# AN ENTROPY PROOF OF THE KAHN-LOVÁSZ THEOREM

JONATHAN CUTLER AND A.J. RADCLIFFE

Abstract. Brègman [2], gave a best possible upper bound for the number of perfect matchings in a balanced bipartite graph in terms of its degree sequence. Recently Kahn and Lovász [8] extended Brègman's theorem to general graphs. In this paper, we use entropy methods to give a new proof of the Kahn-Lovász theorem. Our methods build on Radhakrishnan's [9] use of entropy to prove Brègman's theorem.

## 1. Introduction

Entropy has recently emerged as a powerful tool in combinatorics (see for instance [3, 6, 7]). Radhakrishnan [9] used entropy to give a new proof of Brègman's theorem. While Brègman's theorem is usually stated in terms of the permanent of a square $(0,1)$-matrix, the equivalent version we state uses graph theoretic notation. If $G$ is a graph, we let $\Phi(G)$ be the set of perfect matchings of $G$ and $\phi(G) = |\Phi(G)|$. Also, if $v \in V(G)$, we denote the degree of $v$ by $d(v)$.

**Theorem 1** (Brègman [2])**.** *If $G = G(L, R)$ is a bipartite graph such that $|L| = |R|$, then*

$$\phi(G) \leq \prod_{v \in L} (d(v)!)^{1/d(v)}.$$

The extension of Brègman's theorem to general graphs was achieved by Kahn and Lovász [8], and independently proved by Friedland [4].

**Theorem 2** (Kahn-Lovász [8])**.** *For $G$ an arbitrary graph,*

$$\phi(G) \leq \prod_{v \in V} (d(v)!)^{1/(2d(v))}.$$

The original proof of Kahn and Lovász was never published, see [3], but was supposedly quite long. Friedland's proof is based on an extension of Schrijver's [10] proof of the Brègman inequality. A short proof, deducing the result for general graphs from Brègman's theorem, was given by Alon and Friedland [1]. This paper presents a new proof of Theorem 2 using entropy methods.

We introduce the basics of entropy that will be used in this paper. For a more comprehensive introduction, see, e.g., [5]. In the following definition, and throughout this paper, all logarithms are base two, and all random variables have finite range.

**Definition 1.** The *entropy* of a random variable $X$ is given by

$$H(X) = \sum_x \mathbb{P}(X = x) \log \left( \frac{1}{\mathbb{P}(X = x)} \right).$$

For random variables $X$ and $Y$, the *conditional entropy of $X$ given $Y$* is

$$H(X \mid Y) = \mathbb{E}(H(X \mid Y = y)) = \sum_y \mathbb{P}(Y = y) H(X \mid Y = y).$$

Both entropy and conditional entropy are always non-negative.

One can think of the term $\log(1/\mathbb{P}(X = x))$ appearing in the definition of the entropy as measuring the surprise involved in discovering that the value of $X$ turned out to be $x$ (measured on a logarithmic scale). In these terms $H(X)$ is the expected surprise in learning the value of $X$. The conditional entropy $H(X \mid Y)$ is the expected surprise in learning the value of $X$ given that the value of $Y$ is known. The chain rule (part b) below) shows that also $H(X \mid Y) = H((X, Y)) - H(Y)$. The following theorem collects the basic facts about entropy that we will need.

**Theorem 3.**
*a) If $X$ is a random variable then*

$$H(X) \leq \log |\mathrm{range}(X)|,$$

*with equality if and only if $X$ is uniform on its range.*
*b) If $X = (X_1, X_2, \ldots, X_n)$ is a random sequence then*

$$H(X) = H(X_1) + H(X_2 \mid X_1) + \cdots + H(X_n \mid X_1, X_2, \ldots, X_{n-1}).$$

*c) If $X, Y, Z$ are random variables then*

$$H(X \mid Y, Z) \leq H(X \mid Y).$$

*d) If $X, Y, Z$ are random variables and $Z$ is $Y$-measurable then*

$$H(Y, Z) = H(Y) \qquad \text{and} \qquad H(X \mid Y, Z) = H(X \mid Y).$$

Part c) above is the natural fact that knowing more information does not increase your expected surprise—part d) says that if you could have worked out the extra information for yourself then there is no change in your expected surprise.

