Delay-Complexity Trade-off of Random Linear Network Coding in Wireless Broadcast

Rina Su†, Qifu Tyler Sun†*, Zhongshan Zhang‡

† Department of Communication Engineering, University of Science and Technology Beijing, P. R. China
‡ School of Information and Electronics, Beijing Institute of Technology, P. R. China

Abstract

In wireless broadcast, random linear network coding (RLNC) over GF(2^L) is known to asymptotically achieve the optimal completion delay with increasing L. However, the high decoding complexity hinders the potential applicability of RLNC schemes over large GF(2^L). In this paper, a comprehensive analysis of completion delay and decoding complexity is conducted for field-based systematic RLNC schemes in wireless broadcast. In particular, we prove that the RLNC scheme over GF(2) can also asymptotically approach the optimal completion delay per packet when the packet number goes to infinity. Moreover, we introduce a new method, based on circular-shift operations, to design RLNC schemes which avoid multiplications over large GF(2^L). Based on both theoretical and numerical analyses, the new RLNC schemes turn out to have a much better trade-off between completion delay and decoding complexity. In particular, numerical results demonstrate that the proposed schemes can attain average completion delay just within 5% higher than the optimal one, while the decoding complexity is within 3 times the one of the RLNC scheme over GF(2).

Index Terms

Wireless broadcast, random linear network coding, circular-shift, completion delay, decoding complexity

* Q. T. Sun (Email: qfsun@ustb.edu.cn) is the corresponding author.
I. INTRODUCTION

Wireless broadcast is an important transmission scenario with a variety of applications. For example, in a satellite or cellular network, a satellite or base station needs to broadcast a large file or streaming multimedia data to many users in a timely manner. Such applications require cost efficient transmission techniques. In the literature, linear network coding (LNC) has shown great ability to substantially improve transmission efficiency, and two main types of LNC techniques were extensively studied for wireless broadcast, namely random linear network coding (RLNC) [1]–[7] and instantly decodable network coding (IDNC) [8]–[11].

RLNC [12] linearly combines all original packets at the sender with coefficients randomly and independently selected from a finite field to generate coded packets for transmission without feedback. IDNC [8], [13] can be regarded as a special type of deterministic LNC schemes, defined over GF(2), for the wireless broadcast with feedback. Every coded packet generated by IDNC is specially designed based on receivers’ side information obtained from the feedback, so as to enable as many receivers as possible to recover an original packet upon receiving the coded packet.

Though IDNC focuses more on the instantaneous decodability at receivers, compared with RLNC, it requires higher completion delay, which is a fundamental metric for transmission efficiency and refers to the total number of packets broadcast from the sender till all receivers successfully recover all original packets. It is well-known that when the finite field is sufficiently large, RLNC can achieve the optimal completion delay. However, a stringent issue that hinders the potential applicability of RLNC schemes over a large finite field is the very high decoding complexity. In the present paper, for wireless broadcast, we make a comprehensive analysis of completion delay and decoding complexity for field-based RLNC schemes and introduce a new method, based on circular-shift operations, to design RLNC schemes with a much better trade-off between completion delay and decoding complexity. Only systematic RLNC schemes are considered here because they can reduce the packet decoding delay and encoding/decoding complexity [10]. The main contributions of the present paper are summarized as follows.

• For RLNC schemes over the finite field GF(2^L), we provide explicit formulae for the expected completion delay and theoretically analyze the decoding complexity in terms of the total number of binary operations required for decoding. One may note that Ref. [5] analyzed the expected completion delay for a non-systematic RLNC scheme. Since the
present paper focuses on systematic RLNC schemes, both analysis details and formulae obtained are different from those in [5].

- Even though RLNC schemes over GF(2^L) are known to asymptotically achieve the optimal completion delay with increasing L, we prove that the RLNC scheme over GF(2) can also asymptotically approach the optimal completion delay per packet with the increasing packet number. This intriguing property implies that for the case that the packet number is extremely large, which is impractical though, the RLNC scheme over GF(2) is optimal for both completion delay and decoding complexity.

- Inspired by the negligible computational complexity and hardware amenability of the circular-shift operations on a binary sequence, we propose a new method to design RLNC schemes which replace multiplications in a large finite field by circular-shifts. It is worthwhile noting that prior to this work, circular-shifts have been adopted in [14]–[16] for LNC design in different transmission scenarios other than wireless broadcast, but redundant bits need to be added in their construction of circular-shift LNC. However, the present method does not introduce extra bits in the generation of coded packets. Besides, the proposed new method introduces a new parameter p_0 to control the probability of coding coefficients to be zero.

- We analyze our proposed schemes both theoretically and numerically, which verify that the proposed schemes provide a much better trade-off between completion delay and decoding complexity. In particular, the expected completion delay of the proposed schemes is proved to be no larger than that of the conventional RLNC scheme over GF(q) with q ≤ 1/p_0. Moreover, numerical results demonstrate the average completion delay converges very fast to the optimal one (e.g., when the packet number is 20, the average completion delay is just within 5% higher than the optimal one), while the average number of binary operations for decoding is just within 3 times that of the RLNC scheme over GF(2).

The remainder of the paper is organized as follows. Section II first establishes the system model, and then analyzes the completion delay and decoding complexity of conventional field-based RLNC schemes. Section III introduces and analyzes our proposed RLNC schemes based on circular-shift operations. The performances are numerically compared in Section IV. Finally, Section V concludes the paper.
II. SYSTEM MODEL AND ANALYSIS OF CONVENTIONAL RLNC SCHEMES

A. System Model

Consider a single-hop erasure broadcast system without feedback, in which a unique sender attempts to broadcast $P$ packets to $R$ receivers. Every packet consists of $M$ bits. In each timeslot, the sender can broadcast one packet to all receivers. The memoryless wireless channels between the sender and the receivers are subject to random packet erasures with erasure probability $1 - p_r$ at receiver $r$. Every receiver is interested in recovering all $P$ original packets.

All RLNC transmission schemes studied in this paper are systematic, that is, in the first phase of transmission, the sender will sequentially broadcast all $P$ original (uncoded) packets $m_1, m_2, \ldots, m_P$. In the second phase of transmission, the sender will broadcast coded packets, which are linearly generated based on $P$ original packets, till every receiver can recover all $P$ original packets. The completion delay $D$ of an RLNC scheme is the number of coded packets transmitted by the sender in phase two.

The conventional RLNC scheme is defined over the extension field $\text{GF}(2^L)$, where every packet is regarded as a row vector of $\frac{M}{L}$ symbols over $\text{GF}(2^L)$. Every packet broadcast by the sender is a $\text{GF}(2^L)$-linear combination of $m_1, m_2, \ldots, m_P$. Specifically, every coded packet $m_{P+d}$, $d \geq 1$, randomly generated by the source in phase two can be expressed as

$$m_{P+d} = \sum_{j=1}^{P} \gamma_j m_j,$$

where the coding coefficients $\gamma_j$ are independently and uniformly selected from $\text{GF}(2^L)$. In order to indicate receivers how a packet $m_{P+d} = \sum_{j=1}^{P} \gamma_j m_j$ is formed from the original $P$ packets, the coding vector $f_{P+d} = [\gamma_1, \ldots, \gamma_P]^T$ consisting of $P$ coding coefficients is appended to $m_{P+d}$ as a header. The coding vectors for $P$ original packets form an identity matrix of size $P$, i.e., $[f_j]_{1 \leq j \leq P} = I_P$. When a receiver $r$ obtains $P$ packets whose coding vectors are linearly independent, the $P$ original packets can be decoded at $r$.

When $L$ is large enough, the RLNC scheme over $\text{GF}(2^L)$ can be approximately regarded as the perfect RLNC scheme [11], in which every $P$ packets generated by the source have linearly independent coding vectors. The prefect RLNC scheme is optimal in terms of completion delay $D$. However, the computational complexity of this scheme in both encoding and decoding is

\footnote{For simplicity we assume $L$ divides $M$. In practice, $M$ is much larger than $L$ and dummy bits can be padded into a packet so that $L$ divides $M$.}
high because multiplication in GF($2^L$) has to be invoked. On the contrary, the RLNC scheme over GF(2), i.e. with $L = 1$, only requires bitwise additions among packets in both encoding and decoding. As a result, it involves lowest computational complexity among RLNC schemes, but its completion delay $D$ is relatively higher.

As the conventional RLNC schemes will be the benchmarks for our new proposed RLNC schemes, the following two subsections theoretically analyze their performance in terms of completion delay and decoding complexity.

