COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 15 (2) (1995) 175–185

THE MINIMUM INDEPENDENCE NUMBER FOR DESIGNS

DAVID A. GRABLE, KEVIN T. PHELPS and VOJTĚCH RÖDL*

Received July 17, 1992
Revised May 3, 1994

For $t=2,3$ and $k \geq 2t-1$ we prove the existence of $t-(n,k,\lambda)$ designs with independence number $C_{\lambda,k}n^{(k-t)/(k-1)}(ln\ n)^{1/(k-1)}$. This is, up to the constant factor, the best possible.
Some other related results are considered.

1. Introduction

A $t-(n,k,\lambda)$ *design* is a pair $\mathcal{J}=(V,\mathcal{D})$ where V is an n-set and $\mathcal{D}$ is a multiset of k-subsets of V (called *blocks* or *lines* or *edges*) such that each t-subset of V is contained in exactly λ blocks of $\mathcal{D}$. In a *partial design*, each t-subset is contained in at most λ blocks. Designs and partial designs can be considered as a special class of uniform hypergraphs or as a generalization of finite geometries. In either case the concept of an independent set has been of considerable interest.

A set $S \subseteq V$ is *independent* in $\mathcal{J}=(V,\mathcal{D})$ if no block of $\mathcal{D}$ is contained in S. The *independence number* $\alpha(\mathcal{J})$ is the maximum cardinality of any independent set in $\mathcal{J}$. We are interested in establishing asymptotic bounds on the minimum independence number of all designs of order n with given parameters λ, k, and t. In order to establish an upper bound on this minimum independence number, it is necessary that such a design exist. For this and other reasons, we focus on the cases $t=2$ and $t=3$, although we will prove some of the lemmas for arbitrary t.

Our main theorem is

Theorem 1.1. *Let $t=2$ or $t=3$ and let $k \geq 2t-1$. There exists a constant c such that if q is a sufficiently large prime power and if there exists a $t-(q+t-2,k,\lambda)$ design then there exists a $t-(n,k,\lambda)$ design $\mathcal{J}$ with $n=q^2+t-2$ such that*

$$\alpha(\mathcal{J}) \leq cn^{(k-t)/(k-1)}(\ln n)^{1/(k-1)}.$$

Mathematics Subject Classification (1991): 05 B 05

* Supported by NSF Grant DMS-9011850

Moreover, c is no greater than $2\left(\frac{4\cdot k_{(t)}}{\lambda}\right)^{\frac{1}{k-1}}$.

For $t=2$, $2-(q,k,\lambda)$ designs always exist if q is sufficiently large and satisfies the obvious necessary conditions. Hence we have

Corollary 1.2. *There exist a constant c and infinitely many* $2-(n,k,\lambda)$ *designs* $\mathcal{J}$ *such that*

$$\alpha(\mathcal{J}) \le cn^{(k-2)/(k-1)}(\ln n)^{1/(k-1)}.$$

Moreover, c is no greater than $2\left(\frac{4k(k-1)}{\lambda}\right)^{\frac{1}{k-1}} < 10$.

Similarly, for $t=3$ and $k \ge 5$ infinite classes of designs exist (inversive planes are the obvious example) (cf. [1]).

On the other hand, it is straightforward to extend the lower bound on the independence number of every $\lambda = 1$ partial design (and hence of every $\lambda = 1$ design) given in [9] to arbitrary λ. We will therefore omit the proof of the following theorem:

Theorem 1.3. *Let t, k, and* λ *be positive integer constants with* $2 \le t < k$. *There exists a constant* c' *such that for n sufficiently large, every partial* $t-(n,k,\lambda)$ *design* $\mathcal{J}$ *has*

$$\alpha(\mathcal{J}) \ge c' n^{(k-t)/(k-1)}(\ln n)^{1/(k-1)}.$$

Similar upper and lower bounds are established in [2] and [8] for partial $2-(n,3,1)$ designs (partial Steiner triple systems). Tight bounds for the independence number of partial $t-(n,k,1)$ with $2 \le t < k$ were found in [9].

While our proof of Theorem 1.3 follows an approach similar to [2] and [9], the argument for finding good upper bounds, (i.e. existence of designs with small independence number) is quite different. The only upper bound previously known was for Steiner triple systems [2] and it was different by a multiplicative factor of $O(\sqrt{\ln n})$ from the best lower bound. As a consequence of Theorem 1.1, we have now, up to the multiplicative constant factor, the best upper bound for the independence number of Steiner triple systems.