In Section 2, we present Radhakrishnan's entropy proof of Brègman's theorem as a consequence of his randomized version of the chain rule. Although the argument is exactly that of Radhakrishnan, we believe that its presentation herein presents the ideas clearly and succinctly. In addition it provides a framework for understanding our proof of the Kahn-Lovász, which we present in Section 3.

## 2. Radakrishnan's proof

This section presents the entropy proof of Radhakrishnan of Brègman's theorem, which is as follows.

**Theorem 1.** *If $G = G(L, R)$ is a bipartite graph such that $|L| = |R|$, then*

$$\phi(G) \leq \prod_{v \in L} (d(v)!)^{1/d(v)}.$$

The key idea of Radhakrishnan's proof was to introduce a randomized version of the chain rule. This idea has been used in other entropy proofs and seems to be a powerful tool when applying entropy methods to combinatorial problems.

**Theorem 4** (Radhakrishnan)**.** *Suppose $X = (X_i)_{i \in I}$ is a random vector and $\mathcal{A}$ is an arbitrary covering of $I$. Let $\preceq$ be an ordering on $\mathcal{A}$ chosen randomly (not necessarily uniformly). Then*

$$H(X) = \sum_{A \in \mathcal{A}} H(X_A \mid \preceq, X_B, B \prec A).$$

*Proof.* We prove it for a fixed ordering $\preceq$, and the general result follows by averaging. First note that $H(X) = H\left((X_A)_{A \in \mathcal{A}}\right)$ by repeated application of Theorem 3, part d). Thus, by the chain rule,

$$H(X) = H\left((X_A)_{A \in \mathcal{A}}\right) = \sum_A H(X_A | X_B, B \prec A).$$

□

We are now ready to present the entropy proof of Theorem 1 due to Radhakrishnan. The proof proceeds by applying the randomized chain rule above with respect to orderings of the vertices in $L$. For a fixed matching, then, if we proceed through a particular ordering, each vertex of $L$ has a certain subset of its neighbors as potential partners in the matching. The number of such potential partners turns out to be uniform on the possibilities, and the result follows.

*Proof of Theorem 1.* Let $M$ be a perfect matching of $G$ chosen uniformly at random from $\Phi(G)$, and let $X = (X_e)_{e \in E(G)}$ be the indicator vector of $M$. We define a covering $\mathcal{A} = \{A_v : v \in L\}$ by $A_v = \{vw : w \text{ a neighbor of } v\}$. For $v \in L$ we define $X_v$ to be the unique $M$-neighbor of $v$, and note that $X_v$ and $X_{A_v}$ contain precisely the same information. Given $\preceq$ chosen uniformly at random from the set of all total orderings of $L$ (and independently of $M$), we define $N_v = |A_v \setminus \{vX_w : w \preceq v\}|$. Later, in Lemma 6, we give the easy proof that for any fixed perfect matching $m$ we have

$$\mathbb{P}(N_v = k \mid M = m) = \frac{1}{d(v)}, \qquad \text{for all } k = 1, 2, \ldots, d(v).$$

As $\mathbb{P}(N_v = k \mid M = m) = 1/d(v)$ for any fixed $m$ we see that $N_v$ is uniformly distributed on $\{1, 2, \ldots, d(v)\}$. Now, by Theorem 4 followed by standard uses of the properties of entropy from Theorem 3,

$$\begin{aligned}
H(X) &= \sum_v H(X_v | \preceq, X_w, x \preceq v) \\
&\leq \sum_v H(X_v | \preceq, N_v) \\
&\leq \sum_v H(X_v | N_v) \\
&= \sum_v \sum_{k=1}^{d(v)} \mathbb{P}(N_v = k) H(X_v | N_v = k) \\
&\leq \sum_v \sum_{k=1}^{d(v)} \frac{1}{d(v)} \log(k) \\
&= \sum_v \log(d(v)!)^{1/d(v)}.
\end{aligned}$$

□

## 3. A proof of the Kahn-Lovász theorem

The entropy proof of the Kahn-Lovász theorem is complicated by the fact that there can be edges of the graph (and a fixed matching) amongst the neighbors of a particular vertex. Thus the analogue of the statement that $N_v$ is uniformly distributed is no longer true. However, we still are able to give an entropy bound that proves the theorem.

