

Finite field Kakeya and Nikodym sets in three dimensions

Ben Lund*

Shubhangi Saraf*

Charles Wolf*

December 3, 2016

Abstract

We give improved lower bounds on the size of Kakeya and Nikodym sets over \mathbb{F}_q^3 . We also propose a natural conjecture on the minimum number of points in the union of a not-too-flat set of lines in \mathbb{F}_q^3 , and show that this conjecture implies an optimal bound on the size of a Nikodym set. Finally, we study the notion of a weak Nikodym set and give improved, and in some special cases optimal, bounds for weak Nikodym sets in \mathbb{F}_q^2 and \mathbb{F}_q^3 .

1 Introduction

Let \mathbb{F}_q denote the finite field of q elements. A *Kakeya set* $K \subseteq \mathbb{F}_q^n$ is a set of points which contains ‘a line in every direction’. More precisely, for all $x \in \mathbb{F}_q^n$ there is a $y \in \mathbb{F}_q^n$ such that the line¹ $\{xt + y, t \in \mathbb{F}_q\} \subseteq K$.

The question of establishing lower bounds for Kakeya sets over finite fields was asked by Wolff [12]. In 2008, in a breakthrough result, Dvir [4] showed that for a Kakeya set K over a finite field \mathbb{F} of size q , $|K| > \frac{q^n}{n!}$, thus exactly pinning down the exponent of q in the lower bound. Later in 2008, Saraf and Sudan [11] improved the lower bound to the form $1/2 \cdot \beta^n q^n$, where β is approximately 1/2.6. Moreover, Dvir showed how to construct a Kakeya set of size $\frac{q^n}{2^{n-1}} + O(q^{n-1})$ (see [11]). In 2009, Dvir, Kopparty, Saraf and Sudan [5] proved a lower bound of $\frac{q^n}{2^n}$ for the size of Kakeya sets. Thus the gap between the lower bound and the upper bound given by the construction is only at most a factor of 2, and it is a very interesting question to close this gap. Though we now know extremely strong lower bounds, we still do not know an exact bound for any dimension other than 2. For $n = 2$, Blokhuis and Mazzocca gave exact bounds on the size of a Kakeya set of $q(q+1)/2 + (q-1)/2$ for odd q and $q(q+1)/2$ for even q . In this paper we give improved lower bounds for dimension $n = 3$, using an extension of the argument presented in [11].

A very closely related notion to Kakeya sets is that of Nikodym sets. A *Nikodym set* $\mathcal{N} \subseteq \mathbb{F}_q^n$ is a set of points such that, through each point $p \in \mathbb{F}_q^n$, there is a line ℓ such that $\ell \setminus \{p\} \subseteq \mathcal{N}$.

In fact, a lower bound for Kakeya sets implies a lower bound for Nikodym sets by the following argument: first observe that asymptotically, lower bounds for Kakeya or Nikodym sets will not change regardless of whether the set is over affine or projective spaces over finite fields. Now take a Nikodym set over the finite projective space $PG(n, q)$. We will argue that it is also a Kakeya set. Consider the lines through points in the hyperplane at infinity. Each point determines a line pointing in each different affine “direction.” An entire line pointing in the direction dictated by the point must be included in the Nikodym set. By definition, a set containing a line pointing in every direction is a Kakeya set.

*Rutgers University, supported by NSF grant CCF-1350572.

¹A *line* is an affine subspace of dimension 1.

Almost all lower bounds for Nikodym sets currently follow from a lower bound for Kakeya sets, although we believe that much stronger lower bounds should hold for Nikodym sets. In this paper we study Nikodym sets in 3 dimensions over finite fields and give improved bounds for this setting. We also study a related notion of weak Nikodym sets in 2 and 3 dimensions and give improved, and in some cases optimal, bounds for weak Nikodym sets.

We now present the relevant background as well as state our results for Kakeya and Nikodym sets. In the rest of the paper, all asymptotics will be in terms of q . We will use n to represent the dimension of the underlying space, but we will think of it to be a fixed constant and the underlying field size q to be growing. Thus $o(1)$ will be a function that tends to 0 as q tends to ∞ .

1.1 Kakeya sets: Background and our results

In this paper we prove the following improved lower bounds for Kakeya sets in dimensions $n = 3$.

Theorem 1. *There exists a constant $C > 0$, such that for any prime power $q > C$, if $K \subseteq \mathbb{F}_q^3$ is a Kakeya set, then*

$$|K| \geq 0.2107q^3.$$

Prior to this work, the best lower bound for $n = 3$ was obtained by Saraf and Sudan [11], and they achieved a lower bound of $(0.208)q^3$.

Though the quantitative improvement in the lower bound is small, we believe our proof method is interesting and might be of independent interest. The proof of Saraf and Sudan [11] extended the beautiful polynomial based lower bounds of Dvir [4] by using the notion of the multiplicity of roots of polynomials. Our work uses the notion of “fractional multiplicity” to obtain the improved result. We say a few more words about these proof methods.

Dvir [4] obtained his lower bound via the following argument using polynomials: If the size of K is small, then interpolate a nonzero low degree polynomial P vanishing on all the points of K . Then, use the properties of K to show that P must actually vanish at all points of the underlying space². However this contradicts the low degree of P .

The work of Saraf and Sudan [11] extends this idea by taking a polynomial P that vanishes at each point of K with some higher multiplicity m . To enable this, they allow the degree of P to be somewhat higher, but they cap the individual degree of each variable of P . This idea somehow still enables them to get the same conclusion as Dvir, but now with stronger bounds. The novelty of the current work is that we allow the multiplicity m to take a non-integer value. We need to now specify what it means for a polynomial to vanish with multiplicity m , where m is a positive real number that is not an integer. For this we define a suitable random process which makes the expected multiplicity of P at a point equal to m . By allowing m to take a non-integer value we are able to make finer optimizations.

We prove our results in Section 2.

1.2 Nikodym Sets: Background and our results

The main conjecture in the study of finite Nikodym sets is the following.

Conjecture 2. *Let \mathcal{N} be a Nikodym set in \mathbb{F}_q^n . Then,*

$$|\mathcal{N}| \geq (1 - o(1))q^n.$$

²Actually in this step Dvir uses a polynomial very closely related to P , but for simplicity we think of it to be P itself.

Conjecture 2 is known in some special cases. Feng, Li, and Shen [7] showed that the complement of a Nikodym set in \mathbb{F}_q^2 is at most $q^{3/2} + q$ points. Guo, Kopparty, and Sudan [8] proved Conjecture 2 for all dimensions, but only over fields of constant characteristic. The only known lower bound on the size of a Nikodym set for general n and q matches the corresponding bound for Kakeya sets.

In Section 3, we prove the following theorem which gives the first separation between the minimum possible size of Kakeya and Nikodym sets in \mathbb{F}_q^3 for any sufficiently large prime power q .

Theorem 3. *Let \mathcal{N} be a Nikodym set in \mathbb{F}_q^3 . Then,*

$$|\mathcal{N}| \geq (0.38 - o(1))q^3.$$

While this falls short of proving the case $n = 3$ of Conjecture 2, it does show a separation between Kakeya and Nikodym sets in \mathbb{F}_q^3 , since the construction in [11] gives a Kakeya set of size $(0.25 + o(1))q^3$.

1.2.1 A conjecture on the union of lines

For L a set of lines, we define $P(L)$ to be the collection of points contained in some line of L . More precisely,

$$P(L) = \bigcup_{\ell \in L} \{p \mid p \in \ell\}.$$

In Section 3.2, we show that a slight modification of the proof of Theorem 3 shows that if L is any set of $(0.62 + o(1))q^3$ lines in \mathbb{F}_q^3 , then $|P(L)| \geq (0.38 - o(1))q^3$. Such a result is stronger than Theorem 3 since the definition of a Nikodym set guarantees the existence of a set L of lines, one for each point in the complement of the Nikodym set, such that all but one point of each line of L is contained in the Nikodym set. We also show that this bound is nearly tight.

