

# Upper bounds on the number of Steiner triple systems and 1-factorizations

Nathan Linial\*      Zur Luria†

## Abstract

Let  $STS(n)$  denote the number of Steiner triple systems on  $n$  vertices, and let  $F(n)$  denote the number of 1-factorizations of the complete graph on  $n$  vertices. We prove the following upper bounds.

$$STS(n) \leq \left( (1 + o(1)) \frac{n}{e^2} \right)^{\frac{n^2}{6}}$$

$$F(n) \leq \left( (1 + o(1)) \frac{n}{e^2} \right)^{\frac{n^2}{2}}.$$

Both bounds are conjectured to be sharp. Our main tool is the entropy method.

## 1 Introduction

A Steiner triple system on a vertex set  $V$  is a collection of triples  $T \subseteq \binom{V}{3}$  such that each pair of vertices is contained in exactly one triple from  $T$ . It is well known that a Steiner triple system (STS) on  $n \geq 1$  vertices exists if and only if  $n \equiv 1$  or  $3 \pmod{6}$ .

A 1-factorization of the complete graph on  $n$  vertices  $K_n$  is a partition of the edges of  $K_n$  into  $n - 1$  perfect matchings, or in other words, a proper edge coloring of  $K_n$  using  $n - 1$  colors. It is well known that a 1-factorization of  $K_n$  exists if and only if  $n$  is even.

---

\*Department of Computer Science, Hebrew University, Jerusalem 91904, Israel. e-mail: nati@cs.huji.ac.il . Supported by ISF and BSF grants.

†Department of Computer Science, Hebrew University, Jerusalem 91904, Israel. e-mail: zluria@cs.huji.ac.il .

It has been observed (e.g., [1]) that 1-factorizations and Steiner triple systems are special types of Latin squares. We view a Latin square as an  $n \times n \times n$  array  $A$  with 0–1 entries in which each *line* has exactly one element that equals 1. To see that this description of Latin squares is equivalent to the usual definition, we associate to the array  $A$  a matrix  $L$ , that is defined via  $L(i, j) = k$  where  $k$  is the unique index for which  $A(i, j, k) = 1$ . A 1-factorization is a Latin square  $A$  such that  $A(i, j, k) = 1 \Leftrightarrow A(j, i, k) = 1$  and  $A(i, i, n) = 1$  for all  $i$ . Thus,  $L$  is a symmetric matrix in which all diagonal terms equal  $n$ . A Steiner triple system is a Latin square  $A$  where  $A(i, j, k) = 1$  implies that  $A(\sigma(i), \sigma(j), \sigma(k)) = 1$  for every permutation  $\sigma \in S_3$  on  $i, j, k$ , and  $A(i, i, i) = 1$  for all  $i$ . This can also be expressed in terms of  $L$ , though it's a bit more complicated to formulate.

These relations suggest that there might be deeper analogies to reveal among Latin squares, STS's and 1-factorizations. Indeed, we have recently proved an asymptotic upper bound on the number of Latin hypercubes [6], and here we prove analogous statements for  $STS(n)$  and  $F(n)$ .

The best previously known estimates for the number of  $n$ -point Steiner triple systems are due to Richard Wilson [8].

$$\left(\frac{n}{e^2 3^{3/2}}\right)^{\frac{n^2}{6}} \leq STS(n) \leq \left(\frac{n}{e^{1/2}}\right)^{\frac{n^2}{6}}.$$

Wilson also conjectured that, in fact,  $STS(n) = \left((1 + o(1))\frac{n}{e^2}\right)^{\frac{n^2}{6}}$ . We show that this is an upper bound on the number of Steiner triple systems.

**Theorem 1.1.**

$$STS(n) \leq \left((1 + o(1))\frac{n}{e^2}\right)^{\frac{n^2}{6}}.$$

Even less was previously known concerning the number of 1-factorizations. Peter Cameron [2] showed that

$$F(n) = n^{\left(\frac{1}{2} + o(1)\right)n^2}.$$

We provide a significant improvement to the upper bound, where the uncertainty is moved from the exponent to the base of the expression.

