Capacity Scalability of Batched Network Codes on Line Networks With Outage Links

Yanyan Dong, Jie Wang, Shenghao Yang and Raymond W. Yeung

***Abstract*—Batched network codes are a general framework for network communications, and include both store-and-forward and random linear network coding as special inner codes. The capacity scalability of batched network codes on line networks with the network length has been studied where the network links are discrete memoryless channels (DMCs). Real-world wireless communication channels are more complex than DMCs. We propose an outage link model to approximate the behavior of practical wireless communication devices for slow fading channels and study the capacity scalability of batched network codes in line networks with outage links. For store-and-forward inner codes, the capacity of batched network codes scales in $\Theta(1/L)$ when the network length L goes large under certain technical conditions on the outage links. For random linear inner codes, the capacity of batched network codes scales in $\Theta(1/\ln L)$ or $\Theta(1)$ under different constraints for the coding parameters. Our results demonstrate that the throughput gain of network coding over store-and-forward for multihop networks with wireless links can be unbounded.**

I. Introduction

Network coding at the intermediate network nodes can outperform store-and-forward used in the traditional network communication protocols like TCP/IP in multicast communications [1]–[3]. Random linear network coding (RLNC) provides a decentralized approach for network coding and achieves the multicast capacity of networks with packet loss in a broad setting [4]–[11]. Batched network codes were originally proposed as efficient RLNC schemes for multi-hop wireless networks [12]–[17]. The advantages of batched network coding for multihop line networks with packet loss have been discussed in [18]. Batched network coding has been extended to include more general discrete memoryless channels (DMCs) [19], [20]. For line networks formed by DMCs, the capacity scalability of batched network codes with the network length has been studied in [19]–[22].

Real-world wireless communication channels are more complex than memoryless channels with known channel statistics due to interference, multipath fading, mobility, etc. For slow (quasi-static) fading channels, the channel gain is random but remains constant for the duration of each codeword [23], [24]. The *outage probability* of a real value $r \geq 0$ is the probability that the channel gain prevents reliable communication at rate r within a short period. Without a lower bound on the channel gain, the Shannon capacity of a slow fading channel is zero as no positive rates can be achieved reliably.

Y. Dong and S. Yang are with the School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, Shenzhen, China. J. Wang is with the H. Milton Stewart School of Industrial and Systems Engineering, Georgia Institute of Technology, Atlanta, USA. R. W. Yeung is with the Institute of Network Coding and the Department of Information Engineering, The Chinese University of Hong Kong, Hong Kong, China.

Due to the essential difference in the channel characteristics, the existing capacity scalability results of batched network codes for line networks with DMCs cannot be applied on line networks with slow fading channels. To shed light on the latter, we study in this paper a line network formed by *outage links* that approximate the behavior of practical wireless communication devices for slow fading channels. For many network resource allocation researches (see, e.g., [25], [26]), a network link model has a fixed capacity (bandwidth) so that reliable communication is possible only for rates lower than the capacity. This traditional link model approximates the behavior of using a discrete memoryless channel. Our outage link model generalizes this link model to incorporate slow fading channels. Specifically, an outage link is associated with a non-decreasing function called an *outage function*, which tells the outage probability of communication at a rate.

We study batched network codes for line networks with identical outage links and focus on the cases where the outage function is *non-degraded* (i.e. the outage probability is positive for all positive rates). A batched network code comprises an outer code and an inner code. The outer code encodes the data into a sequence of batches, each of which is a number of coded symbols. The inner code at each node re-encodes the symbols belonging to the same batch for transmission to the next node. For the given inner codes at all the nodes, the end-to-end operation of the network on a batch by the series of the inner code operations is a channel with a batch as the input. The outer code acts as a channel code for this "batch channel" and ensures end-to-end reliability.

A batched network code can be regarded as a general framework for network communications that includes both store-and-forward and random linear coding (RLNC) as special inner codes. We focus on the maximum achievable rate (capacity) of batched network codes for different kinds of inner codes. Under certain conditions on the outage functions, the capacity of batched network codes with store-and-forward inner codes scales in $\Theta(1/L)$ when the network length L tends to infinity. For the random linear inner codes, the capacity of batched network codes scales in $\Theta(1/\ln L)$ or even $\Theta(1)$ under different conditions on the inner code parameters. The formula of the achievable rates of batched codes are obtained for the inner codes analyzed.

Notations: We use $\Pr$ to denote the probability of events. We use $\mathbb{E}[X]$ to denote the expectation value of the random

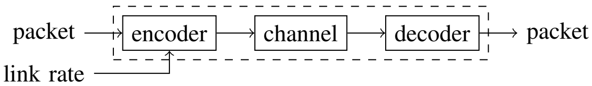

Fig. 1. The dashed box represents an outage link formed by a channel together with a pair of encoder and decoder.

variable X. Denote by $\mathbb{N}$ the set of natural numbers and $\mathbb{Q}$ the set of rational numbers.

II. Outage Links and Batched Network Codes

In this section, we first describe a network link model called an outage link. We then introduce batched network codes for a line network formed by outage links.

A. Outage Links

An *outage link* models the communication between two network nodes called the sender and the receiver, respectively. Let $\mathcal{A}$ be the input/output alphabet of the outage link. The sender can transmit by the outage link a sequence of m symbols from $\mathcal{A}$ by n link uses, where m and n can be any positive integers determined by the sender such that m/n is not larger than a fixed value $r_{\max}$. We call the sequence of m symbols from $\mathcal{A}$ a *packet*, n the *(link) blocklength*, and m/n the *(link) rate* (in terms of symbols in $\mathcal{A}$ per link use).

To model the communication quality, the outage link is associated with an *outage function* $P_{\text{out}}(r)$, which is a non-decreasing function in $0 \leq r \leq r_{\max}$ satisfying $P_{\text{out}}(0) = 0$ and $P_{\text{out}}(r_{\max}) \leq 1$. If a packet is transmitted with rate r, then with probability $P_{\text{out}}(r)$, the packet is erased by the link; otherwise, the packet is correctly received by the receiver. We call $P_{\text{out}}(r)$ the *link loss (or outage) probability* at rate r.

As illustrated in Fig. 1, an *outage link* can be regarded as a channel together with a pair of encoder and decoder with controllable rates. In the following we show connections of the outage links with some commonly used channel models and discuss the empirical approach of obtaining an outage link.

1) Outage Link for Discrete Memoryless Channels: For a discrete memoryless channel (DMC) W with finite input and output alphabets, the Shannon capacity C (bit per use) of the channel is well defined and non-negative. The communication performance of W can be approximated by an outage link Q_{DMC} with $\mathcal{A} = \{0, 1\}$ and the outage function $P_{\text{out}}(r) = 0$ for $0 \leq r < C$ and 1 otherwise. When $0 \leq r < C$, due to the achievability of C for W, there exists a code of rate at least r with an arbitrarily small decoding error probability when the blocklength is sufficiently large. When $r > C$, due to the converse of Wolfowitz [28], the decoding error probability of any code of rate at least r for W is arbitrarily close to 1 when the blocklength is sufficiently large. Therefore, the approximation of the communication performance of a class of codes for W by Q_{DMC} can be arbitrarily accurate for $r \neq C$ with the increasing of the blocklength.

2) Outage Link for Quasi-static Channels: A *quasi-static* channel has been widely used to model wireless communications with slowly-varying fading channel [24]. A quasi-static channel U has a channel status (e.g., channel gain in wireless communications) that is independently chosen by sampling a random variable S but remains constant for transmitting each codeword. We assume that the channel status information is not available at both the sender and the receiver sides. For a fixed status s, assume that U is memoryless and has the capacity $C(s)$. Using the similar argument as for DMCs, the communication performance of a class of codes for U can be approximated by that of an outage link with the outage function $P_{\text{out}}(r) = \Pr\{C(S) \leq r\}$. An example of the outage function we use in this paper is $P_{\text{out}}(r) = \frac{a^r - 1}{a - 1}, r \in [0, 1]$, where $a > 1$ is a constant. This outage function is similar to the one for certain fading channel models [24].

3) Outage Link from Empirical Evaluation: We can use the empirical performance to model the communication performance of practical devices as outage links. Suppose that a sequence of channel codes of different rates are specified, for example, as in both cellular and wireless LAN communication standards. To obtain an outage link model, we can test or perform simulations for each code of rate r and let $P_{\text{out}}(r)$ be the empirical decoding error rate. The outage link model obtained is close to the real performance of the wireless communication system.

B. A Line Network with Outage Links

A line network of length L is formed by a sequence of nodes labeled by $0, 1, \ldots, L$, where directed outage links exist only from node $\ell - 1$ to node ℓ for $\ell = 1, \ldots, L$. We call the link from node $\ell - 1$ to node ℓ the ℓ-th link or link ℓ. To simplify discussion, we assume that all the outage links have the same input/output alphabet $\mathcal{A}$ and outage function P_{out} with the maximum rate $r_{\max}$.

We study the communication from the first node to the last node, which are called the *source node* and the *destination node*, respectively. Nodes $1, 2, \ldots, L - 1$ are also called the *intermediate nodes*, which can help with the communication from the source node to the destination node.

