Electronic Colloquium on Computational Complexity, Report No. 72 (2026)

An Improved Construction of Variety-Evasive Subspace Families

Robert Andrews* Abhibhav Garg†

Abstract

We study the question of explicitly constructing variety-evasive subspace families, a pseudorandom primitive introduced by Guo (Computational Complexity 2024) that generalizes both hitting sets and lossless rank condensers. Roughly speaking, a variety-evasive subspace family $\mathcal{H}$ is a collection of subspaces such that for every algebraic variety V in a fixed family $\mathcal{F}$, there is some subspace $W \in \mathcal{H}$ that is in general position with respect to V.

We give an explicit construction of a subspace families that evade all degree-d varieties in an n-dimensional affine or projective space. Our construction improves on the size of the variety-evasive subspace families constructed by Guo and, for varieties of degree $n^{1+\Omega(1)}$, comes within a polynomial factor of Guo's lower bound on the size of any such variety-evasive subspace family. Our variety-evasive subspace families rely on an improved construction of hitting sets for Chow forms of algebraic varieties.

1 Introduction

1.1 Background

The probabilistic method is a powerful tool with widespread use throughout mathematics. Many objects of interest throughout combinatorics and computer science, such as Ramsey graphs and randomness extractors, can be shown to exist via the probabilistic method, often with excellent parameters. While probabilistic arguments excel at demonstrating existence, they fall short of providing an efficient, deterministic means of constructing the object of interest. One of the main goals of pseudorandomness is to obtain explicit constructions of objects that exhibit properties similar to those enjoyed by a randomly-chosen object. Not only are explicit constructions interesting in their own right, but they are all the more important in algorithmic applications such as derandomization, where the aim is to reduce or eliminate the use of randomness as an algorithmic resource.

Over time, the theory of pseudorandomness has developed into a rich area of theoretical computer science that studies a variety of objects, including expander graphs, list-decodable codes, randomness extractors, pseudorandom generators, and the numerous connections and relationships between them [Vad12]. More recently, a parallel theory of linear-algebraic pseudorandomness has also appeared. This theory studies collections of linear maps that satisfy various pseudorandom properties, including rank extractors and rank condensers, subspace designs, dimension expanders, and subspace-evasive sets, where the dimension of vector spaces plays a role analogous to that of min-entropy in classical pseudorandomness.

In this work, we study the construction of *variety-evasive subspace families*, a linear-algebraic pseudorandom object introduced by Guo [Guo24]. Roughly speaking, a variety-evasive subspace family $\mathcal{H}$ is a collection of linear or affine spaces such that for any algebraic variety V of interest,

*Cheriton School of Computer Science, University of Waterloo. Email: randrews@uwaterloo.ca.
†Cheriton School of Computer Science, University of Waterloo. Email: abhibhav.garg@uwaterloo.ca.

ISSN 1433-8092

there is some subspace $W \in \mathcal{H}$ that is in general position with respect to V. For example, if V is a curve in the plane and $\mathcal{H}$ is a collection of lines, then there should be some line $W \in \mathcal{H}$ such that the intersection $V \cap W$ is nonempty and zero-dimensional. More generally, when the variety V is fixed, most linear spaces (and in fact, most varieties) W will satisfy $\operatorname{codim}(V \cap W) = \operatorname{codim}(V) + \operatorname{codim}(W)$, and a variety-evasive subspace family must contain a subspace W that intersects V in a manner similar to a random subspace. This is the sort of behavior captured by the notion of one variety evading another, defined below.

Definition 1.1 (Evasiveness)**.** Let V and W be irreducible subvarieties of $\mathbb{P}^n$ or $\mathbb{A}^n$. We say that W *evades* V if

$$\dim(V \cap W) \leq \dim(V) + \dim(W) - n.$$

If V and W are affine varieties, we say that W *strongly evades* V if the above holds with equality whenever the right-hand side is nonnegative. If V is a reducible variety, we say that W *(strongly) evades* V if W (strongly) evades each irreducible component of V. ◊

When V and W are affine varieties, it may be the case that $V \cap W = \varnothing$, even though $\operatorname{codim}(V) + \operatorname{codim}(W)$ is not large enough to force this intersection to be empty in general. The notion of W strongly evading V adds the constraint that the intersection $V \cap W$ should have the expected codimension of $\operatorname{codim}(V) + \operatorname{codim}(W)$ whenever this is possible.

As a matter of notational convenience, we also define the notion of a k-subspace family.

Definition 1.2 (k-Subspace family)**.** For $0 \leq k \leq n$, a *k-subspace family* is a finite collection of k-dimensional subspaces of $\mathbb{P}^n$. Similarly, an *affine k-subspace family* is a finite collection of k-dimensional affine subspaces of $\mathbb{A}^n$. ◊

We can now define variety-evasive subspace families, the main object of study in this work.

Definition 1.3 (Variety-evasive subspace families [Guo24])**.** Let $\mathcal{F}$ be a family of subvarieties of $\mathbb{P}^n$ (or of $\mathbb{A}^n$) and let $\mathcal{H}$ be a k-subspace (or affine k-subspace) family.

1. We say that the family $\mathcal{H}$ is *(strongly) $\mathcal{F}$-evasive* if for every $V \in \mathcal{F}$, there is some $W \in \mathcal{H}$ that (strongly) evades V. In the case where $\mathcal{F}$ is the family of all degree-d subvarieties, we say that $\mathcal{H}$ is *(strongly) (n, d)-evasive*.

2. We say that $\mathcal{H}$ is *(strongly) $(\mathcal{F}, \varepsilon)$-evasive* if for every $V \in \mathcal{F}$, a randomly-chosen $W \in \mathcal{H}$ (strongly) evades V with probability at least $1 - \varepsilon$. When $\mathcal{F}$ is the family of all degree-d subvarieties, we say that $\mathcal{H}$ is *(strongly) (n, d, ε)-evasive*. ◊

As observed by Guo [Guo24], variety-evasive subspace families are a common generalization of two natural problems in algebraic pseudorandomness. The first such problem is the construction of hitting sets for arithmetic circuits, a common approach to derandomizing algorithms for the polynomial identity testing problem. A hitting set $\mathcal{H} \subseteq \mathbb{F}^n$ is a collection of points such that for every nonzero polynomial $f \in \mathcal{C}$ in a circuit class $\mathcal{C}$ of interest, there is some point $\boldsymbol{\alpha} \in \mathcal{H}$ such that $f(\boldsymbol{\alpha}) \neq 0$. The point $\boldsymbol{\alpha}$ witnesses the fact that f is nonzero as a polynomial. An efficient, deterministic construction of such a hitting set immediately implies a deterministic algorithm with similar complexity for testing polynomials $f \in \mathcal{C}$. Geometrically, one can view a hitting set as a set of points $\mathcal{H}$ such that for every hypersurface V defined by a polynomial $f \in \mathcal{C}$, there is a point $\boldsymbol{\alpha} \in \mathcal{H}$ such that $\boldsymbol{\alpha} \notin V$. Taking $\mathcal{F}_{\mathcal{C}}$ to be the family of hypersurfaces defined by polynomials in $\mathcal{C}$, a hitting set is precisely a $\mathcal{F}_{\mathcal{C}}$-evasive 0-subspace family.

