On explicit constructions of designs

Xizhi Liu* Dhruv Mubayi†

Department of Mathematics, Statistics, and Computer Science
University of Illinois
Chicago, IL, 60607 U.S.A.

{xliu246,mubayi}@uic.edu

Submitted: Jun 21, 2021; Accepted: Dec 27, 2021; Published: Mar 25, 2022

Abstract

An (n, r, s)-system is an r-uniform hypergraph on n vertices such that every pair of edges has an intersection of size less than s. Using probabilistic arguments, Rödl and Šiňajová showed that for all fixed integers $r > s \geqslant 2$, there exists an (n, r, s)-system with independence number $O\left(n^{1-\delta+o(1)}\right)$ for some optimal constant $\delta > 0$ only related to r and s. We show that for certain pairs (r, s) with $s \leqslant r/2$ there exists an explicit construction of an (n, r, s)-system with independence number $O\left(n^{1-\epsilon}\right)$, where $\epsilon > 0$ is an absolute constant only related to r and s. Previously this was known only for $s > r/2$ by results of Chattopadhyay and Goodman.

Mathematics Subject Classifications: 05B05,05C69,05D40

1 Introduction

For a finite set V and a positive integer r denote by $\binom{V}{r}$ the collection of all r-subsets of V. An r-uniform hypergraph (r-graph) $\mathcal{H}$ is a family of r-subsets of finite set which is called the vertex set of $\mathcal{H}$ and is denoted by $V(\mathcal{H})$. We use $|\mathcal{H}|$ to denote the number of edges in $\mathcal{H}$. A set $I \subset V(\mathcal{H})$ is *independent* in $\mathcal{H}$ if it contains no edge of $\mathcal{H}$. The *independence number* of $\mathcal{H}$, denoted by $\alpha(\mathcal{H})$, is the maximum size of an independent set in $\mathcal{H}$.

For integers $n \geqslant r \geqslant s \geqslant 1$ an (n, r, s)-*system* (also called design) is an r-graph on n vertices such that every pair of edges has an intersection of size less than s. Rödl and Šiňajová [13] proved a lower bound for the independence number of an (n, r, s)-system, and moreover, they showed that there exists an (n, r, s)-system whose independence number achieves the lower bound up to a multiplicative constant factor.

*Research partially supported by NSF awards DMS-1763317 and DMS-1952767.

†Research partially supported by NSF awards DMS-1763317 and DMS-1952767.

Theorem 1 (Rödl–Šiňajová [13])**.** *For fixed integers $r > s \geqslant 2$ there exists a constant $c = c(r,s)$ such that every (n,r,s)-system has independence number at least $cn^{\frac{r-s}{r-1}}(\log n)^{\frac{1}{r-1}}$. Moreover, there exists a constant $C = C(r,s)$ such that there exists an (n,r,s)-system with independence number at most $Cn^{\frac{r-s}{r-1}}(\log n)^{\frac{1}{r-1}}$ for every integer $n \geqslant r$.*

Definition 2. For fixed integers $r \geqslant s \geqslant 1$ we say there is an explicitly construction of an (n,r,s)-system with property $\mathcal{P}$ if there exists an algorithm $\mathcal{A}$ such that for every integer n as input, $\mathcal{A}$ runs in time poly(n) and outputs an (n,r,s)-system with property $\mathcal{P}$.

Explicit constructions of (n,r,s)-systems with certain properties are very useful in theoretical computer science. For example, in the seminal work of Nisan and Wigderson [10], dense (n,r,s)-systems are used to construct pseudorandom generators (PRGs) (see also [17, 12] for more applications). More recently, explicit constructions of (n,r,s)-systems with small independence number were used to construct extractors for adversarial sources [4, 3].

In this note, we focus on the explicit constructions of (n,r,s)-systems with small independence number. Rödl and Šiňajová's proof of the existence of an (n,r,s)-system with small independence number uses the Lovász local lemma, and hence it does not provide an explicit way to construct them. Perhaps the first explicit construction of an $(n,3,2)$-system (also called a Steiner triple system) with independence number $O(n^{1-\epsilon})$ for some absolute constant $\epsilon > 0$ is due to Chattopadhyay, Goodman, Goyal, and Li [4]. Their proof uses results about cap sets (see [5, 6]).

Theorem 3 (Chattopadhyay–Goodman–Goyal–Li [4])**.** *There exists a constant $C \geqslant 1$ such that for every integer $n \geqslant 3$ there exists an explicit construction of an $(n,3,2)$-system with independence number at most $Cn^{0.9228}$.*

Later, using results about linear codes [8, 2] and Sidorenko's recent bounds on the size of sets in $\mathbb{Z}_2^n$ containing no r elements that sum to zero [14, 15], Chattopadhyay and Goodman [3] extended Theorem 3 to all integers $r > s \geqslant 2$ with $s \geqslant \lceil r/2 \rceil$.

Theorem 4 (Chattopadhyay–Goodman [3])**.** *There exists a constant $C \geqslant 1$ such that for every integer $s \geqslant 2$ and every even integer $r > s$ there exists an explicit construction of an (n,r,s)-system with independence number at most $Cr^4 n^{\frac{2(r-s)}{r}}$.*

Remark. For odd r they showed that there exists an explicit construction of an (n,r,s)-system with independence number at most $C(r+1)^4 n^{\frac{2(r+1-s)}{r+1}}$.

