

eScholarship

Combinatorial Theory

Title

Proof of the Kakeya set conjecture over rings of integers modulo square-free N

Permalink

<https://escholarship.org/uc/item/4324c8n4>

Journal

Combinatorial Theory, 1(0)

ISSN

2766-1334

Authors

Dhar, Manik
Dvir, Zeev

Publication Date

2021

DOI

10.5070/C61055361

Copyright Information

Copyright 2021 by the author(s). This work is made available under the terms of a Creative Commons Attribution License, available at

<https://creativecommons.org/licenses/by/4.0/>

Peer reviewed

PROOF OF THE KAKEYA SET CONJECTURE OVER RINGS OF INTEGERS MODULO SQUARE-FREE N

Manik Dhar ^{*1} and Zeev Dvir ^{*2}

¹*Department of Computer Science, Princeton University, Princeton, U.S.A.*
manikd@princeton.edu

²*Department of Computer Science and Department of Mathematics, Princeton University, Princeton, U.S.A.*
zdvir@princeton.edu

Submitted: Nov 25, 2020; Accepted: Apr 12, 2021; Published: Dec 15, 2021

© The authors. Released under the CC BY license (International 4.0).

Abstract. A Kakeya set $S \subset (\mathbb{Z}/N\mathbb{Z})^n$ is a set containing a line in each direction. We show that, when N is any square-free integer, the size of the smallest Kakeya set in $(\mathbb{Z}/N\mathbb{Z})^n$ is at least $C_{n,\epsilon}N^{n-\epsilon}$ for any ϵ – resolving a special case of a conjecture of Hickman and Wright. Previously, such bounds were only known for the case of prime N . We also show that the case of general N can be reduced to lower bounding the \mathbb{F}_p rank of the incidence matrix of points and hyperplanes over $(\mathbb{Z}/p^k\mathbb{Z})^n$.

Mathematics Subject Classifications. 05B20, 05B25

1. Introduction

Given a finite abelian ring R , we consider the space of n -tuples over R , denoted R^n . In this space we may define a line in direction $b \in R^n \setminus \{0\}$ to be a subset of the form $\{a + tb | t \in R\}$ where $a \in R^n$. We denote the set of directions in R^n (projective space) by $\mathbb{P}R^{n-1}$. For now we will postpone the precise definition of $\mathbb{P}R^{n-1}$ to a later stage. A Kakeya set in R^n is a set containing a line in every direction:

Definition 1.1 (Kakeya set). A set $S \subset R^n$ is said to be a Kakeya set if given any direction $b \in \mathbb{P}R^{n-1}$ there exists a point $a \in R^n$ such that the line $\{a + tb | t \in R\}$ is contained in S .

The question of lower-bounding the size of the smallest Kakeya set over finite fields was initially raised by Wolff [Wol99] as a possible approach for attacking the notorious Euclidean Kakeya conjecture in \mathbb{R}^n , and later found other applications including in theoretical computer science (see [Dvi10] for a survey of those). Wolff's conjecture, later known as the finite field

^{*}Research supported by NSF grant DMS-1953807.

Kakeya conjecture stated that, the size of the smallest Kakeya set in \mathbb{F}_q^n should be at least $C_n q^n$ for some constant C_n depending only on the dimension. Coming from the Euclidean problem, one typically thinks of n as fixed and q growing, however, later applications deal with other scenarios and require a more accurate control of the constant. Wolff's conjecture was proved using the polynomial method in [Dvi09] with subsequent improvements given in [SS08, DKSS13] culminating in the following bound.

Theorem 1.2 ([DKSS13]). *Let \mathbb{F}_q denote a finite field of order q and let $S \subset \mathbb{F}_q^n$ be a Kakeya set. Then*

$$|S| \geq \frac{q^n}{(2 - 1/q)^n}$$

When R is not a field much less is known. The problem of lower bounding the size of Kakeya sets for the rings $\mathbb{Z}/p^k\mathbb{Z}$ and $\mathbb{F}_q[x]/\langle x^k \rangle$ was first proposed in [EOT10] as a step in the direction of the Euclidean problem as these rings contain ‘scales’ in a way that does not exist over a finite field and is reminiscent of the real numbers. While the additive combinatorics techniques that preceded the polynomial method [Bou99, KT02] work over any abelian ring, they currently only lead to bounds of the form $|S| \geq |R|^{\alpha n}$ with the $\alpha < 0.6$. Another, more recent, work to study Kakeya sets (and related operators) over finite rings is [HW18] in which a connection between bounds for Kakeya sets over the rings $\mathbb{Z}/p^k\mathbb{Z}$ and the Minkowski dimension of p -adic Kakeya sets is established. For the two dimensional case, when $R = \mathbb{F}_q[x]/\langle x^k \rangle$ or $R = \mathbb{Z}/p^k\mathbb{Z}$, Dummit and Hablicsek showed a (tight) bound of $|S| \geq |R|^2/2k$ in [DH13a].

Similar to the Euclidean setting, Kakeya sets with Haar measure 0 can be constructed for the ring of p -adic integers and the power series ring $\mathbb{F}_q[[x]]$. The constructions can be found in [DH13a, Fra16, Car18, HW18]. As in the Euclidean setting, we want to bound the Minkowski dimension of Kakeya sets for these rings which is connected to the size of Kakeya sets in $\mathbb{Z}/p^k\mathbb{Z}$ and $\mathbb{F}_q[x]/\langle x^k \rangle$.

The Kakeya conjecture over the rings $R = \mathbb{Z}/N\mathbb{Z}$ was stated in [HW18] as follows. As seen above, for finite fields the loss of ϵ in the exponent is not necessary. However, as we shall see later, for composite N we must allow it.

Conjecture 1.1 (Kakeya set conjecture over $\mathbb{Z}/N\mathbb{Z}$). *For all $\epsilon > 0$ and integers n there exists a constant $C_{n,\epsilon}$ such that any Kakeya set $S \subset (\mathbb{Z}/N\mathbb{Z})^n$ satisfies*

$$|S| \geq C_{n,\epsilon} \cdot N^{n-\epsilon}.$$

Already when $N = p_1 \cdot p_2$ is a product of two primes of roughly the same magnitude, the polynomial method fails to work. One way to see this is to notice that any polynomial over $R = \mathbb{Z}/p_1 p_2 \mathbb{Z}$ has degree at most $\max\{p_1 - 1, p_2 - 1\} \approx N^{1/2}$ in each variable. This limits the dimension of the space of polynomials to $\approx N^{n/2}$ and prevents us from interpolating a non-zero polynomial vanishing on S , when S is larger than that dimension (which is the first step in the polynomial method).

Our main contribution is a proof of Conjecture 1.1 for square-free integers N . At this point we should say what is our definition of projective space for these rings as this will determine

the definition of Kakeya sets. For $N = p_1 \cdots p_r$ a product of r distinct primes, the Chinese remainder theorem gives us

$$(\mathbb{Z}/N\mathbb{Z})^n \cong \mathbb{F}_{p_1}^n \times \cdots \times \mathbb{F}_{p_r}^n$$

under the natural isomorphism $x \mapsto (x \pmod{p_i})_{i=1}^r$. For each i the projective space $\mathbb{P}\mathbb{F}_{p_i}^{n-1}$ is defined to be the set of all non-zero vectors in $\mathbb{F}_{p_i}^n$ up to scaling. Finally, we take the projective space to be

$$\mathbb{P}(\mathbb{Z}/N\mathbb{Z})^{n-1} = \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \cdots \times \mathbb{P}\mathbb{F}_{p_r}^{n-1}.$$

In other words, a direction in $(\mathbb{Z}/N\mathbb{Z})^n$ is represented by a vector $b \in (\mathbb{Z}/N\mathbb{Z})^n$ that is non-zero modulo p_i for all i and we identify two directions if they can be obtained from one another by scaling with an invertible ring element.¹

Theorem 1.3 (Kakeya bound for square-free N). *Let $N = p_1 \cdots p_r$ be a product of r distinct primes and set $R = \mathbb{Z}/N\mathbb{Z}$. Any Kakeya Set $S \subseteq R^n$ satisfies*

$$|S| \geq \frac{N^n}{\prod_{i=1}^r (2 - 1/p_i)^n} \geq \frac{N^n}{2^{rn}}.$$

Since the number of factors of N satisfies $r = O(\log N / \log \log N)$ (indeed the asymptotics of r are known [HR17]) we see that the expression in the theorem is lower bounded by $N^{n-O(n/\log \log N)}$ and so it indeed proves Conjecture 1.1.

The tightness of the bound in Theorem 1.3 can be demonstrated by taking the product (via the Chinese remainder theorem) of the best known constructions in $\mathbb{F}_{p_i}^n$ for each factor p_i . In [SS08] it was shown that, for any prime p , there are Kakeya sets in \mathbb{F}_p^n of size bounded above by $p^n/2^{n-1} + Cp^{n-1}$, where C is an absolute constant. Taking the product one obtains the following.