The second task generalized by variety-evasive subspace families is the construction of lossless rank condensers. Rank condensers, first appearing in the work of Gabizon and Raz [GR08], are another

of the myriad objects studied in linear-algebraic pseudorandomness. A lossless rank condenser $\mathcal{E} \subseteq \mathbb{F}^{r\times n}$ is a collection of linear maps $\mathbb{F}^n \to \mathbb{F}^r$ such that for every r-dimensional subspace V, there is some map $E \in \mathcal{E}$ where the image of V under E remains r-dimensional. Dualizing, this is precisely the same as requiring the kernel of E to only intersect V at the origin, or equivalently, that the linear spaces in projective space $\mathbb{P}^{n-1}$ corresponding to $\ker(E)$ and V have empty intersection. Thus, a lossless rank condenser is exactly the same object as an $(n-r-1)$-subspace family in $\mathbb{P}^{n-1}$ that evades all dimension-$(r-1)$ linear spaces.

Besides their generalization of other tasks in algebraic pseudorandomness, explicitly constructing variety-evasive subspace families is a natural task from the point of view of algebraic geometry. For example, as we will see later, variety-evasive subspace families can easily be used to construct Noether normailizing maps for algebraic varieties.

Guo [Guo24] gives the only known construction of variety-evasive subspace families. To describe his result, we need the following function. For $n, d \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n-1\}$, let $N(k, d, n)$ be the function given by

$$N(k,d,n) \coloneqq \min\left(\binom{(k'+1)(n'+1+d)}{(k'+1)d}, \binom{(n-k)(n'+1+d)}{(n-k)d}\right)$$

where $k' \coloneqq \min(k, d-2)$ and $n' \coloneqq n-(k-k')$. Guo [Guo24, Theorem 1.7] constructed (n, d, ε)-evasive k-subspace families of size

$$\operatorname{poly}\big(N(k,d,n), n, \varepsilon^{-1}\big).$$

Moreover, this construction is explicit and can be carried out in time polynomial in the size of the variety-evasive subspace family $\mathcal{H}$ (and $\log p$ if the field $\mathbb{F}$ has characteristic $p > 0$). Guo's work complements this with a lower bound that shows any (n, d)-evasive k-subspace family $\mathcal{H}$ must have size at least

$$|\mathcal{H}| \geq \begin{cases} (n-k)(k+1)+1 & \text{if } d = 1, \\ \max\Big(d(n-k)(k+1)+1, \binom{d+n-k}{d} + (n-k+1)k\Big) & \text{if } d > 1. \end{cases}$$

This lower bound is tight in the sense that there is a non-explicit construction of a variety-evasive k-subspace family whose size precisely matches the lower bound [Guo24, Section 4].

1.2 Our results

We give an improved construction of (n, d, ε)-evasive k-subspace families. Just like Guo's construction, ours is explicit and can be carried out in time polynomial in the size of the evasive subspace family $\mathcal{H}$ (and $\log p$, if $\mathbb{F}$ has characteristic $p > 0$).

Theorem 1.4. *Let $n, d \in \mathbb{N}$, $k \in \{0, 1, \ldots, n-1\}$, and $0 < \varepsilon < 1$. There is an explicit (n, d, ε)-evasive k-subspace family (resp. strongly (n, d, ε)-evasive affine k-subspace family) $\mathcal{H}$ of size $\operatorname{poly}(((n-k)d+1)^{n-k}, \varepsilon^{-1})$. Moreover, there is a deterministic algorithm that on input (n, d, ε) runs in time $\operatorname{poly}(|\mathcal{H}|)$ and prints defining equations of the subspaces in $\mathcal{H}$.*

To compare our construction with that of Guo, we use the simplified bound from [Guo24, Theorem 1.7], which asserts an explicit construction of an (n, d, ε)-evasive k-subspace family of size $\operatorname{poly}(n^{\min(k+1, n-k, d)d}, d, \varepsilon^{-1})$. In contrast, we construct explicit (n, d, ε)-evasive k-subspace families of size $\operatorname{poly}(((n-k)d+1)^{n-k}, \varepsilon^{-1})$. This improves the dependence on d, which may be exponentially larger than n and k; for example, a variety cut out by $n/2$ quadratic equations will generally have degree $2^{n/2}$.

We also give a simple construction of (n, d)-evasive k-subspace families that eliminates the polynomial overhead appearing in Theorem 1.4.

Theorem 1.5. *Let $n, d \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n-1\}$. There is an explicit (n,d)-evasive k-subspace family (resp. strongly (n,d)-evasive affine k-subspace family) $\mathcal{H}$ of size at most $(nd+1)^{n-k}$. Moreover, there is a deterministic algorithm that receives n, d, and k as input and prints the subspace family $\mathcal{H}$ in time $(nd+1)^{O(n-k)}$.*

When $d \geq n^{1+\varepsilon}$ for some constant $\varepsilon > 0$, Theorem 1.5 comes within a polynomial factor of Guo's lower bound on the size of (n,d)-evasive k-subspace families. To see this, observe that we can bound the size of the (n,d)-evasive k-subspace family constructed in Theorem 1.5 by $d^{O(n-k)}$. On the other hand, Guo showed that any such k-subspace family must have size at least

$$\binom{d+n-k}{n-k} \geq \left(1 + \frac{d}{n-k}\right)^{n-k} \geq \left(1 + \frac{d}{n}\right)^{n-k} \geq d^{\Omega(n-k)}.$$

As an application of our main result, we give an explicit construction of Noether normalizing maps. Noether normalization is a useful basic result in commutative algebra. In geometric language, the Noether normalization lemma states that for every r-dimensional affine variety $V \subseteq \mathbb{A}^n$, there is a surjective finite morphism $\pi : V \to \mathbb{A}^r$. Finite morphisms are particularly nice maps of algebraic varieties: every subvariety of V is mapped to a subvariety of $\mathbb{A}^r$, and the preimage $\pi^{-1}(p)$ of any point $p \in \mathbb{A}^r$ will be a finite set.

Over an infinite field, a randomly-chosen linear map $\pi : \mathbb{A}^n \to \mathbb{A}^r$ will be Noether normalizing with high probability. Guo [Guo24, Theorems 1.12 and 1.13] observed that Noether normalizing maps can easily be constructed from an (n,d)-evasive subspace family. As a corollary of Theorem 1.4, we obtain the following explicit construction of Noether normalizing maps.