The proof of Theorem 3 uses very little information about L (the set of lines corresponding to the complement of a Nikodym set), and there is actually a lot more structure that one might be able to exploit in order to get a stronger result. For example, we show in Section 3.3 that no more than $(1 + o(1))q^{3/2}$ lines of L can be contained in any plane. We believe that the approach of bounding the size of the set of lines associated to the complement of a Nikodym set could lead to a proof of Conjecture 2, if this additional structure of L is used.

To this end, we propose the following conjecture.

Conjecture 4. *If L is a set of lines in \mathbb{F}_q^3 such that $|L| = \Omega(q^3)$, and such that no plane contains $\omega(q)$ lines of L , then $|P(L)| \geq (1 - o(1))q^3$.*

In Section 3.3, we show that Conjecture 4 implies the three dimensional case of Conjecture 2. In addition to making it a very interesting conjecture for understanding Nikodym sets, the conjecture seems also very natural and worthwhile to study for its own sake.

Conjecture 4 resembles a recent result of Ellenberg and Hablisek [6]. A special case of Ellenberg and Hablisek's theorem states that, if p is a prime and L is a set of p^2 lines in \mathbb{F}_p^3 such that no more than p lines of L lie in any plane, then $|P(L)| = \Omega(p^3)$. The main differences between Conjecture 4 and the result of Ellenberg and Hablisek is that we take L to be much larger, we allow the underlying field to have composite order, and our desired conclusion is stronger.

For Ellenberg and Hablisek's result, the condition that the underlying field has prime order is necessary. Indeed, they observe that a nondegenerate Hermitian variety in \mathbb{F}_q^3 for q a perfect square (which we discuss further in Section 4.1.2) contains a set L of q^2 lines, no more than $(1 + o(1))q^{1/2}$ on any plane, such that $|P(L)| = (1 + o(1))q^{5/2}$ points.

Although Conjecture 4 would be sufficient for an application to Conjecture 2, we do not have a counterexample to the following, much stronger, conjecture.

Conjecture 5. *Let $\epsilon > 0$ be any constant and let q be a sufficiently large prime power. Let L be a set of at least $q^{5/2+\epsilon}$ lines in \mathbb{F}_q^3 such that no plane contains more than $(1/2)q^{3/2}$ lines of L . Then, $|P(L)| \geq (1 - o(1))q^3$.*

It may even be that the conclusion $|P(L)| \geq (1 - o(1))q^3$ in Conjecture 5 could be replaced by $|P(L)| \geq q^3 - 2q^{5/2}$ without admitting a counterexample.

There are reasons to be skeptical of Conjecture 5. Although the construction of Ellenberg and Hablisk mentioned above does not directly give a counterexample, it might be possible to construct a counterexample by taking the union of many, carefully chosen, copies of their construction. In fact, in Section 4.1.2 we use Hermitian varieties to construct a set of lines with the following parameters.

Proposition 6. *Let $q = p^2$ for a prime power p . There is a set L of $(1/2 - o(1))q^{7/2}$ lines in \mathbb{F}_q^3 such that no plane contains more than $(1/2)q^{3/2}$ lines of L , and $|P(L)| = q^3 - (1/2 + o(1))q^{5/2}$.*

A proof of Conjecture 4 would be new and very interesting even in the case of prime order fields, for which the above constructions based on Hermitian varieties do not occur and it is thus even more likely that even Conjecture 5 might be true.

1.2.2 Weak Nikodym sets

All existing lower bounds on the size of a Nikodym set use only much weaker properties of Nikodym sets. To capture the part of the definition that is actually used by the existing proofs, we introduce and initiate the explicit study of *weak Nikodym sets*. A weak Nikodym set \mathcal{N} in \mathbb{F}_q^n is a set of points such that, through each point p in the complement \mathcal{N}^c of \mathcal{N} , there is a line ℓ such that $\ell \setminus \{p\} \subseteq \mathcal{N}$.

In Section 4.1.2 we give improved constructions of weak Nikodym sets, and based on these we conjecture that, at least for fields of square order, there are weak Nikodym that contain many fewer points than any Nikodym set. Since current lower bound proofs for Nikodym sets only use the fact that Nikodym sets are also weak Nikodym sets, these proofs are inadequate to prove such a separation.

Further, we slightly improve the bound of Feng, Li, and Shen [7] on the maximum size of the complement of a weak Nikodym set in \mathbb{F}_q^2 , from $q^{3/2} + q$ to $q^{3/2} + 1$. Our new bound is *exactly* tight for weak Nikodym sets in the projective plane over \mathbb{F}_q , for q a perfect square.

2 Makeya sets in 3 dimensions

In this section we give a proof of Theorem 1.

2.1 Preliminary Results and Lemmas

Let $\mathbb{F}_q[x_1, \dots, x_n] = \mathbb{F}_q[\mathbf{x}]$ be the ring of polynomials in x_1, \dots, x_n with coefficients in \mathbb{F}_q .

The following is a basic and well known fact about zeroes of polynomials.

Fact 1. *Let $P \in \mathbb{F}_q[\mathbf{x}]$ be a polynomial of degree at most $q - 1$ in each variable. If $P(a) = 0$ for each $a \in \mathbb{F}_q^n$, then $P \equiv 0$.*

Let $N_q(n, m)$ be the number of monomials in $\mathbb{F}_q[x_1, \dots, x_n]$ of individual degree $< q$ and total degree $< mq$. Note that m need not be a natural number to define $N_q(n, m)$, rather m can be any positive real number.

Lemma 7.

$$N_q(n, m) = \sum_{i=0}^n (-1)^i \binom{n}{i} \binom{\lfloor (m-i)q + n - 1 \rfloor}{n},$$

where $\lfloor x \rfloor$ is the largest integer that is at most x .

Proof. The proof will be via inclusion-exclusion. Consider the total number of monomial terms of a polynomial of total degree strictly less than mq . This equals $\binom{\lfloor mq + n - 1 \rfloor}{n}$. We only want to include those monomials in our count that have individual degree at most $q-1$. Let C_r be the total number of monomials of total degree strictly less than mq and some particular r of the variables having degree q or more. Then by inclusion-exclusion,

$$N_q(n, m) = \sum_{i=0}^n (-1)^i \binom{n}{i} C_i.$$

It is not hard to see that $C_i = \binom{\lfloor (m-i)q + n - 1 \rfloor}{n}$ since if a particular set of i variables must have degree at least q , we can “peel off” degree q part from each of these variables to get a resulting monomial of total degree at most $\lfloor (m-i)q + n - 1 \rfloor$. C_i is then then number of such monomials which equals $\binom{\lfloor (m-i)q + n - 1 \rfloor}{n}$. □

Definition 1. (*multiplicity*) For a polynomial $g \in \mathbb{F}_q[\mathbf{x}]$, we say g vanishes at a point \mathbf{a} with multiplicity m if $g(\mathbf{x} + \mathbf{a})$ has no monomial term of degree lower than m .

The following lemma is a simple adaptation of a lemma from [11] (where instead of two sets S_1 and S_2 there was only one set).

Lemma 8. Let $m_1 \geq 0$ and $m_2 \geq 0$ be integers and $m > 0$ be a real number. Let $S_1, S_2 \subset \mathbb{F}_q^n$ be disjoint sets such that $|S_1| \binom{m_1 + n - 1}{n} + |S_2| \binom{m_2 + n - 1}{n} < N_q(n, m)$. Then there exists a non-zero polynomial $g \in \mathbb{F}_q[\mathbf{x}]$ of total degree less than mq and individual degree at most $q-1$ such that g vanishes on each point of S_1 with multiplicity m_1 and on S_2 with multiplicity m_2 .