Our main results in this note extend Theorem 3 for certain values of r and s in the range $s < \lceil r/2 \rceil$ which was not addressed by Theorem 4.

Our proof of the first theorem below is based on a recent result about the maximum size of a set in $\mathbb{Z}_6^n$ that avoids 6-term arithmetic progressions [11].

Theorem 5. *There exists a constant $C > 0$ such that for every integer $r \in \{4,5,6\}$ and every integer $n \geqslant r$ there exists an explicit construction of an $(n,r,2)$-system $\mathcal{H}$ with $\alpha(\mathcal{H}) \leqslant Cn^{0.973}$.*

Using a lemma about the independence number of the product of two hypergraphs we are able to extend Theorem 5 to a wider range of r and s.

For every integer $s = 3^{\ell_1}4^{\ell_2}5^{\ell_3}6^{\ell_4}+1$, where $\ell_1, \ell_2, \ell_3, \ell_4 \geqslant 0$ are integers, define

$$R(s) = \begin{cases} 6(s-1) & \text{if} \quad \ell_1 = \ell_2 = \ell_3 = 0 \\ 5(s-1) & \text{if} \quad \ell_1 = \ell_2 = 0 \quad \text{and} \quad \ell_3 \neq 0 \\ 4(s-1) & \text{if} \quad \ell_1 = 0 \quad \text{and} \quad \ell_2 \neq 0 \\ 3(s-1) & \text{if} \quad \ell_1 \neq 0 \end{cases}$$

Theorem 6. *For every integer s of the form $3^{\ell_1}4^{\ell_2}5^{\ell_3}6^{\ell_4}+1$, where $\ell_1, \ell_2, \ell_3, \ell_4 \geqslant 0$ are integers, and every integer r satisfying $2s \leqslant r \leqslant R(s)$ there exist constants $C = C(\ell_1, \ell_2, \ell_3, \ell_4), \epsilon = \epsilon(\ell_1, \ell_2, \ell_3, \ell_4) > 0$ such that for every integer $n \geqslant r$ there exists an explicit construction of an (n, r, s)-system with independence number at most $Cn^{1-\epsilon}$.*

The following result focusing on $(n, 5, 4)$-systems uses a different argument and it improves the bound $O(n^{2/3})$ given by Theorem 4.

Theorem 7. *There exists a constant $C > 0$ such that for every integer $n \geqslant 5$ there exists an explicit construction of an $(n, 5, 4)$-systems with independence number at most $Cn^{\log_3 2} \leqslant Cn^{0.631}$.*

We prove Theorems 5 and 6 in Section 2, and prove Theorem 7 in Section 3.

2 Proofs of Theorems 5 and 6

2.1 Proof of Theorems 5

Let us first introduce a construction of r-graphs based on r-term arithmetic progressions (r-AP) over $\mathbb{Z}_r^k$. We do not allow trivial progressions so an r-AP has r distinct elements.

Construction $\mathcal{A}(r,k)$. Let $r \geqslant 3$ and $k \geqslant 1$ be integers. The hypergraph $\mathcal{A}(r,k)$ is the r-graph with vertex set $V = \mathbb{Z}_r^k$ and edge set

$$\left\{ \{v_1, \ldots, v_r\} \in \binom{V}{r} : v_1, \ldots, v_r \text{ form an } r\text{-AP} \right\}.$$

Remarks.

- It is clear that $\mathcal{A}(r,k)$ can be constructed in time poly $\left(r^k\right)$ for all integers $r, k \geqslant 1$.
- Even though we defined $\mathcal{A}(r,k)$ for all integers $r \geqslant 3$, in the proof of Theorem 5 we will consider only the case $r = 6$.

The following easy proposition shows that for every integer $r \geqslant 3$ the hypergraph $\mathcal{A}(r,k)$ is *linear*, i.e. every pair of edges has an intersection of size at most one.

Proposition 8. *Let $r \geqslant 3$, $k \geqslant 1$ be integers and $n = r^k$. Then $\mathcal{A}(r,k)$ is an $(n, r, 2)$-system.*

Proof of Proposition 8. Suppose to the contrary that there exist two distinct edges $E, E' \in \mathcal{H}$ such that $|E \cap E'| \geqslant 2$. Assume that $E = \{a, a+d, \dots, a+(r-1)d\}$ for some $a, d \in \mathbb{Z}_r^k$ and d is not the zero vector. Without loss of generality we may assume that $a \in E \cap E'$ (otherwise we can choose an arbitrary element in $E \cap E'$ and rename it as a) and assume that $E' = \{a, a+id, \dots, a+(r-1)id\}$ for some integer $i \in [r-1]$. Since $|E'| = r$, the set $\{0, id \pmod r, \dots, (r-1)id \pmod r\}$ has size r. Therefore, sets $\{0, id \pmod r, \dots, (r-1)id \pmod r\}$ and $\{0, 1, \dots, r-1\}$ are identical, which implies that $E = E'$, a contradiction. Therefore, $\mathcal{A}(r,k)$ is an $(n,r,2)$-system. □

The next proposition shows that in order to prove Theorem 5 it suffices to find an explicit construction of an $(n,6,2)$-system with independence number $O(n^{1-\epsilon})$.

