On the Sizes of Unions of Circles over Finite Fields

Nikola Staykov

Under the direction of

Elia Portnoy
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 31, 2020

Abstract

This paper considers unions of circles over finite fields. We generalize an approach used by Oberlin, where in place of unions of lines we consider unions of circles. First we prove that there exists a dimension m, for which a generalized version of the so-called Wolff axiom holds for m-planes and m-spheres without any structural restrictions on the initial set of circles. Then we use this fact to make a construction of higher-dimensional spheres and planes in order to estimate the number of pairs of points on the circles from the initial set. We manage to obtain the bounds $P| \gtrsim |F|^{\frac{3}{2}d+\frac{\beta}{2}+\frac{1}{2}}$ and $|P| \gtrsim |F|^{\frac{3}{2}d+\frac{\beta}{2}+\frac{3}{4}}$ when the set of circles satisfies the d-Wolff axiom. Here $|P|$ is the number of pairs of points on the circles, $|F|$ is the size of the field and $d \in \mathbb{Z}$ and $-1 < \beta \leq 2$ are such that the number of circles in the initial set is $|F|^{3(d-1)+\beta}$.

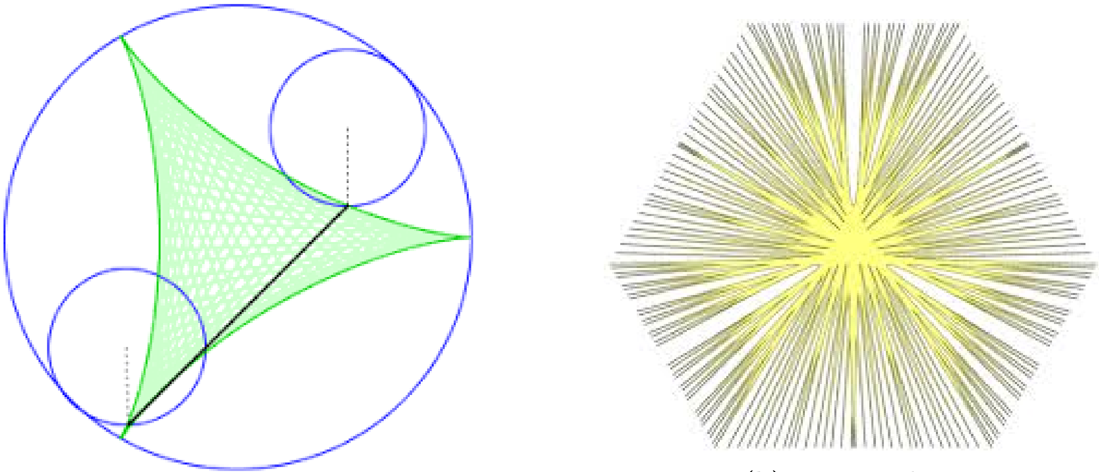
Summary

The goal of this project is to estimate the number of pairs of points in a set of circles over a finite field. We do that by finding an m-sphere which is intersected by many circles, which are not contained in it. We then use the fact that each such circle, along with the initial m-sphere, defines an unique $(m+1)$-sphere. After we divide the intersecting circles into $(m+1)$-spheres we estimate the number of pairs in each one of them in order to generalize the results. That way we obtain information about the number of pairs of points without any structural restrictions, using the fact that they appear on their own.

1 Introduction

The original Kakeya problem, proposed in 1917 [1], asks the following:

Kakeya's Problem. *What is the least area required to continuously and fully rotate a needle of unit length in the plane?*



(a) Deltoid

(b) Besicovitch set

Figure 1: Examples of solutions to the Kakeya problem

A circle with unit diameter is one possible solution to the Kakeya Problem, but it is not the optimal one. The deltoid from Figure 1a for example has half its area and is still a solution. Besicovitch [1] showed that a solution of arbitrarily small area can be constructed. Figure 1b depicts one set constructed with his method. In 1999 Wolff [2] proposed a version of the problem for finite fields. Instead of area, we are trying to find the least number of points to form a line in every direction in a finite vector space. The problem became known as the Finite field Kakeya Conjecture. With $\gtrsim$ we will denote an inequality up to a constant[1].

[1] Throughout the whole paper we can consider q that is substantially bigger than any multiplicative constants independent of q.