**Theorem 1.2.**

$$F(n) \leq \left((1 + o(1))\frac{n}{e^2}\right)^{\frac{n^2}{2}}.$$

We conjecture that this bound actually holds with equality.

Our proofs are based on the entropy method, a useful tool for a variety of counting problems. The basic idea is this: In order to estimate the size of a finite set  $\mathcal{F}$ , we introduce a random variable  $X$  that is uniformly distributed on the elements of  $\mathcal{F}$ . Since  $H(X) = \log(|\mathcal{F}|)$ , bounds on  $H(X)$  readily translate into bounds on  $|\mathcal{F}|$ . The bounds we derive on  $H(X)$  are based on several elementary properties of the entropy function. Namely, if a random variable takes values in a finite set  $S$  then its entropy does not exceed  $\log |S|$  with equality iff the distribution is uniform over  $S$ . Also, if  $X$  can be expressed as  $X = (Y_1, \dots, Y_k)$ , then  $H(X) = \sum_j H(Y_j | Y_1, \dots, Y_{j-1})$ . We can view the expression  $X = (Y_1, \dots, Y_k)$  as a way of gradually revealing the value of the random variable  $X$ . It is a key ingredient of our proofs to randomly select the order  $\prec$  in which the  $Y_i$  are revealed and average over the resulting identities  $H(X) = \sum_j H(Y_j | Y_i \text{ s.t. } i \prec j)$ . Similar ideas can be found in the literature, but to the best of our knowledge this method of proof is mostly due to Radhakrishnan [7]. We deviate somewhat from the standard notation in that our logarithms are always natural, rather than binary. Formally, we should use the notation  $H_e$  for the entropy function, but to simplify matters, we stick to the standard notation  $H(X)$ . We refer the reader to [3] for a thorough discussion of entropy. For an example of the entropy method, see [7].

## 2 An upper bound on 1-factorizations

Let  $n$  be an even integer, and let  $X$  be a random, uniformly chosen 1-factorization of  $K_n$ . Define the random variable  $X_{i,j} = X_{j,i}$  to be the color of the edge  $\{i, j\}$  in  $X$ . In order to analyze these random variables we first select a random ordering, denoted  $\ll$ , of the vertices. Using the relation  $\ll$  we introduce next a random ordering  $\prec$  of the edges as follows: For each vertex  $v$  we choose a random ordering of  $E_v$ , the set of edges  $\{v, u\}$  where  $v \ll u$ . To define the ordering  $\prec$ , we scan the vertices in the order  $\ll$ . For each vertex  $v$ , we scan the edges  $\{u, v\} \in E_v$  in their chosen order. Our proof proceeds by successively revealing the colors of the edges, i.e. the values taken by the variables  $X_{i,j}$ , where the edges are exposed in the order  $\prec$ .

Given two vertices  $i \neq j$ , we are interested in the (random) number of colors which are available for the edge  $\{i, j\}$ , given the values taken by the  $\prec$ -preceding edges. We are unable to determine this number exactly. Rather

we define a random variable  $N_{i,j}$  that is an upper bound on this number. If  $j \ll i$ , then the variable  $X_{i,j}$  is determined by the preceding variable  $X_{j,i}$ , so in this case it is natural to define  $N_{i,j} = 1$ . We proceed to the more interesting case where  $i \ll j$ . Here are two reasons why some color may be unavailable for  $X_{i,j}$ . For every vertex  $t \ll i$  we already know the colors of the edges  $\{t, i\}$  and  $\{t, j\}$ , neither of which can be used for the edge  $\{i, j\}$ . The set of colors that are ruled out for this reason is denoted  $A_{i,j}$ . It is also possible that  $i \ll k$  and  $\{i, k\} \prec \{i, j\}$ , so that  $\{i, j\}$  cannot take the color  $X_{i,k}$ . The set of such colors is denoted  $B_{i,j}$ . Formally:

- $A_{i,j} := \{X_{t,i} | t \ll i\} \cup \{X_{t,j} | t \ll i\}$ .
- $B_{i,j} := \{X_{i,k} | i \ll k \text{ and } \{i, k\} \prec \{i, j\}\}$ .

