An upper bound on the number of Steiner triple systems

Nathan Linial[*] Zur Luria[†]

Abstract

Richard Wilson conjectured in 1974 the following asymptotic formula for the number of n-vertex Steiner triple systems: $STS(n) = \left((1+o(1))\frac{n}{e^2}\right)^{\frac{n^2}{6}}$. Our main result is that

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

The proof is based on the entropy method.

As a prelude to this proof we consider the number $F(n)$ of 1-factorizations of the complete graph on n vertices. Using the Kahn-Lovász theorem it can be shown that

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

We show how to derive this bound using the entropy method. Both bounds are conjectured to be sharp.

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

[*] 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 .

well known that a Steiner triple system on $n \geq 1$ vertices exists if and only if $n \equiv 1$ or $3 \pmod 6$. We denote the number of Steiner triple systems on the vertex set $[n] := \{1, ..., n\}$ by $STS(n)$.

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. Let $F(n)$ denote the number of 1-factorizations of K_n. It is well known that a 1-factorization of K_n exists if and only if n is even.

The main results of this paper are a new upper bound on $STS(n)$ and a new proof of a known upper bound on $F(n)$.

It has been observed (e.g., [3]) 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 [9], 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 [12].

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

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.

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

The Kahn-Lovász theorem shows that a graph with degree sequence $r_1, ..., r_n$ has at most $\prod_{i=1}^{n} (r_i!)^{\frac{1}{2r_i}}$ perfect matchings. In particular a d-regular graph has at most $(d!)^{\frac{n}{2d}}$ perfect matchings. For a proof see Alon and Friedland [1]. These results are inspired by Brégman's proof [2] of Minc's conjecture on the permanent. For a very recent proof of this result that uses the entropy method, see [6].

This theorem easily yields an upper bound on $F(n)$ as follows: Choose first a perfect matching of K_n. The remaining edges constitute an $n-2$ regular graph in which we again choose a perfect matching. We proceed to choose perfect matchings until we exhaust all of $E(K_n)$. The theorem implies that we have at most $((n-k)!)^{\frac{n}{2(n-k)}}$ choices for the k-th step, so that $F(n) \leq \prod_{d=1}^{n-1} (d!)^{\frac{n}{2d}}$. An application of Stirling's formula gives:

Theorem 1.2.

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

One of the results of the present paper is a new proof of this bound.

It is an interesting question to seek lower bounds to complement these upper bounds. We have already mentioned Wilson's lower bound on $STS(n)$. Cameron gave a lower bound for $F(n)$ in [4]. His argument yields

$$F(n) \geq \left((1+o(1))\frac{n}{4e^2}\right)^{\frac{n^2}{2}} .$$

For the sake of completeness we repeat his argument. It starts with the inequality $F(n) \geq L(\frac{n}{2})(F(n/2))^2$, where $L(n)$ is the number of order-n Latin squares. This inequality is shown as follows: Partition the vertex set $[n]$ into two equal parts, and select an arbitrary 1-factor on each. It is well-known and easy to prove that a 1-factorization of $K_{r,r}$ is equivalent to an order-r Latin square. It follows easily from the Van der Waerden conjecture that $L(n) \geq (\frac{(1+o(1))n}{e^2})^{n^2}$ (see [11]). The derivation of Cameron's lower bound is a simple matter now. We note that this argument works when n is divisible by 4. When $n = 4r+2$ some additional care is required.

For the record, we complement Wilson's conjecture with a conjecture on the number of 1-factorizations:

Conjecture 1.3.

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

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 $H(X) = \sum_j H(Y_j|Y_1, \dots, Y_{j-1})$. The expression $X = (Y_1, \dots, Y_k)$ can be viewed 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 in which the variables Y_i are revealed and average over the resulting identities $H(X) = \sum_j H(Y_j|Y_i \text{ s.t. } i \text{ precedes } j)$. Similar ideas can be found in the literature, but to the best of our knowledge this method of proof is mostly due to Radhakrishnan [10]. 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 [5] for a thorough discussion of entropy. For an example of the entropy method, see [10].

