 4.0.2.

As the reader can see, there is nothing particularly special in considering the setting of plane curves. In fact, the concept of simple tangency (see 2.1.19) is applicable to curves in arbitrary projective space: an absolutely irreducible curve C in $\mathbb{P}^n(\overline{\mathbb{F}}_q)$ for $n \in \mathbb{N}$ has simple tangency if there exists a hyperplane $H \subseteq \mathbb{P}^n(\overline{\mathbb{F}}_q)$ intersecting C in $d-1$ smooth points of C such that H intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point. Also the concepts of Galois group of a curve and probabilities of intersections generalize similarly by considering hyperplanes instead of lines.

The generalized statement for the situation of irreducible curves is the Proposition 5.1.4 and we rewrite this in here:

Proposition 5.1.4. *Let C be an absolutely irreducible algebraic curve of degree d in $\mathbb{P}^n$, $n \in \mathbb{N}$, over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \dots, d\}$ we have*

$$p_k(C) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

In particular, $p_{d-1}(C) = 0$ and $p_d(C) = 1/d!$.

Using Proposition 5.1.4, we can compute the probabilities of intersection of a given plane curve C with a random plane curve E of degree e. In fact, via the *Veronese map* we can reduce this situation to the one of Proposition 5.1.4. Let us start by defining the probabilities of intersection of a given curve C with a random curve E in the plane in exactly k points, for $k \in \{0, \dots, de\}$:

$$p_k^N(C, e) := \frac{\left|\left\{\text{curves } E \subseteq \mathbb{P}^2(\mathbb{F}_{q^N}) \text{ of degree } e \,:\, |E(\mathbb{F}_{q^N}) \cap C(\mathbb{F}_{q^N})| = k\right\}\right|}{q^{\binom{e+2}{2}N} + \dots + q^{2N} + q^N + 1},$$

$$p_k(C, e) := \lim_{N \to \infty} p_k^N(C, e) \quad \text{when the limit exists}\,.$$

Recall now that for every $r \in \mathbb{N}$, the Veronese map of degree e is an algebraic morphism embedding $\mathbb{P}^r$ into a larger projective space, so that hypersurfaces of degree e get mapped to hyperplane sections of the image of the map. In this sense,

the Veronese map operates a sort of "linearization" of the problem. In the case of $\mathbb{P}^2$, which is the one that interests us, it is given by

$$\begin{array}{rccc} v_e\colon & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^{\binom{e+2}{2}-1} \\ & (x:y:z) & \mapsto & \left(\{x^a y^b z^c\}_{a+b+c=e}\right) \end{array}.$$

The following lemma ensures that if we start from a plane curve that has simple tangency and we apply the Veronese map, we obtain a curve that has simple tangency.

Lemma 5.1.5. *Let C be a plane curve of degree d with simple tangency and let $e \in \mathbb{N}$. Then the image $\tilde{C} = v_e(C)$ of C under the Veronese map of degree e has also simple tangency.*

PROOF. Let ℓ_1 be a line witnessing simple tangency for C. Select lines $\ell_2, \dots, \ell_e$ in $\mathbb{P}^2$ such that each of them intersects C in d distinct points and $\ell_i \cap \ell_j \cap C$ is empty for all $i \neq j$. Define E as the zero set of the product $\ell_1 \cdots \ell_e$. The Veronese map sends E to a hyperplane section of the Veronese surface; let $\tilde{H}$ be the corresponding hyperplane. Then, by construction, $\tilde{H}$ witnesses simple tangency for $\tilde{C}$. □

Since the Veronese map of degree e defines a bijection between plane curves of degree e and hyperplanes in $\mathbb{P}^{\binom{e+2}{2}-1}$, determining the probabilities $p_k(C, e)$ of intersection of a given plane absolutely irreducible curve C with a random curve of degree e in k points is equivalent to compute the corresponding probabilities of intersection of the image $\tilde{C}$ of C under the Veronese map with hyperplanes. We sum up what we obtained in the following:

CHAPTER 6

An application of Bertini Theorem

The results of this Chapter is based on a collaboration with Josef Schicho [**MS18**].

Given an irreducible variety X over a finite field, the density of hypersurfaces of degree d of intersecting X in an irreducible subvariety tends to 1, when d goes to infinity, by a result of Charles and Poonen. In this note, we analyse the situation fixing $d = 1$ and instead extending the base field. We use this result to compute the probability that a random linear subspace of the right dimension intersects X in a given number of points.

6.1. Introduction

Throughout this paper, when we write $J_m = G(n-m, n)$ we mean the variety of all linear subspaces of codimension m in the projective space $\mathbb{P}^n$, the so-called *Grassmannian*.

A *Chow variety* is a variety whose points correspond to all cycles of a given projective space of given dimension and degree.

The classical Bertini theorems over an infinite field K assert that if a subscheme $X \subset \mathbb{P}^n(K)$ has a certain property (smooth, geometrically irreducible), then for almost all hyperplanes Γ, the intersection $X \cap \Gamma$ has this property too.

It has been shown that if K is a finite field, then the Bertini Theorem about irreducibility can fail, see [**CP16**, Theorem 1.10]. In [**CP16**], the authors considered the density of hypersurfaces (of sufficiently high degree) that intersect a given geometrically irreducible variety in an irreducible subvariety. More precisely: Let $\mathbb{F}_q$ be a finite field of q elements let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Let $S = \mathbb{F}_q[x_0, \ldots, x_n]$ be the homogeneous coordinate ring of $\mathbb{P}^n(\mathbb{F}_q)$, let $S_d \subset S$ be the $\mathbb{F}_q$-subspace of homogeneous polynomials of degree d. For $f \in S_d$, let H_f be the hypersurface defined by $f = 0$. Define the *density* of $\mathcal{P} \subset S_{homog} = \cup_{d=0}^{\infty} S_d$ by

$$\mu(\mathcal{P}) := \lim_{d\to\infty} \frac{|\mathcal{P} \cap S_d|}{|S_d|}.$$

Theorem 6.1.1 (Charles–Poonen)**.** *Let X be a geometric irreducible subscheme of $\mathbb{P}^n(\mathbb{F}_q)$. If $\dim X \geq 2$, then the density of*

$$\{f \in S_{homog} : H_f \cap X \text{ is geometrically irreducible}\}$$

is 1.

Poonen in [**Poo04**] proved a similar result for smoothness.

Theorem 6.1.2 (Poonen)**.** *Let X be a smooth quasiprojective subscheme of $\mathbb{P}^n$ of dimension $m \geq 0$ over $\mathbb{F}_q$. Then there exists a homogeneous polynomial f over $\mathbb{F}_q$ for which the intersection of X and the hypersurface H_f is smooth. In fact, the set of such f has a positive density, equal to $\zeta(m+1)^{-1}$, where ζ is the zeta function.*

Recently, an analogue of this problem for plane curves was investigated in [**Asg18**]. In this paper, we consider an algebraic variety $X \subset \mathbb{P}^n(\mathbb{F}_q)$ of degree d and dimension m over a finite field $\mathbb{F}_q$ with q elements, where q is a prime power. Given such a variety, we can define the probability for a codimension m linear subspace in $\mathbb{P}^n(\mathbb{F}_q)$ to intersect it in exactly k points. Notice that here we consider the mere set-theoretic intersection: no multiplicities are taken into account. We can then consider the same kind of probability, keeping the same variety X, but changing the base field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and so on. In this way, for every $N \in \mathbb{N}$ we define the numbers $p_k^N(X)$, namely the probability for a codimension m linear subspace in $\mathbb{P}^n(\mathbb{F}_{q^N})$ to intersects X in exactly k points. If the limit as N goes to infinity of the sequence $\left(p_k^N(X)\right)_{N\in\mathbb{N}}$ exists, we denote this number by $p_k(X)$. We will compute the exact values $p_k(X)$ for each $k = 0, 1, \dots d$, provided that X satisfies some geometrically properties.

The first our result remains of a similar one by Charles-Poonen. In that case, however, one considers the behaviour of the density as the degree gets larger and larger; here, instead, we fix degree and we extend the base field.

Theorem 6.1.3. *Let X be a geometrically irreducible variety of dimension m in $\mathbb{P}^n$. Then*

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \text{ is geometrically irreducible}\right\}\right|}{\left|\mathbb{P}^*(\mathbb{F}_{q^N})\right|} = 1.$$

We also consider a generalization of the following theorem proved in [**MSG18**].

Theorem 6.1.4. *Let C be an geometrically irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \dots, d\}$ we have*

$$p_k(C) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

In particular, $p_{d-1}(C) = 0$ and $p_d(C) = 1/d!$.

Theorem 6.1.5. *Let X be a geometrically irreducible variety of dimension m and degree d in projective space $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has simple tangency property. Then for every $k \in \{0, \dots d\}$ we have*

$$p_k(X) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

First we use Bertini Theorem and Lang-Weil Theorem [**LW54**, Theorem 1] to show that for a general hyperplane Γ the intersection $X \cap \Gamma$ is irreducible, provided that X is a given geometrically irreducible variety.

Sketch of proof: Given a variety X of dimension m in $\mathbb{P}^n(\mathbb{F}_{q^N})$, we want to know how the probability of the intersection between X and a random linear subvariety V of codimension m in $\mathbb{P}^n(\mathbb{F}_{q^N})$ behaves. To do this we first intersect X with a linear subspace Γ containing V. By Bertini Theorem for a hyperplane, when $N \to \infty$ we get a geometrically irreducible curve and by Lemma 6.2.6 it must be a curve with simple tangency. Then after some calculation we can show that the desired probability coincides with $p_k(C)$.

6.2. Main results

Let X be an irreducible algebraic variety over a finite field $\mathbb{F}_q$. Define

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \quad \text{is geometrically irreducible}\right\}\right|}{\left|\check{\mathbb{P}}^n(\mathbb{F}_{q^N})\right|}. \tag{28}$$

By applying the Bertini Theorem for an infinite field [**Jou83**, Theorem 6.3(4)] we show that $\mu_e(X) = 1$. In other words the intersection $X(\mathbb{F}_{q^N}) \cap \Gamma(\mathbb{F}_{q^N})$ is also geometrically irreducible, for a generic hyperplane Γ, if $N \to \infty$.

Theorem 6.2.1. *Let X be a geometrically irreducible variety of dimension m in $\mathbb{P}^n$. Then*

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \textit{ is geometrically irreducible}\right\}\right|}{\left|\check{\mathbb{P}}^n(\mathbb{F}_{q^N})\right|} = 1.$$

Proof. Let $\mathcal{H}_{d,m-1}$ be the Chow variety of cycles in $\mathbb{P}^n$ of dimension $m-1$ and degree d in $\mathbb{P}^n$. Let $\Omega \subset S_1$ be the set of hyperplanes intersection with X is reducible of dimension $m-1$. More precisely if $\Gamma \in \Omega$, then $X \cap \Gamma = X_1 \cup X_2$, where $X_i \in \mathcal{H}_{d_i,m_i}$ for $i = 1, 2$ and $\max(m_1, m_2) = m-1$ and $d_1 + d_2 = d$.

First we show that Ω is a closed set. To do this, consider the rational map

$$\Phi_X : S_1 \dashrightarrow \mathcal{H}_{d,m-1} \quad \Gamma \mapsto \Gamma \cap X.$$

Indeed $\Omega = \bigcup_{d_1,d_2,d_1+d_2=d} \Phi^{-1}(\mathcal{H}_{d_1,m_1} \times \mathcal{H}_{d_2,m_2})$. Hence Ω is an algebraic variety. By Bertini Theorem $\dim \Omega < \dim S_1 = n+1$. Hence the probability that an element in S_1 is in Ω tends to 0. More precisely, by the Lang-Weil Theorem this probability is bounded by

$$\frac{(q^N)^{\dim \Omega}}{(q^N)^{\dim S_1}} \to 0 \quad \text{for } N \to \infty. \qquad \square$$

Let X be a variety in projective space $\mathbb{P}^n(K)$, where K is an algebraically closed perfect field. We define the *conormal* variety of X as the Zariski closure of the set

$$\mathrm{con}(X) := \left\{(p, \Gamma) \in X \times (\mathbb{P}^n)^* : T_p(X) \subset \Gamma\right\}.$$

Let π_2 be the second projection $\mathrm{con}(X) \to \pi_2(\mathrm{con}(X)) := X^*$, which is called the conormal map. If $\mathrm{con}(X)$ and $\mathrm{con}(X^*)$ are isomorphic by the map which flips the two entries of a pair in a product variety, then we say that X is *reflexive*.