The set of colors that are not ruled out for the first reason is denoted:

$$\mathcal{M}_{i,j} := [n-1] \setminus A_{i,j}$$

and those remaining after further forbidding colors due to the second reason:

$$\mathcal{N}_{i,j} := \mathcal{M}_{i,j} \setminus B_{i,j}.$$

As mentioned, we seek to define a random variable  $N_{i,j}$  that is an upper bound on the number of possible values for  $X_{i,j}$  given the  $\prec$ -previous edge colors. To this end we define  $N_{i,j}$  as the cardinality of  $\mathcal{N}_{i,j}$ . As it turns out, a cruder upper bound on the number of possible values for  $X_{i,j}$  is useful as well. Namely, one that takes into account only the colors of the edges involving vertices that  $\ll$ -precede  $i$ . This is accomplished by the random variable  $M_{i,j}$  which is defined as  $|\mathcal{M}_{i,j}|$ .

Fix an ordering  $\prec$ . We apply the chain rule for the entropy function and conclude that

$$\log(F(n)) = H(X) = \sum_{(i,j)} H(X_{i,j} | X_e : e \prec \{i, j\}) \leq \sum_{(i,j)} \mathbb{E}_X[\log(N_{i,j})].$$

Next we take the expectation with respect to the random choice of the order  $\prec$ .

$$\log(F(n)) \leq \mathbb{E}_{\prec} \left[ \sum_{(i,j)} \mathbb{E}_X[\log(N_{i,j})] \right] = \sum_{(i,j)} \mathbb{E}_X[\mathbb{E}_{\prec}[\log(N_{i,j})]].$$

Fix a 1-factorization  $X$  and a pair  $i \neq j$ . If  $j \ll i$ , then  $\log(N_{i,j}) = 0$ . The probability that  $i \ll j$  is  $\frac{1}{2}$ , so that

$$\log(F(n)) \leq \frac{1}{2} \sum_{(i,j)} \mathbb{E}_X[\mathbb{E}_{\prec|i \ll j}[\log(N_{i,j})]].$$

A natural approach is to bound the expectation  $\mathbb{E}_{\prec|i \ll j}[\log(M_{i,j})]$  using Jensen's inequality. As it turns out, this yields a somewhat weaker upper bound. Rather we argue as follows:

$$\begin{aligned} \mathbb{E}_{\prec|i \ll j}[\log(M_{i,j})] &= \mathbb{E}_{\ll|i \ll j}[\log(M_{i,j})] = \\ &\mathbb{E}_{p|i \ll j}[\mathbb{E}_{\ll|p, i \ll j}[\log(M_{i,j})]] \leq \mathbb{E}_{p|i \ll j}[\log(\mathbb{E}_{\ll|p, i \ll j}[M_{i,j}])] \end{aligned} \quad (1)$$

For the first equality note that  $\mathcal{M}_{i,j}$  depends only on the ordering  $\ll$ . Next we condition on  $p$ , the position of  $i$  in  $\ll$  and then, finally we resort to Jensen's inequality. In order to bound this expression it is necessary to understand the distribution of  $p$  and the expectation of  $M_{i,j}$  given  $p$ .

