On the Capacity of Network Coding for Random Networks

Aditya Ramamoorthy, *Student Member, IEEE*,
Jun Shi, *Student Member, IEEE*, and
Richard D. Wesel, *Senior Member, IEEE*

Abstract—We study the maximum flow possible between a single-source and multiple terminals in a weighted random graph (modeling a wired network) and a weighted random geometric graph (modeling an *ad-hoc* wireless network) using network coding. For the weighted random graph model, we show that the network coding capacity concentrates around the expected number of nearest neighbors of the source and the terminals. Specifically, for a network with a single source, l terminals, and n relay nodes such that the link capacities between any two nodes is independent and identically distributed (i.i.d.) $\sim X$, the maximum flow between the source and the terminals is approximately $nE\lceil X \rceil$ with high probability. For the weighted random geometric graph model where two nodes are connected if they are within a certain distance of each other we show that with high probability the network coding capacity is greater than or equal to the expected number of nearest neighbors of the node with the least coverage area.

Index Terms—Minimum cut, multicast, network coding, random geometric graphs, random graphs.

I. INTRODUCTION

Consider a communication network where one source node wants to transmit information through a network to multiple terminal nodes. This correspondence considers the problem of finding the capacity of this scenario for random networks. The capacity under consideration here is the graph-theoretic max-flow capacity, not the capacity in the information-theoretic sense.

It is a known fact that routing achieves the max-flow capacity [1] of a network when transmissions are from a single source to a single terminal (for a wired network). However, in their seminal paper Ahlswede *et al.* [2] showed that for the single-source multiple-terminal case, the information rate to each terminal is the minimum of the individual max-flow bounds over all source–terminal pairs under consideration and that in general we need to code over the links in the network to achieve this capacity. Li *et al.* [3] showed that linear network coding is sufficient for achieving the capacity of the transmission of a single source to multiple terminals. Subsequent work by Koetter and Médard [4] and Jaggi *et al.* [5] presented constructions of linear multicast network codes. A randomized construction of multicast codes was presented by Ho *et al.* [6] and Chou *et al.* [7] demonstrated a practical scheme for performing randomized network coding. More recently, several authors have considered the use of network coding for nonmulticast problems [8] where there are multiple sources and multiple receivers and the receivers have arbitrary sets of demands. These problems are substantially harder and, in fact, it is necessary to utilize nonlinear solutions in some cases [9]. Network coding has also been considered for the transmission of correlated sources over a network in [10], [11].
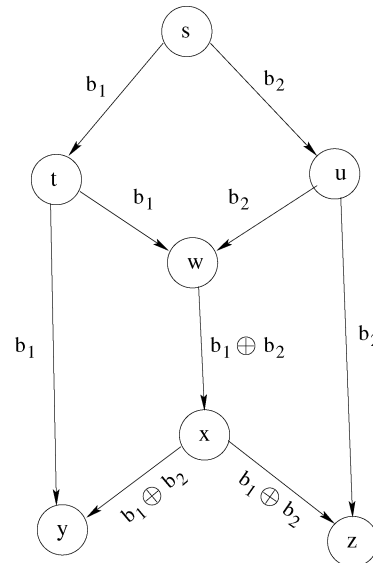
Fig. 1. Network with source s and terminals y and z. Note that sending $b_1 \oplus b_2$ on the $w \to x$ link is more efficient than simply forwarding b_1 or b_2.

It is important to clearly differentiate between routing and network coding. We say that a network employs routing when each node in the network performs only a replicate and forward function. Thus, each node can create multiple copies of a received packet and forward it on different lines. *Network coding*, on the other hand, refers to the situation when each node has the ability to perform operations such as linear combinations on the received data and then send the result on different lines. So, routing is a special case of network coding.

The usefulness of network coding can be understood by considering a simple topology shown in Fig. 1, which we borrowed from [2]. In Fig. 1, each link can transmit a single bit, error free and delay free. Observe that performing network coding (as shown in Fig. 1) enables transmission of both b_1 and b_2 to both the terminals y and z in a single transmission whereas routing would require more transmissions. In this correspondence, only the source and the terminal nodes are communicating with each other and the rest of the nodes are acting as relays.

Sections II and III prove high-probability results for the multicast capacity under network coding of weighted random graphs as described in [12] (a model for wired networks) and weighted random geometric graphs as described in [13] (a model for wireless networks), respectively. Section IV provides simulations that confirm the results and Section V concludes the correspondence.

II. WIRED NETWORKS—THE WEIGHTED RANDOM GRAPH MODEL

Consider a single-source multiple-terminal transmission, where we denote the source s and the terminals $t_1, \ldots, t_l$. Let there be n relay nodes in the network. As shown in Fig. 2, the links between the relay nodes are bi-directional with equal capacity in both directions (a model along the same lines was considered in [14]). The source s has only outgoing links and the terminals $t_i, 1 \le i \le l$ only have incoming links.

Definition 1: We assume the following model on the graph.

1) The source node s is connected to each relay node i by a link of capacity C_{si} (it has only outgoing links).
2) Each relay node i is connected to another relay node j by a link of capacity C_{ij}. There exists a directed link from i to j of capacity C_{ij} and a directed link from j to i of capacity C_{ji} such that $C_{ji} = C_{ij}$.
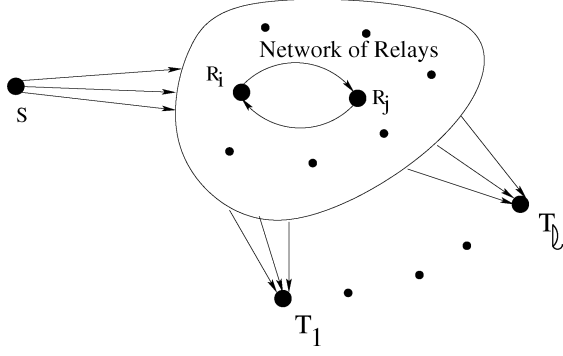
Fig. 2. Connectivity of the different types of nodes present in the network. The source node S has only outgoing edges whereas the terminals T_i's have only incoming edges. The inter-relay connections are all bi-directional.
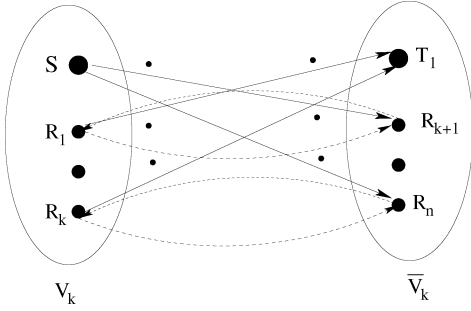

Fig. 3. There are $\binom{n}{k}$ cuts for which $|V_k| = k + 1$ and $|\bar{V}_k| = n - k + 1$. The figure shows one such cut. The broken lines depict the links between relay nodes. The solid lines depict the links between the source/terminals and the relay nodes.