Proof. The total number of possible monomials in g is $N_q(n, m)$. We consider the coefficients of these monomials to be free variables. For each point $\mathbf{a} \in \mathbb{F}_q^n$, requiring that the polynomial vanishes on \mathbf{a} with multiplicity m_i adds $\binom{m_i + n - 1}{n}$ homogeneous linear constraints on these coefficients. Requiring that g vanishes on each point of S_1 with multiplicity m_1 and on S_2 with multiplicity m_2 imposes a total of $|S_1| \binom{m_1 + n - 1}{n} + |S_2| \binom{m_2 + n - 1}{n}$ homogeneous linear constraints. Since $|S_1| \binom{m_1 + n - 1}{n} + |S_2| \binom{m_2 + n - 1}{n} < N_q(n, m)$, thus the total number of homogeneous linear constraints is strictly less than the number of variables and hence a nonzero solution exists. Thus there exists a non-zero polynomial $g \in \mathbb{F}_q[\mathbf{x}]$ of total degree less than mq and individual degree at most $q-1$ such that g vanishes on each point of S_1 with multiplicity m_1 and on S_2 with multiplicity m_2 . □

For $g \in \mathbb{F}_q[\mathbf{x}]$ let $g_{\mathbf{a}, \mathbf{b}}(t) = g(\mathbf{a} + t\mathbf{b})$ denote its restriction to the “line” $\{\mathbf{a} + t\mathbf{b}, t \in \mathbb{F}_q\}$.

The lemma below is a basic result that also appears in [11].

Lemma 9. If $g \in \mathbb{F}_q[\mathbf{x}]$ vanishes with multiplicity m at some point $\mathbf{a} + t_0\mathbf{b}$ then $g_{\mathbf{a}, \mathbf{b}}$ vanishes with multiplicity m at t_0 .

Proof. By definition, the fact that g has a zero of multiplicity m at $\mathbf{a} + t_0\mathbf{b}$ implies that the polynomial $g(\mathbf{x} + \mathbf{a} + t_0\mathbf{b})$ has no support on monomials of degree less than m . Thus under the homogeneous substitution of $\mathbf{x} \rightarrow t\mathbf{b}$, we get no monomials of degree less than m either, and thus we have t^m divides $g(t\mathbf{b} + \mathbf{a} + t_0\mathbf{b}) = g(\mathbf{a} + (t + t_0)\mathbf{b}) = g_{\mathbf{a},\mathbf{b}}(t + t_0)$. Hence $g_{\mathbf{a},\mathbf{b}}$ has a zero of multiplicity m at t_0 . □

The following theorem was the lower bound result from [11].

Theorem 10 (Kakeya lower bound from [11]). *If K is a Kakeya set in \mathbb{F}_q^n , then $|K| \geq \frac{1}{\binom{m+n-1}{n}} N_q(n, m)$.*

By setting $n = 3$ and $m = 2$, it is concluded in [11] that for a Kakeya set $K \subseteq \mathbb{F}_q^n$, $|K| \geq \frac{5}{24}q^3 \approx 0.2083q^3$. We manage to obtain our strengthened lower bound by allowing m to take values that are not necessarily integers. In particular, we introduce a notion of vanishing with fractional multiplicity and show that it can be used for an improved bound.

2.2 Proof of Theorem 1

Let $K \subseteq \mathbb{F}_q^3$ be a Kakeya set. As a first step in the proof, we will interpolate a nonzero polynomial vanishing on the points of K with some possibly fractional multiplicity m . If we wanted to interpolate a polynomial vanishing with multiplicity m where m is sandwiched between two positive integers u and $u + 1$, one way to do this could be that independently for each point we could make it vanish with multiplicity u with some probability, say α , and with multiplicity $u + 1$ with probability $1 - \alpha$, so that in expectation the multiplicity of vanishing would be at least m . It turns out that the main property of the multiplicities of vanishing we will need is that on each *line* of the Kakeya set, almost the correct (α) fraction of points have multiplicity of vanishing being at least u and the rest have multiplicity of vanishing at least $u + 1$. To do this we will first identify an appropriate subset S of the Kakeya set on which we will want the vanishing multiplicity to be u , and in the lemma below we show that such a set can be suitably picked.

Lemma 11. *Let $K \subseteq \mathbb{F}_q^3$ be a Kakeya set. Let $0 \leq \alpha \leq 1$, and $\delta = \frac{1}{\sqrt[3]{q}}$. Then there exists a constant $C > 0$ such that for $q > C$ we can pick a subset $S \subset K$ such that $||S| - \alpha|K|| < \delta\alpha|K|$, and such that for each line L contained in $|K|$, $||L \cap S| - \alpha q| < \delta\alpha q$.*

Proof. Consider a random subset $S \subset K$, where we choose each point in S independently with probability α . By the Chernoff Bound, $\mathbb{P}[||S| - \alpha|K|| \geq \delta\alpha|K|] \leq \exp(-\frac{\alpha|K|\delta^2}{3})$. Since $|K|$ is certainly larger than q , $\exp(-\frac{\alpha|K|\delta^2}{3}) \leq \exp(-\frac{\alpha q\delta^2}{3})$.

Note also that there are only $q^4 + q^3 + q^2$ distinct lines in \mathbb{F}_q^3 , and thus at most $q^4 + q^3 + q^2$ lines in K . Let L be any line in K . Again, via the Chernoff Bound, we have $\mathbb{P}[||L \cap S| - \alpha q| \geq \delta\alpha q] \leq \exp(-\frac{\alpha q\delta^2}{3})$. By the union bound, the probability that any one of the lines in K has more than $(1 + \alpha\delta)q$ or fewer than $(1 - \alpha\delta)q$ points in S is at most $(q^4 + q^3 + q^2) \exp(-\frac{\alpha q\delta^2}{3})$.

Thus if we show that $\exp(-\frac{\alpha q\delta^2}{3}) + (q^4 + q^3 + q^2) \exp(-\frac{\alpha q\delta^2}{3}) < 1$, then by the probabilistic method, such a subset S with the desired properties exists. Since $\lim_{q \rightarrow \infty} \exp(-\frac{\alpha q\delta^2}{3}) + (q^4 + q^3 + q^2) \exp(-\frac{\alpha q\delta^2}{3}) = 0$ for the appropriately chosen δ , there exists some constant $C > 0$ such that for $q > C$, there exists such a set S . □

Lemma 12. Let $K \subseteq \mathbb{F}_q^3$ be a Kakeya set. Let $u \in \{1, 2\}$, let α be such that $0 \leq \alpha \leq 1$, $\delta = \frac{1}{\sqrt[3]{q}}$ and $m = (\alpha - \delta\alpha)u + (1 - \alpha - \delta\alpha)(u + 1)$. Then

$$N_q(3, m) \leq (\alpha + \delta\alpha) \binom{2+u}{3} |K| + (1 - \alpha + \delta\alpha) \binom{3+u}{3} |K|.$$

Proof. Suppose for contradiction, $N_q(3, m) > (\alpha + \delta\alpha) \binom{2+u}{3} |K| + (1 - \alpha + \delta\alpha) \binom{3+u}{3} |K|$. By Lemma 11, choose S such that each line in K has between $\alpha q - \delta\alpha q$ and $\alpha q + \delta\alpha q$ points in S and $\|S\| - \alpha|K| < \delta\alpha|K|$. In particular $|S| < (\alpha + \delta\alpha)|K|$ and $|K \setminus S| < (1 - \alpha + \delta\alpha)|K|$. Then by Lemma 8 there exists a nonzero polynomial $g \in \mathbb{F}_q[x_1, x_2, x_3]$ with total degree less than mq and individual degree less than q such that g vanishes on S with multiplicity at least u and on $K \setminus S$ with multiplicity at least $u + 1$. Let d denote the degree of g . Let $g = g_0 + g_1$, where g_0 denotes the homogeneous part of degree d and g_1 the part with degree less than d . Note that g_0 also has degree at most $q - 1$ in each of its variables.

