

Larger Nearly Orthogonal Sets over Finite Fields

Ishay Haviv* Sam Mattheus† Aleksa Milojević‡ Yuval Wigderson§

Abstract

For a field \mathbb{F} and integers d and k , a set $\mathcal{A} \subseteq \mathbb{F}^d$ is called k -nearly orthogonal if its members are non-self-orthogonal and every $k+1$ vectors of \mathcal{A} include an orthogonal pair. We prove that for every prime p there exists some $\delta = \delta(p) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k$, there exists a k -nearly orthogonal set of at least $d^{\delta \cdot k / \log k}$ vectors of \mathbb{F}^d . The size of the set is optimal up to the $\log k$ term in the exponent. We further prove two extensions of this result. In the first, we provide a large set \mathcal{A} of non-self-orthogonal vectors of \mathbb{F}^d such that for every two subsets of \mathcal{A} of size $k+1$ each, some vector of one of the subsets is orthogonal to some vector of the other. In the second extension, every $k+1$ vectors of the produced set \mathcal{A} include $\ell+1$ pairwise orthogonal vectors for an arbitrary fixed integer $1 \leq \ell \leq k$. The proofs involve probabilistic and spectral arguments and the hypergraph container method.

1 Introduction

For a field \mathbb{F} and an integer d , two vectors $u, v \in \mathbb{F}^d$ are called orthogonal if they satisfy $\langle u, v \rangle = 0$ with respect to the standard inner product defined by $\langle u, v \rangle = \sum_{i=1}^d u_i \cdot v_i$. A vector $u \in \mathbb{F}^d$ is called self-orthogonal if $\langle u, u \rangle = 0$, and it is called non-self-orthogonal otherwise. For integers k and ℓ with $k \geq \ell$, a set $\mathcal{A} \subseteq \mathbb{F}^d$ is said to be (k, ℓ) -nearly orthogonal if its vectors are non-self-orthogonal and any set of $k+1$ members of \mathcal{A} includes $\ell+1$ pairwise orthogonal vectors. Let $\alpha(d, k, \ell, \mathbb{F})$ denote the largest possible size of a (k, ℓ) -nearly orthogonal subset of \mathbb{F}^d . For the special case of $\ell = 1$, we refer to a $(k, 1)$ -nearly orthogonal set as k -nearly orthogonal, and we let $\alpha(d, k, \mathbb{F}) = \alpha(d, k, 1, \mathbb{F})$. Note that for a field \mathbb{F} and an integer d , $\alpha(d, 1, \mathbb{F})$ is the largest possible size of a set of non-self-orthogonal vectors in \mathbb{F}^d that are pairwise orthogonal, hence $\alpha(d, 1, \mathbb{F}) = d$.

A simple upper bound on $\alpha(d, k, \mathbb{F})$ stems from Ramsey theory. To see this, consider a k -nearly orthogonal set $\mathcal{A} \subseteq \mathbb{F}^d$, and let G denote the graph on the vertex set \mathcal{A} , in which two vertices are adjacent if and only if their vectors are orthogonal. Since the vectors of \mathcal{A} are non-self-orthogonal and lie in \mathbb{F}^d , the graph G has no clique of size $d+1$. Since every $k+1$ members of \mathcal{A} include an orthogonal pair, the graph G has no independent set of size $k+1$. It thus follows that the

*School of Computer Science, The Academic College of Tel Aviv-Yaffo, Tel Aviv, Israel. Supported in part by the Israel Science Foundation (grant No. 1218/20).

†Department of Mathematics and Data Science, Vrije Universiteit Brussel, Brussel, Belgium.

‡Department of Mathematics, ETH Zürich, 8092 Zürich, Switzerland. Email address: aleksa.milojevic@math.ethz.ch. Supported in part by SNSF grant 200021_196965.

§Institute for Theoretical Studies, ETH Zürich, 8092 Zürich, Switzerland. Email address: yuval.wigderson@eth-its.ethz.ch. Supported by Dr. Max Rössler, the Walter Haefner Foundation, and the ETH Zürich Foundation.

size of \mathcal{A} is smaller than the Ramsey number $R(d+1, k+1)$. Using the upper bound on Ramsey numbers of Erdős and Szekeres [12], it follows that $\alpha(d, k, \mathbb{F}) < \binom{d+k}{k}$, so in particular, we have $\alpha(d, k, \mathbb{F}) \leq O(d^k)$ for every fixed integer k . A poly-logarithmic improvement follows from the upper bound on Ramsey numbers due to Ajtai, Komlós, and Szemerédi [1].

The problem of determining the values of $\alpha(d, k, \mathbb{F})$ where \mathbb{F} is the real field \mathbb{R} was suggested by Erdős in the late eighties (see [16]). By considering a set that consists of the vectors of k pairwise disjoint orthogonal bases of \mathbb{R}^d , it follows that $\alpha(d, k, \mathbb{R}) \geq k \cdot d$. Rosenfeld [17] proved that this bound is tight for $k = 2$, and Füredi and Stanley [13] showed that $\alpha(4, 5, \mathbb{R}) \geq 24$, which implies that it is not tight in general. They further showed that for every fixed integers d and ℓ , the limit of $\alpha(d, k, \ell, \mathbb{R})/k$ with k tending to infinity exists and grows exponentially in d . Alon and Szegedy [4] proved that for every integer $\ell \geq 1$ there exists a constant $\delta = \delta(\ell) > 0$, such that for all integers d and $k \geq \ell$ with $k \geq 3$, it holds that

$$\alpha(d, k, \ell, \mathbb{R}) \geq d^{\delta \cdot \log k / \log \log k}, \quad (1)$$

where here and throughout the paper, all logarithms are in base 2. On the upper bound side, Balla, Letzter, and Sudakov [6] proved that $\alpha(d, k, \mathbb{R}) \leq O(d^{(k+1)/3})$ for every fixed integer k , improving on the $O(d^k)$ bound that follows from the Erdős–Szekeres bound. Yet, the known lower and upper bounds on $\alpha(d, k, \mathbb{R})$ for general values of d and k are rather far apart.