It is known that if the field K has zero characteristic, then every variety is reflexive; this is not true in characteristic $p > 0$. The following theorem is useful for checking if a given projective variety is reflexive or not. see [**Wal56**].

Theorem 6.2.2 (Monge-Segre-Wallace)**.** *A projective variety X is reflexive if and only if the conormal map π_2 is separable.*

In [**HK85**] the authors proved the following result, called the Generic Order of Contact Theorem:

Theorem 6.2.3. *A projective curve Z is non-reflexive if and only if for a general point p of Z and a general tangent hyperplane H to Z at p, we have*

$$[K(\mathrm{con}(Z)) : K(Z^*)]_{isep} = I(p, Z.H).$$

Where $I(p, Z.H)$ is the intersection multiplicity of Z and H at p, and $[K(\mathrm{con}(Z)) : K(Z^*)]_{isep}$ is the inseparable degree extension.

A combination of these two theorems implies

Corollary 6.2.4. *If C is a geometrically irreducible reflexive curve of degree d in $\mathbb{P}^n(\overline{\mathbb{F}_q})$, then there exists a hyperplane $H \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ intersecting C in $d-1$ smooth points of C such that H intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point. We say C has simple tangency.*

Definition 6.2.5. Let X be a geometrically irreducible variety in $\mathbb{P}^n(K)$ of dimension m. We say that X has the simple tangency property if there exist a linear subspace $\Gamma \in J_{m-1}$ such that the curve $X \cap \Gamma$ has simple tangency.

Lemma 6.2.6. *Suppose that X is a geometrically irreducible variety of degree d and dimension m in $\mathbb{P}^n(K)$ with simple tangency property. Then for a general linear subspace $\Gamma \in J_{m-1}$ the intersection $X \cap \Gamma$ is a curve with simple tangency.*

Proof. Let $\mathcal{H}_{d,m}$ be the Chow variety. Let $\mathcal{H}'_{d,1}$ be the set of all curves in $\mathbb{P}^n(K)$ of degree d and without simple tangency. Define

$$\Phi_X \colon J_{m-1} \dashrightarrow \mathcal{H}_{d,1}, \qquad (X, \Gamma) \mapsto X \cap \Gamma.$$

Notice that Φ_X in general is a rational map but we can consider the restriction Φ_X to $\mathrm{dom}(\Phi_X)$ if necessary to Φ_X be a morphism. For a fixed $X \in \mathcal{H}_{d,m}$,

$$\Omega_X = \Big\{ \Gamma \in J_{m-1} : \quad X \cap \Gamma \quad \text{does not have simple tangency} \Big\}.$$

Indeed $\{X\} \times \Omega_X \cong \Omega_X$, by the definition we have $\Omega_X \subset \Phi^{-1}(\mathcal{H}'_{d,1})$. Since X is a variety with simple tangency property there exists a linear subspace $\Gamma \in J_{m-1}$ such that $\Gamma \cap X$ is a curve with simple tangency, hence $\Phi^{-1}(\mathcal{H}'_{d,1})$ is a proper set. We need to only show that $\Phi^{-1}(\mathcal{H}'_{d,1})$ is a close set. The proof of the lemma is a consequence of the following claim.

Claim. $\mathcal{H}'_{d,1}$ is a closed set in $\mathcal{H}_{d,1}$.

Proof of the claim. By Theorem 6.2.2 a curve C is in $\mathcal{H}'_{d,1}$ if and only if its conormal map is not separable. This is the case if and only if the Jacobian of the conormal map vanishes identically. This can be expressed as algebraic equations in the curve, hence the set $\mathcal{H}'_{d,1}$ is closed. □

Let us first formulate the definition of the probabilities that we want to compute.

Definition 6.2.7 (Probabilities of intersection)**.** Let q be a prime power and let $X \subset \mathbb{P}^n\big(\mathbb{F}_q\big)$ be a geometrically irreducible variety of dimension m and degree d defined over $\mathbb{F}_q$. For every $N \in \mathbb{N}$ and for every $k \in \{0, \dots, d\}$, the *k-th probability of intersection* $p_k^N(X)$ of varieties of codimension m with X over $\mathbb{F}_{q^N}$ is

$$p_k^N(X) := \frac{\Big|\big\{V \in J_m \,:\, |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\big\}\Big|}{|J_m(\mathbb{F}_{q^N})|}.$$

Theorem 6.2.8. *Let X be a geometrically irreducible variety of dimension m and degree d in projective space $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has the simple tangency property. Then for every $k \in \{0, \dots d\}$ we have*

$$p_k(X) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

PROOF. Define

$$I = \big\{(V, W) \in J_m \times J_{m-1} : V \subset W\big\}.$$

From Definition 6.2.7, we have

$$p_k^N(X) = \frac{\big|\big\{V \in J_m : |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\big\}\big|}{|J_m|} = \frac{\big|\big\{(V, W) \in I : |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\big\}\big|}{|I|}.$$

By extending this formula over all $W \in J_{m-1}$ we obtain

$$\sum_{W \in J_{m-1}} \frac{\big|\big\{(V, W) \in I : |V \cap X \cap W| = k\big\}\big|}{|I|}. \tag{29}$$

Where for a generic W the intersection $X \cap W$ must be geometrically irreducible curve by Theorem 6.1.3. Since any two linear subspaces have same number of points over a finite field we can write:

$$\sum_{W \in J_{m-1}} \frac{\big|\big\{V \subset W : |V \cap X \cap W| = k\big\}\big|}{\big|\big\{V : V \subset W\big\}\big|} \Bigg/ \frac{|I|}{\big|\big\{V : V \subset W_0\big\}\big|} \tag{30}$$

But the denominator of Equation (30) is $|J_{m-1}|$. Let us write $J_{m-1} = A \sqcup B$, where

$$A = \big\{W \in J_{m-1} : X \cap W \quad \text{is irreducible and has simple tangency}\big\},$$

and

$$B = \big\{W \in J_{m-1} : X \cap W \quad \text{is reducible or without simple tangency}\big\}.$$

From these and Equation (30) we obtain

$$p_k^N(X) = \frac{\sum_{W \in A} p_k^N(X \cap W) + \sum_{W \in B} \delta_B}{|J_{m-1}|},$$

where $\delta_B = \delta$ is a number in interval $[0, 1]$. Hence

$$\frac{|p_k^N(X \cap W_0)||A| + \delta|B|}{|J_{m-1}|}.$$

By Lemma 6.2.6 we know that $\frac{|B|}{|J_{m-1}|} \to 0$, when $q \mapsto \infty$. This implies

$$p_k^N(X \cap W_0) = \frac{p_k^N(X \cap W_0)|A|}{|J_{m-1}|}.$$

Note that $X \cap W_0$ is a curve of degree d. Hence the result is a consequence of the [**MSG18**, Proposition 5.2]. □

It is natural to consider the probabilities of intersection of a variety X of degree d and dimension m in $\mathbb{P}^n$ with a random variety Y of degree e and codimension m in $\mathbb{P}^n$. If X is a hypersurface and Y is a curve, via the *Veronese map* we can reduce this situation to the one of [**MSG18**, Proposition 5.2]. This motivates us to pose the following conjecture.

Conjecture 6.2.9. *Let X be a geometrically irreducible variety of dimension m and degree d in $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has the simple tangency property. Let $e \in \mathbb{N}$ be a natural number. Then for every $k \in \{0, 1, \dots ek\}$ the probability that a random irreducible variety of degree e and codimension m intersects X in exactly k points is given by*

$$p_k(X,e) = \sum_{s=k}^{de} \frac{(-1)^{k+s}}{s!} \binom{s}{k}.$$

If we removed the word "irreducible" in the conclusion above, then the conjecture would be false: the set of varieties in $\mathbb{P}^n$ of degree d and codimension m is bijective to the set of points in a Zariski-dense and open set of a Chow variety. The Chow variety has several components of maximal dimension; the smallest case for which this happens is $m = e = 2$ and $n = 3$. Here there is an 8-dimensional set of irreducible conics and an 8-dimensional set of reducible conics (pairs of lines). One can show that the probability that an irreducible conic intersect X in k points is as stated in the conjecture, but for the reducible conics, the probabilities differ. The total probabilities would be the arithmetic means of both, which would then also differ from the statement above.

CHAPTER 7

A family of four-variable expanders with quadratic growth

The result of this Chapter has already published in Moscow Journal of Combinatorics and Number Theory [**Mak18**].

7.1. Sumset and product set

Throughout this chapter, when we write $X \gg Y$, this means that $X \geq cY$, for some absolute constant $c > 0$.

This chapter is containing a result in the fields of *additive combinatorics* and, discrete geometry. In this area usually, we start out with some finite set X, which is a subset of a vector space and by following some rule, X will define a new set X' which is also finite. The process by which X' is defined will usually be some elementary arithmetic or geometric operation; for example, if X is a set of points in the plane, then by connecting every pair of points a set of lines is formed which plays the role of X'. Next, this new set X' is studied, and usually the focus of this stage of the study falls on the cardinality of X' in comparison to the generating set X, where the best possible upper and lower bounds for $\|X'\|$ are sought.

Let's look at a classic and easy example in order to shed more light on these vague comments. Let $A \subset \mathbb{R}$ be some finite set. The set of all pairwise sums generated by A forms a new set called the *sum set* of A, denoted

$$A + A := \{a + b : a, b \in A\}$$

According to regime outlined above, we would like to know about the cardinality of this set. Easily we have $|A + A| \geq |A|$, since for any fixed element $a \in A$ the set $\{a + b : b \in A\}$ is a subset of $A + A$ with cardinality A. By an argument which is less trivial we can show that

$$|A + A| \geq 2|A| - 1.$$

By considering an N-term arithmetic progression i.e $A = \{a, a+d, \ldots, a+(N-1)d\}$ we can see the above lower bound is tight. In fact the equality holds only if A is an arithmetic progression.

The product set is defined in a similar way, $AA := \{ab : a, b \in A\}$. It has been shown that for every finite set A

$$|AA| \geq 2|A| - 1.$$

It is not difficult to show $|AA| = 2|A| - 1$ if and only if A is a geometric progression. Bounds for the cardinality of sum set and product set became more interesting when studying the relationship between $|AA|$ and $A + A|$.

Consider the case where $A = \{1, 2, \ldots, N\}$, in this case as we have seen $A + A$ has the smallest possible size, but the product set became very large; indeed $|AA| = |A|^{2-o(1)}$, and so the product set is almost as large as possible.

A similar situation arises in reverse if A is taken to be a geometric progression. For example if $A = \{2, 2^2, 2^3, \dots, 2^N\}$, then it follows that $|A + A| = \binom{|A|}{2} + |A|$, the most possible cardinality, while the product set has the smallest possible cardinality.

We have looked at only two extremal example, but one might speculate that it is not possible to find a finite set such that both sum set and product set are small. If we assume A has an additive structure then the product set will grow very large, and likewise if A has a multiplication property then the sum set must be very large.

