Canad. Math. Bull. Vol. 66 (2), 2023, pp. 654–664
http://dx.doi.org/10.4153/S0008439522000625

Nearly sharp Lang–Weil bounds for a hypersurface

Kaloyan Slavov

Abstract. We improve to nearly optimal the known asymptotic and explicit bounds for the number of $\mathbb{F}_q$-rational points on a geometrically irreducible hypersurface over a (large) finite field. The proof involves a Bertini-type probabilistic combinatorial technique. Namely, we slice the given hypersurface with a random plane.

1 Introduction

Let $n \geq 2$ and $d \geq 1$, and let $\mathbb{F}_q$ be a finite field. Let $X \subset \mathbb{P}^n$ be a geometrically irreducible hypersurface of degree d over $\mathbb{F}_q$. Lang and Weil [4] have established the bound

$$|\#X(\mathbb{F}_q) - \#\mathbb{P}^{n-1}(\mathbb{F}_q)| \leq (d-1)(d-2)q^{n-3/2} + O_{n,d}(q^{n-2}), \tag{1.1}$$

where the implicit constant can depend only on d and n (but not on q or X). We prove that, in fact, the implicit constant can be taken to be an *absolute constant*—independent of n and d altogether—in the regime of interest $q \gg_d 1$.

Theorem 1.1 *Let $X \subset \mathbb{P}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then*

$$|X(\mathbb{F}_q)| \geq q^{n-1} - (d-1)(d-2)q^{n-3/2} - O_d(q^{n-5/2}) \qquad \textit{and}$$
$$|X(\mathbb{F}_q)| \leq q^{n-1} + (d-1)(d-2)q^{n-3/2} + (1+\pi^2/6)q^{n-2} + O_d(q^{n-5/2}).$$

Example 1.2 (Cone over a maximal curve) Let (d, q_0) be such that there exists a (nonsingular) maximal curve $C = \{f = 0\}$ in $\mathbb{P}^2$ over $\mathbb{F}_{q_0}$ of degree d. Let q be a power of q_0, and let $X = \{f = 0\} \subset \mathbb{P}^n_{\mathbb{F}_q}$ be a projective cone over C. Then

$$\#X(\mathbb{F}_q) = q^{n-1} \pm (d-1)(d-2)q^{n-3/2} + q^{n-2} + q^{n-3} + \cdots + 1,$$

with $\pm$ depending on whether q is an odd or an even power of q_0. Thus, the constant $1 + \pi^2/6$ in the upper bound exhibited in Theorem 1.1 cannot possibly be improved by more than $\pi^2/6$, and the constant 0 in the lower bound in Theorem 1.1 cannot be improved by more than 1.

Received by the editors May 13, 2022; revised October 4, 2022; accepted October 4, 2022.
Published online on Cambridge Core October 18, 2022.
This research was supported by the NCCR SwissMAP of the SNSF.
AMS subject classification: **14G15**, **11T06**, **14G05**, 05B25.
Keywords: Lang–Weil bound, hypersurface, Bertini's theorem, random sampling.

In most of this article, we work in affine space. For a geometrically irreducible hypersurface $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ of degree d, [4] states that

$$|\#X(\mathbb{F}_q) - q^{n-1}| \le (d-1)(d-2)q^{n-3/2} + C_d q^{n-2}, \tag{1.2}$$

where C_d can depend only on d and n. Our notation highlights the more important dependence of C_d on d and suppresses the dependence on n (usually one thinks of n as being fixed from the beginning).

The problem of giving explicit versions of (1.2) and of improving the dependence of C_d on d has a long history, which we now briefly summarize. See [2] for a more detailed account.