In a recent paper, Balla [5] considered a bipartite variant of the notion of nearly orthogonal sets, giving rise to the following definition. For a field \mathbb{F} and integers d and k , let $\beta(d, k, \mathbb{F})$ denote the largest possible size of a set $\mathcal{A} \subseteq \mathbb{F}^d$ of non-self-orthogonal vectors, such that for every two (not necessarily disjoint) sets $A_1, A_2 \subseteq \mathcal{A}$ of size $k+1$ each, there exist vectors $v_1 \in A_1$ and $v_2 \in A_2$ with $\langle v_1, v_2 \rangle = 0$. Since such a set \mathcal{A} is k -nearly orthogonal, it follows that $\alpha(d, k, \mathbb{F}) \geq \beta(d, k, \mathbb{F})$. It was proved in [5] that there exists a constant $\delta > 0$, such that for all integers d and $k \geq 3$, it holds that $\beta(d, k, \mathbb{R}) \geq d^{\delta \cdot \log k / \log \log k}$. This strengthens the result given in (1) for the case $\ell = 1$.

The study of nearly orthogonal sets over finite fields was proposed by Codenotti, Pudlák, and Resta [11]. Motivated by questions in circuit complexity, they explored the quantity $\alpha(d, 2, \mathbb{F}_2)$, which in turn, attracted further attention in the area of information theory (see, e.g., [8, 9, 10]). In striking contrast to the real field [17], it was shown in [14] that there exists a constant $\delta > 0$ such that $\alpha(d, 2, \mathbb{F}_2) \geq d^{1+\delta}$ for infinitely many integers d . It was recently shown in [10] that for every prime p there exists a constant $\delta = \delta(p) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k^{1/(p-1)}$, it holds that $\beta(d, k, \mathbb{F}) \geq d^{\delta \cdot k^{1/(p-1)} / \log k}$. In particular, for the binary field, it follows that $\alpha(d, k, \mathbb{F}_2) \geq \beta(d, k, \mathbb{F}_2) \geq d^{\Omega(k/\log k)}$, and this is tight up to the $\log k$ term in the exponent.

1.1 Our Contribution

In the present paper, we prove lower bounds on $\alpha(d, k, \ell, \mathbb{F})$ and $\beta(d, k, \mathbb{F})$ for fields \mathbb{F} of finite characteristic. The following theorem improves the aforementioned result of [10] for all fields of finite characteristic at least 3.

Theorem 1.1. *For every prime p , there exists a constant $\delta = \delta(p) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k$, it holds that*

$$\beta(d, k, \mathbb{F}) \geq d^{\delta \cdot k / \log k}.$$

Note that the condition $d \geq k$ in Theorem 1.1 is essential, in the sense that for arbitrary integers d and k , the bound guaranteed by the theorem might exceed the number of vectors in \mathbb{F}^d .

Recalling that $\alpha(d, k, \mathbb{F}) \geq \beta(d, k, \mathbb{F})$, Theorem 1.1 implies that for every prime p , there exists a constant $\delta = \delta(p) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k$, it holds that $\alpha(d, k, \mathbb{F}) \geq d^{\delta \cdot k / \log k}$. The following theorem extends this implication to the quantities $\alpha(d, k, \ell, \mathbb{F})$ for an arbitrary fixed integer $\ell \geq 1$.

Theorem 1.2. *For every prime p and every integer $\ell \geq 1$, there exists a constant $\delta = \delta(p, \ell) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k \geq \ell$, it holds that*

$$\alpha(d, k, \ell, \mathbb{F}) \geq d^{\delta \cdot k / \log k}.$$

The proofs of Theorems 1.1 and 1.2 rely on the probabilistic approach of Alon and Szegedy [4] in their construction of large nearly orthogonal sets over the reals (see also [5, 10]). The main novel ingredients, which might be of independent interest, are estimations for the number of subgraphs of certain types in pseudo-random graphs (specifically, regular graphs with small absolute values of non-trivial eigenvalues). For Theorem 1.1, we prove an upper bound on the number of bounded-size bi-independent sets, i.e., pairs of sets of vertices with no edge connecting a vertex of one set to a vertex of the other (see Theorem 2.4). The proof of this result adapts a technique of Alon and Rödl [3] for counting independent sets in pseudo-random graphs. For Theorem 1.2, we prove an upper bound on the number of bounded-size subgraphs that contain no copy of some arbitrary fixed graph (see Theorem 2.6). The proof incorporates the hypergraph container method, developed independently by Balogh, Morris, and Samotij [7] and by Saxton and Thomason [18], and a result of Alon on the number of copies of a fixed graph in pseudo-random graphs (see [15]). To establish Theorems 1.1 and 1.2, we apply these results to an appropriate family of graphs, termed orthogonality graphs and studied in [2, 20], and combine the obtained bounds with the technique of [4]. In fact, for convenience of presentation, we prove the existence of a set of vectors that simultaneously yields the bounds stated in both theorems (see Theorem 3.1 and the paragraph that follows it).

We finally mention that our results provide, for every field \mathbb{F} of finite characteristic, k -nearly orthogonal sets over \mathbb{F} whose size is optimal up to the $\log k$ term in the exponent. As noted earlier, over the real field, the gap between the known lower and upper bounds is more pronounced. It would be interesting to narrow the gaps in both cases.

2 Counting Subgraphs of Pseudo-random Graphs

In this section, we prove our results on counting subgraphs of pseudo-random graphs. We start with a brief introduction to the concept of (n, d, λ) -graphs.

2.1 Pseudo-random Graphs

An (n, d, λ) -graph is a d -regular graph on n vertices, such that the absolute value of every eigenvalue of its adjacency matrix, besides the largest one, is at most λ . Throughout the paper, the graphs may have loops, at most one at each vertex, where a loop contributes 1 to the degree of its vertex. It is well known that (n, d, λ) -graphs with λ significantly smaller than d enjoy strong

pseudo-random properties and behave, in various senses, like a random graph on n vertices and edge probability d/n . For a thorough introduction to the topic, the reader is referred to [15].

We state below two results on (n, d, λ) -graphs. The first is the following lemma given in [3].