This problem was first studied by Erdős-Szemerédi [**ES83**], who conjectured that, for all $\epsilon > 0$ and for any finite set $A \subset \mathbb{N}$,

$$\max\{|A + A|, |AA|\} \geq c(\epsilon)|A|^{2-\epsilon}.$$

It is natural to extend this for other settings (such as $\mathbb{R}$), and also to change the polynomials $F(x, y) = x + y$ and $F(x, y) = xy$ defining the sum and product sets to other polynomials or rational functions. In recent years much research has been done in this direction.

The aim of this chapter is to consider a certain class of rational functions of four variables and the size of the cardinality of values of them on some Cartesian products.

For many such functions, the images of sets are known to always grow. For example, the authors of [**MRNS15**] have studied several multivariable polynomials, including the function

$$G(x_1, x_2, x_3, x_4, x_5) = x_1(x_2 + x_3 + x_4 + x_5).$$

More precisely they showed that, for any finite set $A \subset \mathbb{R}$,

$$|A(A + A + A + A)| \gg \frac{|A|^2}{\log |A|},$$

where $A(A + A + A + A) := \{x_1(x_2 + x_3 + x_4 + x_5) : x_i \in A\}$.

In [**MRNS17**], the authors studied a more complicated function, namely

$$H(x_1, x_2, x_3, x_4, x_5) = (x_1 + x_2 + x_3 + x_4)^2 + \log x_5.$$

They showed that, for any finite $A \subset \mathbb{R}$,

$$|\left\{(a_1 + a_2 + a_3 + a_4)^2 + \log a_5 : a_i \in A\right\}| \gg \frac{|A|^2}{\log |A|}.$$

In the same circle of ideas, [**BRN15**] investigated the rational function $F(x_1, x_2, x_3, x_4) = \frac{x_1+x_2}{x_3+x_4}$, showing that for any finite set $A \subset \mathbb{R}$, we have

$$|F(A, A, A, A)| \geq 2|A|^2 - 1.$$

Our result is a generalization of the method of [**MRNS15**, Corollary 3.1], where they used the Szemerédi-Trotter Theorem to prove that for any finite set $A \subset \mathbb{R}$:

$$\left|\frac{A - A}{A - A}\right| \gg |A|^2.$$

A stronger version of this result, with a multiplicative constant 1, follows from an earlier geometric result of Ungar [**Ung82**].

In this chapter we consider a certain class of rational functions of four variables. Suppose that $g(x, y)$ is a polynomial of two variables of degree d. Let

$$F(x_1, x_2, y_1, y_2) = \frac{g(x_1, y_1) - g(x_2, y_2)}{y_2 - y_1}$$

be a four-variable rational function in terms of x_1, x_2, y_1, y_2. The main theorem of this paper is the following result concerning the growth of F.

Theorem 7.1.1. *Suppose that $g(x, y)$ is a polynomial of degree d, that $y_2 - y_1$ does not divide $g(x_1, y_1) - g(x_2, y_2)$, and that $A \subset \mathbb{R}$ is a finite set. Then*

$$|X| \gg_d |A|^2, \quad \text{where } X := \left\{ \frac{g(a_1, b_1) - g(a_2, b_2)}{b_2 - b_1} : a_1, a_2, b_1, b_2 \in A \right\}.$$

Notice that the following example shows that the condition that the denominator cannot be a divisor of the numerator is necessary.

Example 7.1.2. *Suppose that $g(x, y) = y^2$ and $A = \{1, 2, \dots n\}$. Then*

$$X = \left\{ \frac{b_1^2 - b_2^2}{b_2 - b_1} : b_1, b_2 \in A \right\}$$

equals $-\{b_2 + b_1 : b_i \in A\}$ and has cardinality $O(n)$.

Furthermore, notice that the condition rules out a degenerate case where the polynomial $g(x, y)$ does not depend on x.

On the other hand, it is known that for some polynomials g, the result of Theorem 7.1.1 is tight. For example, if we define $g(x_1, y_1) = x_1$ then Theorem 7.1.1 recovers the result of [**MRNS15**] and [**Ung82**]. This is known to be tight, since for the set $A = \{1, \dots, N\}$,

$$\left| \frac{A - A}{A - A} \right| = O(N^2).$$

However, we are not aware of any other polynomials g for which the bound in Theorem 7.1.1 is tight, and whether or not the bound can be improved for some particular g is an interesting question.

Our main result has some similarities with a result of Raz, Sharir and Solymosi [**RSS15**] concerning the growth of two variable polynomials. Their result states that, if F is a two variable polynomial with bounded degree, then for any $A, B \subset \mathbb{R}$ with $|A| = |B| = n$,

$$|F(A, B)| \gg_d n^{4/3},$$

provided that F satisfies a non-degeneracy condition. This condition states that F cannot be of one of the following forms

(1) $F(u, v) = f(g(u) + h(v))$,
(2) $F(u, v) = f(g(u) \cdot h(v))$.

This result gave an improvement upon an earlier result of Elekes and Ronyai [**ER00**].

7.1.1. The Szemerédi-Trotter Theorem. The essential ingredient used to prove our result is a corollary of the *Szemerédi-Trotter* Theorem [**ST83**], which gives a bound for the number of lines in the plane containing at least a fixed number of points k from a given finite set, that is, the number of *k-rich* lines.

Theorem 7.1.3 (Szemerédi-Trotter)**.** *Suppose that P is a set of n points and $\mathcal{L}$ is a set of m lines in $\mathbb{R}^2$. Then*

$$\mathcal{I}(P, \mathcal{L}) \ll n^{\frac{2}{3}} m^{\frac{2}{3}} + n + m. \tag{31}$$

Corollary 7.1.4. *Let $k, n \geq 2$ be natural numbers and fix $d \in \mathbb{N}$ such that $8d \leq k \leq d\sqrt{n}$. Let $\mathcal{L}$ be a set of n lines in the plane, and let $t_{\geq k}$ denote the number of points in the plane contained in at least k elements of $\mathcal{L}$, where each line appears with multiplicity at most d. Then*

$$t_{\geq k} = O_d\left(\frac{n^2}{k^3}\right).$$

7.1.2. Main Results. Suppose that $A, B \subset \mathbb{R}$ are finite, and $g(x_1, y_1)$ is a polynomial of degree d. We associate an element of $A \times B$ with a line via

$$A \times B \ni (a, b) \longleftrightarrow l_{a,b} : y = bx - g(a, b).$$

Consider $\mathcal{L} = \{\ell_{a,b} : a, b \in A \times B\}$ as a multi-set. Then $\mathcal{L}$ is a set of $|A||B|$ lines, such that each line appears at most d times. We also define the quantity

$$n(x, y) = \left|\left\{(a, b) \in A \times B \,:\, (x, y) \in l_{a,b}\right\}\right|,$$

which is interpreted geometrically as the number of lines of $\mathcal{L}$ that pass through (x, y).

Lemma 7.1.5. *Suppose that $d \in \mathbb{N}$ is fixed. Suppose that $A, B, X \subset \mathbb{R}$ are finite and satisfy $|X| \leq \frac{|A||B|}{4d^2}$, with $0 \notin X$. Then*

$$\sum_{x \in X} \sum_{y} n^2(x, y) \ll |A|^{\frac{3}{2}} |B|^{\frac{3}{2}} |X|^{\frac{1}{2}}. \tag{32}$$

Proof. The amount of t-rich points is given by

$$R_t := \left\{(x, y) \in \mathbb{R}^2 : n(x, y) \geq t\right\}.$$

We first show that

$$|R_t| \ll \frac{|A|^2 |B|^2}{t^3}.$$

First, we bound $n(x, y)$ for a given point (x, y). For fixed $b_0 \in B$ we obtain a line with slope b_0 passing through (x, y) and a one variable polynomial equation $g(a, b_0)$. Since each line is determined uniquely, by its slope and one point on it (for fixed b_o and (x, y) the equation $g(a, b_0) = 0$ has at most d distinct solutions), we have

$$n(x, y) \leq d|B|.$$

With a similar argument for fixed $a \in A$ we obtain a univariate polynomial equation. Since each line is determined uniquely by its y-intercept and one point on it we have:

$$n(x, y) \leq d|A|.$$

These together imply:

$$n(x, y) \leq d(\min\{|A|, |B|\}) \leq (d|A|d|B|)^{\frac{1}{2}} = d|\mathcal{L}|^{\frac{1}{2}}.$$

This implies there are no points incident to more than $d\sqrt{|\mathcal{L}|}$ lines in $\mathcal{L}$, and by applying Corollary 7.1.4 we get:

$$|R_t| \ll \frac{|\mathcal{L}|^2}{t^3} \leq \frac{|A|^2 |B|^2}{t^3}.$$

Let $\Delta > 2d$ be an integer to be specified later. We have

$$\sum_{x \in X} \sum_{y} n^2(x, y) \leq \sum_{x \in X} \sum_{n(x,y) \leq \Delta} n^2(x, y) + \sum_{\substack{(x,y) \\ n(x,y) > \Delta}} n^2(x, y). \tag{33}$$

The first term is bounded by $\Delta|A||B||X|$, in fact

$$\sum_{x \in X} \sum_{n(x,y) \leq \Delta} n^2(x, y) \leq \Delta \sum_{x \in X} \sum_{y} n(x, y) = \Delta|A||B| \sum_{x \in X} 1 = \Delta|A||B||X|. \tag{34}$$

For second term we have:

$$\sum_{\substack{(x,y)\\ n(x,y)>\Delta}} n^2(x,y) = \sum_{j\geq 1} \sum_{2^{j-1}\Delta\leq n(x,y)\leq 2^j\Delta} n^2(x,y) \ll$$

$$\ll \sum_{j\geq 1} \frac{|A|^2|B|^2}{(2^j\Delta)^3}\cdot(2^j\Delta)^2 = \frac{|A|^2|B|^2}{\Delta}\sum_{j\geq 1}\frac{1}{2^j} = \frac{|A|^2|B|^2}{\Delta}. \tag{35}$$

For an optimal choice, set the parameter $\Delta = \left\lceil \frac{(|A||B|)^{1/2}}{|X|^{1/2}} \right\rceil > 2d$. Combining the bounds from (33) and (34) and (35), it follows that

$$\sum_x \sum_y n^2(x,y) \ll |A|^{\frac{3}{2}}|B|^{\frac{3}{2}}|X|^{\frac{1}{2}}. \qquad \square$$

Proof of Theorem 6.1.5. Consider:

$$|X| = \left|\left\{(x,a_1,a_2,b_1,b_2) : x = \frac{g(a_1,b_1)-g(a_2,b_2)}{b_1-b_2}, a_i,b_i\in A\right\}\right|$$

$$= \left|\left\{(x,a_1,a_2,b_1,b_2) \,:\, b_1x - g(a_1,b_1) = b_2x - g(a_2,b_2)\right\}\right| =$$

$$\sum_x\sum_y n^2(x,y) \ll |A|^3|X|^{\frac{1}{2}}.$$

On the other hand, $|X|\geq |A|^4$. Hence we obtain:

$$|A|^4 \ll |A|^3|X|^{\frac{1}{2}}, \quad \text{hence} \quad |X| \gg |A|^2. \qquad \square$$

Corollary 7.1.6. *Suppose that $P = A\times A$ is a set of $|A|^2$ points. Let l be the y-axis. Suppose that $B(P)$ is the set of all bisectors determined by P. Then $|B\cap l|\gg |A|^2$.*

Proof. By a simple calculation we can see that the equation of the bisector determined by two points (x_1,y_1) and (x_2,y_2) in the s,t plane is:

$$s = \frac{2(x_1-x_2)t + (x_2^2-x_1^2)+(y_2^2-y_1^2)}{2(y_2-y_1)}.$$

Inserting $t=0$, the hitting point has coordinate

$$\left(0, \frac{(x_2^2-x_1^2)+(y_2^2-y_1^2)}{2(y_2-y_1)}\right).$$

Setting $g(x,y) = -2(x^2-y^2)$, we obtain the result by Theorem 7.1.1. $\square$

As we mentioned, this bound is tight for some polynomials, for instance $g(x,y)=x$. However, we expect that if $F(x_1,x_2,y_1,y_2)$ is a generic rational function satisfying the condition of the Theorem 7.1.1 we have $|X|\gg |A|^3$.