In section 2, we give an entropy proof of theorem 1.2. Using similar methods, in section 3 we give an entropy proof of theorem 1.1.

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 $X_{\{i,j\}}$ to be the color of the edge $\{i, j\}$ in X. In order to analyze these random variables we first fix an ordering of the edges and we seek to bound the number of colors which are available for the edge $\{i, j\}$, given the colors of the preceding edges.

A color c is unavailable for $X_{\{i,j\}}$ if there is a previously seen variable of the form $X_{\{i,k\}}$ or $X_{\{k,j\}}$ which is equal to c. Let $N_{\{i,j\}}$ denote the number of available colors. It is really an upper bound on the number of values that $X_{\{i,j\}}$ can take given values for previously seen variables. Note that $N_{\{i,j\}}$ depends both on X and on the ordering.

We first apply the chain rule for the entropy function.

$$\log(F(n)) = H(X) = \sum_{\{i,j\}} H(X_{\{i,j\}}|X_{\{k,l\}} : \{k,l\} \text{ precedes } \{i,j\}) \tag{1}$$

$$= \sum_{\{i,j\}} \mathbb{E}_X[H(X_{\{i,j\}}|X_{\{k,l\}} = x_{\{k,l\}} : \{k,l\} \text{ precedes } \{i,j\})].$$

We now use the bound $H(X) \leq \log(|Range(X)|)$ and conclude that

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

This bound holds for any ordering of the edges. We choose a random ordering by selecting a random mapping $\lambda : \binom{[n]}{2} \to [0,1]$. Edges are scanned according to the order of the real numbers $\lambda(\{i,j\})$ starting from the largest values. Of course we may assume that λ is $1:1$. This description of the ordering turns out to simplify matters in the discussion below.

We now take the expectation with respect to the random choice of the ordering, i.e., the choice of the mapping λ.

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

We bound the expectation $\mathbb{E}_\lambda[\log(N_{\{i,j\}})]$ using Jensen's inequality. If we do this right away, the resulting upper bound is not optimal. Therefore, we first condition on the value of $\lambda(\{i,j\})$ and only then use Jensen's inequality.

$$\mathbb{E}_\lambda[\log(N_{\{i,j\}})] = \mathbb{E}_{\lambda(\{i,j\})}[\mathbb{E}_\lambda[\log(N_{\{i,j\}})|\lambda(\{i,j\})]] \leq$$

$$\mathbb{E}_{\lambda(\{i,j\})}[\log(\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\})])]$$

In order to evaluate this expression it is necessary to compute the expectation of $N_{\{i,j\}}$ given $\lambda(\{i,j\})$.

Lemma 2.1. $\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\})] = 1 + (n-2)\lambda(\{i,j\})^2$.

Proof. The true color of the edge $\{i,j\}$ in X is obviously always available to $X_{\{i,j\}}$. For each remaining color c, there is an edge of the form $\{i,a\}$ and an edge of the form $\{b,j\}$ that take the color c in X. If either of these edges λ-precedes $\{i,j\}$ then c is unavailable.

The edge $\{i,j\}$ precedes any edge of smaller λ value. Since these values are chosen independently, the probability that c is available is $\lambda(\{i,j\})^2$, and the result follows from the linearity of the expectation. □

Using lemma 2.1, we have

$$\mathbb{E}_{\lambda(\{i,j\})}[\log(\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\})])] = \int_0^1 \log(1+(n-2)t^2)dt$$

$$= \log(n-1) - 2 + \frac{2\arctan(\sqrt{n-2})}{\sqrt{n-2}}$$

$$= \log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right).$$

Consequently,

$$\log(F(n)) \leq \sum_{\{i,j\}} \log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right)$$

$$= \binom{n}{2}\left(\log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right)\right)$$

which yields the bound

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

3 An upper bound on the number of Steiner triple systems

The ideas here are similar to those in section 2, but the details are different.