- Schmidt has shown that in the case of the lower bound, one can take $C_d = 6d^2$ for $q \gg_{n,d} 1$ (see [5]) and in the case of the upper bound, one can take $C_d = 4d^2k^{2^k}$, where $k = \binom{d+1}{2}$ (see Theorem 4C on page 208 and Theorem 5A on page 210 in [6]).
- Ghorpade and Lachaud [3] use ℓ-adic étale cohomology techniques to prove that one can take C_d to be a *polynomial* in d (of degree that depends on n) in the case of the upper bound as well. Explicitly, one can take $C_d = 12(d+3)^{n+1}$ in (1.2).
- Cafure and Matera [2] prove that one can take $C_d = 5d^{13/3}$ in (1.2); moreover, if $q > 15d^{13/3}$, one can take $C_d = 5d^2 + d + 1$ (this is a polynomial whose degree does not grow with n).
- The author [7] has established the lower bound (for any $\varepsilon > 0$)
$$|X(\mathbb{F}_q)| \ge q^{n-1} - (d-1)(d-2)q^{n-3/2} - (d+2+\varepsilon)q^{n-2}$$
for $q \gg_\varepsilon 1$.
- The author's Theorem 8 in the preprint [8] implies that for every $\varepsilon > 0$ and $\varepsilon' > 0$, we have
$$|X(\mathbb{F}_q)| \le q^{n-1} + (d-1)(d-2)q^{n-3/2} + ((2+\varepsilon)d + 1 + \varepsilon')q^{n-2}$$
as long as $q \gg_{\varepsilon,\varepsilon'} 1$.
- When $\dim X = 1$ (equivalently, $n = 2$), Aubry and Perret have proved (apply Corollary 2.5 in [1] to the closure of X in $\mathbb{P}^2$) that one can take $C_d = d - 1$ in the case of the lower bound and $C_d = 1$ in the case of the upper bound:
$$q - (d-1)(d-2)\sqrt{q} - d + 1 \le |X(\mathbb{F}_q)| \le q + (d-1)(d-2)\sqrt{q} + 1. \tag{1.3}$$

1.1 Upper bounds

The affine version of the asymptotic upper bound in Theorem 1.1 reads as follows.

Theorem 1.3 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then*

$$|X(\mathbb{F}_q)| \le q^{n-1} + (d-1)(d-2)q^{n-3/2} + \left(1 + \pi^2/6\right) q^{n-2} + O_d(q^{n-5/2}), \tag{1.4}$$

where the implied constant depends only on d and can be computed effectively.

We can give an explicit bound, as in the following theorem.

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press

Theorem 1.4 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Suppose that $q > 15d^{13/3}$. Then*

$$|X(\mathbb{F}_q)| \leq q^{n-1} + (d-1)(d-2)q^{n-3/2} + 5q^{n-2}. \tag{1.5}$$

Example 1.5 (Cylinder over a maximal curve) Let $d \geq 3$ be such that $d-1$ is a prime power. Let q be an odd power of $(d-1)^2$. Consider the curve $C = \{y^{d-1} + y = x^d\}$ in $\mathbb{A}^2_{\mathbb{F}_q}$. It is known (see, for example, [9]) that $\#C(\mathbb{F}_q) = q + (d-1)(d-2)\sqrt{q}$. Then the number of $\mathbb{F}_q$-points on $C \times \mathbb{A}^{n-2}$ is $q^{n-1} + (d-1)(d-2)q^{n-3/2}$. Thus, the constant 5 in (1.4) cannot possibly be improved by more than 5.

Remark 1.6 While the cylinder $C \times \mathbb{A}^{n-2}$ in Example 1.5 is nonsingular, its Zariski closure in $\mathbb{P}^n$ has a large (in fact, $(n-3)$-dimensional) singular locus. In general, let $X \subset \mathbb{A}^n$ be a geometrically irreducible hypersurface such that $\#X(\mathbb{F}_q) \geq q^{n-1} + (d-1)(d-2)q^{n-3/2} - O_d(q^{n-2})$ for large q. Theorem 6.1 in [3] implies that the Zariski closure of X in $\mathbb{P}^n$ must have singular locus of dimension $n-3$ or $n-2$.

We exhibit a forbidden interval for $|X(\mathbb{F}_q)|$ that improves Theorem 4 in [7]. The statement below does not require X to be geometrically irreducible.

Theorem 1.7 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a hypersurface of degree d. If*

$$|X(\mathbb{F}_q)| \leq \frac{3}{2}q^{n-1} - (d-1)(d-2)q^{n-3/2} - (d^2+d+1)q^{n-2}, \tag{1.6}$$

then in fact

$$|X(\mathbb{F}_q)| \leq q^{n-1} + (d-1)(d-2)q^{n-3/2} + 12q^{n-2}. \tag{1.7}$$

Remark 1.8 Let us write $g(d) + \cdots$ for an effectively computable $g(d) + g_1(d)$, where $g_1(d) = o(g(d))$ for $d \to \infty$. Theorem 1.7 has content when the right-hand side of (1.6) exceeds the right-hand side of (1.7), which takes place for $q > 16d^4 + \cdots$. Thus, in the presence of Theorem 1.4, Theorem 1.7 addresses the range $16d^4 + \cdots < q < 15d^{13/3}$. Notice that in the Lang–Weil bound (1.2), the approximation term q^{n-1} dominates the error precisely when $q > d^4 + \cdots$. This is why it is reasonable to frame the entire discussion of the Lang–Weil bound in the range $q > d^4 + \cdots$. For example, any lower Lang–Weil bound is trivial for q below this threshold.