Proposition 9. *Suppose that there exists an (n,r,s)-system with independence number at most α. Then there exists an (n,r',s)-system with independence number at most α for every integer $r' \in [s+1, r]$.*

Proof. Let $\mathcal{H}$ be an (n,r,s)-system with independence number at most α. Let $V = V(\mathcal{H})$. Fix an integer $r' \in [s+1, r]$. Let the r'-graph $\mathcal{H}'$ be obtained from $\mathcal{H}$ in the following way: for every edge $E \in \mathcal{H}$ replace it by an arbitrary r'-set $E' \subset E$. It is clear that $\mathcal{H}'$ is an r'-graph on V. Now suppose that $S \subset V$ is a set of size strictly greater than α. Then, by assumption, there exists an edge $E \in \mathcal{H}$ such that $E \subset S$. It follows from the definition of $\mathcal{H}'$ that there exists $E' \in \mathcal{H}$ such that $E' \subset E \subset S$. So, S is not an independent set in $\mathcal{H}'$, which implies that $\alpha(\mathcal{H}') \leqslant \alpha$. □

Another ingredient we need for the proof of Theorem 5 is the following result due to Pach and Palincza [11].

Theorem 10 (Pach–Palincza [11]). *Suppose that k is a sufficiently large integer. Then every set of $\mathbb{Z}_6^k$ of size greater than $(5.709)^k$ contains a 6-AP.*

Now we are ready to prove Theorem 5.

Proof of Theorem 5. By Proposition 9, it suffices to prove that there exists an $(n,6,2)$-system $\mathcal{H}$ with $\alpha(\mathcal{H}) = O(n^{0.973})$.

First, for all integers n of the form 6^k we let the construction be $\mathcal{H} = \mathcal{A}(6,k)$. It follows from Proposition 8 that $\mathcal{H}$ is an $(n,6,2)$-system. On the other hand, it follows from the definition of $\mathcal{A}(6,k)$ that a set $S \subset V$ is independent in $\mathcal{A}(6,k)$ iff it does not contain a 6-AP. So, by Theorem 10, $|S| \leqslant (5.709)^k$. Therefore, $\alpha(\mathcal{H}) \leqslant (5.709)^k \leqslant n^{0.973}$.

Now suppose that n is not of the form 6^k. Then let k be the smallest integer such that $n \leqslant 6^k$. Let $\mathcal{H}$ be any n-vertex induced subgraph of $\mathcal{A}(6,k)$. Then $\alpha(\mathcal{H}) \leqslant \alpha(\mathcal{A}(6,k)) \leqslant (5.709)^k \leqslant 6n^{0.973}$. □

2.2 Proof of Theorem 6

Given two hypergraphs $\mathcal{H}_1$ and $\mathcal{H}_2$, the *direct product* of $\mathcal{H}_1$ and $\mathcal{H}_2$, denoted by $\mathcal{H}_1 \square \mathcal{H}_2$, is the hypergraph on $V(\mathcal{H}_1) \times V(\mathcal{H}_2)$ with edge set

$$\{E_1 \times E_2 \colon E_1 \in \mathcal{H}_1 \text{ and } E_2 \in \mathcal{H}_2\},$$

where $\times$ denotes the usual cartesian product of sets.

Remark. It is clear that there exists an algorithm $\mathcal{A}'$ such that for every input $(\mathcal{H}_1, \mathcal{H}_2)$, $\mathcal{A}'$ runs in time $\operatorname{poly}(|\mathcal{H}_1| \cdot |\mathcal{H}_2|)$ and outputs $\mathcal{H}_1 \square \mathcal{H}_2$.

One nice property of the operation defined above is that the direct product of two designs is still a design.

Lemma 11. *Suppose that $\mathcal{H}_1$ is an (n_1, r_1, s_1)-system and $\mathcal{H}_2$ is an (n_2, r_2, s_2)-system. Then $\mathcal{H}_1 \square \mathcal{H}_2$ is an $(n_1 n_2, r_1 r_2, \max\{r_1(s_2-1)+1, r_2(s_1-1)+1\})$-system.*

Proof. Let $n = n_1 n_2$, $r = r_1 r_2$, and $s = \max\{r_1(s_2-1)+1, r_2(s_1-1)+1\}$. It is clear that $\mathcal{H}_1 \square \mathcal{H}_2$ is an r-graph on n vertices. So it suffices to show that every s-set of $V(\mathcal{H}_1) \times V(\mathcal{H}_2)$ is contained in at most one edge in $\mathcal{H}_1 \square \mathcal{H}_2$.

Fix an s-set $S \subset V(\mathcal{H}_1) \times V(\mathcal{H}_2)$. Suppose to the contrary that there exist two distinct edges $E, E' \in \mathcal{H}_1 \square \mathcal{H}_2$ such that $S \subset E \cap E'$. Assume that $E = E_1 \times E_2$ and $E' = E_1' \times E_2'$, where $E_1, E_1' \in \mathcal{H}_1$, $E_2, E_2' \in \mathcal{H}_2$, and $(E_1, E_2) \neq (E_1', E_2')$. Since $E \cap E' = (E_1 \cap E_1') \times (E_2 \cap E_2')$, we have $|E \cap E'| = |E_1 \cap E_1'| \times |E_2 \cap E_2'|$. On the other hand, since $(E_1, E_2) \neq (E_1', E_2')$, we have either $E_1 \neq E_1'$ or $E_2 \neq E_2'$. In the former case we have $|E \cap E'| = |E_1 \cap E_1'| \times |E_2 \cap E_2'| \leqslant r_2(s_1 - 1) < s$, and in the latter case we have $|E \cap E'| = |E_1 \cap E_1'| \times |E_2 \cap E_2'| \leqslant r_1(s_2 - 1) < s$, both contradict the assumption that $S \subset E \cap E'$ and $|S| = s$. $\square$

Using Lemma 11 we obtain the following corollary.