Let X be a uniformly chosen random Steiner triple system on n vertices. Define $X_{\{i,j\}}$ to be the unique vertex k such that $\{i,j,k\}$ is a triple in X.

As above, for a given order on the pairs we define a random variable $N_{\{i,j\}}$.

Let $X_{\{i,j\}} = k$, and let $F_{\{i,j\}}$ denote the event that $\{i,j\}$ precedes both $\{j,k\}$ and $\{i,k\}$. If $F_{\{i,j\}}$ doesn't occur, set $N_{\{i,j\}} := 1$.

Let $t \in [n] \setminus \{i,j,k\}$ be a vertex. Since $\{i,j,t\} \notin X$, there are vertices a and b such that $\{i,a,t\}, \{j,b,t\} \in X$. We say that the vertex t is unavailable for $X_{\{i,j\}}$ if any of the six pairs in these triples precede $\{i,j\}$. If $F_{\{i,j\}}$ does occur, define $N_{\{i,j\}}$ to be the number of available vertices.

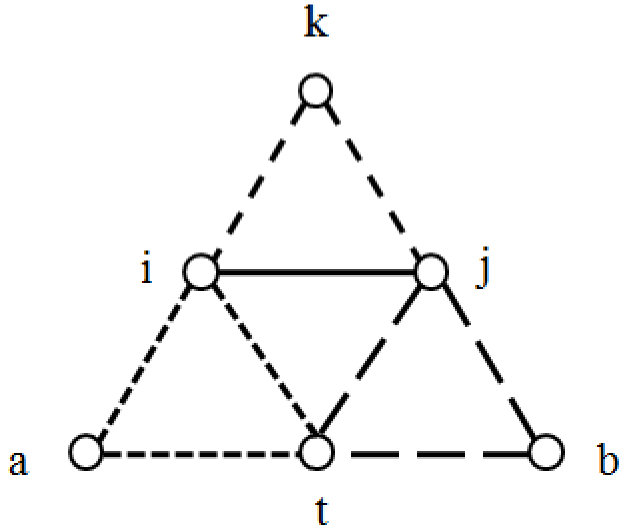

Figure 1: If either of the triangles $\{t,i,a\}$ or $\{t,j,b\}$ are revealed before $X_{\{i,j\}}$, then t is unavailable.

Now, If $F_{\{i,j\}}$ doesn't occur, then $X_{\{i,j\}}$ is uniquely determined by the preceding variables. Otherwise, the unavailable vertices are ruled out as possible values for $X_{\{i,j\}}$. If, for instance, $\{a,t\}$ is revealed before $\{i,j\}$, then by the time that $X_{\{i,j\}}$ is revealed to us we already know that $\{i,a,t\} \in X$, and therefore $\{i,j,t\} \notin X$ and $X_{\{i,j\}} \neq t$.

Thus, $N_{\{i,j\}}$ is an upper bound on the number of vertices that are available for $X_{\{i,j\}}$, given the values of the preceding variables.

For a given ordering of the pairs, as in Equation (1) we derive:

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

As before, we choose a random ordering by selecting a random mapping $\lambda : \binom{[n]}{2} \to [0,1]$. Pairs are considered by decreasing order of their λ values. We take the expectation over the choice of λ to obtain

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

Let us fix X and an edge $\{i,j\}$ and turn to bound $\mathbb{E}_\lambda[\log(N_{\{i,j\}})]$. The next step is to condition over $\lambda(\{i,j\})$.

$$\mathbb{E}_\lambda[\log(N_{\{i,j\}})] = \mathbb{E}_{\lambda(\{i,j\})}[\mathbb{E}_\lambda[\log(N_{\{i,j\}})|\lambda(\{i,j\})]].$$