Conjecture 1.1 (Wolff, 1999)**.** *Let $\mathbb{F}_q^n$ be an n-dimensional finite space over $\mathbb{F}_q$. If L is a set of lines in $\mathbb{F}_q^n$ and L contains a line in every direction, then the number of points on the lines is $\gtrsim q^n$, the constant depends only on n.*

There the author introduces an axiom, which captures some of the fundamental properties of a Kakeya set:

Axiom (Wolff, 1999)**.** *Let $\mathbb{F}_{p^r}$ be a finite field with p^r elements and let $\mathbb{F}_{p^r}^n$ be an n-dimensional vector space over $\mathbb{F}_{p^r}$, where p is a prime and r is a positive integer. A collection $\mathcal{L}$ of lines in $\mathbb{F}_{p^r}^n$ is said to obey the Wolff axiom if for each $2 \leq k \leq n-1$, every $(k+1)$-dimensional affine subspace $V \subset \mathbb{F}_{p^r}^n$ contains at most p^{rk} lines in $\mathcal{L}$.*

In 2009 Dvir [3] proved Conjecture 1.1 using the polynomial method. His approach is compared to previous methods and approaches by Larry Guth in Polynomial Methods in Combinatorics [4]. Previous to the polynomial method approach, Wolff's axiom [2] played a major role in acquiring lower bounds for the finite field Kakeya problem (Conjecture 1.1). In [5] Oberlin considered unions of lines in $\mathbb{F}^n$ without any structural hypothesis, as opposed to the finite field Kakeya problem. He provided a tight bound for the number of points on the lines. We are interested in a similar approach to bounding the number of points in a set of circles in $\mathbb{F}^n$.

In Section 2 we provide the definitions and preliminary results needed in the latter parts of the paper. We define the notion of a k-sphere in $\mathbb{F}_q^n$ as well as adapt the concepts *stem* and *hairbrush* used by Wolff in [2] in the context of circles instead of lines. We also introduce the definition of a *page*, which is closely related to the previous two.

In Section 3 the main approach of the paper is thoroughly explained. First we introduce variations of the bush and hairbrush methods adapted for circles. Then we prove the existence of a dimension m, for which the m-dimensional Wolff axiom is not satisfied for a set of m-spheres and planes, but holds for higher-dimensional objects. It is important to notice that

that is true even without any structural restrictions on the initial set of circles. Finally we construct a generalized hairbrush, using an m-sphere or an m-plane for the stem. The pages of this hairbrush are $(m+1)$-planes and $(m+1)$-spheres. Using the generalized Wolff axiom we apply induction to the pages in order to obtain a bound for the number of pairs of points on the circles. We prove the main result of the paper, namely that for a set of circles $\mathcal{C}$ with cardinality $|F|^{3(d-1)+\beta}$ for some integer d and $-1 < \beta \leq 2$ we have $\gtrsim |F|^{\frac{3}{2}d+\frac{\beta+1}{2}}$ pairs of points. Furthermore if $\mathcal{C}$ satisfies the d-Wolff axiom we have $\gtrsim |F|^{\frac{3}{2}d+\frac{\beta}{2}+\frac{3}{4}}$ pairs of points.

In Section 4 we summarize the results of the paper, namely Theorem 3.7. Furthermore we show the achieved improvement over the results obtained from the Bush argument.

In Section 5 we discuss possible directions for future development of the project. We propose a conjecture providing a tight bound for the number of pairs given the size of the set of circles.

2 Preliminaries

In this section we introduce definitions, results and ideas integral for the later sections of the paper. We begin with the definition of an m-sphere inside $\mathbb{F}_q^{m+1}$.

Definition 2.1. An *m-sphere* $S_r(c)$ inside the finite field $\mathbb{F}_q^{m+1}$ with center $c = (c_1, \ldots, c_m)$ and radius $r \in F$ is the set of solutions to the equation

$$(x_1 - c_1)^2 + \cdots + (x_{m+1} - c_{m+1})^2 = r.$$

A k-sphere for $k < m$ in $\mathbb{F}_q^{m+1}$ can be obtained by intersecting an m-sphere with a $(k+1)$-plane. This is the only $(k+1)$-plane containing the k-sphere. We note that we call an 1-sphere a *circle* and that a 0-sphere is a pair of points in $\mathbb{F}_q^n$, since it is the intersection of a circle and a line in $\mathbb{F}_q^n$.