1.2 Lower bounds

The proof of Theorem 4 in [7] actually gives a lower bound which is tighter for $q \gg 1$ than the one stated in [7].

Theorem 1.9 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then*

$$|X(\mathbb{F}_q)| \geq q^{n-1} - (d-1)(d-2)q^{n-3/2} - dq^{n-2} - O_d(q^{n-5/2}), \tag{1.8}$$

where the implied constant depends only on d and can be computed explicitly.

We give a version with an explicit lower bound as well.

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press

Theorem 1.10 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Suppose that $q > 15d^{13/3}$. Then*

$$|X(\mathbb{F}_q)| \geq q^{n-1} - (d-1)(d-2)q^{n-3/2} - (d+0.6)q^{n-2}. \tag{1.9}$$

Example 1.11 As in Example 1.5, let $d \geq 3$ be such that $q_0 := d-1$ is a prime power. The curve $\{y^{d-1}z + yz^{d-1} = x^d\}$ in $\mathbb{P}^2$ over $\mathbb{F}_{q_0}$ intersects the line $x = 0$ at d distinct points defined over an extension $\mathbb{F}_{q_1}$ of $\mathbb{F}_{q_0}$. Let q be an even power of q_1. Then the affine curve $C := \{y^{d-1}z + yz^{d-1} = 1\}$ in $\mathbb{A}^2_{\mathbb{F}_q}$ satisfies $\#C(\mathbb{F}_q) = q - (d-1)(d-2)\sqrt{q} - d + 1$. Consequently, the number of $\mathbb{F}_q$-points on the hypersurface $C \times \mathbb{A}^{n-2}$ in $\mathbb{A}^n$ is $q^{n-1} - (d-1)(d-2)q^{n-3/2} - (d-1)q^{n-2}$. Therefore, the constant $d + 0.6$ in (1.9) cannot possibly be improved by more than 1.6.

We can elaborate on (1.8) by pushing the implied constant further down.

Corollary 1.12 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then*

$$\begin{aligned} |X(\mathbb{F}_q)| \geq{}& q^{n-1} - (d-1)(d-2)q^{n-3/2} - dq^{n-2} - 2(d-1)(d-2)q^{n-5/2} \\ &- (2(d-1)^2(d-2)^2 + d^2/2 + d + 2 + \pi^2/6)q^{n-3} - O_d(q^{n-7/2}). \end{aligned} \tag{1.10}$$

A lower Lang–Weil bound can be useful in proving that a geometrically irreducible hypersurface $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ has an $\mathbb{F}_q$-rational point. It is known (see Theorem 5.4 in [2] and its proof) that if $q > 1.5d^4 + \cdots$, then $X(\mathbb{F}_q) \neq \varnothing$. Notice that the approximation term q^{n-1} in (1.10) dominates the remaining explicit terms already for $q > d^4 + \cdots$. Based on this heuristic, we state the following conjecture.

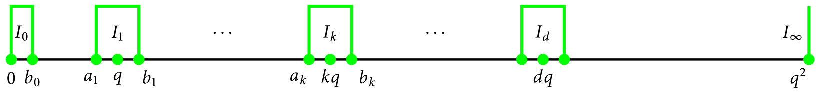
Conjecture 1.13 *There exists an effectively computable function $g_1(d) = O(d^{7/2})$ as $d \to \infty$ with the following property. Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a geometrically irreducible hypersurface of degree d. Then $X(\mathbb{F}_q) \neq \varnothing$ as long as $q > d^4 + g_1(d)$.*

Remark 1.14 In contrast to the upper bounds, all lower bounds in the affine cases above (including (1.3) and Example 1.11) contain a d in the coefficient of q^{n-2}. This is an artifact of affine space; the discrepancy disappears in projective space (Theorem 1.1).