Lemma 2.1 ([3, Lemma 2.2]). *Let $G = (V, E)$ be an (n, d, λ) -graph, and let $B \subseteq V$ be a set of vertices. Define*

$$C = \left\{ u \in V \mid |N(u) \cap B| \leq \frac{d}{2n} \cdot |B| \right\},$$

where $N(u)$ denotes the set of neighbors of u in G (including u itself, if there is a loop at u). Then

$$|B| \cdot |C| \leq \left(\frac{2\lambda n}{d} \right)^2.$$

The second result that we state here was proved by Alon (see [15]). Here, for a graph F , we denote the maximum degree of F by $\Delta(F)$, the automorphism group of F by $\text{Aut}(F)$, and the number of its edges by $e(F)$. For a graph G and a subset U of its vertex set, $G[U]$ stands for the subgraph of G induced by U .

Theorem 2.2 ([15, Theorem 4.10]). *Let $G = (V, E)$ be an (n, d, λ) -graph with, say, $d \leq 0.9 \cdot n$. Let F be a fixed graph on ℓ vertices, and let $u \leq n$ satisfy $u = \omega\left(\lambda \cdot \left(\frac{n}{d}\right)^{\Delta(F)}\right)$. Then, for every set $U \subseteq V$ of size u , the number of (not necessarily induced) copies of F in $G[U]$ is $(1 + o(1)) \cdot \frac{u^\ell}{|\text{Aut}(F)|} \cdot \left(\frac{d}{n}\right)^{e(F)}$.*

Remark 2.3. *Strictly speaking, G represents in Theorem 2.2 an infinite sequence (G_n) of graphs, where G_n has n vertices for each n , and the $o(\cdot)$ and $\omega(\cdot)$ notations are used with respect to n that tends to infinity. The same convention will be used in Theorem 2.6.*

2.2 Bi-independent Sets

We prove the following bipartite analogue of a result of Alon and Rödl [3].

Theorem 2.4. *Let $G = (V, E)$ be an (n, d, λ) -graph, and let $s = \frac{2n \log n}{d}$. Then for every integer $k \geq s$, the number of pairs (U_1, U_2) of (not necessarily disjoint) subsets of V with $|U_1| = |U_2| = k$, such that no edge of G connects a vertex of U_1 to a vertex of U_2 , is at most*

$$\frac{1}{k!} \cdot n^{2s} \cdot \left(\frac{2\lambda n}{d} \right)^{2 \cdot (k-s)}.$$

Proof: Consider the sequences $u_1, v_1, u_2, v_2, \dots, u_k, v_k$ of $2k$ vertices of G , such that the vertices u_1, \dots, u_k are distinct, the vertices v_1, \dots, v_k are distinct, and no edge of G connects a vertex of $\{u_1, \dots, u_k\}$ to a vertex of $\{v_1, \dots, v_k\}$. Such a sequence can be chosen in k iterations, where the i th iteration, $0 \leq i < k$, is dedicated to choosing u_{i+1} and v_{i+1} . Let $B_0 = V$, and for each $i \in [k-1]$, let B_i denote the set of all vertices of G that are not adjacent to any of the vertices of $\{u_1, \dots, u_i\}$. We further define

$$C_i = \left\{ u \in V \mid |N(u) \cap B_i| \leq \frac{d}{2n} \cdot |B_i| \right\}$$

and apply Lemma 2.1 to obtain that $|B_i| \cdot |C_i| \leq \left(\frac{2\lambda n}{d}\right)^2$.

Suppose that we have already chosen the first $2i$ vertices $u_1, v_1, \dots, u_i, v_i$, and consider the choice of u_{i+1} and v_{i+1} . Since v_{i+1} is not allowed to be adjacent to the vertices of $\{u_1, \dots, u_i\}$, it

must be chosen from B_i . Further, if u_{i+1} is not chosen from C_i , then $|N(u_{i+1}) \cap B_i| > \frac{d}{2n} \cdot |B_i|$, and thus $|B_{i+1}| < (1 - \frac{d}{2n}) \cdot |B_i|$. Therefore, for at most $s = \frac{2n \log n}{d}$ of the indices i , it holds that $u_{i+1} \notin C_i$. On the other hand, if u_{i+1} is chosen from C_i , then the number of possibilities to choose u_{i+1} and v_{i+1} is at most $|B_i| \cdot |C_i| \leq (\frac{2\lambda n}{d})^2$. It thus follows that the number of ways to choose the sequence $u_1, v_1, \dots, u_k, v_k$ does not exceed

$$\binom{k}{s} \cdot n^{2s} \cdot \left(\frac{2\lambda n}{d}\right)^{2 \cdot (k-s)}.$$

Indeed, there are $\binom{k}{s}$ ways to choose s indices covering all the indices i with $u_{i+1} \notin C_i$, and for each such index, there are at most n^2 ways to choose u_{i+1} and v_{i+1} . As shown above, for each of the remaining $k - s$ indices i , there are at most $(\frac{2\lambda n}{d})^2$ ways to choose u_{i+1} and v_{i+1} . We finally divide the obtained bound by $(k!)^2$, to avoid counting the permutations of the vertices of $\{u_1, \dots, u_k\}$ and of $\{v_1, \dots, v_k\}$. This yields the desired bound and completes the proof. ■

We derive the following corollary.

Corollary 2.5. *Let $G = (V, E)$ be an (n, d, λ) -graph, and let $s = \frac{2n \log n}{d}$. Then for every integer k , the number of pairs (U_1, U_2) of (not necessarily disjoint) subsets of V with $|U_1| \leq k$ and $|U_2| \leq k$, such that no edge of G connects a vertex of U_1 to a vertex of U_2 , is at most*

$$(k+1)^2 \cdot \max\left(n, \left(\frac{2\lambda n}{d}\right)^2\right)^{s+k}.$$

Proof: For a given integer k and for arbitrary integers $0 \leq k_1, k_2 \leq k$, consider the pairs (U_1, U_2) of subsets of V with $|U_1| = k_1$ and $|U_2| = k_2$, such that no edge of G connects a vertex of U_1 to a vertex of U_2 . Suppose without loss of generality that $k_1 \leq k_2$. If $k_1 < s$, then the number of these pairs is clearly bounded by $n^{k_1+k_2} < n^{s+k}$. Otherwise, by Theorem 2.4, there are at most

$$n^{2s} \cdot \left(\frac{2\lambda n}{d}\right)^{2 \cdot (k_1-s)}$$

ways to choose k_1 vertices for each of U_1 and U_2 , and there are at most $n^{k_2-k_1}$ ways to choose additional $k_2 - k_1$ vertices for U_2 . Therefore, the number of pairs in this case does not exceed

$$n^{2s} \cdot \left(\frac{2\lambda n}{d}\right)^{2 \cdot (k_1-s)} \cdot n^{k_2-k_1} \leq \max\left(n, \left(\frac{2\lambda n}{d}\right)^2\right)^{2s+(k_1-s)+(k_2-k_1)} \leq \max\left(n, \left(\frac{2\lambda n}{d}\right)^2\right)^{s+k}.$$

The proof is completed by considering all the possible values of the integers k_1 and k_2 . ■

2.3 F -free Subgraphs

For a graph F , a graph is called F -free if it contains no (not necessarily induced) copy of F . We prove the following theorem (see Remark 2.3).