Theorem 1.4. *Let $N = p_1 \cdots p_r$ be a product of distinct primes and n an integer. There exist a Kakeya Set $S \subseteq (\mathbb{Z}/N\mathbb{Z})^n$ with*

$$|S| \leq \prod_{i=1}^r \left(\frac{p_i^n}{2^{n-1}} + Cp_i^{n-1} \right),$$

where $C > 1$ is an absolute constant.

Hence, when all the prime factors p_i of N are sufficiently large (also as a function of r), we see that the main term in the construction is off by at most a factor of $2^r = N^{o(1)}$ from the lower bound of Theorem 1.3. Notice that, while the upper bound is obtained from a product of Kakeya

¹In both [EOT10, HW18], where the emphasis was on rings such as $\mathbb{Z}/p^k\mathbb{Z}$ or $\mathbb{F}_q[x]/x^k$, the definition of projective space over a ring R require the direction b to have at least one invertible coordinate. This definition leads to the same notion of projective space as ours for the rings $\mathbb{Z}/p^k\mathbb{Z}$ or $\mathbb{F}_q[x]/x^k$. However, in the case of $\mathbb{Z}/N\mathbb{Z}$ where N has more than one distinct prime factors their definition is different than ours. In our definition a direction might have all coordinates as zero-divisors. For example, in the case of composite square free N if the reductions $b \pmod{p_i}$ have disjoint supports we get lines with directions represented by non-zero divisors in each co-ordinate. Requiring at least one invertible coordinate leads, in the case of composite square free N , to a definition that is basis dependent and less natural.

sets modulo each prime factor, a general Kakeya set in $(\mathbb{Z}/N\mathbb{Z})^n$ might not have this product structure (otherwise the proof of the lower bound would be trivial).

Our proof of Theorem 1.3 also outlines a specific problem whose solution could lead to a bound for general (non square-free) modulo N . Consider the $p^{kn} \times p^{kn}$ matrix $W_{p^k, n}$ whose rows/columns are indexed by elements of R^n where $R = \mathbb{Z}/p^k\mathbb{Z}$ and whose (x, y) 'th entry is 1 if $\langle x, y \rangle = 0 \pmod{p^k}$ and 0 otherwise. We call $W_{p^k, n}$ the *point-hyperplane incidence matrix* of R^n . Since $W_{p^k, n}$ has zero-one entries, we can view it as a matrix over any field and, in particular, compute its rank over \mathbb{F}_p . We show that this rank lower bounds the size of any Kakeya set.

Theorem 1.5. *Given a prime p and integers k, n , every Kakeya set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$ satisfies*

$$|S| \geq \text{rank}_{\mathbb{F}_p}(W_{p^k, n}).$$

Hence, proving a lower bound of, say, $p^{(1-\epsilon)kn}$ for small $\epsilon > 0$ on the rank of the incidence matrix $W_{p^k, n}$ would lead to new bounds for Kakeya sets in $(\mathbb{Z}/p^k\mathbb{Z})^n$. Furthermore, using our techniques, these bounds will then imply the appropriate bounds for N which is a product of prime powers. The work of [GD68, MM68, Smi69] shows such rank bounds hold for $W_{p, n}$ when $k = 1$ or when R a finite field. We will use these bounds to prove a slightly weaker bound leading up to Theorem 1.3. Currently we are able to show that the rank of $W_{p^k, n}$ is only larger than $\approx p^{kn/2}$ which does not lead to any non-trivial bounds on the size of Kakeya sets. The matrix $W_{p^k, n}$, which is referred to in the literature as the incidence matrix of *Hjelmslev spaces* was shown to have full rank over the rational numbers [LV14] but the rank over \mathbb{F}_p seems to be open. We note that our reduction is only in one direction – showing that $W_{p^k, n}$ has low rank would not imply the existence of small Kakeya sets using our theorem.

1.1. Overview of the proof

Our proof consists of two main parts. The first gives a new formulation of the polynomial proof for Kakeya sets over finite fields (in our case, prime N). Our proof relies on the same underlying principles of the polynomial method but uses them in a way that gives us more control. The second part uses this modified proof for general square-free N by inducting on the number of prime factors. We now describe each part in more detail.

Consider a Kakeya set $S \subset \mathbb{F}_p^n$. The first new idea in the proof is to replace the size of the set S with the rank of a $0 - 1$ matrix M_S we call the *line-matrix* of S . This matrix has a row for each direction $b \in \mathbb{PF}_p^{n-1}$ and that row is the indicator vector $\mathbf{1}_{L(b)}$ for a line $L(b) \subset S$ in direction b . That is, each column of M_S is indexed by some $x \in \mathbb{F}_p^n$ and the b 'th row has ones in positions indexed by the points in $L(b)$ and zeros everywhere else. It is not hard to show (and proven in Lemma 2.2) that, over any field,

$$\text{rank}(M_S) \leq |S| \leq p \cdot \text{rank}(M_S)$$

and so the rank is a good proxy for $|S|$ (for the upper bound we require that S is, in some sense, a minimal Kakeya set). We will bound the rank of M_S over \mathbb{F}_p by constructing two fixed matrices (independent of S) which we denote for now by A and B such that A has high rank and $A = M_S \cdot B$. Since the rank of $M_S \cdot B$ is at most the rank of M_S we get that $|S| \geq \text{rank}(A)$.

We leave the description of the matrices A and B (which involves polynomials) to the technical sections as these are not needed to explain the second part of the proof. One comment is that the above outline is only enough to prove a slightly weaker version of Theorem 1.3 (with the “right” exponent n but worse dependence on r). To prove the tighter bound as in the theorem we need to work with a variant of M_S in which each line $L(b)$ has many rows associated with it, each supported on $L(b)$ but with different non-zero values. The construction of the fixed matrices A and B is also different and uses the extended variant of the polynomial method using high order derivatives (as in [DKSS13]). We present both the simplified and full proof in the technical sections below.

With the first part in place, we can now describe the case of composite N . For simplicity, assume $N = p \cdot q$ is a product of two primes and let $R = \mathbb{Z}/N\mathbb{Z}$. Notice that, by the Chinese remainder theorem, $R^n \cong \mathbb{F}_p^n \times \mathbb{F}_q^n$ and any line $L(b)$ in direction $b \in \mathbb{P}R^{n-1}$ is a Cartesian product of a line $L_p(b) \subset \mathbb{F}_p^n$ and a line $L_q(b) \subset \mathbb{F}_q^n$. Notice that each of the lines $L_p(b), L_q(b)$ might depend on both the $b \pmod{p}$ part and the $b \pmod{q}$ part of the direction b (otherwise our lives would be much easier as S would be a product of a Kakeya set in \mathbb{F}_p^n and a Kakeya set in \mathbb{F}_q^n). We construct the line matrix M_S as before, working over the field \mathbb{F}_p and treating the rows of M_S as elements in the tensor product $\mathbb{F}_p^{p^n} \otimes \mathbb{F}_p^{q^n}$. That is, each row is a function from R^n to \mathbb{F}_p . From the above discussion, each row $\mathbf{1}_{L(b)}$ is the tensor product of $\mathbf{1}_{L_p(b)}$ and $\mathbf{1}_{L_q(b)}$. We now recall the matrices A and B from the first part so that, $A = M_T \cdot B$ for any Kakeya set $T \subset \mathbb{F}_p^n$. The final step of the proof is multiplying M_S by the Kronecker product $B \otimes I_{q^n}$, where I_{q^n} is a $q^n \times q^n$ identity matrix and analysing the dimension of the space spanned by the rows. This requires both the rank bound on A as well as the inductive bound on Kakeya sets over \mathbb{F}_q^n (which imply rank bounds on the corresponding line-matrix over any field, including \mathbb{F}_p).

To prove Theorem 1.5 we would ideally like to construct a matrix B such that $W_{p^k, n} = M_S \cdot B$ (which would prove the theorem by the above discussion). While we are not able to directly do that, we are able to construct a *complex* matrix B such that $M_S \cdot B$ has the same support as $W_{p^k, n}$ and whose non-zero entries are all complex roots of unity of order p^k . We then show that the complex rank of such a matrix is lower bounded by the \mathbb{F}_p rank of $W_{p^k, n}$.

1.2. Organization

In Section 2 we (re)prove the finite field Kakeya conjecture using the rank of the line matrix M_S . In Section 3 we show how to handle multiple prime factors by proving a weaker version of Theorem 1.3 for the special case $N = pq$. In Section 4 we prove Theorem 1.3 in full generality by adding the use of high order derivatives. In Section 5 we discuss the case of prime powers $R = \mathbb{Z}/p^k\mathbb{Z}$ and prove Theorem 1.5.

2. Warm-up 1: Reproving the finite field bound

We start by defining the line-matrix M_S associated with a Kakeya set $S \subset R^n$.