Now fix a ‘‘direction’’ $\mathbf{b} \in \mathbb{F}_q^3$. Since K is a Kakeya set, there exists $\mathbf{a} \in \mathbb{F}_q^3$ such that the line $\mathbf{a} + t\mathbf{b} \in K$ for all $t \in \mathbb{F}_q$. So consider $g_{a,b}(t)$, the univariate polynomial of g restricted to the line $\mathbf{a} + t\mathbf{b}$. By Lemma 11 and Lemma 9, there are at least $(1 - \delta)\alpha q$ choices of t where $g_{a,b}$ vanishes with multiplicity at least u and there are at least $q - \alpha q - \delta\alpha q$ choices of t , where $g_{a,b}$ vanishes with multiplicity at least $u + 1$. So in total, $g_{a,b}$ has at least $(\alpha - \delta\alpha)uq + (1 - \alpha - \delta\alpha)(u + 1)q = mq$ zeros, which is more than its degree. Therefore, $g_{a,b}$ must be identically zero. In particular, its leading coefficient must be 0. Since this leading coefficient equals $g_0(\mathbf{b})$, $g_0(\mathbf{b}) = 0$. Since \mathbf{b} was chosen arbitrarily, this must happen for all $\mathbf{b} \in \mathbb{F}_q^3$. However, by Fact 1, this contradicts the fact that g_0 is a nonzero polynomial of degree at most $q - 1$ in each of its variables. \square

Proof of Theorem 1. Let $\delta = \frac{1}{\sqrt[3]{q}}$, let $u \in \{1, 2\}$, let α be such that $0 \leq \alpha \leq 1$, and $m = (\alpha - \delta\alpha)u + (1 - \alpha - \delta\alpha)(u + 1)$. Note that once we set the value for u and m between 1 and 2, this will determine a value for α . For now suppose we have chosen some values for u , α and m .

By Lemma 12, $|K| \geq \frac{N_q(3, m)}{(\alpha + \delta\alpha) \binom{2+u}{3} + (1 - \alpha + \delta\alpha) \binom{3+u}{3}}$. Since we are considering $|K|$ as q grows asymptotically, we only need to consider the leading term when $N_q(3, m)$ is expressed as a polynomial in q . Also, note that δ becomes small as q grows large.

The reason we only let u take value 1 or 2 is the following. Since we only care about polynomials with individual variable degree less than q , the total degree must be less than $3q$. Choosing a value of m that is greater than or equal to 3 will just end up being somewhat redundant and end up giving a worse bound. Thus we only consider $m < 3$. Given the relationship between u and m and given that u needs to be an integer, the only choices for u are hence 1 or 2 as in the statement of the above lemma.

When $u = 1$, this makes $m = 2 - (1 + o(1))\alpha$ for large q . By Lemma 7,

$$N_q(3, m) = \left(\frac{-2m^3 + 9m^2 - 9m + 3}{6} + o(1) \right) q^3.$$

Substituting $u = 1$, by Lemma 12 we get that

$$|K| \geq \left(\frac{-2m^3 + 9m^2 - 9m + 3}{6(4 - 3\alpha)} + o(1) \right) q^3 = \left(\frac{-2m^3 + 9m^2 - 9m + 3}{6(3m - 2)} + o(1) \right) q^3.$$

We maximize this for $1 \leq m \leq 2$. For $m=1.84$, this gives $|K| \geq (0.21076 + o(1))q^3$. When $u = 2$, the best lower bound achieved in this case is $|K| \geq (.2083 + o(1))q^3$. Thus overall the best lower bound we achieve is $(0.21076 + o(1))q^3$. \square

3 Nikodym sets in 3 dimensions and the union of lines

In this section, we investigate Nikodym sets in \mathbb{F}_q^3 and give improved lower bounds.

We will find it easier to work with the complement of a Nikodym set rather than the Nikodym set itself. We define

$$f(n, q) = \text{the maximum size of the complement of a Nikodym set in } \mathbb{F}_q^n.$$

We additionally denote the complement of a set \mathcal{N} by \mathcal{N}^c .

Using this notation, Conjecture 2 states that $f(n, q) = o(q^n)$, and Theorem 3 states that $f(3, q) \leq (0.62 + o(1))q^3$.

In Section 3.1, we prove Theorem 3; as mentioned in the introduction, this is the first separation demonstrated between the minimum size of a Nikodym set and the minimum size of a Kakeya set in \mathbb{F}_q^3 that is valid for an arbitrary finite field \mathbb{F}_q .

In Section 3.2, we show that the proof of Theorem 3 given in Section 3.1 immediately implies a lower bound on the number of points incident to a large set of lines, and that this bound is nearly tight. This implies that any substantial improvement to Theorem 3 will need to use some property of Nikodym sets that is not exploited by the proof given in Section 3.1.

In Section 3.3, we observe that a weak Nikodym set has the property that not too many of the lines given by its definition can lie in any single plane. We further suggest that exploiting this property might lead to a proof of Conjecture 2 in the three dimensional case. In particular, we show that a proof of Conjecture 4 would immediately imply the case $n = 3$ of Conjecture 2.

3.1 Proof of Theorem 3

Our bound on $f(3, q)$ will use a bound on the number of incidences between points and lines. The bound we will use was essentially proved by Lund and Saraf in [10], but is not explicitly stated there; a similar bound was obtained by Bennett, Iosevich, and Pakianathan [2]. We show how to recover the bound from arguments given in [10].

Given a set P of points and a set L of lines, we denote the number of incidences between P and L as

$$I(P, L) = |\{(p, \ell) \in P \times L \mid p \in \ell\}|.$$

Theorem 13. *Let L be a set of lines and P a set of points in \mathbb{F}_q^3 . Then,*

$$I(P, L) \leq (1 + o(1)) \left(|P||L|q^{-2} + q\sqrt{|P||L|(1 - |P|q^{-3})(1 - |L|q^{-4})} \right).$$

Proof. A (d_U, d_V) -biregular graph G is a bipartite graph such that each left vertex has degree d_U and each right vertex has degree d_V . We denote by $e(G)$ the number of edges in a graph G , and by $G(S, T)$ the number of edges between two subsets S, T of the vertices of a graph. We will use the expander mixing lemma [1], specifically the following bipartite version. A proof of Lemma 14 is given in [10], and an equivalent result was proved much earlier by Haemers, e.g. [9].

