

# On the Optimal Block Length for Joint Channel and Network Coding

Christian Koller\*, Martin Haenggi\*, Jörg Kliewer†, and Daniel J. Costello, Jr.\*

\*Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, USA

Email: {ckoller, mhaenggi, costello.2}@nd.edu

†Klipsch School of Electrical and Computer Engineering, New Mexico State University, Las Cruces, NM 88003, USA

Email: jkliwer@nmsu.edu

**Abstract**—Channel coding alone is not sufficient to reliably transmit a message of finite length from a source to one or more destinations. To ensure that no data is lost, channel coding on the physical layer needs to be combined with rateless erasure correcting schemes such as automatic repeat request (ARQ) or random linear network coding (RLNC) on a higher layer. In this paper we consider channel coding on a binary symmetric channel and random linear network coding for erasure correction. Given a message of length  $K$  and network coding over a finite Galois field of size  $q$ , we obtain the optimal number of blocks for network coding that minimizes the expected number of transmissions. We consider both a single link and broadcast to  $n$  destinations. As the field size of network coding gets large and the expected coding overhead in blocks becomes small, we show that, given our assumptions, the benefit of using a larger channel coded block outweighs the advantage of employing network coding over many blocks and the optimal number of number of blocks tends to one, making RLNC equivalent to simple ARQ.

## I. INTRODUCTION

We consider a message of finite length  $K$  that is transmitted from a source to one or more destinations using wireless broadcast over independent binary symmetric channels (BSCs). In this setting, channel coding alone is not sufficient to guarantee reliable communication. To ensure that no data is lost, channel coding on the physical layer needs to be combined with rateless erasure correcting schemes such as automatic repeat request (ARQ) [1] or random linear network coding (RLNC) [2].

RLNC has recently been shown to improve network performance for broadcast and multicast scenarios. Considering packet erasure channels on the link layer, RLNC has been shown to improve throughput and delay in wireless broadcast scenarios [3]–[6]. In [6] the joint design of network coding and MAC protocols was considered.

In contrast to the above work, we consider the joint design of channel and network coding. We assume that the size of a block is not predetermined and, given a finite total message length  $K$ , the source may choose the optimal number of blocks so that the throughput of the overall system is maximized.

The joint design and optimal rate allocation between channel and network coding for the block fading channel has been investigated in [7]–[9], where the tradeoff between the two

schemes is analyzed as the block length on the physical layer gets large and the probability of block erasure is given by the outage probability of the block fading channel.

Joint error and erasure correcting coding for the finite message length regime was analyzed in [10], [11]. In [11] the interaction of RLNC and continuous-time orthogonal waveform channels is investigated. In [10] the authors bound the performance of random coding on the physical and link layer using error exponents. Both papers aim to maximize throughput given a maximum delay constraint.

In contrast, in this paper we use RLNC in a rateless fashion to achieve reliable communication as in, e.g. file transfer. Thus we do not enforce a maximum delay constraint but use the expected number of transmissions at the source as the performance metric. More specifically we aim to answer the questions:

- Given a RLNC scheme over a finite Galois field of size  $q$  and a message length  $K$ , what is the optimum number of blocks  $m$  that the source should use to broadcast the message?
- What is the optimal channel coding rate for the individual blocks to minimize the expected number of transmissions?

In our analysis, we take the coding overhead of RLNC into account. Similar to other rateless coding schemes [12], [13], RLNC over a finite Galois field  $q$  exhibits a coding overhead, i.e., a receiver on average needs to correctly receive more than  $m$  blocks in order to decode. Note that the coding overhead is a property of the code itself and different from the signaling overhead. The signaling overhead of RLNC can be made very small, e.g., by synchronizing a pseudo-random number generator between the source and the destinations, so we neglect it in this paper.

## II. SYSTEM MODEL

We consider joint channel and network coding to broadcast a message of length  $K$  from one source to  $n$  destinations as shown in Fig. 1. The source is connected to each of the destinations via an i.i.d. memoryless BSC with the identical crossover probability  $p$ . As shown in Fig. 2, the source splits the message into  $m$  blocks  $B_i$ ,  $i = 1, \dots, m$ , of length  $k = K/m$ . The source then performs RLNC over the  $m$  blocks using a code over a finite Galois field  $q$ .