Our construction is probabilistic, and in fact, similar to [2]. In this paper, however, we have found an improved way to estimate the size of the independence number. Unfortunately, our techniques do not apply to Steiner quadruple systems $(3-(n,4,\lambda)$ designs).

As another consequence, we establish upper and lower bounds on the minimum i-indepedence number $\alpha_i(\mathcal{J})$ of designs and partial designs $\mathcal{J}=(V,\mathcal{D})$. Briefly, a set $S \subseteq V$ is *i-independent* if $|L \cap S| \le i$ for all $L \in \mathcal{D}$. Note that a $(k-1)$-independent set is simply an independent set.

The concept of i-independence has been studied in finite geometries, primarily for $i=2$ where a 2-independent set is referred to as an *arc* or a *cap* (cf. [7]). It has been considered for hypergraphs as well (cf. [6]) but to a lesser extent and is a natural concept for designs. We establish the following bounds on the minimum i-independence number of designs and partial designs.

Corollary 1.4. *Let $t=2$ or $t=3$, let $i \geq 2t-2$, and $k>i$. There exists a constant c such that if q is a sufficiently large prime power and there exists a $t-(q+t-2,k,\lambda)$ design then there exists a $t-(n,k,\lambda)$ design $\mathcal{J}$ with $n=q^2+t-2$ such that*

$$\alpha_i(\mathcal{J}) \leq cn^{(i-t+1)/i}(\ln n)^{1/i}.$$

Corollary 1.5. *Let i, t, k, and λ be positive integer constants such that $2 \leq t \leq i < k$. There exists a constant c' such that for n sufficiently large, every partial $t-(n,k,\lambda)$ design $\mathcal{J}$ has*

$$\alpha_i(\mathcal{J}) \geq c'n^{(i-t+1)/i}(\ln n)^{1/i}.$$

We delay the proof of Corollary 1.4 until after the proof of Theorem 1.1 since there is some dependence, but prove Corollary 1.5 immediately. Given a partial $t-(n,k,\lambda)$ design $\mathcal{J}$, replace each block of $\mathcal{J}$ with a complete $(i+1)$-uniform hypergraph on k points to form a partial t–$(n,i+1,\lambda\binom{k-t}{i+1-t})$ design $\mathcal{J}'$. Theorem 1.3 implies that

$$\alpha(\mathcal{J}') \geq c'n^{(i-t+1)/i}(\ln n)^{1/i}$$

where c' is a constant depending only on i, t, k, and λ. One only need notice that $\alpha_i(\mathcal{J})=\alpha(\mathcal{J}')$ to see that the corollary is true.

As a final remark, by modifying the approach of [9], we can show that for $2 \leq t \leq i < k$ there exists a constant c such that, for n sufficiently large, there exists a partial $t-(n,k,1)$ design $\mathcal{J}$ with

$$\alpha_i(\mathcal{J}) \leq cn^{(i-t+1)/i}(\ln n)^{1/i}.$$

2. Proof of Theorem 1.3

In this section we wish to construct $t-(n,k,\lambda)$ designs with minimum independence number where λ, k, and t, are constant parameters and n is sufficiently large. We show how to do this at least for those parameters where the designs exist sufficiently often ($t=2$ or $t=3$; $k=p+1$, p a prime power). However, we will prove our main lemmas for arbitrary t.

First, recall that there are an infinite number of values of $q \equiv 1 \pmod{k(k-1)}$ where q is a prime power. For these values of q, there exist affine planes (2–$(q^2,q,1)$ designs) and, if q is sufficiently large, 2–(q,k,λ) designs. The standard technique of replacing each line in the affine plane independently with an arbitrary copy of the $2-(q,k,\lambda)$ design produces a $2-(q^2,k,\lambda)$ design. These systems behave randomly enough to establish a reasonable upper bound on the minimum independence number.

In a similar manner, there exist inversive planes (3–$(q^2+1,q+1,1)$ designs) and assuming that there exists a $3-(q+1,k,\lambda)$ design we can use the same technique to produce random $3-(q^2+1,k,\lambda)$ designs.