CHAPTER 8

Some conjectures and future planned work

In this chapter we consider several problems and conjectures.

8.1. Sets in general position over finite fields

Recall that for a finite set P in the real plane, an ordinary line is a line passing through exactly two points from P. As we have seen in Chapter 1, if P is a set of n points with at most $O(Kn)$ ordinary lines, then all but $O(K)$ points of P lie on some cubic curve. However, Ben Green posed a conjecture stating that the situation is different over finite fields.

We say that a set of points P in the plane is in *general position* if no line meets P in more than two points. In the literature this kind of set is called an *arc*. The classification of arcs over finite fields is an active area in finite geometry and cryptography.

There is a straightforward calculation to get an upper bound for the cardinality of an arc over a finite field with q elements, where q is a prime power.

If P is an arc in the projective plane over $\mathbb{F}_q$, then

(1) if q is even, then $|P| \leq q+2$.
(2) if q is odd, then $|P| \leq q+1$.

The proof is easy. Let P be a set with no three points on a line. Pick an arbitrary $x \in P$. There are exactly $q+1$ lines through x, and since no three points of P are collinear, we see that $|P| \leq q+2$ (until now it does not matter whether q is odd or even). If q is odd, pick a point say y outside of P, for every $x \in P$ there is a line $l_{x,y}$ through x and y. if $|A| = q+2$, then precisely $\frac{(q+2)}{2}$ of these lines meet P and this is a contradiction (since $q+2$ is odd, hence $q+2/2$ is not integer).

On the other hand if q is even, then it is not hard to construct an arc with cardinality $q+2$. By Qvist's Theorem if C is a conic, then there exists a point N, such that, the set of tangents to C is the pencil of all lines through N. Just C take $P = C \cup N$.

One of the most important results in finite projective geometry concerning arcs is Segre's Theorem [**Seg55**].

Theorem 8.1.1. *Let $q = p^\alpha$ be a prime power, where p is odd. If P is an arc with cardinality $|P| = q+1$, then P is described by a quadratic equation.*

The following conjecture was posed by Ben Green in a conference in honor of Peter Sarnak on his 61st Birthday[1].

Conjecture 8.1.2 (Ben Green)**.** *Suppose that P is a set of points in general position over the finite field $\mathbb{F}_p$, where p is a prime number. Then apart from $o(p)$ points, P lies on a cubic curve.*

[1] https://www.youtube.com/watch?v=30XnS0KQz-Q

More precisely there exists a function $f : \mathbb{N} \longrightarrow \mathbb{N}$ such that $f \in o(\mathrm{id})$ and for every prime number p and for every subset S in $\mathbb{F}_p^2$ with no three points on a line, there exists a subset S_p of S with $|S_p| = f(p)$ and the points $S - S_p$ lie on a cubic curve.

There are some examples and results that support this conjecture. For instance there are some curves of higher degree over $\mathbb{F}_p$ with no three points collinear, however these curves over $\mathbb{F}_p$ are presented by some quadratic equations, and they have completely different behaviour over the algebraic closure of $\mathbb{F}_p$.

Example 8.1.3. *Consider the curve C given by the equation*

$$x^p y + y^p z + z^p x = 0.$$

As we have seen in Example 2.1.21, this curve has no simple tangency, and it was shown in [**Rat87**, Example 2.16] *that the Galois group of C is $PGL(2, p)$. Since $PGL(2, p)$ is sharply three transitive, we have $p_3(C) = \ldots p_{p-1}(C) = 0$ and $p_{p+1}(C) = \frac{1}{|PGL(2,p)|}$.*

On the other hand by Fermat's Little Theorem $a^p = a$ for all $a \in \mathbb{F}_p$. Hence $C(\mathbb{F}_p)$ is presented by the quadric curve $xy + yz + zx = 0$.

Example 8.1.4. *Let C be the rational space curve*

$$[x_0 : x_1] \mapsto [x_0^{p+1} : x_0^p x_1 : x_0 x_1^p : x_1^{p+1}].$$

It was shown [**Rat87**, Example 2.15] *that C is a curve without simple tangency and its Galois group is sharply three transitive, hence $p_3(C) = \ldots p_{2p+1}(C) = 0$ and $p_{2p+2}(C) = \frac{1}{|G|}$, where G is the Galois group of C. On the other by Fermat's Little Theorem this curve over $\mathbb{F}_p$ is the same as the conic defined by $[x_0^2 : x_0 x_1 : x_0 x_1 : x_1^2] = [x_0^2 : x_0 x_1 : x_1^2]$.*

Theorem 8.1.5 (Segre)**.** *Suppose that Δ is an arc in the projective plane $\mathbb{P}^2(\mathbb{F}_q)$, where q is a prime power of an odd prime number. Then $|\Delta| \leq q+1$. If $|\Delta| = q+1$, then Δ is a non-degenerate conic.*

A generalization of this theorem is the following, see [**HT15**, Theorem 4.5].

Theorem 8.1.6. *If Δ is an arc in the projective plane over $\mathbb{F}_q$ where q is a prime power of some odd prime number and $|\Delta| \geq q - \frac{\sqrt{q}}{4} + O(1)$, then Δ is contained in a conic.*

When q is a prime number, Voloch in [**Vol90**] found a better bound.

Theorem 8.1.7 (Voloch1990)**.** *Let p be a prime number, let δ be an arc of cardinality at least $\frac{44p}{45} + \frac{8}{9}$ in $\mathbb{F}_p^2$. Then δ is contained in a conic.*

The following example shows that Theorem 8.1.5 does not hold if q is an even number.

Example 8.1.8. *Let $q = 2^m$ for some m, and let $\sigma \colon \mathbb{F}_q \longrightarrow \mathbb{F}_q$ be the automorphism sending x to x^{2e} for some $e \in \mathbb{N}$. The set*

$$\{(1, t, \sigma(t)) : t \in \mathbb{F}_q\} \cup \{(0, 0, 1), (0, 1, 0)\}$$

is a $(q + 2, 2)$-arc, whenever $(e, m) = 1$.

On the other hand, it is not too hard to construct an arc contained in a cubic curve. Suppose that (E, E_0) and $(E', 0'_E)$ are two elliptic curves and $\phi \colon (E', 0'_E) \longrightarrow (E, E_0)$ is a group homomorphism of degree 2. Then $\phi(E)/E$ is a group of order two. For simplicity we let $H = \phi(E)$.

Proposition 8.1.9. *Let* $\frac{E}{H} = \{H, x+H\}$. *Then* $x+H$ *is a set contained in* E *such that no three points are collinear.*

PROOF. Suppose that three points $p_1, p_2, p_3 \in x+H$ are collinear, then $p_1 + p_2 + p_3 = 0$. Let $p_i = x + h_i$ for $i = 1, 2, 3$, so $x + h_1 + x + h_2 + x + h_3 = 0$. Hence $3x = -(h_1 + h_2 + h_3) \in H$, in other words $3(x+H) = H$ and this means the order of $x+H$ must be a divisor of 3. However the group $\frac{E}{H}$ has 2 elements and by Lagrange's theorem the order of $x+H$ must be 1. Hence $x \in H$ and this is a contradiction. Hence no three points are collinear in this coset. □

We say that a finite set P of cardinality n is a k-arc (or (n,k)-arc) if no $k+1$ points of P are collinear and also there exists a line containing k points. In the following we construct a k-arc.

k-arc construction First let us to define a group structure on a curve of genus one in the higher dimension by using co-hyperplanity. For simplicity we only focus on space curves.

We start with a sphere in 3-space and intersect with a quadric surface. The intersection is a quartic curve which in general has genus one (in the smooth case). It is possible to define a group structure, abelian, such that $p+q+r+s=0$ if and only if the 4 points p, q, r, s are coplanar.Take a point whose osculating plane has contact order 4. There are exactly 16 complex points (in the smooth case) with this property, and either 4 or 8 of them are real. This point will be your neutral element o. For any two points p, q, let E be the plane passing through p, q, o. It intersects the curve in a 4th point, call it r. Let E' be a plane containing r and the tangent line at o. It intersects the curve also in a 4th point (the intersection at o counts twice). This you define as $p+q$.

Now if C is an elliptic curve of degree k in the projective plane, then we can define a group structure on C such that if k points $p_1, \dots p_k \in C$ are collinear, then $p_1 + \cdots + p_k = 0$. In fact it is a consequence of the following theorem.

Theorem 8.1.10. *Let* $C \subset \mathbb{P}^n$ *be a curve of genus one and* $\deg(C) = k$. *Then*

(1) $k \geq n+1$
(2) *if* $k > n+1$, *then there exists a curve* $C' \subset \mathbb{P}^{k-1}$ *and a projection map (birational)* $C' \to C$.

Now we are ready to define k-arcs for arbitrary k. To do this, take a prime p not dividing k, then take a subgroup H of index p, and then let P be a coset of H not equal to H. The neutral element o of the group structure on C must be chosen so that any k collinear points must be zero. With a similar argument as above we can show that P is a k-arc. An k-arc is called *complete* if it is not contained in a $(k+1)$-arc. The complete k-arcs are very important structures in finite projective geometry. The following result was proved in [**HP16**].

Theorem 8.1.11. *Let* μ *denote the minimum cardinality of a complete* k*-arc. Then*

$$\mu \geq \sqrt{k(k-1)(q+1)}.$$

For proving the completeness of the arc introduced in Proposition 8.1.9, see [**Giu02**]. This result motivates us to pose the following conjecture

On the other hand, by using some combinatorics, we can give a simple and short proof for this result.

A set of a group is *sum-free* set, if it contains no solution to $x + y = z$. It has already shown see [**DY69**] and [**GR05**, Proposition 5.3], that if G is a finite group and S is a sum-free subset of G, then the cardinality of S is at most $\frac{|G|}{2}$.

By considering Proposition 8.1.9, it is clear that the coset $x + H$ is sum-free subset of cardinality $\frac{|E|}{2}$. Hence by applying the result of preceding paragraph we conclude that, it must be a complete arc.

Let G be a group , a subset S of G is called *k-sum-free*, if it has no solution to $x_1 + \cdots + x_{k-1} = x_k$.

Conjecture 8.1.12. *Let G be a finite group of order n, if S is a k-sum-free subset of G, then $|S| \leq \frac{n}{k-1}$.*

Combining this conjecture with Construction 8.1, implies the following conjecture.

Conjecture 8.1.13. *For every $k \geq 3$ the k-arc defined by elliptic curves (Construction 8.1) of degree k as above is complete k-arc.*

8.2. Sylvester-Gallai over the complex numbers

As we have seen in Section 1.1.1 (Theorem 1.1.15) the Sylvester-Gallai Theorem does not hold in the complex plane. Thus there are some configurations of non-collinear points with no ordinary lines. The following conjecture is an analogue of Theorem 3.3.2 for a finite set in the complex plane without any ordinary lines.

Conjecture 8.2.1. *Let P be a set of n non collinear points in the complex plane. If P has no ordinary lines, then P is contained in a cubic curve γ (probably three non-concurrent lines).*

Notice that by [**KN73**, Theorem 3.12] the condition that the lines must be non-concurrent in the above conjecture is necessary.

Theorem 8.2.2. *Let P be a finite set in $\mathbb{C}^2$ that is not contained in one line. If P is contained in three concurrent lines, then P spans an ordinary line that does not contain the common point of the three lines.*

8.3. Finite subsets of the plane with many 3-rich lines

We have seen in Section 1.1 that if P is a set of n points in $\mathbb{R}^2$ with at least $\frac{n^2}{6} - O(n)$ 3-rich lines, then all points except a few of them must lie on a cubic curve, by Theorem 3.3.2. It is natural to state the following conjecture.