We say that an outage function P_{out} is *degraded* if $P_{\text{out}}(r_0) = 0$ for a certain $r_0 > 0$. For an outage link with a degraded outage function, a packet can be transmitted with zero loss probability when the link rate is not larger than r_0. For the line network discussed in this paper, if the outage function is degraded, a constant positive rate can be achieved for any L. Henceforth in this paper, we focus on non-degraded outage functions (i.e., $P_{\text{out}}(r) > 0$ for $r > 0$), which is closer to the real-world wireless communication scenario with fading and interference.

Though it is possible to formulate a general code for the line network (see [22, Appendix A]), it would be of little help due to the difficulty of analyzing the code performance. Instead, we study *batched (network) codes* that have been discussed for line networks of DMCs [19], [20]. Batched codes not only facilitate theoretical analysis, but also provide parameters to control the coding complexities and the buffer sizes at the intermediate nodes. In the following of this section, we introduce batched codes for a line network with outage links.

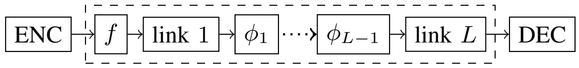

Fig. 2. The dashed box represents a batch channel. ENC and DEC are respectively the encoder and decoder of the outer code for the batch channel.

C. Batched codes for Line Networks

A batched code for the communication from the source node to the destination node has an outer code and an inner code. The message of the source node is from a finite set. The source node encodes the message by the outer code into a sequence of batches, each of which includes a number m of symbols from $\mathcal{A}$, where m is a positive integer called the *(symbol-wise) batch size* and $\mathcal{A}$ is the finite alphabet used by the link input/output.

The inner code at each node *re-encodes* the symbols belonging to the same batch. The number of uses n_ℓ of link ℓ per batch is called the blocklength of the inner code, which can be different for different links.

- At the source node that generates the batches, the inner code f is performed on the original m symbols of a batch and takes non-negative integers n_1 and m_1 as parameters. The inner code f generates a sequence of m_1 symbols in $\mathcal{A}$, which can be transmitted on the outgoing link in terms of one or multiple packets with totally n_1 link uses.
- At an intermediate network node ℓ ($1 \leq \ell < L$), the inner code ϕ_ℓ is performed on the received symbols (in $\mathcal{A}$) belonging to the same batch to generate a sequence of $m_{\ell+1}$ symbols in $\mathcal{A}$, which can be transmitted on the outgoing link in terms of one or multiple packets with totally $n_{\ell+1}$ link uses.

The inner code of a batched code consists of the functions f and $\{\phi_\ell\}$. Note that m_ℓ and n_ℓ, $\ell = 1, \dots, L$ can be random variables, which may depend on the number of received symbols at each node, so that the inner codes f and ϕ_ℓ are random.

As illustrated in Fig. 2, for the given inner code operations at all the nodes, the end-to-end operation of the network on a batch by the series of the inner code operations can be regarded as a channel with $\mathcal{A}^m$ as the input alphabet, called a *batch channel*. The outer code acts as a channel code for this batch channel. As the inner code is independent for each batch, the batch channel is memoryless batch-wisely. Let $\mathbf{X}$ be a random variable on $\mathcal{A}^m$. Let $\mathbf{Y}$ be the output of the link L when the input of the batch channel is $\mathbf{X}$. For a given inner code, the maximum achievable rate (the Shannon capacity) of the outer code is $\max_{p_\mathbf{X}} I(\mathbf{X};\mathbf{Y})$ with $\mathbb{E}[n_\ell]$ uses of link ℓ. When talking about the achievable rate of the batched code for the line network, we normalize the rate of the outer code by $\max_{l=1}^L \mathbb{E}[n_\ell]$ (the maximum average link usage every batch).

In the following two sections, we will introduce several classes of inner codes, and discuss how to maximize the achievable rate of the outer code for each class of inner codes.

III. Store-and-Forward Inner Codes

Store-and-forward has been widely used in traditional network communications and can be regarded as special inner codes of a batched code. In this section, we study the achievable rates of batched codes with the store-and-forward inner codes. We derive the capacity (maximum achievable rate) scalabilities of batched codes under different constraints of the link outage function.

A. General Store-and-Forward Inner Codes

A store-and-forward inner code is defined as follows: At the source node, the inner code transmits the m symbols of a batch as a packet through the link 1 by fixed n_1 link uses so that the link rate is m/n_1. At the intermediate node ℓ ($1 \leq \ell < L$), if a batch is successfully received, the node will store this batch and forward it as a packet to the outgoing link $\ell+1$ with $n_{\ell+1}^+$ link uses, where $n_{\ell+1}^+$ is a fixed positive integer; if a batch is not received, then no packets are transmitted. For convenience, let $n_1^+ = n_1$. For $\ell = 2, \dots, L$, n_ℓ is a random variable over $\{0, n_\ell^+\}$ with

$$\Pr\{n_\ell = n_\ell^+\} = p_{\ell-1} \triangleq \prod_{i=1}^{\ell-1} \left(1 - P_{\mathrm{out}}\left(\frac{m}{n_i^+}\right)\right). \qquad (1)$$

So $\mathbb{E}[n_\ell] = n_\ell^+ p_{\ell-1}$ for given n_i^+ for $i = 1, \dots, \ell-1$.

With a store-and-forward inner code, the end-to-end batch channel is a packet erasure channel with the input alphabet $\mathcal{A}^m$ and the erasure probability $1 - p_L$. Therefore the maximum achievable rate of the outer code is mp_L (symbols per batch) with $\mathbb{E}[n_\ell]$ uses of link ℓ.

In the following of this section, we analyze the capacity scalability of store-and-forward inner codes for two cases: one has the identical link rate for all links and the other has variable links rates for different links.

B. Capacity Scalability with Identical Link Rate

When $n_\ell^+ = n$ for any ℓ, by (1), the average number of uses of link ℓ per batch is

$$n\left(1 - P_{\mathrm{out}}\left(m/n\right)\right)^{\ell-1}, \qquad (2)$$

which is upper bounded by n link uses at link 1. The maximum achievable rate of the outer code (normalized by n) is $\frac{m}{n}\left(1 - P_{\mathrm{out}}\left(\frac{m}{n}\right)\right)^L$. Denote

$$R_L^{(0)}(r) = r(1 - P_{\mathrm{out}}(r))^L. \qquad (3)$$

Then the capacity of the batched codes with the store-and-forward inner codes using identical link rate is

$$C_L^{(0)} \triangleq \sup_{r \in [0, r_{\max}] \cap \mathbb{Q}} R_L^{(0)}(r).$$

We obtain capacity scalability results for $C_L^{(0)}$ in the following theorem, where the proof is in Appendix A.

Theorem 1. *Consider a line network of length L formed by identical outage links with the outage function P_{out}.*

1) *When there exists constants $b, c > 0$ such that $P_{\text{out}}(r) \geq cr$ for $r \leq b$, it holds that $C_L^{(0)} = O(1/L)$.*
2) *When there exists constants $b, c' > 0$ such that $P_{\text{out}}(r) \leq c'r$ for $r \leq b$, it holds that $C_L^{(0)} = \Omega(1/L)$. Moreover, when $r = \Theta(1/L)$, $R_L^{(0)}(r) = \Omega(1/L)$.*

Note that when P_{out} is degraded, a constant rate is achievable. The condition in Theorem 1-1) implies that P_{out} is non-degraded. The condition in Theorem 1-2) is non-trivial for non-degraded P_{out}.

To better understand the conditions on P_{out} in Theorem 1, suppose $P_{\text{out}}(r)$ is differentiable around 0. Then, the condition in Theorem 1-1) is equivalent to $\liminf_{r\to 0^+} P'_{\text{out}}(r) > 0$, and the condition of Theorem 1-2) is equivalent to $\limsup_{r\to 0^+} P'_{\text{out}}(r) < \infty$. When the conditions in 1) and 2) of Theorem 1 hold simultaneously, batched codes can achieve the capacity scalability $\Theta(1/L)$ under the store-and-forward inner code with the identical link rate.

C. Scalability with Variable Link Rates

In the case $n_\ell^+ = n$ for all ℓ discussed above, the average number of link uses decreases with the number of hops (ref. (2)). We introduce a new inner code scheme that allows n_ℓ^+ to be varying hop-by-hop such that the average number of link uses is upper bounded by n. For a fixed value of m, let $n'_1 = n$ and

$$n'_{\ell+1} = \frac{n'_\ell}{1 - P_{\text{out}}(m/n'_\ell)}, \quad \ell = 1, \ldots, L-1. \tag{4}$$

Let $n_1^+ = n$ and for $2 \leq \ell \leq L$, let $n_\ell^+ = \lfloor n'_\ell \rfloor$. We can verify that $\mathbb{E}[n_1] = n$, and for $\ell = 2, \ldots, L$, $\mathbb{E}[n_\ell] \leq n$.