**B. Completion Delay Analysis**

Throughout the paper, unless otherwise specified, for a considered RLNC scheme, let $D_r$ denote the number of coded packets transmitted in phase two by the source till receiver $r$ is able to successfully recover all $P$ original packets. Then, the completion delay $D$ can be defined as

$$D = \max\{D_1, D_2, \ldots, D_R\},$$

and the expectation of $D$ can be characterized as

$$\mathbb{E}[D] = \sum_{d \geq 0} \Pr(D > d) = \sum_{d \geq 0} \left(1 - \prod_{1 \leq r \leq R} \Pr(D_r \leq d)\right).$$

Consider the conventional RLNC scheme over GF($q$), where $q = 2^L$. At receiver $r$, denote by $U_r$ the number of successfully received uncoded packets in phase one, and assume that for the $U_r$ uncoded packets and all the coded packets successfully received, the columnwise juxtaposition of their coding vectors forms a matrix of rank $U_r + j$. When receiver $r$ successfully obtains a new coded packet, note that the probability for the new packet to be innovative, i.e., its coding vector is linearly independent of the previous ones, is $1 - q^{U_r+j-P}$. For brevity, write

$$p'_{r,U_r+j} = p_r(1 - q^{U_r+j-P}).$$

Assume $U_r = u$. When $u = P$, all the original packets have already been successfully received during the first $P$ rounds of transmission, so that $D_r = 0$. When $u < P$, receiver $r$ still requires to receive $P - u$ innovative coded packets. Thus, $D_r$ can be expressed as

$$D_r = A_1 + A_2 + \ldots + A_{P-u},$$

where $A_j, 1 \leq j \leq P - u$, represents the number of packets obtained by receiver $r$ during the process that the number of innovative packets at receiver $r$ increases from $u + j - 1$ to $u + j$. Thus, for $a_j \geq 1$,

$$\Pr(A_j = a_j) = (1 - p'_{r,u+j-1})^{a_j-1}p'_{r,u+j-1}.$$
Consequently, for \( d > 0 \), the conditional probability of \( D_r \) equal to \( d \) given \( U_r = u \) can be characterized as

\[
\Pr(D_r = d|U_r = u) = \begin{cases} 
0, & u = P, u < P - d \\
\sum_{a \in A_{P-u,d}} \prod_{j=1}^{P-u} (1 - p'_{r,a+j-1})^{a_j-1} p'_{r,u+j-1}, & \text{otherwise}
\end{cases}
\]

where \( A_{P-u,d} \) is defined as the collection of \((P-u)\)-tuples \( a = (a_1, \ldots, a_{P-u}) \) subject to \( a_1, \ldots, a_{P-u} \in \mathbb{Z}^+ \) and \( a_1 + \ldots + a_{P-u} = d \). Note that \( u < P - d \) expresses the case that the number of successfully received packets by receiver \( r \) is less than \( P \), not sufficient to recover all \( P \) original packets. Based on (7), the probability distribution of \( D_r \) can be formulated as

\[
\Pr(D_r = 0) = p_r^P
\]

and for \( d > 0 \),

\[
\Pr(D_r = d) = \sum_{u = \max\{0, P - d\}}^{P-1} \binom{P}{u} p_r^u (1 - p_r)^{P-u} \Pr(D_r = d|U_r = u).
\]

By plugging (8) into (3), we can get a formula to compute the expected value of \( D \) for the conventional RLNC scheme over GF(\( q \)). Even though the computation of \( \mathbb{E}[D] \) in terms of (3) involves an infinite term summation, the term \( 1 - \prod_{1 \leq r \leq R} \Pr(D_r \leq d) \) converges to 0 quickly when \( d \) increases. Therefore, a very close approximate for \( \mathbb{E}[D] \) can be obtained based on (3) when \( P \) is not large.

Note that the above analysis on \( \mathbb{E}[D] \) also applies to an odd prime power \( q \), though such \( q \) is not the focus of this paper.

When \( q \) increases, \( p'_{r,u+j} \) tends to 1 for all \( U_r + j < P \), so that the completion delay of the RLNC scheme over GF(\( q \)) approaches to the one of the perfect RLNC scheme, where as long as \( P \) packets are received by receiver \( r \), the original \( P \) packets can be recovered. For the perfect RLNC scheme, \( P + D_r \) follows the negative binomial distribution with the probability mass function as \( \Pr(D_r = d) = \binom{P+d-1}{d} p_r^P (1 - p_r)^d, d \geq 0 \). Recall that for positive integers \( a \) and \( b \), the regularized incomplete beta function \( I_x(a, b+1) \) can be expressed in the following combinatorial manner \( I_x(a, b+1) = \sum_{j=0}^{b} \binom{a+j-1}{a-1} x^j (1-x)^{a} \). As a result, for the perfect RLNC scheme, \( \Pr(D_r \leq d) = I_{p_r}(P, d+1) \), and

\[
\mathbb{E}[D] = \sum_{d \geq 0} (1 - \prod_{1 \leq r \leq R} I_{p_r}(P, d+1)).
\]

For a given packet number \( P \), let \( D^{GF(2^L)} \) and \( D^{perf} \) respectively denote the completion delay of the RLNC scheme over GF(\( 2^L \)) and the perfect RLNC scheme. It is well known that \( D^{GF(2)} \)
has the largest value. However, the next theorem unveils an inherent connection between $D_{GF(2)}$ and $D_{perf}$.

**Theorem 1.** $\lim_{P \to \infty} \mathbb{E}[D_{GF(2)}]/P = \lim_{P \to \infty} \mathbb{E}[D_{perf}]/P$.

**Proof:** Please refer to Appendix A.

C. Decoding Complexity Analysis

For the conventional RLNC scheme over $GF(2^L)$, assume that receiver $r$ has successfully obtained $U_r$ uncoded packets $m'_1, \ldots, m'_{U_r}$ and $P - U_r$ coded packets $m'_{U_r+1}, \ldots, m'_P$, whose coding vectors are linearly independent. We next analyze the number of binary operations required to recover the original $P$ packets $m_1, \ldots, m_P$ from $m'_1, \ldots, m'_P$. Assume $m_j = m'_j$ for all $1 \leq j \leq U_r$. Further, in this subsection, denote the coding vector for $m'_j$ by $f_j = [\gamma_{j1} \ldots \gamma_{jP}]^T$, so that $m'_j = \sum_{1 \leq j' \leq P} \gamma_{jj'} m_{j'}$.

The decoding process consists of two phases. In phase I, receiver $r$ removes the information of uncoded packets $m'_1, \ldots, m'_{U_r}$ from coded packets $m'_{U_r+1}, \ldots, m'_P$, and resets $f_{U_r+1}, \ldots, f_P$ by respectively restricting to their last $P - U_r$ entries. Specifically, for $U_r + 1 \leq j \leq P$, reset $m'_j$ as

$$m'_j = m'_j - \sum_{1 \leq j' \leq U_r} \gamma_{jj'} m'_{j'}.$$  \hspace{1cm} (10)

After phase I, the coded packets $m'_{U_r+1}, \ldots, m'_P$ are purely linear combinations of $m_{U_r+1}, \ldots, m_P$, and the updated coding vectors become $(P - U_r)$-dimensional. Write $\mathcal{A} = \{m'_{U_r+1}, \ldots, m'_P\}$.

The decoding process of phase II consists of two steps to recover $m_{U_r+1}, \ldots, m_P$ from $m'_{U_r+1}, \ldots, m'_P$. In the first step of phase II, recursively perform the following procedure. From $\mathcal{A}$, select a coded packet, denoted by $m'_{j_0}$, whose coding vector contains only one nonzero entry, say, $\gamma_{joj'}$. Thus, $m'_{j_0} = \gamma_{joj'} m'_{j'}$. Remove $m'_{j_0}$ from $\mathcal{A}$, recover $m_{j'}$ by the operation $\gamma_{joj'}^{-1} m'_{j_0}$. For every remaining coded packet $m'_j$ in $\mathcal{A}$, reset it by subtracting $m'_{j'}$ from $m'_j$ via

$$m'_j = m'_j - \gamma_{jj'} m'_{j'}.$$  \hspace{1cm} (11)

Restrict the coding vector for $m'_j$ to an $|\mathcal{A}|$-dimensional one by deleting the position where $\gamma_{jj'}$ locates. The above recursive procedure ends till the updated $|\mathcal{A}|$-dimensional coding vector for every coded packet in $\mathcal{A}$ contains at least two nonzero entries, that is, each of the remaining coded packets in $\mathcal{A}$ is a linear combination of at least two original packets.
After the first step of phase II decoding, if $A$ is empty, it means all $P$ original packets have been successfully recovered. Otherwise, continue to perform the second step. Without loss of generality, assume $A = \{m'_{P-|A|+1}, \ldots, m'_P\}$, and $m_{P-|A|+1}, \ldots, m_P$ are the remaining original packets to be recovered from $A$. In step two, first compute the inverse matrix, denoted by $D = [\beta_{jj'}]_{1 \leq j,j' \leq |A|}$, of the columnwise juxtaposition matrix of $|A|$-dimensional coding vectors for packets in $A$. Then, the original packet $m_{P-|A|+j}$, $1 \leq j \leq |A|$, can be recovered by

$$m_{P-|A|+j} = \sum_{1 \leq j' \leq |A|} \beta_{jj'} m'_{P-|A|+j'}.$$  

(12)

We now analyze the binary operation number involved in the above decoding process. Follow the same consideration in [15], assume it takes $L$ binary operations to compute the addition of two elements in GF($2^L$), and at least $2L^2$ binary operations to compute the multiplication of two elements in GF($2^L$). Since every packet contains $M/L$ symbols over GF($2^L$), it takes at least $M/(2L^2 + L)$ binary operations to compute one term $m'_j - \gamma_{jj'} m'_j$ for nonzero $\gamma_{jj'}$ in (10). In addition, since the probability for $\gamma_{jj'}$ to be nonzero equals to $(2^L - 1)/2^L$, it can be easily deduced that the number of binary operations required for receiver $r$ in the decoding process of phase I is

$$U_r(P - U_r) \frac{2L - 1}{2^L} \frac{M}{L}(2L^2 + L)$$

(13)

In the first step of phase II decoding, the recursive procedure takes $P - U_r - |A|$ iterations, where $A$ refers to the final set of coded packets after the first step. The number of binary operations required in this step at receiver $r$ is

$$\sum_{j=|A|+1}^{P-U_r} \left( \frac{M}{L}(2L^2) + (j - 1) \frac{2L - 1}{2^L} \frac{M}{L}(2L^2 + L) \right)$$

(14)

In the second step of phase II decoding, it takes additional

$$\phi(D) \frac{M}{L}(2L^2) + (\phi(D) - |A|) \frac{M}{L}$$

(15)

binary operations to recover the last $|A|$ original packets according to (12), where $\phi(D)$ refers to the number of nonzero entries in the decoding matrix $D$. We remark here that the computational complexity to compute the inverse matrix $D$ is ignored, because in practice the packet length $M$ and the number of symbols $M/L$ is much larger than the size $|A|$ of $D$.