Theorem 2.6. *Let $G = (V, E)$ be an (n, d, λ) -graph with, say, $d \leq 0.9 \cdot n$. Suppose that $n = \Theta(d)$ and $n = \omega(\lambda)$. Then, for every fixed graph F and for all integers $k \leq n$, the number of sets $U \subseteq V$ of size at most k for which $G[U]$ is F -free is at most*

$$2^{O(\log n \cdot \log(\frac{n}{\lambda}))} \cdot \lambda^k.$$

The Container Method. In what follows, we present a statement of the container method, as given by Saxton and Thomason in [19]. We start with some notations. For an integer $\ell \geq 2$, let H be an ℓ -uniform hypergraph on the vertex set V . Let $P(V)$ denote the power set of V , and let $e(H)$ denote the number of hyperedges in H . For a set $U \subseteq V$, let $H[U]$ denote the sub-hypergraph of H induced by U . The set U is called an independent set of H if $e(H[U]) = 0$. For a set $\sigma \subseteq V$ of size $|\sigma| \leq \ell$, let $d(\sigma)$ denote the number of hyperedges in H that contain σ . For each $2 \leq j \leq \ell$ and for every vertex $v \in V$, let $d^{(j)}(v)$ denote the maximum of $d(\sigma)$ over all sets $\sigma \subseteq V$ with $|\sigma| = j$ and $v \in \sigma$. It clearly holds that $d^{(j)}(v) \leq |V|^{\ell-j}$. For each $2 \leq j \leq \ell$ and for any real $\tau > 0$, we define $\delta_j(H, \tau) = \frac{1}{\tau^{j-1} \cdot \ell \cdot e(H)} \cdot \sum_{v \in V} d^{(j)}(v)$ and $\delta(H, \tau) = 2^{\binom{\ell}{2}-1} \cdot \sum_{j=2}^{\ell} 2^{-\binom{j-1}{2}} \cdot \delta_j(H, \tau)$.

The following theorem forms a simplified version of [19, Theorem 5.1].

Theorem 2.7 ([19]). *For a fixed integer $\ell \geq 2$, let H be an ℓ -uniform hypergraph on the vertex set V , and let e_0 be an integer satisfying $e_0 \leq e(H)$. Let $\tau : P(V) \rightarrow \mathbb{R}^+$ be a function such that for every set $U \subseteq V$ with $e(H[U]) \geq e_0$, it holds that*

$$\tau(U) < \frac{1}{2} \quad \text{and} \quad \delta(H[U], \tau(U)) \leq \frac{1}{12 \cdot \ell!}.$$

Define

$$f_0 = \max\{-|U| \cdot \tau(U) \cdot \log \tau(U) \mid U \subseteq V, e(H[U]) \geq e_0\}.$$

Then there exists a collection $\mathcal{C} \subseteq P(V)$, such that

1. every independent set of H is contained in some set of \mathcal{C} ,
2. $e(H[C]) \leq e_0$ for each $C \in \mathcal{C}$, and
3. $\log |\mathcal{C}| \leq O(f_0 \cdot \log(\frac{e(H)}{e_0}))$.

Equipped with Theorem 2.7, we are ready to prove Theorem 2.6.

Proof of Theorem 2.6: Fix a graph F on ℓ vertices, and let H denote the ℓ -uniform hypergraph on the vertex set of G , where a set U of ℓ vertices forms a hyperedge in H if and only if $G[U]$ contains a copy of F . By Theorem 2.2, using $n = \Theta(d)$ and $n = \omega(\lambda)$, the number of hyperedges of H satisfies $e(H) = \Theta(n^\ell)$. For a given integer $k \leq n$, our goal is to prove that the number of independent sets in H of size at most k is bounded by $2^{O(\log n \cdot \log(\frac{n}{\lambda}))} \cdot \lambda^k$. Notice that it suffices to prove such a bound on the number of independent sets in H of size exactly k .

We apply the container method, described in Theorem 2.7. Define, say, $e_0 = \lambda^\ell \cdot \log(\frac{n}{\lambda})$, and notice that the assumption $n = \omega(\lambda)$ implies that $e_0 = \omega(\lambda^\ell)$. For a set $U \subseteq V$ of size u , consider the hypergraph $H[U]$, denote $m = e(H[U])$, and suppose that $m \geq e_0$. This obviously implies that $u \geq e_0^{1/\ell} = \omega(\lambda)$, hence using $n = \Theta(d)$, we can apply Theorem 2.2 to obtain that $m = \Theta(u^\ell)$. For each $2 \leq j \leq \ell$, every vertex $v \in U$ satisfies in $H[U]$ that $d^{(j)}(v) \leq u^{\ell-j}$, hence for any $\tau > 0$,

$$\delta_j(H[U], \tau) \leq \frac{u \cdot u^{\ell-j}}{\tau^{j-1} \cdot \ell \cdot m} \leq O\left(\frac{1}{(\tau \cdot u)^{j-1}}\right).$$

Setting $\tau(U) = \frac{a}{u}$ for a sufficiently large constant a , it holds that

$$\delta(H[U], \tau(U)) \leq O\left(\sum_{j=2}^{\ell} \delta_j(H[U], \tau(U))\right) \leq \frac{1}{12 \cdot \ell!}.$$

For a growing n , using $u = \omega(\lambda)$, it further follows that $\tau(U) < 1/2$. We also observe that the quantity f_0 from Theorem 2.7 satisfies $f_0 \leq O(\log n)$. Indeed, for every set $U \subseteq V$, our definition of τ implies that $-|U| \cdot \tau(U) \cdot \log \tau(U) \leq O(\log |U|) \leq O(\log n)$. We finally notice, using $e(H) = \Theta(n^\ell)$ and $e_0 \geq \lambda^\ell$, that $\log(\frac{e(H)}{e_0}) \leq O(\log(\frac{n}{\lambda}))$.