First, we need a lemma which establishes an upper bound on the number of independent sets of size z in an arbitrary t–(q,k,λ) design $\mathcal{J}$. Let $\alpha(\mathcal{J},z)$ denote this number. Throughout, we will work asymptotically and will require some standard notation. For functions f and g of q, we write $f=o(g)$ or $f \ll g$ when $\lim_{q\to\infty} f/g=0$.

Lemma 2.1. *For an arbitrary $t-(q,k,\lambda)$ system $\mathcal{J}$ and $1 \ll z \ll q^{\frac{k-t}{k}}$, we have*

$$\alpha(\mathcal{J},z) = \binom{q}{z}\left(1 - \frac{\lambda}{k(k-1)\dots(k-t+1)}\frac{z^k}{q^{k-t}}(1+o(1))\right).$$

Proof. The proof uses inclusion-exclusion to find upper and lower bounds on $\alpha(\mathcal{J},z)$ which are asymptotically equivalent. Let $b=\lambda\binom{q}{t}/\binom{k}{t}$ be the number of blocks in $\mathcal{J}$.

First a lower bound. The number of z-sets containing at least one block is at most $b\binom{q-k}{z-k}$. Therefore,

$$\begin{aligned}\alpha(\mathcal{J},z) \geq \binom{q}{z} - b\binom{q-k}{z-k} &= \binom{q}{z}\left(1 - b\frac{z^k}{q^k}(1+o(1))\right)\\ &= \binom{q}{z}\left(1 - \frac{\lambda}{k_{(t)}}\frac{z^k}{q^{k-t}}(1+o(1))\right).\end{aligned}$$

To find an upper bound, let p_i be the number of pairs of blocks of $\mathcal{J}$ which intersect in exactly i points, $0 \leq i \leq k$. Then the number of z-sets containing at least two blocks is at most

$$\sum_{i=0}^{k} p_i\binom{q-2k+i}{z-2k+i} = \binom{q}{z}(1+o(1))\sum_{i=0}^{k} p_i\frac{z^{2k-i}}{q^{2k-i}}. \tag{1}$$

We will prove that each term of the right-hand sum (and hence the entire sum) is asymptotically negligible compared to z^k/q^{k-t}.

For $0 \leq i \leq t$, it isn't too hard to see that

$$p_i \leq b\binom{k}{i}\binom{q-i}{t-i}(\lambda-1)/\binom{k-i}{t-i}2 = c_i q^{2t-i}(1+o(1))$$

for some constant c_i. This is the number of ways to pick the first edge multiplied by the number of ways to pick the i points to be shared, the number of ways to pick a t-set containing those i points, and the number of ways to pick another block containing that t-set. It is then divided by the number of ways to pick the t-set such that we obtain the same block and by 2 to compensate for the fact that we counted each pair twice. Therefore, the i^{th} term of (1) is asymptotically negligible compared to z^k/q^{k-t} as long as

$$z^{2k-i}q^{i-2k+2t-i} \ll z^k q^{t-k}.$$

This is true as long as $z \ll q^{\frac{k-t}{k-i}}$ and, in particular, as long as $z \ll q^{\frac{k-t}{k}}$.

In the case where $t+1 \leq i \leq k$, we see that

$$p_i \leq b\binom{k}{i}\lambda/2 = c_i q^t(1+o(1))$$

for some constant c_i. Thus, the i^{th} term of (1) is asymptotically negligible compared to z^k/q^{k-t} as long as

$$z^{2k-i}q^{i-2k+t} \ll z^k q^{t-k}.$$

This is true as long as $z \ll q$ and therefore as long as $z \ll q^{\frac{k-t}{k}}$.

The promised upper bound on $\alpha(\mathcal{J}, z)$ is then

$$\begin{aligned}\alpha(\mathcal{J}, z) &\leq \binom{q}{z} - b\binom{q-k}{z-k} + \sum_{i=0}^{k} p_i \binom{q-2k+i}{z-2k+i} \\ &= \binom{q}{z}\left(1 - \frac{\lambda}{k_{(t)}}\frac{z^k}{q^{k-t}}(1+o(1))\right)\end{aligned}$$

as long as $1 \ll z \ll q^{\frac{k-t}{k}}$. This proves the lemma. ∎

The next two lemmas are generalizations of results in [4] (related statements were considered in [3] and [5]).