Definition 2.1 (Line matrix of S). The line matrix M_S for a Kakeya set S in R^n is a matrix with 0, 1 entries where the columns are indexed by points in R^n and the rows are indexed by directions $b \in \mathbb{P}R^{n-1}$ and the row corresponding to b is the indicator vector $\mathbf{1}_{L(b)} \in \{0, 1\}^{|R^n|}$

of a line $L(b)$ in direction b contained in S (if there is more than one such line, we pick the first one in some pre-determined order).

We note as M_S is a matrix with 0, 1 entries we can treat it as a matrix over any field \mathbb{F} . Given any integer matrix M we let $\text{rank}_{\mathbb{F}}(M)$ refer to the rank of the matrix M over the field \mathbb{F} .

Lemma 2.2 (Rank-Size relation). *Let $S \subseteq \mathbb{R}^n$ be a Kakeya set and \mathbb{F} a field. Then*

$$|S| \geq \text{rank}_{\mathbb{F}}(M_S).$$

Furthermore, if S' is the set of non-zero columns in M_S (by identifying the columns by their indices in \mathbb{R}^n we see that S' is itself also a Kakeya set in \mathbb{R}^n) then

$$\text{rank}_{\mathbb{F}}(M_S) \geq \frac{|S'|}{|R|}.$$

Proof. The lower bound on $|S|$ is trivial since all rows are supported on elements of S . To prove the other direction we iteratively pick lines from S' as follows. We first start with a line L_1 . After picking lines L_1, L_2, \dots, L_t we pick a line L_{t+1} which is not completely contained in the union $\bigcup_{i=1}^t L_i$. The size of the union $\bigcup_{i=1}^t L_i$ is at most $|R|t$ so, since S' is defined to be the union of the lines forming the rows of M_S , we can continue this procedure as long as $t|R| < |S'|$. This will give us a set of lines L_1, \dots, L_r where $r = \lceil |S'|/|R| \rceil$ with the property that the line L_{t+1} is not completely contained in $\bigcup_{i=1}^t L_i$ for all $t < |S'|/|R|$. The vectors $\mathbf{1}_{L_i}$ are clearly linearly independent since they correspond to an upper triangular matrix after changing the basis using an appropriate permutation matrix. \square

From now on we will focus on giving a lower bound on the rank of M_S for a Kakeya set $S \subset \mathbb{F}_p^n$ with p prime. As outlined in the proof overview, we are looking to construct two matrices A and B so that $A = M_S \cdot B$ for any Kakeya set S and such that A has high rank. Both A and B will be related to the point-hyperplane incidence matrix which we now define. By a hyperplane we mean a subset $H_b \subset \mathbb{F}_p^n$ of the form $H_b = \{a \in \mathbb{F}_p^n, |\langle b, a \rangle = 0\}$. We denote by $\bar{H}_b = \{a \in \mathbb{F}_p^n, |\langle b, a \rangle \neq 0\}$ the complement of the hyperplane.

Definition 2.3 (Point-hyperplane incidence matrix). Given a prime p and a natural number n we define the point-hyperplane incidence matrix $W_{p,n}$ to be the $p^n \times p^n$ matrix whose columns are the indicator vectors of the hyperplanes $\mathbf{1}_{H_b}$ over all $b \in \mathbb{F}_p^n$ and the rows are indexed by points in \mathbb{F}_p^n . Notice that each row/column of $W_{p,n}$ (except for the one indexed by zero) is repeated $p-1$ times as scaling by a non-zero field element does not affect whether or not the inner product is 0.

Our proof will rely on the following simple but useful property of this matrix.

Lemma 2.4 (Action of $W_{p,n}$ on lines). *Let $L \subseteq \mathbb{F}_p^n$ be a line in direction $b \in \mathbb{P}\mathbb{F}_p^{n-1}$ and let $\mathbf{1}_L \in \mathbb{F}_p^{p^n}$ be its (row) indicator vector. Then, over the field \mathbb{F}_p , we have*

$$\mathbf{1}_L \cdot W_{p,n} = \mathbf{1}_{\bar{H}_b}.$$

Hence, the product only depends on the direction of the line L .

Proof. The coordinate of $\mathbf{1}_L \cdot W_{p,n}$ indexed by $a \in \mathbb{F}_p^n$ is the inner product of $\mathbf{1}_L$ and $\mathbf{1}_{H_a}$ and so is equal to the size (mod p) of the intersection $L \cap H_a$. For $a = 0$ the intersection size is $|L| = p$ which is zero mod p . This is also the 0 entry in $\mathbf{1}_{\overline{H}_b}$ since $0 \notin \overline{H}_b$. Now suppose $a \neq 0$. The size of the intersection of a line L with a non-trivial hyperplane H_a can have one of three values. If the direction b of the line L is not in H_a then $|L \cap H_a| = 1$. If $b \in H_a$ then $|L \cap H_a|$ can be either 0 or $|L|$ which are both equal to 0 modulo p . Hence, over \mathbb{F}_p we have $(\mathbf{1}_L \cdot W_{p,n})_a = (\mathbf{1}_{\overline{H}_b})_a$. \square

We will also need a bound on the rank of the matrix $W_{p,n}$. These matrices have been studied in the coding community since the 1960's and their rank has been computed via several methods. In particular, the following is a special case of results appearing in [GD68, MM68, Smi69]. The proofs involve using studying the point-hyperplane incidence matrix for the projective space \mathbb{PF}_p^n , identifying \mathbb{PF}_p^n with the cyclic group $\mathbb{F}_{p^{n+1}}^\times / \mathbb{F}_p^\times$, and using its representation theory over \mathbb{F}_p .

Theorem 2.5 (\mathbb{F}_p -rank of $W_{p,n}$). *Let $W_{p,n}$ be the point-hyperplane incidence matrix of \mathbb{F}_p^n . Then*

$$\text{rank}_{\mathbb{F}_p}(W_{p,n}) = \binom{p+n-2}{n-1} + 1.$$

We will conclude this section by demonstrating how the information obtained so far for $W_{p,n}$ can be used to give a bound on Kakeya sets over prime order finite fields.²

Theorem 2.6. *Let $S \subset \mathbb{F}_p^n$ be a Kakeya set. Then*

$$|S| \geq \binom{p+n-2}{n-1}.$$

Proof. Working over the field \mathbb{F}_p , let M_S be the line matrix of S and let

$$A = M_S \cdot W_{p,n}.$$

By Lemma 2.4 we have that the row of A indexed by $b \in \mathbb{PF}_p^{n-1}$ is the indicator vector $\mathbf{1}_{\overline{H}_b}$. Let $A' = J - A$ where J is a matrix with all entries equal to one. Then, the matrix A' has the same rows (without repetition) as those of $W_{p,n}$ and hence the same rank. Since J is rank one, we get that

$$\text{rank}_{\mathbb{F}_p}(A) \geq \text{rank}_{\mathbb{F}_p}(W_{p,n}) - 1 = \binom{p+n-2}{n-1}.$$

Since

$$|S| \geq \text{rank}_{\mathbb{F}_p}(M_S) \geq \text{rank}_{\mathbb{F}_p}(M_S \cdot W_{p,n})$$

we get the claimed bound. \square

²One can generalize the proof using $W_{p,n}$ also to fields of size p^t but the resulting bounds are not as good as the ones obtained directly from the polynomial methods.

The relationship between the above proof and the polynomial method proof appearing in [Dvi09] is somewhat elusive at this point and will become clearer when we prove the stronger bound appearing in Theorem 1.3. However, the proof of this section could be taken on its own as a ‘new’ proof of the finite field bound which does not use polynomials in any explicit way (but, in turn, relies on the rank bound of Theorem 2.5). The bound obtained above only gives an exponent of $n - 1$ instead of n . However, this can be amplified to $n - \epsilon$ for all ϵ using a standard tensoring trick (see Lemma 3.3).

3. Warm-up 2: Product of two primes

In this section we show how the proof of the finite field case given in the previous section allows us to work with composite (square-free) modulus. For the sake of simplicity we deal with the case of two distinct primes as it already contains all the technical details of the general case.

First, we define the Kronecker Product of two matrices and its relation to the tensor product. We denote $[r] = \{1, 2, \dots, r\}$.

Definition 3.1 (Kronecker Product of two matrices). Given a field \mathbb{F} and two matrices M_A and M_B of sizes $n_1 \times m_1$ and $n_2 \times m_2$ corresponding to linear maps $A : \mathbb{F}^{n_1} \rightarrow \mathbb{F}^{m_1}$ and $B : \mathbb{F}^{n_2} \rightarrow \mathbb{F}^{m_2}$ respectively, we define the Kronecker product $M_A \otimes M_B$ as a matrix of size $n_1 n_2 \times m_1 m_2$ with its rows indexed by elements in $[n_1] \times [n_2]$ and its columns indexed by elements in $[m_1] \times [m_2]$ such that

$$M_A \otimes M_B((r_1, r_2), (c_1, c_2)) = M_A(r_1, c_1)M_B(r_2, c_2),$$

where $r_1 \in [n_1], r_2 \in [n_2], c_1 \in [m_1]$ and $c_2 \in [m_2]$. $M_A \otimes M_B$ corresponds to the matrix of the linear map $A \otimes B : \mathbb{F}^{n_1} \otimes \mathbb{F}^{n_2} \cong \mathbb{F}^{n_1 n_2} \rightarrow \mathbb{F}^{m_1} \otimes \mathbb{F}^{m_2} \cong \mathbb{F}^{m_1 m_2}$.