With the above inner code scheme, the maximum achievable rate of the outer code (normalized by n) is

$$R_L^{(1)}(m,n) \triangleq \frac{m}{n} \prod_{\ell=1}^{L} \left(1 - P_{\text{out}}\left(\frac{m}{n_\ell^+}\right)\right).$$

Then the capacity of the batched codes with the store-and-forward inner codes with variable link rates is

$$C_L^{(1)} \triangleq \sup_{m,n\in\mathbb{N}, m/n \leq r_{\max}} R_L^{(1)}(m,n).$$

Notice that the link rate m/n_ℓ^+ in this inner code scheme is no more than m/n and then the link loss probability for each link is no more than $P_{\text{out}}(m/n)$. Thus $R_L^{(1)}(m,n) \geq R_L^{(0)}(m/n)$ and hence $C_L^{(1)} \geq C_L^{(0)}$ (see Fig. 3 for an illustration). Therefore $C_L^{(1)}$ is also $\Omega(1/L)$ under condition in Theorem 1-2). Now we will show the upper bound on $C_L^{(1)}$.

Definition 1. *$\{x_i\}_{i=1}^\infty$ is called an output-alternating input sequence of a function f defined over $\mathcal{X} \subset \mathbb{R}$ if*

1) *$\{x_i\}_{i=1}^\infty \subset \mathcal{X}$ is strictly monotonic, and*
2) *$\big(f(x_{2k-1}) - f(x_{2k})\big)\big(f(x_{2k}) - f(x_{2k+1})\big) < 0$ and $\big(f(x_{2k}) - f(x_{2k+1})\big)\big(f(x_{2k+1}) - f(x_{2k+2})\big) < 0$ for any $k \geq 1$.*

For a differentiable function f, when it has a bounded output-alternating input sequence, f has infinite oscillations around a certain point, e.x. $f(x) = \sin(1/x), x \in \mathbb{R} \setminus \{0\}$.

The following theorem is proved in Appendix B.

Theorem 2. *Consider a line network of length L formed by identical outage links with outage function $P_{\text{out}}(r)$, $r \in [0, r_{\max}]$ which satisfies the following conditions*

1) *$P_{\text{out}}(r)$ is non-degraded and continuous;*
2) *$r(1-P_{\text{out}}(r))$ has no output-alternating input sequences;*
3) *P_{out} is differentiable around 0, $\lim_{r\to 0^+} P'_{\text{out}}(r) > 0$ and $\lim_{r\to 0^+} rP'_{\text{out}}(r)$ is bounded.*

It holds that $C_L^{(1)} = O(1/L)$.

As an example, we can see that $P_{\text{out}}(r) = \frac{a^r - 1}{a-1}$, $r \in [0,1]$ with $a > 1$ satisfies the condition of the above theorem. Overall, the capacities for batched code with these two store-and-forward schemes maximized over m, n are both $\Theta(1/L)$ under proper conditions on the outage function.

IV. Random Linear Inner Codes

We investigate the random linear inner codes introduced in random linear network coding (RLNC) [5], [6], which has been studied in batched codes [12]–[17].

A. Formulation

Suppose that the input/output alphabet $\mathcal{A}$ of the outage links is the finite field of q elements. We consider a batched code with the symbol-wise batch size m, i.e., each batch has m symbols in $\mathcal{A}$. Let n be a positive integer. The random linear inner code we will introduce has two more parameters M and N which are positive integers such that M divides m and N divides n. Usually, M and N are much smaller than m and n. In many practical settings of random linear inner codes [18], M is less than 100 and n is a couple of thousand.

We first describe the random linear inner code at the source node. The m symbols of a batch are put into an $\frac{m}{M} \times M$ matrix denoted by $\mathbf{X}$. Then an $(\frac{m}{M} + M) \times M$ matrix $\tilde{\mathbf{X}}$ is formed by adding the $M \times M$ identity $\mathbf{I}_M$ matrix on top of $\mathbf{X}$, i.e.,

$$\tilde{\mathbf{X}} = \begin{bmatrix} \mathbf{I}_M \\ \mathbf{X} \end{bmatrix}.$$

Next, an $(\frac{m}{M} + M) \times N$ matrix $\mathbf{U}_1$ is generated as

$$\mathbf{U}_1 = \tilde{\mathbf{X}}\mathbf{B}_0, \tag{5}$$

where $\mathbf{B}_0$ is an $M \times N$ uniformly random matrix over $\mathcal{A}$ (i.e, all entries uniformly at random chosen from $\mathcal{A}$). Each column of $\mathbf{U}_1$ is transmitted as a packet using link 1 by n/N link uses. The rate of link 1 is

$$r \triangleq \frac{m/M + M}{n/N}. \tag{6}$$

Next, we describe the operation at other nodes recursively. For $1 \leq \ell \leq L$, suppose that node $\ell - 1$ transmits N packets of a batch at rate r. Let N_ℓ be the number of correctly received packets by node ℓ, which follows the binomial distribution $\mathrm{B}(N, 1 - P_{\text{out}}(r))$. Denote by $\tilde{\mathbf{Y}}_\ell$ the $(\frac{m}{M} + M) \times N_\ell$ matrix formed by juxtaposing the N_ℓ received packets of the batch transmitted by the node $\ell-1$. When $1 \le \ell < L$, node ℓ generates an $(\frac{m}{M}+M) \times N$ matrix

$$\mathbf{U}_{\ell+1} = \tilde{\mathbf{Y}}_\ell \mathbf{B}_\ell \tag{7}$$

where $\mathbf{B}_\ell$ is an N-column uniformly random matrix over $\mathcal{A}$. Each column of $\mathbf{U}_{\ell+1}$ is transmitted as a packet using link $\ell+1$ by n/N link uses so that the link rate is r as defined in (6). When no packets are received for a batch, i.e., $\tilde{\mathbf{Y}}_\ell$ is the empty matrix, no packets are transmitted.

At the destination node, the received matrix $\tilde{\mathbf{Y}}_L$ for a batch is used for the outer code decoding. Let $\mathbf{H}_\ell$ be the first M rows of $\tilde{\mathbf{Y}}_\ell$, and let $\mathbf{Y}_\ell$ be the remaining part of $\tilde{\mathbf{Y}}_\ell$. According to the above formulation, we can derive that $\mathbf{Y}_\ell = \mathbf{X}\mathbf{H}_\ell$ for $\ell = 1, \ldots, L$. For the inner code formulated above, the end-to-end batch channel is a matrix multiplication channel with the input $\mathbf{X}$ and output $(\mathbf{Y}_L, \mathbf{H}_L)$ such that $\mathbf{Y}_L = \mathbf{X}\mathbf{H}_L$.

According to the capacity of the matrix multiplication channel [29], the achievable rate of the batched code with random linear inner coding is

$$\frac{m}{nM}\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)] = \left(\frac{r}{N} - \frac{M}{n}\right)\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)],$$

where the expected rank $\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)]$ depends on M, N and the link loss probability $P_{\mathrm{out}}(r)$ (see the formula in [18, Sec. 4.1]). Let

$$R_L^{(2)}(M,N,r) = \frac{r}{N}\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)].$$

When n is much larger than MN/r, $R_L^{(2)}(M,N,r)$ gives a close approximation of the achievable rate of the batched code with random linear inner coding.

B. Scalability of Random Linear Inner Code

We study the supremum of $R_L^{(2)}(M,N,r)$ for M, N and $r \in [0, r_{\max}] \cap \mathbb{Q}$ subject to different constraints on M and N, which affect the inner code complexity in (5) and (7).

When $M = N = 1$, we see that the random linear inner code is similar to a store-and-forward inner code, except that a received packet is multiplied by a random scalar before forwarding. With probability $1/q$, the scalar takes value 0 so that the packet is useless for decoding. Therefore, in this case, it is not surprising that random linear inner codes are even worse than store-and-forward inner codes. In [22], it has been shown that when $M = O(1)$,

$$\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)] = \Theta((1-(P_{\mathrm{out}}(r)+(1-P_{\mathrm{out}}(r))/q)^N)^L).$$

When $M, N = \Theta(1)$, $\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)] = \Theta(\exp(-L))$ as

$$(P_{\mathrm{out}}(r)+(1-P_{\mathrm{out}}(r))/q)^N \ge 1/q^N.$$

Thus the supremum of $R_L^{(2)}(M,N,r)$ with $M, N = O(1)$ is $\Theta(\exp(-L))$. Let

$$C_L^{(2)}(M,N) \triangleq \sup_{r\in\mathbb{Q}\cap[0,r_{\max}]} R_L^{(2)}(M,N,r).$$

As illustrated in Fig. 3, when q is large and L is small, $C_L^{(2)}(1,1)$ is almost the same with $C_L^{(0)}$. The scalability issue

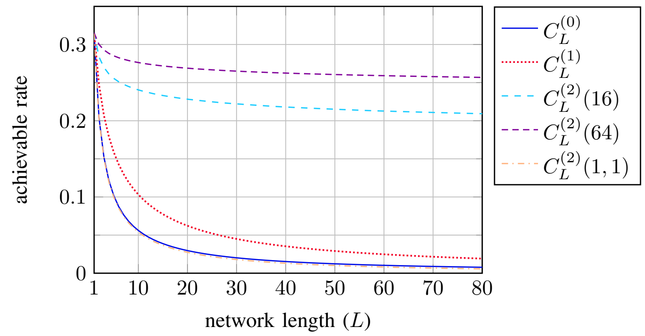

Fig. 3. $P_{\mathrm{out}}(r) = \frac{e^r-1}{e-1}, r \in [0,1]$. $C_L^{(2)}(1,1)$, $C_L^{(2)}(16)$ and $C_L^{(2)}(64)$ are obtained when $q = 256$.

when $M = N = 1$ can be resolved using *systematic random linear inner codes* [18, Sec. 4.2], which is not elaborated in this paper.