Lemma 2.2. *For a complex number μ and a $v \times b$ 0-1 matrix A with constant row sum r such that any two rows have exactly s ones in common, the rows of the complex matrix*

$$B = (\mu+1)A - J$$

will be orthogonal if and only if

$$\mu = \frac{r - s \pm \sqrt{r^2 - sb}}{s}.$$

Proof. For any two rows b_i and b_j, $\langle b_i, b_j \rangle = \mu^2 s - 2\mu(r-s) + (b-2r+s)$ and this is zero if and only if μ is a root of the quadratic equation. ∎

Note that μ is real as long as $r^2 \geq sb$ which is true in all of the cases we will be concerned with.

Lemma 2.3. *For a $v \times b$ 0-1 matrix A with constant row sum r such that any two rows have exactly s ones in common ($r^2 \geq sb$) and for any $\alpha v \times \beta b$ submatrix of A with rows indexed by R and columns indexed by C, if we let*

$$\mathcal{X} = \left(\frac{\alpha v}{\beta b}\right)^{\frac{1}{2}} (\mu^2 r + b - r)^{\frac{1}{2}}$$

then

$$\frac{1}{\mu+1}(\alpha v - \mathcal{X}) \le \frac{1}{|C|}\sum_{L\in C} c_L \le \frac{1}{\mu+1}(\alpha v + \mathcal{X})$$

where c_L is the number of ones in column L of the submatrix and μ is as in the previous lemma. In particular, if $\mathcal{X} = o(\alpha v)$ then

$$\frac{1}{|C|}\sum_{L\in C} c_L = \frac{\alpha v}{\mu+1}(1+o(1)).$$

Proof. Let $B=(\mu+1)A-J$ and μ be as in the previous lemma so that the rows of B are orthogonal. Consider the submatrix of B whose rows are indexed by R and whose columns are indexed by C. Let $s_1, s_2, \dots, s_{\alpha v}$ be the rows of the submatrix of B and let $b_1, b_2, \dots, b_{\alpha v}$ be the corresponding rows of B.

Let

$$\xi = (\xi_1, \xi_2, \dots, \xi_{\beta b}) = \sum_{i=1}^{\alpha v} s_i.$$

First, the Cauchy-Swartz inequality gives that

$$\frac{1}{\beta b}\left(\sum_{j=1}^{\beta b} \xi_j\right)^2 \le \sum_{j=1}^{\beta b} \xi_j^2.$$

And then this is

$$\sum_{j=1}^{\beta b} \xi_j^2 = \|\xi\|^2 = \left\|\sum_{i=1}^{\alpha v} s_i\right\|^2 \le \left\|\sum_{i=1}^{\alpha v} b_i\right\|^2 = \sum_{i,j}\langle b_i, b_j\rangle.$$

But the rows of B are orthogonal so this is

$$\sum_{i,j}\langle b_i, b_j\rangle = \sum_{i=1}^{\alpha v}\|b_i\|^2 = \alpha v(\mu^2 r + b - r).$$

For a column $L\in C$, let c_L be the number of ones in column L of the submatrix and for a row $P\in R$, let r_P be the number of ones in row P of the submatrix. Note that $\sum_{L\in C} c_L = \sum_{P\in R} r_P$. Since,

$$\sum_{j=1}^{\beta b} \xi_j = (\mu+1)\sum_{L\in C} c_L - \alpha v \beta b,$$

we have that

$$\frac{1}{\beta b}\left((\mu+1)\sum_{L\in C} c_L - \alpha\beta v b\right)^2 \le \alpha v(\mu^2 r + b - r).$$

Letting

$$\mathcal{X} = \left(\frac{\alpha v}{\beta b}\right)^{\frac{1}{2}} (\mu^2 r + b - r)^{\frac{1}{2}}$$

we conclude that

$$\frac{1}{\mu+1}(\alpha v - \mathcal{X}) \leq \frac{1}{|C|}\sum_{L\in C} c_L \leq \frac{1}{\mu+1}(\alpha v + \mathcal{X}).$$

In particular, if $\mathcal{X} = o(\alpha v)$ then

$$\frac{1}{|C|}\sum_{L\in C} c_L = \frac{\alpha v}{\mu+1}(1+o(1)). \qquad \blacksquare$$

We note that a similar statement could be made concerning

$$\frac{1}{|R|}\sum_{P\in R} r_P.$$

We consider two examples which are the basis of our main theorem.