The following lemma approximates the number of k-planes inside an m-plane, the set of which is known as a Grassmannian (for proof see Tarizadeh [6] and Oberlin [5]).

Lemma 2.1. *For integers $0 \leq k \leq d$ let the set of k-dimensional subspaces of $\mathbb{F}_q^d$ be $\mathrm{Gr}(d,k)$ and the set of k-planes in $\mathbb{F}_q^d$ be $\mathrm{Gr}'(d,k)$. Then*

$$|G(d,k)| = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{d-1})}{(q^d-1)(q^d-q)\dots(q^d-q^{d-1})}$$

and

$$|Gr'(d,k)| \approx q^{(k+1)(d-k)}.$$

We use the fact that in the previous lemma $|G(d,k)| \approx q^{k(d-k)}$.

In the next lemma we estimate the number of k-spheres inside an m-sphere.

Lemma 2.2. *The number of k-spheres inside an m-sphere in $\mathbb{F}_q^n$ is $\approx q^{(k+2)(m-k)}$.*

Proof. A k-sphere is contained in an unique $(k+1)$-plane and an m-sphere in an unique $(m+1)$-plane respectively. Intersecting a $(k+1)$-plane in the $(m+1)$-plane containing the m-sphere with the said m-sphere, we get an unique k-sphere. Therefore what we want is the number of $(k+1)$-planes inside an $(m+1)$-plane. By Lemma 2.1 it is $\approx q^{(k+2)(m-k)}$. □

The following result is known as the Lang-Weil [7] bound. Let V be a variety over the finite field $\mathbb{F}_q^n$ of dimension r and degree d. We will denote this with $V = V_{n,r,d}$. We give an estimate for the number of rational points $N = \#V(\mathbb{F}_{\shortparallel})$ of V over.

Theorem 2.3 (Hasse-Weil)**.** *There exists a constant $A(n,d,r)$ depending only on n,d,r such that for any variety $V = V_{n,d,r}$ defined over a finite field $\mathbb{F}_q^n$ we have*

$$|N - q^r| \leq \delta q^{r-\frac{1}{2}} + A(n,d,r)q^{r-1},$$

where $\delta = (d-1)(d-2)$.

Applying the result to a sphere as previously defined gives us an estimate for the number of its rational points. A k-sphere is defined by a variety of dimension k and therefore the number of rational points on it is $\approx q^k$.

We now provide definitions for a *stem*, *hairbrush* and a *page*, which are integral to the construction considered in the paper. These definitions are inspired by the construction proposed by Oberlin for lines and planes in [5] and Wolff's approach in [2]. The intuitive meaning behind the names comes from their usage in the calssical problem by Wolff for lines but we maintain for consistency with [5, 2].

Definition 2.2. Let $\mathcal{C}$ be a set of circles in $\mathbb{F}_q^n$ and P be the set of points on those circles. For an m-sphere or an m-plane $S \subset P$ we define a *hairbrush* with a *stem* S as:

$$\{c \in \mathcal{C} : |c \cap S| = 2,\ c \not\subset S\}.$$

In other words this is the collection of circles that intersect the stem in precisely 2 points. Furthermore, we call each $(m+1)$-plane or $(m+1)$-sphere, containing the stem, a *page*.

We note that if the stem is an m-plane all pages are $(m+1)$-planes and if the stem is an m-sphere all pages except one are $(m+1)$-spheres. In this case the $(m+1)$-plane containing the m-sphere is also a page.

3 Circles and spheres in finite fields

In this section we generalize some of the results in [5] with respect to circles and m-spheres instead of lines and m-planes.

Lemma 3.1. *Suppose we have circles $c_1, \dots, c_m$ in $\mathbb{F}_q^n$ and $m < \frac{q}{2}$. Then*

$$\left| \bigcup_{j=1}^{m} c_j \right| \geq \frac{qm}{2}.$$

Proof. Each two circles intersect in at most 2 points. Suppose we add the circles one by one. Then

$$\left| \bigcup_{j=1}^{m} c_j \right| \geq q + (q-2) + \cdots + (q - 2(m-1)) = qm - (m-1)m \geq \frac{qm}{2}.$$

□

The following is a modified version of the Bush argument adapted for circles (see [4]).