3) Each relay node i is connected to each terminal node t_j by a link of capacity C_{it_j}. Terminal nodes have only incoming links.
4) All the link capacities are independent and identically distributed (i.i.d.) $\sim X, X \geq 0$, such that $E[X] < \infty$.

Henceforth, we shall refer to this model as the $\mathcal{G}^{\mathrm{WRG}}$ (WRG stands for weighted random graph) model, and our results shall be for random instances of it. Similar techniques were used in [15] in an algorithmic context.

A. Weighted Random Graph Model—The General Case

First consider the case $l = 1$, i.e., only one receiver terminal for simplicity. The results will generalize for larger l.

Lemma 1: Let G be a random instance of the model $\mathcal{G}^{\mathrm{WRG}}$ with $l = 1$. Let $\varphi(\theta) = E[e^{-\theta X}]$, for $\theta > 0$ and $E[X] = \mu$. Let

$$C_k = \sum_{i=k+1}^{n} C_{si} + \sum_{j=1}^{k} \sum_{i=k+1}^{n} C_{ji} + \sum_{i=1}^{k} C_{it_1}$$

be the capacity of a cut in G as shown in Fig. 3. The cut is defined by partitioning the vertex set V into a set V_k ($|V_k| = k + 1$) such that $s \in V_k$ and the complementary set $\bar{V}_k$ ($|\bar{V}_k| = n - k + 1$) such that $t_1 \in \bar{V}_k$ (thus, C_k is the capacity of a particular instance of a cut in which $|V_k| = k + 1$ and $|\bar{V}_k| = n - k + 1$). If $0 < \epsilon < 1$, then

$$P(C_k \leq (1 - \epsilon)E[C_k]) \leq e^{-(n+k(n-k))a(\epsilon)} \tag{1}$$

where, $a(\epsilon)$ is a function such that $\ln \varphi(\theta) + \theta(1 - \epsilon)\mu \leq -a(\epsilon) < 0$ for some $\theta > 0$.

Proof: Since

$$C_k = \sum_{i=k+1}^{n} C_{si} + \sum_{j=1}^{k} \sum_{i=k+1}^{n} C_{ji} + \sum_{i=1}^{k} C_{it_1}$$

where all the terms are distributed i.i.d $\sim X$, we obtain $E[C_k] = (n + k(n - k))\mu$.

Let $\theta > 0$. Then

$$
\begin{aligned}
P(C_k &\leq (1 - \epsilon)E[C_k]) \\
&= P(e^{-\theta C_k} \geq e^{-\theta(1-\epsilon)E[C_k]}) \\
&\leq \frac{E[e^{-\theta C_k}]}{e^{-\theta(1-\epsilon)E[C_k]}} \quad \text{(using Markov's inequality)} \\
&= [\varphi(\theta)]^{n+k(n-k)} \exp[\theta(1-\epsilon)(n + k(n - k))\mu] \\
&= \exp[(n + k(n - k))(\ln \varphi(\theta) + \theta(1 - \epsilon)\mu)] \\
&\leq \exp[-(n + k(n - k))a(\epsilon)]. \tag{2}
\end{aligned}
$$

It is possible to prove the existence of a function $a(\epsilon)$, such that for some $\theta > 0$ (see Theorem 6 in the Appendix)

$$\ln \varphi(\theta) + \theta(1 - \epsilon)\mu \leq -a(\epsilon) < 0, \qquad \text{for some } \theta > 0. \tag{3}$$

This proves the bound. □

Based on the above lemma we can obtain a corollary that bounds the probability that any cut in the graph falls below $(1 - \epsilon)$ times its mean value.

Corollary 1: Let G be a random instance of the model $\mathcal{G}^{\mathrm{WRG}}$ with $l = 1$. Let C_k be as defined in Lemma 1. Define A_k to be the event $\{C_k < E[C_k](1 - \epsilon)\}$. Then

$$P(\cup_k A_k) \leq 2 \exp[-na(\epsilon)](1 + \exp[-na(\epsilon)/2])^n. \tag{4}$$

Proof: From Lemma 1 we know that

$$P(A_k) \leq \exp[-(n + k(n - k))a(\epsilon)]. \tag{5}$$

There are a maximum of 2^n cuts in the graph. A union bound on all A_k's gives

$$
\begin{aligned}
P(\cup_k A_k) &\leq \sum_{k=0}^{n} \binom{n}{k} \exp[-(n + k(n - k))a(\epsilon)] \\
&\leq \exp[-na(\epsilon)] \sum_{k=0}^{n} \binom{n}{k} \exp[-k(n - k)a(\epsilon)] \\
&= \beta \sum_{k=0}^{n} \binom{n}{k} \beta^{n\frac{k}{n}(1-\frac{k}{n})}, \quad \text{where } \beta = \exp[-na(\epsilon)] < 1 \\
&= \beta \left[\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \beta^{n\frac{k}{n}(1-\frac{k}{n})} + \sum_{k=\lfloor n/2 \rfloor+1}^{n} \binom{n}{k} \beta^{n\frac{k}{n}(1-\frac{k}{n})} \right] \\
&\leq \beta \left[\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} \beta^{n\frac{k}{2n}} + \sum_{k=\lfloor n/2 \rfloor+1}^{n} \binom{n}{k} \beta^{n\frac{1}{2}(1-\frac{k}{n})} \right]
\end{aligned}
$$

since, when $\frac{k}{n} \in [0, 1/2]$, $\frac{k}{n}\left(1 - \frac{k}{n}\right) \geq \frac{k}{2n}$

and when $\frac{k}{n} \in [1/2, 1]$, $\frac{k}{n}\left(1 - \frac{k}{n}\right) \geq \frac{n-k}{2n}$

$$
\begin{aligned}
&\leq 2\beta[1 + \sqrt{\beta}]^n \\
&= 2 \exp[-na(\epsilon)][1 + \exp(-na(\epsilon)/2)]^n. \tag{6}
\end{aligned}
$$

□

Similarly, we can upper-bound the probability that a random instance of $\mathcal{G}^{\mathrm{WRG}}$ with $l = 1$, has a minimum cut $\leq (1 - \epsilon)E[C_0]$. Note that $E[C_0]$ is the expected value of the total flow to the nearest neighbors (i.e., nodes that can be reached in one hop) of the source. $E[C_n]$ is the expected value of the total flow from the nearest neighbors of the terminal to the terminal itself. By symmetry $E[C_n] = E[C_0]$.