Example 1 Let A be the point-line incidence matrix of the affine plane of order q so that $v = q^2$, $b = q^2 + q$, $r = q + 1$, and $s = 1$. Then $\mu = q + \sqrt{q+1}$ and

$$\mathcal{X} = \left(\frac{\alpha}{\beta}\right)^{\frac{1}{2}} q^{\frac{3}{2}}(1+o(1)).$$

Assuming $\alpha\beta q \gg 1$ (that is, $\alpha\beta q \to \infty$ as $q \to \infty$), this implies that $\mathcal{X} = o(\alpha q^2)$. Thus we have,

$$\begin{aligned}\frac{1}{|C|}\sum_{L\in C} c_L &= \frac{1}{q+1+\sqrt{q+1}}\alpha q^2(1+o(1)) \\ &= \alpha q(1+o(1)).\end{aligned}$$

In this context, c_L, the number of ones in column L of the submatrix, is $|R\cap L|$.

Example 2 Let A be the point-line incidence matrix of an inversive plane of order q so that $v = q^2+1$, $b = q(q^2+1)$, $r = q^2 + q$, and $s = q+1$. Then

$$\mu = q - 1 + \left(\frac{q(q-1)}{q+1}\right)^{\frac{1}{2}}$$

and

$$\mathcal{X} = \left(\frac{\alpha}{\beta}\right)^{1/2} q^{3/2}(1+o(1)).$$

Thus, assuming that $\alpha\beta q \gg 1$, we have $\mathcal{X} = o(\alpha q^2) = o(\alpha v)$. Again we have

$$\frac{1}{|C|}\sum_{L\in C} c_L = \alpha q(1+o(1))$$

and again $c_L = |R\cap L|$.

We summarize these examples and Lemma 2.3 in the following corollary.

Corollary 2.4. *Let $(V,\mathcal{L})$ be an affine or inversive plane of order q, let $R \subseteq V$, let $C \subseteq \mathcal{L}$, let $\alpha = |R|/|V|$, and let $\beta = |C|/|\mathcal{L}|$. If $\alpha\beta q \gg 1$ then*

$$\frac{1}{|C|}\sum_{L\in C} c_L = \alpha q(1+o(1))$$

where $c_L = |R\cap L|$.

Now we are ready to complete the proof of Theorem 1.1. Recall that λ, k, and t are constants with $t=2$ or $t=3$ and $k \geq 2t-1$. We are given a $t-(q+t-2,k,\lambda)$ design $\mathcal{J}_t$ and wish to show that there exists a $t-(q^2+t-2,k,\lambda)$ design with low independence number.

Let $(V,\mathcal{L}_2)$ be an affine plane of order q and let $(V,\mathcal{L}_3)$ be an inversive plane of order q. Then $|\mathcal{L}_t| = q^t+q$ for $t=2,3$. Replace each line $L \in \mathcal{L}_t$ by a copy of $\mathcal{J}_t$. In this way we obtain at least

$$\left(\frac{q!}{|\mathrm{Aut}\,\mathcal{J}_t|}\right)^{q^t+q}$$

different $t-(n,k,\lambda)$ systems (where $n=q^2$ or q^2+1). Let the random variable $\mathcal{S}_t$ be a $\lambda-(n,k,t)$ design which takes on each of these systems with equal likelihood. We will show that the probability that

$$\alpha(\mathcal{S}_t) > cn^{\frac{k-t}{k-1}}(\ln n)^{\frac{1}{k-1}}$$

(where c is a constant to be determined later) is strictly less than one. This will prove the theorem.

Set

$$\alpha = cn^{-\frac{t-1}{k-1}}(\ln n)^{\frac{1}{k-1}}$$

and consider a fixed set $R \subseteq V$, with

$$|R| = \alpha n = cn^{\frac{k-t}{k-1}}(\ln n)^{\frac{1}{k-1}}.$$

Fix $\varepsilon > 0$ (say $\varepsilon = 1/2$) and let C_1 and C_2 be the subsets of lines $L \in \mathcal{L}_t$, such that $c_L = |R\cap L| > (1+\varepsilon)\alpha q$ and $c_L < (1-\varepsilon)\alpha q$, respectively. We will show that $|C_1| < \frac{1}{4}|\mathcal{L}_t|$ and that $|C_2| < \frac{1}{4}|\mathcal{L}_t|$. Indeed, if $|C_1| \geq \frac{1}{4}|\mathcal{L}_t|$ then we can apply Corollary 2.4 to arrive at a contradiction. As $\beta \geq 1/4$, we have