Throughout the paper, $[A_{jj'}]_{j,j'}$ denotes the matrix generated by $A_{jj'}$, with $j$ and $j'$ respectively representing the column and the row index.
For the case that \( L \) is large, since every random coding coefficient is nonzero with high probability, the probability to perform step 1 of phase II decoding is low. As a consequence, we can assume that the decoding matrix \( D \) is of size \( P - U_r \), and \( \phi(D) = (P - U_r)^2 \). Based on (13) and (15), the number of binary operations for decoding is approximated as \( M[(2L + 1)P - 1](P - U_r) \). As \( E[U_r] = Pp_r \) and \( E[U_r^2] = Pp_r(Pp_r - p_r + 1) \), the expected number of binary operations for decoding is

\[
MP[(2L + 1)P - 1](1 - p_r) 
\]

For the case \( L = 1 \), as there is no need to do multiplication in an extension field, it takes \( U_rM \) binary operations to compute (10). In addition, instead of (15), where \( \phi(D) \) needs to be approximated, we can choose an alternative lower bound \( M(|A| - 1) \) on the number of binary operations required to recover the last \( |A| \) original packets from the coded packets in \( A \). In total, the expected number of binary operations for decoding is lower bounded by

\[
\frac{M}{2} [(P^2 - P)p_r(1 - p_r) + 3|A| - 2].
\]

### III. Proposed Circular-Shift RLNC Schemes

For RLNC schemes over large GF(\( 2^L \)), though it can approach a near optimal completion delay, the decoding complexity becomes much higher because the decoding process involves heavy multiplications in GF(\( 2^L \)). One possible way to alleviate the decoding complexity imposed by extension field multiplication is to use sparse encoding vectors. This inspired us to increase the probability of zero coding coefficients in RLNC scheme design. Furthermore, in order to avoid extension-field multiplication, Ref. [15] motivates us to adopt circular-shift operations in RLNC design. It turns out that compared with the perfect RLNC scheme, the proposed *circular-shift RLNC* schemes, have comparative completion delay but a much lower decoding complexity.

#### A. Scheme Description

Hereafter in this paper, let \( L \) be an even integer such that \( L + 1 \) is a prime with primitive root 2, that is, the multiplicative order of 2 modulo \( L + 1 \) is equal to \( L \). Denote by \( C_{L+1}^L \) the \((L + 1) \times (L + 1)\) cyclic permutation matrix \[
\begin{bmatrix}
0 & I_L \\
1 & 0
\end{bmatrix}
\]. For a binary sequence \( m \) of length \( L + 1 \), the linear operation \( mC_{L+1}^l, 1 \leq l \leq L + 1 \), is equivalent to a circular-shift of \( m \) by \( l \) bits to the right. Define another \( L \times (L + 1) \) matrix \( G \) and \((L + 1) \times L \) matrix \( H \) over GF(2) by

\[
G = [I_L \ 1], H = [I_L \ 0]^T,
\]

(18)
i.e., the first $L$ columns in $G$ and the first $L$ rows in $H$ are identity matrix, while all entries in the last column in $G$ equal to 1 and all entries in the last row in $H$ equal to 0.

Write

$$C = \{0, GC_{L+1}H, GC_{L+1}^2H, \ldots, GC_{L+1}^{L+1}H\}.$$  \hspace{1cm} (19)

Note that $GC_{L+1}^{L+1}H = I_L$.

Same as in the previous section, regard every packet $m_j$ of $M$ bits as a row vector $[s_{j,1}, s_{j,2}, \ldots, s_{j,M}]$ of $\frac{M}{L}$ symbols, where every symbol $s_{j,j'}$ itself is merely regarded as an $L$-dimensional row vector over $GF(2)$ rather than an element in $GF(2^L)$. For a given $\Gamma \in C$, denote by $\Gamma \circ m_j$ the following linear operation on $m_j$

$$\Gamma \circ m_j = [s_{j,1}\Gamma, s_{j,2}\Gamma, \ldots, s_{j,M}\Gamma],$$  \hspace{1cm} (20)

that is, to perform symbol-wise multiplication by $\Gamma$ on $m_j$.

Same as in the conventional systematic RLNC schemes, for the proposed circular-shift RLNC scheme, the sender will first sequentially broadcast $P$ original $M$-bit packets $m_1, m_2, \ldots, m_P$ and then random linear combinations $m_{P+1}, m_{P+2}, \ldots, m_{P+D}$ of the $P$ original packets till every receivers can recover all $P$ original packets. The random linear combinations are based on the linear operations $\circ$ with coefficients selected from $C$. Specifically, every coded packet $m_{P+d}, d \geq 1$, can be expressed as

$$m_{P+d} = \sum_{j=1}^{P} \Gamma_j \circ m_j,$$  \hspace{1cm} (21)

where the coding coefficients $\Gamma_j$ are randomly and independently selected from $C$ according to

$$\Pr(\Gamma_j = \Gamma) = \begin{cases} p_0, & \Gamma = 0 \\ \frac{1-p_0}{L+1}, & \Gamma \in C \setminus \{0\} \end{cases}$$  \hspace{1cm} (22)

Note that when coding coefficients are generated, there is a particular parameter $p_0$ to control the probability of 0 to occur. The more frequent occurrence of 0 in the coding coefficients will help reduce the decoding complexity at receivers, but will increase the completion delay. We shall assume that $p_0$ is a rational number no smaller than $1/(L+2)$. When $p_0 = 1/(L+2)$, the probability to choose 0 is same as to choose a particular nonzero coding coefficient from $C$.

Since the proposed RLNC schemes inherit the linearity among vectors with the (matrix) coefficients selected from $C$, they belong to vector linear network coding \cite{17}.

\footnote{Throughout the paper, 1 and 0 refer to an all-one matrix and an all-zero matrix, respectively. The size of 0 or 1, if not explicitly explained, can be inferred in the context.}
By a slight abuse of notation, define the coding vector of a packet to be a \( PL \times L \) matrix over \( \text{GF}(2) \) as follows. Every coding vector can be regarded as a \( P \times 1 \) block matrix which is a coding coefficient (matrix) belonging to \( C \). For an original (uncoded) packet \( m_j, 1 \leq j \leq P \), the \( j \)th block in its coding vector \( F_j \) is the identity matrix \( I_L \), while all other blocks are \( L \times L \) zero matrices. Thus, \( \{F_j\}_{1 \leq j \leq P} = I_{PL} \). For a coded packet \( m_{P+d} = \sum_{j=1}^{P} \Gamma_j \circ m_j \), its coding vector \( F_{P+d} \) is defined as \( F_{P+d} = [\Gamma_1^T \Gamma_2^T \ldots \Gamma_P^T]^T \). As there are only \( L+2 \) possible choices for coding coefficients, only \( \lfloor P \log_2(L+2) \rfloor \) bits are sufficient in the packet header to store the coding coefficient information.

For \( J \geq 2 \), assume that receiver \( r \) has successfully received \( J-1 \) packets, and denote by \( F \) the \( PL \times (J-1)L \) matrix over \( \text{GF}(2) \) obtained by column-wise juxtaposition of the coding vectors for the \( J-1 \) packets. For the \( J \)th successfully received packet with the coding vector \( F_J \), it is said to be innovative if \( \text{rank}(F_J F) - \text{rank}(F) = L \). As long as a receiver obtains \( P \) innovative packets, that is, their coding vectors can be columnwise juxtaposed into a \( PL \times PL \) full rank matrix over \( \text{GF}(2) \), the \( P \) original packets can be decoded at \( r \).

We next analyze the completion delay of the proposed circular-shift RLNC scheme. Let \( 2 \leq J \leq P \) and \( q \) be a prime power no larger than \( 1/p_0 \). Consider a \( PL \times JL \) matrix \( F_{J,\Gamma} = [\Gamma_{j,j'}]_{1 \leq j \leq J, 1 \leq j' \leq P} \) over \( \text{GF}(2) \) with \( \Gamma_{j,j'} \in C \) subject to

- the \( PL \times (J-1)L \) submatrix \( [\Gamma_{j,j'}]_{1 \leq j < J, 1 \leq j' \leq P} \) is full rank (over \( \text{GF}(2) \)),
- every \( \Gamma_{j,j'} \) is randomly selected from \( C \) according to the distribution prescribed in (22),

and another \( P \times J \) matrix \( F_{J,\gamma} = [\gamma_{j,j'}]_{1 \leq j \leq J, 1 \leq j' \leq P} \) over \( \text{GF}(q) \) with \( \gamma_{j,j'} \in \text{GF}(q) \) subject to

- the \( P \times (J-1) \) submatrix \( [\gamma_{j,j'}]_{1 \leq j < J, 1 \leq j' \leq P} \) is full rank,
- every \( \gamma_{j,j'} \) is independently and randomly selected from \( \text{GF}(q) \) with \( \Pr(\gamma_{j,j'} = \gamma) = 1/q \) for all \( \gamma \in \text{GF}(q) \).

Lemma 2. \( \Pr(\text{rank}(F_{J,\Gamma}) = JL) \geq 1 - p_0^{P-J+1} \geq \Pr(\text{rank}(F_{J,\gamma}) = J) \).