Corollary 2: Let $C_{\min}(s \to t_1)$ denote the $s \to t_1$ minimum cut of a random instance of $\mathcal{G}^{\mathrm{WRG}}$ with $l = 1$. Then

$$P\left(C_{\min}(s \to t_1) \leq (1 - \epsilon)E[C_0]\right)$$
$$\leq 2\exp(-na(\epsilon))\left(1 + \exp(-na(\epsilon)/2)\right)^n. \quad (7)$$

Proof: Let us define $\tilde{A}_k$ to be the event $\{C_k < (1-\epsilon)E[C_0]\}$ and A_k to be the event that $\{C_k < (1-\epsilon)E[C_k]\}$. Recall that $E[C_0] = n\mu$ and $E[C_k] = (n + k(n-k))\mu$ so that, $E[C_k] \geq E[C_0]$ for $k \geq 0$. So

$$P(\tilde{A}_k) \leq P(A_k). \quad (8)$$

Thus,

$$P(C_{\min}(s \to t_1) \leq (1 - \epsilon)E[C_0]) = P(\cup_k \tilde{A}_k)$$
$$\leq \sum_k P(\tilde{A}_k)$$
$$\leq \sum_k P(A_k). \quad (9)$$

From Corollary 1 the result follows. $\square$

The above corollary bounds the probability that the $s \to t_1$ minimum cut falls below $(1 - \epsilon)E[C_0]$. In the general case, we have l terminals. Therefore, the probability that at least one of the $s \to t_i, 1 \leq i \leq l$ minimum cuts is less than $(1 - \epsilon)E[C_0]$ can again be bounded by a union bound.

Theorem 1: Consider the model specified in Definition 1. Let $a(\epsilon)$ be a function of ϵ, such that $\ln \varphi(\theta) + \theta(1 - \epsilon)\mu \leq -a(\epsilon) < 0$, for some $\theta > 0$. If $\epsilon < 1$, then with probability at least

$$1 - l \cdot 2\exp[-na(\epsilon)][1 + \exp(-na(\epsilon)/2)]^n$$

the network coding capacity $C_{s,t_1,\ldots,t_l}^{NC} > (1 - \epsilon)E[C_0]$.

Proof:

$$P(C_{s,t_1,\ldots,t_l}^{NC} \leq (1 - \epsilon)E[C_0])$$
$$= P(\cup_{i=1}^l \{C_{\min}(s \to t_i) \leq (1 - \epsilon)E[C_0]\})$$
$$\leq \sum_{i=1}^l P(C_{\min}(s \to t_i) \leq (1 - \epsilon)E[C_0]) \quad (10)$$
$$\leq l \cdot 2\exp(-na(\epsilon))(1 + \exp(-na(\epsilon)/2))^n$$
$$\Rightarrow P(C_{s,t_1,\ldots,t_l}^{NC} > (1 - \epsilon)E[C_0])$$
$$\geq 1 - l \cdot 2\exp(-na(\epsilon))(1 + \exp(-na(\epsilon)/2))^n. \quad \square$$

Theorem 2: Consider the model specified in Definition 1 with the additional condition that $\zeta(\theta) = E[e^{\theta X}] < \infty$ for $\theta \in [0, \theta']$. Let $b(\epsilon)$ be a function of ϵ such that $\ln \zeta(\theta) - \theta(1+\epsilon)\mu \leq -b(\epsilon) < 0$ for some $0 < \theta < \theta'$. If $\epsilon > 0$, then with probability at least $1 - e^{-nb(\epsilon)}$, the network coding capacity $C_{s,t_1,\ldots,t_l}^{NC} \leq (1 + \epsilon)n\mu$.

Proof: To show the upper bound on $P(C_{s,t_1,\ldots,t_l}^{NC} \geq (1+\epsilon)n\mu)$ it is sufficient to consider the cut separating the source from all the other nodes. Let $\theta > 0$

$$P(C_{s,t_1,\ldots,t_l}^{NC} \geq (1 + \epsilon)n\mu) \leq P(\sum_{i=1}^n C_{si} \geq (1 + \epsilon)n\mu)$$
$$\leq \frac{E[e^{\theta \sum_{i=1}^n C_{si}}]}{e^{\theta(1+\epsilon)n\mu}}$$
$$= \exp[n(\ln \zeta(\theta) - \theta(1 + \epsilon)\mu)]$$
$$\leq \exp[-nb(\epsilon)]. \quad (11)$$

It is possible to prove the existence of $b(\epsilon)$ so that for some θ

$$\ln \zeta(\theta) - \theta(1 + \epsilon)\mu < -b(\epsilon) < 0$$

(see Theorem 7 in the Appendix). $\square$

Together, Theorems 1 and 2 show a concentration of the network coding capacity around $n\mu$. We can specialize the above result to obtain more concrete statements about models where we fix the link capacity distribution. To illustrate the results more clearly we consider a model similar to the random graph $G(n, p)$ [12], where the link capacities are Bernoulli random variables with parameter p and a model where the link capacities are exponentially distributed with parameter λ.

B. Random Graph Model With Bernoulli Distributed Weights

Under this model we assume that the link capacities are distributed as Bernoulli random variables with parameter p.

$$\varphi(\theta) = 1 - p(1 - e^{-\theta})$$
$$\leq \exp(p(e^{-\theta} - 1)). \quad (12)$$

Thus, we have

$$\ln \varphi(\theta) + \theta(1 - \epsilon)\mu \leq p(e^{-\theta} - 1) + p\theta(1 - \epsilon). \quad (13)$$

The right-hand side (RHS) is minimized by $\theta = -\ln(1-\epsilon)$ (by simple differentiation and some algebra). So

$$-a(\epsilon) = -p(\epsilon + (1 - \epsilon)\ln(1 - \epsilon))$$
$$\leq -p\frac{\epsilon^2}{2}. \quad (14)$$

Now we are in a position to evaluate the bound in Corollary 2.

Theorem 3: Consider the model specified above with Bernoulli distributed link capacities with parameter p with l terminals. Let

$$\epsilon = \sqrt{\frac{4d\ln n}{np}}$$

with $d > 1$. If $\epsilon < 1$, then with probability $1 - O(l/n^{2d})$ the network coding capacity $C_{s,t_1,\ldots,t_l}^{NC} > (1 - \epsilon)np$ and with probability $1 - O(1/n^{8pd})$, $C_{s,t_1,\ldots,t_l}^{NC} \leq (1+\epsilon)np$.