**Lemma 2.1.** *The probability that  $i$  occupies the  $p$ -th position in  $\ll$ , given that  $i \ll j$  is*

$$2 \frac{n-p}{n(n-1)}.$$

*Proof.* We are sampling uniformly from among the  $\frac{n!}{2}$  permutations in which  $i \ll j$ . To specify such a permutation in which  $i$  is in the  $p$ -th position, we must assign  $j$  to one of the  $n-p$  positions following  $i$ . There are  $(n-2)!$  ways to order remaining elements with a total of  $(n-p)(n-2)!$  such permutations. The conclusion follows.  $\square$

**Lemma 2.2.**  $\mathbb{E}_{\ll|p, i \ll j}[M_{i,j}] = 1 + \frac{(n-p-1)(n-p-2)}{(n-1)}$ .

*Proof.* Now we are sampling uniformly from among the  $(n-p)(n-2)!$  permutations in which  $i$  is in the  $p$ -th position and  $i \ll j$ . If  $X_{i,j} = s$ , then clearly the color  $s$  belongs to  $\mathcal{M}_{i,j}$ . This corresponds to the 1 term in the lemma. For any other color  $t \neq s$ , let  $a$  (resp.  $b$ ) be the unique vertex such that  $X_{i,a} = t$  (resp.  $X_{j,b} = t$ ). Clearly,  $t \in \mathcal{M}_{ij}$  iff  $i \ll a, b$ . But

$$\Pr(i \ll a, b | i \text{ is in position } p, i \ll j) = \frac{(n-p-1)(n-p-2)}{(n-1)(n-2)}.$$

There are  $n-2$  colors  $t \neq s$  and the conclusion follows.  $\square$

Using lemmas 2.1 and 2.2, we have

$$\begin{aligned}
& \mathbb{E}_{p|i \ll j}[\log(\mathbb{E}_{\ll|p, i \ll j}[M_{i,j}])] = \\
& \sum_{p=1}^{n-1} 2 \frac{n-p}{n(n-1)} \log\left(1 + \frac{(n-p-1)(n-p-2)}{(n-1)}\right) = \\
& = \frac{2}{n(n-1)} \sum_1^{n-2} r \log\left(1 + \frac{r(r-1)}{n-1}\right) = \\
& = \frac{2}{n^2} \sum_1^{n-1} r \log\left(1 + \frac{r(r-1)}{n-1}\right) + o(1) = \frac{2}{n^2} \sum_1^{n-1} r \log\left(\frac{r^2}{n}\right) + o(1).
\end{aligned}$$

The function  $r \log(\frac{r^2}{n})$  is unimodal, and its minimum is achieved at  $r = \frac{\sqrt{n}}{e}$ . Therefore

$$\sum_1^{n-1} r \log\left(\frac{r^2}{n}\right) \leq \int_0^n u \log\left(\frac{u^2}{n}\right) du + 2\frac{\sqrt{n}}{e}.$$

Thus,

$$\begin{aligned}
\mathbb{E}_{p|i \ll j}[\log(\mathbb{E}_{\ll|p, i \ll j}[M_{i,j}])] & \leq \frac{2}{n^2} \int_0^n u \log\left(\frac{u^2}{n}\right) du + o(1) \\
& \log n - 1 + o(1). \tag{2}
\end{aligned}$$

We next proceed to consider colors that are ruled out due to variables that correspond to edges in  $E_i$ . An edge  $\{i, k\}$  may rule out additional colors if  $X_{i,k} \in \mathcal{M}_{i,j}$ . There are  $M_{i,j} - 1$  such edges, one for each color in  $\mathcal{M}_{i,j} \setminus X_{i,j}$ . Consequently, we are only interested in counting such edges that  $\prec$ -precede  $\{i, j\}$ .

$$\begin{aligned}
& \mathbb{E}_{\prec|i \ll j}[\log(N_{i,j})] = \mathbb{E}_{\prec|M_{i,j}, i \ll j}[\log(N_{i,j})] = \\
& \sum_l \Pr(M_{i,j} = l) \mathbb{E}_{\prec|M_{i,j}=l, i \ll j}[\log(N_{i,j})] = \\
& \sum_l \Pr(M_{i,j} = l) \frac{\log(l!)}{l} = \sum_l \Pr(M_{i,j} = l) (\log l - 1 + o(1)) = \\
& \mathbb{E}_{\prec|i \ll j}[\log(M_{i,j})] - 1 + o(1) \leq \log n - 2 + o(1).
\end{aligned}$$

We used the fact that given  $M_{i,j} = m$ , the number  $N_{i,j}$  of possible values for the random variable  $X_{i,j}$  is uniformly distributed between 1 and  $m$ . In the final step we used Equations 1 and 2.