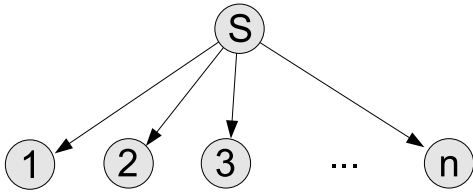


Fig. 1. Broadcast from one source to  $n$  destinations over independent BSCs.

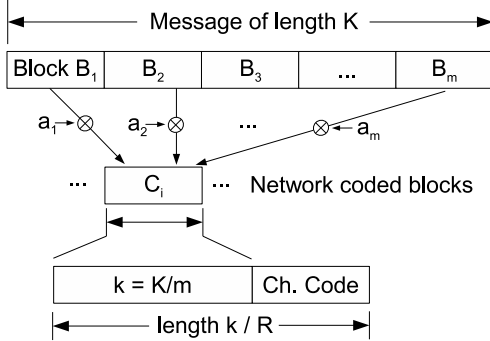


Fig. 2. The source divides the message of length  $K$  into  $m$  blocks. RLNC is done to create network coded blocks. Each coded block is individually protected by a channel code of rate  $R$ .

To create a network coded block  $C_i$ , the source randomly chooses a vector  $\mathbf{a}$  of length  $m$  of coefficients from  $\text{GF}(q)$ . The network coded block  $C_i$  is then the linear combination of the  $m$  blocks multiplied by the vector  $\mathbf{a}$

$$C_i = \sum_{j=1}^m a_j B_j.$$

Each block  $C_i$  is protected by a channel code of rate  $R$ . We consider random coding on the physical layer and bound the performance of the channel code using the error exponent for the BSC. After the transmission of each block, feedback is used to report the decoding success or failure to the source. We assume that feedback from the destinations is instantaneous and reliable. We now describe the code properties of channel and network coding in more detail.

#### A. Channel coding

The block error probability  $\epsilon(K, m, R, p)$  of random coding on the BSC can be bounded using the random coding error exponent  $E(R)$ :

$$\epsilon(K, m, R, p) = e^{-\frac{KE(R)}{mR}}. \quad (1)$$

Below a critical rate  $R_{crit}$  the random coding error exponent for the BSC is given by

$$E(R) = R_0 - R, \quad (2)$$

where  $R_0$  is the cutoff rate of the channel which depends on the crossover probability  $p$  of the BSC and is given by [14]

$$R_0 = \ln(2) - \ln(1 + 2\sqrt{p(1-p)}).$$

Above the critical rate, an upper bound on the block error probability is given by using the sphere packing exponent. Throughout the analysis in this paper, we assume that for all rates the error exponent is given by (2). In this way we are

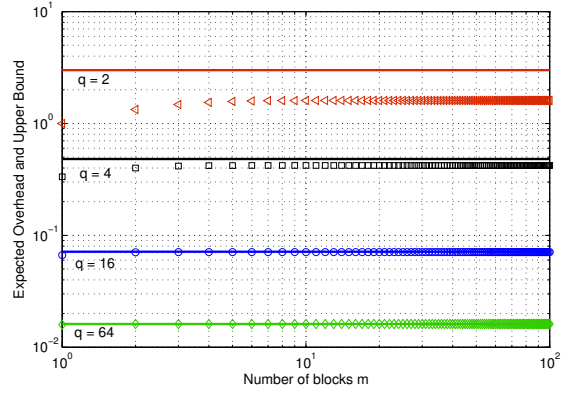


Fig. 3. Expected overhead  $X(q, m)$  (markers) and the upper bound on the expected overhead  $X_q$  (solid lines).

not able to code beyond the cutoff rate of the channel, but we expect the block error probabilities for small to medium block lengths that we obtain to be closer to the performance of existing coding schemes, such as Reed-Solomon codes or convolutional codes.