In practice, M is usually fixed to be a small integer, e.g., 16 or 64, and N and r can be optimized to maximize $R_L^{(2)}$. Define

$$C_L^{(2)}(M) \triangleq \sup_{r\in\mathbb{Q}\cap[0,r_{\max}], N\in\mathbb{N}^+} R_L^{(2)}(M,N,r).$$

As illustrated in Fig. 3 by curves for $C_L^{(2)}(16)$ and $C_L^{(2)}(64)$, random linear inner codes can have significant rate gain if M and N are allowed to be slightly larger than 1.

In the following theorem, we discuss the scalability of the supremum of $R_L^{(2)}$ when $N = O(\ln L)$. The proof is in Appendix D.

Theorem 3. *Consider a line network of length L formed by identical outage links with the outage function P_{out}. Suppose the uniformly random linear coding is applied, $P_{\mathrm{out}}(r)$ is non-degraded and $P_{\mathrm{out}}(r_0) < 1$ for some $r_{\max} \ge r_0 > 0$.*

1) *When $M = O(1)$ and $N = O(\ln L)$, for any field size q, the supremum of $R_L^{(2)}(M,N,r)$ is $\Theta(1/\ln L)$. Moreover, when r is fixed with $P_{\mathrm{out}}(r) \in (0,1)$, $R_L^{(2)}(M,N,r)$ is $\Theta(1/\ln L)$.*
2) *When $M = O(\ln L)$ and $N = O(\ln L)$ and the field size $q \ge 2M$, the supremum of $R_L^{(2)}(M,N,r)$ is $\Theta(1)$. Moreover, when r is fixed with $P_{\mathrm{out}}(r) \in (0,1)$, $R_L^{(2)}(M,N,r)$ is $\Theta(1)$.*

V. Concluding Remarks

For line networks of DMCs, existing works showed that random linear inner codes do not have advantages in scalability over the decode-and-forward inner codes, though the former can potentially achieve higher rates than the latter. In contrast, for line networks of outage links which approximate the performance of slow fading wireless channels, random linear inner codes have scalability advantages over the store-and-forward inner codes (which is same as decode-and-forward).

Moreover, our proof for achieving $\Theta(1)$ using random linear inner codes in Theorem 3 implies that batched codes with random linear inner codes also achieve $\Theta(1)$ for line networks with DMCs under certain coding parameter conditions, which has not been shown previously in literature.

REFERENCES

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

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

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

[4] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. Allerton Conf. Comm., Control, and Computing*, Oct. 2003.

[5] T. Ho, B. Leong, M. Medard, R. Koetter, Y. Chang, and M. Effros, "The benefits of coding over routing in a randomized setting," in *Proc. IEEE ISIT '03*, Jun. 2003.

[6] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[7] S. Jaggi, P. A. Chou, and K. Jain, "Low complexity optimal algebraic multicast codes," in *Proc. IEEE ISIT '03*, Jun. 2003.

[8] P. Sanders, S. Egner, and L. Tolhuizen, "Polynomial time algorithms for network information flow," in *Proc. ACM SPAA '03*, New York, NY, USA, 2003, pp. 286–294.

[9] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 789–804, 2006.

[10] Y. Wu, "A trellis connectivity analysis of random linear network coding with buffering," in *Proc. IEEE ISIT '06*, Jul. 2006.

[11] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "On coding for reliable communication over packet networks," *Physical Communication*, vol. 1, no. 1, pp. 3–20, 2008.

[12] D. Silva, W. Zeng, and F. R. Kschischang, "Sparse network coding with overlapping classes," in *Proc. NetCod '09*, Jun. 2009, pp. 74–79.

[13] A. Heidarzadeh and A. H. Banihashemi, "Overlapped chunked network coding," in *Proc. ITW '10*, Jan. 2010, pp. 1–5.

[14] Y. Li, E. Soljanin, and P. Spasojevic, "Effects of the generation size and overlap on throughput and complexity in randomized linear network coding," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1111–1123, Feb. 2011.

[15] S. Yang and R. W. Yeung, "Batched sparse codes," *IEEE Trans. Inform. Theory*, vol. 60, no. 9, pp. 5322–5346, Sep. 2014.

[16] B. Tang, S. Yang, Y. Yin, B. Ye, and S. Lu, "Expander chunked codes," *EURASIP Journal on Advances in Signal Processing*, vol. 2015, no. 1, pp. 1–13, Dec. 2015.

[17] B. Tang and S. Yang, "An LDPC approach for chunked network codes," *IEEE/ACM Trans. Netw.*, vol. 26, no. 1, pp. 605–617, Feb. 2018.

[18] S. Yang and R. W. Yeung, *BATS Codes: Theory and Practice*, ser. Synthesis Lectures on Communication Networks. Morgan & Claypool Publishers, 2017.

[19] S. Yang, J. Wang, Y. Dong, and Y. Zhang, "On the capacity scalability of line networks with buffer size constraints," in *Proc. IEEE ISIT '19*. IEEE, 2019, pp. 1507–1511.

[20] S. Yang and J. Wang, "Upper bound scalability on achievable rates of batched codes for line networks," in *2020 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2020, pp. 1629–1634.

[21] U. Niesen, C. Fragouli, and D. Tuninetti, "On capacity of line networks," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4039–4058, 2007.

[22] S. Yang, J. Wang, Y. Dong, and Y. Zhang, "Capacity scalability of line networks with batched codes," *arXiv preprint arXiv:2105.07669*, 2021.

[23] G. J. Foschini and M. J. Gans, "On limits of wireless communications in a fading environment when using multiple antennas," *Wireless personal communications*, vol. 6, no. 3, pp. 311–335, 1998.

[24] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge university press, 2005.

[25] F. P. Kelly, A. K. Maulloo, and D. K. Tan, "Rate control for communication networks: shadow prices, proportional fairness and stability," *Journal of the Operational Research society*, vol. 49, no. 3, pp. 237–252, 1998.

[26] S. H. Low, *Analytical methods for network congestion control*, ser. Synthesis Lectures on Communication Networks. Morgan & Claypool Publishers, 2017.

[27] Y. Dong, J. Wang, S. Yang, and R. W. Yeung, "Capacity scalability of batched network codes on line networks with outage links (full version)." [Online]. Available: https://shhyang.github.io/research/22outagefull.pdf

[28] J. Wolfowitz, "The coding of messages subject to chance errors," *Illinois Journal of Mathematics*, vol. 1, no. 4, pp. 591–606, 1957.

[29] S. Yang, J. Meng, and E.-h. Yang, "Coding for linear operator channels over finite fields," in *Proc. IEEE ISIT '10*, Jun. 2010, pp. 2413–2417.

Appendix A
Proof of Theorem 1

Lemma 1. *Let $a > 1$. When $P_{\text{out}}(r) = \frac{a^r-1}{a-1}$, $r \in [0,1]$, $C_L^{(0)} = \Theta(1/L)$ and the maximum value is achieved when the link rate satisfies $m/n = \Theta(1/L)$.*

Proof: For $a > 1$, let

$$H_L(r) = r\left(1 - \frac{a^r-1}{a-1}\right)^L. \tag{8}$$

Solve $H_L'(r) = 0$, i.e.

$$H_L'(r) = \left(\frac{a-a^r}{a-1}\right)^L - \frac{a^r rL\ln a}{a-1}\left(\frac{a-a^r}{a-1}\right)^{L-1} = 0,$$

which is equivalent to

$$a - a^r(1 + rL\ln a) = 0.$$

Let $g_L(r) = a - a^r(1+rL\ln a)$ and denote by r_L^* the solution of $g_L(r) = 0$, $r > 0$. Due to

$$g_L(r)\begin{cases} > 0, & r < r_L^*, \\ < 0, & r > r_L^*, \end{cases}$$

$H_L(r)$ is non-decreasing in $[0, r_L^*]$ and non-increasing in $[r_L^*, 1]$. Observe that for arbitrary $\epsilon < a-1$,

$$\lim_{L\to\infty} g_L\left(\frac{a-1+\epsilon}{L\ln a}\right) = \lim_{L\to\infty} a - (a+\epsilon)\cdot a^{\frac{a-1+\epsilon}{L\ln a}} = -\epsilon,$$
$$\lim_{L\to\infty} g_L\left(\frac{a-1-\epsilon}{L\ln a}\right) = \lim_{L\to\infty} a - (a-\epsilon)\cdot a^{\frac{a-1-\epsilon}{L\ln a}} = \epsilon.$$