Corollary 12. *Let $(\ell_1, \ell_2, \ell_3, \ell_4) \in \mathbb{N}^4$, $s = 3^{\ell_1} 4^{\ell_2} 5^{\ell_3} 6^{\ell_4} + 1$, $m \in \mathbb{N}$, $m_{i,j} \in \mathbb{N}$ for $i \in [\ell_j]$ and $j \in [4]$, and $M = m \prod_{j=1}^{4} \prod_{i=1}^{\ell_j} m_{i,j}$. Suppose that $\mathcal{H}_{i,j}$ is an $(m_{i,j}, 3, 2)$-system for $i \in [\ell_j]$ and $j \in [4]$, and $\mathcal{G} = \square_{j=1}^{4} \square_{i=1}^{\ell_j} \mathcal{H}_{i,j}$. Then the following hold.*

(1) Suppose that $\ell_1 \neq 0$ and $\mathcal{H}$ is an $(m, 3, 2)$-system. Then $\mathcal{H} \square \mathcal{G}$ is an $(M, 3(s-1), s)$-system.

(2) Suppose that $\ell_1 = 0$, $\ell_2 \neq 0$, and $\mathcal{H}$ is an $(m, 4, 2)$-system. Then $\mathcal{H} \square \mathcal{G}$ is an $(M, 4(s-1), s)$-system.

(3) Suppose that $\ell_1 = \ell_2 = 0$, $\ell_3 \neq 0$, and $\mathcal{H}$ is an $(m, 5, 2)$-system. Then $\mathcal{H} \square \mathcal{G}$ is an $(M, 4(s-1), s)$-system.

(4) Suppose that $\ell_1 = \ell_2 = \ell_3 = 0$, $\ell_4 \neq 0$, and $\mathcal{H}$ is an $(m, 6, 2)$-system. Then $\mathcal{H} \square \mathcal{G}$ is an $(M, 6(s-1), s)$-system.

The proof of Corollary 12 requires some simple but tedious calculations and we omit it here. Corollary 12 explains the reason we define $R(s)$ in the first section.

Next, we will show that the independence number of the direct product of two hypergraphs with small independence number is still relatively small. To prove this we will use the following bipartite version of the Dependent random choice lemma. Its proof is basically the same as proofs in [7, 9, 1, 16], and for the sake of completeness we include it here.

For a graph G and a set $T \subset V(G)$ we use $N(T)$ to denote the common neighbors of T in G.

Lemma 13 (Dependent random choice, see [7, 9, 1, 16]). *Let a, m, n_1, n_2, r be positive integers and $d_1 \geqslant 0$ be a real number. Let $G = G[V_1, V_2]$ be a bipartite graph with $|V_1| = n_1$, $|V_2| = n_2$, and $|G| \geqslant d_1 n_1$. If there exists a positive integer t such that*

$$\frac{n_1 d_1^t}{n_2^t} - \binom{n_1}{r}\left(\frac{m}{n_2}\right)^t \geqslant a.$$

Then there exists a subset $U \subset V(G)$ of size at least a such that every set of r vertices in U has at least m common neighbors.

Proof. Pick a set T of t vertices from V_2 uniformly at random with repetition. Set $A = N(T) \subset V_1$ and let X denote the cardinality of A. By the linearity of expectation,

$$\mathbb{E}[X] = \sum_{v \in V_1}\left(\frac{|N(v)|}{n_2}\right)^t = n_2^{-t}\sum_{v \in V_1}|N(v)|^t \geqslant n_2^{-t} n_1 \left(\frac{\sum_{v \in V_1}|N(v)|}{n_1}\right)^t \geqslant \frac{n_1 d_1^t}{n_2^t}.$$

Let Y be the random variable counting the number of subsets $S \subset A$ of size r with fewer than m common neighbors. For a given such subset S the probability that it is a subset of A equals $\left(\frac{|N(S)|}{n_2}\right)^t$. Since there are at most $\binom{n_1}{r}$ subsets $S \subset V_1$ of size r for which $|N(S)| < m$, it follows that

$$\mathbb{E}[Y] \leqslant \binom{n_1}{r}\left(\frac{m}{n_2}\right)^t.$$

By the linearity of expectation,

$$\mathbb{E}[X - Y] \geqslant \frac{n_1 d_1^t}{n_2^t} - \binom{n_1}{r}\left(\frac{m}{n_2}\right)^t \geqslant a.$$

Hence there exists a choice of T for which the corresponding set $A = N(T)$ satisfies $X - Y \geqslant a$. Deleting one vertex from each subset S of A of size r with fewer than m common neighbors. We let U be the remaining subset of A. The set U has at least $X - Y \geqslant a$ vertices and all subsets of size r have at least m common neighbors. $\square$

The following lemma gives an upper bound for the independence number of the direct product of two hypergraphs.