Lemma 3.2 (Bush argument)**.** *Suppose we have circles $c_1, \ldots, c_M$ in $\mathbb{F}_q^n$. Let $P = \{p : p \in c_j\}$ for some j and $Q = \{(x, y) : (x, y) \subset c_i\}$ for some i. Then*

$$|P| \gtrsim qM^{\frac{1}{3}}$$

and

$$|Q| \gtrsim q^2 M^{\frac{1}{2}}.$$

Proof. Let $P_{c_j} = \{p : p \in c_j\}$. From Theorem 2.3 $|P_{c_j}| \approx q$ for each $j = 1, \ldots, M$. The number of doubles $(C_i, q) : q \in Q$ is Mq^2 since each circle generates $\approx q^2$ doubles. Therefore there exists a pair $q \in Q$, which participates in at least $\dfrac{Mq^2}{|Q|}$ doubles and therefore circles. Two circles may intersect in at most two points and each circle contains $\approx q$ points. Noting that $|Q| \leq |P|^2$ we get $|P| \gtrsim \dfrac{Mq^3}{|P|^2}$, hence $|P| \gtrsim M^{\frac{1}{3}} q$. Similarly $|Q| \gtrsim \dfrac{Mq^4}{|Q|}$, hence $|Q| \gtrsim M^{\frac{1}{2}} q^2$. □

One of the fundamental tools used in this paper is the hairbrush argument. The idea is similar to that used by Oberlin in [5], but we apply it with respect to circles instead of lines.

Theorem 3.3 (Hairbrush argument)**.** *Suppose we have circles $c_1, \cdots, c_M$ in $\mathbb{F}_q^n$ and there are $\leq \dfrac{q}{2}$ circles in each 2-plane and 2-sphere. Then*

$$\left| \bigcup_{j=1}^{M} C_j \right| \gtrsim q^{5/3} M^{1/3}.$$

Proof. First we will find a hairbrush with $\dfrac{q^4 M}{2|P|^2}$ circles. Let $\mathcal{C} = \{c_i\}$ and $\mu(x, y)$ be the number of circles, containing $(x, y) \in P^2$. We know that

$$\sum_{x,y} \mu(x, y) \approx q^2 M. \tag{1}$$

Consider the quadruples $(c_i, c_j, x, y) \in \mathcal{C} \times \mathcal{C} \times P \times P$, where $(x, y) = c_i \cap c_j$. The number of triples is $\sum_p \mu(p)^2$, but from Jensen and (1) we get $\sum_p \mu(p)^2 \geq \dfrac{q^4 M^2}{|P|^2}$. Therefore there exists a stem $c_i \in \mathcal{C}$ with a hairbrush of size at least $\dfrac{q^4 M}{2|P|^2}$. Consider all 2-spheres containing c_i and

the unique 2-plane containing c_i. Each circle from the hairbrush is in exactly one 2-sphere or in the said 2-plane. For every page s we denote with $H(s)$ the number of circles from the hairbrush in s. We know that $\sum_s |H(s)| \geq \dfrac{q^4 M}{2|P|^2}$.
From the problem statement we know that $|H(s)| \leq \dfrac{q}{2}$ for each s and therefore we can apply Lemma 3.1 for each page. We get that the number of points in $s \backslash c_i \gtrsim |H(s)|q$. Therefore $|P| \geq \sum_s |H(s)|q \gtrsim \dfrac{q^5 M}{|P|^2}$. This implies $|P| \gtrsim q^{5/3} M^{1/3}$. □

Now we introduce a generalized version of the Wolff axiom, concerning higher-dimensional objects.

Axiom. *Consider a set of circles $\mathcal{C}$ in the finite field $\mathbb{F}_q^n$. We say that $\mathcal{C}$ satisfies the m-Wolff axiom for some $m \leq n$ if for every m-sphere or m-plane S*

$$|\{c \in \mathcal{C} :\subset S\}| \leq q^{3(m-1)-1}.$$

The following lemma shows that even without any structural hypothesis we can find a dimension m, for which a significantly large (with respect to the original set of circles) subset of the initial set circles is concentrated into a number of m-spheres and m-planes. From this set of m-spheres and m-planes we later choose the stem of our modified hairbrush.