#### B. Random linear network coding

The network coding coefficients  $\mathbf{a}$  of every correctly received block  $C_i$  corresponds to a column in the received matrix  $\mathbf{A}$ . Once a receiver has collected  $m$  linearly independent columns, it can recover the message using Gaussian elimination. On average, more than  $m$  received blocks are needed to do so. Given  $m + x$  correctly received blocks, the probability that a decoding attempt fails is given by [15]

$$\mathbb{P}_F(m, x, q) = 1 - \prod_{i=1}^m (1 - q^{-x-i}), \quad (3)$$

where we call  $x$  the coding overhead. The expected overhead  $X(q, m)$  of RLNC in blocks is given by [16]

$$X(q, m) = \sum_{i=1}^m \frac{1}{q^i - 1}. \quad (4)$$

We now use a result from [15] to bound (3) as

$$q^{-x-1} \leq \mathbb{P}_F(x, q) < \frac{1}{q-1} q^{-x}, \quad (5)$$

which can be used to derive an upper bound on the expected overhead of RLNC that is independent of the coding window size  $m$ . The probability that overhead  $x = i$  is required to decode is upper bounded by

$$\begin{aligned} \mathbb{P}(x = i, q) &= \mathbb{P}_F(i-1, q) - \mathbb{P}_F(i, q) \\ &< \frac{1}{q-1} q^{-i+1} - q^{-i-1} = \frac{q^2 - q + 1}{q(q-1)} q^{-i}, \end{aligned} \quad (6)$$

and the expected overhead is thus upper bounded by

$$X(q, m) < \frac{q^2 - q + 1}{q(q-1)} \sum_{i=1}^{\infty} i q^{-i} = \frac{q^2 - q + 1}{(q-1)^3} \triangleq X_q. \quad (7)$$

For  $q > 2$  and  $K > 1$ , (7) is tighter than the two bounds presented in [16]. Also, the upper bound becomes tighter as

the field size  $q$  increases. Fig. 3 shows the overhead of RLNC for several Galois field sizes  $q$ . The larger the Galois field size  $q$ , the better the performance of RLNC, and the quicker the expected overhead converges to a constant. In the analysis of Section III we model the expected overhead of RLNC to be a constant fractional block independent of the number of blocks  $m$ , which is a very good model for larger Galois fields.

### III. UNICAST TO ONE DESTINATION

In this section we focus on the case where one source transmits to  $n = 1$  destination and is constrained to use RLNC on the link layer. The performance of ARQ is achieved as the size of the Galois field gets large. The expected number of blocks that the source needs to transmit is given by

$$\mathbb{E}(M_1) \leq \frac{m + X_q}{1 - \epsilon(K, m, R, p)}. \quad (8)$$

Using (1) and (2) we obtain

$$\mathbb{E}(M_1) \leq \frac{K(1 + X_q/m)}{R(1 - \exp\{-\frac{K}{m}(R_0/R - 1)\})} \quad (9)$$

for the expected number of channel symbols sent by the source. To minimize the expected number of symbols sent, we use the partial derivatives of (9) with respect to  $R$  and  $m$  to find the optimal channel coding rate and the optimal number of blocks, respectively. It can be shown that (9) is convex in both  $R$  and  $m$ , so that a minimum indeed exists.

#### A. The optimal channel coding rate

Taking the partial derivative of (9) with respect to  $R$  and setting it to zero, we obtain

$$1 - e^{-k(\frac{R_0}{R} - 1)} - k \frac{R_0}{R} e^{-k(\frac{R_0}{R} - 1)} = 0,$$

where  $k = K/m$  is the block length of the channel code. Substituting  $t = k \frac{R_0}{R}$ , we obtain

$$-(t + 1)e^{-(t+1)} = -e^{-k+1},$$

which can be solved using the Lambert-W function  $W(x)$ , where the Lambert-W function is the solution to

$$x = W(x)e^{W(x)}.$$

The optimal channel coding rate as a fraction of the cutoff rate of the channel is then given by

$$\frac{R}{R_0} = \frac{-k}{W_{-1}(-e^{-(k+1)}) + 1}. \quad (10)$$

For negative arguments, the Lambert-W function has two solutions. However, since the ratio  $R/R_0$  must be between zero and one, we require  $W(x) \leq -1$ . So the solution must be on the lower branch of the Lambert-W function, denoted by  $W_{-1}(x)$ . The optimal channel coding rate ratio  $R/R_0$  is only a function of the block length  $k$  and is independent of the expected overhead of RLNC. It is thus also the optimal channel coding rate for a scheme employing ARQ. Later, in Fig. 5, it is shown as the  $n = 1$  curve. As the block length  $k$  increases, the optimal channel coding rate ratio  $R/R_0$  tends to 1.

