On the size of unions of lines in $\mathbb{F}^n$ satisfying the Wolff axiom

Kristian Georgiev

under the direction of
Hong Wang
Massachusetts Institute of Technology

Research Science Institute
July 28, 2015

Abstract

The paper deals with finding unions of lines in $\mathbb{F}_{p^{2k}}^n$ which obey the Wolff axiom and have minimal size. We provide an extension of the constructions for $\mathbb{F}_{p^{2k}}^3$, obtained by Tao in 2002, to a construction for $\mathbb{F}_{p^{2k}}^n$. We determine the size of the union of lines in our construction in $\mathbb{F}_{p^{2k}}^n$ to be $O\left(p^{1.6kn}\right)$. We prove that our construction obeys the Wolff axiom up to a heuristically negligible number of lines. The next step would be to prove rigorously that this number is indeed negligible.

Summary

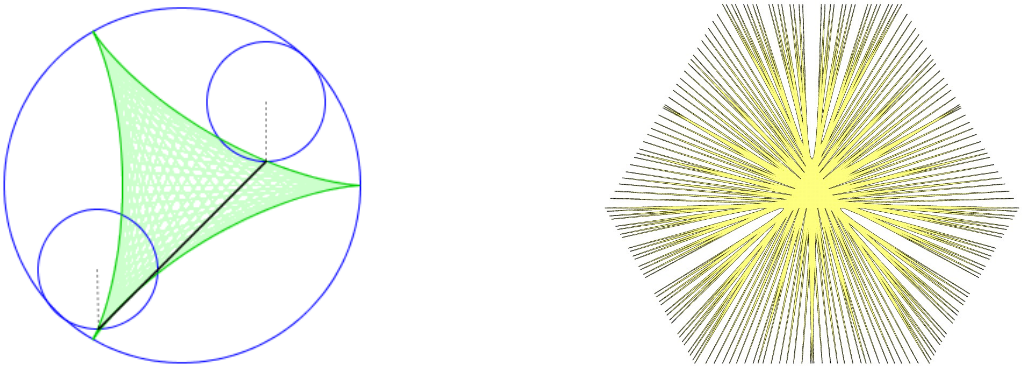
In our project, we examine sets of lines in certain classical objects in abstract algebra. The goal is to evaluate the minimal size of sets of lines which satisfy certain conditions formulated by Thomas Wolff in 1995. We do that by determining the smallest possible surface that contains the whole set of lines. We find a general form of that surface in n dimensions, which has applications in physics. It turns out that the size of our set is significantly smaller than expected. This result may give helpful insight on how to approach problems with similar formulation.

1 Introduction

A problem posed by Sochi Kakeya in 1917 raised a great interest among the mathematical community because of its simple formulation and unexpected development.

> **Kakeya needle problem.** *What is the least amount of area required to continuously rotate a needle of unit length in the plane by a full rotation?*

It was conjectured that a deltoid (Figure 1a) that is inscribed in a circle of diameter $3/2$ units was the optimal solution. Its area is half of the area of the unit circle. It turned out, however, that such figures may have arbitrarily small area (Figure 1b), as shown by Besicovitch [1] in 1928.



(a) Deltoid

(b) Besicovitch set

Figure 1: Sets satisfying the Kakeya problem [2]

He also showed that for $n \geq 2$ there are subsets of $\mathbb{R}^n$ of measure zero which contain a unit line segment in each direction. Such sets are called *Besicovitch sets*. This observation led to the Kakeya conjecture, which states the following.

Kakeya conjecture. *A Besicovitch set S in $\mathbb{R}^n$ must have (Hausdorff or Minkowski) dimension at least n.*

This conjecture helped initiate the field of mathematics known as *geometric measure theory*. Besicovitch has proven the conjecture for $n = 2$, but it remains open in higher dimensions. In 1999, Wolff posed the finite field analogue to the Kakeya conjecture. The discrete nature of the finite fields simplifies the problem and removes several technicalities. Thus, proving the conjecture over finite fields may give a clearer idea of how to proceed in the original conjecture. The finite field Kakeya conjecture was proven by Zeev Dvir [3] in 2008.

In [4] Wolff proposes a conjecture similar to the finite field Kakeya conjecture in which the condition "there is a line in every direction" is replaced with the condition "there are at most p^{kd} lines in every $(k+1)$-plane." The latter condition is known as the *Wolff axiom.*

Wolff axiom. Consider the finite field $\mathbb{F}_{p^d}$ of order p^d in the n-dimensional space $\mathbb{F}_{p^d}^n$, where p is a prime and d is a positive integer. A collection $\mathcal{L}$ of lines in $\mathbb{F}_{p^d}^n$ is said to obey the *Wolff axiom* if for each $2 \leq k \leq n-1$, every $(k+1)$-dimensional affine subspace $V \subset \mathbb{F}_{p^d}^n$ contains at most $O(|\mathbb{F}_{p^d}|^k)$ lines in $\mathcal{L}$. [5]

The focus of interest in our research is the following problem.

Conjecture 1.1 **(Main Problem).** *Let $\mathcal{L} = \{l_i\}$ $(i = 1, 2, \ldots, p^{dn-d})$ be a set of lines in $\mathbb{F}_{p^d}^n$ obeying the Wolff axiom. Let $\Sigma = \cup l_i$. Then the asymptotic size of Σ is of order p^{dn}. That is, $|\Sigma| = O(p^{dn})$.*

Now note that families of lines that lie in different directions (Besicovitch sets) obey the Wolff axiom, although the converse is not true in general. Consequently, a lower bound for the sets obeying the Wolff axiom provides a lower bound for Besicovitch sets as well. This strategy has been used by Thomas Wolff [4] in 1995 and Terence Tao [5] in 2002. However, in 2008 Dvir [3] provided a stronger bound for Besicovitch sets than the ones in [4] and [5] without referring to sets satisfying the Wolff axiom.

Wolff provided a lower bound for the size of such sets [4] in 1995 using the *hairbrush argument.* The main goal of our project is to determine whether the hairbrush argument bound (discussed in Section 3) is sharp in dimensions higher than four. An additional motivation to tackle this problem is a statement of Tao in [5, p. 2]:"It seems of interest to extend this construction to higher dimensions, though perhaps the bound of $|F|^{\frac{n+2}{2}}$ is not necessarily sharp for large n." Here *this construction* refers to the construction showing that the hairbrush argument bound is sharp in four dimensions and "$|F|^{\frac{n+2}{2}}$" is the bound obtained by the hairbrush argument.

We are interested in the asymptotic behavior of $|\Sigma|$ as p tends to infinity, i.e. in finding the exponent ψ for which

$$|\Sigma| = O(p^{\psi}).$$

To this goal we introduce in Section 2 some preliminary definitions and theorems that we shall need throughout this paper. We present a lower bound on the size of Σ obtained by Wolff's hairbrush argument by T. Wolff in Section 3. In Section 4 we discuss the previous results in this area, including constructions for vector spaces of dimension three derived from the *Heisenberg group*. We present in Section 5 a construction based on the constructions in Section 4 for vector spaces of dimension four which obeys the Wolff axiom. Then we generalize the construction to dimension n. The proof that this generalized construction satisfies the Wolff axiom, however, is up to a heuristically negligible number of lines for now.

2 The Frobenius automorphism

General definitions and theorems about finite fields are introduced in Appendix A.

We now introduce the Frobenius automorphism, which plays a pivotal role throughout this paper.