Conjecture 8.3.1. *Let P be a set of n non-collinear points in $\mathbb{R}^2$. If P spans δn^2 3-rich lines then there exists a constant δ' (independent of n) and a cubic curve γ such that $\delta' n$ points of P lie on γ.*

A one dimensional analogue of this conjecture was studied in [**GE13**], see Theorem 1.1.11, where they also posed the following conjecture.

Conjecture 8.3.2. *Let P be a set of points in $\mathbb{R}^2$ with at least δn 3-rich lines. Then there exists a cubic curve γ, such that $p \cap \gamma$ has cardinality at least 10.*

Notice that every 9 points lie on a cubic curve, thus the first non trivial case is that 10 of them lie on a cubic curve. We can simplify this conjecture as follows.

Conjecture 8.3.3. *Let P be a set of n points in the plane with a quadratic number 3-rich lines. Then there exist three lines l_1, l_2, l_3 such that $P \cap (l_1 \cup l_2 \cup l_3)$ is a set of 6 points with 3 3-rich lines.*

8.4. Directions over finite fields

Definition 8.4.1. Let E be a set of cardinality n in $\mathbb{P}^2(\mathbb{F}_q)$, define the set of directions determined by E as

$$D(E) = \{x - y : x, y \in E\}$$

under the equivalence relation that two vectors V_1, V_2 are equivalent if and only if there exists a $\lambda \in \mathbb{F}_q$ such that $V_1 = \lambda V_2$.

It is natural to ask what the smallest natural number n is, such that there exists a subset E of cardinality n in the affine plane $A^2(\mathbb{F}_q)$, that generates all directions in affine plane $A^2(\mathbb{F}_q)$. In other words, since there are q directions in the affine plane $A^2(\mathbb{F}_q)$, this is equivalent to saying $|D(E)| = q$. We can see that if E is a set in $\mathbb{P}^2(\mathbb{F}_q)$ that spans all directions, then $|E| \geq \sqrt{2q}$. Most probably such a set does not exist. In the following we consider this question and we will pose a conjecture concerning this.

Here we give several examples of sets of cardinality $2\sqrt{q}$, that span all directions. Notice that we can work also over projective plane $\mathbb{P}^2(\mathbb{F}_q)$, the only difference being that we count the infinite (vertical) direction too.

Lemma 8.4.2. *If $\mathbb{Z}_q$ is a field with q elements. Then there exist two subsets A and B of cardinality $\sqrt{q}$ of $\mathbb{Z}_q$ such that $\mathbb{Z}_q = A + B$.*

Proof. Let $A = \{1, 2, 3, ...\sqrt{q}\}$ and $B = \{\sqrt{q}, 2\sqrt{q}, 3\sqrt{q}, ...q\}$ be two arithmetic progressions, then we can see that $A + B = \mathbb{Z}_q$. □

Corollary 8.4.3. *Let C be the union $A \cup B$. Then C is a set of cardinality $2\sqrt{q}$ such that $C + C = \mathbb{Z}_q$.*

Lemma 8.4.4. *Let $\mathbb{F}_q$ be a field with $q = p^n$ elements with n even. Then there is a set A of cardinality $2\sqrt{q} - 1$ such that $A + A = \mathbb{F}_q$*

Proof. Let $\{\beta_1, ...\beta_n\}$ be a basis for $\mathbb{F}_q$ and define $C := \langle \beta_1, ...\beta_{\frac{n}{2}} \rangle$ and $D :=< \beta_{\frac{n}{2}+1}, ...\beta_n >$. Now just take $A = C \cup D$ and so we can see $A + A = \mathbb{F}_q$. □

Remark 8.4.5. Note if we want to apply the above configuration when n is odd then we get a set A of cardinality $\sqrt{p}\sqrt{q} + \frac{\sqrt{q}}{\sqrt{p}} + 1$ and the cardinality depends on p, so when we fix n and p goes to infinity we cannot get $2\sqrt{q} - 1$.

The following is a well-known theorem in finite fields, see [**IMP11**]:

Theorem 8.4.6. *Every non-collinear set of cardinality more that $q + 1$ in $\mathbb{F}_q$ determines all directions in $\mathbb{P}^2(\mathbb{F}_q)$.*

Lemma 8.4.7. *Let $A \subset \mathbb{F}_q$ be a set such that $\frac{A-A}{A-A} \neq \mathbb{F}_q$ then for any $x \notin \frac{A-A}{A-A}$ we have $|A + xA| = |A|^2$*

Proof. Let x be such as in the assumption. Then for any $a, b, c, d \in A$ we have $x \neq \frac{a-b}{c-d}$ and this means $cx - dx \neq a - b$ or $a + dx \neq cx + b$ and this implies all sums in $A + xA$ are distinct. □

If A is a subset that satisfies the assumption in Lemma 8.4.7 with $|A| = \sqrt{q}$, then for any x that is not in $\frac{A-A}{A-A}$ we have $A + xA = \mathbb{F}_q$.

Note that $\frac{A-A}{A-A}$ is the set of slopes of lines defined by the point set $A \times A$ in $\mathbb{F}_q$.

Corollary 8.4.8. *Let A be a set of $\sqrt{q}$ points in $\mathbb{F}_q$. Then either $A \times A$ determines all directions in the $\mathbb{F}_q$ or there exist an $x \in \mathbb{F}_q$ such that the set $E = \{(a, a^2) : a \in A\} \cup \{(b, b^2) : b \in xA\}$ of cardinality $2\sqrt{q}$ determines all directions.*

Next we give some examples of sets with a few points in the finite plane that generate all directions. The key property for these construction is that we have several sets A and B such that $A + B = \mathbb{F}_q$.

Example 8.4.9. *Let E be the following set*

$$\{(0, -a) : a \in A\} \cup \{(1, b) : b \in B\}.$$

Where A and B have been chosen such that $A + B = \mathbb{F}_q$. Then E is a set of cardinality $2\sqrt{q}$ that spans all directions.

To do this, let $v \in \mathbb{F}_q$. We want to find two points in E say $(0, -a)$ and $(1, b)$ such that the slope of the line through these two points is v. More precisely $\frac{b-(-a)}{1-0} = v$, or equivalently $b + a = v$. Such a and b exist by construction ($A + B = \mathbb{F}_q$).

As another example consider the following.

Example 8.4.10. *Let A and B satisfy $A + B = \mathbb{F}_q$ Consider the parabola $y = x^2$ and let E be the following set*

$$\{(a, a^2) : a \in A\} \cup \{(b, b^2) : b \in B\}$$

The direction set determined by E is the following.

$$\left\{ \frac{b^2 - a^2}{b - a} : a \in A, b \in B \right\} = \{(a + b) : a \in A, b \in B\} = \mathbb{F}_q$$

We use the following theorem to construct another example of a small set in $\mathbb{F}_p$, where p is a prime number, that determines all directions. It was proven in [**RNSW18**].

Theorem 8.4.11. *Let $A = \{1, 2, 3, \ldots, \lambda\}$ in $\mathbb{F}_p$ such that p is a prime number. Then there exists a set B in $\mathbb{F}_p$ of cardinality at most $\frac{2p}{\lambda}$ such that $AB = \mathbb{F}_q$*

Example 8.4.12. *Let E be a set of cardinality $3\sqrt{q}$, defined as follows.*

$$E = \{(0, -b) : a \in B\} \cup \{(a, 0) : a \in A^{-1}\}.$$

Where $AB = \mathbb{F}_p$ as above. Then if we consider the slopes of the lines generated by E, we can see their slopes are $\frac{b}{a}$, and by construction they give all slopes in $\mathbb{F}_p$.

In all these examples, the set E that determines all direction is a subset of a conic (two parallel lines, parabola, two intersect line). Hence we pose the following conjecture

Conjecture 8.4.13. *If E is a set of cardinality less than $c\sqrt{q}$ for some constant c in finite field $\mathbb{F}_q$ such that $|D(E)| = q + 1$, then the points of E lie on a conic.*

Conjecture 8.4.14. *Let E be a subset of the affine (projective) plane over a finite field $\mathbb{F}_q$. Suppose that E spans all directions. Then*

$$|E| \geq 2\sqrt{q}.$$

This problem has a connection with the sum-product set type problems. Let

$$A = \{1, 2, 3, ..., \sqrt{q}\} \cup \left\{ -\sqrt{q}, -2\sqrt{q}, ..., -\sqrt{q - 1}\sqrt{q} \right\}.$$

Obviously, we have $A - A = \mathbb{F}_q$. Naturally we are asking whether we can find a set A with cardinality less than $2\sqrt{q}$ such that $A - A = \mathbb{F}_q$?

Since we are not aware about existence or non-existence of such a construction, we give the following conjecture.

Conjecture 8.4.15. *If A is a set in the finite field $\mathbb{F}_q$ such that $A - A = \mathbb{F}_q$, then $|A| \geq 2\sqrt{q}$.*

We now give several geometric properties concerning the sets that span all directions over a finite field $\mathbb{F}_q$. Recall that if P is a set of points in the plane, an ordinary line is a line contains exactly two points of P.

The following proposition concerns the number of ordinary lines spanned by a set of points in the plane that generates all directions.

Proposition 8.4.16. *Let E be a set of $2\sqrt{q}$ points in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ such that E spans all directions in the affine plane. Then the number of ordinary lines defined by E is at least cq for some constant $c > 0$ independent of E.*

PROOF. Define the set

$$P(E) := \{(e_1, e_2) : (e_1, e_2) = (e_2, e_1), \quad e_1 \neq e_2\},$$

and define $L(E)$ as the distinct lines defined by E.

Let $P_O(E)$ be the set of pairs in $P(E)$ corresponding to ordinary lines and similarly let $L_O(E)$ be the set of ordinary lines determined by points of E. Obviously the natural map

$$F \colon P(E) \longrightarrow L(E)$$

is a surjective map. Also we have a map $G \colon P_O(E) \longrightarrow L_O(E)$ that is a one to one correspondence between these two sets. Now consider the restriction of the map F,

$$f \colon P(E) - P_O(E) \longrightarrow L(E) - L_O(E).$$

If l is any line in $L(E) - L_O(E)$, then since this line is not an ordinary line, there exist at least 3 points in $P(E) - P_O(E)$ such that the line associated with them is l. This means the restriction map is at least a three to one map, hence we have

$$\binom{2\sqrt{q}}{2} - N_2 \geq 3(q + 1 - N_2).$$

If we simplify this inequality, we obtain $N_2 \geq \frac{q+\sqrt{q}+3}{2}$, and this completes the proof. □

Actually in this poof we only used this fact that E is a set of points such that the number of lines are spanned by E is of order n, where n is the cardinality of P. Hence we have

Corollary 8.4.17. *Let E be a set of n points in the plane that spans at least the order of n^2 distinct lines. Then the number of ordinary lines defined by E is at least*

$$\frac{n^2}{2} + \frac{n+3}{4}$$

The following lemma concerns the maximum size of the intersection of a line in $\mathbb{A}(\mathbb{F}_q)$ with a set E of size $2\sqrt{q}$ffl that spans all directions.