Lemma 14. *Suppose that $\mathcal{H}_1$ is an r_1-graph on n_1 vertices with $\alpha(\mathcal{H}_1) < n_1/f(n_1)$ and $\mathcal{H}_2$ is an r_2-graph on n_2 vertices with $\alpha(\mathcal{H}_2) < n_2/g(n_2)$ for some real numbers $f(n_1), g(n_2) \geqslant 1$. Then $\mathcal{H}_1 \Box \mathcal{H}_2$ is an r_1r_2-graph on n_1n_2 vertices with $\alpha(\mathcal{H}_1 \Box \mathcal{H}_2) < n_1n_2/h(n_1, n_2)$, where $h(n_1, n_2) = (f(n_1)/2)^{1/t}$ and $t = \left\lceil \frac{\log\left(n_1^{r_1-1} f(n_1)/r_1!\right)}{\log g(n_2)} \right\rceil$.*

Proof. Let $f = f(n_1)$, $g = g(n_2)$, $t = \lceil \frac{\log\left(n_1^{r_1-1} f/r_1!\right)}{\log g} \rceil$, $h = h(n_1, n_2) = (f/2)^{1/t}$, $d_1 = n_2/h$, $m = n_2/g$, and $a = n_1/f$. Let $S \subset V(\mathcal{H}_1) \times V(\mathcal{H}_2)$ be a set of size $d_1 n_1 = n_1 n_2/h$. Define an auxiliary bipartite graph $G = G[V_1, V_2]$ with $V_1 = V(\mathcal{H}_1)$ and $V_2 = V(\mathcal{H}_2)$, and $u \in V_1$, $v \in V_2$ are adjacent iff $(u, v) \in S$. Since

$$\begin{aligned}\frac{n_1 d_1^t}{n_2^t} - \binom{n_1}{r_1}\left(\frac{m}{n_2}\right)^t - a &\geqslant \frac{n_1}{h^t} - \frac{n_1^{r_1}}{r_1!}\frac{1}{g^t} - \frac{n_1}{f} \\ &= n_1\left(\frac{2}{f} - \frac{n_1^{r_1-1}}{r_1!}\frac{1}{g^t} - \frac{1}{f}\right) \geqslant n_1\left(\frac{2}{f} - \frac{1}{f} - \frac{1}{f}\right) = 0,\end{aligned}$$

it follows from Lemma 13 that there exists a set $U \subset V_1$ of size n_1/f such that every r_1-subset of U has at least n_2/g common neighbors. Since $\alpha(\mathcal{H}_1) < n_1/f$, there exists an r_1-subset $E_1 \subset U$ such that $E_1 \in \mathcal{H}_1$. Let $W = N(E_1)$. Since $|W| \geqslant n_2/g > \alpha(\mathcal{H}_2)$, there exists an r_2-subset $E_2 \subset W$ such that $E_2 \in \mathcal{H}_2$. Since every pair $\{u, v\}$ with $u \in E_1$ and $v \in E_2$ is an edge in G, the set $E_1 \times E_2$ is contained in S. This implies that S is not an independent set in $\mathcal{H}_1 \Box \mathcal{H}_2$ as it contains the edge $E_1 \times E_2 \in \mathcal{H}_1 \Box \mathcal{H}_2$. Therefore, $\alpha(\mathcal{H}_1 \Box \mathcal{H}_2) < n_1n_2/h$. $\square$

Now we are ready to prove Theorem 6. As indicated by Corollary 12 our construction will be the direct product of some $(m_i, 3, 2)$-systems, $(m_j, 4, 2)$-systems, $(m_k, 5, 2)$-systems, and $(m_\ell, 6, 2)$-systems depending on the value of $\ell_1, \ell_2, \ell_3, \ell_4$, where the choice of integers m_i, m_j, m_k, m_ℓ can be optimized so that the independence number of the resulting construction is as small as possible. In the following proof we will use an inductive argument to show that this construction has small independence number. In order to keep the argument simple, we will not try to optimize the choice of integers m_i, m_j, m_k, m_ℓ.

Proof of Theorem 6. We prove this theorem by induction on $\sum_{i\in[4]} \ell_i$. Theorem 5 shows that the base case $\sum_{i\in[4]} \ell_i = 0$ holds, so we may assume that $\sum_{i\in[4]} \ell_i \geqslant 1$. Let $s = 3^{\ell_1}4^{\ell_2}5^{\ell_3}6^{\ell_4} + 1$, and let us assume, for the sake of simplicity, that $\ell_1 \geqslant 1$ (the other cases can be proved using a similar argument). By Proposition 9 it suffices to show there is an explicit construction of an $(n, R(s), s)$-system with independence number $O(n^{1-\epsilon})$.