We will need the following simple property of Kronecker products which follows from the corresponding property of the tensor product of linear maps.

Fact 3.1 (Multiplication of Kronecker products). *Given matrices A_1, A_2, B_1 and B_2 of sizes $a_1 \times n_1, a_2 \times n_2, n_1 \times b_1$ and $n_2 \times b_2$ we have the following identity,*

$$(A_1 \otimes A_2) \cdot (B_1 \otimes B_2) = (A_1 \cdot B_1) \otimes (A_2 \cdot B_2).$$

For the rest of this section, let $N = pq$ be a product of distinct primes and denote $R = \mathbb{Z}/N\mathbb{Z}$. Recall that, via the Chinese remainder theorem, we have a natural isomorphism between R and $\mathbb{F}_p \times \mathbb{F}_q$ which extends to $R^n \cong \mathbb{F}_p^n \times \mathbb{F}_q^n$. We will work in the tensor product $\mathbb{F}_p^{p^n} \otimes \mathbb{F}_p^{q^n}$ which we will identify with the space $\mathbb{F}_p^{N^n}$. If we consider $v \in \mathbb{F}_p^{p^n}$ as a function $v : \mathbb{F}_p^n \mapsto \mathbb{F}_p$ and $u \in \mathbb{F}_p^{q^n}$ as a function $u : \mathbb{F}_q^n \mapsto \mathbb{F}_p$ then their tensor product $v \otimes u \in \mathbb{F}_p^{N^n}$ is the function $v \otimes u : R^n \mapsto \mathbb{F}_p$ defined by $(v \otimes u)(x_p, x_q) = v(x_p) \cdot u(x_q)$ where $(x_p, x_q) \in \mathbb{F}_p^n \times \mathbb{F}_q^n$ is a general element in R^n via the Chinese remainder theorem.

We will need the following simple lemma on the rank of certain sets of vectors inside the tensored space.

Lemma 3.2. *Let V and U be finite dimensional vector spaces over an arbitrary field \mathbb{F} . Let $A = \{v_1, v_2, \dots, v_n\} \subseteq V$ be a set of linearly independent vectors and $B_1, B_2, \dots, B_n \subseteq U$ be subsets such that each B_i spans a subspace of dimension at least k . Then the space spanned by the vectors $\bigcup_{i=1}^n \{v_i \otimes y \mid y \in B_i\}$ has dimension at least nk in $V \otimes U$.*

Proof. Let $C = \{c_1, \dots, c_m\}$ be some basis of U where we let m be the dimension of U . Then $v_i \otimes c_j$ where $i \in [n]$ and $j \in [m]$ form a linearly independent set of vectors in $V \otimes U$. For each set B_i we can find a set of k linearly independent vectors $B'_i = \{b_1^i, \dots, b_k^i\}$ all of which can be written as a linear combination of elements in C .

We will show the set of vectors $\bigcup_{i=1}^n \{v_i \otimes y \mid y \in B'_i\}$ is linearly independent to prove the lemma. Let us consider a linear combination of these vectors which equals 0,

$$\sum_{i=1}^n \sum_{j=1}^k \alpha_{i,j} v_i \otimes b_j^i = 0,$$

where $\alpha_{i,j}$ are scalars. This means,

$$\sum_{i=1}^n v_i \otimes \left(\sum_{j=1}^k \alpha_{i,j} b_j^i \right) = 0. \quad (3.1)$$

Consider the linear projection operator P_i defined on $\text{span}\{v_i, i \in [n]\} \otimes U$ as,

$$P_i(v_j \otimes c_k) = \begin{cases} c_k & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}.$$

Applying P_i on (3.1) gives us,

$$\sum_{j=1}^k \alpha_{i,j} b_j^i = 0.$$

As b_1^i, \dots, b_k^i are linearly independent we have $\alpha_{i,j} = 0$ for all i and j . \square

We will also need the following simple claim which allows one to amplify a bound of the form N^{n-c} for some constant c to a bound of the form $N^{n-\epsilon}$ for any $\epsilon > 0$.

Lemma 3.3. *If S is a Kakeya set in R^n where $R = \mathbb{Z}/N\mathbb{Z}$ for square-free N , then $S^t \subseteq R^{tn}$ which is the product of S with itself t times is also a Kakeya set in R^{tn} .*

Proof. It is enough to consider the case $t = 2$. Let $b \in \mathbb{P}R^{2n-1}$ be some direction and, by abuse of notation, let us think of $b \in R^{2n}$ as some representative of this direction. Write $b = (b', b'')$ where b' is the first n coordinates of b and b'' are the last n coordinates (each corresponding to a different copy of S). If $N = p_1 \cdots p_r$, for each i we let $b'_i = b' \pmod{p_i}$ and similarly for b'' . If all b'_i and b''_i are non-zero then we are in a situation where b' and b'' are ‘legal’ directions in $\mathbb{P}R^{n-1}$ and so there will be lines L', L'' in S in these directions. Therefore the product $L' \times L'' \subseteq S^2$ will contain a line in direction b .

A slightly more delicate case occurs when some of the b'_i or b''_i are zero. In this case, let $L' \subset S$ be a line in some direction c' that agrees with b' modulo all p_i for which b'_i is non zero and take L'', c'' in a similar manner. We now have to check that the product $L' \times L''$ contains a line in direction $b = (b', b'')$. Suppose $L' = \{a' + tc' \mid t \in R\}$ and similarly $L'' = \{a'' + tc'' \mid t \in R\}$. Consider the line in R^{2n} in direction $b = (b', b'')$ through $a = (a', a'')$. A general point on this line looks like $x(t) = (a' + tb', a'' + tb'')$. Now, the set $L' \times L''$ contains all points of the form $y(t', t'') = (a' + t'c', a'' + t''c'')$. We now have to check that the point $x(t)$ as above is in this product. Let $t' \in R$ be the same as t but with $t' \equiv 0 \pmod{p_i}$ for all p_i such that $b'_i = 0$ and similarly let t'' be the same as t but with $t'' \equiv 0 \pmod{p_i}$ for all p_i such that $b''_i = 0$. We have $t'c' = tb'$ and similarly $t''c'' = tb''$. Therefore, $x(t) = y(t', t'')$ and we are done. \square

We are now ready to prove the main result of this section.

Theorem 3.4 (Kakeya bound in $(\mathbb{Z}/pq\mathbb{Z})^n$). *Let p and q be distinct primes and let $S \subset (\mathbb{Z}/pq\mathbb{Z})^n$ be a Kakeya set. Then, for any $\epsilon > 0$ there exists a constant $C_{n,\epsilon}$ depending only on n and ϵ so that*

$$|S| \geq C_{n,\epsilon} \cdot (pq)^{n-\epsilon}.$$

Proof. Let $R = \mathbb{Z}/pq\mathbb{Z}$. All our vectors and matrices will be over \mathbb{F}_p . Given a Kakeya set $S \subseteq R^n$ consider the line matrix M_S associated with S over the field \mathbb{F}_p . Our goal is to lower bound $\text{rank}_{\mathbb{F}_p}(M_S)$. For a direction

$$b = (b_p, b_q) \in \mathbb{PF}_p^{n-1} \times \mathbb{PF}_q^{n-1},$$

the row in M_S corresponding to b will be the indicator vector $\mathbf{1}_{L(b)} \in \mathbb{F}_p^{|R^n|}$ of a line in direction b contained in S denoted

$$L(b) = L(b_p, b_q) = L_p(b_p, b_q) \times L_q(b_p, b_q)$$

which is itself Cartesian product of lines $L_p(b_p, b_q) \subseteq \mathbb{F}_p^n$ in the direction b_p and $L_q(b_p, b_q) \subseteq \mathbb{F}_q^n$ in the direction b_q . Note, $L_p(b_p, b_q)$ includes b_q because the lines $L_p(b_p, c_1)$ and $L_p(b_p, c_2)$ can be potentially different when $c_1 \neq c_2$. Finally, notice that the indicator vector $\mathbf{1}_{L(b)} \in \mathbb{F}_p^{|R^n|}$ equals the tensor product

$$\mathbf{1}_{L(b)} = \mathbf{1}_{L_p(b_p, b_q)} \otimes \mathbf{1}_{L_q(b_p, b_q)}.$$

Let $W_{p,n}$ be the point-hyperplane incidence matrix defined in the previous section. Let I_{q^n} be the identity matrix of size $q^n \times q^n$. The rows and columns in I_{q^n} are thought to be indexed by points in \mathbb{F}_q^n . Consider the Kronecker product $W_{p,n} \otimes I_{q^n}$. We will examine the product

$$M_S \cdot (W_{p,n} \otimes I_{q^n}).$$

If we look at the row in M_S indexed by a direction $b = (b_p, b_q) \in \mathbb{PF}_p^{n-1} \times \mathbb{PF}_q^{n-1}$, the corresponding row in $M_S \cdot (W_{p,n} \otimes I_{q^n})$ is the product,

$$\begin{aligned} \mathbf{1}_{L(b)} \cdot (W_{p,n} \otimes I_{q^n}) &= (\mathbf{1}_{L_p(b_p, b_q)} \otimes \mathbf{1}_{L_q(b_p, b_q)}) \cdot (W_{p,n} \otimes I_{q^n}) \\ &= (\mathbf{1}_{L_p(b_p, b_q)} \cdot W_{p,n}) \otimes \mathbf{1}_{L_q(b_p, b_q)} \quad (\text{Using Fact 3.1}) \\ &= \mathbf{1}_{\bar{H}_{b_p}} \otimes \mathbf{1}_{L_q(b_p, b_q)}, \end{aligned} \tag{3.2}$$

where we recall \overline{H}_c is the set $\{x \mid \langle x, c \rangle \neq 0\} \subseteq \mathbb{F}_p^n$ where $c \in \mathbb{PF}_p^{n-1}$ and the last step in (3.2) uses Lemma 2.4.