Consequently,

$$\log(F(n)) \leq \frac{1}{2} \sum_{(i,j)} (\log n - 2 + o(1)) = \binom{n}{2} (\log n - 2 + o(1))$$

which yields the bound  $F(n) \leq ((1 + o(1)) \frac{n}{e^2})^{\frac{n^2}{2}}$  as claimed.

### 3 An upper bound on the number of Steiner triple systems

The ideas here are similar, but the details are different.

Let  $X$  be a uniformly chosen random Steiner triple system on  $n$  vertices. Define  $X_{i,j} = X_{j,i}$  to be the unique vertex  $k$  such that  $\{i, j, k\}$  is a triple in  $X$ . As before, we define next a random ordering  $\ll$  on the vertices and a random ordering  $\prec$  of the edges.

Fix a Steiner triple system  $X$ , orderings  $\ll$  and  $\prec$  and a pair of vertices  $i \neq j$ . Let  $X_{i,j} = k$ . We want to define a random variable  $N_{i,j}$  that is an upper bound on the number of vertices that are available for  $X_{i,j}$ , given the values of the preceding variables. Let  $F_{i,j}$  denote the event that  $i \ll j, k$  and  $\{i, j\} \prec \{i, k\}$ . Clearly,  $\Pr(F_{i,j}) = \frac{1}{6}$ . If  $F_{i,j}$  doesn't occur, then  $X_{i,j}$  is uniquely determined by the preceding variables, so in this case we define  $N_{i,j}$  to be 1.

Let  $t \neq X_{i,j}$  be a vertex. We consider two classes of reasons for which  $t$  may be ruled out as the value of  $X_{i,j}$  given the previously revealed choices. The first is the union of the following three events:  $t \ll i$ ,  $X_{i,t} \ll i$  and  $X_{j,t} \ll i$ . Namely, the variables corresponding to vertices that  $\ll$ -precede  $i$  reveal a triple that includes  $t$  and either  $i$  or  $j$ , so that  $\{i, j, t\}$  cannot be a triple in  $X$ . The second possibility is the union of the events  $\{i, X_{i,t}\} \prec \{i, j\}$  and  $\{i, t\} \prec \{i, j\}$ , where the revealed triple  $\{i, t, X_{i,t}\}$  rules out the possibility that  $\{i, j, t\}$  is in  $X$ .

We define the set of vertices which are ruled out for  $X_{i,j}$  due to the first reason:

$$A_{i,j} := \{t \mid t \ll i \text{ or } X_{i,t} \ll i \text{ or } X_{j,t} \ll i\}.$$

Among the remaining vertices we consider those that are unavailable due to the second reason

$$B_{i,j} := \{t \notin A_{i,j} \mid \{i, t\} \prec \{i, j\} \text{ or } \{i, X_{i,t}\} \prec \{i, j\}\}.$$

Further,

$$\mathcal{M}_{i,j} := (V \setminus \{i, j\}) \setminus A_{i,j}.$$

$$\mathcal{N}_{i,j} := \mathcal{M}_{i,j} \setminus B_{i,j}.$$

As before we define  $N_{i,j}$  as the cardinality of  $\mathcal{N}_{i,j}$ . Also, let  $M_{i,j} := |\mathcal{M}_{i,j}|$ .