Definition 2.1. A mapping $f : \mathbb{F} \to \mathbb{H}$ of the field $\mathbb{F}$ into the field $\mathbb{H}$ is called a *homomorphism* of $\mathbb{F}$ into $\mathbb{H}$ if f preserves the operations of $\mathbb{F}$. If f is a bijection, then f is called an *isomorphism*. An isomorphism of $\mathbb{F}$ onto itself is called an *automorphism*.

Definition 2.2. Let $\mathbb{F}$ be a field of characteristic p. Then the *Frobenius automorphism* on $\mathbb{F}$ is the map $\Phi : \mathbb{F} \to \mathbb{F}$ defined by $\Phi : \alpha \mapsto \alpha^p$.

It is straightforward to check that $\Phi(\alpha\beta) = \Phi(\alpha)\Phi(\beta)$ for each α and β of $\mathbb{F}$. What is more interesting is that the Frobenius map also respects the addition of $\mathbb{F}$.

Proposition 1. *If α, $\beta \in \mathbb{F}$, we have $\Phi(\alpha + \beta) = \Phi(\alpha) + \Phi(\beta)$.*

Proof. $\Phi(\alpha + \beta) = (\alpha + \beta)^p$ where p is the field characteristic. The binomial theorem gives

$$(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k}.$$

Because p is prime, $\binom{p}{k}$ is divisible by p for every $0 < k < p$. Thus, the coefficients of all terms excluding α^p and β^p are divisible by the characteristic p and hence they vanish. It follows that

$$\Phi(\alpha + \beta) = (\alpha + \beta)^p = \alpha^p + \beta^p = \Phi(\alpha) + \Phi(\beta).$$

□

A direct consequence of LemmaA.1 is

Remark. The Frobenius automorphism raised to the power of n fixes all elements of $\mathbb{F}_{p^n}$. In other words, that is, $\Phi(\alpha)^n = \alpha$ for each $\alpha \in \mathbb{F}_{p^n}$.

We use this fact many times throughout the paper and it plays a crucial role in obtaining the results for the cases when the order of the field is an even power of a prime.

Definition 2.3. Let $\mathbb{F}_{p^n}$ be a finite field and $\alpha \in \mathbb{F}_{p^n}$. The powers of $\Phi(\alpha)$, that is, $\Phi(\alpha)^i$, $i = 1, 2, \ldots, n-1$ are called the *Galois conjugates* of α.

Definition 2.4. Let $\mathbb{F}_{p^n}$ be a finite field and $\alpha \in \mathbb{F}_{p^n}$. Define the map $\mathrm{Tr}_p(\alpha) : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ by

$$\mathrm{Tr}_p(\alpha) = \sum_{i=0}^{n-1} \Phi(\alpha)^i.$$

$\mathrm{Tr}_p(\alpha)$ is called the *trace* of α.

Remark. The trace of α is equal to the sum of the Galois conjugates of α and α itself for all $\alpha \in \mathbb{F}_{p^n}$.

Before examining the properties of the trace map, we present a lemma regarding subfields of prime order.

Lemma 2.1. *Let Φ be the Frobenius map and α be an element of the field $\mathbb{F}_{p^n}$. Then $\Phi(\alpha) = \alpha$ if and only if α is an element of the prime subfield $\mathbb{F}_p$.*

A proof of this lemma can be found in [6]. We will use the converse direction of this lemma several times in Section 5. We now introduce the trace map which is used throughout the entire paper.

Lemma 2.2. *For all $\alpha \in \mathbb{F}_{p^n}$, $\mathrm{Tr_p}(\alpha) \in \mathbb{F}_p$.*

Proof. We note that

$$\Phi(\mathrm{Tr_p}(\alpha)) = \sum_{i=1}^{n-1} \Phi(\alpha)^i + \Phi(\alpha)^n$$

and $\Phi(\alpha)^n = \alpha$. Therefore

$$\Phi(\mathrm{Tr}_p(\alpha)) = \mathrm{Tr}_p(\alpha).$$

From Lemma 2.1 we conclude that $\mathrm{Tr}_p(\alpha)$ is an element of $\mathbb{F}_p$. □

We have shown that $\mathrm{Tr}_p(\alpha)$ maps $\mathbb{F}_{p^n}$ onto $\mathbb{F}_p$. The following lemma shows another property of the trace map.

Lemma 2.3. *For all $a, b \in \mathbb{F}_p$ and $\alpha, \beta \in \mathbb{F}_{p^n}$, $\mathrm{Tr_p}(a\alpha + b\beta) = a \cdot \mathrm{Tr_p}(\alpha) + b \cdot \mathrm{Tr_p}(\beta)$.*

The lemma is a direct corollary of Proposition 1 and Lemma 2.2.

Having introduced the definitions and theorems we use throughout the paper, we present the hairbrush argument in the next section.

3 The hairbrush argument

The hairbrush argument was first introduced by Wolff in [4]. It gives a lower bound on the size of unions of lines that satisfy the Wolff axiom.

Theorem 3.1. *Let $\mathbb{F}_{p^d}^n$ be a vector space of dimension n over the finite field $\mathbb{F}_{p^d}$. Let $\mathcal{L}$ be a set of $p^{d(n-1)}$ lines l_i obeying the Wolff axiom and the set of points Σ be $\cup l_i$. Then $|\Sigma| \geq O(p^{\frac{d(n+2)}{2}})$.*

It has been shown by Tao and Mockenhaupt that the hairbrush argument gives the sharp lower bound for $\mathbb{F}_{p^d}^2$, $\mathbb{F}_{p^{2k}}^3$ [7] and $\mathbb{F}_{p^d}^4$ [5], where p is prime and k and d are positive integers. The main idea of the argument is to find the line l_0 in $\mathcal{L}$ that intersects the largest number of lines in $\mathcal{L}$ and to examine the lines which intersect l_0.

The rough idea behind the proof is as follows. Because there should be a large number of intersections between lines of the union, we can consider the line l_0 which intersects the most lines l_i and find the number of points in Σ on the planes in which l_0 lies. The details of the proof can be found in [4].

The hairbrush argument provides us with a non-trivial lower bound which is valid for $\mathbb{F}_{p^d}^n$ for all $n \in \mathbb{N}$.

However, it has not been proven that this bound is sharp in the general case. Constructions have been provided only for vector spaces of dimension $n \leq 4$. The constructions for $\mathbb{F}_{p^d}^3$, which are presented in Section 4, exploit the Heisenberg group and will serve as a basis for our constructions introduced in Section 5. The constructions for $\mathbb{F}_{p^d}^2$ and $\mathbb{F}_{p^d}^4$ are presented in Appendix B and Appendix C, respectively.

4 Heisenberg group and sets derived from it in $\mathbb{F}_{p^d}^3$

The constructions in $\mathbb{F}_{p^d}^3$, where p is prime, have been achieved by T. Tao [7] in 2002 for even d and by J. Ellenberg and M. Hablicsek [8] in 2013 for odd d. We state them without proof. The construction presented by Tao in [7] relies on the Heisenberg group and on the fact that in fields of the type $\mathbb{F}_{p^{2k}}$, the map $\Phi : \alpha \mapsto \alpha^{p^k}$ is an involution. To discuss Tao's construction, we introduce the Heisenberg group.

Definition 4.1. The *Heisenberg group* $\mathbb{H} \in \mathbb{F}_{p^{2k}}^3$ is defined by

$$\mathbb{H} = \left\{(\zeta_1, \zeta_2, \zeta_3) \in \mathbb{F}_{p^{2k}} \quad : \quad \zeta_1 - \zeta_1^{p^k} - \zeta_2\zeta_3^{p^k} + \zeta_2^{p^k}\zeta_3 = 0\right\}.$$

Here is how this group is used in Tao's construction:

Construction for $\mathbb{F}_{p^{2k}}^3$ (Tao). The surface cut out by the polynomial

$$\zeta_1 - \zeta_1^{p^k} - \zeta_2\zeta_3^{p^k} + \zeta_2^{p^k}\zeta_3 = 0$$

has $p^{5k} = q^{5/2}$ points and $p^{4k} = q^2$ lines.