Denote the set of vectors

$$V = \{\mathbf{1}_{\overline{H}_c} \mid c \in \mathbb{PF}_p^{n-1}\} \subset \mathbb{F}_p^{p^n}$$

and, for each $c \in \mathbb{PF}_p^{n-1}$, the set of vectors

$$B_c = \{\mathbf{1}_{L_q(c, b_q)} \mid b_q \in \mathbb{PF}_q^{n-1}\} \subset \mathbb{F}_p^{q^n}.$$

From Theorem 2.5 (following the argument in Theorem 2.6) we know that the dimension the space spanned by V is at least $\binom{p+n-2}{n-1}$. Next, fix some $c \in \mathbb{PF}_p^{n-1}$. The vectors forming B_c are the indicators of a set of lines in every direction in \mathbb{F}_q^n . Lemma 2.2, combined with the bound on Kakeya sets in \mathbb{F}_q^n (Theorem 1.2) imply that B_c will have rank at least $q^{n-1}2^{-n}$ over any field and in particular over \mathbb{F}_p . Hence, by Lemma 3.2 we have that the set of vectors

$$\{\mathbf{1}_{\overline{H}_c} \otimes u \mid c \in \mathbb{PF}_p^{n-1}, u \in B_c\}$$

has rank at least

$$\binom{p+n-2}{n-1} \cdot q^{n-1}2^{-n}.$$

Since these are the rows of M_S after multiplying by a matrix $W_{p,n} \otimes I_{q^n}$ we get that this is also a lower bound on the rank of M_S . By Lemma 2.2, we have that

$$|S| \geq \binom{p+n-2}{n-1} \cdot q^{n-1}2^{-n} \geq C_n \cdot N^{n-1}$$

for some constant C_n depending only on n . The bound in the theorem now follows from applying the weaker bound on the t -fold Cartesian product $S^t = S \times \dots \times S \subset \mathbb{R}^{nt}$ (which is also a Kakeya set by Lemma 3.3) and then use the fact that $|S^t| = |S|^t$. \square

4. The general square-free N case

To get the bound stated in Theorem 1.3 we will generalize the proof structure of Section 2 to use ideas from the extended polynomial method using high order multiplicities as in [DKSS13].

We begin with some definitions and basic results concerning polynomials over finite fields. We let $\mathbb{F}_p[x_1, \dots, x_n]_{=d}$ denote the vector space of homogeneous n -variate degree d polynomials over \mathbb{F}_p and $\mathbb{F}_p[x_1, \dots, x_n]_{\leq d}$ denote the space of polynomials of degree at most d . We let

$$\delta_{n,d} = \binom{n+d-1}{n-1}$$

denote the dimension of the space $\mathbb{F}_p[x_1, \dots, x_n]_{=d}$ and

$$\Delta_{n,d} = \binom{n+d}{n}$$

the dimension of $\mathbb{F}_p[x_1, \dots, x_n]_{\leq d}$. For a tuple $\mathbf{i} \in \mathbb{Z}_{\geq 0}^n$ we define the weight of \mathbf{i} as

$$\text{wt}(\mathbf{i}) = \sum_{j=1}^n i_j.$$

Definition 4.1 (Hasse Derivatives). Given a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ for any field \mathbb{F} and an $\mathbf{i} \in \mathbb{Z}_{\geq 0}^n$ the i th *Hasse derivative* of f is the polynomial $f^{(\mathbf{i})}$ in the expansion $f(x + z) = \sum_{\mathbf{j} \in \mathbb{Z}_{\geq 0}^n} f^{(\mathbf{j})}(x)z^{\mathbf{j}}$ where $x = (x_1, \dots, x_n)$, $z = (z_1, \dots, z_n)$ and $z^{\mathbf{j}} = \prod_{k=1}^n z_k^{j_k}$.

Definition 4.2 (Multiplicity). For a polynomial $f \in \mathbb{F}[x_1, \dots, x_n]$ and a point $a \in \mathbb{F}^n$ we say f vanishes on a with *multiplicity* $m \in \mathbb{Z}$, if m is the largest integer such that all Hasse derivatives of f of weight strictly less than m vanish on a . We use $\text{mult}(f, a)$ to refer to the multiplicity of f at a .

Notice, $\text{mult}(f, a) = 1$ just means $f(a) = 0$. Also the number of Hasse derivatives over $\mathbb{F}[x_1, \dots, x_n]$ with weight strictly less than m is $\Delta_{n, m-1}$. One can also check that for a univariate polynomial $f(x)$ to vanish at a with multiplicity m , f must be divisible by $(x - a)^m$.

We will need an extended Schwartz–Zippel bound [Sch79, Zip79] which leverages multiplicities. The proof can be found in [DKSS13].

Lemma 4.3 (Schwartz–Zippel with multiplicities). *Let $f \in \mathbb{F}[x_1, \dots, x_n]_{\leq d}$, with \mathbb{F} an arbitrary field and $d \in \mathbb{Z}$. Then for any finite subset $U \subseteq \mathbb{F}$,*

$$\sum_{a \in U^n} \text{mult}(f, a) \leq d|U|^{n-1}.$$

We now define a family of linear maps sending a polynomial to a list of its evaluations (with derivatives) over some set. These maps (or more precisely, the matrices representing them) will replace the matrices $W_{p,n}$ used in Section 2.

Definition 4.4 (Evaluation maps). For a prime p , natural numbers n and m , given a set A in \mathbb{F}_p^n , we let

$$\text{EVAL}_A^m : \mathbb{F}_p[x_1, \dots, x_n] \rightarrow \mathbb{F}^{|A|\Delta_{n, m-1}}$$

refer to the linear map from $\mathbb{F}_p[x_1, \dots, x_n]$ to the evaluation of all Hasse derivatives of weight strictly less than m over the set A . We treat the points in the co-domain $\mathbb{F}_p^{|A|\Delta_{n, m-1}}$ as column vectors of length $|A|\Delta_{n, m-1}$ indexed by tuples $(x, \mathbf{j}) \in A \times \mathbb{Z}_{\geq 0}^n$ with $\text{wt}(\mathbf{j}) < m$. The (x, \mathbf{j}) th entry of $\text{EVAL}_A^m(f)$ for a polynomial $f \in \mathbb{F}_p[x_1, \dots, x_n]$ is $f^{(\mathbf{j})}(x)$. For singleton sets $\{x\}$ we omit the curly braces and write EVAL_x^m .

We will now construct matrices C_L^k which will replace the indicators $\mathbf{1}_{L(b)}$ used as the rows of M_S in the proofs of the previous sections. Intuitively, the matrix C_L^k for some line L in direction b corresponds to the linear map which takes as input the evaluations (up to some order m depending on k) of a polynomial f on the line L and output the evaluation of f (up to order k) at the point b . This is possible as long as the degree of f is not too big as a consequence of Lemma 4.3.

Lemma 4.5 (The decoding matrix C_L^k). *Given a prime p , numbers $k, n, m \in \mathbb{Z}_{\geq 0}$ where $p|k$ and $m = 2k - k/p$, and a line $L \subseteq \mathbb{F}_p^n$ in the direction $b \in \mathbb{P}\mathbb{F}_p^{n-1}$, we can construct a $\Delta_{n,k-1} \times p^n \Delta_{n,m-1}$ matrix C_L^k such that,*

1. *The rows in the matrix C_L^k are indexed by points $\mathbf{i} \in \mathbb{Z}_{\geq 0}^n$, $\text{wt}(\mathbf{i}) < k$ and the columns are indexed by tuples $(x, \mathbf{j}) \in \mathbb{F}_p^n \times \mathbb{Z}_{\geq 0}^n$ with $\text{wt}(\mathbf{j}) < m$.*
2. *The only non-zero columns are the ones corresponding to tuples (x, \mathbf{j}) with $x \in L$.*
3. *For a polynomial $f \in \mathbb{F}_p[x_1, \dots, x_n]_{=kp-1}$ we have,*

$$C_L^k \cdot \text{EVAL}_{\mathbb{F}_p^n}^m(f) = \text{EVAL}_b^k(f).$$

Proof. We will need the following two claims.