Corollary 1.6. *Let $n, d \in \mathbb{N}$, $r \in \{0, 1, \ldots, n\}$, $k := n - r - 1$, and let $\varepsilon > 0$. There is an explicit collection $\mathcal{L}$ of linear maps $\mathbb{A}^n \to \mathbb{A}^r$ of size $\mathrm{poly}(((n-k)d)^{n-k}, \varepsilon^{-1})$ and computable in time $\mathrm{poly}(|\mathcal{L}|)$ such that the following hold.*

1. *For every projective variety $V \subseteq \mathbb{P}^n$ of dimension $r-1$ and degree at most d, at least a $1-\varepsilon$ fraction of maps $\pi \in \mathcal{L}$ induce a surjective finite morphism from V to $\mathbb{P}^{r-1}$.*
2. *For every affine variety $V \subseteq \mathbb{A}^n$ of dimension r and degree at most d, at least a $1-\varepsilon$ fraction of maps $\pi \in \mathcal{L}$ restrict to a surjective finite morphism from V to $\mathbb{P}^r$.*

The proof of Corollary 1.6 is exactly the same as [Guo24, Theorems 1.12 and 1.13], but using the (n,d,ε)-evasive subspace families of Theorem 1.4 instead of the subspace families constructed by Guo, so we omit further details.

2 Preliminaries

Throughout this work, we use $\mathbb{F}$ to denote an algebraically closed field. The ring of polynomials in $n+1$ variables is denoted $\mathbb{F}[x_0, \ldots, x_n]$. We use bold letters for vectors, whose length will be clear from context. We use vector notation to denote monomials: given $\mathbf{a} \in \mathbb{N}^{n+1}$, we write $\mathbf{x}^{\mathbf{a}}$ for the monomial $x_0^{a_0} \cdots x_n^{a_n}$. We use $\mathbb{A}^n$ and $\mathbb{P}^n$ to denote n-dimensional affine and projective spaces, respectively.

2.1 Algebraic geometry

We assume basic algebraic geometry at the level of [Sha94]. For us, an *algebraic variety* is a Zariski-closed subset of $\mathbb{A}^n$ or $\mathbb{P}^n$; in particular, a variety may be reducible. We adopt the convention that the degree of a variety is the sum of the degrees of all of its irreducible components. For this notion of degree, the following inequality holds, which we call Bézout's inequality.

Lemma 2.1 (Bézout's inequality)**.** *For any two varieties V and W, we have* $\deg(V \cap W) \leq \deg V \cdot \deg W$.

A proof of the affine version of Lemma 2.1 is given in [Hei83, Theorem 1], while a proof of the projective version follows immediately from [Ful84, Chapter 2.3].

We also need the following lemma, which shows that varieties of small degree and dimension are contained in linear subspaces of small dimension.

Lemma 2.2. *For every projective variety V, there exists a linear subspace L of dimension at most* $\dim V \cdot \deg V$ *such that $V \subseteq L$.*

Proof. First, suppose V is irreducible. Let $L \subseteq \mathbb{P}^n$ be a minimal linear subspace such that $V \subseteq L$. By [Har13, Corollary 18.12], we can deduce that V has codimension at most $\deg V - 1$ within L. It follows that L has dimension at most $\dim V + \deg V - 1$.

Now let V be an arbitrary projective variety and let $V_1, \ldots, V_t$ be the irreducible components of V. Each V_i is contained in a linear subspace L_i of dimension at most $\dim V_i + \deg V_i - 1$. Let L be the smallest linear subspace that contains $\bigcup_{i=1}^{t} L_i$. Since each irreducible component V_i is contained in L, the variety V is likewise contained in L. We have

$$\dim L \leq \sum_{i=1}^{t} \dim L_i \leq \sum_{i=1}^{t} (\dim V_i + \deg V_i - 1).$$

By Bézout's inequality, we have $\sum_{i=1}^{t} \deg V_i \leq \deg V$ and $t \leq \deg V$. Combined with the fact that $\dim V_i \leq \dim V$, the required statement follows. □

2.2 Variety-evasive subspace families

In this subsection, we gather some preparatory lemmas for the construction of variety-evasive k-subspace families. In particular, we will see that to construct (n, d, ε)-evasive k-subspace families, it suffices to construct a k-subspace family that evades degree-d varieties of dimension $n - k - 1$, and that we may further assume these varieties live in an ambient space of dimension $(n - k - 1)d$. In addition to this, we will see that an (n, d, ε)-evasive k-subspace family automatically yields an (n, d, ε')-evasive affine k-subspace family with only a mild loss in ε'.

We first cite a lemma of Guo [Guo24] that shows constructing an (n, d, ε)-evasive k-subspace family reduces to the task of constructing a k-subspace that ε-evades equidimensional subvarieties of dimension $n - k - 1$ and degree d.

Lemma 2.3 ([Guo24, Lemma 3.1])**.** *Let $\mathcal{F}$ be the family of equidimensional projective subvarieties of $\mathbb{P}^n$ of dimension $n - k - 1$ and degree at most d. Suppose $\mathcal{H}$ is an $(\mathcal{F}, \varepsilon)$-evasive k-subspace family. Then $\mathcal{H}$ is (n, d, ε)-evasive.*

Next, we show that the dimension of the ambient space can be reduced. As a consequence of Lemma 2.2, it suffices to construct variety-evasive subspace families when the ambient dimension n is at most $\deg V \cdot \dim V$. Essentially the same reduction is used in the constructions of Guo [Guo24]. We give a proof for completeness.

Lemma 2.4. *Let $r := n - k - 1$ and let $\mathcal{H}$ be a given $(rd - r - 1)$-subspace family of linear subspaces of $\mathbb{P}^{rd}$ of size T.*

1. *If $\mathcal{H}$ is (rd, d)-evasive, then we can construct an (n, d)-evasive k-subspace family of size* $\mathrm{poly}(T, n, d)$ *in time* $\mathrm{poly}(T, n, d)$.

2. *If $\mathcal{H}$ is (rd, d, ε)-evasive, then we can construct an $(n, d, 2\varepsilon)$-evasive k-subspace family of size* $\mathrm{poly}\big(T, n, d, \varepsilon^{-1}\big)$ *in time* $\mathrm{poly}\big(T, n, d, \varepsilon^{-1}\big)$.

Proof. We first carry out the construction of an (n, d)-evasive k-subspace family in detail. After this, we briefly remark how to modify the construction to obtain an (n, d, ε)-evasive k-subspace family.