We discuss a slight generalization of the problem that we face. We discuss the process of picking a random element from a family of sets, where some have already been ruled out. These are the ones appearing before some distinguished element in a random ordering. In the graph context we will have a random ordering on edges of a fixed matching incident to neighbors of a vertex $v$—the distinguished element will be the matching edge incident with $v$.

**Definition 2.** Suppose that $\mathcal{A} = (A_x)_{x \in I}$ is a family of non-empty disjoint finite sets and let $*$ be a distinguished element of $I$. Suppose that $\preceq$ is a uniformly random (total) ordering of $I$. We define a random variable $X_{\mathcal{A}}$ that we call a *uniform random late choice from* $\mathcal{A}$ by picking an element of

$\bigcup_{x \succeq *} A_x$ uniformly at random. For notational convenience we define

$$\mathcal{U}(\mathcal{A}, \preceq) = \bigcup_{x \succeq *} A_x.$$

In the next lemma we prove that a certain conditional entropy associated with a random late choice is greatest when all the $A_x$ are singletons. In our graph context this corresponds to the situation when there are no matching edges between neighbors of $v$.

**Lemma 5.** *Let $\mathcal{A} = (A_x)_{x \in I}$ be a family of non-empty disjoint finite sets and $\preceq$ be a uniform random ordering on $I$. Let $\mathcal{B}$ be the family $(\{a\})_{a \in U}$, where $U = \bigcup_{x \in I} A_x$, and let $\preceq_{\mathcal{B}}$ be a uniformly random ordering on $U$. We write $n$ for $|U|$. Then*

$$H(X_{\mathcal{A}} \,\big|\, \preceq) \leq H(X_{\mathcal{B}} \,\big|\, \preceq_{\mathcal{B}}) = \frac{\log(n!)}{n},$$

*with equality if and only if $V$ is a uniform random late choice and $|A_x| = 1$ for all $x \in I$.*

*Proof.* Set $k = |I|$. For each value of $n$, we prove the result by downwards induction on $k$. The case $k = n$ is precisely the equality in the statement of the lemma. In this case we have

$$\begin{aligned}
H(X_{\mathcal{A}} \,\big|\, \preceq) &= \frac{1}{n!} \sum_{\preceq} \log |\mathcal{U}(\mathcal{A}, \preceq)| \\
&= \frac{1}{n!} \sum_{\preceq} \log |\{x \in I \,:\, x \succeq *\}| \\
&= \sum_{i=1}^{n} \frac{1}{n!} \Big| \{\preceq \,:\, |\{x \in I \,:\, x \succeq *\}| = i\} \Big| \log(i) \\
&= \sum_{i=1}^{n} \frac{1}{n} \log(i) \\
&= \frac{\log(n!)}{n}.
\end{aligned}$$

Suppose then that $k < n$. There exists some $A_x$ with $|A_x| \geq 2$. We first consider the case $x \neq *$. We will build a family $\mathcal{A}'$ that is identical with $\mathcal{A}$ except that $A_x$ is split into two nonempty parts, $A_{x'}$ and $A_{x''}$. (Here we have introduced two new elements into the index set and deleted $x$, so $I' = I \setminus \{x\} \cup \{x', x''\}$.) We introduce a new uniform random ordering $\preceq'$ on $I'$. We will show

$$H(X_{\mathcal{A}} \,\big|\, \preceq) < H(X_{\mathcal{A}'} \,\big|\, \preceq') \leq \frac{\log(n!)}{n}.$$