Fix n and let $m = \lceil \sqrt{n} \rceil$, $s_1 = 3^{\ell_1 - 1}4^{\ell_2}5^{\ell_3}6^{\ell_4} + 1$, $r_1 = 3(s_1 - 1)$. By the induction hypothesis, there exists an explicit construction $\mathcal{H}_1$ of an (m, r_1, s_1)-system with $\alpha(\mathcal{H}_1) \leqslant C_1 m^{1-\epsilon_1}$, where $C_1 > 0$ and $\epsilon_1 > 0$ are constants only related to r_1 and s_1. On the other hand, by Theorem 5, there exists an explicit construction $\mathcal{H}_2$ of an $(m, 3, 2)$-system with $\alpha(\mathcal{H}_2) \leqslant C_2 m^{1-\epsilon_2}$, where $C_2 > 0$ and $\epsilon_2 > 0$ are absolute constants. Let $C = C(C_1, C_2, \epsilon_1, \epsilon_2) > 0$ be a sufficiently large constant, $\epsilon = \epsilon(C_1, C_2, \epsilon_1, \epsilon_2) > 0$ be a sufficiently small constant (C and ϵ can be determined from the proof below), and let $\mathcal{H}_3 = \mathcal{H}_1 \square \mathcal{H}_2$. Then by Lemma 11, $\mathcal{H}_3$ is an $(m^2, 3(s-1), s)$-system. Applying Lemma 14 to $\mathcal{H}_3$ with $f(m) = m^{\epsilon_1}/C_1$, $g(m) = m^{\epsilon_2}/C_2$ we obtain $t = \lceil \frac{\log(r_1! C_1)}{\log C_2} \frac{r_1 - 1 + \epsilon_1}{\epsilon_2} \rceil$, $h(m,m) = (m^{\epsilon_1}/2C_1)^{1/t}$, and $\alpha(\mathcal{H}_3) \leqslant m^2/h(m,m) \leqslant Cn^{1-\epsilon}$ (we can choose $C > 0$ to be sufficiently large and $\epsilon > 0$ to be sufficiently small such that the last inequality holds for all integers n). Finally, to obtain an explicit construction of an $(n, 3(s-1), s)$-system with independent number at most $Cn^{1-\epsilon}$ one just needs to take any n-vertex induced subgraph of $\mathcal{H}_3$. $\square$

Remark. As we mentioned before, one could change the number of vertices in each design in the proof above to get a better bound. For example, for $(\ell_1, \ell_2, \ell_3, \ell_4) = (2, 0, 0, 0)$, Theorem 3 with our proof above gives an $(n, 27, 10)$-design with independence number $O(n^{1-\epsilon})$, where $\epsilon \approx 6.8732 \times 10^{-6}$. On the other hand, if we take the direct production of three copies of $(\lceil n^{1/3} \rceil, 3, 2)$-systems with independence number $O(n^{0.9228 \times 1/3})$, we obtain an $(n, 27, 10)$-design with independence number $O(n^{1-\epsilon'})$, where $\epsilon' \approx 3.5396 \times 10^{-5}$.

3 $(n, 5, 4)$-systems

We prove Theorem 7 in this section. We will show how to construct an $(n, 5, 4)$-system with small independence number inductively. More specifically, assuming that we have an $(m, 5, 4)$-system $\mathcal{H}$ with small independence number, we will construct a $(3m, 5, 4)$-system $\mathcal{H}'$ with small independence number by first taking three disjoint copies of $\mathcal{H}$, then embedding the vertex set of each copy of $\mathcal{H}$ into some finite field, and finally adding some crossing edges that satisfy a particular equation. The set of crossing edges we add will be sparse enough to make sure the resulting construction is a $(3m, 5, 4)$-system, but dense enough to make sure the resulting construction has small independence number.

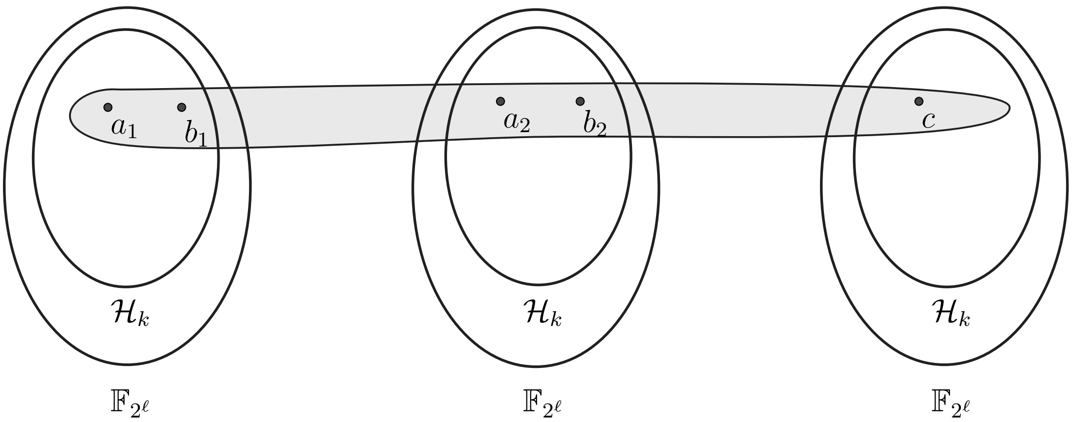

Figure 1: The induction step for constructing $\mathcal{H}_{k+1}$ using $\mathcal{H}_k$.

Proof of Theorem 7. We will show that it suffices to choose $C = 21$. Similar to the proof of Theorem 5 it suffices to show an explicit construction of an $(n, 5, 4)$-system with independence number at most $7n^{\log_3 2} - \frac{\sqrt{2}}{2-\sqrt{3}}n^{1/2}$ (this is slightly stronger that what we need) for all integers n of the form 3^k, and we will prove it by induction on k.