1.3 Outline

This paper builds upon the author's earlier work [7] and is inspired by Tao's discussion [10] of the Lang–Weil bound through random sampling and the idea of Cafure–Matera [2] to slice X with planes (a plane is a two-dimensional affine linear subvariety of $\mathbb{A}^n_{\mathbb{F}_q}$). If $H \subset \mathbb{A}^n_{\mathbb{F}_q}$ is any plane, then $\#(X \cap H)(\mathbb{F}_q)$ is either q^2, 0, or $\approx kq$, where k is the number of geometrically irreducible $\mathbb{F}_q$-irreducible components of $X \cap H$. For $0 \leq k \leq d$, we exhibit a small interval $I_k = [a_k, b_k]$ containing kq so that if we also define $I_\infty = \{q^2\}$, then each $\#(X \cap H)(\mathbb{F}_q)$ belongs to $\bigcup I_k$.

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press



The problem when it comes to the upper bound is that when k is large, planes H with $\#(X \cap H)(\mathbb{F}_q) \in I_k$ contribute significantly toward the count $\#X(\mathbb{F}_q)$. However, it turns out that the number of such H's decreases quickly as k grows.

2 A collection of small intervals

Lemma 2.1 [5, Lemma 5] *Let $C \subset \mathbb{A}^2_{\mathbb{F}_q}$ be a curve of degree d. Let k be the number of geometrically irreducible $\mathbb{F}_q$-irreducible components of C. Then*

$$|\#C(\mathbb{F}_q) - kq| \le (d-1)(d-2)\sqrt{q} + d^2 + d + 1.$$

It will be crucial to give a refined upper bound when $k = 1$.

Lemma 2.2 *Let $C \subset \mathbb{A}^2_{\mathbb{F}_q}$ be a curve of degree d. Suppose that C has exactly one geometrically irreducible $\mathbb{F}_q$-irreducible component. Then*

$$|C(\mathbb{F}_q)| \le q + (d-1)(d-2)\sqrt{q} + 1.$$

Proof Let $C_1, \ldots, C_s$ be the $\mathbb{F}_q$-irreducible components of C. Suppose that C_1 is geometrically irreducible, but C_i is not for $i \ge 2$. Let $e = \deg(C_1)$. Note that $(d, e) \ne (2, 1)$.

Using the Aubry–Perret bound (1.3) for C_1 and Lemma 2.3 in [2] for each C_i with $i \ge 2$, we estimate

$$\begin{aligned}
|C(\mathbb{F}_q)| &\le |C_1(\mathbb{F}_q)| + \sum_{i=2}^{s} |C_i(\mathbb{F}_q)| \\
&\le q + (e-1)(e-2)\sqrt{q} + 1 + \sum_{i=2}^{s} (\deg C_i)^2/4 \\
&\le q + (e-1)(e-2)\sqrt{q} + 1 + (d-e)^2/4 \\
&\le q + (d-1)(d-2)\sqrt{q} + 1;
\end{aligned}$$

to justify the last inequality in the chain, note that it is equivalent to

$$(d-e)\left((d+e-3)\sqrt{q} - \frac{d-e}{4}\right) \ge 0$$

and holds true because either $e = d$, or else $d - e > 0$, and we can write

$$(d+e-3)\sqrt{q} - \frac{d-e}{4} \ge (d+e-3)\sqrt{2} - \frac{d-e}{4} \ge \frac{(4\sqrt{2}-1)d + (4\sqrt{2}+1)e - 12\sqrt{2}}{4} > 0$$

(using that $e \ge 1$ and $d \ge 3$ on the last step). ∎

Let $a_0 = 0$, $b_0 = d^2/4$, $a_1 = q - (d-1)(d-2)\sqrt{q} - d + 1$, and $b_1 = q + (d-1)(d-2)\sqrt{q} + 1$. For $2 \le k \le d$, set $a_k = kq - (d-1)(d-2)\sqrt{q} - d^2 - d - 1$ and

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press

$b_k = kq + (d-1)(d-2)\sqrt{q} + d^2 + d + 1$. Finally, set $a_\infty = b_\infty = q^2$. Define $I_k := [a_k, b_k]$ for $k \in \{0, \dots, d\} \cup \{\infty\}$.