Proof: Based on the preceding derivation , we can evaluate the RHS of the bound in Corollary 2 with

$$\epsilon = \sqrt{\frac{4d\ln n}{np}}.$$

Therefore,

$$P(C_{\min}(s \to t_i) \leq (1 - \epsilon)np) \leq \frac{2}{n^{2d}}\left[1 + \frac{1}{n^d}\right]^n$$
$$= \frac{2}{n^{2d}}\left[\sum_{k=0}^n \binom{n}{k}\left(\frac{1}{n^d}\right)^k\right]$$
$$\leq \frac{2}{n^{2d}}\sum_{k=0}^\infty \left(\frac{n}{n^d}\right)^k$$
$$\leq \frac{2}{n^{2d} - n^{1+d}}, \quad \text{since } d > 1$$
$$\approx O\left(\frac{1}{n^{2d}}\right). \quad (15)$$

So as in Theorem 1

$$P(C_{s,t_1,\ldots,t_l}^{NC} \leq (1-\epsilon)np) = P(\cup_{i=1}^{l} \{C_{\min}(s \rightarrow t_i) \leq (1-\epsilon)np\})$$

$$\leq \sum_{i=1}^{l} P(C_{\min}(s \rightarrow t_i) \leq (1-\epsilon)np)$$

$$\approx O\left(\frac{l}{n^{2d}}\right). \tag{16}$$

The upper bound on $P(C_{s,t_1,\ldots,t_l}^{NC})$ simply reduces to a Chernoff bound for Bernoulli random variables [16]

$$P(C_{s,t_1,\ldots,t_l}^{NC} \geq (1+\epsilon)np)$$

$$\leq P(\sum_{i=1}^{n} C_{si} \geq (1+\epsilon)np)$$

$$\leq P(|\sum_{i=1}^{n} C_{si} - np| \geq np\epsilon)$$

$$\leq 2e^{-2np^2\epsilon^2} \text{ By a simple Chernoff Bound [16]}$$

$$= O\left(\frac{1}{n^{8pd}}\right). \tag{17}$$

□

C. Random Graph Model With Exponentially Distributed Weights

Here we assume that the capacity of each link is distributed as an exponential random variable with mean λ. Thus, in this case

$$\varphi(\theta) = \int_0^{\infty} e^{-\theta x} \lambda e^{-\lambda x} dx$$

$$= \frac{\lambda}{\theta + \lambda}. \tag{18}$$

Therefore, we can write

$$\ln \varphi(\theta) + \theta(1-\epsilon)\frac{1}{\lambda} = -\ln\left(\frac{\theta + \lambda}{\lambda}\right) + \frac{\theta}{\lambda}(1-\epsilon). \tag{19}$$

The RHS is minimized by $\theta = \frac{\lambda\epsilon}{1-\epsilon}$ and so we can obtain

$$-a(\epsilon) = \epsilon + \ln(1-\epsilon)$$

$$\leq -\frac{\epsilon^2}{2}. \tag{20}$$

It is now straightforward to derive an upper bound on the probability that the $s \rightarrow t_i$ (for some i) minimum cut of a random instance of the graph falls below $(1-\epsilon)\frac{n}{\lambda}$ using Corollary 2. Subsequently, we can obtain the bound on the probability that the network coding capacity falls below $(1-\epsilon)\frac{n}{\lambda}$.

Theorem 4: Consider the model specified above with exponentially distributed link capacities with parameter λ. Let

$$\epsilon = \sqrt{\frac{4d \ln n}{n}}$$

with $d > 1$. If $\epsilon < 1$, then with probability $1 - O(l/n^{2d})$, the network coding capacity $C_{s,t_1,\ldots,t_l}^{NC} > (1-\epsilon)\frac{n}{\lambda}$ and with probability $1 - O(1/n^{\frac{4d}{5}})$, $C_{s,t_1,\ldots,t_l}^{NC} \leq (1+\epsilon)n/\lambda$.

Proof: The first part of the claim is obvious by simply utilizing Corollary 2 with

$$\epsilon = \sqrt{\frac{4d \ln n}{n}}.$$

For the second part of the claim, we need to produce a suitable $b(\epsilon)$ as in Theorem 2. It can be easily verified that

$$E[e^{\theta X}] = \frac{\lambda}{\lambda - \theta}, \qquad \theta < \lambda.$$

It can be also be shown that $\left(\frac{\lambda}{\lambda - \theta}\right)^n e^{-n\theta \frac{(1+\epsilon)}{\lambda}}$ is minimized by setting $\theta = \lambda \frac{\epsilon}{1+\epsilon}$. After some manipulation we can obtain

$$P(C_{s,t_1,\ldots,t_l}^{NC} \geq (1+\epsilon)\frac{n}{\lambda}) \leq e^{n(\ln(1+\epsilon)-\epsilon)}. \tag{21}$$

We further observe that

$$\ln(1+\epsilon) - \epsilon = \ln\left(\frac{1+\epsilon}{e^\epsilon}\right)$$

$$\leq \ln\left(\frac{1+\epsilon}{1+\epsilon+\epsilon^2/2}\right)$$

$$= \ln\left(1 - \frac{\epsilon^2}{2+2\epsilon+\epsilon^2}\right)$$

$$\leq -\frac{\epsilon^2}{2+2\epsilon+\epsilon^2}$$

$$\leq -\epsilon^2/5, \qquad \text{since } \epsilon < 1. \tag{22}$$

Finally, we have

$$P(C_{s,t_1,\ldots,t_l}^{NC} \geq (1+\epsilon)\frac{n}{\lambda}) \leq e^{-n\epsilon^2/5} \tag{23}$$

and the result follows by substituting the appropriate value of ϵ. □

In both the bounds above, for higher d, the probability that the network coding capacity falls below $(1-\epsilon)n\mu$ is lower. At the same time, a higher d causes ϵ to increase. There is tradeoff between these two parameters that decides the tightness of the bound. We remark at this point that the above results are general in the sense that they can be re-derived for link capacity distributions that are not the same for source–relay, relay–relay, and relay–terminal. Under moderate conditions on the distributions the high-probability bound on the capacity would continue to hold.

Thus, in a weighted random graph there is a strong case for using network coding since the network coding capacity is with high probability the expected total flow to the nearest neighbors of the source. On average we shall not lose much because of the random nature of the graph. Note that for a wired network, the capacity of the single-source multiple-terminal information transfer (i.e., the network coding capacity) is actually achievable. There exists a network code that can be found in polynomial time [5] that achieves this capacity. However, the result above is an "existence result," we do not provide an algorithm for finding the network code.

While the minimum of the max-flows from s to $t_i, 1 \leq i \leq l$ is greater than $(1-\epsilon)n\mu$ with high probability, the extent to which network coding is actually required to achieve this capacity has not been investigated in this work. In many cases investigated by other authors [17], routing has been found to perform reasonably well.