Now, we derive from Theorem 2.7 that there exists a collection $\mathcal{C} \subseteq P(V)$, such that

1. every independent set of H is contained in some set of \mathcal{C} ,
2. $e(H[C]) \leq e_0$ for each $C \in \mathcal{C}$, and
3. $\log |\mathcal{C}| \leq O(f_0 \cdot \log(\frac{e(H)}{e_0})) \leq O(\log n \cdot \log(\frac{n}{\lambda}))$.

By Theorem 2.2, there exists a constant c_0 , such that every set $U \subseteq V$ with $|U| > c_0 \cdot e_0^{1/\ell} = \omega(\lambda)$ satisfies $e(H[U]) = \Theta(|U|^\ell) > e_0$. Hence, Item 2 above implies that $|C| \leq c_0 \cdot e_0^{1/\ell}$ for each $C \in \mathcal{C}$. It therefore follows from Item 1 that the number of independent sets of H of size k does not exceed

$$\begin{aligned} |\mathcal{C}| \cdot \binom{c_0 \cdot e_0^{1/\ell}}{k} &\leq 2^{O(\log n \cdot \log(\frac{n}{\lambda}))} \cdot \left(\frac{c_0 \cdot e_0^{1/\ell} \cdot e}{k}\right)^k \\ &\leq 2^{O(\log n \cdot \log(\frac{n}{\lambda}))} \cdot \lambda^k \cdot \left(\frac{c_0 \cdot \log^{1/\ell}(\frac{n}{\lambda}) \cdot e}{k}\right)^k \\ &\leq 2^{O(\log n \cdot \log(\frac{n}{\lambda}))} \cdot \lambda^k. \end{aligned}$$

Here, the first inequality follows by Item 3 and the inequality $\binom{n}{k} \leq (\frac{n \cdot e}{k})^k$, and the second by the definition of e_0 . For the third inequality, notice that the term $(\frac{c_0 \cdot \log^{1/\ell}(\frac{n}{\lambda}) \cdot e}{k})^k$ is bounded from above by 1 for $k \geq c_0 \cdot \log^{1/\ell}(\frac{n}{\lambda}) \cdot e$, and by $2^{O(\log n \cdot \log(\frac{n}{\lambda}))}$ for any other k . This completes the proof. \blacksquare

3 Nearly Orthogonal Sets over Finite Fields

In this section, we establish the following theorem.

Theorem 3.1. *For every prime p and every integer $\ell \geq 2$, there exists a constant $\delta = \delta(p, \ell) > 0$, such that for every field \mathbb{F} of characteristic p and for all integers $k \geq 2$ and $d \geq k \geq \ell$, the following holds. There exists a set \mathcal{A} of at least $d^{\delta \cdot k / \log k}$ non-self-orthogonal vectors of \mathbb{F}^d , such that*

1. every set $A \subseteq \mathcal{A}$ with $|A| = k$ includes ℓ pairwise orthogonal vectors, and
2. for every two sets $A_1, A_2 \subseteq \mathcal{A}$ with $|A_1| = |A_2| = 2k - 1$, there exist vectors $v_1 \in A_1$ and $v_2 \in A_2$ with $\langle v_1, v_2 \rangle = 0$.

We observe that Theorem 3.1 yields Theorems 1.1 and 1.2. Indeed, for Theorem 1.1, apply the theorem with k being $\lfloor \frac{k}{2} \rfloor + 1$ and with $\ell = 1$ to obtain, using Item 2, the desired bound on $\beta(d, k, \mathbb{F})$ for an appropriate $\delta = \delta(p)$. For Theorem 1.2, apply the theorem with k and ℓ being $k + 1$ and $\ell + 1$ respectively to obtain, using Item 1, the desired bound on $\alpha(d, k, \ell, \mathbb{F})$.

Towards the proof of Theorem 3.1, we apply the results from the previous section to a family of graphs, defined next.

3.1 The Orthogonality Graph

For a prime p , let \mathbb{F}_p denote the field of order p . For a prime p and an integer t , let $G(p, t)$ denote the graph whose vertices are all the nonzero vectors in \mathbb{F}_p^t , where two such (not necessarily distinct) vectors are adjacent if and only if they are orthogonal. The second largest eigenvalue of $G(p, t)$ was determined in [2, 20], as stated below.

Proposition 3.2 ([2, 20]). *For every prime p and every integer t , the graph $G(p, t)$ is an (n, d, λ) -graph for*

$$n = p^t - 1, \quad d = p^{t-1} - 1, \quad \text{and} \quad \lambda = (p - 1) \cdot p^{t/2-1}.$$

By applying Corollary 2.5 to the graph $G(p, t)$, we obtain the following result.

Theorem 3.3. *For every prime p , there exists a constant $c = c(p)$, such that for all integers t and k , the number of pairs (C_1, C_2) of subsets of $\mathbb{F}_p^t \setminus \{0\}$ with $|C_1| \leq k$ and $|C_2| \leq k$, such that $\langle v_1, v_2 \rangle \neq 0$ for all $v_1 \in C_1$ and $v_2 \in C_2$, is at most $2^{c \cdot (t^2+k)} \cdot p^{t \cdot k}$.*

Proof: Fix a prime p , and let t and k be some integers. By Proposition 3.2, the graph $G(p, t)$ is an (n, d, λ) -graph for $n = p^t - 1$, $d = p^{t-1} - 1$, and $\lambda = (p - 1) \cdot p^{t/2-1} \leq p^{t/2}$. Letting $s = \frac{2n \log n}{d}$, it holds that $s = \Theta(t)$, and it is not difficult to verify that $(\frac{2\lambda n}{d})^2 \geq n$. By Corollary 2.5, the number of pairs (C_1, C_2) of sets of vertices of $G(p, t)$ with $|C_1| \leq k$ and $|C_2| \leq k$, such that no edge connects a vertex of C_1 to a vertex of C_2 , is at most

$$\begin{aligned} (k+1)^2 \cdot \left(\frac{2\lambda n}{d}\right)^{2 \cdot (s+k)} &= (k+1)^2 \cdot \left(\frac{2n}{d}\right)^{2 \cdot (s+k)} \cdot \lambda^{2s} \cdot \lambda^{2k} \\ &\leq 2^{O(k)} \cdot 2^{O(s+k)} \cdot 2^{O(s \cdot t)} \cdot p^{t \cdot k} \leq 2^{O(t^2+k)} \cdot p^{t \cdot k}. \end{aligned}$$

By the definition of the graph $G(p, t)$, the proof is completed. ■

By applying Theorem 2.6 to the graph $G(p, t)$, we obtain the following result.