Lemma 2.3 *Let $X \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a hypersurface of degree d. Let $H \subset \mathbb{A}^n_{\mathbb{F}_q}$ be a plane. Then $\#(X \cap H)(\mathbb{F}_q) \in I_k$ for some $k \in \{0, \dots, d\} \cup \{\infty\}$.*

Proof If $X \cap H = \varnothing$, then $\#(X \cap H)(\mathbb{F}_q) = 0 \in I_0$. If $H \subset X$, then $X \cap H = H$ and $\#(X \cap H)(\mathbb{F}_q) = q^2 \in I_\infty$. Suppose that $X \cap H \neq \varnothing$ and $H \not\subset X$. Let k be the number of geometrically irreducible $\mathbb{F}_q$-irreducible components of the degree d plane curve $X \cap H \subset H \simeq \mathbb{A}^2_{\mathbb{F}_q}$. Then $0 \le k \le d$. If $k = 0$, the proof of Lemma 11 in [7] gives $\#(X \cap H)(\mathbb{F}_q) \le d^2/4$. If $k = 1$, we use Lemma 2.2 and the lower bound from (1.3) applied to a geometrically irreducible $\mathbb{F}_q$-irreducible component (necessarily of degree $\le d$) of X. For $2 \le k \le d$, use Lemma 2.1. ■

Alternatively, one could take $b_d = dq$ by the Schwartz–Zippel lemma.

When it comes to giving an upper bound for $|X(\mathbb{F}_q)|$, it will be more convenient to work with $J_1 := I_0 \cup I_1$ and $J_i := I_i$ for $i \in \{2, \dots, d\} \cup \{\infty\}$.

3 Probability estimates

We spell out in detail the proof of Theorem 1.3; the proofs of the remaining results will then require only slight modifications. The implied constant in each O-notation is allowed to depend only on d (a priori, possibly also on n), but not on q or X.

Proof of Theorem 1.3 Set $N := |X(\mathbb{F}_q)|$. For a plane $H \subset \mathbb{A}^n_{\mathbb{F}_q}$ chosen uniformly at random, consider $\#(X \cap H)(\mathbb{F}_q)$ as a random variable. Let μ and σ^2 denote its mean and variance. Lemma 10 in [7] and (1.2) imply

$$\mu = \frac{N}{q^{n-2}} \quad \text{and} \quad \sigma^2 \le \frac{N}{q^{n-2}} \le q + O(\sqrt{q}). \tag{3.1}$$

Write

$$\frac{N}{q^{n-2}} = \mu \le \sum_{k \in \{1,\dots,d\} \cup \{\infty\}} \operatorname{Prob}\Big(\#(X \cap H)(\mathbb{F}_q) \in J_k\Big) b_k. \tag{3.2}$$

For $k \in \{1, \dots, d\} \cup \{\infty\}$, denote

$$p_k := \operatorname{Prob}\Big(\#(X \cap H)(\mathbb{F}_q) \in J_k\Big).$$

We can assume that q is large enough so that the intervals $J_1, \dots, J_d$ are pairwise disjoint.

Let $k \in \{2, \dots, d\}$. If H is a plane such that $\#(X \cap H)(\mathbb{F}_q) \in J_k \cup \dots \cup J_d$, then

$$|\#(X \cap H)(\mathbb{F}_q) - \mu| \ge a_k - \frac{N}{q^{n-2}} \ge (k-1)q - O(\sqrt{q}). \tag{3.3}$$

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press

Define t via $(k-1)q - O(\sqrt{q}) = t\sigma$; then Chebyshev's inequality and the variance bound (3.1) imply

$$\begin{aligned} p_k + \cdots + p_d = \operatorname{Prob}\Big(\#(X \cap H)(\mathbb{F}_q) \in J_k \cup \cdots \cup J_d\Big) &\le \frac{1}{t^2} \\ &= \frac{\sigma^2}{((k-1)q - O(\sqrt{q}))^2} \\ &\le \frac{q + O(\sqrt{q})}{((k-1)q - O(\sqrt{q}))^2} \\ &= \frac{1}{(k-1)^2 q} + O(q^{-3/2}). \end{aligned} \tag{3.4}$$

If H is a plane such that $\#(X \cap H)(\mathbb{F}_q) = q^2$, then

$$|\#(X \cap H)(\mathbb{F}_q) - \mu| = q^2 - \frac{N}{q^{n-2}} \ge q^2 - O(q).$$

Define t via $q^2 - O(q) = t\sigma$; then

$$p_\infty \le \frac{1}{t^2} = \frac{\sigma^2}{(q^2 - O(q))^2} \le \frac{q + O(\sqrt{q})}{(q^2 - O(q))^2} = q^{-3} + O(q^{-7/2}), \quad \text{and hence} \quad p_\infty b_\infty = O(q^{-1}).$$