So when L is large enough, $g_L(\frac{a-1-\epsilon}{L\ln a}) > \epsilon/2$ and $g_L(\frac{a-1+\epsilon}{L\ln a}) < -\epsilon/2$. Thus,

$$\frac{a-1-\epsilon}{L\ln a} < r_L^* < \frac{a-1+\epsilon}{L\ln a}.$$

Then when L is large enough,

$$\frac{a-1-\epsilon}{L\ln a}\left(\frac{a-a^{\frac{a-1-\epsilon}{L\ln a}}}{a-1}\right)^L \le H_L(r_L^*) < \frac{a-1+\epsilon}{L\ln a}.$$

Since

$$\begin{aligned}\lim_{L\to\infty}\left(\frac{a-a^{\frac{a-1-\epsilon}{L\ln a}}}{a-1}\right)^L &\ge \lim_{L\to\infty}\left(\frac{a-1-\frac{2(a-1-\epsilon)}{L}}{a-1}\right)^L \\ &= \lim_{L\to\infty}\left(1-\frac{2(a-1-\epsilon)}{L(a-1)}\right)^L \\ &= \exp\left(-\frac{2(a-1-\epsilon)}{a-1}\right),\end{aligned}$$

we have $H_L(r_L^*) = \Theta(1/L)$ and the maximum value is achieved when $r_L^* = \Theta(1/L)$. There exists $r_L' \in \mathbb{Q}^+$ between $\frac{a-1-\epsilon}{L\ln a}$ and $\frac{a-1+\epsilon}{L\ln a}$ such that

$$C_L^{(0)} = \sup_{r\in[0,r_{\max}]\cap\mathbb{Q}} H_L(r) = H_L(r_L') = \Theta(1/L).$$

■

Proof of Theorem 1-1) : Since

$$\lim_{a\to+\infty}\left(\frac{a^r-1}{a-1}\right)'\Big|_{r=0} = \lim_{a\to+\infty}\frac{\ln a}{a-1} = 0,$$

then for any $c_0 > 0$, there exists $a > 1, b_0 > 0$ such that $c_0 r \ge \frac{a^r-1}{a-1}$ for $r \le b_0$. Suppose $P_{\text{out}}(r) \ge cr$ for $r \le b$ where $b, c > 0$. Then there exists $a > 1, b' > 0$ such that

$$P_{\text{out}}(r) \ge cr \ge \frac{a^r-1}{a-1} \text{ for } r \le b'.$$

Then for $H_L(r)$ as defined in (8) and $R_L^{(0)}(r)$ as defined in (3) using $P_{\text{out}}(r)$, $R_L^{(0)}(r) \le H_L(r)$. By Lemma 1, $\sup_{r\in\mathbb{Q}\cap[0,b']} R_L^{(0)}(r) = O(1/L)$. Observe that

$$\begin{aligned}\sup_{r\in\mathbb{Q}\cap[b',r_{\max}]} R_L^{(0)}(r) &= \sup_{r\in\mathbb{Q}\cap[b',r_{\max}]} r(1-P_{\text{out}}(r))^L \\ &\le r_{\max}(1-P_{\text{out}}(b'))^L.\end{aligned}$$

Thus $C_L^{(0)} = O(1/L)$. ■

Proof of Theorem 1-2): When L is large enough such that $\frac{1}{L} \le b$, ($R_L^{(0)}$ is defined in (3))

$$\begin{aligned}R_L^{(0)}\left(\frac{1}{L}\right) &= \frac{1}{L}\left(1-P_{\text{out}}\left(\frac{1}{L}\right)\right)^L \\ &\ge \frac{1}{L}(1-c'/L)^L.\end{aligned}$$

Thus $R_L^{(0)}(\frac{1}{L}) = \Omega(1/L)$, and hence $C_L^{(0)} = \Omega(1/L)$. ■

Appendix B
Proof of Theorem 2

To prove Theorem 2, we propose an upper bound for $C_L^{(1)}$ (defined in Section III-C) and identify the scalability of this upper bound.

Define $f(r) \triangleq r(1-P_{\text{out}}(r))$. Let

$$R_1(r) = f(r), \tag{9}$$

and for $i = 2, 3, \ldots$, $R_i(r)$ is recursively defined by

$$R_i(r) = f(R_{i-1}(r)). \tag{10}$$

Lemma 2. $C_L^{(1)} \le C_L^u \triangleq \max_{r\in[0,r_{\max}]} R_L(r)$.

Proof: Let $m \in \mathbb{N}, n \in \mathbb{N}^+$ and $r = \frac{m}{n}$. For $\ell = 1, \ldots, L$, let $r_\ell = \frac{m}{n_\ell'}(1-P_{\text{out}}(m/n_\ell'))$, where n_ℓ' is defined in (4). Then $r_1 = f(r)$ and for $\ell = 2, \ldots, L$,

$$r_\ell = r_{\ell-1}(1-P_{\text{out}}(r_{\ell-1})) = f(r_{\ell-1}),$$

which implies $r_\ell = R_\ell(r)$, and especially,

$$R_L(r) = r_L = \frac{m}{n}\prod_{\ell=1}^{L}(1-P_{\text{out}}(m/n_\ell')) \ge R_L^{(1)}(m,n).$$

Thus $C_L^u = \max_{r\in[0,r_{\max}]} R_L(r) \ge C_L^{(1)}$. ■

The first three conditions on P_{out} in Theorem 2 are repeated as follows:

Condition 1. *The outage function satisfies*

1) *P_{out} is non-degraded;*

2) $P_{\text{out}}(r)$ *is continuous for* $r \in [0, r_{\max}]$*;*
3) $r(1 - P_{\text{out}}(r))$ *has no alternating output sequence on* $[0, r_{\max}]$.

Lemma 3. *Assume Condition 1 is in force. Then* $C_L^u \to 0$ *as* $L \to \infty$*. Furthermore, there exists* L_0, r^* *such that* $C_L^u = R_L(r^*)$ *when* $L \geq L_0$*, i.e.* r^* *remains the same for all* $L \geq L_0$.

Proof: According to Condition 1-2), $R_L(r)$ is a continuous function over a compact set $[0, r_{\max}]$, thus the maximizer of $R_L(r)$ always exists. For any $L \geq 1$, let $\tilde{r}_L$ satisfy

$$\tilde{r}_L \in \underset{r \in [0, r_{\max}]}{\arg\max} \; R_L(r).$$

According to the definition of C_L^u it holds that

$$C_{L+1}^u = R_{L+1}(\tilde{r}_{L+1}) = R_L(f(\tilde{r}_{L+1})) \leq R_L(\tilde{r}_L) = C_L^u,$$

which shows C_L^u is non-increasing in L. Therefore, the limit $\lim_{L\to\infty} C_L^u$ exists.

Assume that there exists fixed L_0 and r^* such that $r^* \in \arg\max_r \; R_L(r)$ for $L \geq L_0$. Then

$$\lim_{L\to\infty} C_L^u = \lim_{L\to\infty} R_L(r^*) \triangleq R^*,$$

which implies $f(R^*) = R^*$, i.e., R^* is a fixed point for the function $f(r)$. According to Condition 1-1), the outage function $P_{\text{out}}(r) > 0$ for $r > 0$ and therefore $f(r) < r$ for $r > 0$. As a consequence, the fixed point solution $R^* = 0$.

In the following we show that when there is no fixed L_0 and r^* such that $r^* \in \arg\max_r \; R_L(r)$ for $L \geq L_0$, there is an alternating output sequence for $f(r)$ on $[0, r_{\max}]$, which contradicts with Condition 1-3). The condition above can be rephrased as follows. For any L', there exists $L'' > L'$ such that for any $r \in \arg\max_r R_{L'}(r)$, it holds that $r \notin \arg\max_r R_{L''}(r)$.