$$\alpha\beta q \geq \frac{c}{4}n^{-\frac{t-1}{k-1}}(\ln n)^{\frac{1}{k-1}}\sqrt{n} \gg 1$$

as long as $k \geq 2t-1$. (This last condition on k means that our proof misses the important class of designs with $t=3$ and $k=4$.) Corollary 2.4 therefore gives that

$$\frac{1}{|C_1|}\sum_{L\in C_1} c_L = \alpha q(1+o(1)).$$

When q is sufficiently large, this contradicts the fact that $c_L \geq (1+\varepsilon)\alpha q$ for each $L \in C_1$. Hence $|C_1| < \frac{1}{4}|\mathcal{L}_t|$. In a similar way one can show that $|C_2| < \frac{1}{4}|\mathcal{L}_t|$.

Set $C = \mathcal{L}_t \setminus (C_1 \cup C_2)$. Then for $L \in C$,

$$(1-\varepsilon)\alpha q < c_L < (1+\varepsilon)\alpha q.$$

Since

$$(1+\varepsilon)\alpha q \le \frac{3}{2} c n^{-\frac{t-1}{k-1}} (\ln n)^{\frac{1}{k-1}} \sqrt{n} \le \frac{3}{2} c n^{\frac{k-2t+1}{2k-2}} (\ln n)^{\frac{1}{k-1}}$$
$$\le \frac{3}{2} c (\ln n)^{\frac{1}{k-1}} q^{\frac{k-2t+1}{k-1}} \ll q^{\frac{k-t}{k}}$$

we can apply Lemma 2.1 and the fact that $c_L = |R \cap L| > (1-\varepsilon)\alpha q = \alpha q/2$ to obtain

$$\begin{aligned}
\Pr[R \cap L \text{ is independent in } \mathcal{S}_t] &= \Pr[R \cap L \text{ is independent in the copy of } \mathcal{J}_t \text{ on } L] \\
&= \frac{\alpha(\mathcal{J}_t, c_L)}{\binom{q}{c_L}} \\
&\le \left(1 - \frac{\lambda}{k(k-1)\dots(k-t+1)} \frac{c_L^k}{q^{k-t}} (1+o(1))\right) \\
&< \left(1 - \frac{\lambda}{k_{(t)} \cdot 2^k} \alpha^k q^t (1+o(1))\right).
\end{aligned}$$

Since the events "$R \cap L$ is independent in $\mathcal{S}_t$" for $L \in \mathcal{L}_t$ are mutually independent, we infer that

$$\begin{aligned}
\Pr[R \text{ is independent in } \mathcal{S}_t] &= \prod_{L \in \mathcal{L}_t} \Pr[R \cap L \text{ is independent in } \mathcal{S}_t] \\
&\le \prod_{L \in C} \Pr[R \cap L \text{ is independent in } \mathcal{S}_t] \\
&< \left(1 - \frac{\lambda}{k_{(t)} 2^k} \alpha^k q^t (1+o(1))\right)^{\frac{1}{2} q^t} \\
&< \exp\left(-\frac{1}{2} \frac{\lambda}{k_{(t)} 2^k} c^k n^{-\frac{k(t-1)}{k-1}} (\ln n)^{\frac{k}{k-1}} n^t (1+o(1))\right) \\
&= \exp\left(-\frac{1}{2} \frac{\lambda}{k_{(t)} 2^k} c^k n^{\frac{k-t}{k-1}} (\ln n)^{\frac{k}{k-1}} (1+o(1))\right).
\end{aligned}$$

But there are

$$\binom{n}{\alpha n} < n^{\alpha n} = \exp(\alpha n \ln n) = \exp(c n^{\frac{k-t}{k-1}} (\ln n)^{\frac{k}{k-1}})$$

choices of the set $R \subset V$, $|R| = \alpha n$ and thus,

$$\Pr[\alpha(\mathcal{S}_t) \ge \alpha n] < \sum_R \Pr[R \text{ is independent in } \mathcal{S}_t]$$

$$< \binom{n}{\alpha n} \exp\left(-\frac{1}{2}\frac{\lambda}{k_{(t)}2^k} c^k n^{\frac{k-t}{k-1}} (\ln n)^{\frac{k}{k-1}} (1+o(1))\right)$$

$$< \exp\left(\left(c - \frac{1}{2}\frac{\lambda}{k_{(t)}2^k} c^k\right) n^{\frac{k-t}{k-1}} (\ln n)^{\frac{k}{k-1}} (1+o(1))\right).$$