We begin by constructing an $(n, 1)$-evasive $(n - rd - 1)$-subspace family $\widehat{\mathcal{H}}$. By Lemma 2.3, it suffices to build a collection $W_1, \ldots, W_s$ of linear subspaces in $\mathbb{P}^n$ such that for any linear subspace $L \subset \mathbb{P}^n$ of dimension rd, there is some W_i such that $L \cap W_i = \varnothing$. Such a family of subspaces W_i is precisely the nullspaces of the matrices in a *rank extractor*. Forbes and Shpilka [FS12], together with the improved analysis of Forbes, Saptharishi, and Shpilka [FSS14], gave an explicit construction of such a rank extractor of size $s = rd(n - rd) + 1$. For each $i \in [s]$, we pick points $v_{i,0}, \ldots, v_{i,n} \in \mathbb{P}^n$ such that $\mathrm{span}(v_{i,0}, \ldots, v_{i,n}) = \mathbb{P}^n$ and $\mathrm{span}(v_{i,rd+1}, \ldots, v_{i,n}) = W_i$.

Let $\mathcal{H} = \{Y_1, \ldots, Y_T\} \subseteq \mathbb{P}^{rd}$ be the given (rd, d)-evasive $(rd - r - 1)$-subspace family. For each Y_i, we pick $rd - r$ points $u_{i,0}, \ldots, u_{i,rd-r-1} \in \mathbb{P}^{rd}$ that span Y_i.

Now we define linear subspaces $Z_{i,j} \subseteq \mathbb{P}^n$ for every $1 \le i \le s$ and $1 \le j \le T$ that will form the required (n, d)-evasive k-subspace family. Let $\phi_i : \mathbb{P}^{rd} \to \mathbb{P}^n$ be the linear map that sends the point e_ℓ to $v_{i,\ell}$, where e_ℓ denotes the point in $\mathbb{P}^{rd}$ whose ℓ-th coordinate is 1 and whose remaining coordinates are zero. We take $Z_{i,j}$ to be the k-subspace given by

$$Z_{i,j} \coloneqq \mathrm{span}(v_{i,rd+1}, \ldots, v_{i,n}, \phi_i(u_{j,0}), \ldots, \phi_i(u_{j,rd-r-1})).$$

Given the subspace families $\mathcal{H}$ and $\widehat{\mathcal{H}}$, it is clear that we can construct the subspaces $Z_{i,j}$ in $\mathrm{poly}(T, n, d)$ time by iterating over the product set $\mathcal{H} \times \widehat{\mathcal{H}}$.

It remains to show that the k-subspace family $\{Z_{i,j} : i \in [s], j \in [T]\}$ is (n, d)-evasive. To this end, let $V \subseteq \mathbb{P}^n$ be an equidimensional variety of dimension r and degree d. By Lemma 2.2, there is a linear subspace X of dimension rd that contains V. Since $\widehat{\mathcal{H}} = \{W_1, \ldots, W_s\}$ is $(n, 1)$-evasive, there is some W_i such that $W_i \cap X = \varnothing$; without loss of generality, we may assume that $W_1 \cap X = \varnothing$. For each $0 \le i \le rd$, the intersection $\mathrm{span}(W_1, v_{i,1}) \cap X$ consists of a single point in $\mathbb{P}^n$, which we denote by a_i. Comparing dimensions, we see that $\mathrm{span}(a_0, \ldots, a_{rd}) = X$. Let $\psi : \mathbb{P}^{rd} \to \mathbb{P}^n$ denote the linear map that maps e_i to a_i. Since $v_{1,i} \in \mathrm{span}(W_1, \psi(e_i))$, it follows that $\mathrm{span}(W_1, \psi(e_i)) = \mathrm{span}(W_1, \phi_1(e_i)) = \mathrm{span}(W_1, v_{i,1})$.

The image of the map ψ is exactly X, and so ψ is an isomorphism between $\mathbb{P}^{rd}$ and X. Since $V \subseteq X$, the preimage of V under ψ is also a variety of dimension r and degree d. Because $\mathcal{H} = \{Y_1, \ldots, Y_T\}$ is (rd, d)-evasive, there is some Y_j such that $Y_j \cap \psi^{-1}(V) = \varnothing$; without loss of generality, we may assume that Y_1 does not intersect $\psi^{-1}(V)$. The choice of the map ψ implies that $Z_{1,1} = \mathrm{span}(W_1, \psi(Y_1))$. Now suppose towards a contradiction that there is a point $b \in V \cap Z_{1,1}$. The point b lies in $\mathrm{span}(\psi(c), w)$, for some $c \in Y_1$ and $w \in W_1$. Since $b, \psi(c) \in X$ and $X \cap W_1 = \varnothing$, we deduce $b = \psi(c)$ in $\mathbb{P}^n$. This contradicts the fact that $Y_1 \cap \psi^{-1}(V) = \varnothing$.

Since V was an arbitrary equidimensional variety, we can invoke Lemma 2.3 to conclude that the constructed k-subspace is (n, d)-evasive. To construct an (n, d, ε)-evasive k-subspace family, the only part of the construction that changes is that the $(n, 1)$-evasive subspace family used in the first step must be replaced by an $(n, 1, \varepsilon)$-evasive subspace family. The Forbes–Shpilka construction of rank extractors also produces this $(n, 1, \varepsilon)$-evasive subspace family, incurring only a $1/\varepsilon$ multiplicative increase in the size of the subspace family. □

Finally, we show that any (n, d, ε)-evasive k-subspace family immediately yields an (n, d, ε')-evasive affine k-subspace family with only a small loss in the parameter ε'.

Lemma 2.5. *Let $\mathcal{H}$ be an (n, d, ε)-evasive k-subspace family. Let $\mathcal{H}' \subseteq \mathcal{H}$ be the subfamily of subspaces not contained in the hyperplane at infinity. Then the restriction of $\mathcal{H}'$ to the affine chart of points at finite distance is a strongly $(n, d, 2\varepsilon/(1-\varepsilon))$-evasive affine k-subspace family.*

Proof. Since $\mathcal{H}$ is (n, d, ε)-evasive, at most ε fraction of the elements of $\mathcal{H}$ are contained in $\mathrm{V}(x_0)$, the hyperplane at infinity, so $|\mathcal{H}'| \geq (1-\varepsilon)|\mathcal{H}|$. For the rest of this proof, let $\varepsilon' \coloneqq \varepsilon/(1-\varepsilon)$. The family $\mathcal{H}'$ is (n, d, ε')-evasive.

Let $\mathcal{H}_\infty$ be the restriction to $\mathrm{V}(x_0)$ of those subspaces in $\mathcal{H}'$. This is a $(k-1)$-subspace family of size at least $(1-\varepsilon)|\mathcal{H}|$. Let $V \subseteq \mathbb{P}^{n-1}$ be any variety of degree at most d. We can identify $\mathbb{P}^{n-1}$ with the hyperplane at infinity in $\mathbb{P}^n$. This way, V can be viewed as a variety in $\mathbb{P}^n$. All except $\varepsilon|\mathcal{H}|$ elements in $\mathcal{H}'$ evade V. Therefore, $\mathcal{H}_\infty$ is a $(n-1, d, \varepsilon')$-variety evasive subspace family.