It provides a counterexample to Conjecture 1.1 for $\mathbb{F}_{p^d}^3$ where d is even and proves the sharpness of the hairbrush bound for fields of the type $\mathbb{F}_{p^{2k}}$ in 3 dimensions.

The size of the set of points Σ, containing the union of lines, depends on the structure of the underlying field. The bound $|\Sigma| = O(p^{5d/2})$ derived from the hairbrush argument is sharp only for fields of the type $\mathbb{F}_{p^{2k}}$. This result shows the importance of the field structure.

The main method used to determine the cardinality of Σ is to find a surface contained in $\mathbb{F}_{p^d}^3$ which contains at least p^{2d} lines satisfying the Wolff axiom. The cardinality of Σ then is the number of points in this surface. This method is used by both Tao and by Ellenberg and Hablicsek and it will be the basis of our construction. The latter construct a counterexample to Conjecture 1.1 for $\mathbb{F}_{p^d}^3$ where d is a positive integer.

Construction for $\mathbb{F}_{p^d}^3$ (Ellenberg and Hablicsek)**.** Consider the hypersurface X of $\mathbb{F}_{p^d}^3$ cut out by the polynomial

$$f(\alpha, \beta, \gamma) = \mathrm{Tr}_p(\alpha) + \mathrm{Tr}_p(\beta\gamma^p) - \mathrm{Tr}_p(\beta^p\gamma).$$

It contains p^{3d-1} points and there are p^{2d} lines in X that satisfy the Wolff axiom.

Remark. For a field $\mathbb{F}_{p^d}$, one can find a surface which contains $p^{3d-d/s}$ points, where s is the smallest nontrivial divisor of d, in which there are p^{2d} lines that obey the Wolff axiom. This is possible because a field $\mathbb{F}_{p^d}$ can be represented as a vector space of dimension d/s over $\mathbb{F}_{p^s}$.

In Section 5 we expand the constructions presented in this section to higher dimensions.

5 Sets derived from the Heisenberg group in $\mathbb{F}_{p^d}^n$ for $n > 3$

In this section we examine the sharpness of the bound obtained by the hairbrush argument in vector spaces of dimension $n > 3$. The main goal is to find a series of constructions for smaller n ($n = 4, 5, 6, \ldots$) that follow particular patterns with hope of generalizing them. Thus, we will be able to expand the constructions for vector spaces of arbitrarily large dimension.

We need the following definitions.

Definition 5.1. The *prime dimension* $\dim_p(\mathbb{F}_{p^d}^n)$ of a space $\mathbb{F}_{p^d}^n$ over a finite field $\mathbb{F}_{p^d}$ is defined by $\dim_p(\mathbb{F}_{p^d}^n) = d\cdot(\dim(\mathbb{F}_{p^d}^n))$, provided that a field extension $\mathbb{F}_{p^d}/\mathbb{F}_p$ can be represented as a d-dimensional vector space over $\mathbb{F}_p$.

For instance, $\mathbb{F}_{p^2}^5 = 10$.

In analogy with the Galois conjugates (Definition 2.3) of an element α of $\mathbb{F}_{p^d}$, we define

Definition 5.2. The polynomials

$$(f)^{p^i},\ i = 1, 2, \dots, d-1$$

are the *conjugate polynomials* of the polynomial f with coefficients in $\mathbb{F}_{p^d}$.

Definition 5.3. Let $\mathbb{F}_{p^d}$ be a finite field with $d = a \cdot k$. We define the k-trace of an element $\alpha \in \mathbb{F}_{p^d}$ as

$$\mathrm{Tr}_k(\alpha) = \sum_{i=1}^{a} \alpha^{p^{i \cdot k}}.$$

Remark. We denote α^{p^k} by $\bar{\alpha}$ because the map $\Phi : \alpha \mapsto \alpha^{p^k}$ is an involution in $\mathbb{F}_{p^{2k}}$

We use this notation to describe our constructions more concisely.

Corollary 5.1. *For all* $\alpha \in \mathbb{F}_{p^d}$*, we have* $\mathrm{Tr_k}(\alpha) \in \mathbb{F}_{p^k}$*.*

This is a direct corollary of Lemma 2.2.

5.1 Construction in four dimensions

We start with extending the sets derived from the Heisenberg group to vector spaces of dimension four.

Our construction proves that the hairbrush bound is sharp only for fields of the type $\mathbb{F}_{p^d}$ where d is even. For odd d the size of our construction is no longer equal to the hairbrush bound. For that reason, we build the construction only for fields of that type.

Construction for $\mathbb{F}_{p^{2k}}^4$. Let A be the algebraic variety in $\mathbb{F}_{p^{2k}}^4$ cut out by the polynomial

$$f_A = \mathrm{Tr}_k(\alpha_1) + \mathrm{Tr}_k(\alpha_2) + \mathrm{Tr}_k(\alpha_3) + \mathrm{Tr}_k(\alpha_4) \tag{1}$$

with coefficients in $\mathbb{F}_{p^{2k}}$. If we consider f_A as a map $\mathbb{F}_{p^{2k}} \to \mathbb{F}_{p^k}$, f_A takes every value of $\mathbb{F}_{p^k}$ exactly p^k times. Therefore, A has prime dimension $\dim_p(A) = 2nk - k$ and as a result it contains p^{2nk-k} points. We now find the number of lines that lie in A. However, we consider only the lines that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely. This allows us to parameterize the lines and thus verify the Wolff axiom with less effort. The lines we examine are of the form

$$\mathcal{L}_{(a,b,c,u,v,w)} = \left\{(a,b,c,0) + t(u,v,w,1) \middle| \, t \in \mathbb{F}_{p^d}\right\}. \tag{2}$$

We now parameterize the lines in the surface. We get that $\alpha_1 = a + ut$, $\alpha_2 = b + vt$, $\alpha_3 = c + wt$ and $\alpha_4 = t$. If A contains the lines of the form $\mathcal{L}$, then the quadruples $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ are solutions of equation (1) for any value of t. We get the following constraints from equation (1) for the coefficients c_j of the jth power of t.

$$\begin{cases} c_0 = \mathrm{Tr}_k(a) + \mathrm{Tr}_k(b) + \mathrm{Tr}_k(c) \\ c_{t^p} = u^p + v^p + w^p \\ c_{\bar{t}} = \bar{u} + \bar{v} + \bar{w}. \end{cases} \tag{3}$$

Because the coefficients vanish, we get that $c_0 = c_t = c_{t^p} = c_{\bar{t}} = 0$. We note that $\mathrm{Tr}_k(a) \in \mathbb{F}_{p^k}$ and $\mathrm{Tr}_k(a)$ attains each value of $\mathbb{F}_{p^k}$ exactly p^k times. We also notice that the polynomials determining $c_{\bar{t^i}}$ are conjugate to each other and hence without loss of generality, we examine only c_t (the other equations do not provide new information). In total, for each of a, b, u and v we have p^{2k} choices, for c we have p^k choices and w is fixed by u and v. Altogether, there are $p^{2k} \cdot p^{2k} \cdot p^{2k} \cdot p^{2k} \cdot p^k = p^{9k}$ lines lying in A.