Now define two infinite sequences $\{L_i\}_{i=1}^{\infty}$ and $\{r_i^*\}_{i=1}^{\infty}$. Let $L_1 = 1$, and

$$r_1^* \in \underset{r \in [0, r_{\max}]}{\arg\max} \, R_1(r).$$

For $i \geq 2$, define L_i to be the smallest $L > L_{i-1}$ such that

$$r_{i-1}^* \notin \underset{r \in [0, r_{\max}]}{\arg\max} \, R_L(r),$$

and let

$$r_i^* \in \underset{r \in [0, r_{\max}]}{\arg\max} \, R_{L_i}(r).$$

According the above definition, for any $i \geq 2$,

$$R_{L_i}(r_i^*) > R_{L_i}(r_{i-1}^*), \tag{11}$$

$$r_{i-1}^* \in \underset{r \in [0, r_{\max}]}{\arg\max} \; R_L(r), \qquad L_{i-1} \leq L < L_i. \tag{12}$$

Let

$$\begin{aligned}
a(i) &\triangleq R_{L_i-1}(r_i^*), \\
b(i) &\triangleq R_{L_i-1}(r_{i-1}^*), \\
c(i) &\triangleq R_{L_i-2}(r_{i-1}^*).
\end{aligned}$$

For $i \geq 2$, by (12), it holds that

$$b(i) \geq a(i). \tag{13}$$

If the equality in (13) holds,

$$R_{L_i}(r_i^*) = f\big(a(i)\big) = f\big(b(i)\big) = R_{L_i}(r_{i-1}^*),$$

which contradicts with (11) and thus the inequality in (13) is strict, i.e.,

$$b(i) > a(i). \tag{14}$$

Since $f(r) < r$ for $r > 0$, we have

$$R_j(r) < R_k(r), \text{ for any } j > k, \tag{15}$$

which together with (14) implies for $i \geq 2$,

$$f\big(a(i)\big) = R_{L_i}(r_i^*) < a(i) < b(i) = f\big(c(i)\big), \tag{16}$$

and for any $i \geq 3$,

$$a(i) < b(i) < c(i). \tag{17}$$

By (11) and (16),

$$f(b(i)) < f(a(i)) < f(c(i)), \quad \forall i \geq 3. \tag{18}$$

Due to (15) and $L_{i+1} - 2 \geq L_i - 1$, for any i,

$$c(i+1) = R_{L_{i+1}-2}(r_i^*) \leq R_{L_i-1}(r_i^*) = a(i). \tag{19}$$

Define a sequence $\{x_i\}_{i=1}^{\infty}$ by $x_1 = c(3)$ and for $k \geq 1$, $x_{2k} = b(k+2)$, and

$$x_{2k+1} = \begin{cases} a(k+2), & \text{if } f(a(k+2)) \geq f(c(k+3)), \\ c(k+3), & \text{otherwise.} \end{cases}$$

From (17) and (19), $\{x_i\}_{i=1}^{\infty}$ is strictly decreasing. From (18), it can be verified that

$$f(x_1) - f(x_2) = f\big(c(3)\big) - f\big(b(3)\big) > 0,$$

and for $k \geq 2$,

$$\begin{aligned}
&f(x_{2k-1}) - f(x_{2k}) \\
=&\max\Big(f\big(a(k+1)\big), f\big(c(k+2)\big)\Big) - f\big(b(k+2)\big) \\
>&0,
\end{aligned}$$

and for $k \geq 1$,

$$\begin{aligned}
&f(x_{2k}) - f(x_{2k+1}) \\
=&f\big(b(k+2)\big) - \max\Big(f\big(a(k+2)\big), f\big(c(k+3)\big)\Big) \\
<&0.
\end{aligned}$$

Thus $\{x_i\}_{i=1}^{\infty}$ is an alternating output sequence of f. The proof is completed since this implication contradicts with Condition 1-3). ■

Lemma 4. *Consider a line network of length* L *formed by identical outage links with the outage function* $P_{\text{out}}(r) = \frac{a^r - 1}{a-1}$, $r \in [0, 1]$*, where* $a > e$ *is a constant. Then it holds that* $C_L^{(1)} = O(1/L)$.

Proof: Let $f(r) = r\left(1 - \frac{a^r-1}{a-1}\right)$. Taking the first and second order derivatives of $f(r)$ over r, we get

$$f'(r) = \frac{a - a^r(1+r\ln a)}{a-1},$$
$$f''(r) = \frac{a^r \ln a(-2-r\ln a)}{a-1}.$$

Note that $f'(0) = 1$, $f'(1) = -a\ln a/(a-1) < 0$, and

$$f''(r) < 0,\ r \in [0,1].$$

There exists $r^* \in (0,1)$ such that $f'(r^*) = 0$. Then $f(r)$ is strictly increasing in $[0, r^*]$ and strictly decreasing in $[r^*, 1]$.

We first show that $C_L^u = R_L(r^*)$ for any L. For $r \in [0,1] \setminus \{r^*\}$,

$$R_1(r) = f(r) < f(r^*) < r^*.$$

Then as $f(r)$ is strictly increasing in $[0, r^*]$,

$$R_2(r) = f(f(r)) < f(f(r^*)) < f(r^*) < r^*.$$

Iteratively, we have $R_L(r) < R_L(r^*)$ and thus $C_L^u = R_L(r^*)$ for any L.

Now we show that there exists $\bar{L}$ such that for all $L \geq \bar{L}$, as long as $r < \frac{a-1}{L}$, it holds that $f(r) < \frac{a-1}{L+1}$. Let $L_0 = \lceil \frac{a-1}{r^*} \rceil$. Then $\frac{a-1}{L} \leq r^*$ and for $L \geq L_0$ and $r < \frac{a-1}{L}$, it holds that

$$f(r) < f\left(\frac{a-1}{L}\right).$$

We find

$$f\left(\frac{a-1}{L}\right) - \frac{a-1}{L+1} = \frac{L(1-a^{\frac{a-1}{L}}) + a - a^{\frac{a-1}{L}}}{L(L+1)}.$$

Since $\tau(L) := L(1-a^{\frac{a-1}{L}}) + a - a^{\frac{a-1}{L}}$ is a continuous function of L, and

$$\lim_{L\to\infty} \tau(L) = (a-1)(1-\ln a) < 0,$$

we can assert that there exists L_1 so that when $L \geq \bar{L} := \max(L_0, L_1)$, for $L \geq \bar{L}$,

$$f(r) < \frac{a-1}{L+1},\ \text{when } r < \frac{a-1}{L}. \tag{20}$$

In Lemma 3 we showed that $R_L(r^*) \to 0$, as $L \to \infty$, hence there exists a sufficiently large L_2 so that $R_{L_2}(r^*) < (a-1)/\bar{L}$. With $R_{L_2}(r^*)$ in place of r and $\bar{L}$ in place of L in (20),

$$R_{L_2+1}(r^*) = f(R_{L_2}(r^*)) < \frac{a-1}{\bar{L}+1}.$$

If $R_{L_2+k}(r^*) < (a-1)/(\bar{L}+k)$, by applying (20) similarly, we get

$$R_{L_2+k+1}(r^*) = f(R_{L_2+k}(r^*)) < \frac{a-1}{\bar{L}+k+1}.$$

Thus by induction, we have

$$R_L(r^*) < \frac{a-1}{\bar{L}+L-L_2},\ \text{for any } L \geq L_2.$$

Hence $C_L^u = R_L(r^*) = O(1/L)$ and then $C_L^{(1)} = O(1/L)$. ■

Proof of Theorem 2: Let $P_{\text{out}}(r)$ be an outage function so that conditions in Theorem 2 are satisfied. Note that

$$\lim_{a\to\infty} \left(\frac{a^r-1}{a-1}\right)'\Bigg|_{r=0} = \lim_{a\to\infty} \frac{\ln a}{a-1} = 0,$$

and $\lim_{r\to 0^+} P'_{\text{out}}(r) > 0$. Hence, there exists a sufficiently large a_0 and a constant $c > 0$ so that

$$P_{\text{out}}(r) \geq \tilde{P}_{\text{out}}(r) \triangleq \frac{a_0^r - 1}{a_0 - 1}, \quad r \in [0, c].$$

Let $\tilde{f}(r) = r\left(1 - \tilde{P}_{\text{out}}(r)\right)$ and $f(r) = r(1 - P_{\text{out}}(r))$. Then

$$f(r) \leq \tilde{f}(r),\ r \in [0, c]. \tag{21}$$

$R_L(r)$ is obtained by (9) and (10) with the outage probability function $P_{\text{out}}(r)$ and $f(r)$. By similar definition, let

$$\tilde{R}_1(r) = \tilde{f}(r),$$

and for $i = 2, 3, \ldots$, $\tilde{R}_i(r)$ is recursively defined by

$$\tilde{R}_i(r) = \tilde{f}(\tilde{R}_{i-1}(r)).$$

Take the derivative over r around 0,

$$f'(r) = 1 - P_{\text{out}}(r) - rP'_{\text{out}}(r).$$

We find

$$\begin{aligned} 0 &= \lim_{r\to 0} \frac{(P_{\text{out}}(r) - P_{\text{out}}(0))r}{r} \\ &= \lim_{r\to 0} \frac{P'_{\text{out}}(r)r + P_{\text{out}}(r) - P_{\text{out}}(0)}{1} \\ &= \lim_{r\to 0} rP'_{\text{out}}(r), \end{aligned} \tag{22}$$

where the equality in (22) holds by the L'Hospital's rule. Consequently $f'(r) \to 1$ as $r \to 0$. Thus, there exists $0 < b \leq c$ such that $f(r)$ is strictly increasing over $[0, b]$.