To be precise, we show that for a fixed ordering $\preceq_0$ on $I_0 = I \setminus \{x\}$, the total contribution to $H(X_{\mathcal{A}} \,|\preceq)$ coming from orderings $\preceq$ on $I$ which restrict to $\preceq_0$ on $I_0$ is no bigger than the total for $H(X_{\mathcal{A}'} \,|\preceq')$ where again $\preceq'$ restricts to $\preceq_0$. I.e., we show

$$\frac{1}{k!} \sum_{\substack{\preceq \\ \preceq|_{I_0} = \preceq_0}} \log\left(|\mathcal{U}(\mathcal{A}, \preceq)|\right) < \frac{1}{(k+1)!} \sum_{\substack{\preceq' \\ \preceq'|_{I_0} = \preceq_0}} \log\left(\left|\mathcal{U}(\mathcal{A}', \preceq')\right|\right). \tag{$\dagger$}$$

We let

$$S = |\mathcal{U}(\mathcal{A} \setminus \{A_x\})|, \qquad d' = |A_{x'}|, \qquad d'' = |A_{x''}|, \quad \text{and} \quad d = |A_x| = d' + d''.$$

Since the position of $*$ in $\preceq_0$ is fixed, the only relevant issues are the positions of $x$ in $\preceq$ and $x', x''$ in $\preceq'$. Suppose that $*$ is the $j^{\text{th}}$ smallest element in $\preceq_0$. The possible values for $|\mathcal{U}(\mathcal{A}, \preceq)|$ are $S$ and $S + d$. There are $j$ orderings (exactly those in which $x$ appears before $*$) for which the value is $S$, and $k - j$ for which the value is $S + d$. (Note that since there are $k - 1$ elements of $I_0$, there

are $k$ positions in which $x$ can be inserted.) Similarly, the four possible values for $|\mathcal{U}(\mathcal{A}', \preceq')|$ are $S$, $S+d'$, $S+d''$, and $S+d$, with respective frequencies $j(j+1)$, $j(k-j)$, $j(k-j)$, and $(k-j)(k-j+1)$. Therefore, proving (†) is equivalent to proving (after multiplying by $(k+1)!$ and exponentiating)

$$\left[S^j(S+d)^{k-j}\right]^{k+1} < S^{j(j+1)}(S+d')^{j(k-j)}(S+d'')^{j(k-j)}(S+d)^{(k-j)(k-j+1)}.$$

Canceling common factors, this is equivalent to

$$S^{j(k-j)}(S+d)^{j(k-j)} < (S+d')^{j(k-j)}(S+d'')^{j(k-j)}.$$

Taking the $j(k-j)^{\text{th}}$ root, this is $S(S+d) = S^2 + dS < S^2 + dS + d'd''$.

In the case $x = *$, the situation is more straightforward. Rather than changing the index set, by deleting one element and adding two, instead we simply add a new element, $*'$. Proceeding as above we end up comparing $S$ to a geometric mean of $(S, S, \ldots, S, S+d, S+d, \ldots, S+d)$. To be precise, given a fixed ordering $\preceq_0$ of the original index set, there are $k+1$ orderings of the new index set that agree with $\preceq_0$. If $*$ is the $j^{\text{th}}$ element in $\preceq_0$, then, with $S$ defined as above, $j$ of these orderings have $|\mathcal{U}(\mathcal{A}, \preceq)| = S$ and $k-j+1$ have $|\mathcal{U}(\mathcal{A}, \preceq)| = S+d$. □

The other ingredient of our proof is the idea, due to Cuckler and Kahn [3], of exploiting the fact that a uniformly random ordering on the vertices of $G$ induces a uniformly random ordering on the edges of any fixed perfect matching. If the vertices of a graph $G$ are ordered by labeling them $1, 2, \ldots, n$, then, for any subset of edges $F \subseteq E(G)$, we define the *induced lexicographic ordering on* $F$ to be the lexicographic ordering on $F$, where edges are thought of as elements of $\binom{[n]}{2}$.