Lemma 3.4. *Let $\mathcal{C}$ be a collection of k-spheres in $\mathbb{F}_q^n$ and suppose d is a nonnegative integer with $k \leq d \leq n$. There is an integer m with $k \leq m \leq d$, a collection of m-spheres and m-planes $S_1, \ldots, S_N$, and collections of k-spheres $\mathcal{C}_{S_1}, \ldots, \mathcal{C}_{S_N}$ such that*

a) $\mathcal{C}_{S_i} \cap \mathcal{C}_{S_j} = \varnothing$ for all distinct i and j;
b) $\mathcal{C}_{S_i} \subset \mathcal{C}$ for all i and $c \subset S_i$ for $c \in \mathcal{C}_{S_i}$;
c) if $m > k$ then $|\mathcal{C}_{S_i}| \geq q^{(k+2)(m-k)-1}$;
d) if $m = k$ then $|\mathcal{C}_{S_i}| = 1$;
e) letting $\mathcal{C}^m = \cup_i \mathcal{C}_{S_i}$, we have $|\mathcal{C}^m| \geq 2^{-(d-m+1)}|\mathcal{C}|$;
f) if $m < m' \leq d$ then for every m'-sphere or m'-plane S the m'-Wolff axiom holds.

Proof. We set $\mathcal{C}^{*,d+1} = \mathcal{C}$ and go through the following procedure starting with $m = d$:

1. Set U to be the union of all collections of k-spheres $\mathcal{C}_{S_1}, \dots, \mathcal{C}_{S_j}$ we have chosen at this point (possibly 0);

2. If there is an m-sphere or an m-plane S_{j+1}, for which
$$|\{c \in \mathcal{C}^{*,m+1} \backslash U : c \subset S_{j+1}\}| > q^{(k+2)(m-k)-1},$$
we set
$$\mathcal{C}_{S_{j+1}} = \{c \in \mathcal{C}^{*,m+1} \backslash U : c \subset S_{j+1}\};$$

3. Repeat steps one and two until no longer possible;

4. Set $\mathcal{C}^{*,m} = \mathcal{C}^{*,m+1} \backslash U$.

If $|\mathcal{C}^{*,m}| < \dfrac{|\mathcal{C}^{*,m+1}|}{2}$ then e) is satisfied and we are done. Otherwise we continue with $m-1$. If we reach $m = k$ let $S_1, \dots, S_N$ be an enumeration of $\mathcal{C}^{*,k+1}$. We set $\mathcal{C}_{S_i} = \{S_i\}$ and we are done. □

The next lemma allows us to divide the set of circles in a hairbrush. If the stem is an m-plane, the pages will be $(m+1)$-planes. If the stem is an m-sphere, all the pages except one will be $(m+1)$-spheres, but we must also consider the $(m+1)$-plane containing the stem as a possible page.

Lemma 3.5. *Suppose that S is an m-sphere or an m-plane in $\mathbb{F}_q^n$ and consider a hairbrush with stem S. Then we can find pages $Q_1, \dots, Q_N$, such that for all pairs p and circles c satisfying*

a) $p \subset c$,
b) $|c \cap S| = 2$,
c) $p \cap S = \varnothing$

we have $c \subset T_i$ for some i and $p \not\subset T_{i'}$ for $i' \neq i$.

Proof. First let S be an m-sphere. We will use the fact that an m-sphere is defined by $m+1$ points if they do not lie in the same $(m+1)$-plane. Two $(m+1)$-spheres intersect in at most an m-sphere. Therefore if we only consider two $(m+1)$-spheres Q_i and Q_j, containing S, we have $Q_i \cap Q_j = S$. Furthermore for each circle c such that $|c \cap S| = 2$ there exists an unique $(m+1)$-sphere or an $(m+1)$-plane Q_i such that $S \subset Q_i$ and $c \subset Q_i$. Consider $m+1$ points on S and one point $x \in S \backslash c$. We know that x exists since $|c \cap S| = 2$ and c is defined by 3 points. If c is in the same $(m+1)$-plane as S, then we will consider it as a page instead of an $(m+1)$-sphere. These $m+2$ points define an unique page since they are not in the same $(m+1)$-plane. Therefore we can find the Q_i's as desired. Now if S is an m-plane we go through the same operation, but all the pages are going to be $(m+1)$-planes. an $(m+1)$-plane is defined by $(m+2)$-points and we have $|c \cap S| = 2$ for each c. Therefore each circle lies in an unique page. □

The next lemma provides us with a simple tool to estimate the number of rational points on a collection of m-spheres and m-planes, given a restriction on the number of m-dimensional objects.