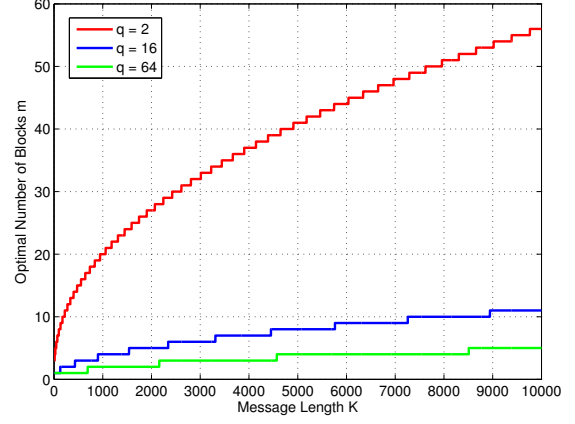


Fig. 4. Optimal number of blocks  $m$  given the message length  $K$  for RLNC over different Galois field sizes. Transmission to  $n = 1$  destination.

To evaluate the Lambert-W function we use the closed form approximation [17]

$$W_{-1}(x) \approx \ln(-x) - \frac{1}{A_1} \left[ 1 - \frac{1}{1 + \frac{A_1 \sqrt{\sigma/2}}{1 - A_2 \sigma \exp\{-A_3 \sqrt{\sigma}\}}} \right],$$

where

$$\sigma = -\ln(-x) - 1,$$

$A_1 = 0.3361$ ,  $A_2 = 0.0042$ , and  $A_3 = 0.0201$ . The approximation has a maximum relative error of only 0.025%.

#### B. The optimal number of blocks

Taking the partial derivative of (9) with respect to  $m$ , we obtain

$$e^{\frac{K}{m}(\frac{R_0}{R} - 1)} = \left( 1 + \left( \frac{K}{X_q} + \frac{K}{m} \right) \left( \frac{R_0}{R} - 1 \right) \right)$$

for the optimal number of blocks  $m$ , given a fixed channel coding rate ratio  $R/R_0$ . We can again use the Lambert-W function to solve for  $m$ , and the optimum number of blocks  $m$ , given  $R$ , is

$$m = \frac{-W_{-1}(-e^{-(1+zK/X_q)}) + 1 + zK/X_q}{zK}, \quad (11)$$

where  $z = R_0/R - 1$ .

To obtain the optimal number of blocks  $m$  that minimizes the expected number of transmissions we solve (11) and (10) jointly, using

$$z = \frac{W_{-1}(-e^{-(K/m+1)}) + K/m + 1}{-K/m} \quad (12)$$

in (11). Fig. 4 shows the optimal number of blocks  $m$  given a message length  $K$  and RLNC over  $GF(q)$ . The upper bound on the expected overhead (7) is not very tight for  $q = 2$ : however, the expected overhead  $X(2, m)$  converges fairly quickly and is basically constant for  $m \geq 10$ . In the computation of the optimal number of blocks for  $q = 2$ , we therefore use  $X(2, 100)$  instead of  $X_q$  in (11). As the message length  $K$  increases, we observe that minimum number of transmissions

at the source is achieved for a larger number of blocks  $m$ . On the other hand, since the expected coding overhead in blocks decreases with increasing Galois field size, the optimal number of blocks decreases in  $q$ , making the size  $k$  of the blocks larger, implying stronger channel coding so that the individual blocks are less likely to be erased.

### C. Large Galois field considerations

A common assumption in the analysis of network coding is that RLNC is done over a sufficiently large Galois field that the coding overhead is negligible, i.e.,  $X_q \approx 0$  for large  $q$ . If we set  $X_q = 0$  in (9), the only dependence on  $m$  is in the error exponent in the denominator. So the smallest possible  $m$ , i.e.,  $m = 1$ , minimizes the expected number of transmissions. Thus, in the absence of a coding overhead, the optimal strategy for the source is to use a channel code on the whole message and not divide it up into smaller blocks.