Lemma 8.4.18. *Suppose that E is a set of $2\sqrt{q}$ points in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ that spans all directions. Suppose that l is a line in the plane containing t points from E. Then $t \leq \frac{3}{2}\sqrt{q}$.*

PROOF. Let l be a line that intersects E in t points. We want to show that $t \leq \frac{3}{2}\sqrt{q}$. Let m be the number of points in E that do not lie on l, obviously we have $m + t = 2\sqrt{q}$. Since E spans all directions, the number of lines generated by E must be bigger than $q + 1$, which implies that

$$tm + \binom{m}{2} > q + 1.$$

If we write t in term of m we obtain a polynomial of m

$$f(m) = -\frac{m^2}{2} + (2\sqrt{q} - \frac{1}{2})m - (q + 1) > 0.$$

We would like to know for which range of m this polynomial has positive value. The discriminant of this polynomial is $\Delta = 2q - 2\sqrt{q} - \frac{7}{4} > 0$, hence it has two distinct roots say m_0 and m_1. Without loss of generality assume $m_1 > m_0$.

$$f(m) = (m - m_0)(m - m_1).$$

Notice that $t \geq \frac{3}{2}\sqrt{q}$ if and only $m \geq \frac{1}{2}\sqrt{q}$. By computing the roots of this polynomial we have for all

$$(2 - \sqrt{2})\sqrt{q} \approx m_0 \leq m \leq 2\sqrt{q} \leq m_1 \approx (2 + \sqrt{2})\sqrt{q}, \qquad f(m) > 0.$$

Hence $t \leq \frac{3}{2}\sqrt{q}$. □

APPENDIX A

Blaschke-Bol type problem

A.1. Sylvester-Gallai for infinite sets

In this section we consider a classical theorem in web geometry and its relation with the results of Green and Tao in [**GT13**]. Before we state the theorem we consider some examples and definitions. In this section we are using the following references [**Bla55**], [**GT13**] and [**Nil13**].

There are several counterexamples to show that the Sylvester-Gallai Theorem 1.1.1 does not hold when the given set P is an infinite set. In other words Sylvester-Gallai Theorem 1.1.1 guarantees that as long as a point set P is a finite non-collinear set, then there exists at least one line that meets P in exactly two points. However in the following examples we will see that when P is an infinite set, we may have the case that every line meets P in exactly three points. For more details see [**GT13**, Section 2].

Recall for a given set of points in the plane a k-rich line is a line that meets P in exactly k points, especially, an ordinary line means a 2-rich line. First consider an infinite set on three concurrent lines. After applying a projective transformation we can assume these three lines are parallel lines

$$\begin{aligned} l_1 &= \big\{[x_1 : 0 : 1] : x_1 \in \mathbb{R}\big\} \cup \big\{[1 : 0 : 0]\big\} \\ l_2 &= \big\{[x_2 : 1 : 1] : x_2 \in \mathbb{R}\big\} \cup \big\{[1 : 0 : 0]\big\} \\ l_3 &= \big\{[x_3 : 2 : 1] : x_3 \in \mathbb{R}\big\} \cup \big\{[1 : 0 : 0]\big\}. \end{aligned} \tag{36}$$

Observe that $[x_1 : 0 : 1]$, $[x_2 : 1 : 1]$ and $[x_3 : 2 : 1]$ are collinear if and only if $x_1 + x_3 = 2x_2$. Thus, if we consider the infinite point set

$$P := \{[n_1 : 0 : 1] : n \in \mathbb{Z}\} \cup \{[n_2 : 1 : 1] : n_2 \in \mathbb{Z}\} \cup \{[n_3 : 2 : 1] : n_3 \in \mathbb{Z}\}, \tag{37}$$

there are no ordinary lines; in fact every line joining a point in $P \cap l_1$ with a point of $P \cap l_2$ meets a point of $P \cap l_3$.

There is a similar example involving three non-concurrent lines. Again, after applying a projective transformation, we may work with the lines

$$\begin{aligned} l_1 &= \big\{[x : 0 : 1] : x \in \mathbb{R}\big\} \cup \big\{[1 : 0 : 0]\big\}, \\ l_2 &= \big\{[0 : y : 1] : y \in \mathbb{R}\big\} \cup \big\{[0 : 1 : 0]\big\}, \\ l_3 &= \big\{[-z : 1 : 0] : z \in \mathbb{R}\big\} \cup \big\{[1 : 0 : 0]\big\}. \end{aligned} \tag{38}$$

observe that for $x, y, z \in \mathbb{R}^*$, three points $[x : 0 : 1]$, $[0 : y : 1]$ and $[-z : 1 : 0]$ are collinear if and only if $z = x/y$. Thus, if we consider the infinite point set

$$P = \{[2^n : 0 : 1] : n \in \mathbb{Z}\} \cup \{[0 : 2^m : 1] : m \in \mathbb{Z}\} \cup \{[2^s : 1 : 0] : s \in \mathbb{Z}\}, \tag{39}$$

then again there are no lines in the plane that meet P in precisely two points.

Finally, we consider a different situation. In this example P is an infinite set with few ordinary lines contained in a cubic curve. Consider the cuspidal singular cubic curve γ given by the equation $yz^2 = x^3$. Removing the singular point at $[0 : 1 : 0]$, we may parameterise the smooth points γ^* of this curve by $\{[t : t^3 : 1] : t \in \mathbb{R}\}$. It is not too hard to see that three points $[t_1 : t_2^3 : 1]$, $[t_2 : t_2^3 : 1]$ and $[t_3 : t_3^3 : 1]$ on the curve are collinear if and only if $t_1 + t_2 + t_3 = 0$. Now let P be

$$P = \{[n : n^3 : 1] : n \in \mathbb{Z}\}.$$

Then there are very few ordinary lines, indeed only those lines that are tangent to γ at a point $[n : n^3 : 1]$ and meet γ at the second point $[-2n : (-2n)^3 : 1]$.

Again, like the configurations of finite sets with few ordinary lines (Theorem 1.1.9), we can see that all these above examples contained in some cubic curve.

A.2. Web Geometry

A.2.1. Definition of a web. Let X be a 2 dimensional real or complex manifold. A 3-web on X is given by three foliations of smooth curves in general position (for each point $p \in X$ there are exactly one curve from each family through p). Two webs W and W' on X are locally equivalent at $p \in X$, if there exists a local diffeomorphism on a neighborhood of p that exchanges them.

A 3-web is called *linear* if it is given by three foliations of straight lines. A web that is equivalent to a linear web is called *linearizable*. A 3-web is called *parallelizable* if it is equivalent to three families of parallel lines.

Definition A.2.1 (hexagonal 3 web)**.** Suppose that $\mathcal{F}_r$, $\mathcal{F}_g$ and $\mathcal{F}_b$ are three families of red, green, and blue, lines respectively. The colouring lines form a (hexagonal) web if there is a disk Ω satisfying the following 2 conditions:

Foliation condition: For each point A of the disk there exists exactly one line of each colour passing through A; and the lines of different colours do not coincide

Closure condition: Take an arbitrary point O inside the disk. Draw the red, green, and the blue line through the point. On the red line take an arbitrary point 1 inside the disk. Draw the green line through the point. Suppose that the green line intersects the blue line through the point O at a point 2. The green and the blue line through the point 2 have already been drawn; draw the red one. The intersection point of the obtained red line with the green line through the point O is denoted by 3. Continuing this construction we get the points 4;5;6;7. The closure condition asserts that if all the above points belong to the disk then $7 = 1$. See Figure 1

Note that any three families $\mathcal{F}_r$, $\mathcal{F}_g$ and $\mathcal{F}_b$ that satisfied only in the first condition is called a 3-web.

Theorem A.2.2 (Chasles)**.** *Consider* 6 *sides and* 3 *diagonals-in total* 9 *lines-of a Brainchon-hexagonal (Figures 2, 3.), if* 8 *of them are tangent to a curve of class* 3*, then also the* 9*th is tangent.*

I appreciate Josef Schicho, who translated the proof of the following theorem from [**Bla55**, Page 24].

Theorem A.2.3 (Graf-Saure)**.** *A web of lines is hexagonal if and only if it is the web of tangents to an algebraic curve of class* 3*.*

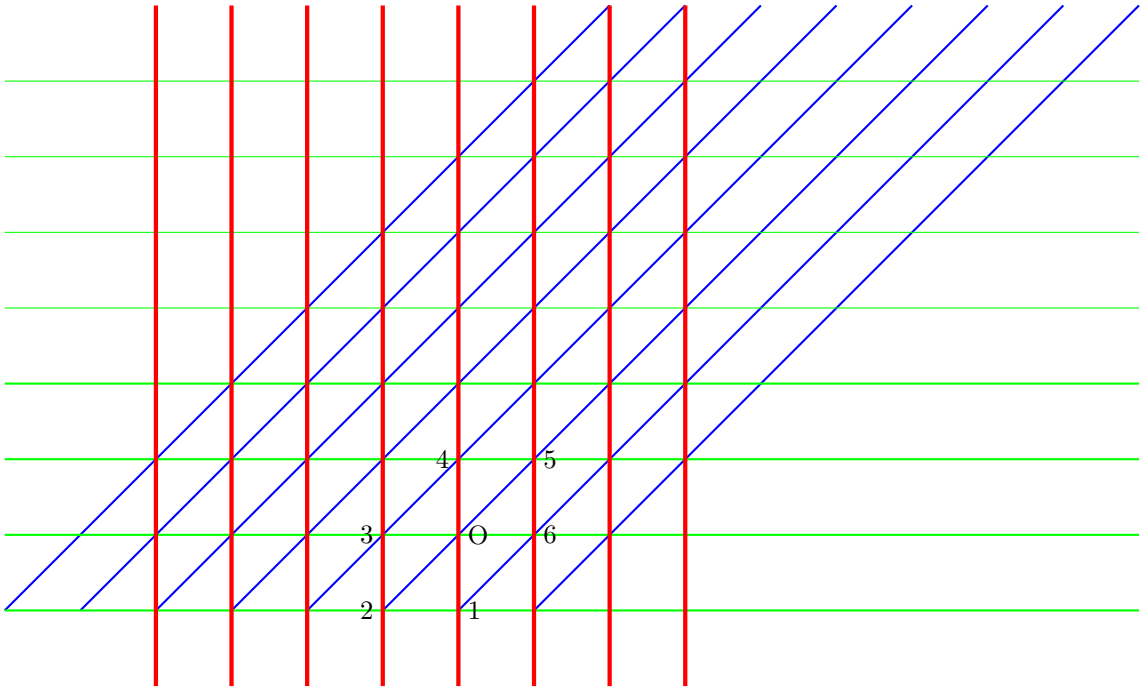


FIGURE 1.

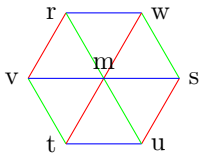


FIGURE 2.

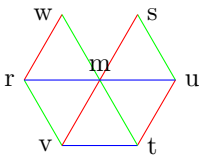


FIGURE 3.

The dual version of this theorem is the following:

Theorem A.2.4. *Suppose that a set of lines $\mathcal{F}$ satisfy the hexagon 3-web condition. Then these lines form a web if and only if in some cartesian coordinate system their coordinates satisfy a fixed equation of degree 3.*

This means: Let C be a curve of class 3. Assume p is a point lying on 3 distinct real tangent lines $1, 2, 3.$ to C. Then there is a neighbourhood Ω of q such that all points $q \in \Omega$ lie on 3 distinct real tangents. If q moves continuously to p then all of the these tangents through q goes to either $1, 2$ or 3. This induces a partition of the tangents to C meeting Ω in to 3 classes each lying a bundle of curves in Ω, if Ω fulfilles convexity properties. Since any two tangents have at most one point

in common, these bundles form a web. The theorem of Graf and Sauer says, that each such web is hexagonal. Conversely, in a hexagonal web of lines, all lines are tangent to a curve of class 3.

PROOF. The first part of Theorem A.2.3 follows immediately: every 3-web of tangents to a curve of class 3 is hexagonal.

If we form a Brianchon-hexagon around m, as in Figure 3, then we need to check if the not yet drawn line through s also passes through w. But this is a consequence of Theorem A.2.2.

Conversely, assume we have a hexagonal web. We chose a real triangle and describe all figures D_n (here D_n means a triangle with n^2 sub triangle Figure 5). First we will prove all lines in all those figures are tangent to one and the same curve C of class 3. If we can do that, then the proof is done, because any line in the web is a limit of lines in some D_n and must therefore also be a tangent.