III. *Ad-Hoc* Wireless Networks—The Weighted Random Geometric Graph Model

At first, one might consider network coding inappropriate for a distributed wireless network because transmissions from relatively simple distributed wireless nodes (such as wireless sensor networks) are typically omnidirectional, precluding the transmission of different bits from the same node to different links at the same instant of time and in the same frequency band. However, communication has been shown to dominate all other sources of energy consumption in a sensor network. So, in order to save power, wireless sensor nodes typically will go into a sleep mode from which they periodically awaken to listen for transmissions. Furthermore, nodes negotiate time slots and frequency slots with which to communicate for both transmission and reception, also with a desire to minimize power drain. Under these practical assumptions, network coding solutions would be possible to
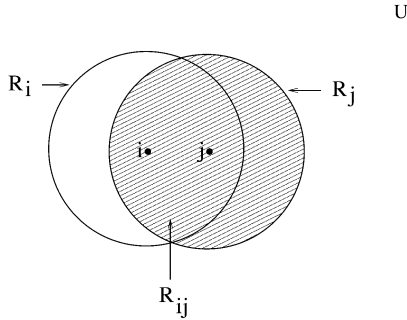
Fig. 4.　If a third node k is connected to j then it surely falls in the shaded area R_j. If it falls in $R_{ij} = R_i \cap R_j$ then it is also connected to i.

implement in a wireless network. Observe that many sensor networks would need a sensor node to periodically send data to a set of other nodes. Network coding might provide a viable solution to the low-energy single-source multiple terminal information transfer problem where distinct edges correspond to different frequencies or time slots in a single transmission frame.

A. Weighted Random Geometric Graph Model

The weighted random graph model of Section II is not a realistic model for a wireless *ad-hoc* network or sensor network because it places edges between nodes independent of the distance between them. In fact, distance is a critical factor in determining the connectivity properties of a wireless network since propagation losses cause the power of the signal to fall off as $r^{-\alpha}$ where r is the distance between the nodes and $2 \leq \alpha \leq 4$. Thus, we have to use a different model for wireless networks.

Definition 2:　The following model is assumed for the wireless network.

1) The source, terminals, and the relay nodes are scattered independently and uniformly on the unit square $[0, 1]^2$.
2) The source node s is connected to each relay node i by a link of capacity C_{si} (it has only outgoing links).
3) Each relay node i is connected to another relay node j by a link of capacity C_{ij}. There exists a directed link from i to j of capacity C_{ij} and a directed link from j to i of capacity C_{ji} such that $C_{ji} = C_{ij}$.
4) Each relay node i is connected to each terminal node t_j by a link of capacity C_{it_j} (it has only incoming links).
5) Interference effects are neglected.
6) Let the distance between nodes i and j be denoted $d(i, j)$. The link capacity between nodes i and j, C_{ij} is assumed to have the following form:

$$C_{ij} = \begin{cases} 1, & \text{if } d(i, j) \leq r \\ 0, & \text{otherwise.} \end{cases} \qquad (24)$$

This model is similar to a class of graphs known in mathematical literature as Random Geometric Graphs [13].

Henceforth, we shall refer to the above model as the $\mathcal{G}^{\mathrm{WRGG}}$ (WRGG stands for Weighted Random Geometric Graph) model with parameter r. This model is fundamentally different from the WRG model because of the inherent dependencies in the connectivity among different nodes. This is discussed in more detail in the discussion that follows. Consider three vertices i, j, k in a graph from the above model as illustrated in Fig. 4. The region R_i is the circle centered at i. Since node placements are i.i.d. uniform, it follows that

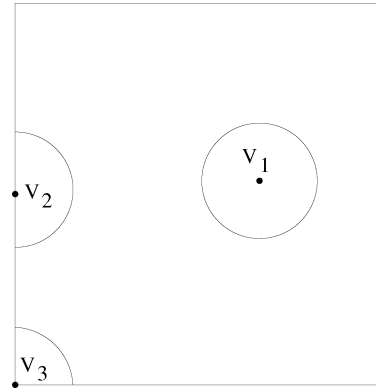$$P[i \rightarrow k] = P[i \rightarrow j]. \qquad (25)$$

Fig. 5.　Different coverage area that nodes may have depending on their position on the unit square. Node V_1 has the maximum coverage area as it lies sufficiently in the interior followed by V_2 that lies on an edge and V_3 that lies on a corner.

Now consider the probability, $P[i \rightarrow k | i \rightarrow j, k \rightarrow j]$. For simplicity of explanation, we neglect the effects arising from the placement of nodes near the boundaries in the following argument. From Fig. 4

$$P[i \rightarrow k | i \rightarrow j, k \rightarrow j] = \frac{\mathrm{Area}(R_{ij})}{\mathrm{Area}(R_j)}. \qquad (26)$$

To see this, observe that given that $i \rightarrow j$ and $k \rightarrow j$, we know that $i \in R_{ij}$ and $k \in R_j$, respectively. Thus, the only way in which i can be connected to k is if $k \in R_{ij}$. Also note that in general

$$\frac{\mathrm{Area}(R_{ij})}{\mathrm{Area}(R_j)} \neq \frac{\mathrm{Area}(R_i)}{\mathrm{Area}(U)} \qquad (27)$$

which, in turn, means that

$$P[i \rightarrow k | i \rightarrow j, k \rightarrow j] \neq P[i \rightarrow k]. \qquad (28)$$

The analysis is further complicated by the fact that the connectivity of a node in the case of the WRGG is position dependent. If either the source or any of the terminal nodes is located close to the boundary, it is highly probable that the max-flow is much lower compared to the situation when they are located sufficiently in the interior. As a result, unlike the case of the WRG, the network coding capacity does not concentrate about a particular value. However, even in this case we can provide high probability statements about the behavior of the network coding capacity. This analysis only provides an upper bound on the amount of information flow possible, in part because max-flow bounds are upper bounds in general for wireless systems [18, Ch. 14], and in part because interference is ignored.

B. A High-Probability Result

We proceed by demonstrating that the WRGG can be treated in a manner very similar to the WRG case under certain conditions. Consider Fig. 5. Node V_1 that lies in the interior has coverage area $\mu = \pi r^2$. On the other hand, node V_2 lying on an edge has coverage area $\pi r^2/2$ and node V_3 lying on a corner has a coverage region $\mu' = \pi r^2/4$. The event that either the source or one of the terminals lies in a corner occurs with constant probability so in general any high probability result about the capacity will be dominated by this event.