Now, let us consider the the hypersurface B in $\mathbb{F}^4_{p^{2k}}$ cut out by the polynomial

$$f_B = \mathrm{Tr}_k(\alpha_1) + \mathrm{Tr}_k(\alpha_2) + \mathrm{Tr}_k(\alpha_3\bar{\alpha}_4) \tag{4}$$

with coefficients in $\mathbb{F}_{p^{2k}}$. Note that B also contains p^{2nk-k} points. Analogously, we examine only the lines that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely. They are of the form (2). Using analogous techniques, we get the following system

$$\begin{cases} c_0 = \mathrm{Tr}_k(a) + \mathrm{Tr}_k(b) \\ c_{t^p} = u^p + v^p + \bar{c} \\ c_{\bar{t}} = \bar{u} + \bar{v} + c \\ c_{\bar{t}+1} = \mathrm{Tr}_k(w). \end{cases} \tag{5}$$

Here c_{t^i} is the coefficient of t^i, $\alpha_1 = a + ut$, $\alpha_2 = b + vt$, $\alpha_3 = c + wt$, and $\alpha_4 = t$. We note that the polynomials determining c_{t^p} and $c_{\bar{t}}$ are conjugate to each other and again we can examine only c_{t^p} without loss of generality. In total, for a, u and v we have p^{2k} choices, for b and w we have p^k choices, and c is fixed by u and v. Altogether, the hypersurface B contains p^{8k} lines that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely.

Consider the surface C obtained by intersecting A and B. We are interested in the number of points in C and the number of lines that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely in C. The lines, again, are of the form (2). From (3) and (5) we get the following system of equations.

$$\begin{cases} \mathrm{Tr}_k(a) + \mathrm{Tr}_k(b) = 0 \\ \mathrm{Tr}_k(c) = 0 \\ u + v + w = 0 \\ w = c^p. \end{cases} \tag{6}$$

Remark. Only non-conjugate polynomials are included in this system of equations.

Here, for a and u we have p^{2k} choices, for c and v we have p^k choices, and w is fixed by c. Altogether, we have p^{6k} lines lying in C that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely.

The surface C contains fewer lines than either A or B and therefore $C \not\equiv A$ and $C \not\equiv B$. Therefore, from Theorem 6.29 in [9, p. 82] we get that $\dim_p(C) = \dim_p(A) - k = 2nk - 2k$. Hence, C contains p^{2nk-2k} points.

Let us summarize what we have so far. The surface C contains p^{2nk-2k} points and p^{6k}

lines. The hairbrush bound yields that the minimal size of a set obeying the Wolff axiom is $|\Sigma| = O(p^{3d})$. Thus, we have a sufficient number of lines in C and when $d = 2k$ the bound is attained. What is left is only to verify that the lines in C satisfy the Wolff axiom. We do that thoroughly in Appendix D. The result is that the Wolff axiom is indeed satisfied.

In conclusion, our union of p^{6k} lines which obey the Wolff axiom is contained in a set with p^{2nk-2k} points.

We have shown that sets derived from the Heisenberg group can be extended to four dimensions. An important note, however, is that the construction presented here is valid only for fields of the type $\mathbb{F}_{p^{2k}}$. Tao proved that the hairbrush bound is sharp in dimension four. His construction is presented in Appendix C. Our construction is built in a different manner. We approach the problem by intersecting surfaces which contain lots of lines without being too plane-like. This allows us to generalize our construction to higher dimensions. A downside of our construction, however, is that it depends on the order of the underlying field and more precisely, on the smallest non-trivial divisor of d in $\mathbb{F}_{p^d}$.

5.2 Construction in n dimensions

Before we examine the general case, we investigate some properties of the surfaces we examined that make them suitable for our construction. Choosing to work only with k-traces, we ensure that the number of equations in the system that determines the number of lines depends only on the smallest non-trivial divisor s of d for fields of the type $\mathbb{F}_{p^d}$. Because we are examining only fields of the type $\mathbb{F}_{p^{2k}}$, in our construction we take $s = 2$. Consequently, we have fewer restrictions for the lines. This results in more lines on the surface. This makes such surfaces useful for our purposes because we want to intersect as many surfaces as possible to obtain a size as small as possible and each intersection reduces the number of points and consequently the number of lines.

Now we generalize our construction to vector spaces of dimension n over $\mathbb{F}_{p^{2k}}$. The construction procedure is as follows.

(*i*) Find a general form of the hypersurfaces.

(*ii*) Determine the number of lines contained in each hypersurface.

Remark. In $\mathbb{F}^n_{p^{2k}}$ we only examine lines that intersect the $\alpha_1\alpha_2\ldots\alpha_{n-1}$ plane transversely. The reasoning is analogous to the one applied in the construction for $\mathbb{F}^4_{p^{2k}}$.

(*iii*) Determine the number of hypersurfaces that we have to intersect.

(*iv*) Verify that the selected lines satisfy the Wolff axiom.

Construction for $\mathbb{F}^n_{p^{2k}}$. Let us examine a set of algebraic varieties $\{X_i\}$ in $\mathbb{F}^n_{p^{2k}}$ such that X_i, $i = 0, 1, \ldots, \lfloor n/2 \rfloor$, are cut out by the polynomials

$$Y_i = A(n-2i) + M(2i), \tag{7}$$

where $A(n-2i)$ is the *addition* part, defined as

$$A(n-2i) = \sum_{l=1}^{n-2i} \mathrm{Tr}_k(\alpha_l), \tag{8}$$

and $M(2i)$ is the *multiplication* part, defined as

$$M(2i) = \sum_{j=0}^{i-1} \mathrm{Tr}_k(\alpha_{n+2(j-i)+1} \cdot \bar{\alpha}_{n+2(j-i)+2}). \tag{9}$$

Each of the hypersurfaces X_i has p^{2nk-k} points. We determine the number of lines that each X_i contains in Appendix E. The result is that there are a total of $p^{k(4n-7)}$ lines through X_0 and $p^{4k(n-2)}$ in X_i when $i > 0$.

So far, we have completed the first two steps (*i*) and (*ii*) of the construction plan. Now we start intersecting the surfaces we described. We do this step by step to see the number of lines at each step and determine whether there are sufficiently many.

The system of equations determining the lines in the intersection $X_0 \cap X_1$ is as follows.

$$\begin{cases} \sum_{j=1}^{n-2} \mathrm{Tr}_k(r_j) = 0 \\ \sum_{j=1}^{n-1} s_j = 0 \\ s_{n-1} = \bar{r}_{n-1} \\ \mathrm{Tr}_k(s_{n-1}) = 0. \end{cases} \tag{10}$$

Here, we have p^k choices for r_{n-2} and r_{n-1}. Additionally, s_{n-1} is fixed by r_{n-1}, and we have one choice for s_{n-2}. Altogether, we have $p^{2k(2n-5)}$ lines in $X_0 \cap X_1$. Furthermore, $\dim_p(X_0 \cap X_1) = 2nk - 2k$.

Remark. The construction in $\mathbb{F}_{p^{2k}}^4$ is exactly the intersection of $X_0 \cap X_1$ and indeed when $n = 4$, $2k(2n-5) = 6k$.