Note that $b_k - b_{k-1} = q + O(1)$ for $2 \le k \le d$. We now go back to (3.2) and apply the Abel summation formula:

$$\begin{aligned} \frac{N}{q^{n-2}} = \mu &\le (p_1 + \cdots + p_d)b_1 + (p_2 + \cdots + p_d)(b_2 - b_1) + \cdots + p_d(b_d - b_{d-1}) + p_\infty b_\infty \\ &\le b_1 + \frac{1}{1^2} + \cdots + \frac{1}{(d-1)^2} + O(q^{-1/2}) \\ &\le q + (d-1)(d-2)\sqrt{q} + 1 + \pi^2/6 + O(q^{-1/2}). \end{aligned}$$

Multiply both sides by q^{n-2} to arrive at (1.4).

Going through all the explicit inequalities with an O-term, one can compute explicitly a possible value of the constant implicit in (1.4). In fact, since the Cafure–Matera bound gives a choice of C_d in the Lang–Weil bound that depends only on d and not on n, a second look at all the inequalities written down in the proof above reveals that the implied constant in (1.4) can likewise be chosen not to depend on n. ∎

For the rest of the paper, we follow the notation and proof of Theorem 1.3.

Proof of Theorem 1.9 Say that a plane H is "bad" if $\#(X \cap H)(\mathbb{F}_q) \in I_0$ and "good" otherwise. If $H \subset \mathbb{A}^2_{\mathbb{F}_q}$ is a bad plane, then

$$|\#(X \cap H)(\mathbb{F}_q) - \mu| \ge \frac{N}{q^{n-2}} - \frac{d^2}{4} \ge q - O(\sqrt{q}).$$

By computations similar to the ones in the proof of Theorem 1.3, the probability that a plane is bad is at most $q^{-1} + O(q^{-3/2})$. Every good plane contributes at least a_1 to the mean. Therefore,

$$\frac{N}{q^{n-2}} = \mu \geq (1 - q^{-1} - O(q^{-3/2}))(q - (d-1)(d-2)\sqrt{q} - d + 1),$$

giving (1.8). ■

Proof of Corollary 1.12 In fact, the proofs of Theorems 1.3 and 1.9 give an algorithm that takes as input a half-integer $r \geq 0$ and constants[1] $C_d^{(j)}$ and $D_d^{(j)}$ for each half-integer $1/2 \leq j \leq r$ such that

$$|X(\mathbb{F}_q)| \leq q^{n-1} + \sum_{j=1/2}^{r} C_d^{(j)} q^{n-1-j} + O_d(q^{n-r-3/2}) \qquad \text{(summation over half-integers)}$$

and

$$|X(\mathbb{F}_q)| \geq q^{n-1} - \sum_{j=1/2}^{r} D_d^{(j)} q^{n-1-j} - O_d(q^{n-r-3/2}) \qquad \text{(summation over half-integers),}$$

and returns as output four additional $C_d^{(r+1/2)}$, $C_d^{(r+1)}$, $D_d^{(r+1/2)}$, and $D_d^{(r+1)}$ such that

$$|X(\mathbb{F}_q)| \leq q^{n-1} + \sum_{j=1/2}^{r+1} C_d^{(j)} q^{n-1-j} + O_d(q^{n-r-5/2}) \qquad \text{(summation over half-integers)}$$

and

$$|X(\mathbb{F}_q)| \geq q^{n-1} - \sum_{j=1/2}^{r+1} D_d^{(j)} q^{n-1-j} - O_d(q^{n-r-5/2}) \qquad \text{(summation over half-integers).}$$

Initiating the algorithm with $r = 0$ and the rather weak version

$$q^{n-1} - O_d(q^{n-3/2}) \leq |X(\mathbb{F}_q)| \leq q^{n-1} + O_d(q^{n-3/2})$$

of (1.2), we obtained (1.4) and (1.8). In turn, taking the upper bound for N from (1.4) and the lower bound for N from (1.8) as input, we obtain (1.10). ■