Theorem 3.4. *For every prime p and every integer $\ell \geq 2$, there exists a constant $c = c(p, \ell)$, such that for all integers t and k , the number of subsets of $\mathbb{F}_p^t \setminus \{0\}$ of size at most k that include no ℓ pairwise orthogonal vectors is at most $2^{c \cdot t^2} \cdot p^{t \cdot k/2}$.*

Proof: Fix a prime p and an integer $\ell \geq 2$, and let t and k be some integers. It may be assumed that t is sufficiently large, because if t is bounded by some constant, then so is k , and the statement of the theorem trivially holds with an appropriate constant c . By Proposition 3.2, the graph $G(p, t)$ is an (n, d, λ) -graph for $n = p^t - 1$, $d = p^{t-1} - 1$, and $\lambda = (p - 1) \cdot p^{t/2-1} \leq p^{t/2}$. Note that $d \leq 0.9 \cdot n$, and that for a growing t , we have $n = \Theta(d)$ and $n = \omega(\lambda)$. Applying Theorem 2.6 with F being the complete graph K_ℓ of order ℓ , we obtain that the number of sets of at most k vertices of $G(p, t)$ with no copy of K_ℓ is at most

$$2^{O(\log^2 n)} \cdot \lambda^k \leq 2^{O(t^2)} \cdot p^{t \cdot k/2}.$$

By the definition of the graph $G(p, t)$, the proof is completed. ■

3.2 Proof of Theorem 3.1

Before turning to the proof of Theorem 3.1, let us collect a few notations and facts about the tensor product operation on vectors, which plays a central role in the argument. For a field \mathbb{F} and integers t_1, t_2 , the tensor product $w = u \otimes v$ of two vectors $u \in \mathbb{F}^{t_1}$ and $v \in \mathbb{F}^{t_2}$ is defined as the vector in $\mathbb{F}^{t_1 \cdot t_2}$, whose coordinates are indexed by the pairs (i_1, i_2) with $i_1 \in [t_1]$ and $i_2 \in [t_2]$, defined by $w_{(i_1, i_2)} = u_{i_1} \cdot v_{i_2}$. Note that for integers t and m and for given vectors $v_1, \dots, v_m \in \mathbb{F}^t$, the vector $v_1 \otimes \dots \otimes v_m$ lies in \mathbb{F}^{t^m} and consists of all the t^m possible products of m values, one from each vector v_j with $j \in [m]$. It is well known and easy to verify that for vectors $u_1, \dots, u_m \in \mathbb{F}^t$ and $v_1, \dots, v_m \in \mathbb{F}^t$, the two vectors $u = u_1 \otimes \dots \otimes u_m$ and $v = v_1 \otimes \dots \otimes v_m$ satisfy

$$\langle u, v \rangle = \prod_{j=1}^m \langle u_j, v_j \rangle. \quad (2)$$

Proof of Theorem 3.1: Let p be a fixed prime, and let $\ell \geq 2$ be a fixed integer. It suffices to prove the result for the field \mathbb{F}_p of order p , because it forms a sub-field of every field of characteristic p . For integers t and m , let $Q \subseteq (\mathbb{F}_p^t)^m$ denote the collection of all m -tuples of non-self-orthogonal vectors of \mathbb{F}_p^t . Notice that the number of non-self-orthogonal vectors in \mathbb{F}_p^t is at least p^{t-1} , because any choice for the first $t-1$ entries of a vector in \mathbb{F}_p^t can be extended to a non-self-orthogonal vector by choosing for its last entry either 0 or 1. This implies that $|Q| \geq p^{m \cdot (t-1)}$.

We apply the probabilistic method. For an integer n , let $\mathcal{Z} = (z_1, \dots, z_n)$ be a random sequence of n elements chosen uniformly and independently from Q , and let $\mathcal{A} \subseteq \mathbb{F}_p^{t^m}$ be the set of all m -fold tensor products of the m -tuples of \mathcal{Z} , that is, the vectors $v_1 \otimes \dots \otimes v_m$ for which $z_i = (v_1, \dots, v_m)$ for some $i \in [n]$. The vectors of \mathcal{A} are non-self-orthogonal, because for every $(v_1, \dots, v_m) \in Q$, it follows from (2) that the vector $v = v_1 \otimes \dots \otimes v_m$ satisfies $\langle v, v \rangle = \prod_{i=1}^m \langle v_i, v_i \rangle \neq 0$. We will show that for a given integer k and for an appropriate choice of the integers t, m , and n , the set \mathcal{A} satisfies with positive probability the properties declared in the theorem.

Let \mathcal{C}_1 denote the collection of all subsets of $\mathbb{F}_p^t \setminus \{0\}$ of size at most k that include no ℓ pairwise orthogonal vectors. Consider the collection

$$\mathcal{B}_1 = \{C^{(1)} \times C^{(2)} \times \dots \times C^{(m)} \mid C^{(j)} \in \mathcal{C}_1 \text{ for all } j \in [m]\}.$$

Notice that each set $B \in \mathcal{B}_1$ consists of at most k^m m -tuples of vectors in \mathbb{F}_p^t . Let \mathcal{E}_1 denote the event that some set of \mathcal{B}_1 includes at least k elements of the sequence \mathcal{Z} . More formally, we define \mathcal{E}_1 as the event that there exist sets $B \in \mathcal{B}_1$ and $I \subseteq [n]$ with $|I| = k$, such that $\{z_i \mid i \in I\} \subseteq B$. By the union bound, it follows that

$$\Pr[\mathcal{E}_1] \leq |\mathcal{B}_1| \cdot \binom{n}{k} \cdot \left(\frac{k^m}{|Q|}\right)^k \leq |\mathcal{B}_1| \cdot \left(\frac{n \cdot k^m}{p^{m \cdot (t-1)}}\right)^k. \quad (3)$$