The system of equations determining the lines in the intersection $X_0 \cap X_1 \cdots \cap X_l$ after a series of routine operations is as follows.

$$\begin{cases} \sum_{j=1}^{n-2} \mathrm{Tr}_k(r_j) = 0 \\ \mathrm{Tr}_k(s_{n-1}) = 0 \\ \mathrm{Tr}_k(r_{n-3} \cdot \bar{r}_{n-2}) = \mathrm{Tr}_k(r_{n-3}) + \mathrm{Tr}_k(r_{n-2}) \\ \dots \\ \mathrm{Tr}_k(r_{n-2l+1} \cdot \bar{r}_{n-2l+2}) = \mathrm{Tr}_k(r_{n-2l+1}) + \mathrm{Tr}_k(r_{n-2l+2}) \\ s_{n-1} = \bar{r}_{n-1} \\ \sum_{j=1}^{n-1} s_j = 0 \\ \mathrm{Tr}_k(s_{n-3} \cdot \bar{s}_{n-2}) = 0 \\ \dots \\ \mathrm{Tr}_k(s_{n-2l+1} \cdot \bar{s}_{n-2l+1}) = 0 \\ s_{n-3} + s_{n-2} = \bar{r}_{n-2} \cdot s_{n-3} + \bar{r}_{n-3} \cdot s_{n-2} \\ \dots \\ s_{n-2l+1} + s_{n-2l+2} = \bar{r}_{n-2l+2} \cdot s_{n-2l+1} + \bar{r}_{n-2l+1} \cdot s_{n-2l+2}. \end{cases} \tag{11}$$

In Appendix F we analyze the number of lines in the resulting surface. We conclude that in an n-dimensional vector space the resulting surface $X_0 \cap X_1 \cap \cdots \cap X_l$ of the intersection of $l+1$ surfaces contains $p^{k(4n-5l-5)}$ lines. From this we see that l should be at most $\frac{2n-3}{5}$. Otherwise, the resulting surface would have an insufficient number of lines. Because we want the set of points to be of minimal size, we want the resulting surface to be an intersection of as many X_i as possible. Therefore, for l we obtain

$$l = \left\lfloor \frac{2n-3}{5} \right\rfloor.$$

With that, we have completed the third step (iii) of the construction plan. It remains to be shown that the union of lines we selected satisfies the Wolff axiom. We do this in Appendix G. However, our proof is not valid for a particular number of m-lines. We conclude that this number is negligible heuristically, provided with the result for the construction in dimension four. Additionally, we have checked explicitly the number of lines that ought to be removed in the cases $n = 5, 6, 7$. For these cases the heuristic argument holds.

In conclusion, the size of our construction is

$$O\left(p^{2k\left(n-\left(\frac{\left\lfloor\frac{2n-3}{5}\right\rfloor+1}{2}\right)\right)}\right) = O\left(p^{2k\left(\frac{4}{5}n\right)}\right). \tag{12}$$

Thus, we provide a counterexample to Conjecture 1.1. However, $O\left(p^{2k\left(\frac{4}{5}n\right)}\right) > O\left(p^{2k\left(\frac{n+2}{2}\right)}\right)$ and therefore we do not prove that the hairbrush bound is sharp for all n. In Appendix H we visualize the size of our construction and compare it to the hairbrush bound and the trivial construction with size $O(p^{dn})$.

6 Future development

An object of future research is to prove rigorously that the final result does not depend on the number of lines we need to remove from our construction. A reasonable approach is an induction on the case in four dimensions. It would also be interesting to generalize the constructions in Section 5 from $\mathbb{F}^n_{p^{2k}}$ to $\mathbb{F}^n_{p^d}$. Taking into consideration the paper of Ellenberg and Hablicsek [8], this task seems feasible with an analogous approach.

7 Conclusion

In this project we have constructed a general form of unions of lines in $\mathbb{F}^n_{p^{2k}}$ based on the Heisenberg group. They satisfy the Wolff axiom up to a heuristically negligible number of lines. Additionally, the four dimensional case is examined and the Wolff axiom is verified for it.

In particular, the algebraic structure of the unions of lines satisfying the Wolff axiom may be advantageous for understanding the structure of sets satisfying the Kakeya conjecture.

8 Acknowledgments

I would like to thank my mentor Hong Wang of the Massachusetts Institute of Technology for her invaluable suggestions and discussions. I would alsto like to thank Dr. Tanya Khovanova for the helpful discussions. I thank Prof. Larry Guth and Prof. David Jerison for their many helpful advice and ideas. I am indebted to my tutor Dr. John Rickert for the various helpful discussions and suggestions. I would like to express my gratitude towards Dr. Evgenia Sendova, Shashwat Kishore, Daniel Vitek, Bertrand Stone and Katerina Velcheva for their helpful comments.

I would also like to express my gratitude towards the Center for Excellence in Education, the Research Science Institute, the Massachusetts Institute of Technology and the High School Science Institute as well as Dr. Petar Kenderov, America for Bulgaria Foundation and Sts. Cyril and Methodius International Foundation whose sponsorship gave me the opportunity to participate at RSI and conduct research.

References

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

[2] L'aiguille de Kakeya. http://eljjdx.canalblog.com/archives/2011/01/23/20181660.html, 2011. Accessed: 2015-07-16.

[3] Z. Dvir. On the size of Kakeya sets over finite fields. *arXiv:0803.2336*, pages 1–5, 2008.

[4] T. Wolff. An improved bound for Kakeya type maximal functions. *Revista Matemtica Iberoamericana*, 11:651–674, 1995.

[5] T. Tao. A new bound for finite field Besicovitch sets in four dimensions. *arXiv:math/0204251*, 2002.

[6] K. Conrad. Finite fields. http://www.math.uconn.edu/kconrad/blurbs/galoistheory/finitefields.pdf, 2013.

[7] T. Tao and G. Mockenhaupt. Restriction and Kakeya phenomena for finite fields. *arXiv:math/0204234*, 2010.

[8] J. S. Ellenberg and M. Hablicsek. An incidence conjecture of Bourgain over finite fields of positive characteristic. *arXiv:1311.1479*, 2013.

[9] D. Harari. Géométrie algébrique, M2, Orsay.

[10] G. Birkhoff and S. M. Lane. *A Survey of Modern Algebra.* The MacMillan Company, 1941.

Appendix A General definitions for finite fields

Here we introduce general definitions for finite fields and their structure.

Definition A.1. A *field* is a set $\mathbb{F}$ on which two binary operations, called *addition* and *multiplication*, are defined and which contains two distinguished elements 0 and e, usually denoted by 1, with $0 \neq e$. Furthermore, $\mathbb{F}$ is an abelian group with respect to addition having 0 as the identity element, and the nonzero elements of $\mathbb{F}$ form an abelian group with respect to multiplication having e as the identity element. The two operations of addition and multiplication are linked by the distributive law $a(b + c) = ab + ac$. The second distributive law $(b + c)a = ba + ca$ follows automatically from the commutativity of multiplication.

The element 0 is called the *zero element* and e is called the *multiplicative identity element*. The number of elements in the field is called the *order* of the field. The order of a finite field is always a prime or a prime power [10]. A *subfield* of a field $\mathbb{F}$ is a subset of $\mathbb{F}$ which is itself a field with induced operations from $\mathbb{F}$. The smallest subfield is called the *prime* subfield.

Definition A.2. There is a smallest positive integer p satisfying the condition

$$\underbrace{e + e + \cdots + e}_{p \text{ times}} = 0$$

for the multiplicative identity e in $\mathbb{F}_q$. This number is called the *characteristic* of the finite field $\mathbb{F}_q$.

When the field $\mathbb{F}$ is finite, its characteristic is a positive integer. This statement does not hold for fields in general. However, we work only with fields of finite order. Another note is that the characteristic p is always prime. Otherwise $\mathbb{F}$ would not be a field because the divisors of p would not have multiplicative inverses.

Definition A.3. A field $\mathbb{F}$ is said to be an *extension field*, denoted $\mathbb{F}/K$, of a field K if K is a subfield of $\mathbb{F}$.

Definition A.4. A *splitting field* of a polynomial with coefficients in a field $\mathbb{F}_{p^d}$ is a smallest field extension of that field over which the polynomial splits into linear factors.