**Lemma 6.** *Let $G$ be a graph and $m$ a perfect matching in $G$. If $\preceq_V$ is a random ordering of $V(G)$, we define $\preceq_E$ to be the induced lexicographic ordering on $m$. Then $\preceq_E$ is uniform on the set of all orders of $m$. Moreover, for a particular edge $xy \in m$, the ordering $\preceq_E$ is independent of the event $\{x \preceq_V y\}$.*

*Proof.* For any permutation of the edges of $m$, there is a permutation of $V(G)$ inducing it. Therefore, the uniformity of $\preceq_V$ implies that of $\preceq_E$. Similarly, the transposition $(x\ y)$ maps the event $\{\preceq_E = \preceq_0, x \preceq_V y\}$ to the event $\{\preceq_E = \preceq_0, y \preceq_V x\}$ and hence, by the uniformity of $\preceq_V$,

$$\mathbb{P}(\preceq_E = \preceq_0, x \preceq_V y) = \mathbb{P}(\preceq_E = \preceq_0, y \preceq_V x),$$

i.e., $\preceq_E$ is independent of the event $\{x \preceq_V y\}$. □

We now describe the setup that allows us to connect uniform random late choices and the Kahn-Lovász theorem.

**Definition 3.** Given a graph $G$, a vertex $v \in V(G)$, and a perfect matching $m \in \Phi(G)$, we define

$$I_v = \{e \in m : e \text{ is incident with a neighbor of } v\}.$$

If $e \in I_v$, we set

$$A_e = e \cap N(v),$$

so that if $w$ is a neighbor of $v$ whose $m$-neighbor $u$ is also adjacent to $v$, then $A_{wu} = \{w, u\}$, whereas if $u$ is not adjacent to $v$ (in particular if $u = v$), then $A_{wu} = \{w\}$. We let $\mathcal{A}_v = \{A_e : e \in I_v\}$, from which we distinguish the element $\{v'\} = A_{\{v,v'\}}$, where $v'$ is the $m$-neighbor of $v$. Also, given a uniform random ordering $\preceq_V$ on $V$, we define $N_v$ to be the random variable

$$N_v = \begin{cases} |\{w \sim v : w \succeq_V v \text{ and } u \succeq_V v \text{ where } u \text{ is the } m\text{-neighbor of } w\}| & \text{if } v \prec_V v', \\ 0 & \text{otherwise.} \end{cases}$$

Our final lemma relates the entropy of a random late choice from $\mathcal{A}_v$ to the distribution of $N_v$.

**Lemma 7.** *With the setup of the previous definition, if $X_{\mathcal{A}_v}$ is a uniform random late choice from $\mathcal{A}_v$ then*

$$H(X_{\mathcal{A}_v} \mid \preceq_{I_v}) = \sum_{i=1}^{d_v} \mathbb{P}(N_v = i \mid v \prec_V v') \log(i). \tag{‡}$$

*Proof.* Let $k = |\mathcal{A}_v|$ and $n = |V(G)|$. We have

$$H(X_{\mathcal{A}_v} \mid \preceq_{I_v}) = \frac{1}{k!} \sum_{\preceq_{I_v}} \log\left(|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})|\right) = \frac{1}{n!} \sum_{\preceq_V} \log\left(|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})|\right).$$

We note that if $v \prec_V v'$, then $|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})| = N_v$, where the right-hand side, being a random variable, is a function of $\preceq_V$. Otherwise, of course, $N_v = 0$. By Lemma 6, the event $\{v \prec_V v'\}$ is independent of the induced ordering $\preceq_{I_v}$ so

$$\frac{1}{n!} \sum_{\preceq_V} \log\left(|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})|\right) = \frac{2}{n!} \sum_{\substack{\preceq_V \\ v \prec_V v'}} \log\left(|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})|\right).$$

Therefore

$$H(X_{\mathcal{A}_v} \mid \preceq_{I_v}) = \frac{2}{n!} \sum_{\substack{\preceq_V \\ v \prec_V v'}} \log\left(|\mathcal{U}(\mathcal{A}_v, \preceq_{I_v})|\right) = \sum_{i=1}^{d_v} \mathbb{P}(N_v = i \mid v \prec_V v') \log(i).$$

□

We are now ready to prove the Kahn-Lovász theorem.

*Proof of Theorem 2.* Let $M$ be a perfect matching of $G$ chosen uniformly at random from $\Phi(G)$, and let $X = (X_e)_{e \in E}$ be the indicator vector of $M$. For $v \in V(G)$, we also set $X_v = w$ where $vw \in M$. We pick a uniformly random total ordering $\preceq_V$ on $V(G)$. We let $Q_v$ be the indicator random variable for the event $\{X_v \prec_V v\} = \{v = X_w \text{ for some } w \prec_V v\}$.