In other to prove this, first show that: The lines of a figure D_n are tangent to a curve C_n of class 3. For $n \geq 4$, C_n is uniquely determined. We first show that this for $n = 1, 2, 3, 4$ and then by induction.

For $n = 3$ the number of lines in D_3 is 9, see Figure 4, they are surely tangent of some curve of class 3. For $n = 4$ we consider Figure 4. We temporary leave out a row of triangles and consider the figure D_3 in 145. Hence the lines are 9 lines of the Brainchon-hexagon around 7. So there is 1-parameter set of curves of class 3 tangent to all lines. From this family we pick C which is also tangent to 23. This is a linear condition on the 1-parameter, which surely can be fulfilled. With the exception of 46 and 58 all lines in the figure are tangents.

In the Braianchon-hexagon around 9, 8 lines are tangent to C, and by Theorem 1.1.10 the 9th has to be, and this is 46. Analogously 58 is a tangent as well. So we have found one curve C_4. It is unique, because 2 such curves would have 12 common tangents, which is impossible.

Now we prove the claim for D_n by induction. If we leave out a row of triangles from Figure 5, it remains a figure D_{n-1} in 145. Its lines are tangent to a curve C_{n-1} of class 3, by induction hypothesis. Let 6 be a point of the configuration distinct from $4, 5$ and its neighbours. Since $n - 1 \geq 4$ such a point exists. In the Brainchon-hexagon around 6 again 8 lines are tangent to C_{n-1}, hence also the 9th and this is 23.

As above we show that the last 2 lines 47 and 58 are tangents to C_{n-1}. This case is therefore tangent to all lines in D_n, hence it is the desired C_n and it is unique because C_{n-1} as already is unique. From the construction $C_{n-1} = C_n$ for $n \geq 5$, hence the claim is proven. □

More precisely Graf and Sauer proved a theorem, which in web geometry language can be stated as follows: a linear web is parallelizable if and only if it is associated with an algebraic curve of degree 3, i.e. if its leaves are tangent lines to an algebraic curve of degree 3 ([**Bla55**, page 24]). This theorem is a special case of N.H. Abel's classical theorem and its converse: the general Lie-Darboux-Griffiths theorem [**Gri76**].

Now let P be a set of n points in the plane with few ordinary lines (it means there are at most $O(Kn)$ ordinary lines for some $K = O(\log(\log(n)))$). As we have seen in 1.1 Inequality 5 ensuring that in the dual graph Γ_P resembles a triangulation when t_2 is small. In other words (with some elegant combinatorial argument due

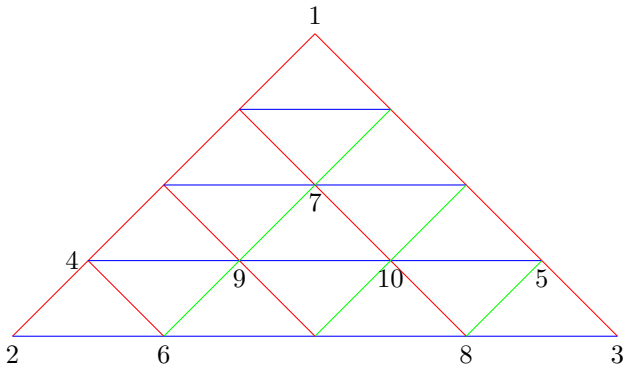


FIGURE 4.

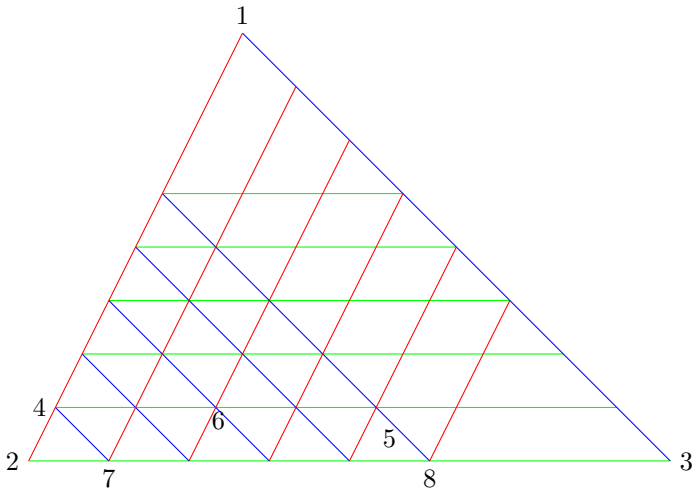


FIGURE 5.

to Green and Tao) we conclude that Γ_P contains many hexagons next each other and by applying Theorem 1.1.10, they proved most of the points of P must lie on a cubic curve.

Bibliography

[ABSR15a] Julio C. Andrade, Lior Bary-Soroker, and Zeev Rudnick, *Shifted convolution and the Titchmarsh divisor problem over* $\mathbb{F}_q[t]$, Philos. Trans. Roy. Soc. A **373** (2015), no. 2040.

[ABSR15b] ———, *Shifted convolution and the Titchmarsh divisor problem over* $\mathbb{F}_q[t]$, Philos. Trans. Roy. Soc. A **373** (2015), no. 2040.

[Asg18] Shamil Asgarli, *Sharp Bertini theorem for plane curves over finite fields*, Available at https://arxiv.org/abs/1804.01569.

[Bal18] Simeon Ball, *On sets defining few ordinary planes*, Discrete Comput. Geom. **60** (2018), no. 1, 220–253. MR 3807355

[Bas01] A. B. Basset, *An elementary treatise on cubic and quartic curves*, Available at https://archive.org/details/anelementarytre02bassgoog.

[BB94] A. Bálintová and V. Bálint, *On the number of circles determined by n points in the Euclidean plane*, Acta Math. Hungar. **63** (1994), no. 3, 283–289. MR 1261471

[BGS74] Stefan A. Burr, Branko Grünbaum, and N. J. A. Sloane, *The orchard problem*, Geometriae Dedicata **2** (1974), 397–424. MR 0337659

[BHW11] A. A. Bruen, J. W. P. Hirschfeld, and D. L. Wehlau, *Cubic curves, finite geometry and cryptography*, Acta Appl. Math. **115** (2011), no. 3, 265–278. MR 2823118

[Bix06] Robert Bix, *Conics and cubics*, second ed., Undergraduate Texts in Mathematics, Springer, New York, 2006, A concrete introduction to algebraic curves. MR 2242725

[Bla55] Wilhelm Blaschke, *Einführung in die Geometrie der Waben*, Birkhäuser Verlag, Basel und Stuttgart, 1955. MR 0075630

[Bla00] David E. Blair, *Inversion theory and conformal mapping*, Student Mathematical Library, vol. 9, American Mathematical Society, Providence, RI, 2000. MR 1779832

[BMP05] Peter Brass, William Moser, and János Pach, *Research problems in discrete geometry*, Springer, New York, 2005. MR 2163782

[BPBSR84] Marcel Berger, Pierre Pansu, Jean-Pic Berry, and Xavier Saint Raymond, *Problems in geometry*, Problem Books in Mathematics, Springer-Verlag, New York, 1984, Translated from the French by Silvio Levy. MR 772926

[BRN15] Antal Balog and Oliver Roche-Newton, *New sum-product estimates for real and complex numbers*, Discrete Comput. Geom. **53** (2015), no. 4, 825–846. MR 3341581

[BSJ12] Lior Bary-Soroker and Moshe Jarden, *On the Bateman-Horn conjecture about polynomial rings*, Münster J. Math. **5** (2012), 41–57.

[BW05] Andreas O. Bender and Olivier Wittenberg, *A potential analogue of Schinzel's hypothesis for polynomials with coefficients in* $\mathbb{F}_q[t]$, Int. Math. Res. Not. (2005), no. 36, 2237–2248. MR 2181456

[CL05] Antoine Chambert-Loir, *A field guide to algebra*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2005. MR 2089461

[CM68] D. W. Crowe and T. A. McKee, *Sylvester's problem on collinear points*, Math. Mag. **41** (1968), 30–34. MR 0235452

[Cox69] H. S. M. Coxeter, *Introduction to geometry*, second ed., John Wiley & Sons, Inc., New York-London-Sydney, 1969. MR 0346644

[CP16] François Charles and Bjorn Poonen, *Bertini irreducibility theorems over finite fields*, J. Amer. Math. Soc. **29** (2016), no. 1, 81–94. MR 3402695

[CS93] J. Csima and E. T. Sawyer, *There exist* $6n/13$ *ordinary points*, Discrete Comput. Geom. **9** (1993), no. 2, 187–202. MR 1194036

[Die12] Claus Diem, *On the discrete logarithm problem for plane curves*, J. Théor. Nombres Bordeaux **24** (2012), no. 3, 639–667.

[DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, SIAM J. Comput. **42** (2013), no. 6, 2305–2328.

[Dvi09] Zeev Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), no. 4, 1093–1097. MR 2525780

[DY69] Palahenedi Hewage Diananda and Hian Poh Yap, *Maximal sum-free sets of elements of finite groups*, Proc. Japan Acad. **45** (1969), 1–5. MR 0245662

[EGH96] David Eisenbud, Mark Green, and Joe Harris, *Cayley-Bacharach theorems and conjectures*, Bull. Amer. Math. Soc. (N.S.) **33** (1996), no. 3, 295–324. MR 1376653

[Ell67] P. D. T. A. Elliott, *On the number of circles determined by n points*, Acta Math. Acad. Sci. Hungar. **18** (1967), 181–188. MR 0213939

[Ent18] Alexei Entin, *Monodromy of hyperplane sections of curves and decomposition statistics over finite fields*, Available at https://arxiv.org/abs/1805.05454.

[EPS06] Noam Elkies, Lou M. Pretorius, and Konrad J. Swanepoel, *Sylvester-Gallai theorems for complex numbers and quaternions*, Discrete Comput. Geom. **35** (2006), no. 3, 361–373. MR 2202107

[ER00] György Elekes and Lajos Rónyai, *A combinatorial problem on polynomials and rational functions*, J. Combin. Theory Ser. A **89** (2000), no. 1, 1–20. MR 1736139

[ES83] Paul Erdös and Endre Szemerédi, *On sums and products of integers*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 213–218. MR 820223

[GE13] Endre Szabò György Elekes, *On triple lines and cubic curves — the orchard problem revisited*, Available at https://arxiv.org/abs/1302.5777.

[Giu02] Massimo Giulietti, *On plane arcs contained in cubic curves*, Finite Fields Appl. **8** (2002), no. 1, 69–90. MR 1872792

[GK15] Larry Guth and Nets Hawk Katz, *On the Erdös distinct distances problem in the plane*, Ann. of Math. (2) **181** (2015), no. 1, 155–190. MR 3272924

[GR05] Ben Green and Imre Z. Ruzsa, *Sum-free sets in abelian groups*, Israel J. Math. **147** (2005), 157–188. MR 2166359

[Gri76] Phillip A. Griffiths, *Variations on a theorem of Abel*, Invent. Math. **35** (1976), 321–390. MR 0435074

[GT13] Ben Green and Terence Tao, *On sets defining few ordinary lines*, Discrete Comput. Geom. **50** (2013), no. 2, 409–468. MR 3090525

[GW10] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I*, Advanced Lectures in Mathematics, Vieweg + Teubner, Wiesbaden, 2010, Schemes with examples and exercises. MR 2675155

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977, Graduate Texts in Mathematics, No. 52. MR 0463157

[Hil20] H. Hilton, *Plane algebraic curves*, Available at https://archive.org/details/cu31924001544216.