Proof of Theorem 1.1 We now slice with a random plane $H \subset \mathbb{P}^n_{\mathbb{F}_q}$. The mean μ of $\#(X \cap H)(\mathbb{F}_q)$ is $N\rho_1$, where $N = |X(\mathbb{F}_q)|$ and $\rho_1 = (q^3 - 1)/(q^{n+1} - 1)$ is the probability that a plane passes through a given point. Let ρ_2 be the probability that a plane passes through two distinct given points. Explicitly (in terms of q-binomial coefficients), $\rho_2 = \binom{n-1}{1}_q / \binom{n+1}{3}_q$. One verifies directly that $\rho_2 \leq \rho_1^2$ and expresses σ^2 as in [10]:

$$N^2\rho_1^2 + \sigma^2 = \mu^2 + \sigma^2 = \mu + N(N-1)\rho_2 \leq \mu + N^2\rho_2$$

to deduce $\sigma^2 \leq \mu$.

We can still take $I_0 = [0, d^2/4]$. Use the projective version of (1.3) (Corollary 2.5 in [1]). Adapt I_1 with $a_1 = q - (d-1)(d-2)\sqrt{q} + 1$. Use $I_\infty = \{q^2 + q + 1\}$. Up to a summand d to account for points at infinity, the remaining a_k and b_k are unchanged.

[1] We refer to $C_d^{(j)}$ and $D_d^{(j)}$ interchangeably as constants or as functions of d depending on the context.

Proceed as in the proof of Theorems 1.3 and 1.9. On the very last step in proving either bound, multiply by $1/\rho_1$ rather than by q^{n-2} and use that $1/\rho_1 = q^{n-2} + O(q^{n-5})$. ■

4 Explicit versions

Proof of Theorem 1.4 The statement clearly holds for $d = 1$, so assume that $d \geq 2$. We will use the explicit Cafure–Matera bound for N. Replace the variance bound (3.1) by

$$\sigma^2 \leq \frac{N}{q^{n-2}} \leq q + (d-1)(d-2)\sqrt{q} + 5d^2 + d + 1 \leq (8.44/7.44)q;$$

to verify the last inequality above, we argue as follows. For any $c_1 > 0$ and $c_2 > 0$, the function $q \mapsto q/(c_1\sqrt{q} + c_2)$ is increasing. Therefore,

$$\frac{q}{(d-1)(d-2)\sqrt{q} + 5d^2 + d + 1} > \frac{15d^{13/3}}{(d-1)(d-2)\sqrt{15}d^{13/6} + 5d^2 + d + 1}.$$

It remains to check that the function $g(d)$ on the right-hand side above satisfies $g(d) > 7.44$ for any integer $d \geq 2$. On the one hand, g grows like $d^{1/6}$, so one easily exhibits a d_0 such that $g(d) > 7.44$ for $d > d_0$. Then a simple computer calculation checks that $g(d) > 7.44$ for integers $d \in \{2, \ldots, d_0\}$ as well.

In the same way, one readily checks that the intervals $J_1, \ldots, J_d$ are pairwise disjoint.

For $k \in \{2, \ldots, d\}$, replace (3.3) by

$$a_k - \frac{N}{q^{n-2}} \geq (k-1)q - 2(d-1)(d-2)\sqrt{q} - 2(3d^2 + d + 1) \geq (5.45/7.45)(k-1)q;$$

to check the last inequality, one has to consider only $k = 2$ and to argue as above.

For $k \in \{2, \ldots, d\}$, (3.4) is now replaced by

$$p_k + \cdots + p_d \leq \frac{(8.44/7.44)q}{((5.45/7.45)(k-1)q)^2} < \frac{2.12}{(k-1)^2 q}.$$

To bound $p_\infty b_\infty$, note that $q > 15d^{13/3} > 15 \times 2^{13/3} > 302$, so

$$p_\infty b_\infty \leq \frac{(8.44/7.44)q}{(q^2 - (8.44/7.44)q)^2} q^2 = \frac{8.44 \times 7.44q}{(7.44q - 8.44)^2} < 0.01.$$

Since $b_k - b_{k-1} = q$ for $3 \leq k \leq d$, but $b_2 - b_1 = q + d^2 + d$, we have to estimate $(d^2 + d)/q < (d^2 + d)/15d^{13/3} < 0.02$. The Abel summation argument now gives

$$\frac{N}{q^{n-2}} \leq q + (d-1)(d-2)\sqrt{q} + 1 + 2.12(\pi^2/6 + 0.02) + 0.01 < q + (d-1)(d-2)\sqrt{q} + 5.$$

■

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press

Proof of Theorem 1.7 Again, assume $d \geq 2$. We can assume that the right-hand side of (1.7) is less than the right-hand side of (1.6); i.e.,

$$4(d-1)(d-2)\sqrt{q} + 2(d^2 + d + 13) < q.$$

This inequality implies in particular that the intervals $J_1, \ldots, J_d$ are pairwise disjoint. Note that it is equivalent to $q > r(d)^2$, where $r(d)$ is the positive root of the quadratic equation $x^2 - 4(d-1)(d-2)x - 2(d^2 + d + 13) = 0$.