Now consider the hypothetical situation in which all nodes adjust their transmit power so that the area of their region of coverage $= \mu' = \pi r^2/4$. This would require the nodes lying strictly in the interior of the unit square to reduce their power. Note that μ' can be interpreted as a probability since the square is assumed to be of unit area and hence $0 \leq \mu' \leq 1$. If the nodes operate with a larger power, the max-flow

can only improve. Let $i, j_1, j_2, \ldots, j_k$ be a set of nodes. Let $\mathrm{pos}(k)$ be the random variable denoting the position of a node k. Then

$$P[C_{ij_1} = z_1, C_{ij_2} = z_2, \ldots, C_{ij_k} = z_k]$$

$$= \int_{[0,1]^2} f_{\mathrm{pos}(i)}(A)$$
$$\times P[C_{ij_1} = z_1, C_{ij_2} = z_2, \ldots, C_{ij_k} = z_k | \mathrm{pos}(i) = A] dA$$

$$= \int_{[0,1]^2} \Pi_{\alpha=1}^{k} P[C_{ij_\alpha} = z_\alpha | \mathrm{pos}(i) = A] dA$$

by the conditional independence of C_{ij_α}'s given i's position

$$= \int_{[0,1]^2} \Pi_{\alpha=1}^{k} (\mu')^{z_\alpha} (1 - \mu')^{1-z_\alpha} dA$$

$$= \Pi_{\alpha=1}^{k} (\mu')^{z_\alpha} (1 - \mu')^{1-z_\alpha}$$

$$= \Pi_{\alpha=1}^{k} P[C_{ij_\alpha} = z_\alpha]. \qquad (29)$$

This demonstrates that the capacities of the outgoing links from any particular node are independent. By a very similar argument it can be shown that the capacities of the incoming links into a particular node are independent as well. The assumption that the connectivity of node i is the same irrespective of its location on the square is crucial to the above observation.

Lemma 2: Let G be a random instance of $\mathcal{G}^{\mathrm{WRGG}}$ with $l = 1$. Let μ' be the probability that two nodes are connected under the hypothetical assumption that all nodes reduce their power as explained above. Let

$$C_k = \sum_{i=k+1}^{n} C_{si} + \sum_{j=1}^{k} \sum_{i=k+1}^{n} C_{ji} + \sum_{i=1}^{k} C_{it_1}$$

be the capacity of a cut in G as shown in Fig. 3. The cut is defined by partitioning the vertex set V into a set $V_k (|V_k| = k + 1)$ such that $s \in V_k$ and the complementary set $\bar{V}_k (|\bar{V}_k| = n - k + 1)$ such that $t_1 \in \bar{V}_k$. Then

$$P[C_k \leq (1 - \epsilon)(n + k(n - k))\mu'] \leq e^{-(n+k(n-k))\mu'\frac{\epsilon^2}{2}}. \qquad (30)$$

Proof: Consider

$$C_k = \sum_{i=k+1}^{n} C_{si} + \sum_{j=1}^{k} \sum_{i=k+1}^{n} C_{ji} + \sum_{i=1}^{k} C_{it_1}. \qquad (31)$$

By the argument presented earlier, outgoing/incoming links from/to any particular node are independent. In addition, two links that have no node in common are anyway independent. Thus, all the terms in the above sum are independent. Therefore, bounding the probability that the cut falls below $(1 - \epsilon)(n + k(n - k))\mu'$ reduces to the situation in Lemma 1. The theorem follows from Lemma 1 and the discussion in Section II-C. $\qquad \square$

It is now straightforward to conclude the high-probability statement on the network coding capacity for the wireless case, based on arguments similar to the ones made in Theorem 3.

Theorem 5: Let G be a random instance of $\mathcal{G}^{\mathrm{WRGG}}$, with parameter r. Let $\mu' = \pi r^2/4$ (since the square is of unit area we can treat μ' as a probability) and

$$\epsilon = \sqrt{\frac{4d \ln n}{n \mu'}}$$

with $d > 1$. If $\epsilon < 1$, then with probability $1 - O(l/n^{2d})$, the network coding capacity $C_{s,t_1,\ldots,t_l}^{NC} > (1 - \epsilon)n\mu'$.

Proof: The proof follows by making the hypothetical assumption that all nodes adjust their power so that their coverage area $= \mu' = \pi r^2/4$. Then Lemma 2 holds and the stated result holds by a discussion identical to the one presented in the proof of Theorem 3. In reality, of
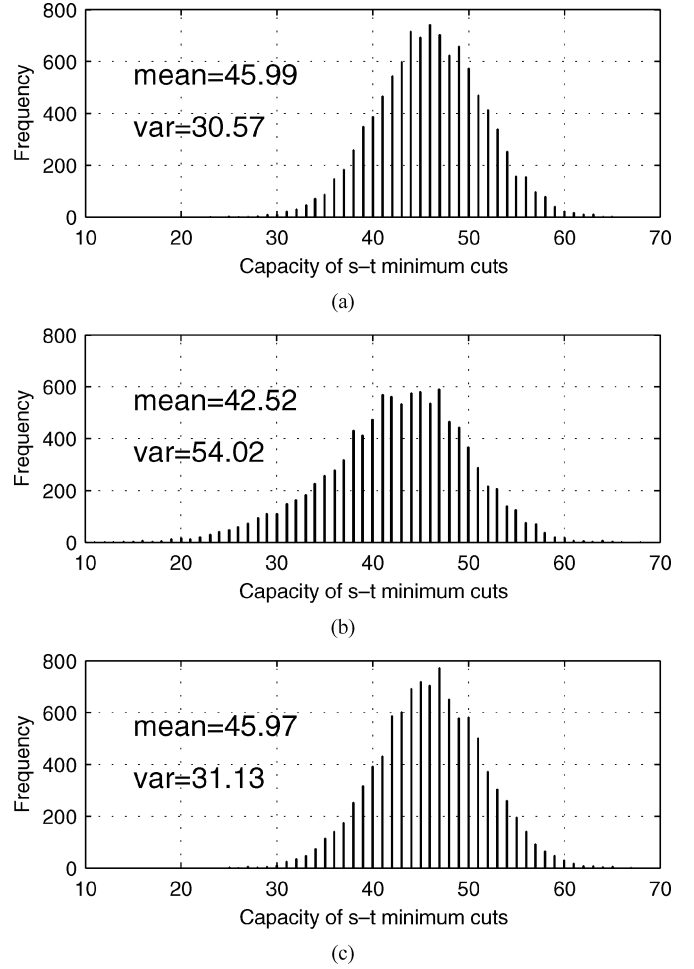

Fig. 6. Histograms of $s - t$ minimum cuts for (a) weighted random graphs with Bernoulli links, (b) weighted random geometric graphs with parameter $r = 0.1262$, and (c) weighted random geometric graphs with $r = 0.1262$ and toroidal distance metrics.

course, many nodes shall have coverage that exceeds μ'. However, this can only cause the minimum cut to improve. Thus, the lower bound on the probability still holds. $\qquad \square$

It is important to note that this is essentially the best that one can hope for since with constant probability $= 1 - (1 - 4\beta)^{l+1}$ either the source or one of the terminals lies in a region of area β near the corners of the unit square. One can impose restrictions on the positions of the sources and the terminals, e.g., force their positions to be sufficiently within the interior of the unit square, etc. One can also consider scenarios where the nodes at the boundary use directional antennas so that their connectivity is not reduced. However, in this work we have not considered those possibilities.