If only one block is being transmitted, there is no reason to multiply that block with a randomly chosen coefficient, and RLNC becomes equivalent to a ARQ, where the whole message is repeated until it is received correctly by the destination.

## IV. BROADCAST TO $n > 1$ DESTINATIONS

We begin this section by considering wireless broadcast to  $n > 1$  destinations using ARQ, where every block is repeated by the source until all destinations received it correctly.

### A. Broadcast using ARQ

The expected number of blocks that the source needs to transmit is given by [5]

$$\mathbb{E}_{\text{ARQ}}(M_n) = \sum_{i=0}^{\infty} 1 - (1 - \epsilon(K, m, R, p))^i. \quad (13)$$

After some straightforward manipulations we can transform (13) into the finite sum

$$\mathbb{E}_{\text{ARQ}}(M_n) = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} \frac{1}{1 - p^i}$$

and using (1) and (2) we obtain

$$\mathbb{E}_{\text{ARQ}}(N_n) = \sum_{i=1}^n (-1)^{i+1} \binom{n}{i} \frac{K}{R \left(1 - e^{-i \frac{K}{m} (R_0/R - 1)}\right)}$$

for the expected number of transmissions. Again, since the number of blocks  $m$  only appears in the error exponent, it follows that the best strategy for the source is to encode and transmit the whole message at once and repeat it if necessary. So for ARQ, we obtain  $m = 1$  as the optimal number of blocks and  $k = K$ . For the optimal channel coding rate ratio we use the partial derivative w.r.t.  $R$  to obtain

$$\sum_{i=1}^n (-1)^i \binom{n}{i} \frac{1 - e^{-izK} i \frac{KR_0}{R} e^{-izK}}{(1 - e^{-izK})^2} = 0, \quad (14)$$

with  $z = R_0/R - 1$ . For  $n = 1$ , (14) reduces to (10) and for larger  $n$ , we numerically find the zero crossing of (14). The optimal rate ratio  $R/R_0$  for different numbers of destinations

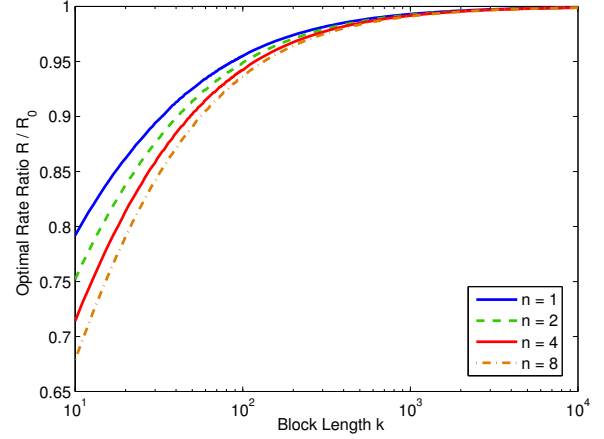


Fig. 5. Optimal channel coding rate  $R$  as a fraction of the cutoff rate  $R_0$  for different block lengths  $k$ . For broadcast using ARQ, we have  $k = K$ .

is shown in Fig. 5. While the optimal number of blocks stays constant at  $m = 1$ , the optimal channel coding rate  $R$  as a fraction of the cutoff rate  $R_0$  decreases as the number of broadcast destinations increases.