The random variable  $M_{i,j}$  gives an upper bound on the number of values that are still available for  $X_{i,j}$  given the values of the random variables that involve vertices that  $\ll$ -precede  $i$ . Likewise,  $N_{i,j}$  is an upper bound on the number of possible values for  $X_{i,j}$  when all  $\prec$ -preceding choices are known.

For a given ordering  $\prec$  we derive:

$$\log(STS(n)) = H(X) = \sum_{(i,j)} H(X_{i,j} \mid X_e : e \prec \{i, j\}) \leq \sum_{(i,j)} \mathbb{E}_X[\log(N_{i,j})].$$

We take the expectation over the random choice of  $\prec$  to obtain

$$\log(STS(n)) \leq \sum_{(i,j)} \mathbb{E}_X[\mathbb{E}_{\prec}[\log(N_{i,j})]].$$

Let us fix  $X$  and a pair  $i \neq j$  and turn to bound  $\mathbb{E}_{\prec}[\log(N_{i,j})]$ . With probability  $\frac{5}{6}$  there holds  $\log(N_{i,j}) = 0$ , so that

$$\mathbb{E}_{\prec}[\log(N_{i,j})] = \Pr(F_{i,j}) \mathbb{E}_{\prec \mid F_{i,j}}[\log(N_{i,j})] = \frac{1}{6} \mathbb{E}_{\prec \mid F_{i,j}}[\log(N_{i,j})].$$

Clearly,  $\mathcal{M}_{i,j}$  depends only on the ordering  $\ll$ . If  $p$  is the position of  $i$  in  $\ll$ , then

$$\begin{aligned} \mathbb{E}_{\prec \mid F_{i,j}}[\log(M_{i,j})] &= \mathbb{E}_{\ll \mid F_{i,j}}[\log(M_{i,j})] = \\ \mathbb{E}_{p \mid F_{i,j}}[\mathbb{E}_{\ll \mid p, F_{i,j}}[\log(M_{i,j})]] &\leq \mathbb{E}_{p \mid F_{i,j}}[\log(\mathbb{E}_{\ll \mid p, F_{i,j}}[M_{i,j}])]. \end{aligned} \quad (3)$$

The last inequality follows from Jensen's inequality. We next analyze the distribution of  $p$  and the expectation of  $M_{i,j}$  given  $p$ . In the following lemmas we denote  $X_{i,j}$  by  $k$ .

**Lemma 3.1.** *The probability that  $i$  occupies the  $p$ -th position in  $\ll$ , given  $F_{i,j}$ , is*

$$3 \frac{(n-p)(n-p-1)}{n(n-1)(n-2)}.$$

*Proof.* We are sampling  $\ll$  uniformly from among the  $\frac{n!}{3}$  permutations in which  $i$  precedes  $j$  and  $k$ . To specify such a permutation in which  $i$  is in the  $p$ -th position we should place  $j$  in any of the  $n-p$  positions following  $i$ , and then  $k$  in one of the  $n-p-1$  remaining positions following  $i$ . The remaining vertices can be ordered in  $(n-3)!$  ways for a total of  $(n-p)(n-p-1)(n-3)!$  such permutations. The conclusion follows.  $\square$

**Lemma 3.2.**  $\mathbb{E}_{\ll|p,F_{i,j}}[M_{i,j}] = 1 + \frac{(n-p-2)(n-p-3)(n-p-4)}{(n-4)(n-5)}$ .

*Proof.* Now we are sampling uniformly from the set of orderings in which  $i \ll j, k$  where  $i$  is in the  $p$ -th position. Clearly  $k \in \mathcal{M}_{i,j}$ . This corresponds to the 1 term. If  $t \in V \setminus \{i, j, k\}$ , let  $a$  (resp.  $b$ ) be the unique vertex such that  $X_{i,a} = t$  (resp.  $X_{i,b} = t$ ). The vertex  $t$  forms a triple with  $i$  and  $a$ , and a triple with  $j$  and  $b$ . If an edge from either of these triples is exposed before  $\{i, j\}$ , then  $t$  is ruled out for  $X_{i,j}$ . Note that  $t \in \mathcal{M}_{i,j}$  iff  $i \ll a, b, t$ .