Furthermore, we can express the additive structure of the extension field $\mathbb{F}/K$ as a vector space over K.

Definition A.5. Let n be a positive integer. The *degree* of a subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$ is defined as $\dfrac{n}{d}$ where $d|n$.

It is known that there exists a unique subfield $\mathbb{F}_{p^d}$ of $\mathbb{F}_{p^n}$ for every $d|n$.

The Theorems A.1-A.3 and Lemma A.1 are proved in a handout on finite fields by K. Conrad [6]. They give a general classification of finite fields. Although we do not apply them directly in the paper, they play an essential role in understanding the structure of finite fields.

Theorem A.1. Let p be prime and $\pi(x)$ be a monic irreducible in $\mathbb{F}_p[x]$ of degree n. Then $\mathbb{F}_p[x]/(\pi(x))$ is a field of order p^n.

Theorem A.2. Every finite field is isomorphic to $\mathbb{F}_p[x]/(\pi(x))$ for some prime p and some monic irreducible $\pi(x)$ in $\mathbb{F}_p[x]$.

Theorem A.3. For every prime power p^n there exists a unique field of order p^n.

Lemma A.1. A field of prime power order p^n is a splitting field of $X^p - X$ over $\mathbb{F}_p$.

Appendix B On the case $n = 2$

This case is significantly easier than the general case because the Wolff axiom becomes vacuous. The absence of the Wolff axiom reduces the problem to the following.

Problem in two dimensions. *Consider a two-dimensional vector space $\mathbb{F}_{p^d}^2$ over a finite field $\mathbb{F}_{p^d}$. Let $\mathcal{L} = l_i, i = 1, 2, ..., p^d$ be a set of lines in $\mathbb{F}_{p^d}^2$. Consider the set Σ of points on l_i where $\Sigma = \cup l_i$. The cardinality of Σ is $O(p^{2d})$.*

Proof. The upper bound of the total number of points in Σ is q^2. This upper bound is reached if no two lines l_i intersect. Every two non-parallel lines intersect at exactly one point. To prove the lower bound, we evaluate the size of the set T of intersection points between lines in $\mathcal{L}$. Let there be a line l_i pointing in each of the q directions (e.g. there are no parallel lines in $\mathcal{L}$). Every two lines in $\mathcal{L}$ intersect. We have

$$|T| \leq \frac{(p^d-1)(p^d-2)}{2}. \tag{13}$$

$$|T_{MAX}| = \frac{(p^d-1)(p^d-2)}{2}. \tag{14}$$

Because $|T_{MAX}| + |\Sigma_{MIN}| = p^{2d}$. This implies that

$$|\Sigma_{MIN}| = p^{2d} - |T_{MAX}| \geq \frac{p^{2d}+3p^d-2}{2} = \frac{p^{2d}}{2} \ as\ p \to \infty.$$

Therefore $|\Sigma| = O(p^{2d})$ as $p \to \infty$, and the desired result is achieved. □

Appendix C Construction for the case $n = 4$ not derived from the Heisenberg group

A construction that proves the hairbrush argument bound sharp for $\mathbb{F}_q^4$ has been given by T. Tao in [5] in 2002.

Construction for $\mathbb{F}_{p^d}^4$ (T. Tao). Let $\langle , \rangle : \mathbb{F}_q^4 \times \mathbb{F}_q^4 \to \mathbb{F}_q$ be a *non-degenerate symmetric quadratic form* on $\mathbb{F}_q^4$. Let P be the unit sphere”

$$P := \{x \in \mathbb{F}_q^4 : \langle x, x \rangle = 1\}.$$

and let L be the set of all lines of the form $x + tv : t \in \mathbb{F}_q$, where $x \in \mathbb{F}_q^4$, $v \in \mathbb{F}_q^4 \backslash \{0\}$ are such that $\langle x, x\rangle = 1$, $\langle v, x\rangle = 0$, and $\langle v, v\rangle = 0$. Then $|L| \sim |F|^3$ and obeys the Wolff axiom, while $|P| \sim |F|^3$ and contains all the lines in the set of lines L.

What is more interesting, however, is the fact that this construction, contrary to the ones in our paper, yields exactly the hairbrush argument for every field $\mathbb{F}_{p^d}$ where p is prime and d is a positive integer. A natural question that follows is whether this construction can be extended to higher dimensions.

However, this construction is not derived the from the Heisenberg group and the properties of the surface containing the set are different. It would be interesting to try extending this construction to higher dimensions.

Appendix D Verifying Wolff axiom for the construction in $\mathbb{F}_{p^{2k}}^4$

We have to verify three conditions.

(i) There are at most p^{6k} lines in every 4-plane.

(ii) There are at most p^{4k} lines in every 3-plane.

(iii) There are at most p^{2k} lines in every plane.

The first condition is evidently satisfied because the total number of lines is p^{6k}.

To verify the second condition, note that we examined only the lines that intersect the $\alpha_1\alpha_2\alpha_3$ plane transversely. Because of that, we can parameterize each line with a point on the plane and a direction. Let P be a 3-plane and P_0 be the $\alpha_1\alpha_2\alpha_3$ plane. If $P \equiv P_0$, there are no lines lying in P because all the lines intersect it transversely. If $P \not\equiv P_0$, then $P \cap P_0$ is a plane (2-plane). We now find the number of points $(a, b, c, 0)$ and the number of directions $(u, v, w, 1)$ that satisfy the system of equations

$$\begin{cases} Tr_k(a) + Tr_k(b) = 0 \\ Tr_k(c) = 0 \\ Aa + Bb + Cc + E = 0 \\ u + v + w = 0 \\ w = c^p \\ Au + Bv + Cw + D = 0. \end{cases} \tag{15}$$

First, we note that w is determined by c. However, we have three cases depending on the values of A, B, C and D.

Case 1 $(A, B, C, D) = (1, 1, 1, 0)$

Case 2 $(A, B) = (1, 1)$, $(C, D) \neq (1, 0)$

Case 3 $(A, B) \neq (1, 1)$

In *Case* 1 we have p^{2k} choices for a and u, and p^k choices for b. Despite the fact that w and c are fixed, we have a total of p^{5k} lines. Therefore, the lines on this plane violate the Wolff axiom. We can consider this case as *bad*. We can disregard the lines on this plane, however, because we can replace them with the Heisenberg group in three dimensions in Section 4 which has size $O(q^{5/2}) < O(q^3)$ and therefore does not change the final answer.

In *Case* 2 we have p^{2k} choices for u and p^k choices for a. Consequently, a and u fix b, c, v and w. Altogether, we have p^{3k} lines and the Wolff axiom is satisfied.

In *Case* 3 we have p^{2k} choices for a and p^k choices for b. Consequently, a and b fix c, u, v and w. In total, again, we have p^{3k} lines and the Wolff axiom is satisfied.

Only the last condition remains. Let P_1 be a plane. If P_1 does not intersect P_0 transversely, then there are no lines in P_1. Otherwise the intersection $P_0 \cap P_1$ is a line. We determine the number of points $(a, b, c, 0)$ and number of directions $(u, v, w, 1)$ that satisfy the following system of equations.

$$\begin{cases} Tr_k(a) + Tr_k(b) = 0 \\ Tr_k(c) = 0 \\ Aa + Bb + Cc + E = 0 \\ Au + Bc + Cw + E = 0 \\ u + v + w = 0 \\ w = c^p \\ Fa + Gb + Hc + I = 0 \\ Fu + Gv + Hw + I = 0. \end{cases} \tag{16}$$

Using analogous reasoning, we see that the Wolff axiom is satisfied in this case as well. We conclude that this union of lines satisfies the Wolff axiom.