Let \mathcal{C}_2 denote the collection of all pairs (C_1, C_2) of subsets of $\mathbb{F}_p^t \setminus \{0\}$ of size at most k , such that no vector of C_1 is orthogonal to a vector of C_2 . Consider the collection \mathcal{B}_2 of all pairs (B_1, B_2) of the form

$$B_1 = C_1^{(1)} \times C_1^{(2)} \times \dots \times C_1^{(m)} \text{ and } B_2 = C_2^{(1)} \times C_2^{(2)} \times \dots \times C_2^{(m)}, \quad (4)$$

where $(C_1^{(1)}, C_2^{(1)}), (C_1^{(2)}, C_2^{(2)}), \dots, (C_1^{(m)}, C_2^{(m)})$ are m pairs of the collection \mathcal{C}_2 . As before, each B_1 and B_2 consists of at most k^m m -tuples of vectors in \mathbb{F}_p^t . Let \mathcal{E}_2 denote the event that there exist a pair $(B_1, B_2) \in \mathcal{B}_2$ and disjoint sets $I_1, I_2 \subseteq [n]$ with $|I_1| = |I_2| = k$, such that $\{z_i \mid i \in I_1\} \subseteq B_1$ and $\{z_i \mid i \in I_2\} \subseteq B_2$. By the union bound, it follows that

$$\Pr[\mathcal{E}_2] \leq |\mathcal{B}_2| \cdot \binom{n}{k}^2 \cdot \left(\frac{k^m}{|Q|}\right)^{2k} \leq |\mathcal{B}_2| \cdot \left(\frac{n \cdot k^m}{p^{m \cdot (t-1)}}\right)^{2k}. \quad (5)$$

Let us set the parameters of the construction, ensuring that the event $\mathcal{E}_1 \vee \mathcal{E}_2$ occurs with probability smaller than 1. Let d and k be two integers satisfying $d \geq k \geq \ell$. We may assume, whenever needed, that k is sufficiently large, because constant values of k can be handled by an appropriate choice of the constant δ from the assertion of the theorem, using the d vectors of the standard basis of \mathbb{F}_p^d . By Theorems 3.4 and 3.3, there exists a constant $c \geq 1$, such that $|\mathcal{C}_1| \leq 2^{c \cdot t^2} \cdot p^{t \cdot k/2}$ and $|\mathcal{C}_2| \leq 2^{c \cdot (t^2+k)} \cdot p^{t \cdot k}$, implying that

$$|\mathcal{B}_1| = |\mathcal{C}_1|^m \leq 2^{cm \cdot t^2} \cdot p^{mtk/2} \quad \text{and} \quad |\mathcal{B}_2| = |\mathcal{C}_2|^m \leq 2^{cm \cdot (t^2+k)} \cdot p^{mtk}. \quad (6)$$

Let t be the largest integer satisfying, say, $k \geq 5c \cdot t$, and let m be the largest integer satisfying $d \geq t^m$. By the assumption $d \geq k$, we have $m \geq 1$. Set $n = \lfloor p^{m \cdot t/4} \rfloor$. Combining (3) and (6), we obtain that

$$\Pr[\mathcal{E}_1] \leq 2^{cm \cdot t^2} \cdot p^{mtk/2} \cdot \left(\frac{n \cdot k^m}{p^{m \cdot (t-1)}}\right)^k \leq 2^{cm \cdot t^2} \cdot \left(\frac{k^m}{p^{m \cdot (t/4-1)}}\right)^k \leq \left(2^{t/5} \cdot \frac{5c(t+1)}{p^{t/4-1}}\right)^{mk} < \frac{1}{2},$$

where the second inequality holds by our choice of n , the third by our choice of t , and the fourth by the assumption that k (and thus t) is sufficiently large. By a similar calculation, combining (5) and (6), we obtain that

$$\Pr[\mathcal{E}_2] \leq 2^{cm \cdot (t^2+k)} \cdot p^{mtk} \cdot \left(\frac{n \cdot k^m}{p^{m \cdot (t-1)}}\right)^{2k} \leq 2^{2cm \cdot t^2} \cdot \left(\frac{k^m}{p^{m \cdot (t/4-1)}}\right)^{2k} < \frac{1}{2},$$

where for the second inequality we further use the inequality $k \leq t^2$, which holds assuming that k is sufficiently large. It thus follows, by the union bound, that the probability that the event $\mathcal{E}_1 \vee \mathcal{E}_2$ occurs is smaller than 1. This implies that there exists a choice for the sequence \mathcal{Z} for which the event $\mathcal{E}_1 \vee \mathcal{E}_2$ does not occur. We fix such a choice for \mathcal{Z} and consider the corresponding set \mathcal{A} .

We show now that the set \mathcal{A} satisfies the required properties. We start by proving that every set $A \subseteq \mathcal{A}$ with $|A| = k$ includes ℓ pairwise orthogonal vectors. To do so, we show that for every set $I \subseteq [n]$ with $|I| = k$, the m -fold tensor products associated with the m -tuples of $\{z_i \mid i \in I\}$ include ℓ pairwise orthogonal vectors. So assume for contradiction that there exists a set $I \subseteq [n]$ with $|I| = k$ that does not satisfy this property. For each $j \in [m]$, let $C^{(j)}$ denote the set of the j th projections of the tuples of $\{z_i \mid i \in I\}$, and notice that $|C^{(j)}| \leq k$. Using the property of tensor product given in (2), it follows that $C^{(j)}$ does not include ℓ pairwise orthogonal vectors. Therefore, the set $C^{(1)} \times C^{(2)} \times \dots \times C^{(m)}$ lies in \mathcal{B}_1 and contains $\{z_i \mid i \in I\}$. This contradicts the fact that the event \mathcal{E}_1 does not occur for our choice of \mathcal{Z} .