But

$$\begin{aligned} \Pr(i \ll a, b, t | i \text{ is in position } p, i \ll j, k) = \\ \frac{(n-p-2)(n-p-3)(n-p-4)}{(n-3)(n-4)(n-5)}. \end{aligned}$$

There are  $n-3$  such vertices  $t$ , and the conclusion follows.  $\square$

Using lemmas 3.1 and 3.2, we have

$$\begin{aligned} \mathbb{E}_{p|F_{i,j}}[\log(\mathbb{E}_{\ll|p,F_{i,j}}[M_{i,j}])] = \\ \sum_{p=1}^{n-2} 3 \frac{(n-p)(n-p-1)}{n(n-1)(n-2)} \log\left(1 + \frac{(n-p-2)(n-p-3)(n-p-4)}{(n-4)(n-5)}\right) = \\ \frac{3}{n(n-1)(n-2)} \sum_{r=2}^{n-1} r(r-1) \log\left(1 + \frac{(r-2)(r-3)(r-4)}{(n-4)(n-5)}\right). \end{aligned}$$

As in the previous section, the next step is to collect together lower order terms and obtain

$$\frac{3}{n^3} \int_0^n u^2 \log\left(\frac{u^3}{n^2}\right) dx + o(1) = \log n - 1 + o(1).$$

Together with 3, this implies that

$$\mathbb{E}_{\prec|F_{i,j}}[\log(M_{i,j})] = \log n - 1 + o(1). \quad (4)$$

We next show that for every  $1 \leq l \leq n$ ,

$$\mathbb{E}_{\prec|F_{i,j}, M_{i,j}=l}[\log(N_{i,j})] = \log l - 1 + o(1).$$

Let  $q$  be the position taken by  $\{i, j\}$  in the uniformly chosen random ordering of the edges in  $E_i$ , and let  $m = |E_i|$ . Again, by Jensen

$$\mathbb{E}_{\prec|F_{i,j}, M_{i,j}=l}[\log(N_{i,j})] \leq \mathbb{E}_{q|F_{i,j}, M_{i,j}=l}[\log(\mathbb{E}_{\prec|q, F_{i,j}, M_{i,j}=l}[N_{i,j}])].$$

The following two lemmas describe the distribution of  $q$  and the expectation of  $N_{i,j}$  given  $q$ . We maintain the notation that  $k$  is the vertex  $X_{i,j}$ .

**Lemma 3.3.** *The probability that  $\{i, j\}$  occupies the  $q$ -th position in the ordering of  $E_i$ , given  $F_{i,j}$ , is*

$$2 \frac{(m-q)}{m(m-1)}.$$

*Proof.* There are  $\frac{m!}{2}$  orderings of  $E_i$  in which  $\{i, j\}$  precedes  $\{i, k\}$ . There are  $m-q$  possible positions for  $\{i, k\}$  following  $\{i, j\}$ . The conclusion follows.  $\square$

**Lemma 3.4.**  $\mathbb{E}_{\prec|q, F_{i,j}, M_{i,j}=l}[N_{i,j}] = 1 + \frac{(m-q-1)(m-q-2)}{(m-2)(m-3)}(l-1)$ .

*Proof.* Now we are sampling uniformly from the set of orderings of  $E_i$  in which  $\{i, j\}$  precedes  $\{i, k\}$  and  $\{i, j\}$  is in the  $q$ -th position. For each vertex  $v$ , we determine the probability that  $v \in \mathcal{N}_{i,j}$ , and then use the linearity of the expectation to obtain the result. We consider only vertices in  $\mathcal{M}_{i,j}$ .