Appendix E Number of lines in the surface X_i for each $0 < i < n/2$

The number of lines in the surface X_i is determined by the following system of equations (only non-conjugate polynomials are presented for conciseness).

$$\begin{cases} \sum_{j=1}^{n-2i} \mathrm{Tr}_k(r_j) + \sum_{m=1}^{i-1} (\mathrm{Tr}_k(r_h \cdot \bar{r}_{h+1})) = 0 \\ \sum_{j=1}^{n-2i} s_j + \sum_{m=1}^{i-1} (\bar{r}_h \cdot s_{h+1} + \bar{r}_{h+1} \cdot s_h) + \bar{r}_{n-1} = 0 \\ \sum_{m=1}^{i-1} \mathrm{Tr}_k(s_h \cdot s_{h+1}) + \mathrm{Tr}_k(s_{n-1}) = 0. \end{cases} \tag{17}$$

Here the equation of the line $(\alpha_1, \alpha_2 \ldots \alpha_n)$ is $(r_1, r_2 \ldots, r_{n-1}, 0) + t(s_1, s_2 \ldots, s_{n-1}, 1)$ and $h = 2(i+m)-1$. We examine only the lines that intersect the $\alpha_1\alpha_2 \ldots \alpha_{n-1}$ plane transversely.

Therefore, we get that $r_n = 0$ and $s_n = 1$. This is the reason why m ranges to $i-1$ instead of i in (17). If $i = 0$, the system simplifies to

$$\begin{cases} \displaystyle\sum_{j=1}^{n-1} \mathrm{Tr}_k(r_j) = 0 \\ \displaystyle\sum_{j=1}^{n-1} s_j = 0. \end{cases} \tag{18}$$

We have p^k choices for r_{n-1}, one choice for s_{n-1} and p^{2k} choices for the others. Therefore, we have a total of $p^{k(4n-7)}$ lines through X_0.

If $i = 1$, the system simplifies to

$$\begin{cases} \displaystyle\sum_{j=1}^{n-2} \mathrm{Tr}_k(r_j) = 0 \\ \displaystyle\sum_{j=1}^{n-2} s_j + \mathrm{Tr}_k(r_{n-1}) = 0 \\ \mathrm{Tr}_k(s_{n-1}) = 0. \end{cases} \tag{19}$$

Here, we have p^k choices for r_{n-2} and s_{n-1}, one choice for r_{n-1} and p^{2k} choices for the others. Therefore, we have a total of $p^{4k(n-2)}$ lines through X_1.

If $i > 1$, the system (17) remains unchanged and we have p^{3k} choices for r_{n-2} and r_{n-3} altogether, p^k choices for s_{n-1}, one choice for r_{n-1} and p^{2k} choices for the others regardless of the value of i. In total, we have $p^{4k(n-2)}$ lines in X_i when $i > 1$.

Appendix F Number of lines in $X_0 \cap X_1 \cdots \cap X_l$

To analyze the system of equations (11), we separate the system into $l-1$ parts (denoted here by *Part* 1 and $\sum_{j=2}^{l-1}$ Part j), solve them separately, and then combine them.

Part 1

$$\begin{cases} \sum_{j=1}^{n-2} \mathrm{Tr}_k(r_j) = 0 \\ \sum_{j=1}^{n-1} s_j = 0 \\ s_{n-1} = \bar{r}_{n-1} \\ \mathrm{Tr}_k(s_{n-1}) = 0. \end{cases} \tag{20}$$

This part is identical to the system for $X_0 \cap X_1$ in (10). Therefore, we already know how to solve it.

$\sum_{j=2}^{l-1}$ *Part j*

$$\begin{cases} \mathrm{Tr}_k(r_{n-2j+1} \cdot \bar{r}_{n-2j+2}) = \mathrm{Tr}_k(r_{n-2j+1}) + \mathrm{Tr}_k(r_{n-2j+2}) \\ \mathrm{Tr}_k(s_{n-2j+1} \cdot \bar{s}_{n-2j+1}) = 0 \\ s_{n-2j+1} + s_{n-2j+2} = \bar{r}_{n-2j+2} \cdot s_{n-2j+1} + \bar{r}_{n-2j+1} \cdot s_{n-2j+2}. \end{cases} \tag{21}$$

The other parts are all the same but for different r and s and it is sufficient to solve one. Thus, without loss of generality, we can solve only the system

$$\begin{cases} \mathrm{Tr}_k(r_{n-3} \cdot \bar{r}_{n-2}) = \mathrm{Tr}_k(r_{n-3}) + \mathrm{Tr}_k(r_{n-2}) & (22) \\ \mathrm{Tr}_k(s_{n-3} \cdot \bar{s}_{n-2}) = 0 & (23) \\ s_{n-3} + s_{n-2} = \bar{r}_{n-2} \cdot s_{n-3} + \bar{r}_{n-3} \cdot s_{n-2}. & (24) \end{cases}$$

From (24) we express s_{n-2} as

$$s_{n-2} = \frac{s_{n-3}(1 - \bar{r}_{n-2})}{\bar{r}_{n-3} - 1}. \tag{25}$$

From (23) and (25) we get

$$s_{n-3}^{p^k+1} \left(\left(\frac{1 - r_{n-2}}{r_{n-3} - 1} \right) + \left(\frac{1 - \bar{r}_{n-2}}{\bar{r}_{n-3} - 1} \right) \right) = 0. \tag{26}$$

Therefore, either s_{n-3} or $\left(\dfrac{1-r_{n-2}}{r_{n-3}-1}\right)+\left(\dfrac{1-\bar{r}_{n-2}}{\bar{r}_{n-3}-1}\right)$ should be equal to 0. In the latter case we get that

$$\begin{aligned}&r_{n-2}\cdot\bar{r}_{n-3}+\bar{r}_{n-2}\cdot r_{n-3}=r_{n-3}+\bar{r}_{n-3}+r_{n-2}+\bar{r}_{n-2}-2\\&\mathrm{Tr}_k(r_{n-3}\cdot\bar{r}_{n-2})=\mathrm{Tr}_k(r_{n-3})+\mathrm{Tr}_k(r_{n-2})-2.\end{aligned}\tag{27}$$

From (22) and (27) we reach a contradiction. It follows that $s_{n-3}=0$. Consequently, (24) shows that $s_{n-2}=0$ as well.

Let us combine *Part* 1 and $\sum_{j=2}^{l-1}$ *Part* j. We find that s_{n-j} ($j=1,2,\dots,2l$) are fixed and we have p^k choices for r_{n-1} and r_{n-2l}. Additionally, we have a total of p^{3k} choices for each of the pairs (r_{n-2j},r_{n-2j-1}) ($j=1,2,\dots,l-1$). For the others we have p^{2k} choices.

In total, we have $p^{4(n-1)}/(p^{4kl}\cdot p^{kl-k}\cdot p^{2k})=p^{k(4n-5(l+1))}$ lines in $X_0\cap X_1\cap\cdots\cap X_l$. Taking a look back to the main problem, we need $p^{2k(n-1)}$ lines. Therefore, we find that

$$\begin{aligned}&k(4n-5(l+1))\geq 2k(n-1)\\&l\leq\frac{2n-3}{5}.\end{aligned}\tag{28}$$

Therefore, in an n-dimensional vector space the number $l+1$ (because l ranges from 0) of surfaces we intersect should be at most $\frac{2(n+1)}{5}$.