We now show that the restriction of $\mathcal{H}'$ to the affine chart is strongly $(n, d, 2\varepsilon')$-evasive for affine varieties. Let $V \subseteq \mathbb{A}^n$ be an affine variety of degree d. Identifying $\mathbb{A}^n$ with the affine chart, we can consider $V \subseteq \mathbb{P}^n$. Let $\overline{V}$ be the projective closure of V, and let V_∞ denote $\overline{V} \cap \mathrm{V}(x_0)$. Both $\overline{V}$ and V_∞ have degree at most d.

Suppose $H \in \mathcal{H}'$ is such that H evades $\overline{V}$ and $H \cap \mathrm{V}(x_0 = 0)$ evades V_∞. Let W be an irreducible component of V, let $\overline{W}$ be the projective closure of W, and let W_∞ denote $\overline{W} \cap \mathrm{V}(x_0)$. By assumption, every component of $\overline{W} \cap H$ has dimension $\dim \overline{W} + k - n$. If $\dim \overline{W} + k - n < 0$, then this intersection is empty. In this case, $W \cap H \cap \mathbb{A}^n$ is also empty, and therefore $H \cap \mathbb{A}^n$ evades W. Otherwise, we have $\dim \overline{W} + k - n \geq 0$.

To show that $H \cap \mathbb{A}^n$ evades W, it suffices to show that $\overline{W} \cap H \not\subseteq \mathrm{V}(x_0)$. This will guarantee that $W \cap H \cap \mathbb{A}^n$ is nonempty and has the correct dimension. To this end, note that $\dim W_\infty = \dim W - 1$. Since $H \cap \mathrm{V}(x_0)$ evades W_∞, every component of $\overline{W} \cap H \cap \mathrm{V}(x_0)$ has dimension $\dim \overline{W} + k - n - 1$. Since every component of $\overline{W} \cap H$ has dimension $\dim \overline{W} + k - n$, no component of $\overline{W} \cap H$ lies completely in the hyperplane at infinity, completing the proof that $H \cap \mathbb{A}^n$ evades W. Since this holds for every component W of V, we deduce that $H \cap \mathbb{A}^n$ evades V.

Because $\mathcal{H}'$ and $\mathcal{H}_\infty$ are (n, d, ε')-evasive and $(n-1, d, \varepsilon')$-evasive, respectively, the fraction of hyperplanes in $\mathcal{H}'$ such that either H does not evade $\overline{V}$ or such that $H \cap \mathrm{V}(x_0)$ does not evade V_∞ is at most $2\varepsilon'$. Therefore, the restriction of $\mathcal{H}'$ to the affine chart is a strongly $(n, d, 2\varepsilon')$-evasive affine k-subspace family. □

3 Construction of variety-evasive subspace families

We give two constructions of variety-evasive subspace families. The first is a simple construction meant to illustrate our main technical observation. The second is a more involved construction that allows us to obtain improved epsilon variety-evasive subspace families.

3.1 Basic construction

Let $V \subseteq \mathbb{P}^n$ be an projective variety of dimension r. The intersection of V with a general hyperplane is a variety of dimension $r-1$. Typically, to obtain an effective version of this fact, one picks a point on each component of V and controls the probability that a randomly-chosen hyperplane H does not pass through the chosen points. If H does not pass through these points, then H properly intersects each component of V, so the intersection $V \cap H$ will have dimension exactly $r-1$.

We implement this argument in the following lemma. Here, the coefficients of the hyperplane H are not picked independently, but are instead chosen from points of the form $(1, \gamma, \gamma^2, \ldots, \gamma^n)$ for $\gamma \in \mathbb{F}$.

Lemma 3.1. *Let $V \subseteq \mathbb{P}^n$ be a projective variety of dimension r and degree d. Let $V_1, \dots, V_t$ be the irreducible components of V. There exists a polynomial $P \in \mathbb{F}[z]$ of degree at most nd such that for any γ with $P(\gamma) \neq 0$, every hyperplane section $V_i \cap \mathrm{V}\left(\sum_{j=0}^{n} \gamma^j x_j\right)$ has dimension $\dim V_i - 1$.*

Proof of Lemma 3.1. From each irreducible component V_i of V, we pick a point p_i. The number of components of V is bounded by the degree d. Consider the polynomial $Q(\mathbf{x}, z) \coloneqq \sum_{i=0}^{n} z^i x_i$. The evaluation $Q(p_i, z)$ is a nonzero polynomial in z, since the point p_i has at least one nonzero coordinate. Set $P(z) \coloneqq \prod_{i=1}^{t} Q(p_i, z)$.

It is clear that P is a polynomial of degree $nt \leq nd$. To show that P satisfies the claimed property, let $\gamma \in \mathbb{F}$ be a point such that $P(\gamma) \neq 0$ and consider the linear form $L(\mathbf{x}) \coloneqq \sum_{i=0}^{n} \gamma^i x_i$. By construction, we have that $L(p_i) = Q(p_i, \gamma)$. Because $P(\gamma) \neq 0$, it follows that $Q(p_i, \gamma) \neq 0$. In particular, the linear form L does not vanish identically V_i. Therefore $V_i \cap \mathrm{V}(L)$ has dimension $\dim V_i - 1$ by [CLO15, Chapter 9, Section 4, Corollary 4]. □

We can also deduce a similar statement for affine varieties.

Lemma 3.2. *Let $V \subseteq \mathbb{A}^n$ be an affine variety of degree d. Let $V_1, \dots, V_t$ be the irreducible components of V. There exists a polynomial $P \in \mathbb{F}[z]$ of degree at most nd such that for any γ with $P(\gamma) \neq 0$, every hyperplane section $V_i \cap \mathrm{V}\left(1 + \sum_{j=1}^{n} \gamma^j x_j\right)$ has dimension $\dim V_i - 1$.*

Proof of Lemma 3.1. Let $\overline{V}$ denote the projective closure of V. The number of components of $\overline{V}$ is bounded by the degree d. Each irreducible component $\overline{V}_i$ of $\overline{V}$ is the projective closure of a component V_i of V. Therefore, for every i we have $\dim(\overline{V}_i \cap \mathrm{V}(x_0)) = \dim \overline{V}_i - 1$. For each i such that $\dim \overline{V}_i \geq 1$, and for each irreducible component $\overline{V}_{i,j}$ of $\overline{V}_i \cap \mathrm{V}(x_0)$, pick a point $p_{i,j} \in \overline{V}_{i,j}$. For those i such that $\dim \overline{V}_i = 0$, let $p_{i,1}$ be the single point of $\overline{V}_i$.