For $k \leqslant 3$ we have $7\left(3^k\right)^{\log_3 2} - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2} \geqslant 3^k$, so we may assume that $k \geqslant 4$ and focus on the induction step. Fix an integer k and let $\mathcal{H}_k$ be a $(3^k, 5, 4)$-system with $\alpha(\mathcal{H}_k) \leqslant 7\left(3^k\right)^{\log_3 2} - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2} = 7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}$. Let $\ell \in \mathbb{N}$ such that $2^\ell \geqslant 3^k > 2^{\ell-1}$. Let U_1, U_2, U_3 be three pairwise disjoint copies of $\mathbb{F}_{2^\ell} \setminus \{0\}$, where $\mathbb{F}_{2^\ell}$[1] is the finite field of order 2^ℓ with characteristic 2. For $i \in [3]$ let $\psi_i \colon V(\mathcal{H}_k) \to U_i$ be an injection and let $V_i = \psi_i(V(\mathcal{H}_k))$. Let $\mathcal{H}_{k+1}$ be the 5-graph on $V = V_1 \cup V_2 \cup V_3$ whose edge set is (see Figure 1)

$$\mathcal{H}_{k+1} = \left\{\{a_1, b_1, a_2, b_2, c\} \in \binom{V}{5} : a_1, b_1 \in V_1, a_2, b_2 \in V_2, c \in V_3, a_1 + b_1 \cdot c = a_2 + b_2 \cdot c\right\} \cup \left(\bigcup_{i \in [3]} \psi_i\left(\mathcal{H}_k\right)\right).$$

Claim 15. *$\mathcal{H}_{k+1}$ is a $(3^{k+1}, 5, 4)$-system.*

Proof. Let $S = \{a, b, c, d\} \subset V_1 \cup V_2 \cup V_3$ be a set of size 4. It is clear that if $|S \cap V_i| \geqslant 3$ for some $i \in [3]$ or $|S \cap V_3| \geqslant 2$, then S can be contained in at most one edge of $\mathcal{H}_{k+1}$. So we may assume that $|S \cap V_1|, |S \cap V_2| \leqslant 2$ and $|S \cap V_3| \leqslant 1$.

Suppose that $|S \cap V_1| = |S \cap V_2| = 2$, and without loss of generality we may assume that $S \cap V_1 = \{a, b\}$ and $S \cap V_2 = \{c, d\}$. By the definition of $\mathcal{H}_{k+1}$, every vertex $e \in V_3$ that satisfies $\{a, b, c, d, e\} \in \mathcal{H}_{k+1}$ must satisfy $a + c \cdot e = b + d \cdot e$ or $a + d \cdot e = d + c \cdot e$. Since both equations yield $e = \frac{a+b}{c+d}$ (here we used the fact that $x - y = x + y$ holds for all $x, y \in \mathbb{F}_{2^\ell}$), such vertex e is unique. Therefore, S is contained in at most one edge in $\mathcal{H}_{k+1}$.

Suppose that $|S \cap V_1| = 2$ and $|S \cap V_2| = |S \cap V_3| = 1$. Without loss of generality we may assume that $S \cap V_1 = \{a, b\}$, $S \cap V_2 = \{c\}$, and $S \cap V_3 = \{d\}$. It is easy to see that every vertex $e \in V$ that satisfies $\{a, b, c, d, e\} \in \mathcal{H}_{k+1}$ must satisfy

- $e \in V_2$, and
- $a + c \cdot d = b + e \cdot d$ or $a + e \cdot d = b + c \cdot d$.

Since both $a + c \cdot d = b + e \cdot d$ and $a + e \cdot d = b + c \cdot d$ imply $e = \frac{a+b}{d} + c$ (here we used the fact that $x - y = x + y$ holds for all $x, y \in \mathbb{F}_{2^\ell}$ again), such vertex e is unique. Therefore, S is contained in at most one edge in $\mathcal{H}_{k+1}$.

By symmetry, for the other cases one can show that S is contained in at most one edge in $\mathcal{H}_{k+1}$. Therefore, $\mathcal{H}_{k+1}$ is a $(3^{k+1}, 5, 4)$-system. $\square$

Claim 16. $\alpha(\mathcal{H}_{k+1}) \leqslant 2\left(7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}\right) + \sqrt{2} \cdot 3^{k/2}$.

[1]It is clear that $\mathbb{F}_{2^\ell}$ can be constructed in time poly(2^ℓ) for every integer $\ell \geqslant 1$.

Proof. Suppose to the contrary that there exists an independent set $S \subset V$ of size greater than $2\left(7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}\right) + \sqrt{2} \cdot 3^{k/2}$. Let $S_i = S \cap V_i$ and $s_i = |S_i|$ for $i \in [3]$. Since S is independent in $\mathcal{H}_{k+1}$, S_i must be independent in $\psi_i(\mathcal{H}_k)$. Therefore, $s_i \leqslant \alpha(\mathcal{H}_k) \leqslant 7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}$ for $i \in [3]$ and consequently, $s_i > \sqrt{2} \cdot 3^{k/2}$ for $i \in [3]$. Moreover, we have $s_1 + s_2 > 7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2} + \sqrt{2} \cdot 3^{k/2}$ and hence,

$$s_1 \cdot s_2 > \left(7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}\right) \cdot \sqrt{2} \cdot 3^{k/2} \geqslant \sqrt{2}\left(7 - \frac{\sqrt{2}}{2-\sqrt{3}}\right) \cdot 2^k \cdot 3^{k/2} \geqslant 2 \cdot 3^k \geqslant 2^\ell.$$