Claim 4.1. *For homogenous polynomials f of degree $kp - 1$ we have*

$$\text{EVAL}_L^m(f) = 0 \implies \text{EVAL}_b^k(f) = 0, \quad (4.1)$$

where $m = 2k - k/p$.

The proof can be found in Theorem 11 (in the arxiv version) and Theorem 3.2 (in the SIAM version) of [DKSS13] and is a consequence of Lemma 4.3.

Claim 4.2. *Let A be an $n_1 \times w$ matrix and B be an $n_2 \times w$ matrix both over a field \mathbb{F} and suppose that, for all $x \in \mathbb{F}^w$ we have,*

$$Ax = 0 \implies Bx = 0.$$

Then there exists a matrix C of size $n_2 \times n_1$ such that $C \cdot A = B$.

Proof. For all $x \in \mathbb{F}^w$, $Ax = 0 \implies Bx = 0$ means the kernel of A is a subset of the kernel of B . This means every row of B is spanned by the row space of A . This immediately implies that we can construct C such that $CA = B$. \square

Combining the two claims lets us construct a matrix C' such that

$$C' \cdot \text{EVAL}_L^m(f) = \text{EVAL}_b^k(f). \quad (4.2)$$

The columns in C' are indexed by tuples $(x, \mathbf{j}) \in L \times \mathbb{Z}_{\geq 0}^n$ such that $\text{wt}(\mathbf{j}) < m$. We add zero columns to C' corresponding to tuples $(x, \mathbf{j}) \in (\mathbb{F}_p^n \setminus L) \times \mathbb{Z}_{\geq 0}^n$ with $\text{wt}(\mathbf{j}) < m$. This gives us C_L^k . By construction it satisfies the first two properties. The third property follows from (4.2). \square

In our proof, it will be convenient to work with the following extension of rank for sets of matrices.

Definition 4.6 (crank of a set of matrices). Given a finite set $T = \{A_1, \dots, A_n\}$ of matrices over a field \mathbb{F} having the same number of columns we let $\text{crank}(T)$ be the rank of the matrix obtained by concatenating all the elements A_i in T along their columns. In other words it is the dimension of the subspace spanned by the vectors in the set $\bigcup_{i=1}^n \{r \mid r \text{ is a row in } A_i\}$.

We will use a simple lemma which follows from the definition.

Lemma 4.7 (crank bound for multiplying matrices). *Given matrices A_1, \dots, A_n of size $a \times b$ and a matrix H of size $b \times c$ we have*

$$\text{crank}\{A_i\}_{i=1}^n \geq \text{crank}\{A_i \cdot H\}_{i=1}^n.$$

We now need an extension of Lemma 3.2 for this definition.

Lemma 4.8 (crank bound for tensor products). *Given matrices A_1, \dots, A_n of size $a_1 \times a_2$ over a field \mathbb{F} such that $\text{crank}\{A_i\}_{i=1}^n \geq r_1$ and matrices $B_{i,j}$ over the field \mathbb{F} for $i \in [n]$ and $j \in [m]$ of size $b_1 \times b_2$ such that $\text{crank}\{B_{i,j}\}_{j=1}^m \geq r_2$ for all $i \in [n]$ we have,*

$$\text{crank}\{A_i \otimes B_{i,j} \mid i \in [n], j \in [m]\} \geq r_1 r_2.$$

Proof. Let $V = \bigcup_{i=1}^n \{w \mid w \text{ is a row in } A_i\}$ and $U_i = \bigcup_{j=1}^m \{w \mid w \text{ is a row in } B_{i,j}\}$ for $i \in [n]$. V has rank at least r_1 and each of the U_i will have rank at least r_2 . Using Lemma 3.2 we see that the set of vectors $\bigcup_{i=1}^n \{w_1 \otimes w_2 \mid w_1 \text{ is a row in } A_i, w_2 \in U_i\}$ will have rank at least $r_1 r_2$. This gives us the desired crank bound too. \square

4.1. Proof of Theorem 1.3

We are now ready to prove our main result restated here for convenience.

Theorem 1.3. *Let $N = p_1 \dots p_r$ for distinct primes p_1, \dots, p_r . Any Kakeya Set $S \subseteq (\mathbb{Z}/N\mathbb{Z})^n$ satisfies*

$$|S| \geq \frac{N^n}{\prod_{i=1}^r (2 - 1/p_i)^n}.$$

Proof. We will prove this using induction over r . When $r = 1$ the result is known via Theorem 1.2.

Let us assume the bound holds for a product of r primes. Let $N = p_1 \dots p_{r+1}$ for $r+1$ distinct primes and $R = \mathbb{Z}/N\mathbb{Z}$. To prove a lower bound let us take a Kakeya set S in R^n . For convenience we let $N_0 = p_2 p_3 \dots p_{r+1}$ and $R_0 = \mathbb{Z}/N_0\mathbb{Z}$.

All our matrices and indicator vectors will be over \mathbb{F}_{p_1} . By the Chinese remainder theorem R^n is isomorphic to $\mathbb{F}_{p_1}^n \times R_0^n$. Every direction $b \in \mathbb{P}R^{n-1}$ is represented by a tuple $(b_1, b_0) \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}$. Any line $L \subseteq R^n$ in direction $b = (b_1, b_0) \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}$ is a product of lines $L_1 \subseteq \mathbb{F}_{p_1}^n$ in direction b_1 and $L_0 \subseteq R_0^n$ in direction b_0 . The indicator vector $\mathbf{1}_L \in \mathbb{F}_{p_1}^{|R^n|}$ will equal $\mathbf{1}_{L_1} \otimes \mathbf{1}_{L_0} \in \mathbb{F}_{p_1}^{|\mathbb{F}_{p_1}^n \times R_0^n|}$.

For each direction $b \in \mathbb{P}R^{n-1}$ we must have a line $L(b)$ contained in S . If there are many such lines we pick one arbitrarily. The line $L(b)$ will be the product of lines $L_1(b)$ and $L_0(b)$ in $\mathbb{F}_{p_1}^n$ and R_0^n respectively.

Let us fix a natural number k divisible by p_1 . For a direction b consider the matrix $C_{L_1(b)}^k$ (given by Lemma 4.5) over the field \mathbb{F}_{p_1} which will be of size $\Delta_{n,k-1} \times p_1^n \Delta_{n,m-1}$ with

$$m = 2k - k/p_1.$$

The following claim generalizes Lemma 2.2 and allows us to lower bound $|S|$ using a rank bound (in this case the rank of the matrix containing all rows in all $C_{L(b)}^k$).

Claim 4.3 (crank-Size relation).

$$|S| \binom{m+n-1}{n} \geq \text{crank}\{C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}\}_{b \in \mathbb{P}R^{n-1}}.$$

Proof. The columns in $C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}$ for all b , are indexed by tuples $(x, \mathbf{j}) \in R^n \times \mathbb{Z}_{\geq 0}^n$ with $\text{wt}(\mathbf{j}) < m$. By Lemma 4.5 we see the non-zero columns in $C_{L(b)}^k \otimes \mathbf{1}_{L_0(b)}$ will correspond to tuples with $x \in L_1(b) \subseteq S$. In general in all the matrices in the set $\{C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}\}_{b \in \mathbb{P}R^{n-1}}$ the non-zero columns all correspond to points $(x, \mathbf{j}) \in S \times \mathbb{Z}_{\geq 0}^n$ with $\text{wt}(\mathbf{j}) < m$. This gives us the required bound. \square

Let E be a matrix of size $p_1^n \Delta_{n,m-1} \times \delta_{n,kp_1-1}$ representing the linear map $\text{EVAL}_{\mathbb{F}_{p_1}^n}^m$ restricted to the space $\mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$ (with some arbitrary basis). Given a direction $b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}$, we let D_{b_1} be the $\Delta_{n,k-1} \times \delta_{n,kp_1-1}$ matrix representing the linear map $\text{EVAL}_{b_1}^k$ restricted to the space $\mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$. For $b = (b_1, b_0) \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}$, Lemma 4.5 implies

$$C_{L(b)}^k \cdot \text{EVAL}_{\mathbb{F}_{p_1}^n}^m(f) = \text{EVAL}_{b_1}^k(f)$$

for any $f \in \mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$. This implies

$$C_{L(b)}^k \cdot E = D_{b_1}.$$

Let $I_{N_0^n}$ be the identity matrix of size $N_0^n \times N_0^n$. Using Lemma 4.7 we have,

$$\begin{aligned} \text{crank}\{C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}\}_{b \in \mathbb{P}R^{n-1}} &\geq \text{crank}\{(C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}) \cdot (E \otimes I_{N_0^n})\}_{b \in \mathbb{P}R^{n-1}} \\ &= \text{crank}\{(C_{L_1(b)}^k \cdot E) \otimes \mathbf{1}_{L_0(b)}\}_{b \in \mathbb{P}R^{n-1}} \quad (\text{By Fact 3.1}) \\ &= \text{crank}\{D_{b_1} \otimes \mathbf{1}_{L_0(b_1, b_0)}\}_{b=(b_1, b_0) \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}}. \end{aligned} \tag{4.3}$$

To lower bound $\text{crank}\{D_{b_1} \otimes \mathbf{1}_{L_0(b_1, b_0)}\}_{b_1, b_0 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}}$ we will use Lemma 4.8. To that end we want to lower bound $\text{crank}\{D_{b_1}\}_{b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}}$ and $\text{crank}\{\mathbf{1}_{L_0(c, b_0)}\}_{b_0 \in \mathbb{P}R_0^{n-1}}$ for $c \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}$.