Appendix G Verifying Wolff axiom for the construction in $\mathbb{F}^n_{p^{2k}}$

We have to verify $n-1$ conditions: There are at most $p^{2kn-i-1}$ lines in every $(n-i)$-plane, for $0<i<n$. The condition for $i=0$ is not satisfied if we take into account all the lines in $X_0\cap X_1\cap\cdots X_l$. Therefore, we have to remove some of the lines in order to meet the given conditions. More precisely, we ought to have $p^{2k(n-1)}$ lines, but instead we have $p^{k(4n-5l-5)}$ lines. Therefore, we have to fix a number of parameters. The product of their number of

choices should be p^{γ} where γ is

$$\begin{aligned}\gamma &= k(4n-5l-5)-2k(n-1)\\ &= k(2n-5l-3) \qquad (29)\\ &= k(2n-5\left\lfloor\frac{2n-3}{5}\right\rfloor-3).\end{aligned}$$

In the following table we present, without loss of generality, the parameters we fix in each of the five cases.

n modulo 5	difference	parameters we fix
$n \equiv 0 \pmod 5$	p^{2k}	r_1
$n \equiv 1 \pmod 5$	p^{4k}	r_1 and r_2
$n \equiv 2 \pmod 5$	p^{k}	r_{n-1}
$n \equiv 3 \pmod 5$	p^{3k}	r_{n-2} and r_{n-3}
$n \equiv 4 \pmod 5$	0	–

We now have exactly $p^{2k(n-1)}$ lines and therefore the first condition is satisfied. Let us denote the constraints (11) by $\mathcal{C}$. The constraints for the lines in the ith condition for $i \geq 1$ are of the form

$$\begin{cases}\mathcal{C}\\ \displaystyle\sum_{j=1}^{n-1} R_{n-1,\,j}\cdot r_j + R_{n-1,\,n} = 0\\ \displaystyle\sum_{j=1}^{n-1} R_{n-1,\,j}\cdot s_j + R_{n-1,\,n} = 0\\ \cdots\\ \displaystyle\sum_{j=1}^{n-1} R_{n-i,\,j}\cdot r_j + R_{n-i,\,n} = 0\\ \displaystyle\sum_{j=1}^{n-1} R_{n-i,\,j}\cdot s_j + R_{n-i,\,n} = 0.\end{cases} \qquad (30)$$

For general m-planes the procedure is as follows.

We divide the system into $i+1$ parts (denoted here by *Part* 1 and $\sum_{m=2}^{i+1}$ *Part* m).

Part 1 $\mathcal{C}$

$\sum_{m=2}^{i+1}$ *Part* m

$$\begin{cases} \sum_{j=1}^{n-1} R_{n-m,\,j} \cdot r_j + R_{n-m,\,n} = 0 \\ \sum_{j=1}^{n-1} R_{n-m,\,j} \cdot s_j + R_{n-m,\,n} = 0. \end{cases} \tag{31}$$

We already know how to solve the first part of the system - it is identical to the solution (11). Therefore, we have to solve only the remaining i parts. Because they are linearly independent, each pair

$$\begin{cases} \sum_{j=1}^{n-1} R_{n-m,\,j} \cdot r_j + R_{n-m,\,n} = 0 \\ \sum_{j=1}^{n-1} R_{n-m,\,j} \cdot s_j + R_{n-m,\,n} = 0. \end{cases} \tag{32}$$

fixes exactly one r_j and one s_j. In total, we have $p^{k(4n-5l-5)}/p^{4km} = p^{k(4n-5l-4m-5)}$ lines. The condition is that the lines should be less than $p^{2kn-2km}$. It is satisfied if

$$k(2n-5l-5-2m) \leq 0. \tag{33}$$

The minimum value of $l = \left\lfloor \frac{2n-3}{5} \right\rfloor = \frac{2n-7}{5}$ is attained when $n \equiv 1 \pmod 5$. We find that the conditions are satisfied if

$$\begin{aligned} & k(2n-2n+7-5-2m) \leq 0 \\ & k(2-2m) \leq 0. \end{aligned} \tag{34}$$

This is true for every $m \geq 1$.

However, analogically to the verification of the Wolff axiom in four dimensions, there are some specific cases that we need to examine.

For example, let $(r_{n-2,0}, r_{n-3,0})$ be a solution to the equation

$$\mathrm{Tr}_k(r_{n-2} + r_{n-3}) = \mathrm{Tr}_k(r_{n-2} \cdot \bar{r}_{n-3}) \tag{35}$$

and P be an $(n-2)$-plane defined by

$$\begin{aligned} \alpha_{n-2} &= r_{n-2,0} \\ \alpha_{n-3} &= r_{n-3,0}. \end{aligned} \tag{36}$$

There are $p^{2k(n-3)+k}$ lines on P. Consequently, P does not satisfy the Wolff axiom. Analogously to the construction in four dimensions, we can delete these lines. It is left to verify that there are enough lines after removing all *bad* m-planes ($m \leq n-2$). Heuristically, this should be true, based on the result in four dimensions. Furthermore, the authors have checked explicitly the number of lines that need to be removed for $n = 5, 6, 7$. For these cases the heuristic argument holds. Nevertheless, it should be examined and proved rigorously.

Appendix H Plot of the size of our construction compared to the hairbrush bound and the trivial construction

The y axis plots ψ in $p^{d\psi}$ which is indicative of the size of the set. The x axis plots the dimension n. The blue line represents the size of the trivial construction of size p^{dn}. The orange line represents the size of our construction. The green line represents the hairbrush bound.

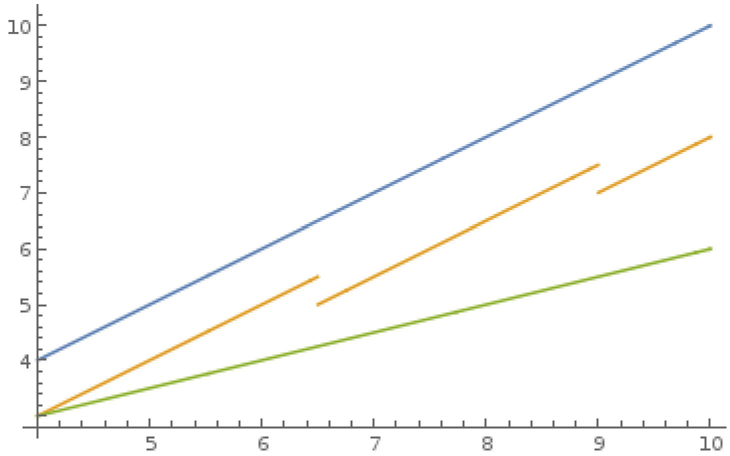


Figure 2: For $4 \leq n \leq 10$

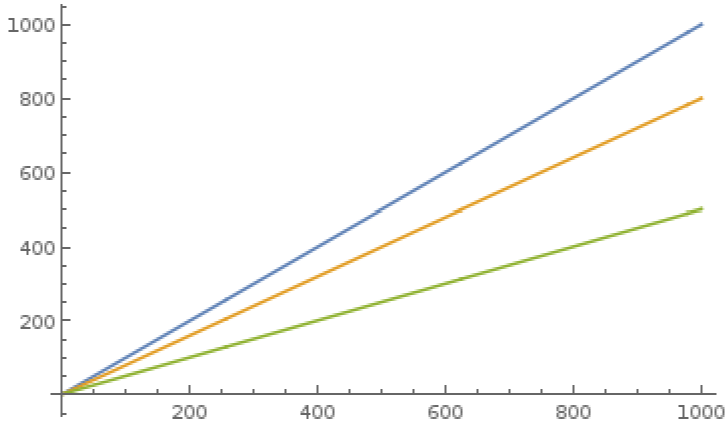


Figure 3: For $4 \leq n \leq 1000$