Proof: Please refer to Appendix [B]. \( \blacksquare \)

Consider the proposed circular-shift RLNC scheme with \( p_0 \geq 1/(L+2) \) and the conventional RLNC scheme over \( \text{GF}(q) \) with \( q \) a prime power no larger than \( 1/p_0 \). Denote by \( D_{\text{circ}} \) and by \( D_{\text{GF}(q)} \) their respective completion delay, as well as by \( D_{r,\text{circ}} \) and by \( D_{r,\text{GF}(q)} \) their respective
completion delay for receiver $r$. Thus, we have
\[ D_{\text{circ}} = \max\{D_{\text{circ}}^1, D_{\text{circ}}^2, \ldots, D_{\text{circ}}^R\} \]
\[ D_{\text{GF}(q)} = \max\{D_{\text{GF}(q)}^1, D_{\text{GF}(q)}^2, \ldots, D_{\text{GF}(q)}^R\} \]  

**Theorem 3.** $\mathbb{E}(D_{\text{circ}}) \leq \mathbb{E}(D_{\text{GF}(q)})$ and $\mathbb{E}(D_{\text{circ}}^r) \leq \mathbb{E}(D_{\text{GF}(q)}^r)$. 

**Proof:** Similar to (3),
\[ \mathbb{E}[D_{\text{circ}}^r] = \sum_{d \geq 0} \left(1 - \prod_{1 \leq r \leq R} \Pr(D_{\text{circ}}^r \leq d)\right), \]
\[ \mathbb{E}[D_{\text{GF}(q)}^r] = \sum_{d \geq 0} \left(1 - \prod_{1 \leq r \leq R} \Pr(D_{\text{GF}(q)}^r \leq d)\right). \tag{24} \]

Thus, it suffices to prove that for each receiver $r$ and $d \geq 0$,
\[ \Pr(D_{\text{circ}}^r \leq d) \geq \Pr(D_{\text{GF}(q)}^r \leq d) \forall d \geq 0, \tag{25} \]
whose proof can be found in Appendix-C. Since $\mathbb{E}(D_{\text{circ}}^r) = \sum_{d \geq 0} \left(1 - \Pr(D_{\text{circ}}^r \leq d)\right)$, $\mathbb{E}(D_{\text{GF}(q)}^r) = \sum_{d \geq 0} \left(1 - \Pr(D_{\text{GF}(q)}^r \leq d)\right)$, Eq. (25) implies $\mathbb{E}(D_{\text{circ}}^r) \leq \mathbb{E}(D_{\text{GF}(q)}^r)$. $\blacksquare$

In the proposed RLNC scheme, the set $C$ of $L \times L$ matrices for coding coefficient selection is particularly designed, so that the decoding complexity of the proposed scheme can be significantly reduced compared with the conventional RLNC scheme over $\text{GF}(2^L)$. The insights are as follows.

First, for every symbol $s$, i.e., a binary row vector of length $L$, when it is (right) multiplied by a binary matrix of size $L, L(L - 1)$ binary operations are required in general. However, for a nonzero matrix $\Gamma = GC_{L+1}^l H$ in $C$, it only requires $L - 1$ binary operations to compute $s\Gamma$, where the only binary operations are performed in computing $sG$ while the complexity of a circular-shift operation on a binary sequence can be ignored (See, e.g., [14] [15]). Moreover, the next proposition justifies that to compute $s\Gamma^{-1}$ only takes $L - 1$ binary operations as well.

**Proposition 4.** For a nonzero matrix $\Gamma = GC_{L+1}^l H$ in $C$,
\[ \Gamma G = GC_{L+1}^l, \tag{26} \]
\[ \Gamma^{-1} = GC_{L+1}^{l-1} H. \tag{27} \]

**Proof:** Observe that $HG = \begin{bmatrix} I_L & 1 \\ 0 & 0 \end{bmatrix} = I_{L+1} + [0 \ 1]$, where $[0 \ 1]$ refers to $(L + 1) \times (L + 1)$ matrix with all-zero entries in the first $L$ columns and all-one entries in the last column. Consequently, $(GC_{L+1}^l H)G = I_L + GC_{L+1}^l [0 \ 1]$. Because $C_{L+1}^l [0 \ 1] = [0 \ 1]$ and $G[0 \ 1] = 0$, ...
\[GC_L^{t+1}[0\ 1] = 0.\] Eq. (26) is thus proved. Due to (26), 
\[(GC_{L+1}^t H) (GC_{L+1}^{t+1} H) = GC_{L+1}^t C_{L+1}^{t+1} H = GI_{L+1} = I_L.\]

Moreover, for a positive integer \(J\), consider a full rank (over GF(2)) block matrix \(\Gamma_{jj'} \in \mathbb{R}\) with every nonzero block \(\Gamma_{jj'} = GC_{L+1}^{a_{jj'}} H\). We next provide a formula to concisely characterize the inverse matrix \(D = [B_{jj'}]_{1 \leq j, j' \leq J}\) of \(\Gamma_{jj'} \in \mathbb{R}\), where every block \(B_{jj'}\) is also an \(L \times L\) matrix. It turns out that for every block \(B_{jj'}\) in \(D\), to compute \(sB_{jj'}\) requires at most \(L(L + 1)/2 - 2\) binary operations, which are also fewer than the number \(L(L - 1)\) of binary operations to compute \(s\) multiplied by a general matrix.

Observe that the set \(\mathcal{R} = \{\sum_{t=0}^{L} a_t C_{L+1}^{t}, a_t \in GF(2)\}\) forms a commutative ring of circulant matrices of size \(L + 1\). In \(\mathcal{R}\), for every \(\Psi = \sum_{t=0}^{L} a_t C_{L+1}^{t}\), define \(\sigma(\Psi)\) of it as follows. If the number of nonzero coefficients \(\{a_0, a_1, \ldots, a_L\}\) is larger than \(L/2\), then \(\sigma(\Psi) = \sum_{t=0}^{L} (1 + a_t) C_{L+1}^{t}\), i.e., \(\sigma(\Psi) = \Psi + 1\). Otherwise, \(\sigma(\Psi) = \Psi\). In this way, \(\sigma(\Psi)\) is always a summation of at most \(L/2\) cyclic permutation matrices.

In addition, for every matrix \([\Psi_{jj'}]_{1 \leq j, j' \leq J}\) over \(\mathcal{R}\), though it can be regarded as a matrix of size \(J(L + 1)\) over GF(2), we impose the computation of its determinant to be conducted over \(\mathcal{R}\). Specifically, denote by \(\Lambda\) the determinant of \([\Psi_{jj'}]_{1 \leq j, j' \leq J}\) over \(\mathcal{R}\)
\[\Lambda = \det ([\Psi_{jj'}]_{1 \leq j, j' \leq J}) = \sum_{\tau \in S_J} \prod_{j=1}^{J} \Psi_{j\tau(j)},\]
where \(S_J\) refers to the permutation group consisting of all permutations on \(\{1, 2, \ldots, J\}\).

**Theorem 5.** Consider a full rank matrix \([G\Psi_{jj'} H]_{1 \leq j, j' \leq J}\), where \(\Psi_{jj'} \in \mathcal{R}\), its inverse matrix can be represented as the block matrix \(D = [B_{jj'}]_{1 \leq j, j' \leq J}\) with every block of \(L \times L\) matrix \(B_{jj'} \in \mathcal{R}\) defined as
\[G\sigma(A^{2L-2} \det(M_{jj'})) H,\]
where \(M_{jj'}\) is the matrix obtained from \([\Psi_{jj'}]_{1 \leq j, j' \leq J}\) by deleting its \(j'^{th}\) block row and \(j^{th}\) block column, and its determinant is also computed over \(\mathcal{R}\).

**Proof:** For \(1 \leq j, j' \leq J\), denote by \(B_{jj'}' \in \mathcal{R}\) the \(L \times L\) matrix
\[B_{jj'}' = A^{2L-2} \det(M_{jj'}'),\]
so that it is equivalent to show
\[[G\Psi_{jj'} H]_{1 \leq j, j' \leq J}[G\sigma(B_{jj'}')] H]_{1 \leq j, j' \leq J} = I_{JL}.\]
By application of Lemma 3 in [18], we can obtain the following proposition

\[
[G \Psi_{jj'}]_{1 \leq j, j' \leq J} [G B_{jj'}' H]_{1 \leq j, j' \leq J} = I_{JL}. \tag{32}
\]

Further, since Eq. (26) in Proposition 4 implies that for \( \Psi_1, \Psi_2 \in \mathcal{R} \),

\[
(G \Psi_1 H)(G \Psi_2 H) = G \Psi_1 \Psi_2 H, \tag{33}
\]

the following can be deduced from Eq. (32)

\[
[G \Psi_{jj'} H]_{1 \leq j, j' \leq J} [G B_{jj'}' H]_{1 \leq j, j' \leq J} = I_{JL}. \tag{34}
\]

By the definition of \( \sigma \), either \( \sigma(B_{jj'}') = B_{jj'}' \) or \( \sigma(B_{jj'}') = B_{jj'}' + 1 \). Since \( G1 = 0 \),

\[
[G \Psi_{jj'} H]_{1 \leq j, j' \leq J} [G \sigma(B_{jj'}') H]_{1 \leq j, j' \leq J} = [G \Psi_{jj'} H]_{1 \leq j, j' \leq J} [G B_{jj'}' H]_{1 \leq j, j' \leq J} = I_{JL}. \tag{35}
\]

**Example.** Assume \([\Psi_{jj'}]_{1 \leq j, j' \leq 3} = \begin{bmatrix} I_5 & C_5 & C_5 \\ I_5 & C_2^\mathcal{R} & C_3^\mathcal{R} \\ I_5 & C_3 & C_4 \end{bmatrix} \). One may check that \( \det([\Psi_{jj'}]_{1 \leq j, j' \leq 3}) = I_5 + C_5^3 \), and \([M_{jj'}]_{1 \leq j, j' \leq 3} = \begin{bmatrix} 0 & I + C_5^4 & C_3^3 + C_4^3 \\ C_5^3 + C_5^4 & C_5 + C_4^3 & C_5 + C_3^3 \\ C_5^2 + C_3^3 & C_5 + C_3^3 & C + C_3^2 \end{bmatrix} \). Based on (29), \([B_{jj'}]_{1 \leq j, j' \leq 3} = \begin{bmatrix} 0 & C_2^3 + C_5^4 & C_5 + C_3^3 \\ C_5 + C_3^3 & C_5 & C_5^3 \\ I_5 + C_5^2 & C_3^3 & C_5 + C_4^3 \end{bmatrix} \). One may further check that \( (I_3 \otimes G)[\Psi_{jj'}]_{1 \leq j, j' \leq 3} (I_3 \otimes H) [B_{jj'}]_{1 \leq j, j' \leq 3} = I_{12} \).