Lemma 14 (Bipartite expander mixing lemma, [10]). *Let G be a (d_U, d_V) -biregular graph with left vertices U and right vertices V . Let A be the (square) adjacency matrix of G , and let $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_{|U|+|V|}$ be the eigenvalues of A . Let $\lambda = \lambda_2/\lambda_1$. Let $S \subseteq U$ with $|S| = \alpha|U|$ and let $T \subseteq V$ with $|T| = \beta|V|$. Then,*

$$\left| \frac{e(S, T)}{e(G)} - \alpha\beta \right| \leq \lambda\sqrt{\alpha\beta(1 - \alpha)(1 - \beta)}.$$

Construct a bipartite graph G with left vertices U being the points of \mathbb{F}_q^3 , and right vertices V being the lines of \mathbb{F}_q^3 , with (p, ℓ) in the edge set of G if and only if $p \in \ell$. The number of points in \mathbb{F}_q^3 is $|U| = q^3$; the number of lines is $|V| = (1 + o(1))q^4$; and the number of incidences between points and lines in \mathbb{F}_q^3 is $e(G) = (1 + o(1))q^5$. It is shown in Section 4 of [10] that the largest eigenvalue of this graph is $(1 + o(1))q^{3/2}$, and the second largest eigenvalue is $(1 + o(1))q$. We are interested in the number of incidences between a set $P \subseteq U$ and $L \subseteq V$. This is exactly the number of edges between P and L in G , and hence we apply Lemma 14 with $\alpha = |P|q^{-3}$ (which is the density of P in U) and $\beta = (1 - o(1))|L|q^{-4}$ (which is the density of L in V), to get that

$$|(1 + o(1))(I(P, L)q^{-5} - |L||P|q^{-7})| \leq (1 + o(1))q^{-4}\sqrt{|P||L|(1 - |P|q^{-3})(1 - |L|q^{-4})}.$$

Thus, simplifying we get

$$I(P, L) \leq (1 + o(1)) \left(|P||L|q^{-2} + q\sqrt{|P||L|(1 - |P|q^{-3})(1 - |L|q^{-4})} \right).$$

□

Now, we complete the proof of Theorem 3.

Proof of Theorem 3. Suppose that \mathcal{N}^c is the complement of a weak Nikodym set in \mathbb{F}_q^3 . Let L be a set of $|\mathcal{N}^c|$ lines such that each line has exactly one point in common with \mathcal{N}^c , and there is exactly one line of L through each point of \mathcal{N}^c ; the existence of such a set is guaranteed by the definition of a weak Nikodym set. Let $P = \mathcal{N}^c$; by definition, $|P| = q^3 - |L|$. Then each line of L is incident to exactly $q - 1$ points of P , so $I(P, L) = (q - 1)|L|$. Applying Theorem 13, we get that

$$(q - 1)|L| \leq (1 + o(1)) \left((q^3 - |L|)|L|q^{-2} + q\sqrt{(q^3 - |L|)|L|(1 - |L|q^{-3})} \right).$$

Simplifying the above expression one can show (with a little bit of effort) that

$$|L| \leq \left((\sqrt{5} - 1)/2 + o(1) \right) q^3 \leq (1 + o(1))0.62q^3.$$

Simplifying the first inequality to get the second one is a messy calculation that we omit, but it can easily be seen that for instance setting $|L|/q^3$ to be any constant greater than 0.62 in the first inequality yields a contradiction, for q sufficiently large. □

3.2 The union of lines

The proof of Theorem 3 only uses the fact that the definition of a Nikodym set N guarantees the existence of $|\mathcal{N}^c|$ distinct lines, each of which are incident to at least $q - 1$ points of \mathcal{N} . While we do not believe that Theorem 3 is anywhere near tight, the same proof gives a nearly tight lower bound on the size of the union of any set of at least $0.62q^3$ lines.

Recall from the introduction that, for any set L of lines,

$$P(L) = \{p \in \ell \mid \ell \in L\}.$$

Proposition 15. *If L is a set of $0.62q^3$ lines in \mathbb{F}_q^3 , then $|P(L)| \geq (1 - o(1))0.38q^3$.*

Proof. Since each point on any line in L is contained in $P = P(L)$, the number of incidences between L and P is $q|L| = 0.62q^4$. Applying Theorem 13,

$$0.62q^4 \leq (1 + o(1))(0.62|P|q + q\sqrt{0.62|P|q^3(1 - |P|q^{-3})}), \text{ so, simplifying as before,}$$

$$|P| > (1 - o(1))0.38q^3.$$

□

We now show that without any further condition on the set of lines, Proposition 15 is nearly tight.

Proposition 16. *There is a set L of $(1 - o(1))0.62q^3$ lines in \mathbb{F}_q^3 such that $|P(L)| < 0.43q^3$.*

Proof. Let p be an arbitrary point of \mathbb{F}_q^3 . We show below that we can choose a set Π of $0.62q$ planes incident to p , such that no line is contained in 3 planes of Π . The set L will be the set of all lines contained in the union of the planes of Π . By inclusion-exclusion, the total number of lines chosen is $|L| \geq 0.62q^3 - \binom{0.62q}{2} = (1 - o(1))0.62q^3$, and the total number of points on these lines is $(0.62q^3 - 1) - (q - 1)\binom{0.62q}{2} + 1 < 0.43q^3$, for q sufficiently large.

To choose the set Π , we first project from the point p ; this is a map from the lines incident to p to points in $PG(2, q)$, the projective plane over \mathbb{F}_q . In this projection, each plane incident to p corresponds to a line in $PG(2, q)$. A conic in $PG(2, q)$ is a set of $q + 1$ points, no three collinear; the projective dual to a conic is a set of $q + 1$ lines, no three coincident. By choosing Π to be an arbitrary subset of size $0.62q$ among the planes associated to such a set of lines, we ensure that no three contain a common line. □

3.3 Coplanar lines and Conjecture 4

A consequence of the near tightness of Proposition 15 is that any substantial improvement to Theorem 3 must use some additional information about Nikodym sets, beyond the fact that the definition of a Nikodym set \mathcal{N} guarantees the existence of $|\mathcal{N}^c|$ distinct lines, each incident to $q - 1$ points of \mathcal{N} . One such property is that no plane can contain too many of the lines associated to the complement of a Nikodym set.

Proposition 17. *Let $\mathcal{N} \subseteq \mathbb{F}_q^3$ be a Nikodym set. Let L be a set of lines, such that each line of L is incident to exactly one point of \mathcal{N}^c , and each point of \mathcal{N}^c is incident to exactly one line of L . Then any plane in \mathbb{F}_q^3 contains at most $(1 + o(1))q^{3/2}$ lines of L .*

Note that the existence of a set satisfying the conditions on L in this proposition is guaranteed by the definition of a Nikodym set.

Proof. Let π be a plane, and let L' be the subset of lines of L that are contained in π . Let $P \subseteq \mathcal{N}^c$ be the set of points associated to lines in L' . From the definition, P is the complement of a planar weak Nikodym set in π . By Theorem 26 (or from the result of Feng, Li, and Shen [7]), $|L'| = |P| \leq (1 + o(1))q^{3/2}$. □

The observation recorded in Proposition 17 enables us to show that Conjecture 4 implies the three dimensional case of Conjecture 2. Since Proposition 17 only gives an upper bound of $(1 + o(1))q^{3/2}$ lines contained in any plane, while Conjecture 4 requires a bound of any function in $\omega(q)$, we will need to use some additional incidence theory to bridge the gap. In particular, we will use the following lemma, which is a special case of Corollary 6 in [10].

Lemma 18 ([10]). *For $k > 1$, a set of kq planes in \mathbb{F}_q^3 is incident to at least $(1 - \frac{1}{k-1+k-1})q^3$ points. A set of kq lines in \mathbb{F}_q^2 is incident to $(1 - \frac{1}{k-1+k-1})q^2$ points.*

We now prove that Conjecture 4 implies the three dimensional case of Conjecture 2.

Theorem 19. *If Conjecture 4 holds, then the case $n = 3$ of Conjecture 2 holds.*

Proof. Suppose that Conjecture 4 holds.

Let \mathcal{N}^c be the complement of a Nikodym set in \mathbb{F}_q^3 . Let L be a set of lines such that each line of L is incident to exactly one point of \mathcal{N}^c , and each point of \mathcal{N}^c is incident to exactly one line of L ; the existence of such a set is guaranteed by the definition of a Nikodym set. Let $L_1 \subset L$ be an arbitrary subset of $\lfloor |L|/2 \rfloor$ lines of L , and let $P \subset \mathcal{N}^c$ be the set of points in \mathcal{N}^c that are not incident to any line in L_1 .