By Lemma 3, there exists $\tilde{r} \in (0,1), r^* \in (0, r_{\max}]$ such that for sufficiently large L,

$$\max_r \tilde{R}_L(r) = \tilde{R}_L(\tilde{r}),\ \max_r R_L(r) = R_L(r^*)$$

and

$$\lim_{L\to\infty} \tilde{R}_L(\tilde{r}) = \lim_{L\to\infty} R_L(r^*) = 0.$$

Then there exists L_2, L_3 such that

$$\tilde{R}_L(\tilde{r}) < b,\ \text{for } L \geq L_2,$$
$$0 < R_{L_3}(r^*) < \tilde{R}_{L_2}(\tilde{r}).$$

As a result,

$$\begin{aligned} R_{L_3+1}(r^*) &= f(R_{L_3}(r^*)) \\ &< f(\tilde{R}_{L_2}(\tilde{r})) \qquad (23) \\ &\leq \tilde{f}(\tilde{R}_{L_2}(\tilde{r})) \qquad (24) \\ &= \tilde{R}_{L_2+1}(\tilde{r}), \end{aligned}$$

where (23) is due to $f(r)$ is strictly increasing over $[0, b]$ and (24) holds by (21). By similar argument, if $0 < R_{L_3+k}(r^*) <$

$\tilde{R}_{L_2+k}(\tilde{r})$, we have $R_{L_3+k+1}(r^*) < \tilde{R}_{L_2+k+1}(\tilde{r})$. Using induction, for $L \geq L_3$ it holds that

$$C_L^u = R_L(r^*) < \tilde{R}_{L+L_2-L_3}(\tilde{r}).$$

By Lemma 4, $\tilde{R}_{L+L_2-L_3}(\tilde{r}) = O(1/L)$. Hence $C_L^{(1)} = O(1/L)$. ■

APPENDIX C
ADDITIONAL RESULTS FOR EXPECTED RANK FUNCTION

We present some preliminary results from [22, Theorem 5] for the expected rank function for the sake of completeness. The expected rank function can be expressed as

$$\begin{aligned}&\mathbb{E}[\mathrm{rank}(\mathbf{H}_L)]\\ =&\lambda_1^L v_{M,1} u_{1,1}\left(1+\sum_{i=2}^{M}\frac{\lambda_i^L v_{M,i}}{\lambda_1^L v_{M,1}u_{1,1}}\sum_{j=1}^{i} j u_{i,j}\right),\end{aligned} \tag{25}$$

where for $0 \leq i, j \leq M$,

$$\lambda_j = \sum_{k=j}^{N} f\big(k; N, P_{\text{out}}(r)\big)\zeta_j^k,$$

$$v_{i,j} = \begin{cases} 0 & i < j, \\ \zeta_j^i & i \geq j. \end{cases}$$

Here $f(k; N, P_{\text{out}}(r))$ is the probability mass function (PMF) of the binomial distribution with parameters N and $1 - P_{\text{out}}(r)$:

$$f\big(k; N, P_{\text{out}}(r)\big) = \binom{N}{k}\big(1 - P_{\text{out}}(r)\big)^k P_{\text{out}}(r)^{N-k},$$

and ζ_r^m is the probability of the $r \times m$ totally random matrix is full rank:

$$\zeta_r^m = \begin{cases} 1 & r = 0, \\ \prod_{i=m-r+1}^{m}(1 - q^{-i}) & 1 \leq r \leq m. \end{cases}$$

Denote the matrix $\mathbf{V} = (v_{i,j})_{0 \leq i,j \leq M}$, and $u_{i,j}$ the (i,j)-th entry of $\mathbf{V}^{-1}$. It can be checked that $u_{i,j} = 0$ for $i < j$ and $u_{i,i} = 1/\zeta_i^i$. In particular, the coefficient

$$\lambda_1 = 1 - \big(P_{\text{out}}(r) + \frac{1 - P_{\text{out}}(r)}{q}\big)^N.$$

For large L, it holds that

$$\max_N \lambda_1^L / N = \Theta(1/\ln L), \tag{26}$$

where the maximum value is achieved if $N = \Theta(\ln L)$.

Lemma 5. *For $0 \leq i, j \leq M$ and $i \geq j$,*

$$u_{i,j} = \frac{(-1)^{i-j} q^{-\frac{(i-j)(i-j-1)}{2}}}{\zeta_j^j \zeta_{i-j}^{i-j}}.$$

Proof. Define an $(M+1) \times (M+1)$ lower triangular matrix U with the (i,j) entry

$$\frac{(-1)^{i-j} q^{-\frac{(i-j)(i-j-1)}{2}}}{\zeta_j^j \zeta_{i-j}^{i-j}} \triangleq U(i,j), \quad i \geq j.$$

We want to show $VU = I$, in which I is an identity matrix. Equivalently, we need to show

$$\sum_{i=0}^{M} v_{m,i} U(i,k) = \begin{cases} 1 & m = k, \\ 0 & m > k. \end{cases}$$

When $m = k$, since $U(m,m) = 1/\zeta_m^m$,

$$\sum_{i=0}^{M} v_{m,i} U(i,m) = v_{m,m} U(m,m) = 1.$$

For $m > k$,

$$\sum_{i=0}^{M} v_{m,i} U(i,k) = \sum_{i=k}^{m} v_{m,i} U(i,k).$$

In the following, we will show $\sum_{i=k}^{m} v_{m,i} U(i,k) = 0$, $m > k$. When $m = k+1$,

$$\begin{aligned}&\sum_{i=m-1}^{m} v_{m,i} U(i,k)\\ =&v_{m,m-1} U(m-1,m-1) + v_{m,m} U(m,m-1)\\ =&\zeta_{m-1}^m \frac{1}{\zeta_{m-1}^{m-1}} + \zeta_m^m \frac{-1}{\zeta_{m-1}^{m-1}\zeta_1^1}\\ =&0.\end{aligned}$$

When $m > k+1$, for any $r \in \{k+1, k+2, \ldots, m-1\}$, let

$$S_r \triangleq \sum_{i=r}^{m} v_{m,i} U(i,k) = \sum_{i=r}^{m} \frac{(-1)^{i-k} q^{-\frac{(i-k)(i-k-1)}{2}}}{\zeta_k^k \zeta_{i-k}^{i-k}} \zeta_i^m.$$

We use induction to prove

$$S_r = \frac{(-1)^{r-k} q^{-\frac{(r-k)(r-k-1)}{2}} \zeta_r^m}{\zeta_{r-k-1}^{r-k-1} \zeta_k^k (1 - q^{-(m-k)})} \triangleq W(r).$$

First, we have

$$\begin{aligned}S_{m-1} =& \frac{(-1)^{m-1-k} q^{-\frac{(m-1-k)(m-2-k)}{2}}}{\zeta_k^k \zeta_{m-1-k}^{m-1-k}} \zeta_{m-1}^m +\\ &\frac{(-1)^{m-k} q^{-\frac{(m-k)(m-k-1)}{2}}}{\zeta_k^k \zeta_{m-k}^{m-k}} \zeta_m^m\\ =& \frac{(-1)^{m-k-1} q^{-\frac{(m-k-1)(m-k-2)}{2}} \zeta_{m-1}^m}{\zeta_{m-k-2}^{m-k-2} \zeta_k^k (1 - q^{-(m-k)})}\\ =& W(m-1).\end{aligned}$$

Assume that

$$S_r = W(r) = \frac{(-1)^{r-k} q^{-\frac{(r-k)(r-k-1)}{2}} \zeta_r^m}{\zeta_{r-k-1}^{r-k-1} \zeta_k^k (1 - q^{-(m-k)})}.$$

Then

$$\begin{aligned}&S_{r-1}\\ =& \frac{(-1)^{r-k-1} q^{-\frac{(r-k-1)(r-k-2)}{2}} \zeta_{r-1}^m}{\zeta_k^k \zeta_{r-k-1}^{r-k-1}} + S_r\\ =& \frac{(-1)^{r-k-1} q^{-\frac{(r-k-1)(r-k-2)}{2}} \zeta_{r-1}^m}{\zeta_{r-k-2}^{r-k-2} \zeta_k^k (1 - q^{-(m-k)})}\\ =& W(r-1).\end{aligned}$$

By induction on r, we have

$$S_{k+1} = W(k+1) = \frac{-\zeta_{k+1}^m}{\zeta_k^k(1-q^{-(m-k)})}.$$

Thus

$$\begin{aligned} S_k &= S_{k+1} + \frac{\zeta_k^m}{\zeta_k^k} \\ &= \frac{-\zeta_{k+1}^m}{\zeta_k^k(1-q^{-(m-k)})} + \frac{\zeta_k^m}{\zeta_k^k} \\ &= 0. \end{aligned}$$

The proof is completed. □

Lemma 6. *For any m and r, it holds that*

$$c_0 \le \zeta_r^m \le 1, \quad \forall m, r, \tag{27}$$

where $c_0 := \lim_{m\to\infty} \zeta_m^m > 0$.