Due to (1.6), now we can use the variance bound $\sigma^2 \leq N/q^{n-2} \leq (3/2)q$. Furthermore, (1.6) gives

$$a_k - \frac{N}{q^{n-2}} = kq - (d-1)(d-2)\sqrt{q} - (d^2 + d + 1) - \frac{N}{q^{n-2}} \geq \frac{k-1}{2}q$$

for $2 \leq k \leq d$. Therefore, $p_k + \cdots + p_d$ is now bounded by $6/((k-1)^2 q)$.

We bound $(d^2 + d)/q$ by $(d^2 + d)/(r(d))^2 < 0.16$ for $d \geq 2$. Finally, note that $q > r(2)^2 = 38$, so $q \geq 41$, and we can bound $p_\infty b_\infty$ by $6q/(2q-3)^2 < 0.04$. Therefore,

$$\frac{N}{q^{n-2}} \leq q + (d-1)(d-2)\sqrt{q} + 1 + 6(\pi^2/6 + 0.16) + 0.04 < q + (d-1)(d-2)\sqrt{q} + 12.$$

■

Proof of Theorem 1.10 As above, assume that $d \geq 2$. We bound the variance as

$$\sigma^2 \leq \frac{N}{q^{n-2}} \leq q + (d-1)(d-2)\sqrt{q} + 5d^2 + d + 1 \leq (8.44/7.44)q.$$

Moreover,

$$\frac{N}{q^{n-2}} - \frac{d^2}{4} \geq q - (d-1)(d-2)\sqrt{q} - 21d^2/4 - d - 1 \geq (6.44/7.44)q.$$

From here, we bound the probability that a plane is bad by $1.6/q$. Thus,

$$\frac{N}{q^{n-2}} \geq \left(1 - \frac{1.6}{q}\right)(q - (d-1)(d-2)\sqrt{q} - d + 1) \geq q - (d-1)(d-2)\sqrt{q} - (d + 0.6).$$

■

References

[1] Y. Aubry and M. Perret, *A Weil theorem for singular curves*. In: R. Pellikaan, M. Perret, and S. G. Vlădu (eds.), Arithmetic, geometry, and coding theory, Contemporary Mathematics, 1996, Walter de Gruyter, Berlin–New York, pp. 1—8. https://doi.org/10.1515/9783110811056.1

[2] A. Cafure and G. Matera, *Improved explicit estimates on the number of solutions of equations over a finite field*. Finite Fields Appl.. **12**(2006), 155–185.

[3] S. Ghorpade and G. Lachaud, *Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields*, Moscow Math J. **2**(2002), no. 3, 589–631.

[4] S. Lang and A. Weil, *Number of points of varieties in finite fields*. Amer. J. Math. **76**(1954), 819–827.

[5] W. Schmidt, *A lower bound for the number of solutions of equations over finite fields*. J. Number Theory **6**(1974), no. 6, 448–480.

[6] W. Schmidt, *Equations over finite fields: an elementary approach*, Lectures Notes in Mathematics, 536, Springer, New York, 1976.

[7] K. Slavov, *An application of random plane slicing to counting F_q -points on hypersurfaces*. Finite Fields Appl. 48(2017), 60–68.

[8] K. Slavov, *An application of random plane slicing to counting F_q-points on hypersurfaces*. Preprint, 2021. arXiv:1703.05062v3

[9] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics, 254, Springer, Berlin–Heidelberg, 2009.

[10] T. Tao, *The Lang–Weil bound*, 2012. Available at https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/.

Department of Mathematics, ETH Zürich, Rämistrasse 101, Zürich 8092, Switzerland
e-mail: kaloyan.slavov@math.ethz.ch

https://doi.org/10.4153/S0008439522000625 Published online by Cambridge University Press