Let $\alpha(q) \in \omega(q)$, and let Π be the set of planes that contain more than $\alpha(q)$ lines of L_1 . Let $L_2 \subseteq L_1$ be the subset of lines in L_1 that are each contained in some plane of Π .

Suppose that $|L_2| = \Omega(q^{5/2} \log(q))$. Since each plane $\pi \in \Pi$ contains at least $\alpha(q)$ lines of L_2 , Lemma 18 implies that the probability that a uniformly chosen point of π is not on any line of L_2 is bounded above by $(1 + o(1))q/\alpha(q)$. By Proposition 17, no plane of Π contains more than $(1 + o(1))q^{3/2}$ lines of L_2 ; hence, $|\Pi| \geq (1 - o(1))q^{-3/2}|L_2| = \Omega(q \log q)$. By Lemma 18, the probability that a uniformly chosen point of \mathbb{F}_q^3 is not on any plane of Π is bounded above by $O(1/\log(q))$. By a union bound, all but $O(q^3/\log(q) + q^4/\alpha(q)) = o(q^3)$ points of \mathbb{F}_q^3 are contained in some line of L_2 . By construction, half of the points of \mathcal{N}^c are not in any line of L_1 , and hence $|\mathcal{N}^c| = o(q^3)$.

Now, suppose that $|L_2| = O(q^{5/2} \log q) = o(q^3)$. By construction, no plane contains more than $\alpha(q)$ lines of $L_1 \setminus L_2$. Hence, Conjecture 4 implies that either $|L_1 \setminus L_2| = o(q^3)$, and hence $|\mathcal{N}^c| = o(q^3)$, or $|P(L_1 \setminus L_2)| = (1 - o(1))q^3$, and hence $|\mathcal{N}^c| = o(q^3)$. \square

4 Weak Nikodym sets

In this section, we begin the investigation of *weak Nikodym sets*, with a particular focus on possible differences between weak Nikodym sets and Nikodym sets.

We will find it convenient to work in projective geometry; we denote the n dimensional projective geometry over \mathbb{F}_q as $PG(n, q)$.

We define (weak) Nikodym sets in projective geometry the same way as in affine geometry. We say \mathcal{N} is a Nikodym set if, through each point p in $PG(n, q)$ there is a line ℓ such that $\ell \setminus \{p\} \subseteq \mathcal{N}$, and \mathcal{N} is a weak Nikodym set if, through each point $p \in \mathcal{N}^c$, there is a line ℓ such that $\ell \setminus \{p\} \subseteq \mathcal{N}$.

Let

- $f(n, q)$ = the maximum size of the complement of a Nikodym set in \mathbb{F}_q^n ,
- $f_w(n, q)$ = the maximum size of the complement of a weak Nikodym set in \mathbb{F}_q^n ,
- $f^*(n, q)$ = the maximum size of the complement of a Nikodym set in $PG(n, q)$,
- $f_w^*(n, q)$ = the maximum size of the complement of a weak Nikodym set in $PG(n, q)$.

There are some easy relations among the above quantities. From the definitions, a Nikodym set is also a weak Nikodym set. Hence,

$$f_w(n, q) \geq f(n, q), \tag{1}$$

$$f_w^*(n, q) \geq f^*(n, q). \tag{2}$$

Suppose that \mathcal{N}^c is the complement of a (weak) Nikodym set in \mathbb{F}_q^n . Take the projective closure of \mathbb{F}_q^n by adding a hyperplane, and include the new hyperplane in \mathcal{N} . This expanded \mathcal{N} is still a (weak) Nikodym set, and hence

$$f_w^*(n, q) \geq f_w(n, q), \quad (3)$$

$$f^*(n, q) \geq f(n, q). \quad (4)$$

Suppose that \mathcal{N}^c is the complement of a (weak) Nikodym set in $PG(n, q)$. The expected number of points of \mathcal{N}^c contained in a hyperplane chosen uniformly at random is $E = (1 + o(1))\mathcal{N}^c/q$; hence, there exists a hyperplane that contains at most E points of \mathcal{N}^c . We can obtain a (weak) Nikodym set in \mathbb{F}_q^n by removing this hyperplane, and hence

$$f_w(n, q) \geq (1 + o(1))(1 - 1/q)f_w^*(n, q), \quad (5)$$

$$f(n, q) \geq (1 + o(1))(1 - 1/q)f^*(n, q). \quad (6)$$

We can do somewhat better when $n = 2$.

Suppose that \mathcal{N}^c is the complement of a Nikodym set in $PG(2, q)$. By the definition of a Nikodym set, if we take a point $p \in \mathcal{N}$, there exists a line ℓ through p such that $\ell \in \mathcal{N}$. We can remove ℓ to obtain an affine plane, and \mathcal{N}^c will be the complement of a Nikodym set in this affine plane. Hence, $f(2, q) \geq f^*(2, q)$, and so

$$f(2, q) = f^*(2, q). \quad (7)$$

Suppose that \mathcal{N}^c is the complement of a weak Nikodym set in $PG(n, q)$. If we take a point $p \in \mathcal{N}^c$, there exists a line ℓ through p such that $\ell \setminus \{p\} \in \mathcal{N}$. We can remove ℓ to obtain an affine plane, and $\mathcal{N}^c \setminus \{p\}$ will be the complement of a weak Nikodym set in this affine plane. Hence, $f_w(2, q) + 1 \geq f_w^*(2, q)$, and so

$$f_w^*(2, q) - 1 \leq f_w(2, q) \leq f_w^*(2, q). \quad (8)$$

4.1 Constructions

In this section, we show how to construct two infinite families of point sets that form the complement of (weak) Nikodym sets in $PG(n, q)$; we also (in Section 4.1.2) give the proof of Proposition 6, which provides an extreme example for Conjecture 5.

It is easy to see that a hyperplane in \mathbb{F}_q^n is the complement of a weak Nikodym set consisting of q^{n-1} points, and, to our knowledge, no better construction than this was known. Our first construction is a refinement of this idea, and gives the complement of a Nikodym set consisting of $(1 - o(1))nq^{n-1}$ points, or the complement of a weak Nikodym set consisting of $(1 - o(1))(n + 1)q^{n-1}$ points. Our second construction gives the complement of a weak Nikodym set consisting of $(1 - o(1))q^{n-1/2}$ points, but only works in fields of square order, and cannot be used to construct the complement of a standard Nikodym set. In Section 4.2, we prove an upper bound on the size of the complement of a weak Nikodym set in $PG(2, q)$ that exactly matches this second construction.

4.1.1 Union of hyperplanes with a few points removed

In this section, we construct the complement of Nikodym sets consisting of $(1 - o(1))nq^{n-1}$ points, and the complement of weak Nikodym sets consisting of $(1 - o(1))(n + 1)q^{n-1}$ points. These constructions work for any sufficiently large finite field.

Let q be a prime power; we will assume that q is sufficiently large relative to n .

Let S be the union of $n + 1$ hyperplanes $\Lambda_1, \dots, \Lambda_{n+1}$ in $PG(n, q)$ that do not all pass through a single point. For each $I \subset [n + 1]$ with $1 \leq |I| \leq n$, remove a point p_I from S such that $p_I \in \Lambda_i$ for $i \in I$, and $p_I \notin \Lambda_j$ for $j \notin I$. By simple dimension counting arguments one can show that such a point always exists. Here is a sketch of the argument. For any k between 1 and n , the intersection of any k hyperplanes must be exactly an $n - k$ dimensional space, since if it was larger then there would be a point in common with all the hyperplanes. If we want a point on those k hyperplanes but not on any other plane, then it is easy to see that for q large enough, a random point on the $n - k$ dimensional intersection would not lie on any of the other hyperplanes.