Lemma 3.6. *Suppose that $\mathcal{C}$ is a collection of m-spheres and m-planes(possibly only one of them), $\boldsymbol{P}$ is a collection of $(k-1)$-spheres such that for each $c \in \mathcal{C}$*

$$|\{p \in \boldsymbol{P} : p \subset c\}| \geq M,$$

and

$$|\mathcal{C}| q^{(k+1)(m-k)} \leq M. \tag{2}$$

Then

$$|\boldsymbol{P}| \gtrsim |\mathcal{C}| M. \tag{3}$$

Proof. For each $c \in \mathcal{C}$, let $\mathbf{P}_c = \{p \in P : p \in c\}$. We enumerate $\mathcal{C} = c_1, \ldots, c_{|\mathcal{C}|}$. Then for each $n \leq |\mathcal{C}|$

$$\begin{aligned}|\mathbf{P}| &\geq \sum_{j=1}^{n} |\mathbf{P}_{c_j}| - \sum_{j=1}^{n} \sum_{j'<j} |\mathbf{P}_{c_j} \cap \mathbf{P}_{c'_j}| \\ &\geq \sum_{j=1}^{n} M - \sum_{j=1}^{n} 2K(j-1)q^{(k+1)(m-k)}.\end{aligned}$$

The second inequality holds because two m-spheres intersect at most in an $(m-1)$-sphere and each $(m-1)$-sphere contains $q^{(k+1)(m-k)}$ $(k-1)$-spheres. By (2) we can now choose $n \approx \dfrac{|\mathcal{C}|}{2K}$ in order to obtain (3). □

The next theorem is the main result of the paper. We use the previous lemmas and results to find a lower bound for the number of pairs on a set of circles of fixed cardinality. If the set of circles satisfies the generalized Wolff axiom, we provide an improved bound.

Theorem 3.7. *Suppose $d \geq 1$ is an integer, $0 < \gamma$ and $\lambda \leq 1$. Let $-1 \leq \beta \leq 2$ and $\mathcal{C}$ is a collection of circles in $\mathbb{F}_q^n$. Suppose that*

$$|\mathcal{C}| \geq \gamma q^{3(d-1)+\beta}$$

and P is a collection of pairs of points in $\mathbb{F}_q^n$ satisfying

$$|\{p \in P : p \in c\}| \geq \lambda q^2$$

for every $c \in \mathcal{C}$. Then we have for some K depending on d, γ, λ,

$$|P| > K q^{\frac{3}{2}d + \frac{\beta}{2} + \frac{1}{2}}.$$

If the d-Wolff axiom is satisfied we have

$$|P| > K q^{\frac{3}{2}d + \frac{\beta}{2} + \frac{3}{4}}.$$

Proof. We are going to do the proof by induction on d.

For the base case when $d = 1$ we apply Lemma 3.6 with $m = 1, k = 1$. We select a subset of $\mathcal{C}$ with size $\min(\lambda, \gamma)q^{\beta}$. The M from Lemma 3.6 in this case is λq^2. We know that $|\{p \in P : p \in c\}| \geq \lambda q^2$ from the proposition statement.

After applying Lemma 3.4 to $\mathcal{C}$, we obtain m-spheres and m-planes $S_1, \ldots, S_N$. Note that if C satisfies the d-Wolff axiom respectively, then we must have $m < d$.

Case 1: $m = d$. We directly apply the Bush argument(Lemma 3.2) to the set of circles. It has size $|\mathcal{C}| = q^{3(d-1)+\beta}$ and therefore we get

$$|P| \gtrsim q^{\frac{3}{2}d+\frac{\beta}{2}+\frac{1}{2}},$$

as we wanted.