Claim 4.4. For all $c \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}$ we have

$$\text{crank}\{\mathbf{1}_{L_0(c, b_0)}\}_{b_0 \in \mathbb{P}R_0^{n-1}} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r+1} (2 - p_i^{-1})^n},$$

Proof. For a fixed $c \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}$ we see that

$$\bigcup_{b_0 \in \mathbb{P}R_0^{n-1}} L_0(c, b_0) \subseteq R_0^n$$

is a Kakeya set in R_0^n which is a union of lines in every direction.

We note $\text{crank}(\{\mathbf{1}_{L_0(c, b_0)}\}_{b_0 \in \mathbb{P}R_0^{n-1}})$ is just the dimension of the subspace spanned by $\{\mathbf{1}_{L_0(c, b_0)}\}_{b_0 \in \mathbb{P}R_0^{n-1}}$. Using Lemma 2.2 and the induction hypothesis we have,

$$\text{crank}(\{\mathbf{1}_{L_0(c, b_0)}\}_{b_0 \in \mathbb{P}R_0^{n-1}}) \geq \frac{|\bigcup_{b_0 \in \mathbb{P}R_0^{n-1}} L_0(c, b_0)|}{|R_0|} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r+1} (2 - p_i^{-1})^n}. \quad (4.4)$$

□

Claim 4.5 (crank bound for $\{D_{b_1}\}_{b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}}$).

$$\text{crank}(\{D_{b_1}\}_{b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}}) \geq \delta_{n, kp_1-1}.$$

Proof. To lower bound $\text{crank}(\{D_{b_1}\}_{b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}})$ we will examine the matrix $D_{\mathbb{P}\mathbb{F}_{p_1}^{n-1}}$ obtained by concatenating all the matrices in $\text{crank}(\{D_{b_1}\}_{b_1 \in \mathbb{P}\mathbb{F}_{p_1}^{n-1}})$ along their columns. We see that this is precisely the matrix for the map $\text{EVAL}_{\mathbb{P}\mathbb{F}_{p_1}^{n-1}}^k$ restricted on the input space $\mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$.

We claim $D_{\mathbb{P}\mathbb{F}_{p_1}^{n-1}}$ is injective over $\mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$. If a polynomial $f \in \mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$ lies in the kernel of $D_{\mathbb{P}\mathbb{F}_{p_1}^{n-1}}$ then that means that f and all its Hasse derivatives of weight at most k vanish over $\mathbb{P}\mathbb{F}_{p_1}^{n-1}$. As f is homogenous, all its Hasse derivatives will be too. This means that f and all its Hasse derivatives of weight at most k vanish over all of $\mathbb{F}_{p_1}^n$. This means f vanishes with multiplicity at least k over all of $\mathbb{F}_{p_1}^n$. By Lemma 4.3 we see that f must be identically zero. Hence, we have the desired injectivity.

As $\mathbb{F}_{p_1}[x_1, \dots, x_n]_{=kp_1-1}$ has dimension δ_{n, kp_1-1} we see that $D_{\mathbb{P}\mathbb{F}_{p_1}^{n-1}}$ must be of rank at least δ_{n, kp_1-1} . This also gives us the desired crank bound. □

Using Lemma 4.8 and equation (4.3) with the bounds from Claim 4.4 and Claim 4.5 we have,

$$\begin{aligned} \text{crank}\{C_{L_1(b)}^k \otimes \mathbf{1}_{L_0(b)}\}_{b \in \mathbb{P}R^{n-1}} &\geq \text{crank}\{D_{b_1} \otimes \mathbf{1}_{L_0(b_1, b_0)}\}_{(b_1, b_0) \in \mathbb{P}\mathbb{F}_{p_1}^{n-1} \times \mathbb{P}R_0^{n-1}} \\ &\geq \frac{N_0^{n-1}}{\prod_{i=2}^{r+1} (2 - p_i^{-1})^n} \cdot \delta_{n, kp_1-1}. \end{aligned}$$

Using Lemma 4.3 we have,

$$|S| \binom{2k - k/p_1 + n - 1}{n} \geq \frac{N_0^{n-1}}{\prod_{i=2}^{r+1} (2 - 1/p_i)^n} \binom{kp_1 + n - 2}{n-1}. \quad (4.5)$$

To get the right bound we assume k is a perfect square and apply (4.5) on the set $S^{\sqrt{k}}$ which is the product of S with itself \sqrt{k} times. It is going to be a Kakeya set in $R^{n\sqrt{k}}$ by Lemma 3.3.

Applying the bound for $S^{\sqrt{k}}$ we have,

$$|S|^{\sqrt{k}} \binom{2k - k/p_1 + \sqrt{kn} - 1}{\sqrt{kn}} \geq \frac{N_0^{\sqrt{kn}-1}}{\prod_{i=2}^{r+1} (2 - 1/p_i)^{\sqrt{kn}}} \binom{kp_1 + \sqrt{kn} - 2}{\sqrt{kn} - 1}.$$

Rearranging the terms we have

$$|S|^{\sqrt{k}} \geq \frac{N^{\sqrt{kn}-1}}{\prod_{i=2}^{r+1} (2 - 1/p_i)^{\sqrt{kn}}} \left(\prod_{i=0}^{\sqrt{kn}-2} \frac{kp_1 + i}{2k - k/p_1 + 1 + i} \right) \frac{\sqrt{kn}}{2k - k/p_1 + \sqrt{kn} - 1}.$$

Taking \sqrt{k} th root on both sides and letting k grow to infinity in the set of numbers which are square multiples of p_1 gives the desired result. \square

5. Kakeya Sets over $\mathbb{Z}/p^k\mathbb{Z}$

In this section we prove Theorem 1.5. Recall that $W_{p^k, n}$ is the $p^{kn} \times p^{kn}$ point-hyperplane incidence matrix defined in the introduction. We want to show the size of any Kakeya set $S \subset (\mathbb{Z}/p^k\mathbb{Z})^n$ is lower bounded by the \mathbb{F}_p rank of $W_{p^k, n}$.

We start with a lemma that generalizes the following simple observation. Suppose we have a matrix M with entries in the set $\{0, 1, -1\}$ and let \hat{M} be the same matrix with all -1 entries replaced with 1s. It is easy to see that

$$\text{rank}_{\mathbb{C}}(M) \geq \text{rank}_{\mathbb{F}_2}(\hat{M})$$

since, if some sub-determinant in \hat{M} is not zero over \mathbb{F}_2 then the corresponding determinant in M cannot be zero over the complex numbers. This trivial claim has the following less trivial generalization involving roots of unity of any prime power order.

Lemma 5.1. *Let γ be a complex primitive p^k th root of unity for prime p and natural number k . Let M be a matrix whose entries belong to the set $\{0, 1, \gamma, \dots, \gamma^{p^k-1}\}$. Let \hat{M} be a matrix of the same dimensions of M and with entries*

$$\hat{M}_{ij} = \begin{cases} 0 & \text{if } M_{i,j} = 0 \\ 1 & \text{otherwise} \end{cases}$$

Then we have,

$$\text{rank}_{\mathbb{C}}(M) \geq \text{rank}_{\mathbb{F}_p}(\hat{M}).$$

Proof. Let $Q(x)$ be a matrix obtained from M by replacing γ with a formal variable x so that $Q(\gamma) = M$ and $Q(1) = \hat{M}$. Let $f(x)$ be the determinant of some sub matrix of $Q(x)$. If

the corresponding sub-determinant of M is zero then we have $f(\gamma) = 0$. As f has integer coefficients it must be divisible by the minimal polynomial of γ which is

$$m(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1} = 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}}.$$

Hence $f(1) = 0$ modulo p and so the corresponding sub-determinant is zero also in \hat{M} when computed over \mathbb{F}_p . This proves the lemma since a non-zero $r \times r$ determinant in \hat{M} over \mathbb{F}_p implies the same non-zero determinant in M (over \mathbb{C}). \square

We are now ready to prove Theorem 1.5, stated here again for convenience.