We next prove that for every two sets $A_1, A_2 \subseteq \mathcal{A}$ with $|A_1| = |A_2| = 2k - 1$, there exist vectors $v_1 \in A_1$ and $v_2 \in A_2$ with $\langle v_1, v_2 \rangle = 0$. To see this, assume for contradiction that there

exist two sets $A_1, A_2 \subseteq \mathcal{A}$ with $|A_1| = |A_2| = 2k - 1$, such that no vector of A_1 is orthogonal to a vector of A_2 . If $|A_1 \cap A_2| \geq k$, then there exists a set of k vectors of \mathcal{A} with no orthogonal pair, in contradiction to the property of \mathcal{A} shown above. Otherwise, there exist disjoint sets $A'_1 \subseteq A_1 \setminus A_2$ and $A'_2 \subseteq A_2 \setminus A_1$ satisfying $|A'_1| = |A'_2| = k$. Let $I_1, I_2 \subseteq [n]$ be sets with $|I_1| = |I_2| = k$, such that the vectors of A'_1 and A'_2 are the m -fold tensor products associated with the m -tuples of $\{z_i \mid i \in I_1\}$ and $\{z_i \mid i \in I_2\}$ respectively. Note that I_1 and I_2 are disjoint. For each $j \in [m]$, let $C_1^{(j)}$ and $C_2^{(j)}$ denote the sets of the j th projections of the tuples of $\{z_i \mid i \in I_1\}$ and $\{z_i \mid i \in I_2\}$ respectively, and notice that $|C_1^{(j)}| \leq k$ and $|C_2^{(j)}| \leq k$. Using the property of tensor product given in (2), it follows that no vector of $C_1^{(j)}$ is orthogonal to a vector of $C_2^{(j)}$. Therefore, there exists a pair $(B_1, B_2) \in \mathcal{B}_2$, defined as in (4), for which it holds that $\{z_i \mid i \in I_1\} \subseteq B_1$ and $\{z_i \mid i \in I_2\} \subseteq B_2$. This contradicts the fact that the event \mathcal{E}_2 does not occur for our choice of \mathcal{Z} .

We finally analyze the size of the collection \mathcal{A} . Recall that the vectors of \mathcal{A} are non-self-orthogonal. It follows from the above discussion that no vector of \mathcal{A} is associated with more than $k - 1$ of the m -tuples of \mathcal{Z} . This implies that

$$|\mathcal{A}| \geq \frac{n}{k-1} \geq p^{\Omega(m \cdot t)} \geq p^{\Omega((\log d) \cdot t / (\log t))} \geq d^{\Omega(t / \log t)} \geq d^{\Omega(k / \log k)},$$

where the multiplicative constants hidden by the Ω notation depend only on p and ℓ . By adding $d - t^m$ zero entries at the end of each vector of \mathcal{A} , we obtain the desired subset of \mathbb{F}_p^d , and the proof is completed. \blacksquare

References

- [1] M. Ajtai, J. Komlós, and E. Szemerédi. A note on Ramsey numbers. *J. Comb. Theory, Ser. A*, 29(3):354–360, 1980.
- [2] N. Alon and M. Krivelevich. Constructive bounds for a Ramsey-type problem. *Graphs and Combinatorics*, 13(3):217–225, 1997.
- [3] N. Alon and V. Rödl. Sharp bounds for some multicolor Ramsey numbers. *Combinatorica*, 25(2):125–141, 2005.
- [4] N. Alon and M. Szegedy. Large sets of nearly orthogonal vectors. *Graphs and Combinatorics*, 15(1):1–4, 1999.
- [5] I. Balla. Orthonormal representations, vector chromatic number, and extension complexity. *arXiv*, abs/2310.17482, 2023.
- [6] I. Balla, S. Letzter, and B. Sudakov. Orthonormal representations of H -free graphs. *Discret. Comput. Geom.*, 64(3):654–670, 2020.
- [7] J. Balogh, R. Morris, and W. Samotij. Independent sets in hypergraphs. *J. Amer. Math. Soc.*, 28(3):669–709, 2015.
- [8] A. Barg and G. Zémor. High-rate storage codes on triangle-free graphs. *IEEE Trans. Inform. Theory*, 68(12):7787–7797, 2022.

- [9] A. Blasiak, R. Kleinberg, and E. Lubetzky. Broadcasting with side information: Bounding and approximating the broadcast rate. *IEEE Trans. Inform. Theory*, 59(9):5811–5823, 2013.
- [10] D. Chawin and I. Haviv. Nearly orthogonal sets over finite fields. In *Proc. of the 40th International Symposium on Computational Geometry (SoCG'24)*, pages 54:1–54:11, 2024.
- [11] B. Codenotti, P. Pudlák, and G. Resta. Some structural properties of low-rank matrices related to computational complexity. *Theor. Comput. Sci.*, 235(1):89–107, 2000.
- [12] P. Erdős and G. Szekeres. A combinatorial problem in geometry. *Compositio Mathematica*, 2:463–470, 1935.
- [13] Z. Füredi and R. P. Stanley. Sets of vectors with many orthogonal pairs. *Graphs and Combinatorics*, 8(4):391–394, 1992.
- [14] A. Golovnev and I. Haviv. The (generalized) orthogonality dimension of (generalized) Kneser graphs: Bounds and applications. *Theory of Computing*, 18(22):1–22, 2022. Preliminary version in CCC'21.
- [15] M. Krivelevich and B. Sudakov. Pseudo-random graphs. In E. Györi, G. O. H. Katona, L. Lovász, and T. Fleiner, editors, *More Sets, Graphs and Numbers: A Salute to Vera Sós and András Hajnal*, pages 199–262. Springer, Berlin, Heidelberg, 2006.
- [16] J. Nešetřil and M. Rosenfeld. Embedding graphs in Euclidean spaces, an exploration guided by Paul Erdős. *Geombinatorics*, 6:143–155, 1997.
- [17] M. Rosenfeld. Almost orthogonal lines in E^d . *DIMACS Series in Discrete Math.*, 4:489–492, 1991.
- [18] D. Saxton and A. Thomason. Hypergraph containers. *Inventiones Mathematicae*, 201(3):925–992, 2015.
- [19] D. Saxton and A. Thomason. Online containers for hypergraphs, with applications to linear equations. *J. Comb. Theory, Ser. B*, 121:248–283, 2016.
- [20] L. A. Vinh. On the number of orthogonal systems in vector spaces over finite fields. *Electr. J. Comb.*, 15(32):1–4, 2008.