Case 2: $m < d$. First we will construct a set of lines and points using a "popularity" argument. We fix a constant C, which is to be determined later. Let

$$\mathbf{P}^{\#} = \{p \in P : |\{c \in \mathcal{C} : p \in c\}|\} \gtrsim Cq^{\frac{3d}{2}+\frac{\beta}{2}-\frac{7}{4}}$$

and

$$\mathcal{C}^{\#} = \{c \in \mathcal{C} \; |\{p \in P^{\#} : p \in c\}| \gtrsim \frac{1}{4}\lambda q^2\}.$$

Letting $\mathcal{C}^m = \cup_j C_{S_j}$ we then have either

$$|P| \geq \frac{\frac{1}{2}\lambda q^2 |\mathcal{C}^m|}{Cq^{\frac{3}{2}d+\frac{\beta}{2}-\frac{7}{4}}} \tag{4}$$

or

$$|\mathcal{C}^{\#}| \geq \frac{1}{8}|\mathcal{C}^m|. \tag{5}$$

If (4) is satisfied then we are done because the right hand side is greater than $q^{\frac{3}{2}d+\frac{\beta}{2}+\frac{3}{4}}$. Now suppose (4) does not hold. We will prove that then (5) is satisfied. Set

$$I = \{(p, c) : p \in \mathbf{P}_c, c \in C^m\},$$

where $\mathbf{P}_c$ is a subset of the pairs in c and $\lambda q^2 \leq |\mathbf{P}_c| < 2\lambda q^2$. Now let

$$I' = \{(p, c) : p \in \mathbf{P}_c \backslash P^{\#}, c \in \mathcal{C}^m\}.$$

Now we have

$$|I'| < Cq^{\frac{3d}{2}+\frac{\beta}{2}-\frac{7}{4}}|\mathbf{P}| < \frac{1}{2}|I|$$

because (4) does not hold. Therefore

$$|\{(p, c) : p \in \mathbf{P}_c \cap \mathbf{P}^{\#}, c \in \mathcal{C}^m\}| \geq \frac{1}{2}\lambda q|\mathcal{C}^m|.$$

Now since

$$|\{(p, c) : p \in \mathbf{P}_c \cap \mathbf{P}^{\#}, c \in \mathcal{C}^m \backslash \mathcal{C}^{\#}\}| \leq \frac{1}{4}\lambda q|\mathcal{C}^m|$$

because of the definition of $C^{\#}$, we have

$$|\{(p,c) : p \in \mathbf{P}_c \cap \mathbf{P}^{\#}, c \in \mathcal{C}^{\#}\}| \geq \frac{1}{4}\lambda q|\mathcal{C}^m|.$$

This gives us (5) by the upper bound on $|\mathbf{P}_c|$. After we acquire a "big" set of "populated" lines and a stem (m-sphere or m-plane), we need to use induction for the circles on each page. This is where the problem arises.

Let $\mathcal{C}^{\#}_{R_j} = \mathcal{C}_{R_j} \cap L^{\#}$ and $P^{\#}_{R_j} = R_j \cap P^{\#}$,

$$\mathcal{C}'_{R_j} = \{c \in \mathcal{C}^m : |c \cap R_j| = 2\},$$

and

$$P'_{R_j} = P \backslash R_j.$$

Fix j so that $|\mathcal{C}^{\#}_{R_j}| \gtrsim |C_{R_j}|$. We use the case $d' = d - 1,\ \beta = 2$ and the inductive hypothesis to get

$$\mathbf{P}^{\#}_{R_j} > q^{\frac{3}{2}m}.$$

For each pair $p \in \mathbf{P}^{\#}_{R_j}$, there are $\geq Cq^{\frac{3}{2}d+\frac{\beta}{2}+c}$ circles from $\mathcal{C}^m$ intersecting p. We have $\lesssim q^{m-1}$ of those circles contained in R_j. Therefore

$$|\{c \in C'_{R_j} : p \in c\}| \geq \frac{1}{2}q^{\frac{3}{2}d+\frac{\beta}{2}-\frac{7}{4}}$$

for a large enough C. Therefore

$$\begin{aligned}|\mathcal{C}'_{R_j}| &\gtrsim |\mathbf{P}^{\#}_{R_j}|q^{\frac{3}{2}d+\frac{\beta}{2}-\frac{7}{4}}\\ &\gtrsim q^{\frac{3}{2}d+\frac{3}{2}m+\frac{\beta}{2}-\frac{7}{4}}\end{aligned}$$