IV. SIMULATIONS AND DISCUSSION

We performed simulations for the weighted random graph with Bernoulli ($p = 0.05$) distributed link capacities, and the weighted random geometric graph with parameter $r = 0.1262$. The number of nodes was chosen to be $n = 1000$. The value of r was chosen so that $p \approx \pi r^2$. Different nodes were declared to be the source and terminal, respectively, and a histogram of the $s - t$ minimum cuts was generated. These results are presented in Fig. 6. Note that the histogram of Fig. 6(b) extends more to the left than the one in Fig. 6(a). The results are in agreement with the theoretically derived results. Note that the histogram of Fig. 6(b) extends to about $10 \approx 45.99/4$.

This means that with high probability, the minimum cut is greater that 10 which is what we have predicted.

To make the inter-node distances more homogeneous, we defined a different toroidal metric [19] for the distance between two nodes. With a toroidal distance metric, nodes at one boundary of the square are considered to be close to the nodes at the opposite boundary, i.e., nodes at the left boundary of a square can have links with nodes at the right boundary, and nodes near the top of the square can have links with those at the bottom. The histogram of the $s - t$ minimum cuts is shown in Fig. 6(c). Note that now the histogram looks very similar to Fig. 6(a). This suggests, that at least for this case, the statistics of the wired network and wireless networks would be similar. As we have shown before, the capacity is basically dominated by the number of nearest neighbors of the source and the terminals. Thus, in practice, to avoid the boundary effects it should be sufficient to choose the source and the terminals to be sufficiently toward the center of the region.

V. Conclusion

We presented high-probability results for the capacity of network coding for two different classes of random networks, namely, the weighted random graph model (modeling wired networks) and the weighted random geometric graph model (modeling wireless networks). For the case of wired networks with a dense collection of relay nodes, the network coding capacity is dominated by the number of nearest neighbors of the source and terminal nodes. In the wireless case, boundary effects cause the nodes near the boundary to have fewer neighbors.

While we have shown high-probability results about the network coding capacity, the extent to which network coding is actually required to achieve it has not been investigated in this work. If the whole topology of the network is known, in many cases routing may perform as well. However, it is important to keep in mind that network coding can be implemented in a distributed fashion [6] and provides a robust solution to the multicast problem as against a routing solution that is equivalent to the hard problem of Steiner tree-packing [20].

Appendix

The proof of the following theorem is based on the argument in [21, pp. 72–73].

Theorem 6: Let $X \geq 0$ be a random variable, such that $E[X] = \mu < \infty$. Let $\varphi(\theta) = E[e^{-\theta X}]$. Then, for $\epsilon > 0$, there exists a $\theta > 0$, such that

$$\ln \varphi(\theta) + \theta(1 - \epsilon)\mu < 0. \tag{32}$$

Proof: Let $\kappa(\theta) = \ln \varphi(\theta)$. We have

$$\kappa(0) = 0 \tag{33}$$

$$\kappa(\theta) + \theta(1 - \epsilon)\mu = \int_0^\theta \kappa'(x) + (1 - \epsilon)\mu \, dx. \tag{34}$$

Thus, it is enough to show that $\kappa'(x)$ exists and $\kappa'(\theta) \to -\mu$ as $\theta \to 0$. For $h \geq 0, x \geq 0, |e^{-hx} - 1| \leq hx$. Define

$$Y_h = \frac{e^{-(\theta+h)X} - e^{-\theta X}}{h}. \tag{35}$$

Note that

$$|Y_h| \leq |e^{-\theta X}| \frac{|e^{-hX} - 1|}{h}$$
$$\leq |e^{-\theta X}|X$$
$$\leq X. \tag{36}$$

We know that $E[X] < \infty$. It is easy to see that

$$\lim_{h \to 0} Y_h = e^{-\theta X} \lim_{h \to 0} \frac{e^{-hX} - 1}{h}$$
$$= -Xe^{-\theta X}. \tag{37}$$

Therefore, using the dominated convergence theorem

$$\varphi'(\theta) = \lim_{h \to 0} \frac{E[e^{-(\theta+h)X}] - E[e^{-\theta X}]}{h}$$
$$= -E[Xe^{-\theta X}]. \tag{38}$$

This implies that $\kappa'(\theta) = \frac{\varphi'(\theta)}{\varphi(\theta)}$. Similarly, we can see that

- $Z_\theta = e^{-\theta X} \leq 1$ and $\lim_{\theta \to 0} Z_\theta = 1$ and thus, $E[e^{-\theta X}] \to 1$ as $\theta \to 0$;
- $Z_\theta = Xe^{-\theta X} \leq X$ and $\lim_{\theta \to 0} Z_\theta = X$. We are given $E[X] < \infty$ and thus, $E[Xe^{-\theta X}] \to E[X]$ as $\theta \to 0$.

The above equations imply

$$-\frac{E[Xe^{-\theta X}]}{E[e^{-\theta X}]} \to -EX = -\mu, \qquad \text{as } \theta \to 0. \tag{39}$$

This shows the existence of a θ, such that $\kappa(\theta) + \theta(1 - \epsilon)\mu < 0$. $\square$

Theorem 7: Let $X \geq 0$ be a random variable, such that $E[X] = \mu$ and $\zeta(\theta') = E[e^{\theta' X}] < \infty$ for some $\theta' > 0$. Then, for $\epsilon > 0$, there exists a $\theta > 0$ such that

$$\ln \zeta(\theta) - \theta(1 + \epsilon)\mu < 0. \tag{40}$$

Proof: As the proof of the preceding theorem, let $\kappa(\theta) = \ln \zeta(\theta)$.

$$\kappa(0) = 1 \tag{41}$$

$$\kappa(\theta) - \theta(1 + \epsilon)\mu = \int_0^\theta \kappa'(x) - (1 + \epsilon)\mu dx. \tag{42}$$

It is enough to show that $\kappa'(x)$ exists and $\kappa'(\theta) \to \mu$ as $\theta \to 0$. Let $0 < \theta < \theta'$. Since we have assumed the existence of $E[e^{\theta' X}]$, we know that $\zeta'(\theta)$ exists [21] and

$$\zeta'(\theta) = E[Xe^{\theta X}]. \tag{43}$$

This implies that $\kappa'(\theta) = \frac{\zeta'(\theta)}{\zeta(\theta)}$. Now

$$e^{\theta' X} \geq e^{\theta X} \to 1, \qquad \text{as } \theta \to 0 \tag{44}$$

$$Xe^{(\theta+\epsilon_1)X} \geq Xe^{\theta X} \to X, \qquad \text{as } \theta \to 0. \tag{45}$$