Consider the polynomial $Q(\mathbf{x}, z) \coloneqq \sum_{i=0}^{n} z^i x_i$. If we evaluate at $p_{i,j}$, we get $Q(p_{i,j}, z)$, which is a nonzero polynomial in $\mathbb{F}[z]$, since $p_{i,j}$ has at least one nonzero coordinate. Set $P(z) \coloneqq \prod_{i,j} Q(p_i, z)$. If we pick $\gamma \in \mathbb{F}$ such that $P(\gamma) \neq 0$, then the linear form $L(\mathbf{x}) \coloneqq \sum_{i=0}^{n} \gamma^i x_i$ is nonzero at every $p_{i,j}$. From this, we can deduce that $\dim(\overline{V}_i \cap \mathrm{V}(L, x_0)) = \dim \overline{V}_i - 2$ for every irreducible component $\overline{V}_i$ of $\overline{V}$ of dimension at least one. Therefore, for any such component, we must have $\dim(V_i \cap \mathrm{V}(\ell)) = \dim V_i - 1$, where $\ell(\mathbf{x}) \coloneqq L(1, x_1, \dots, x_n)$. For the zero-dimensional components of V, we can also deduce that $V_i \cap \mathrm{V}(\ell) = \varnothing$, since L does not vanish at these components. □

Lemma 3.1 allows us to construct a set $\mathcal{H}$ of $nd + 1$ hyperplanes such that for any projective variety $V \subseteq \mathbb{P}^n$ of degree d, there is some $H \in \mathcal{H}$ that properly intersects V, and Lemma 3.2 does the same for affine varieties. By iterating this construction k times, we can obtain an (n, d)-evasive (affine) k-subspace family. We remark that this solves [Guo24, Open Problem 7], which asked for an explicit construction of a polynomial-size (n, d)-evasive k-subspace family when $n - k = O(1)$.

Theorem 1.5. *Let $n, d \in \mathbb{N}$ and $k \in \{0, 1, \dots, n-1\}$. There is an explicit (n, d)-evasive k-subspace family (resp. strongly (n, d)-evasive affine k-subspace family) $\mathcal{H}$ of size at most $(nd+1)^{n-k}$. Moreover, there is a deterministic algorithm that receives n, d, and k as input and prints the subspace family $\mathcal{H}$ in time $(nd+1)^{O(n-k)}$.*

Proof. We start by establishing the projective version of the theorem. Fix pairwise disjoint subsets $B_1, \dots, B_{n-k} \subseteq \mathbb{F}$, each of size $nd + 1$ and not containing 0. For each $\alpha \in \mathbb{F}$, let $L_\alpha(\mathbf{x})$ denote the linear form $x_0 + \alpha x_1 + \cdots + \alpha^n x_n$. For each $\boldsymbol{\gamma} \in \mathbb{F}^{n-k}$, let $H_{\boldsymbol{\gamma}} \subseteq \mathbb{P}^n$ denote the linear subspace $\mathrm{V}\left(L_{\gamma_1}, \dots, L_{\gamma_{n-k}}\right)$. Let $\mathcal{H}$ denote the collection of subspaces $H_{\boldsymbol{\gamma}}$ where $\boldsymbol{\gamma}$ varies over elements in $B_1 \times \cdots \times B_{n-k}$. Finally, let $\mathcal{H}'$ denote the restriction of each element of $\mathcal{H}$ to the affine chart $x_0 = 1$.

We claim that $\mathcal{H}$ and $\mathcal{H}'$ are the required (n,d)-evasive k-subspace and affine k-subspace families, respectively. The bound on the sizes of $\mathcal{H}$ and $\mathcal{H}'$ are clear from construction. To algorithmically produce $\mathcal{H}$ and $\mathcal{H}'$, we simply iterate over the set $B_1 \times \cdots \times B_{n-k}$ and print the subspace $H_{\boldsymbol{\gamma}}$ for every $\boldsymbol{\gamma} \in B_1 \times \cdots \times B_{n-k}$.

To see why $\mathcal{H}$ is (n,d)-evasive, let $V \subseteq \mathbb{P}^n$ be any variety of degree d. By Lemma 3.1, there exists a polynomial $P_1 \in \mathbb{F}[z]$ of degree nd such that for any $\gamma_1 \in \mathbb{F}$ satisfying $P_1(\gamma_1) \neq 0$, the intersection of V_i and $\mathrm{V}(L_{\gamma_1})$ has dimension $\dim V_i - 1$ for every irreducible component V_i of V. By Bézout's inequality (Lemma 2.1), the intersection $V \cap \mathrm{V}(L_{\gamma_1})$ has degree at most d. Since the set B_1 has size $nd+1$, we can find such an element $\gamma_1 \in B_1$. Fix this choice of γ_1. Now invoke Lemma 3.1 for the variety $V \cap \mathrm{V}(L_{\gamma_1})$. This gives us a polynomial P_2 of degree nd whose non-roots define hyperplanes that properly intersect $V \cap \mathrm{V}(L_{\gamma_1})$. Because $|B_2| = nd+1$, we can find a nonroot γ_2 of P_2 that lies in B_2. Moreover, since B_1 and B_2 are disjoint, we are guaranteed that γ_2 is different from γ_1. This implies that the intersection $V_i \cap \mathrm{V}(L_{\gamma_1}) \cap \mathrm{V}(L_{\gamma_2})$ has dimension $\dim V_i - 2$ for every irreducible component V_i of V. Continuing in this manner, we obtain $(\gamma_1, \ldots, \gamma_{n-k}) \in B_1 \times \cdots \times B_{n-k}$ such that the subspace $H_{\boldsymbol{\gamma}}$ evades V.

The affine version for $\mathcal{H}'$ follows the same argument, invoking Lemma 3.2 in place of Lemma 3.1. The fact that no B_i contains 0 implies that each affine subspace in $\mathcal{H}'$ has dimension k. □

3.2 Constructing (n,d,ε)-evasive subspace families

Theorem 1.5 constructs an (n,d)-evasive k-subspace family by building the subspaces iteratively, intersecting $n-k$ hyperplanes one at a time. To improve this to a construction of an (n,d,ε)-evasive k-subspace family, one natural approach is to ensure that at each step, the probability of picking a hyperplane that does not properly intersect a variety V is bounded by $\frac{\varepsilon}{n-k}$. Applying a union bound over the $n-k$ choices of hyperplanes implies that at most an ε fraction of subspaces fail to evade V. However, this enlarges the number of hyperplanes chosen at each step by a factor of $\frac{n-k}{\varepsilon}$, which leads to a $(1/\varepsilon)^{n-k}$ factor in the final size of the subspace family.