Clearly,  $k \in \mathcal{N}_{i,j}$ . This corresponds to the 1 term. If  $t \in \mathcal{M}_{i,j} \setminus \{k\}$ , then  $t \in \mathcal{N}_{i,j}$  iff  $\{i, j\} \prec \{i, a\}, \{i, t\}$ , where  $a$  is the unique vertex such that  $X_{i,a} = t$ . But

$$\Pr(\{i, j\} \prec \{i, a\}, \{i, t\} | \{i, j\} \text{ is in position } q, \{i, j\} \prec \{i, k\}) =$$

$$\frac{(m-q-1)(m-q-2)}{(m-2)(m-3)}.$$

There are  $l-1$  such vertices  $t$ , and the conclusion follows. □

Therefore,

$$\begin{aligned} & \mathbb{E}_{\prec|F_{i,j}, M_{i,j}=l}[\log(N_{i,j})] \leq \\ & \sum_{q=1}^{m-1} \frac{2(m-q)}{m(m-1)} \log\left(1 + \frac{(m-q-1)(m-q-2)}{(m-2)(m-3)}(l-1)\right) = \\ & \frac{2}{m(m-1)} \sum_{r=1}^{m-1} r \log\left(1 + \frac{(r-1)(r-2)}{(m-2)(m-3)}(l-1)\right). \end{aligned}$$

As above, this is equal to

$$\frac{2}{m^2} \int_0^m u \log\left(\frac{u^2}{m^2}l\right) du + o(1) = \log l - 1 + o(1).$$

Putting all of this together, we have

$$\begin{aligned} \mathbb{E}_{\prec|F_{i,j}}[\log(N_{i,j})] &= \sum_{l=1}^n \Pr_{\prec|F_{i,j}}(M_{i,j}=l) \mathbb{E}_{\prec|F_{i,j}, M_{i,j}=l}[\log(N_{i,j})] \leq \\ & \sum_{l=1}^n \Pr_{\prec|F_{i,j}}(M_{i,j}=l) (\log l - 1 + o(1)) = \mathbb{E}_{\prec|F_{i,j}}[\log(M_{i,j})] - 1 + o(1) \leq \\ & \log n - 2 + o(1) \end{aligned}$$

Thus,

$$\begin{aligned} \log(STS(n)) &\leq \frac{1}{6} \sum_{(i,j)} (\log n - 2 + o(1)) = \\ & \frac{\binom{n}{2}}{3} (\log n - 2 + o(1)), \end{aligned}$$

which yields the bound  $STS(n) \leq ((1+o(1))\frac{n}{e^2})^{\frac{n^2}{6}}$  as claimed.

## References

- [1] P. J. CAMERON, *A generalization of  $t$ -designs*, Discrete Math., Discrete Math. 309 (2009), 4835–4842.
- [2] P. J. CAMERON, *Parallelisms of Complete Designs*, London Math. SOC. Lecture Note Ser. 23. Cambridge Univ. Press, Cambridge (1976) 144 pp. MR 54#7269.
- [3] T. M. COVER AND J. A. THOMAS, *Elements of Information Theory*, Wiley, New York, 1991.
- [4] G.P. EGORICHEV, *Proof of the van der Waerden conjecture for permanents*, Siberian Math. J. 22 (1981), 854–859.
- [5] D.I. FALIKMAN, *A proof of the van der Waerden conjecture regarding the permanent of a doubly stochastic matrix*, Math. Notes Acad. Sci. USSR 29 (1981), 475–479.
- [6] N. LINIAL AND Z. LURIA, *An upper bound on the number of higher dimensional permutations*, <http://arxiv.org/abs/1106.0649>.
- [7] JAIKUMAR RADHAKRISHNAN, *An entropy proof of Bregman's theorem*, J. Combinatorial Theory Ser. A 77 (1997), no. 1, 80–83 MR1426744 (97m:15006)
- [8] RICHARD M. WILSON *Nonisomorphic Steiner Triple Systems*, Math. Z. 135 (1974), 303–313.