We now divide $\mathbb{F}_q^n$ into $(m+1)$-pages using Lemma 3.5, all of them containing R_j. Let

$$\mathcal{C}_i = \{c \in \mathcal{C}'_{R_j} : c \subset T_i\},$$

$$P_i = \{p \in P'_{R_j} : p \in T_i\}.$$

Then

$$\begin{aligned}|P| &\geq \sum_i |P_i| \\ &\gtrsim \sum_i \frac{|\mathcal{C}_i|}{q^{\frac{3}{2}m-\frac{5}{2}}} \\ &\geq \frac{|\mathcal{C}'_{R_j}|}{q^{\frac{3}{2}m-\frac{5}{2}}} \\ &\gtrsim q^{\frac{3}{2}d+\frac{b}{2}+\frac{3}{4}}.\end{aligned}$$

In the second inequality we used the fact that the circles in each page satisfy the m-Wolff. Because of that we can find $m' \leq m$ and β' such that the number of circles in the page is $q^{3(m'-1)+\beta'}$ and apply induction to estimate the number of pairs in the page. □

4 Conclusion

We generalized the bush and hairbrush arguments, proposed by Wolff in [2] for lines, with respect to circles. Then we recreated the construction of a generalized bush argument Oberlin proposed in [5] again with respect to circles and k-spheres instead of lines and k-planes as in the original paper. Let $\mathcal{C}$ be a set of circles in $\mathbb{F}_q^n$ and let $|\mathcal{C}| = q^{3(d-1)+\beta}$ for some integer d and $-1 < \beta \leq 2$ and P be the set of pairs of points on those circles. The bush argument yields

$$|P| \gtrsim q^{\frac{3}{2}d+\frac{\beta}{2}+\frac{1}{2}}.$$

We obtained an improved bound for the number of pairs $|P|$ when a d-Wolff axiom holds for $\mathcal{C}$, namely

$$|P| \gtrsim q^{\frac{3}{2}d+\frac{\beta}{2}+\frac{3}{4}}.$$

5 Future Work

We propose the following conjecture for a tight bound for the number of pairs of points in a set of circles.

Conjecture 5.1. *Let $\mathcal{C}$ be a set of circles in $\mathbb{F}_q^n$ and let $|\mathcal{C}| = q^{3(d-1)+\beta}$ for some integer d and $-1 < \beta \leq 2$. Then if P is the set of pairs of points on those circles*

$$|P| > Kq^{2d+\max(0,\beta)}.$$

One case when the proposed boundary is tight is when $\beta = 0$. Then we can fill up a d-plane with all possible circles which are exactly $q^{3(d-1)}$. Another possible area of further research is expanding the type of objects to random varieties, including such of higher degrees. An initial bound should be achievable with similar methods to ours, as we have not used neither the center, nor the radius in an integral way. A problem may arise though with determining the number of rational points on the intersections of more widely-defined varieties.

6 Acknowledgments

I want to express my gratitude towards Elia Portnoy for the inspiring and fruitful mentorship. I am also grateful to Dr.Tanya Khovanova and Dr. Jenny Sendova for the irreplaceable help throughout writing this paper. I am also very grateful for the support of the whole RSI community, especially my counselor group. I extend my gratitude towards Alex Goo for the useful tips and feedback. I highly appreciate the efforts of CEE, RSI and MIT math and thank them as well as all the sponsors for providing me with the opportunity to develop this project.

References

[1] A. S. Besicovitch. The kakeya problem. *The American Mathematical Monthly*, 70(7):697–706, 1963.

[2] T. Wolff. Recent work connected with the kakeya problem. *Prospects in mathematics (Princeton, NJ, 1996)*, 2(129-162):4, 1999.

[3] Z. Dvir. On the size of kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22(4):1093–1097, 2009.

[4] L. Guth. *Polynomial methods in combinatorics*, volume 64. American Mathematical Soc., 2016.

[5] R. Oberlin. Unions of lines in f^n. *Mathematika*, 62(3):738–752, 2016.

[6] A. Tarizadeh. Grassmannians over a finite field. *arXiv preprint arXiv:1911.12622*, 2019.

[7] S. Lang and A. Weil. Number of points of varieties in finite fields. *American Journal of Mathematics*, 76(4):819–827, 1954.