By arguing about the $n-k$ hyperplanes as a whole instead of one at a time, we can improve this $(1/\varepsilon)^{n-k}$ factor to $(1/\varepsilon)^{O(1)}$. To do this requires the notion of the Chow form of a variety, which we now define. The definition and facts we use about the Chow form are classical. The following statements appear in [KPS01, Section 2.1.1], and proofs can be found in [Phi86, Chapter 1].

Definition 3.3. Let $V \subseteq \mathbb{P}^n$ be an equidimensional variety of dimension r and degree d. Let $\mathbf{u}_0, \ldots, \mathbf{u}_r$ be sets of variables, each of size $n+1$. The *Chow form of* V, denoted $\mathcal{C}_V$, is a polynomial in $\mathbb{F}[\mathbf{u}_0, \ldots, \mathbf{u}_r]$ with the following properties.

- For every choice of $\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r \in \mathbb{F}^{n+1}$, the linear subspace $\mathrm{V}\left(\sum_{j=0}^n \gamma_{0,j} x_j, \ldots, \sum_{j=0}^n \gamma_{r,j} x_j\right)$ has a point in V if and only if $\mathcal{C}_V(\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r) = 0$.
- The polynomial $\mathcal{C}_V$ squarefree and homogeneous of degree d in each set of variables $\mathbf{u}_i$. ◊

In other words, the Chow form of a variety characterizes those linear subspaces of dimension at least $n-r+1$ that intersect V. The following is an easy corollary of Lemma 3.1.

Corollary 3.4. *Let $V \subseteq \mathbb{P}^n$ be an equidimensional variety of dimension r and degree d with Chow form $\mathcal{C}_V \in \mathbb{F}[\mathbf{u}_0, \ldots, \mathbf{u}_r]$. Let $v_0, \ldots, v_r$ be new variables and let $\phi : \mathbb{F}[\mathbf{u}_0, \ldots, \mathbf{u}_r] \to \mathbb{F}[\mathbf{v}]$ be the map defined by $\phi(u_{i,j}) = v_i^j$. Then $\phi(\mathcal{C}_V) \neq 0$.*

Proof. Let $\gamma_0 \in \mathbb{F}$ be such that $V_1 \coloneqq V \cap \mathrm{V}(x_0 + \gamma_0 x_1 + \cdots + \gamma_0^n x_n)$ is equidimensional of dimension $r-1$. Such an element exists by Lemma 3.1. The variety V_1 now is equidimensional of dimension $r-1$, and we can invoke Lemma 3.1 again to find a $\gamma_1 \in \mathbb{F}$ such that

$V_2 \coloneqq V_1 \cap \mathrm{V}(x_0 + \gamma_1 x_1 + \cdots + \gamma_1^n x_n)$ is equidimensional of dimension $r-2$. Repeating this, we find $\gamma_0, \ldots, \gamma_r$ such that $V \cap \mathrm{V}\left(\sum_{j=0}^n \gamma_0^j x_j, \ldots, \sum_{j=0}^n \gamma_r^j x_j\right)$ is empty. By Definition 3.3, we have $\phi(\mathcal{C}_V)(\gamma_0, \ldots, \gamma_r) \neq 0$, which shows in particular that $\phi(\mathcal{C}_V)$ is nonzero. □

In the notation of Corollary 3.4, the polynomial $\phi(\mathcal{C}_V)$ is a nonzero polynomial of individual degree nd in $r+1$ variables with the property that the subspace defined by the linear forms with coefficients $\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r$ evades V if $\phi(\mathcal{C}_V)(\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r) \neq 0$. The construction of Theorem 1.5 can be thought of as a construction of a hitting set for the restricted Chow form $\phi(\mathcal{C}_V)$. To obtain (n, d, ε)-evasive k-subspace families, we instead apply an ε-hitting set to the restricted Chow form $\phi(\mathcal{C}_V)$. An *ε-hitting set* has exactly the guarantee we need: it is a finite set $\mathcal{H}$ such that a $1-\varepsilon$ fraction of points $(\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r) \in \mathcal{H}$ satisfy $\phi(\mathcal{C}_V)(\boldsymbol{\gamma}_0, \ldots, \boldsymbol{\gamma}_r) \neq 0$. We make this observation precise in the following corollary.

Corollary 3.5. *Suppose $\mathcal{P}$ is an ε-hitting set for polynomials of individual degree nd in $n-k$ variables. Then there exists a (n, d, ε)-evasive k-subspace family $\mathcal{H}$ of size at most $|\mathcal{P}|$. Moreover, there is a deterministic algorithm that takes $\mathcal{P}$ as input, prints the set $\mathcal{H}$, and runs in time* $\mathrm{poly}(n, |\mathcal{P}|)$.

Proof. The evasive family of subspaces is constructed as follows. For each point $\boldsymbol{\mu} \in \mathcal{P}$, let $H_{\boldsymbol{\mu}}$ be the linear subspace defined by the linear forms $x_0 + \mu_i x_1 + \cdots + \mu_i^n x_n$ for $i \in [n-k]$. Let $\mathcal{H}'$ be the resulting family of subspaces.

Let V an arbitrary equidimensional variety of dimension $n-k-1$ and degree d, and let $\mathcal{C}_V$ be its Chow form. Let ϕ be the map defined in Corollary 3.4, so $\phi(\mathcal{C}_V)$ is a nonzero polynomial of individual degree nd in $n-k$ variables. Since $\mathcal{P}$ is a ε-hitting set for such polynomials, for all except $\varepsilon|\mathcal{P}|$ elements in $\mathcal{P}$, we have $\phi(\mathcal{C}_V)(\boldsymbol{\mu}) \neq 0$. Therefore, for all except $\varepsilon|\mathcal{H}'|$ of the subspaces $H \in \mathcal{H}'$, we have $V \cap H = \varnothing$.

Note that the exceptional set of $\varepsilon|\mathcal{H}'|$ vector spaces $H \in \mathcal{H}'$ such that $V \cap H \neq \varnothing$ contains all those subspaces in $\mathcal{H}'$ that are not k-dimensional. Therefore, if we define $\mathcal{H}$ to be the set of k-dimensional subspaces in $\mathcal{H}'$, then all except $\varepsilon|\mathcal{H}|$ elements in $\mathcal{H}$ evade V. Since V was an arbitrary equidimensional variety of dimension $n-k-1$ and degree d, we can invoke Lemma 2.3 to deduce that $\mathcal{H}$ is (n, d, ε)-evasive.