**Remark 1.** Compared with the circular-shift LNC scheme considered in [15], the one proposed in this paper does not introduce any redundant bit for transmission. The key is Eq. (26) in Proposition 4 which guarantees the correctness of Theorem 5. The insight brought about from (26) is that for arbitrary networks, every circular-shift LNC scheme with redundant bits for transmission may be theoretically transformed to a vector LNC scheme without redundant bits and with the coding coefficients selected from \( \mathcal{R} \). This topic is beyond the scope of this paper and will be investigated elsewhere.

A detailed discussion on the decoding process and the decoding complexity are given in next two subsections.
B. Decoding Algorithm

Assume that receiver $r$ has successfully obtained $U_r$ uncoded packets $m'_1, \ldots, m'_{U_r}$ and $P - U_r$ coded packets $m'_{U_r+1}, \ldots, m'_P$, such that their coding vectors can be columnwise juxtaposed into a $PL \times PL$ full rank matrix. Receiver $r$ remains to decode $P - U_r$ original packets from the coded packets $m'_{U_r+1}, \ldots, m'_P$. In this subsection, for $U_r + 1 \leq j \leq P$, denote by $F_j$ the coding vector, which is an $PL \times L$ matrix, for the coded packet $m'_j$.

Similar to the decoding process of the conventional RLNC schemes described in Section III, the decoding process of the proposed circular-shift RLNC scheme consists of two phases too. In phase I decoding, every coded packet $m'_j$, $U_r + 1 \leq j \leq P$, is updated in the following way

\[
m'_j = m'_j - \sum_{1 \leq j' \leq U_r} \Gamma_{j j'} \circ m'_{j'},
\]

so that the updated coded packets $m'_{U_r+1}, \ldots, m'_P$ are purely linear combinations of $m_{U_r+1}, \ldots, m_P$. Reset the coding vector $F_j$ for every updated coded packet $m'_j = \sum_{U_r+1 \leq j' \leq P} \Gamma_{j j'} \circ m'_{j'}$, $U_r + 1 \leq j \leq P$, to be the $(P - U_r)L \times L$ matrix $[\Gamma_{U_r+1}^{T} \Gamma_{U_r+2}^{T} \ldots \Gamma_{P}^{T}]^{T}$. Note that the $(P - U_r)L \times (P - U_r)L$ matrix $[F_j]_{U_r+1 \leq j \leq P}$ is full rank. Write $A = \{m'_{U_r+1}, \ldots, m'_P\}$.

In the first step of phase II decoding, recursively perform the following procedure. From $A$, select a coded packet denoted by $m'_{j_0}$, whose coding vector is regarded as a $(P - U_r) \times 1$ block matrix, contains only one nonzero block, say, $\Gamma_{j_0 j'}$. Thus, $m'_{j_0} = \Gamma_{j_0 j'} \circ m'_{j'}$. Remove $m'_{j_0}$ from $A$, recover the original packet $m_{j'}$ by the operation

\[
m_{j'} = \Gamma_{j_0 j'}^{-1} \circ m'_{j_0},
\]

where $\Gamma_{j_0 j'}^{-1}$ is the inverse matrix of $\Gamma_{j_0 j'}$ as formulated in (27). For every remaining coded packet $m'_j$ in $A$, reset it by

\[
m'_j = m'_j - \Gamma_{j j'} \circ m'_{j'},
\]

and reduce the coding vector for $m'_j$ to an $|A| \times 1$ block matrix by deleting the block where $\Gamma_{j j'}$ locates. The above recursive procedure ends till every remaining coded packet in $A$ is a linear combination of at least two original packets.

After the first step of phase II decoding, if $A$ is empty, then all $P$ original packets have been successfully recovered. Otherwise, $|A| \geq 2$, and continue to perform the second step. Without loss of generality, assume $A = \{m'_{P-|A|+1}, \ldots, m'_P\}$ and $m'_{P-|A|+1} = \sum_{j'=1}^{|A|} \Gamma_{j' j} \circ m_{P-|A|+j'}$.  

15
In step two, first arbitrarily find a nonzero coefficient, say $\Gamma'_{1,j_0}$, for coded packet $m'_{P-|A|+1}$, and reset
\begin{equation}
m'_{P-|A|+1} = \Gamma'_{1,j_0}^{-1} \circ m'_{P-|A|+1}.
\end{equation}

Next, update $m'_{P-|A|+j}$, $2 \leq j \leq |A|$, as
\begin{equation}
m'_{P-|A|+j} = m'_{P-|A|+j} - \Gamma'_{j,j_0} \circ m'_{P-|A|+1}.
\end{equation}

Concomitantly, for the $(|A| - 1) \times (|A| - 1)$ block matrix of $[\Gamma'_{j,j'} + \Gamma'_{1,j_0}^{-1} \Gamma'_{j,j_0}]_{1 \leq j,j' \leq |A|, j \neq 1, j' \neq j_0}$, compute its inverse matrix $D = [B_{j,j'}]_{1 \leq j,j' \leq |A|}$ according to Theorem 5. Then, the original packet $m_{P-|A|+j}$, $1 \leq j \leq |A|$ with $j \neq j_0$, can be recovered by
\begin{equation}
m_{P-|A|+j} = \sum_{2 \leq j' \leq |A|} B_{j,j'} \circ m'_{P-|A|+j'}.
\end{equation}

Finally, $m_{P-|A|+j_0}$ can be recovered via
\begin{equation}
m_{P-|A|+j_0} = m'_{P-|A|+1} - \sum_{j'=1, j' \neq j_0}^{(|A|)} (\Gamma'_{1,j_0}^{-1} \Gamma'_{1,j'}) \circ m_{P-|A|+j'}.
\end{equation}

**C. Decoding Complexity Analysis**

We now analyze the number of binary operations involved in the decoding process described in the above subsection. As the symbol-wise multiplication $C_{L+1}^t \circ m_j$ on a packet $m_j$ of $M$ bits involves no binary operations, it takes $M(2L-1)/L$ binary operations to compute $\Gamma \circ m_j + m'_j$ for $\Gamma \in \mathbb{C}\{0\}$. Since the probability of coding coefficients $\Gamma_{j,j'}$ in (50) to be a nonzero matrix is equal to $(1 - p_0)$, the number of binary operations required at a receiver for the decoding process of phase I is
\begin{equation}
(P - U_r)U_r(1 - p_0)\frac{M}{L}(2L - 1).
\end{equation}

In the first step of phase II decoding, the number of required binary operations is
\begin{equation}
\sum_{j=|A|+1}^{P-U_r} \frac{M}{L} ((L - 1) + (j - 1)(1 - p_0)(2L - 1))
\end{equation}
where $A$ refers to the final set of coded packets after the first step. In the second step of phase II decoding, it takes $(L - 1)\frac{M}{L}$ binary operations to compute (39), and $(|A| - 1)(2L - 1)\frac{M}{L}$ binary operations to update $m'_{P-|A|+j}$ in (40). Moreover, in (41), every block $B_{j,j'}$ can be expressed as $[G\Psi_{j,j'}H]_{1 \leq j,j' \leq |A|}$ according to Theorem 5 where $\Psi_{j,j'} \in \mathcal{R}$ is summation of at most $L/2$ cyclic permutation matrices. Thus, it takes at most $\frac{M}{L}(L(L+1)/2 - 2)$ binary operations to compute one term $B_{j,j'} \circ m'_{P-|A|+j'}$ in (41). It takes each receiver at most
\begin{equation}
(|A| - 1)^2 \frac{M}{L} \left(\frac{L(L+1)}{2} - 2\right) + (|A| - 1)(|A| - 2)\frac{M}{L}L
\end{equation}
binary operations to compute (41), where all $B_{jj'} = G\Psi_{jj'} H$ are assumed nonzero with $\Psi_{jj'}$ a summation of $L/2$ cyclic permutations matrices. Note that same as in the analysis of conventional RLNC schemes, we ignore the number of operations involved in obtaining $B_{jj'}$, since $|A|$ is relatively small. The number of binary operations in the final procedure (42) to recover the original packet $m_{P-|A|+j_0}$ is $2(|A| - 1)(1 - p_0)M$, where $1 - p_0$ represents the probability for every coefficient $\Gamma_{jj'}$ in (42) to be nonzero.