### B. Broadcast using RLNC

The expected number of blocks that the source needs to transmit using RLNC broadcast is given by [5]

$$\mathbb{E}_{\text{RLNC}}(M_n) = m + \sum_{i=m}^{\infty} 1 - \left[ \sum_{j=m}^i (1 - \epsilon(K, m, R, p))^j \epsilon(K, m, R, p)^{i-j} \mathbb{P}_S(m, j - m, q) \right]^n, \quad (15)$$

where the probability of successful decoding given a received overhead of  $x$  blocks is

$$\mathbb{P}_S(m, x, q) = \prod_{i=1}^m (1 - q^{-x-i}).$$

We solve the above multidimensional optimization problem using numerical methods. Fig. 6 shows the optimal number of blocks given RLNC over GF(64) as the number of broadcast destinations  $n$  increases. The optimal number of blocks  $m$  increases with the number of broadcast destinations  $n$ . When considering broadcasting to a fixed number of destinations and increasing the size of the Galois field of RLNC, we see the same behavior as reported in the previous section for one link. Fig. 7 shows the optimal number of blocks given  $n = 32$  broadcast destinations. The optimal number of blocks again decreases with increasing Galois field size  $q$ . A large Galois field idealization of RLNC is obtained by setting  $\mathbb{P}_S(m, x, q) = 1$  in (15) for all  $x \geq 0$ . In this case, the optimal number of blocks is again  $m = 1$  and RLNC becomes equivalent to ARQ. The expected number of transmissions that the source must perform per message symbol is shown in Fig. 8. We multiply the expected number of transmissions per message symbol by the channel cutoff rate  $R_0$  to get a curve that is independent of the quality of the underlying BSC. The idealized RLNC or ARQ scheme with  $m = 1$  requires

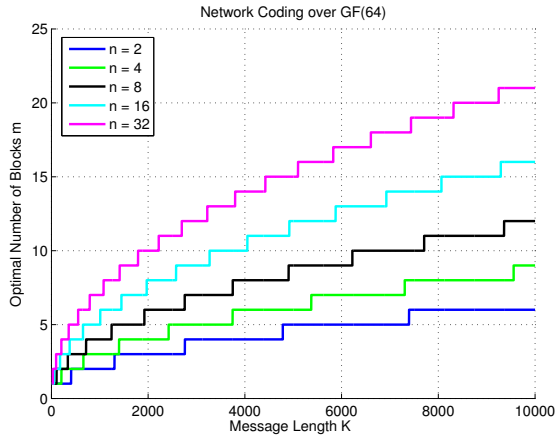


Fig. 6. Optimal number of blocks for RLNC over GF(64) as the number of broadcast destinations  $n$  increases

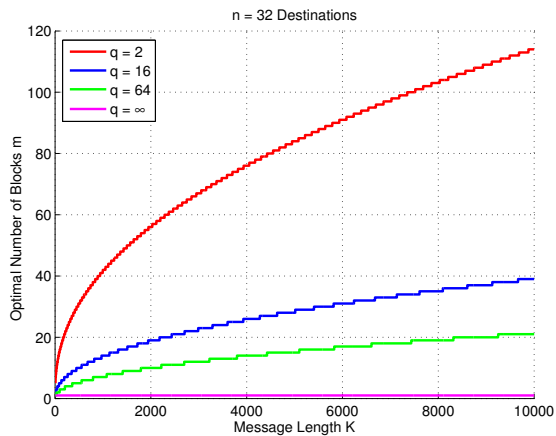


Fig. 7. Optimal number of blocks  $m$  for  $n = 32$  broadcast destinations as the Galois field size of RLNC increases.

the least amount of transmissions, while RLNC over smaller Galois fields performs worse.

## V. CONCLUSIONS

We analyzed the joint design of channel coding for the binary symmetric channel on the physical layer and random linear network coding on the link layer. For RLNC over a finite field of size  $q$  and a message of length  $K$ , we obtain the optimal number of blocks that should be used to minimize the expected number of transmissions at the source. Under the conditions assumed in this paper, we find that, as the field size of RLNC gets large and the expected coding overhead of RLNC in blocks becomes small, the benefit of using a larger channel coded block outweighs the advantage of employing network coding over many blocks and the optimal number of blocks tends to one, thereby making RLNC equivalent to ARQ. Surprisingly this holds for the single link as well as the broadcast scenario, although the broadcast case has been highlighted in the literature as a prime example where performance gains can be achieved using network coding when only the link layer is considered. Irrespective of the number of destinations  $n$ , we find that the optimal number of blocks tends to one as the coding overhead tends to zero. Whether or not this same conclusion holds true in the case of time-varying