Here $\epsilon_1 > 0$ is chosen so that $\theta + 2\epsilon_1 < \theta'$. In addition, $E[e^{\theta' X}] < \infty$. For upper-bounding $E[Xe^{(\theta+\epsilon_1)X}]$ we have the following argument. Let M be such that $M \leq e^{\epsilon_1 M}$.

$$E[Xe^{(\theta+\epsilon_1)X}]$$
$$= E[Xe^{(\theta+\epsilon_1)X}1_{\{X \leq M\}}] + E[Xe^{(\theta+\epsilon_1)X}1_{\{X > M\}}]$$
$$\leq Me^{(\theta+\epsilon_1)M} + E[e^{(\theta+2\epsilon_1)X}]$$
$$< \infty. \tag{46}$$

Thus, by the Dominated Convergence Theorem, we obtain

$$E[e^{\theta X}] \to 1 \tag{47}$$
$$E[Xe^{\theta X}] \to X. \tag{48}$$

The above equations imply

$$\frac{E[Xe^{\theta X}]}{E[e^{\theta X}]} \to E[X], \qquad \text{as } \theta \to 0. \tag{49}$$

This proves the existence of a θ such that

$$\ln \zeta(\theta) - \theta(1 + \epsilon)\mu < 0. \tag{50}$$

REFERENCES

[1] R. K. Ahuja, T. L. Maganti, and J. B. Orlin, *Network Flows:Theory, Algorithms and Applications*. Englewood Cliffs, NJ: Prentice-Hall, 1993.

[2] R. Ahlswede, N. Cai, S.-Y. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[3] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[4] R. Koetter and M. Médard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.

[5] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Trans. Inf. Theory*, submitted for publication.

[6] T. Ho, R. Koetter, M. Médard, M. Effros, J. Shi, and D. Karger, "Toward a random operation of networks," *IEEE Trans. Inf. Theory*, submitted for publication.

[7] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. 41st Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2003.

[8] M. Médard, M. Effros, T. Ho, and D. Karger, "On coding for nonmulticast networks," in *Proc. 41st Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2003.

[9] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2745–2759, Aug. 2005.

[10] T. Ho, M. Médard, M. Effros, and R. Koetter, "Network coding for correlated sources," in *Proc. Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, Mar, 2004.

[11] A. Ramamoorthy, K. Jain, P. A. Chou, and M. Effros, "Separating distributed source coding from network coding," in *Proc. 42nd Allerton Conf. Communication, Control, and Computing*, Monticello, IL, Oct. 2004.

[12] B. Bollobas, *Random Graphs*. London/New York: Academic, 1985.

[13] M. Penrose, *Random Geometric Graphs*. Oxford, U.K.: Oxford Univ. Press, 2003.

[14] G. Kramer and S. Savari, "On networks of two-way channels," in *Proc. DIMACS Workshop on Algebraic Coding Theory and Information Theory*, Piscataway, NJ, Dec. 2003.

[15] D. R. Karger, "Random sampling in cut, flow and network design problems," *Math. of Oper. Res.*, vol. 24, no. 2, pp. 0383–0413, 1999.

[16] R. Motwani and P. Raghavan, *Randomized Algorithms*. Cambridge, U.K.: Cambridge Univ. Press, 1995.

[17] Y. Wu, P. A. Chou, and K. Jain, "A comparison of network coding and tree packing," in *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, Jun./Jul. 2004, p. 143.

[18] T. Cover and J. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[19] C. Bettstetter, "On the minimum node degree and connectivity of a wireless multihop network," in *Proc. MobiHoc*, Lausanne, Switzerland, 2002, pp. 80–91.

[20] K. Jain, M. Mahdian, and M. R. Salavatipour, "Packing Steiner trees," in *Proc. 14th Annu. ACM-SIAM Symp. Discrete Algorithms*, Baltimore, MD, 2003, pp. 266–274.

[21] R. Durrett, *Probability: Theory and Examples*, 2nd ed: Duxbury, 1995.

An Improvement to the Bit Stuffing Algorithm

Sharon Aviran, Paul H. Siegel, *Fellow, IEEE*, and
Jack Keil Wolf, *Life Fellow, IEEE*

Abstract—The bit stuffing algorithm is a technique for coding constrained sequences by the insertion of bits into an arbitrary data sequence. This approach was previously introduced and applied to (d, k) constrained codes. Results show that the maximum average rate of the bit stuffing code achieves capacity when $k = d + 1$ or $k = \infty$, while it is suboptimal for all other (d, k) pairs. Furthermore, this technique was generalized to produce codes with an average rate that achieves capacity for all (d, k) pairs. However, this extension results in a more complicated scheme. This correspondence proposes a modification to the bit stuffing algorithm that maintains its simplicity. We show analytically that the proposed algorithm achieves improved average rates over bit stuffing for most (d, k) constraints. We further determine all constraints for which this scheme produces codes with an average rate equal to the Shannon capacity.

Index Terms—Bit-stuffing encoder, (d, k)-constrained systems, Shannon capacity.

I. INTRODUCTION

A binary sequence satisfies a run-length-limited (RLL) (d, k) constraint if any run of consecutive zeros is of length at most k and any two successive ones are separated by a run of consecutive zeros of length at least d. Such sequences are called (d, k)-*sequences* and are commonly used in magnetic and optical recording [1], [2]. The (d, k) constraint is used in order to solve two problems that arise when performing peak detection: d minimizes intersymbol interference and k assists in timing recovery. Relevant (d, k) pairs range over all integers d, k, such that $0 \le d < k \le \infty$.

One can use a labeled directed graph to generate all possible (d, k)-sequences by reading off the labels along paths in the graph. This graph is referred to as a (d, k) *constraint graph*. A graph that produces these sequences for $k < \infty$ is shown in Fig. 1.

Let $N_{d,k}(n)$ be the number of distinct (d, k)-sequences of length n. The *Shannon capacity* of a (d, k) constraint is defined as

$$C(d, k) = \lim_{n \to \infty} \frac{\log_2 N_{d,k}(n)}{n}.$$

The capacity can be computed by applying a more general result derived by Shannon [3]. It was shown (see, e.g., [1]) that $C(d, k) = \log_2 \lambda_{d,k}$, where $\lambda_{d,k}$ is the largest real eigenvalue of the adjacency matrix of the constraint graph. Therefore, $\lambda_{d,k}$ is the largest real root of the characteristic polynomial of the matrix $P_{d,k}(z)$, which takes the form

$$P_{d,k}(z) = \begin{cases} z^{k+1} - \sum_{j=0}^{k-d} z^j, & k \text{ is finite} \\ z^{d+1} - z^d - 1, & k = \infty. \end{cases}$$

It was further shown that for all values of d and k the capacity exists and that $\lambda_{d,k} \in (1, 2)$ for all (d, k) pairs such that $(d, k) \ne (0, \infty)$.