Proof of Lemma 6: Note that

$$\begin{aligned} c_0 &= \lim_{m\to\infty} \prod_{i=1}^m (1-q^{-i}) \\ &= \exp\left(\sum_{i=1}^{\infty} \ln(1-q^{-i})\right). \end{aligned} \tag{28}$$

Observe that the series $\sum_{i=1}^{\infty} \ln(1-q^{-i})$ is convergent since the ratio

$$\lim_{i\to\infty} \left| \frac{\ln(1-q^{-i-1})}{\ln(1-q^{-i})} \right| = \lim_{i\to\infty} \frac{q^{-i-1}}{q^{-i}} = q^{-1} < 1.$$

As a consequence, the term c_0 in (28) is well-defined and $c_0 > 0$. Then

$$0 < c_0 \le \zeta_r^m \le 1, \quad \forall m, r.$$

■

Lemma 7. *For $i = 2, \dots, M$, it holds that if the field size $q \ge 2M$,*

$$\sum_{j=1}^{i} j u_{i,j} \ge \frac{1}{2}.$$

Proof. Define $J_u(i,j) := j u_{i,j}$. By calculation, for $0 \le w \le \lfloor \frac{i}{2} \rfloor - 1$ it holds that

$$\begin{aligned} & J_u(i, i-2w) + J_u(i, i-2w-1) \\ &= (i-2w)\frac{(-1)^{2w} q^{-\frac{(2w)(2w-1)}{2}}}{\zeta_{i-2w}^{i-2w}\zeta_{2w}^{2w}} + \\ &\qquad (i-2w-1)\frac{(-1)^{2w+1} q^{-\frac{(2w+1)(2w)}{2}}}{\zeta_{i-2w-1}^{i-2w-1}\zeta_{2w+1}^{2w+1}} \\ &= \frac{q^{-\frac{(2w)(2w-1)}{2}}}{\zeta_{i-2w}^{i-2w}\zeta_{2w+1}^{2w+1}} \Big\{ (i-2w)(1-q^{-(2w+1)}) \\ &\qquad -(i-2w-1)q^{-2w}(1-q^{-(i-2w)}) \Big\} \\ &\ge q^{-\frac{(2w)(2w-1)}{2}}/2, \end{aligned} \tag{29}$$

where the relation in (29) holds due to (27) and $q \ge 2M$. We give the specific discussion as follows, let

$$\begin{aligned} A(w) &= (i-2w)(1-q^{-(2w+1)}), \\ B(w) &= (i-2w-1)q^{-2w}(1-q^{-(i-2w)}). \end{aligned}$$

When $w = 0$,

$$\begin{aligned} A(0) - B(0) &= i(1-q^{-1}) - (i-1)(1-q^{-i}) \\ &\ge i(1-q^{-1}) - (i-1) \\ &= 1 - i/q \\ &\ge 1 - i/(2M) \\ &\ge 1/2; \end{aligned}$$

When $w > 0$,

$$\begin{aligned} & A(w) - B(w) \\ &= (i-2w)(1-q^{-(2w+1)}) - (i-2w-1)q^{-2w}(1-q^{-(i-2w)}) \\ &\ge (i-2w)\cdot 1/2 - (i-2w-1)\cdot 1/2 \\ &= 1/2, \end{aligned}$$

since $q^{-(2w+1)} \le 1/2$, $q^{-2w} \le 1/2$ and $1 - q^{-(i-2w)} < 1$.

When i is even,

$$\sum_{j=1}^{i} J_u(i,j) = \sum_{w=0}^{\lfloor \frac{i}{2} \rfloor - 1} \Big(J_u(i, i-2w) + J_u(i, i-2w-1) \Big);$$

when i is odd,

$$\begin{aligned} \sum_{j=1}^{i} J_u(i,j) &= \sum_{w=0}^{\lfloor \frac{i}{2} \rfloor - 1} \Big(J_u(i, i-2w) + J_u(i, i-2w-1) \Big) \\ &\quad + u_{i,1} \\ &> \sum_{w=0}^{\lfloor \frac{i}{2} \rfloor - 1} J_u(i, i-2w) + J_u(i, i-2w-1). \end{aligned}$$

For any i, leveraging the relation (29) implies

$$\sum_{j=1}^{i} J_u(i,j) \ge J_u(i,i) + J_u(i,i-1) \ge 1/2. \tag{30}$$

□

Lemma 8. *Suppose that $1 - P_{\text{out}}(r) - M/N \ge c$ for some constant $c > 0$. For $i = 2, \dots, M$, it holds that*

$$\frac{\lambda_i}{\lambda_1} \ge 1 - e^{-2Nc^2}.$$

Proof: For $i = 2, \dots, M$, we find

$$\begin{aligned} \frac{\lambda_i}{\lambda_1} &= \frac{\sum_{k=i}^{N} f(k; N, P_{\text{out}}(r))\zeta_i^k}{\sum_{k=1}^{N} f(k; N, P_{\text{out}}(r))\zeta_1^k} \\ &\ge c_0 \sum_{k=i}^{N} f(k; N, P_{\text{out}}(r)), \end{aligned}$$

where the inequality is from the relation in Lemma 6. Based on the tail bound of the cumulative density function (CDF) of the binominal distriubtion,

$$\frac{\lambda_i}{\lambda_1} \geq 1 - \exp\left\{-2N\left(1 - P_{\text{out}}(r) - \frac{i-1}{N}\right)^2\right\}.$$

Suppose $\frac{M}{N} \leq 1 - P_{\text{out}}(r) - c$, then

$$1 - P_{\text{out}}(r) - \frac{i-1}{N} \geq 1 - P_{\text{out}}(r) - \frac{M}{N} \geq c,$$

and hence

$$\frac{\lambda_i}{\lambda_1} \geq 1 - \exp(-2Nc^2).$$

■

Appendix D
Proof of Theorem 3

Proof of Theorem 3-1):

By [22, Lemma 17], when $M = O(1)$ and $N = O(\ln L)$,

$$\max_N \frac{\mathbb{E}[\text{rank}(\mathbf{H}_L)]}{N} = \Theta\left(\frac{\ln \frac{1}{P_{\text{out}}(r) + \left(1 - P_{\text{out}}(r)\right)/q}}{\ln L}\right).$$

Then

$$\sup_{N \in \mathbb{N}^+, r \in \mathbb{Q} \cap [0, r_{\max}]} \frac{r\,\mathbb{E}[\text{rank}(\mathbf{H}_L)]}{N} = \Theta\left(\frac{r \ln \frac{1}{P_{\text{out}}(r) + \left(1 - P_{\text{out}}(r)\right)/q}}{\ln L}\right).$$

Due to $0 \leq P_{\text{out}}(r) \leq 1$,

$$1 \geq P_{\text{out}}(r) + (1 - P_{\text{out}}(r))/q \geq 1/q.$$

Since there exists $r_0 > 0$ such that $P_{\text{out}}(r_0) < 1$,

$$\sup_{N \in \mathbb{N}^+, r \in \mathbb{Q} \cap [0, r_{\max}]} \frac{r\,\mathbb{E}[\text{rank}(\mathbf{H}_L)]}{N} = \Theta(1/\ln L),$$

and when r is fixed with $P_{\text{out}}(r) \in (0,1)$, $R_L^{(2)}(M, N, r) = \Theta(1/\ln L)$. ■

Proof of Theorem 3-2): We take a constant r that is independent of hop length L and satisfies $0 < P_{\text{out}}(r) < 1$. Leveraging the expression of expected rank function in (25), we find

$$\begin{aligned}
&\max_N \frac{1}{N}\mathbb{E}[\text{rank}(\mathbf{H}_L)] \\
&= \max_N \frac{\lambda_1^L v_{M,1} u_{1,1}}{N}\left(1 + \sum_{i=2}^{M} \frac{\lambda_i^L v_{M,i}}{\lambda_1^L v_{M,1} u_{1,1}} \sum_{j=1}^{i} j u_{i,j}\right) \\
&= \max_N \Omega\left(\frac{\lambda_1^L}{N}\left(1 + \sum_{i=2}^{M} \frac{\lambda_i^L}{\lambda_1^L} \sum_{j=1}^{i} j u_{i,j}\right)\right),
\end{aligned}$$

where the last relation is because

$$v_{M,1} u_{1,1} = \zeta_1^M / \zeta_1^1 \geq c_0/(1 - q^{-1}), \tag{31a}$$

$$\frac{v_{M,i}}{v_{M,1} u_{1,1}} \geq c_0(1 - q^{-1}). \tag{31b}$$

We pick M so that $M/N \leq 1 - P_{\text{out}}(r) - c$ for some constant $c > 0$. From Lemma 7 and Lemma 8 in Appendix C, it also holds that $\sum_{j=1}^{i} j u_{i,j}$ and $\lambda_i^L / \lambda_1^L$ are uniformly lower bounded for $i = 2, \ldots, M$, which implies

$$\max_N \frac{\mathbb{E}[\text{rank}(\mathbf{H}_L)]}{N} = \max_N \Omega\left(\frac{M\lambda_1^L}{N}(1 - e^{-2Nc^2})^L\right).$$

From [22, Lemma 17] we know $\frac{\lambda_1^L}{N} = \Theta(1/\ln L)$ and $(1 - e^{-2Nc^2})^L = \Theta(1)$ when $N \in [\ln L, 2\ln L]$. In such case,

$$\max_N \frac{1}{N}\mathbb{E}[\text{rank}(\mathbf{H}_L)] = \Omega\left(\frac{M}{\ln L}\right).$$

Then taking $M = \Theta(\ln L)$ gives the rate $\Omega(1)$. When r is fixed with $P_{\text{out}}(r) \in (0,1)$, $R_L^{(2)}(M, N, r) = \Theta(1)$. The proof is completed as the optimal rate is always upper bounded by a constant. ■