We have

$$\begin{aligned}
\log(\phi(G)) &= H(X) \\
&= \sum_{v\in V} H\big(X_v \;\big|\; (X_w,\ w \prec_V v),\ \preceq_V\big) \\
&= \sum_{v\in V} H\big(X_v \;\big|\; N_v,\ Q_v,\ (X_w,\ w \prec_V v),\ \preceq_V\big) \qquad (1)\\
&\le \sum_{v\in V} H\big(X_v \;\big|\; N_v,\ Q_v\big) \\
&= \sum_{v\in V} \mathbb{P}(Q_v=1)\, H\big(X_v \;\big|\; N_v,\ Q_v=1\big) + \sum_{v\in V} \mathbb{P}(Q_v=0)\, H\big(X_v \;\big|\; N_v,\ Q_v=0\big) \\
&= \frac{1}{2}\sum_{v\in V} H\big(X_v \;\big|\; N_v,\ Q_v=0\big) \\
&= \frac{1}{2}\sum_{v\in V}\sum_{k=1}^{d_v} \mathbb{P}(N_v=k, Q_v=0) H\big(X_v \;\big|\; N_v=k,\ Q_v=0\big) \\
&\le \frac{1}{2}\sum_{v\in V}\sum_{k=1}^{d_v} \mathbb{P}(N_v=k, Q_v=0)\log(k) \\
&= \frac{1}{2}\sum_{v\in V}\sum_{k=1}^{d_v}\sum_{m\in\Phi(G)} \mathbb{P}(N_v=k, Q_v=0 \;\big|\; M=m)\log(k)\mathbb{P}(M=m) \\
&= \frac{1}{2}\sum_{v\in V}\sum_{m\in\Phi(G)} H(X_{\mathcal{A}_v} \;\big|\; \preceq_{I_v})\mathbb{P}(M=m) \qquad (2)\\
&\le \frac{1}{2}\sum_{v\in V}\sum_{m\in\Phi(G)} \mathbb{P}(M=m)\left(\frac{\log(d_v!)}{d_v}\right) \qquad (3)\\
&= \frac{1}{2}\sum_{v\in V}\frac{1}{d_v}\log(d_v!).
\end{aligned}$$

Here (1) is a consequence the fact that $Q_v$ and $N_v$ are $((X_w,\ w \prec_V v),\ \preceq_V)$-measurable, (2) is an application of Lemma 7, and (3) follows from Lemma 5. □

## References


1. Noga Alon and Shmuel Friedland, *The maximum number of perfect matchings in graphs with a given degree sequence*, Electron. J. Combin. **15** (2008), no. 1, Note 13, 2. MR MR2398830 (2009b:05210)
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. Bill Cuckler and Jeff Kahn, *Entropy bounds for perfect matchings and Hamiltonian cycles*, Combinatorica **29** (2009), no. 3, 327–335. MR MR2520275
4. Shmuel Friedland, *An upper bound for the number of perfect matchings in graphs*, arXiv (2008), 0803.0864v1.
5. Charles M. Goldie and Richard G. E. Pinch, *Communication theory*, London Mathematical Society Student Texts, vol. 20, Cambridge University Press, Cambridge, 1991. MR MR1143777 (93a:94001)
6. Jeff Kahn, *An entropy approach to the hard-core model on bipartite graphs*, Combin. Probab. Comput. **10** (2001), no. 3, 219–237. MR MR1841642 (2003a:05111)
7. ———, *Entropy, independent sets and antichains: a new approach to Dedekind's problem*, Proc. Amer. Math. Soc. **130** (2002), no. 2, 371–378 (electronic). MR MR1862115 (2002j:05011)
8. Jeff Kahn and László Lovász, *unpublished*.
9. Jaikumar Radhakrishnan, *An entropy proof of Bregman's theorem*, J. Combin. Theory Ser. A **77** (1997), no. 1, 161–164. MR MR1426744 (97m:15006)

10. A. Schrijver, *A short proof of Minc's conjecture*, J. Combinatorial Theory Ser. A **25** (1978), no. 1, 80–83. MR MR0491216 (58 #10481)