We claim that the resulting set S (after deleting the points as mentioned above) is the complement of a weak Nikodym set.

Let q be an arbitrary point of S . Let $J \subseteq [n + 1]$, such that $q \notin \Lambda_j$ for each $j \in J$, and $q \in \Lambda_i$ for $i \notin J$. Note that $1 \leq |J| \leq n$. Let ℓ be the line through q and p_J . Note that ℓ intersects each Λ_i at either q or p_J , and does not intersect any Λ_i at both points. Hence, q and p_J are the only points at which ℓ intersects any Λ_i . Since $p_J \notin S$, q is the unique point in the intersection of S and ℓ . Hence, S is the complement of a weak Nikodym set.

Consequently,

$$f_w^*(n, q) \geq (1 - o(1))(n + 1)q^{n-1}.$$

We can modify S to be the complement of a standard Nikodym set by removing Λ_{n+1} from the construction. Then, for any point $q \notin S$, the line through q and $p_{[n]}$ is disjoint from S . Hence,

$$f^*(n, q) \geq (1 - o(1))nq^{n-1}.$$

4.1.2 Hermitian varieties

In this section, we give an improved construction of weak Nikodym sets in \mathbb{F}_q^3 for square q , and we prove Proposition 6, which describes the construction of an extreme example related to Conjecture 5. Both of these constructions are based on Hermitian varieties.

Let $q = p^2$, for p a prime power. For $v \in \mathbb{F}_q$, we define the conjugate $\bar{v} = v^p$. Since q has order p^2 , we have $\bar{\bar{v}} = v$. We will use homogenous coordinates to represent a point $v \in PG(n, q)$ as a column vector $\mathbf{v} = (v_0, v_1, \dots, v_n)^T$.

A square matrix $H = ((h_{ij}))$ for $i, j = 0, 1, \dots, n$ and $h_{ij} \in \mathbb{F}_q$ is *Hermitian* if $h_{ij} = \overline{h_{ji}}$ for all i, j . Let $\mathbf{x}^T = (x_0, x_1, \dots, x_n)$ and $\bar{\mathbf{x}} = (\bar{x}_0, \bar{x}_1, \dots, \bar{x}_n)^T$. The set of points x in $PG(n, q)$ whose coordinates satisfy $\mathbf{x}^T H \bar{\mathbf{x}} = 0$ for a Hermitian matrix H is a *Hermitian variety*. The *rank* of the Hermitian variety V defined by $\mathbf{x}^T H \bar{\mathbf{x}} = 0$ is defined to be the rank of H . We say that V is *non-degenerate* if its rank is $n + 1$.

Let V be a rank r Hermitian variety in $PG(n, q)$ defined by $\mathbf{x}^T H \bar{\mathbf{x}} = 0$. A point c of V is *singular* if $\mathbf{c}^T H = \mathbf{0}$. Clearly, if V is non-degenerate, it has no singular points. Otherwise, $\mathbf{c}^T H = 0$ has $n - r + 1$ independent solutions, and hence defines an $(n - r)$ -flat, which we term the *singular space* of V .

The set of points corresponding to row vectors \mathbf{x}^T that satisfy the equation $\mathbf{x}^T H \bar{\mathbf{c}} = 0$ is the *tangent space* at \mathbf{c} . If \mathbf{c} is singular, this is the entire space; otherwise, $H \bar{\mathbf{c}}$ is a non-zero vector, and hence the tangent space is a hyperplane.

We will use the following properties of Hermitian varieties, determined by Bose and Chakravarti [3].

Lemma 20 (Section 7 in [3]). *The intersection of a Hermitian variety with a flat space is a Hermitian variety. In particular, a line intersects a Hermitian variety in a single point, $q^{1/2} + 1$ points, or is entirely contained in the variety.*

Given a Hermitian variety V , we define *tangent lines* to be those lines that intersect V in exactly 1 point.

Theorem 21 (Theorem 7.2 in [3]). *If V is a degenerate Hermitian variety of rank $r < n + 1$, and c is a point belonging to the singular space of V , and d is an arbitrary point of V , then each point on the line cd belongs to V .*

Theorem 22 (Theorem 7.4 in [3]). *If V is a non-degenerate Hermitian variety, the tangent hyperplane at a point c of V intersects V in a degenerate Hermitian variety U of rank $n - 1$. The singular space of U consists of the single point c .*

Theorem 23 (Theorem 8.1 in [3]). *The number of points on a non-degenerate Hermitian variety is*

$$\phi(n, q) = (q^{(n+1)/2} - (-1)^{n+1})(q^{n/2} - (-1)^n)(q - 1)^{-1}.$$

The number of points on a degenerate Hermitian variety of rank r is

$$(q^{n-r+1} - 1)\phi(r - 1, q) + (q^{n-r+1} - 1)(q - 1)^{-1} + \phi(r - 1, q).$$

Using the above definitions and properties, we can use Hermitian varieties to construct small weak Nikodym sets, as well as an extreme example for Conjecture 5.

Proposition 24. *Let $q = p^2$ for a prime power p , and let $n \geq 2$.*

$$f_w^* \geq \phi(n, q),$$

where $\phi(n, q) = \Omega(q^{n-1/2})$ is the function defined in Theorem 23.

Proof. Let V be a non-degenerate Hermitian variety in $PG(n, q)$, and let c be a point of V . By Theorem 22, the tangent hyperplane Σ at c intersects V in a Hermitian variety of rank $n - 1$ in $PG(n - 1, q)$. By the second part of Theorem 23, there is a point $d \in \Sigma$ that is not contained in V . By Theorem 21, the intersection of the line cd with V is only the point c itself. Since this holds for an arbitrary point $c \in V$, it holds for each point in V , and hence V is the complement of a weak Nikodym set. The proposition follows from the first part of Theorem 23. \square

In Proposition 24, we use the fact that there is at least one line tangent to V at each point, together with the fact that a tangent line contains exactly one point of V . In fact, we know that there are many tangent lines at each point of V , and we use this fact to prove Proposition 6. Indeed, we prove a slightly stronger result.

Proposition 25. *Let $q = p^2$ for a prime power p , and let $0 < \alpha < 1$. Then, there is a set L of $(\alpha + o(1))q^{7/2}$ lines in \mathbb{F}_q^3 such that no plane contains more than $(\alpha + o(1))q^{3/2}$ lines of L , and $|P(L)| = q^3 - (1 - \alpha + o(1))q^{5/2}$.*

Proposition 6 follows immediately from Proposition 25 by taking $\alpha = 1/2$.

Proof. Let V be a non-degenerate Hermitian variety in $PG(3, q)$. By Theorem 23, we have $|V| = (1 + o(1))q^{5/2}$. Let P be a set of $\lfloor \alpha|V| \rfloor$ of the points of V , chosen uniformly at random. Let L be the set of tangent lines to V at points of P . Since the tangent lines intersect V only at their points of tangency, it is clear that the $\lceil (1 - \alpha)|V| \rceil = (1 - \alpha + o(1))q^{5/2}$ points of $V \setminus P$ are not incident to any line of L . It remains to show $|L| = (\alpha + o(1))q^{7/2}$, and that no plane contains more than $(\alpha + o(1))(q^{3/2})$ lines of L .