Fix $z \in S_3$. Since $s_1 s_2 > 2^\ell$, by the Pigeonhole principle, there exists distinct elements $(a_1, b_1), (a_2, b_2) \in S_1 \times S_2$ such that $a_1 + b_1 \cdot z = a_2 + b_2 \cdot z$. It is easy to see that $a_1 \neq a_2$ and $b_1 \neq b_2$ since otherwise the equation $a_1 + b_1 \cdot z = a_2 + b_2 \cdot z$ would imply $(a_1, b_1) = (a_2, b_2)$, a contradiction. Therefore, $|\{a_1, a_2, b_1, b_2, z\}| = 5$ and hence, $\{a_1, a_2, b_1, b_2, z\} \in \mathcal{H}_{k+1}$. However, this implies that S contains an edge in $\mathcal{H}_{k+1}$, a contradiction. $\square$

Remark. We may assume that $\alpha(\mathcal{H}_k) = \left\lceil 7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2} \right\rceil$ by removing some edges from $\mathcal{H}_k$ if necessary. If we let $n = 3^{k+1}$ and use $f(3^k)$ to denote the independence number of $\mathcal{H}_k$ for $k \in \mathbb{N}$. Then Claim 16 can be rewritten as

$$f(n) \leqslant 2f(n/3) + \sqrt{2/3}\sqrt{n}.$$

By the master theorem, we have $f(n) = O(n^{\log_3 2})$. This explains the $\log_3 2$ in the exponent.

Claim 16 shows that

$$\alpha(\mathcal{H}_{k+1}) \leqslant 2\left(7 \cdot 2^k - \frac{\sqrt{2}}{2-\sqrt{3}}3^{k/2}\right) + \sqrt{2} \cdot 3^{k/2} = 7 \cdot 2^{k+1} - \frac{\sqrt{2}}{2-\sqrt{3}}3^{(k+1)/2}.$$

This completes the proof of the induction step.

Notice that given $\mathcal{H}_k$ the r-graph $\mathcal{H}_{k+1}$ can be constructed in time $\mathrm{poly}(|\mathcal{H}_k|) + \mathrm{poly}(2^\ell) = \mathrm{poly}(3^k)$. So for every integer $k \geqslant 1$ the r-graph $\mathcal{H}_k$ can be constructed in time $\mathrm{poly}(3^k)$. $\square$

Acknowledgements

We would like to thank the referees for their helpful comments and suggestions.

References

[1] N. Alon, M. Krivelevich, and B. Sudakov. Turán numbers of bipartite graphs and related Ramsey-type questions. *Combinatorics, Probability and Computing*, 12(5-6), 477-494. 2003.

[2] R. C. Bose and D. K. Ray–Chaudhuri. On a class of error correcting binary group codes. *Information and Control*, 3:68–79, 1960.

[3] E. Chattopadhyay and J. Goodman. Explicit extremal designs and applications to extractors. arXiv:2007.07772, 2020.

[4] E. Chattopadhyay, J. Goodman, V. Goyal, and X. Li. Extractors for adversarial sources via extremal hypergraphs. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 1184–1197, 2020.

[5] E. Croot, V. F. Lev, and P. P. Pach. Progression-free sets in $\mathbb{Z}_4^n$ are exponentially small. *Ann. of Math. (2)*, 185(1):331–337, 2017.

[6] J. S. Ellenberg and D. Gijswijt. On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression. *Ann. of Math. (2)*, 185(1):339–343, 2017.

[7] J. Fox and B. Sudakov. Dependent random choice. *Random Structures Algorithms*, 38(1-2):68–99, 2011.

[8] A. Hocquenghem. Codes correcteurs d'erreurs. *Chiffers*, 2:147–156, 1959.

[9] A. V. Kostochka and V. Rödl. On graphs with small Ramsey numbers. *J. Graph Theory*, 37(4):198–204, 2001.

[10] N. Nisan and A. Wigderson. Hardness vs. randomness. *J. Comput. System Sci.*, 49(2):149–167, 1994.

[11] P. P. Pach and R. Palincza. Sets avoiding six-term arithmetic progressions in $\mathbb{Z}_6^n$ are exponentially small. arXiv:2009.11897, 2020.

[12] R. Raz, O. Reingold, and S. Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. In *Annual ACM Symposium on Theory of Computing (Atlanta, GA, 1999)*, pages 149–158. ACM, New York, 1999.

[13] V. Rödl and E. Šiňajová. Note on independent sets in Steiner systems. In *Proceedings of the Fifth International Seminar on Random Graphs and Probabilistic Methods in Combinatorics and Computer Science (Poznań, 1991)*, volume 5, pages 183–190, 1994.

[14] A. Sidorenko. Extremal problems on the hypercube and the codegree Turán density of complete r-graphs. *SIAM J. Discrete Math.*, 32(4):2667–2674, 2018.

[15] A. Sidorenko. On generalized Erdős-Ginzburg-Ziv constants for $\mathbb{Z}_2^d$. *J. Combin. Theory Ser. A*, 174:105254, 20, 2020.

[16] B. Sudakov. A few remarks on Ramsey-Turán-type problems. *J. Combin. Theory Ser. B*, 88(1):99–106, 2003.

[17] L. Trevisan. Extractors and pseudorandom generators. *J. ACM*, 48(4):860–879, 2001.