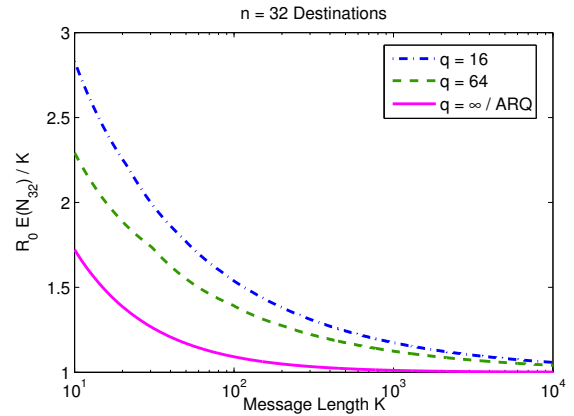


Fig. 8. Expected number of transmissions per message symbol for RLNC broadcast, weighted by the cutoff rate  $R_0$ .

channels when  $n$  is greater than 1 is the subject of ongoing research.

## REFERENCES

- [1] S. Lin, D.J. Costello, and M.J. Miller, "Automatic repeat-request error control schemes," *IEEE Communications Mag.*, vol. 22, no. 12, pp. 5–17, Dec. 1984.
- [2] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.
- [3] D. S. Lun, M. Médard, R. Koetter, and M. Effros, "On coding for reliable communication over packet networks," *Physical Comm.*, vol. 1, no. 1, pp. 3–20, 2008.
- [4] A. Eryilmaz, A. Ozdaglar, M. Médard, and E. Ahmed, "On the delay and throughput gains of coding in unreliable networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5511–5524, Dec. 2008.
- [5] M. Ghaderi, D. Towsley, and J. Kurose, "Network coding performance for reliable multicast," in *Proc. IEEE Military Comm. Conf.*, Orlando, FL, Oct. 2007.
- [6] Y.E. Sagduyu and A. Ephremides, "On joint MAC and network coding in wireless ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3697–3713, Oct. 2007.
- [7] T. Cui, T. Ho, and J. Kliewer, "Achievable rate and optimal physical layer rate allocation in interference-free wireless networks," in *Proc. IEEE Int. Symposium on Inform. Theory*, Seoul, Korea, July 2009.
- [8] C. Berger, S. Zhou, Y. Wen, P. Willett, and K. Pattipati, "Optimizing joint erasure- and error-correction coding for wireless packet transmissions," *IEEE Trans. Wireless Commun.*, vol. 58, no. 11, pp. 4586–4595, Nov. 2008.
- [9] T. A. Courtade and R. D. Wesel, "Optimal allocation of redundancy between packet-level erasure coding and physical-layer channel coding in fading channels," to appear in *IEEE Trans. Comm.*, 2011.
- [10] M. Vehkaperä and M. Médard, "A throughput-delay trade-off in packetized systems with erasures," in *Proc. IEEE Int. Symposium on Inform. Theory*, Adelaide, Australia, Sept. 2005.
- [11] M. Xiao, "Cross-layer design of rateless random network codes for delay optimization," Cape Town, South Africa, July 2010.
- [12] M. Luby, "LT codes," in *Proc. of the 43rd Annual IEEE Symp. on Foundations of Comp. Sc.*, Vancouver, Canada, Nov. 2002, pp. 271–280.
- [13] A. Shokrollahi, "Raptor codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2551–2567, June 2006.
- [14] A. Barg and G.D. Forney, "Random codes: Minimum distances and error exponents," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2568–2573, Sept. 2002.
- [15] G. Liva, E. Paolini, and M. Chiani, "Performance versus overhead for fountain codes over  $\mathbb{F}_q$ ," *IEEE Commun. Lett.*, vol. 14, no. 2, pp. 178–180, 2010.
- [16] D.E. Lucani, M. Médard, and M. Stojanovic, "Random linear network coding for time-division duplexing: Field size considerations," in *Proc. IEEE Global Telecommun. Conf.*, Honolulu, HI, Mar. 2009.
- [17] D.A. Barry, J.-Y. Parlange, G.C. Sander, and M. Sivaplan, "A class of exact solutions for Richards' equation," *Journal of Hydrology*, vol. 142, pp. 1993.