By Theorem 22, the tangent plane Σ to V at an arbitrary point $c \in P$ intersects V in a rank 2 Hermitian variety $U \subseteq \Sigma$, having the single singular point c . From the second part of Theorem 23, we have that U contains $q^{3/2} + q + 1$ points. Together with Theorem 21, this implies that U is the union of $q^{1/2} + 1$ lines coincident at c . The remaining $q - q^{1/2}$ lines contained in Σ and incident to c are tangent lines to V . Hence, L consists of $(q - q^{1/2})|P| = (\alpha + o(1))q^{7/2}$ distinct lines, and tangent planes to V each contain at most $q - q^{1/2}$ lines of L .

By Lemma 20, the intersection of a plane Σ with V is a Hermitian variety U ; if Σ is not tangent to V , then U is non-degenerate. By Theorem 23, we have that $|U| = q^{3/2} + q + 1$, and there is a single tangent line at each of these points. In addition, a line of L will be contained in Σ only if it is tangent to one of the points of U . Hence, in order to show that no plane contains more than $(\alpha + o(1))q^{3/2}$ lines of L , it suffices to show that no plane contains more than $(\alpha + o(1))q^{3/2}$ points of P .

The expected number of points of P on Σ is $\alpha|U|$. Since the points of P are chosen uniformly at random, the Chernoff bound for Bernoulli random variables implies that, for any $0 < \delta < 1$, the probability that we have more than $(1 + \delta)\alpha|U|$ points of P on Σ is bounded above by $e^{-\delta^2\alpha|U|/3}$. Taking a union bound over the $(1 + o(1))q^3$ planes in $PG(3, q)$, we have that the probability that any plane has more than $(1 + \delta)\alpha|U|$ points of P is bounded above by $(1 + o(1))q^3 e^{-(1+o(1))\delta^2\alpha q^{3/2}/3}$. Hence, taking $\delta > (1 + o(1))9\alpha^{-1}q^{-3/4} \log q = o(1)$ ensures that this happens with probability strictly less than 1, and hence there is a choice of P such that there are fewer than $(\alpha + o(1))q^{3/2}$ on any plane. □

4.2 Nikodym sets in two dimensions

In this section, we give an improved upper bound on $f_w^*(2, q)$. Feng, Li, and Shen [7] showed that $f_w(2, q) \leq q^{3/2} + q$; we show that $f_w^* \leq q^{3/2} + 1$, which, by equation 8, immediately implies that $f_w(2, q) \leq q^{3/2} + 1$. The proof is a straightforward application of the Cauchy-Schwarz inequality. The improvement to the bound of Feng, Li, and Shen comes from working in the projective plane, where the Cauchy-Schwarz inequality gives a tight bound.

The main interest of this result is that it shows that we have *exactly* the right bound for $f_w^*(2, q)$.

Theorem 26. *Let q be any prime power. Then*

$$f_w^*(2, q) \leq q^{3/2} + 1.$$

Proof. To each point $p \in \mathcal{N}^c$, associate a line ℓ_p such that $p \in \ell_p$ and $|\ell_p \cap \mathcal{N}| = q$. Let L be the set of these lines; we have $|L| = |\mathcal{N}^c|$.

For any point p , let $L(p) = |\{\ell \in L : p \in \ell\}|$. By the Cauchy-Schwarz inequality,

$$\sum_{p \in \mathcal{N}} L(p)^2 \geq \left(\sum_{p \in \mathcal{N}} L(p) \right)^2 |\mathcal{N}|^{-1}. \quad (9)$$

For any line ℓ , let $N(\ell) = |\{p \in \mathcal{N} : p \in \ell\}|$. Since each line of L contains q points of \mathcal{N} ,

$$\sum_{p \in \mathcal{N}} L(p) = \sum_{\ell \in L} N(\ell) = q|\mathcal{N}^c|.$$

On the other hand, the left hand side of Equation 9 counts the number of triples $(p, \ell, \ell') \in \mathcal{N} \times L \times L$ such that $p \in \ell$ and $p \in \ell'$. Since each pair of distinct lines in L intersects at a unique

point of \mathcal{N} , this counts each pair $(\ell, \ell') \in L \times L$ once if $\ell \neq \ell'$, and $N(\ell) = q$ times if $\ell = \ell'$. Hence,

$$\sum_{p \in \mathcal{N}} L(p)^2 = |L|^2 - |L| + q|L|.$$

Combining these observations, we have

$$|\mathcal{N}^c|^2 - |\mathcal{N}^c| + q|\mathcal{N}^c| \geq q^2|\mathcal{N}^c|^2 (q^2 + q + 1 - |\mathcal{N}^c|)^{-1},$$

and a simple calculation completes the proof. \square

Combined with the lower bound from Section 4.1.2 and Equation 8, for q a perfect square, Theorem 26 implies

$$\begin{aligned} f_w^*(2, q^2) &= q^3 + 1, \\ f_w(2, q^2) &\in \{q^3, q^3 + 1\}. \end{aligned}$$

We understand $f_w^*(2, q)$ completely in the case that q is square. However, it remains to determine $f_w^*(2, q)$ when q is not square, and to determine $f(2, q)$ for any q .

We believe that it may be possible to construct sets of cardinality $\omega(q)$ that form the complement of a weak Nikodym set when q is not prime (but not necessarily square). However, we doubt that it is possible to construct such sets when q is prime. In addition, we suspect that it is impossible to construct sets of size $\omega(q)$ that form the complement of standard Nikodym sets, regardless of the underlying field. In order to make such fine distinctions, some new idea will be needed, since the current techniques do not exploit the extra structure that standard Nikodym sets have beyond weak Nikodym sets. In addition, with the exception of the work of Guo, Kopparty, and Sudan [8], which require that the underlying field have constant characteristic, current methods used to prove lower bounds on the size of a Nikodym set are insensitive to the characteristic of the underlying field.

5 Acknowledgment

We thank Anurag Bishnoi for comments on an earlier version of this paper.

References

- [1] Noga Alon and Fan RK Chung. Explicit construction of linear sized tolerant networks. *Annals of Discrete Mathematics*, 38:15–19, 1988.
- [2] Mike Bennett, Alex Iosevich, and Jonathan Pakianathan. Three-point configurations determined by subsets of \mathbb{F}_q^2 via the Elekes-Sharir paradigm. *Combinatorica*, 34(6):689–706, 2014.
- [3] RC Bose and IM Chakravarti. Hermitian varieties in a finite projective space $PG(N, q^2)$. *Canad. J. Math*, 18:1161–1182, 1966.
- [4] Zeev Dvir. On the size of kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22:1093–1097, 2009.
- [5] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to kakeya sets and mergers. pages 181–190. IEEE Computer Society, 2009.

- [6] Jordan S Ellenberg and Marton Hablicsek. An incidence conjecture of Bourgain over fields of positive characteristic. *arXiv preprint arXiv:1311.1479*, 2013.
- [7] Chunrong Feng, Liangpan Li, and Jian Shen. Some inequalities in functional analysis, combinatorics, and probability theory. *the electronic journal of combinatorics*, 17(1):R58, 2010.
- [8] Alan Guo, Swastik Kopparty, and Madhu Sudan. New affine-invariant codes from lifting. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 529–540. ACM, 2013.
- [9] Willem H Haemers. Interlacing eigenvalues and graphs. *Linear Algebra and its applications*, 226:593–616, 1995.
- [10] Ben Lund and Shubhangi Saraf. Incidence bounds for block designs. *arXiv preprint arXiv:1407.7513*, 2014.
- [11] Shubhangi Saraf and Madhu Sudan. Improved lower bound on the size of kakeya sets over finite fields. *Analysis and PDE*, 1(3):375–379, 2008.
- [12] Thomas Wolff. Recent work connected with the kakeya problem. *Prospects in mathematics (Princeton, NJ, 1996)*, 2:129–162, 1999.