This is less than one for n sufficiently large provided that

$$c > 2\left(\frac{4 \cdot k_{(t)}}{\lambda}\right)^{\frac{1}{k-1}}.$$

For example, when $t=2$ and $k \geq 3$, $c=10$ will suffice for all k and λ. This completes the proof of Theorem 1.1 and Corollary 1.2.

It only remains to prove Corollary 1.4. We wish to prove that for $t=2$ or $t=3$ and $k > i \geq 2t-2$, there exists a constant c such that if q is a sufficiently large prime power and there exists a $t-(q+t-2,k,\lambda)$ design then there exists a $t-(n,k,\lambda)$ design $\mathcal{J}$ with $n=q^2+t-2$ such that

$$\alpha_i(\mathcal{J}) \leq cn^{(i-t+1)/i}(\ln n)^{1/i}.$$

Given a $t-(q+t-2,k,\lambda)$ design $\mathcal{K}$, replace each block of $\mathcal{K}$ with a complete $(i+1)$-uniform hypergraph on k points to form a $t-(q+t-2,i+1,\lambda\binom{k-t}{i-t+1})$ design $\mathcal{K}'$. Apply Theorem 1.1 to $\mathcal{K}'$ to obtain a $t-(n,i+1,\lambda\binom{k-t}{i-t+1})$ design $\mathcal{J}'$ with $n=q^2+t-2$ such that

$$\alpha(\mathcal{J}') \leq cn^{(i-t+1)/i}(\ln n)^{1/i}.$$

Since, in the proof of Theorem 1.1, we constructed $\mathcal{J}'$ from copies of $\mathcal{K}'$, we can replace each copy of $\mathcal{K}'$ in $\mathcal{J}'$ with a copy of $\mathcal{K}$ to form a $t-(n,k,\lambda)$ design $\mathcal{J}$. Lastly note that $\alpha_i(\mathcal{J})=\alpha(\mathcal{J}')$, which is bounded above as desired.

References

[1] T. Beth, D. Jungnickel, and H. Lenz: *Design Theory*, Cambridge University Press, Cambridge, 1986.

[2] M. de Brandes, and V. Rödl: Steiner triple systems with small maximal independent sets, *Ars Combinatoria* **17** (1984), 15–19.

[3] J. Brown, and V. Rödl: A Ramsey type problem concerning vertex colorings, *J. Comb. Theory, Series B* **52** (1991), 45–52.

[4] N. Eaton, and V. Rödl: A canonical Ramsey theorem, *Rand. Struc. Alg.* **3** (1992), 427–444.

[5] P. Frankl, V. Rödl, and R.M. Wilson: The number of submatrices of a given type in a Hadamard matrix and related results, *J. Comb. Theory, Series B* **44** (1988), 317–328.

[6] Z. Füredi: Maximal independent subsets in Steiner systems and in planar sets, *SIAM J. Disc. Math* **4** (1991), 196–199.

[7] J. W. P. Hirschfeld: *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[8] K. T. PHELPS, and V. RÖDL: Steiner triple systems with minimum independence number, *Ars Combinat.* **21** (1986), 167–172.

[9] V. RÖDL, and E. ŠIŇAJOVÁ: Note on independent sets in Steiner systems, *Random Structures and Algorithms* **5** (1994), 183–190.

David A. Grable

Department of Algebra,
Combinatorics, and Analysis
Auburn University
Auburn, AL 36849-5307 USA
dgrable@math.clemson.edu

persent address

Department of Mathematical Sciences,
Clemson University,
Clemson, SC 29634-1907,
USA

Kevin T. Phelps

Department of Algebra,
Combinatorics, and Analysis
Auburn University
Auburn, AL 36849-5307 USA
phelpkt@mail.auburn.edu

Vojtěch Rödl

Department of Mathematics and
Computer Science
Emory University Atlanta,
GA 30322 USA
rodl@mathcs.emory.edu