It is clear that the set $\mathcal{H}'$ can be obtained in polynomial time from the ε-hitting set $\mathcal{P}$. To prune $\mathcal{H}'$ to the (n, d, ε)-evasive k-subspace family $\mathcal{H}$, we need to remove from $\mathcal{H}'$ those subspaces that are not k-dimensional. This is a basic linear algebra calculation that can be performed in $\mathrm{poly}(n)$ time for each element of $\mathcal{H}'$. □

Finally, we need an explicit construction of ε-hitting sets. We do this using a construction of Agrawal, Gurjar, Korwar, and Saxena [AGKS15], as instantiated by Guo [Guo24]. The version we state here is adapted to polynomials of bounded individual degree instead of bounded total degree, but follows exactly the same proof as [Guo24, Lemma 2.3].

Lemma 3.6 ([Guo24, Lemma 2.3], [AGKS15, Lemma 4])**.** *For every $d, n \in \mathbb{N}$ and $\varepsilon \in (0,1)$, there exists an ε-hitting set $\mathcal{P}$ for the set of all polynomials of individual degree d in n variables. The set $\mathcal{P}$ has size and bit complexity* $\mathrm{poly}\left((d+1)^n, \varepsilon^{-1}\right)$ *and can be constructed in time* $\mathrm{poly}(|\mathcal{P}|)$.

Combining Corollary 3.5, Lemma 3.6, and the reductions in Section 2, we obtain our final construction of (n, d, ε)-evasive subspaces.

Theorem 1.4. *Let $n, d \in \mathbb{N}$, $k \in \{0, 1, \ldots, n-1\}$, and $0 < \varepsilon < 1$. There is an explicit (n, d, ε)-evasive k-subspace family (resp. strongly (n, d, ε)-evasive affine k-subspace family) $\mathcal{H}$ of size* $\mathrm{poly}(((n-k)d+1)^{n-k}, \varepsilon^{-1})$. *Moreover, there is a deterministic algorithm that on input (n, d, ε) runs in time* $\mathrm{poly}(|\mathcal{H}|)$ *and prints defining equations of the subspaces in $\mathcal{H}$.*

Proof. We start by constructing an (n, d, ε)-evasive k-subspace family. First suppose $n \leq (n-k)d$. Then the required (n, d, ε)-evasive k-subspace family can be constructed by using Corollary 3.5 instantiated with the ε-hitting set from Lemma 3.6. The resulting variety-evasive subspace family has size and bit complexity $\mathrm{poly}\big((nd+1)^{n-k}, \varepsilon^{-1}\big) \leq \mathrm{poly}\Big(((n-k)d+1)^{n-k}, \varepsilon^{-1}\Big)$, since $n \leq (n-k)d$.

Now suppose $n > (n-k)d$. Let $r := n-k-1$. Using Lemma 3.6 and Corollary 3.5, we can construct an $(rd, d, \varepsilon/2)$-evasive $(rd-r-1)$-subspace family. This family has size $\mathrm{poly}\big((rd+1)^r, \varepsilon^{-1}\big) \leq \mathrm{poly}\Big(((n-k)d+1)^{n-k}, \varepsilon^{-1}\Big)$. We can now invoke Lemma 2.4 to obtain the required (n, d, ε)-evasive subspace family. The size of the resulting family is also bounded by $\mathrm{poly}\Big(((n-k)d+1)^{n-k}, \varepsilon^{-1}\Big)$.

To construct a strongly (n, d, ε)-evasive affine k-subspace family, we first pick ε' such that $\varepsilon = 2\varepsilon'/(1-\varepsilon')$. We construct a (n, d, ε')-evasive k-subspace family using the above construction and then invoke Lemma 2.5 to obtain the required (n, d, ε)-evasive affine k-subspace family. □

References

[AGKS15] Manindra Agrawal, Rohit Gurjar, Arpita Korwar, and Nitin Saxena. "Hitting-Sets for ROABP and Sum of Set-Multilinear Circuits". In: *SIAM J. Comput.* 44.3 (2015), pp. 669–697. DOI: 10.1137/140975103 (cit. on p. 10).

[CLO15] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms - an introduction to computational algebraic geometry and commutative algebra*. 4th ed. Undergraduate texts in mathematics. Springer, 2015. ISBN: 978-3-319-16720-6. DOI: 10.1007/978-3-319-16721-3 (cit. on p. 8).

[FS12] Michael A. Forbes and Amir Shpilka. "On identity testing of tensors, low-rank recovery and compressed sensing". In: *Proceedings of the 44th Annual ACM Symposium on Theory of Computing (STOC 2012)*. 2012, pp. 163–172 (cit. on p. 6).

[FSS14] Michael A. Forbes, Ramprasad Saptharishi, and Amir Shpilka. "Hitting sets for multilinear read-once algebraic branching programs, in any order". In: *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC 2014)*. 2014, pp. 867–875. DOI: 10.1145/2591796.2591816 (cit. on p. 6).

[Ful84] William Fulton. *Introduction to intersection theory in algebraic geometry*. Vol. 54. American Mathematical Soc., 1984 (cit. on p. 5).

[GR08] Ariel Gabizon and Ran Raz. "Deterministic extractors for affine sources over large fields". In: *Combinatorica* 28 (2008), pp. 415–440. DOI: 10.1007/s00493-008-2259-3 (cit. on p. 2).

[Guo24] Zeyu Guo. "Variety Evasive Subspace Families". In: *computational complexity* 33.2 (2024), p. 10. DOI: 10.1007/s00037-024-00256-1 (cit. on pp. 1–5, 8, 10).

[Har13] Joe Harris. *Algebraic geometry: a first course*. Vol. 133. Springer Science & Business Media, 2013. DOI: 10.1007/978-1-4757-2189-8 (cit. on p. 5).

[Hei83] Joos Heintz. "Definability and fast quantifier elimination in algebraically closed fields". In: *Theor. Comput. Sci.* 24.3 (1983), pp. 239–277. DOI: 10.1016/0304-3975(83)90002-6 (cit. on p. 5).

[KPS01] Teresa Krick, Luis Miguel Pardo, and Martín Sombra. "Sharp estimates for the arithmetic Nullstellensatz". In: *Duke Mathematical Journal* 109.3 (2001), pp. 521–598. DOI: 10.1215/S0012-7094-01-10934-4 (cit. on p. 9).

[Phi86] Patrice Philippon. "Critères pour l'indépendance algébrique". In: *Inst. Hautes Études Sci. Publ. Math.* 64 (1986), pp. 5–52. ISSN: 0073-8301,1618-1913. DOI: 10.1007/BF02699191 (cit. on p. 9).

[Sha94] Igor R. Shafarevich. *Basic Algebraic Geometry 1*. Second. Springer Berlin, Heidelberg, 1994, pp. xx+304. ISBN: 3-540-54812-2. DOI: 10.1007/978-3-642-57908-0 (cit. on p. 4).

[Vad12] Salil P. Vadhan. "Pseudorandomness". In: *Foundations and Trends in Theoretical Computer Science* 7.1-3 (2012), pp. 1–336 (cit. on p. 1).

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il