Theorem 1.5. *Given a prime p and numbers k, n , every Kakeya set S in $(\mathbb{Z}/p^k\mathbb{Z})^n$ satisfies,*

$$|S| \geq \text{rank}_{\mathbb{F}_p}(W_{p^k, n}).$$

Proof. Let $R = \mathbb{Z}/p^k\mathbb{Z}$. Given a Kakeya set S in R^n consider the line-matrix M_S given by Definition 2.1. Let γ be a primitive p^k th root of unity in \mathbb{C} and let F be the $p^{kn} \times p^{kn}$ matrix whose rows and columns are indexed by R^n and whose entry in position $(i, j) \in R^n \times R^n$ is

$$F_{i,j} = \gamma^{\langle i, j \rangle}$$

(F is the complex Discrete Fourier Transform matrix for the group R^n).

We consider the product $M_S \cdot F$ over \mathbb{C} . Given a direction $b \in \mathbb{P}R^{n-1}$ and a point $x(b)$ consider a line

$$L(b) = \{x(b) + tb \mid t \in R\}$$

in that direction contained in S . When we multiply the row $\mathbf{1}_{L(b)}$ of M_S with F , the j 'th coordinate, for $j \in R^n$, is given by

$$(\mathbf{1}_{L(b)} \cdot F)_j = \sum_{t \in R} \gamma^{\langle x(b) + tb, j \rangle} = \begin{cases} 0 & \text{if } \langle b, j \rangle \neq 0 \pmod{p^k} \\ p^k \gamma^{\langle x(b), j \rangle} & \text{otherwise} \end{cases}.$$

A lower bound on the rank of $M_S \cdot F$ over \mathbb{C} will give a lower bound on the rank of M_S which, using Lemma 2.2, will give us a lower bound on $|S|$. Applying Lemma 5.1 we have that the rank of $M = p^{-k}(M_S \cdot F)$ over \mathbb{C} is lower bounded by the rank of \hat{M} over \mathbb{F}_p where the entry in position $(b, j) \in R^n \times R^n$ of \hat{M} is

$$\hat{M}_{(b,j)} = \begin{cases} 0 & \text{if } \langle b, j \rangle \neq 0 \pmod{p^k} \\ 1 & \text{otherwise} \end{cases}.$$

This completes the proof since the matrix \hat{M} has the same rows as the matrix $W_{p^k, n}$ (recall that we defined $W_{p^k, n}$ to have repeated rows corresponding to different scaling of the same vector). This completes the proof. \square

This reduces the question of lower bounding the size of Kakeya sets in $(\mathbb{Z}/p^k\mathbb{Z})^n$ to the estimation of the rank of a concrete matrix, independent of the set S . In the next section we show that the matrix $W_{p^k, n}$ contains an identity matrix of size roughly $p^{kn/2}$.

5.1. Rank of $W_{p^k, n}$ via Matching Vector families

Definition 5.2 (Matching Vectors). A *matching vector* (MV) family over $(\mathbb{Z}/N\mathbb{Z})^n$ is a pair (U, V) such that $U = (u_1, \dots, u_m)$ and $V = (v_1, \dots, v_m)$ with each u_i and each v_j belonging to the set $(\mathbb{Z}/N\mathbb{Z})^n$ and such that $\langle u_i, v_j \rangle = 0 \pmod{N}$ iff $i = j$.

The following simple observation relates the size of an MV family with the rank of the point-hyperplane incidence matrix.

Lemma 5.3. *If there exists a matching vector family of size m over $(\mathbb{Z}/p^k\mathbb{Z})^n$ then, for any field \mathbb{F} , we have*

$$\text{rank}_{\mathbb{F}}(W_{p^k, n}) \geq m.$$

Proof. The sub-matrix corresponding to the rows labeled by U and the columns labelled by V in $W_{p^k, n}$ is the identity matrix (after reordering). \square

Constructions of large MV families have found surprising application in combinatorics and theoretical computer science. In particular, constructions of MV families for small composite N (even for $N = 6$) and growing n given by Grolmusz [Gro00] have found a surprisingly large number of applications. For our purposes, when N is a large prime power, we will use a less known construction originally given in [DGY11] and improved by [YGK12].

Theorem 5.4 ([YGK12]). *For every integer n and any sufficiently large N , there exist MV families over $(\mathbb{Z}/N\mathbb{Z})^n$ of size at least,*

$$\left(\frac{N}{n-2}\right)^{(n-2)/2}.$$

Combining this theorem (with $N = p^k$) with Lemma 5.3 and Theorem 1.5 gives us the a lower bound for Kakeya sets in $(\mathbb{Z}/p^k\mathbb{Z})^n$ of the order of $p^{kn/2}$ which is worse than the best known bounds. Using larger MV families to lower bound the rank of $W_{p^k, n}$ cannot lead to significantly stronger bounds as it is shown in [DH13b] that those cannot be larger than $N^{n/2+O(1)}$ for any N .

Acknowledgements

The authors would like to thank Peter Sin and Ivan Landjev for helpful comments.

References

- [Bou99] J. Bourgain, *On the dimension of Kakeya sets and related maximal inequalities*, Geom. Funct. Anal. **9** (1999), no. 2, 256–282.
- [Car18] Xavier Caruso, *Almost all non-archimedean Kakeya sets have measure zero*, Confluentes Mathematici **10** (2018), no. 1, 3–40 (en).
- [DGY11] Zeev Dvir, Parikshit Gopalan, and Sergey Yekhanin, *Matching Vector codes*, SIAM Journal on Computing **40** (2011), no. 4, 1154–1178.

- [DH13a] Evan P. Dummit and Márton Hablicsek, *Kakeya sets over non-archimedean local rings*, Mathematika **59** (2013), no. 2, 257–266.
- [DH13b] Zeev Dvir and Guangda Hu, *Matching-Vector families and LDCs over large modulo*, Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, Springer, 2013, pp. 513–526.
- [DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan, *Extensions to the method of multiplicities, with applications to Kakeya sets and mergers*, SIAM Journal on Computing **42** (2013), no. 6, 2305–2328.
- [Dvi09] Zeev Dvir, *On the size of Kakeya sets in finite fields*, Journal of the American Mathematical Society **22** (2009), no. 4, 1093–1097.
- [Dvi10] _____, *Incidence theorems and their applications*, Foundations and Trends in Theoretical Computer Science **6** (2010), no. 4, 257–293.
- [EOT10] Jordan S Ellenberg, Richard Oberlin, and Terence Tao, *The Kakeya set and maximal conjectures for algebraic varieties over finite fields*, Mathematika **56** (2010), no. 1, 1–25.
- [Fra16] Robert Fraser, *Kakeya-type sets in local fields with finite residue field*, Mathematika **62** (2016), no. 2, 614–629.
- [GD68] J. . Goethals and P. Delsarte, *On a class of majority-logic decodable cyclic codes*, IEEE Transactions on Information Theory **14** (1968), no. 2, 182–188.
- [Gro00] Vince Grolmusz, *Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs*, Combinatorica **20** (2000), no. 1, 71–86.
- [HR17] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n* , Quart. J. **48** (1917), 76–92 (English).
- [HW18] Jonathan Hickman and James Wright, *The Fourier restriction and Kakeya problems over rings of integers modulo n* , Discrete Analysis **11** (2018).
- [KT02] Nets Hawk Katz and Terence Tao, *New bounds for Kakeya problems*, Journal d’Analyse Mathématique **87** (2002), no. 1, 231–263.
- [LV14] Ivan N. Landjev and Peter Vandendriessche, *On the rank of incidence matrices in projective Hjelmslev spaces*, Des. Codes Cryptogr. **73** (2014), no. 2, 615–623.
- [MM68] Florence Jessie MacWilliams and Henry B Mann, *On the p -rank of the design matrix of a difference set*, Information and Control **12** (1968), no. 5, 474–488.
- [Sch79] Jacob T Schwartz, *Probabilistic algorithms for verification of polynomial identities*, International Symposium on Symbolic and Algebraic Manipulation, Springer, 1979, pp. 200–215.
- [Smi69] KJC Smith, *On the p -rank of the incidence matrix of points and hyperplanes in a finite projective geometry*, Journal of Combinatorial Theory **7** (1969), no. 2, 122–129.
- [SS08] 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.

- [Wol99] Thomas Wolff, *Recent work connected with the Kakeya problem*, Prospects in mathematics (Princeton, NJ, 1996) (1999), 29–162.
- [YGK12] Chen Yuan, Qian Guo, and Haibin Kan, *A novel elementary construction of matching vectors*, Information Processing Letters **112** (2012), no. 12, 494–496.
- [Zip79] Richard Zippel, *Probabilistic algorithms for sparse polynomials*, Symbolic and Algebraic Computation (Berlin, Heidelberg) (Edward W. Ng, ed.), Springer Berlin Heidelberg, 1979, pp. 216–226.