As $E[U_r] = Pp_r$ and $E[U_r^2] = Pp_r(Pp_r - p_r + 1)$, the expected number of binary operations for the whole decoding process is upper bounded by

$$M((P^2 - P)p_r(1 - p_r)(1 - p_0)(2 - \frac{1}{L}) + (|A| - 1)^2 \frac{L + 1}{2} + \frac{5L - 2 - 4p_0L + p_0}{L} + \frac{2p_0L - L - 1}{L})$$

(46)

**Remark 2.** If we allow one bit redundancy per symbol for transmission, then the proposed circular-shift RLNC scheme can be modified by randomly selecting the nonzero coding coefficients from the set $\{0, GC_{L+1}, GC_{L+1}^2, \ldots, GC_{L+1}^{L+1}\}$ instead of from $C$. In this way, every packet transmitted from the source in the modified scheme still consists $\frac{M}{L}$ symbols, but every symbol contains $L + 1$ bits. Based on (26), every packet transmitted by the modified scheme can be expressed as $\sum_{j=1}^{P}(\Gamma_j G) \circ m_j$. As a consequence, the decoding process described in the previous subsection can be slightly simplified so that a total of $P\frac{M}{L}(L - 1)$ binary operations can be saved at decoding. This is at a cost of $\frac{M}{L}$ extra bits per packet to be transmitted.

**IV. Numerical Analysis**

In this section, we present numerical results to compare the performance of the proposed RLNC schemes with conventional RLNC schemes. We assume that the system has 60 receivers and the packet erasure probability between the sender and every receiver is 0.15. In the figure legend, the conventional RLNC scheme over $GF(2^L)$ is labeled as “$GF(2^L)$”, and the proposed circular-shift RLNC scheme with symbol length $L$ and zero entry probability $p_0$ is labeled as “C-S $p_0$-0 L”.

Fig. 1 compares the average completion delay per packet of different RLNC schemes as a function of the number of packets $P$. One may observe that the average completion delay of every RLNC scheme, including the conventional one over $GF(2)$, converges to the one of perfect RLNC. This is in line with Theorem[1] Regardless of the choice of $L$ and $p_0$, and the convergence rates of our proposed schemes are higher than that of the conventional RLNC scheme over $GF(2)$. 

17
For instance, for the case $L = 4$, $p_0 = 1/3$, and $P = 20$, the average completion delay of the circular-shift RLNC scheme is only 4.3% higher than the delay of perfect RLNC, while the completion delay of GF(2)-RLNC is higher than that of the perfect RLNC by 48%. The results also show that for fixed $L$, with decreasing $p_0$, the average completion delay of the proposed scheme also decreases. However, for fixed $p_0$, the benefit to reduce the average completion delay is not so obvious by increasing the symbol length $L$ from 4 to 10.

Fig. 2(a) and (b) shows the decoding complexity performance of different RLNC schemes as a function of $P$. The decoding complexity is measured by the average number of binary operations required in the decoding process described in Sec. II-C and Sec. III-B, and the average number of binary operations for decoding depicted in Fig. 2 is normalized by the packet number $P$ and the packet length $M$. From Fig. 2(a), we can see that with increasing $P$, the decoding complexity of every RLNC scheme increases, while the increasing rates of our proposed schemes are much smaller than that of the conventional RLNC scheme over GF(2^4) and are close to that of the conventional RLNC over GF(2).

Fig. 2(b) depicts a clearer comparison of the decoding complexity between our proposed schemes and the RLNC scheme over GF(2). It illustrates that under the same symbol length $L$,
Fig. 2. Average number of binary operations for decoding per packet bit.

the larger the $p_0$ is, the closer the decoding complexity is to $\text{GF}(2)$. It is worthwhile noting that the decoding complexity in Fig. 2 for the RLNC scheme over $\text{GF}(2)$ is based on (17), so it is a
lower bound on the actual number of binary operations required for decoding. In comparison, the decoding complexity in Fig. 2 for the proposed RLNC scheme is based on (46), so it is an upper bound on the actual number of total binary operations required for decoding. Despite of this, one may observe that for the case \( L = 4 \) and \( p_0 = 1/3 \), when \( P \geq 20 \), the binary operation number for decoding by the new scheme is within only 2.5 times that of the RLNC scheme over \( GF(2) \).

V. Concluding Remarks

This paper made a comprehensive study on various systematic random linear network coding (RLNC) schemes for wireless broadcast without feedback. In particular, the newly proposed method to design RLNC schemes based on circular-shift operations presents itself as a new paradigm for RLNC design to have a much better trade-off between completion delay and decoding complexity. Compared with the original circular-shift linear network codes modeled over a (wireline) multicast network in [15], the main distinction of the circular-shift RLNC schemes proposed in the present paper is that no redundant bits need to be transmitted any more. Actually, if we allow a redundant bit to be added to every symbol, the decoding complexity of the proposed circular-shift RLNC schemes can be further reduced, at the cost of increasing the completion delay.

Appendix

A. Proof of Theorem 1

Define two new random variables \( N_r \) and \( Y_{r,N_r} \) as follows. \( N_r \) (\( N_r \geq P \)) represents the number of successfully received packets at receiver \( r \) till \( r \) can recover all \( P \) original packets from them, and \( Y_{r,N_r} \) (\( Y_{r,N_r} \geq P \)) represents the number of packets transmitted by the source till receiver \( r \) successfully obtains \( N_r \) packets. Equivalently,

\[
\Pr(D_{r, GF(2)} = d) = \sum_{n=0}^{d} \Pr(N_r = P + n)\Pr(Y_{r,N_r} = P + d | N_r = P + n)
\]

\[
= \sum_{n=0}^{d} \Pr(N_r = P + n)\Pr(Y_{r,P+n} = P + d). \tag{47}
\]

Note that \( D_{r}^{\text{perf}} = Y_{r,P} \), and generally \( Y_{r,P+n} \) also follows the negative binomial distribution and

\[
\Pr(Y_{r,P+n} = P + d) = \binom{P + d - 1}{n - 1} p_r^{P+n}(1 - p_r)^{d-n} \tag{48}
\]
In order to calculate \( \Pr(N_r = P + n) \), let \( U \) denote the number of uncoded packets among \( N_r \) successfully received packets, so that \( \Pr(N_r = P + n) \) can be further calculated by conditioning on \( U \). In the case \( U = P, \Pr(N_r = P|U = P) = 1 \) and \( \Pr(N_r = P + n|U = P) = 0 \) for \( n > 0 \). In the case \( U = u < P \), write

\[
A_{P-u} = \prod_{j=1}^{P-u} (1 - 2^{-j}) = \prod_{j=0}^{P-u-1} (1 - 2^{u+j-P}), \tag{49}
\]

so that

\[
\Pr(N_r = P + n|U = u) = \begin{cases} 
  A_{P-u}, & n = 0 \\
  A_{P-u} \sum_{u \leq k_1 \leq k_2 \leq \ldots \leq k_n < P} 2^{(k_1-P)+(k_2-P)+\ldots+(k_n-P)}, & n > 0
\end{cases} \tag{50}
\]

As \( U \) follows the binomial distribution with parameter \((P, p_r)\),

\[
\Pr(N_r = P + n) = \sum_{u=0}^{P} \Pr(U = u) \Pr(N_r = P + n|U = u)
= \sum_{u=0}^{P} \binom{P}{u} p_r^u (1 - p_r)^{P-u} \Pr(N_r = P + n|U = u). \tag{51}
\]

We next analyze the expression of \( \Pr(N_r = P + n|U = u) \) in (50). For \( j \geq 1 \), write \( A'_{j1} = 1 \) and recursively define \( A'_{jk} = \sum_{j' = 1}^{j} 2^{-j'} A'_{j'(k-1)} \) for \( k > 0 \). When \( n > 0 \) and \( u < P \), \( \Pr(N_r = P + n|U = u) \) can be expressed in terms of \( A'_{jk} \) as

\[
\Pr(N_r = P + n|U = u) = A_{P-u} \sum_{j' = 1}^{P-u} 2^{-j'} A'_{j'\delta_n}, \tag{52}
\]

where \( A_{P-u} \) is defined in (49). Because \( A'_{jk} \) can be alternatively expressed as

\[
A'_{jk} = 2^{-j} A'_{j(k-1)} + A'_{(j-1)k},
\]

it can be inductively deduced that \( \Pr(N_r = P + n|U = u) \) exponentially decreases and converges to 0 when \( n \) increases, and \( \Pr(N_r = P + n|U = u) \) also converges as \( P - u \) increases. For instance, Table I lists the probability \( \Pr(N_r = P + n|U = u) \) under different choices of \( u \) and \( n \). As a result, when \( P - u \) is larger than a threshold \( \delta_u \) (say, e.g., \( \delta_u = 20 \)), we may assume

\[
\Pr(N_r = P + n|U = u, P - u \geq \delta_u) = \Pr(N_r = \delta_u + n|U = 0) = \tilde{A}_n, \tag{53}
\]

where \( \tilde{A}_n \) is equal to \( A_{\delta_u} \) when \( n = 0 \) and denotes \( A_{\delta_u} \sum_{j' = 1}^{\delta_u} 2^{-j'} A'_{j'\delta_n} \) when \( n > 0 \) for simplicity.
Moreover, because \( \sum_{u=P-\delta_u}^{P} \Pr(U = u) = \sum_{u=P-\delta_u}^{P} (P - \delta_u)P\(1 - p_r\)P - u \) also tends to 0 as \( P \) increases, we may assume that when \( P \) is large enough,

\[
\Pr(N_r = P + n) = \bar{A}_n.
\]

It turns out that when \( P \) is large enough, Eq. (47) can be reduced to

\[
\Pr(D_r^{GF(2)} = d) = \sum_{n=0}^{d} \bar{A}_n \Pr(Y_{r,P+n} = P + d). \tag{54}
\]