The event $F_{\{i,j\}}$ occurs iff $\lambda(\{i,j\}) > \lambda(\{i,k\})$ and $\lambda(\{i,j\}) > \lambda(\{k,j\})$ so that $\Pr(F_{\{i,j\}}|\lambda(\{i,j\})) = \lambda(\{i,j\})^2$. Therefore

$$\begin{aligned}\mathbb{E}_\lambda[\log(N_{\{i,j\}})|\lambda(\{i,j\})] &= \lambda(\{i,j\})^2\mathbb{E}_\lambda[\log(N_{\{i,j\}})|\lambda(\{i,j\}), F_{\{i,j\}}] \\ &\leq \lambda(\{i,j\})^2\log(\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\}), F_{\{i,j\}}]), \qquad (2)\end{aligned}$$

where the final inequality follows from Jensen's inequality.

Lemma 3.1. $\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\}), F_{\{i,j\}}] = 1 + (n-3)\lambda(\{i,j\})^6$.

Proof. The vertex k that participates in a triple with i,j is obviously always available to $X_{\{i,j\}}$. As mentioned, for each remaining vertex t, there are six pairs that $\{i,j\}$ must λ-precede for t to be available, and this occurs with probability $\lambda(\{i,j\})^6$. The result follows from the linearity of the expectation. □

Using 2 and lemma 3.1, we have

$$\begin{aligned}\mathbb{E}_{\lambda(\{i,j\})}[\log(\mathbb{E}_\lambda[N_{\{i,j\}}|\lambda(\{i,j\})])] &= \int_0^1 t^2\log(1+(n-3)t^6)dt \\ &= \frac{1}{3}\left((\log(n-2)-2) + \frac{2\arctan(\sqrt{n-3})}{\sqrt{n-3}}\right) \\ &= \frac{1}{3}\left(\log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right)\right).\end{aligned}$$

Consequently,

$$\begin{aligned}\log(STS(n)) &\leq \sum_{\{i,j\}}\frac{1}{3}\left(\log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right)\right) \\ &= \frac{n^2}{6}\left(\log(n) - 2 + O\left(\frac{1}{\sqrt{n}}\right)\right)\end{aligned}$$

which yields the bound

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

Acknowledgement

We are grateful to the anonymous referees for useful remarks. In particular, we acknowledge comments made by one of the referees that helped us shorten and simplify our proofs.

References

[1] Alon, N. and Friedland, S., *The maximum number of perfect matchings in graphs with a given degree sequence*, the electronic journal of combinatorics, 2008 .

[2] L. M. Brègman, *Certain properties of nonnegative matrices and their permanents*, Dokl. Akad. Nauk SSSR 211 (1973), 27-30. MR MR0327788 (48 #6130)

[3] P. J. Cameron, *A generalization of t-designs*, Discrete Math., Discrete Math. 309 (2009), 4835–4842.

[4] P. J. Cameron, *Parallelisms of Complete Designs*, London Math. SOC. Lecture Note Ser. 23. Cambridge Univ. Press, Cambridge (1976) 144 pp. MR 54#7269.

[5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley, New York, 1991.

[6] Cutler, J. and Radcliffe, AJ, *An entropy proof of the Kahn-Lovász theorem*, the electronic journal of combinatorics, 2011 .

[7] G.P. Egorichev, *Proof of the Van der Waerden conjecture for permanents*, Siberian Math. J. 22 (1981), 854–859.

[8] 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.

[9] N. Linial and Z. Luria, *An upper bound on the number of higher dimensional permutations*, http://arxiv.org/abs/1106.0649.

[10] Jaikumar Radhakrishnan, *An entropy proof of Bregman's theorem*, J. Combinatorial Theory Ser. A 77 (1997), no. 1, 80–83 MR1426744 (97m:15006)

[11] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, Cambridge U.P., 1992.

[12] Richard M. Wilson*Nonisomorphic Steiner Triple Systems*, Math. Z. 135 (1974), 303–313.