[Hir83] F. Hirzebruch, *Arrangements of lines and algebraic surfaces*, Arithmetic and geometry, Vol. II, Progr. Math., vol. 36, Birkhäuser, Boston, Mass., 1983, pp. 113–140. MR 717609

[HK85] Abramo Hefez and Steven L. Kleiman, *Notes on the duality of projective varieties*, Geometry today (Rome, 1984), Progr. Math., vol. 60, Birkhäuser Boston, Boston, MA, 1985, pp. 143–183. MR 895153

[HP16] J. W. P. Hirschfeld and E. V. D. Pichanick, *Bounds for arcs of arbitrary degree in finite Desarguesian planes*, J. Combin. Des. **24** (2016), no. 4, 184–196. MR 3487144

[HT15] J. W. P. Hirschfeld and J. A. Thas, *Open problems in finite projective spaces*, Finite Fields Appl. **32** (2015), 44–81. MR 3293405

[IMP11] Alex Iosevich, Hannah Morgan, and Jonathan Pakianathan, *On directions determined by subsets of vector spaces over finite fields*, Integers **11** (2011), A39, 9. MR 3054259

[Jac21] John Jackson, *Rational amusement for winter evenings. longman, hurst, rees, orme and brown, london*, Available at https://archive.org/details/rationalamuseme00jackgoog.

[Joa48] F. Joachimsthal, *Démonstration d'un théorème de mr. steiner.*, Available at hrefhttps://www.degruyter.com/view/j/crll.1848.issue-36/crll.1848.36.95/crll.1848.36.95.xmlhttps://www.degruyter.com/view/j/crll.1848.issue-36/crll.1848.36.95/crll.1848.36.95.xml.

[Joh77] W. W. Johnson, *Classi cation of plane curves with reference to inversion,*, Available at hrefhttps://archive.org/details/jstor-2635474https://archive.org/details/jstor-2635474.

[Jou83] Jean-Pierre Jouanolou, *Théorèmes de Bertini et applications*, Progress in Mathematics, vol. 42, Birkhäuser Boston, Inc., Boston, MA, 1983. MR 725671

[Kel86] L. M. Kelly, *A resolution of the Sylvester-Gallai problem of J.-P. Serre*, Discrete Comput. Geom. **1** (1986), no. 2, 101–104. MR 834051

[KM58] L. M. Kelly and W. O. J. Moser, *On the number of ordinary lines determined by n points*, Canad. J. Math. **10** (1958), 210–219. MR 0097014

[KN73] L. M. Kelly and S. Nwankpa, *Affine embeddings of Sylvester-Gallai designs*, J. Combinatorial Theory Ser. A **14** (1973), 422–438. MR 0314656

[KW91] Victor Klee and Stan Wagon, *Old and new unsolved problems in plane geometry and number theory*, The Dolciani Mathematical Expositions, vol. 11, Mathematical Association of America, Washington, DC, 1991. MR 1133201

[Lan03] Adrian Langer, *Logarithmic orbifold Euler numbers of surfaces with applications*, Proc. London Math. Soc. (3) **86** (2003), no. 2, 358–396. MR 1971155

[LMM+18] Aaron Lin, Mehdi Makhul, Hossein Nassajian Mojarrad, Josef Schicho, Konrad Swanepoel, and Frank de Zeeuw, *On sets defining few ordinary circles*, Discrete Comput. Geom. **59** (2018), no. 1, 59–87. MR 3738336

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR 0065218

[Mak18] Mehdi Makhul, *A family of four-variable expanders with quadratic growth*, Available at A family of four-variable expanders with quadratic growth.

[Mel41] E. Melchior, *über Vielseite der projektiven Ebene*, Deutsche Math. **5** (1941), 461–475. MR 0004476

[Mot51] Th. Motzkin, *The lines and planes connecting the points of a finite set*, Trans. Amer. Math. Soc. **70** (1951), 451–464. MR 0041447

[MRNS15] Brendan Murphy, Oliver Roche-Newton, and Ilya Shkredov, *Variations on the sum-product problem*, SIAM J. Discrete Math. **29** (2015), no. 1, 514–540. MR 3323540

[MRNS17] Brendan Murphy, Oliver Roche-Newton, and Ilya D. Shkredov, *Variations on the Sum-Product Problem II*, SIAM J. Discrete Math. **31** (2017), no. 3, 1878–1894. MR 3691216

[MS18] Mehdi Makhul and Josef Schicho, *An application of bertini theorem*, Available at https://arxiv.org/abs/1809.04930.

[MSG18] Mehdi Makhul, Josef Schicho, and Matteo Gallet, *Probabilities of incidence between lines and a plane curve over finite fields*, Available at https://arxiv.org/abs/1711.06021.

[Mum99] David Mumford, *The red book of varieties and schemes*, Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999.

[Nil13] Fedor Nilov, *New examples of hexagonal webs of circles*, Available at https://arxiv.org/abs/1309.5029.

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. MR 2144974

[Rat87] Jürgen Rathmann, *The uniform position principle for curves in characteristic p*, Math. Ann. **276** (1987), no. 4, 565–579. MR 879536

[Rio02] John Riordan, *An introduction to combinatorial analysis*, Dover Publications, Inc.,, 2002, Reprint of the 1958 original [Wiley, New York; MR0096594 (20 #3077)].

[RNSW18] Oliver Roche-Newton, Ilya D. Shkredov, and Arne Winterhof, *Packing sets over finite abelian groups*, Integers **18** (2018), Paper No. A38, 9. MR 3794028

[Row06] Louis Halle Rowen, *Graduate algebra: commutative view*, Graduate Studies in Mathematics, vol. 73, American Mathematical Society, Providence, RI, 2006. MR 2242311

[RSDZ16a] Orit E. Raz, Micha Sharir, and Frank De Zeeuw, *Polynomials vanishing on Cartesian products: the Elekes-Szabó theorem revisited*, Duke Math. J. **165** (2016), no. 18, 3517–3566. MR 3577370

[RSDZ16b] ———, *Polynomials vanishing on Cartesian products: the Elekes-Szabó theorem revisited*, Duke Math. J. **165** (2016), no. 18, 3517–3566. MR 3577370

[RSS15] Orit E. Raz, Micha Sharir, and József Solymosi, *On triple intersections of three families of unit circles*, Discrete Comput. Geom. **54** (2015), no. 4, 930–953. MR 3416906

[Seg55] Beniamino Segre, *Ovals in a finite projective plane*, Canad. J. Math. **7** (1955), 414–416. MR 0071034

[Ser66] Jean Pierre Serre, *Advanced problem*, American Mathematical Monthly (1966), Available at hrefhttps://www.jstor.org/stable/i314970https://www.jstor.org/stable/i314970.

[Sha94] Igor R. Shafarevich, *Basic algebraic geometry. 1*, second ed., Springer-Verlag, Berlin, 1994, Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid. MR 1328833

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

[SS08a] Shubhangi Saraf and Madhu Sudan, *An improved lower bound on the size of Kakeya sets over finite fields*, Anal. PDE **1** (2008), no. 3, 375–379.

[SS08b] József Solymosi and Konrad J. Swanepoel, *Elementary incidence theorems for complex numbers and quaternions*, SIAM J. Discrete Math. **22** (2008), no. 3, 1145–1148. MR 2424842

[SS13] József Solymosi and Miloš Stojaković, *Many collinear k-tuples with no $k+1$ collinear points*, Discrete Comput. Geom. **50** (2013), no. 3, 811–820.

[ST83] Endre Szemerédi and William T. Trotter, Jr., *Extremal problems in discrete geometry*, Combinatorica **3** (1983), no. 3-4, 381–392. MR 729791

[ST92] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 1171452

[Sta17] The Stacks Project Authors, *Stacks Project*, http://stacks.math.columbia.edu, 2017.

[Syl93] James J. Sylvester, *Mathematical Question 11851*, Educational Times **59** (1893), 385–394.

[Tao14] Terence Tao, *Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory*, EMS Surv. Math. Sci. **1** (2014), no. 1, 1–46. MR 3200226

[Ung82] Peter Ungar, $2N$ *noncollinear points determine at least* $2N$ *directions*, J. Combin. Theory Ser. A **33** (1982), no. 3, 343–347. MR 676751

[Vak06] Ravi Vakil, *Schubert induction*, Ann. of Math. (2) **164** (2006), no. 2, 489–512. MR 2247966

[Vol90] José Felipe Voloch, *Arcs in projective planes over prime fields*, J. Geom. **38** (1990), no. 1-2, 198–200. MR 1061069

[Wal56] Andrew H. Wallace, *Tangency and duality over arbitrary fields*, Proc. London Math. Soc. (3) **6** (1956), 321–342. MR 0080354

[Wal78] Robert J. Walker, *Algebraic curves*, Springer-Verlag, New York-Heidelberg, 1978, Reprint of the 1950 edition. MR 513824

[Wer12] Thomas Rainer Werner, *Rational families of circles and bicircular quartics*, Available at https://d-nb.info/1024608662/34.

[Zha11] Ruixiang Zhang, *On the number of ordinary circles determined by n points*, Discrete Comput. Geom. **46** (2011), no. 2, 205–211. MR 2812505

Mehdi Makhul BIBLIOGRAPHY

Curriculum Vitae

Altenberger Straße 69
4040 Linz, Austria
☎ (0043) 688 607 46 114
✉ mmakhul@risc.uni-linz.ac.at

Personal data

Date of birth March, 19th 1985
Place of birth Borujerd, Iran
Citizenship Iranian

Education

2015–2018 **PhD in Mathematics**, *J. Kepler University, Linz (Austria)*, Thesis: "Algebraic Geometry Techniques in Incidence Geometry", advisor Josef Schicho.

2009–2011 **Master studies in Mathematics**, *University of Shahid, Beheshti, Tehran (Iran)*.

2004–2009 **Bachelor studies in Mathematics**, *Shahrood University of Technology, Shahrood (Iran)*.

Publications

2018 **On sets defining few ordinary circles**, *joint with A.Lin,H.Nassajian Mojarrad,J.Schicho,K.Swanepoel,F.de Zeeuw*, Discrete and Computational Geometry, no 1, pp 59–87.

2018 **A family of four-variable expanders with quadratic growth**, *M.Makhul*, Moscow Journal of Combinatorics and Number Theory, To appear.

2018 **Probabilities of incidence between lines and a plane curve over finite fields**, *joint with Josef Schicho, Matteo Gallet*, Finite Fields and Their Applications, to appear.

2018 **An application of Bertini Theorem**, *joint with Josef Schicho*, submitted.

2018 **Constructions for the Elekes-Szabó and Elekes-Rónyai problems**, *(joint with Oliver Roche-Newton, Audie Warren and Frank de Zeeuw)*, submitted.

2012 **On Uniformly Boundedness of rational Set in the Plane**, *joint with J. Shafaf*, C.R.Acad.Sci. Paris, Ser.I., no 3-4.
121-124

2009 **Problem 11472 (A Generalization of a Putnam problem)**, *M.Makhul*, Problem 11472. The American Mathematical Monthly, 116(10): 941.

Talks

Invited Lecture, IST, Vienna- November 2018

Invited Lecture, EPFL, Lausanne - October 2016

Visit

Mathematics Department in Ghent University September-October 2018

EPFL, Lausanne October 2016

Teaching experiences

2009-2012 Teaching the Training of the "Mathematics Competition for Undergraduate University Students" in Shahrood University of Technology and Shahid Beheshti University.

2012-2014 Teaching the Training of the "Mathematics Olympiad for High School students

Awards

2013 UNESCO-MESR-MINECO-INDIA research school Fellowship: 1000 Euro, for participating in Fourier analysis of group in combinatorics Shillong, India (November 2013)

2013 The Fellowship for participating in Autumn School on Algebraic Geometry Poitiers University France (September 2013)

2012 ICTP-CIMPA Fellowship: 1000 Euro, for participating in Local Analytic Geometry School, the Abdus Salam International Center for Theoretical Physics (ICTP),Lahore, Pakistan.

2009 Silver Medal at 33th Iranian Mathematic Competition.

Language skills

Persian **Native Language**

English **advanced** *self-assessment*