Similar to (3), \( \mathbb{E}[D_{\text{max}}^{GF(2)}] = \sum_{d\geq 0} \left(1 - \prod_{1 \leq r \leq R} \Pr(D_r^{GF(2)} \leq d)\right) \), it remains to further analyze \( \Pr(D_r^{GF(2)} \leq d) \). Stemming from (54), we have

\[
\Pr(D_r \leq d) = \sum_{d'=0}^{d} \sum_{n=0}^{d} \bar{A}_n \Pr(Y_{r,P+n} = P + d')
\]

\[
= \sum_{n=0}^{d} \bar{A}_n \sum_{d'=n}^{d} \Pr(Y_{r,P+n} = P + d')
\]

\[
= \sum_{n=0}^{d} \bar{A}_n I_{p_r}(P + n, d - n + 1)
\]

Because \( I_{p_r}(P + n, d - n + 1) \leq I_{p_r}(P, d + 1) \) for every \( 0 \leq n \leq d \), and \( \bar{A}_n \) decays exponentially to 0 as \( n \) increases, there exists a bounded integer \( \delta_n \) subject to

\[
\Pr(D_r \leq d) \geq I_{p_r}(P + \delta_n, d - \delta_n + 1) \tag{55}
\]

for all receiver \( r \) and all \( P \) and \( d \geq \delta_n \). It turns out that

\[
\mathbb{E}[D_{\text{max}}^{GF(2)}] \leq \delta_n + \sum_{d \geq \delta_n} \left(1 - \prod_{1 \leq r \leq R} I_{p_r}(P + \delta_n, d - \delta_n + 1)\right) \tag{56}
\]

Recall that \( \mathbb{E}[D_{\text{max}}^{\text{perf}}] = \sum_{d\geq 0} \left(1 - \prod_{1 \leq r \leq R} I_{p_r}(P, d + 1)\right) \). Because when \( P \) increases, the difference between \( I_{p_r}(P, d + 1) \) and \( I_{p_r}(P + \delta_n, d - \delta_n + 1) \) tends to 0 for all \( d \geq \delta_n \), we can now conclude that \( \mathbb{E}[D_{\text{max}}^{GF(2)}]/P \) converges to \( \mathbb{E}[D_{\text{max}}^{\text{perf}}]/P \) when \( P \) goes to infinity.

\[B. \text{ Proof of Lemma 2}\]

Since \( \gamma_{j,j'} \), \( 1 \leq j' \leq P \), are independently and uniformly chosen from \( GF(q) \), \( \Pr(\text{rank}(F_{j,j}) = J) = 1 - (1/q)^{P-J+1} \). Since \( q \leq 1/p_0 \),

\[
\Pr(\text{rank}(F_{j,j}) = J) \leq 1 - p_0^{P-J+1}. \tag{57}
\]
Based on the above properties and in the same way to prove Theorem 1 in [16], it can be proved that 
\[ \Pr(\text{rank}(F_{J,\Gamma}) = JL) \geq 1 - p_0^{P-J+1}. \]

Since \( L + 1 \) is a prime with primitive root 2, we have the following properties to utilize (See, e.g., [15]):

- there is an element in \( GF(2^L) \), denoted by \( \beta \), with multiplicative order \( L+1 \), i.e., \( \beta^{L+1} = 1 \).
- For a polynomial \( f(x) \) over \( GF(2^L) \), if the evaluation \( f(\beta) \neq 0 \), then \( f(\beta^l) \neq 0 \) for all \( 1 \leq \beta \leq L \).

Based on the above properties and in the same way to prove Theorem 1 in [16], it can be proved that 
\[ \text{rank}(F_{J,\Gamma}) = JL \] if and only if the \( P \times J \) matrix \( [\beta_{jj'}]_{1 \leq j \leq J, 1 \leq j' \leq P} \) over \( GF(2^L) \) has full rank \( J \), where

\[
\beta_{jj'} = \begin{cases} 
\beta^{l_{jj'}}, & \text{if } \Gamma_{jj'} = \text{GC}^{l_{jj'}}_{L+1}H \\
0, & \text{if } \Gamma_{jj'} = 0
\end{cases}
(58)
\]

Consequently, it is equivalent to show that

\[
\Pr(\text{rank}(F_{J,\Gamma}) = J) \geq 1 - p_0^{P-J+1},
(59)
\]

where \( F_{J,\beta} = [\beta_{jj'}]_{1 \leq j \leq J, 1 \leq j' \leq P} \) is a \( P \times J \) matrix defined over \( GF(2^L) \) with \( \beta_{jj'} \in \{0, \beta, \beta^2, \ldots, \beta^{L+1}\} \subseteq GF(2^L) \) subject to

- the \( P \times (J-1) \) submatrix \( [\beta_{jj'}]_{1 \leq j < J, 1 \leq j' \leq P} \) is full rank,
- every \( \beta_{jj'} \) is randomly selected from \( \{0, \beta, \beta^2, \ldots, \beta^{L+1}\} \) according to the distribution

\[
\Pr(\beta_{jj'} = \beta^l) = \begin{cases} 
p_0, & \beta^l = 0 \\
\frac{1-p_0}{L+1}, & \beta^l = \beta^1, 1 \leq l \leq L + 1
\end{cases}
(60)
\]

As \( p_0 \) is a rational number, write \( p_0 = a/b \). Expand the set \( \{0, \beta, \beta^2, \ldots, \beta^{L+1}\} \) into a multiset \( \mathcal{M}_\beta \) of cardinality \( b(L+1) \) as follows:

- the multiplicity of 0 is \( a(L+1) \), i.e., \( \mathcal{M}_\beta \) contains \( a(L+1) \) duplicate 0.

### Table I

| \( P - u \) | \( n \) | 0    | 1    | 5    | 10   | 20   |
|-------------|-----|------|------|------|------|------|
| 1           | 0.5 | 0.25 | 1.5625 \times 10^{-2} | 4.8828 \times 10^{-4} | 4.7684 \times 10^{-7} |
| 5           | 0.298 | 0.2887 | 2.9395 \times 10^{-2} | 9.4518 \times 10^{-4} | 9.2387 \times 10^{-7} |
| 10          | 0.2891 | 0.2888 | 3.0256 \times 10^{-2} | 9.7466 \times 10^{-4} | 9.5274 \times 10^{-7} |
| 15          | 0.2888 | 0.2888 | 3.0283 \times 10^{-2} | 9.7558 \times 10^{-4} | 9.5364 \times 10^{-7} |
| 20          | 0.2888 | 0.2888 | 3.0284 \times 10^{-2} | 9.7561 \times 10^{-4} | 9.5367 \times 10^{-7} |
for $1 \leq l \leq L + 1$, the multiplicity of $\beta^l$ is $b - a$, i.e., $\mathcal{M}_\beta$ contains $b - a$ duplicate $\beta^l$.

In this way,

$$\Pr(\text{rank}(\mathbf{F}_{j,\beta}) = J) = 1 - \frac{A_\beta}{(b(L + 1))^P},$$

where $A_\beta$ represents the number of (possibly duplicate) column vectors in $\{[\beta_{J'j}]_{1 \leq j' \leq P} : \beta_{J'j} \in \mathcal{M}_\beta\}$ that can be written as a $\text{GF}(2^L)$-linear combination of the $J - 1$ column vectors $[\beta_{1j}]_{1 \leq j \leq P}, \ldots, [\beta_{(J-1)j}]_{1 \leq j \leq P}$.

As the $P \times (J-1)$ matrix $[\beta_{J'j}]_{1 \leq j < J, 1 \leq j' \leq P}$ has rank $J - 1$, it contains $J - 1$ linearly independent rows. Without loss of generality, assume rank$([\beta_{J'j}]_{1 \leq j', J} = J - 1$. Thus, for each of the $(b(L + 1))^{J-1}$ column vectors $[\beta_{J'j}]_{1 \leq J' J}$ with $\beta_{J'j} \in \mathcal{M}_\beta$, there are unique $\alpha_1, \alpha_2, \ldots, \alpha_{J-1} \in \text{GF}(2^L)$ subject to $\sum_{1 \leq j < J} \alpha_j [\beta_{j'j}]_{1 \leq J' J} = 0$. Moreover, for $J \leq J' \leq P$, $\sum_{1 \leq j < J} \alpha_j \beta_{j'j}$ may or may not be in $\mathcal{M}_\beta$. If $\sum_{1 \leq j < J} \alpha_j \beta_{j'j} \in \mathcal{M}_\beta$, then it has at most $a(L + 1)$ duplicates in $\mathcal{M}_\beta$, since we assume $p_0 = \frac{a}{b} \geq \frac{1}{L+2}$ so that $a(L + 1) \geq b - a$. Thus, $A_\beta$ is upper bounded by $(b(L + 1))^{J-1}(a(L + 1))^{P-J+1}$ and hence,

$$\Pr(\text{rank}(\mathbf{F}_{j,\beta}) = J) = 1 - \frac{A_\beta}{(b(L + 1))^P} \geq 1 - \frac{a}{b(P-J+1)}.$$  

C. Proof of Theorem 5

It remains to prove $\Pr(D_r^{\text{circ}} \leq d) \geq \Pr(D_r^{\text{GF}(q)} \leq d)$ for all $d \geq 0$. Same as the discussion in Sec.II-B, denote by $U_r$ the number of successfully received uncoded packets at receiver $r$ in phase one, and assume that $U_r = u$ with $u < P$. Since when $u + d < P$, $\Pr(D_r^{\text{circ}} \leq d) = \Pr(D_r^{\text{GF}(q)} \leq d) = 0$, we further assume that $d \geq P - u$. Similar to (5), $D_r^{\text{circ}}$ and $D_r^{\text{GF}(q)}$ can be respectively expressed as

$$D_r^{\text{circ}} = A_1^{\text{circ}} + A_2^{\text{circ}} + \ldots + A_{P-u}^{\text{circ}},$$

$$D_r^{\text{GF}(q)} = A_1^{\text{GF}(q)} + A_2^{\text{GF}(q)} + \ldots + A_{P-u}^{\text{GF}(q)},$$

where $A_j^{\text{circ}}$ and $A_j^{\text{GF}(q)}$ respectively represent the number of coded packets obtained by receiver $r$, under the proposed circular-shift RLNC scheme and under the conventional RLNC scheme over $\text{GF}(q)$, during the process that the number of innovative packets at receiver $r$ increases from $u + j - 1$ to $u + j$. Thus, $A_j^{\text{circ}}$ and $A_j^{\text{GF}(q)}$ follow the geometric distribution with the respective parameter $p_{r,u+j-1} = p_r \Pr(\text{rank}(\mathbf{F}_{u+j,r}) = (u + j)L)$ and $p_{r,u+j-1} = \ldots \ldots$
Lemma 2 with the setting $J = u + j$. Consequently,

$$
\Pr(D_r^\text{circ} = d|U_r = u) = \sum_{a \in A_{P-u,d}} \prod_{j=1}^{P-u} (1 - p_{r,u+j-1}^{\text{circ}})^{a_j-1} p_{r,u+j-1}^{\text{circ}},
$$

$$
\Pr(D_r^\text{GF(q)} = d|U_r = u) = \sum_{a \in A_{P-u,d}} \prod_{j=1}^{P-u} (1 - p_{r,u+j-1}^{\text{GF(q)}})^{a_j-1} p_{r,u+j-1}^{\text{GF(q)}},
$$

where $A_{P-u,d}$ is defined in the same way as in (7), that is, every $(P-u)$-tuple $a = (a_1, \ldots, a_{P-u})$ of positive integers satisfies $a_1 + \ldots + a_{P-u} = d$.

For $0 \leq n < P$ and $d \geq n$, define a function $f_{n,d}$ of an $n$-tuple $\mathcal{X}_n = (x_1, \ldots, x_n)$ of variates according to

$$
f_{n,d}(\mathcal{X}_n) = \sum_{a \in A_{n,d}} \prod_{j=1}^{n} (1 - x_j)^{a_j-1} x_j.
$$

Thus,

$$
\Pr(D_r^\text{circ} \leq d|U_r = u) = \sum_{d' = P-u}^{d} f_{P-u,d'}(\varphi^{\text{circ}}),
$$

$$
\Pr(D_r^\text{GF(q)} \leq d|U_r = u) = \sum_{d' = P-u}^{d} f_{P-u,d'}(\varphi^{\text{GF(q)}}),
$$

where $\varphi^{\text{circ}} = (p_{r,u}^{\text{circ}}, p_{r,u+1}^{\text{circ}}, \ldots, p_{r,P-1}^{\text{circ}})$, and $\varphi^{\text{GF(q)}} = (p_{r,u}^{\text{GF(q)}}, p_{r,u+1}^{\text{GF(q)}}, \ldots, p_{r,P-1}^{\text{GF(q)}})$.

For $d \geq n = 1$, $\sum_{d' = 1}^{d} f_{1,d'}(x) = \sum_{d' = 1}^{d} (1 - x)^{d'-1} x = 1 - (1 - x)^d$. Thus, for $x < 1$,

$$
\left(\sum_{d' = 1}^{d} f_{1,d'}(x)\right)' = d(1 - x)^{d-1} > 0,
$$

where the symbol $'$ means the derivative operation. For $d \geq n \geq 2$ and arbitrary $1 \leq j \leq n$, by conditioning on the possible value $d''$ for $a_j$, one may readily deduce

$$
\sum_{d'' = 1}^{d'} f_{n,d''}(\mathcal{X}_n) = \sum_{d' = 1}^{d-1} \sum_{d'' = 1}^{d'-1} f_{n-1,d'-d''}(\mathcal{X}_n \backslash x_j) f_{1,d''}(x_j)
$$

$$
= \sum_{d' = 1}^{d-1} f_{n-1,d'-1}(\mathcal{X}_n \backslash x_j) \sum_{d'' = 1}^{d-1} f_{1,d''}(x_j),
$$
where the last equation can be obtained by changing the way to enumerate all \( \frac{(d+2-n)(d+1-n)}{2} \) possible choices. Thus, for \( 0 < x_1, \ldots, x_n < 1 \),

\[
\frac{\partial}{\partial x_j} \left( \sum_{d'=n}^d f_{n,d'}(X_n) \right) = \sum_{d'=n}^d f_{n-1,d'-1}(X_n \setminus x_j) \frac{\partial}{\partial x_j} \left( \sum_{d'=1}^{d+1-d'} f_{1,d'}(x_j) \right) > 0, \quad (69)
\]

where the last inequality stems from (67) and the fact that \( f_{n,d}(X_n) > 0 \) for all \( d \geq n \geq 1 \) and \( 0 < x_1, \ldots, x_n < 1 \). It turns out that for \( X_n = (x_1, \ldots, x_n) \) and \( X'_n = (x'_1, \ldots, x'_n) \) with \( 0 < x_j \leq x'_j < 1 \) for all \( 1 \leq j \leq n \),

\[
\sum_{d'=n}^d f_{n,d'}(X_n) \leq \sum_{d'=n}^d f_{n,d'}(X'_n).
\]

Since \( P_{r,u+j-1}^{\text{circ}} \geq P_{r,u+j-1}^{\text{GF}(q)} \) for all \( 1 \leq j \leq P - u \),

\[
\Pr(D_r^{\text{circ}} \leq d | U_r = u) = \sum_{d'=P-u}^d f_{P-u,d'}(\mathcal{S}^{\text{circ}}) \geq \sum_{d'=P-u}^d f_{P-u,d'}(\mathcal{S}^{\text{GF}(q)}) = \Pr(D_r^{\text{GF}(q)} \leq d | U_r = u), \quad (70)
\]

and hence

\[
\Pr(D_r^{\text{circ}} \leq d) = \sum_{u=\max\{0,P-d\}}^{P-1} \Pr(D_r^{\text{circ}} \leq d | U_r = u) \Pr(U_r = u) \geq \sum_{u=\max\{0,P-d\}}^{P-1} \Pr(D_r^{\text{GF}(q)} \leq d | U_r = u) \Pr(U_r = u) = \Pr(D_r^{\text{GF}(q)} \leq d). \quad (71)
\]

**REFERENCES**

[1] M. Yu and P. Sadeghi, “Approximating throughput and packet decoding delay in linear network coded wireless broadcast,” *IEEE ITW*, Guangzhou, China, 2018.

[2] I. Chatzigeorgious and A. Tassi, “Decoding delay performance of random linear network coding for broadcast,” *IEEE Trans. Vehicular Technology*, vol. 66, no. 8, 2017.

[3] B. T. Swapna, A. Eryilmaz, and N. B. Shroff, “Throughput-delay analysis of random linear network coding for wireless broadcasting,” *IEEE Trans. Inf. Theory*, vol. 59, no. 10, 2013.

[4] E. Skevakis and I. Lambadaris, “Decoding and file transfer delay balancing in network coding broadcast,” *IEEE ICC*, Kuala Lumpur, Malaysia, 2016.

[5] N. Xie and S. Weber, “Network coding broadcast delay on erasure channels,” *ITA Workshop*, San Diego, CA, 2013.

[6] E. Skevakis and I. Lambadaris, “Optimal control for network coding broadcast,” *IEEE GLOBECOM*, Washington, DC, 2016.

[7] E. Skevakis and I. Lambadaris, “Delay optimal scheduling for network coding broadcast,” *IEEE ICC*, Paris, France, 2017.

[8] P. Sadeghi, R. Shams and Danail Traskov, “An optimal adaptive network coding scheme for minimizing decoding delay in broadcast erasure channels,” *EURASIP J. Wireless Commun. and Netw.*, 2010.

[9] N. Aboutorab, P. Sadeghi and S. Sorour, “Enabling a tradeoff between completion time and decoding delay in instantly decodable network coded systems,” *IEEE Trans. Commun.*, vol. 62, no. 4, 2014.
[10] M. Yu, N. Aboutorab and P. Sadeghi, “From instantly decodable to random linear network coded broadcast,” *IEEE Trans. Commun.*, vol. 62, no. 11, 2014.

[11] S. Sorour and S. Valaee, “Completion delay minimization for instantly decodable network codes,” *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, 2015.

[12] 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. Inf. Theory*, vol. 52, no. 10, 2006.

[13] S. Sorour and S. Valaee, “On minimizing broadcast completion delay for instantly decodable network coding,” *IEEE ICC*, Cape Town, South Africa, 2010.

[14] H. Hou, K. W. Shum, M. Chen and H. Li, “BASIC codes: low-complexity regenerating codes for distributed storage systems,” *IEEE Trans. Inf. Theory*, vol. 62, no. 6, Jun. 2016.

[15] H. Tang, Q. T. Sun, Z. Li, X. Yang and K. Long, “Circular-shift linear network coding,” *IEEE Trans. Inf. Theory*, vol. 65, no. 1, 2019.

[16] Q. T. Sun, H. Tang, Z. Li, X. Yang and K. Long, “Circular-shift linear network codes with arbitrary odd block lengths,” *IEEE Trans. Commun.*, vol. 67, no. 4, 2019.

[17] Q. T. Sun, X. Yang, K. Long, X. Yin, and Z. Li, “On vector linear solvability of multicast networks,” *IEEE Trans. Commun.*, vol. 64, no. 12, 2016.

[18] H. Tang, Q. T. Sun, et. al., “On Encoding and Decoding of Circular-shift Linear Network Codes,” *IEEE Commun. Letters*, vol. 23, no. 5, 2019.