Multiple Access Network Information-flow And Correction codes*

Hongyi Yao[1], Theodoros K. Dikaliotis[2], Sidharth Jaggi[3], Tracey Ho[2]
[1]Tsinghua University [2]California Institute of Technology [3]Chinese University of Hong Kong
[1]yaohongyi03@gmail.com [2]{tdikal, tho}@caltech.edu [3]jaggi@ie.cuhk.edu.hk

Abstract—The network communication scenario where one or more receivers request all the information transmitted by different sources is considered. We introduce distributed polynomial-time network codes in the presence of *malicious nodes*. Our codes can achieve any point inside the rate region of multiple-source multicast transmission scenarios both in the cases of coherent and non-coherent network coding. For both cases the encoding and decoding algorithm runs in $poly(|\mathcal{E}|)exp(s)$ time, where $poly(|\mathcal{E}|)$ is a polynomial function of the number of edges $|\mathcal{E}|$ in the network and $exp(s)$ is an exponential function of the number of sources s. Our codes are fully distributed and different sources require no knowledge of the data transmitted by their peers. Our codes are "end-to-end", that is, all nodes apart from the sources and the receivers are oblivious to the adversaries present in the network and simply implement random linear network coding.

Index Terms—polynomial-time codes, error-correction, double extended field, Gabidulin codes

I. INTRODUCTION

Information dissemination can be optimized with the use of network coding since it maximizes the network throughput in multicast transmission scenarios [1]. At the same time network coding is highly vulnerable to malicious attacks from rogue users. The presence of even a small number of adversarial nodes can contaminate the majority of packets in a network, preventing receivers from decoding.

The work of Cai-Yeung [2] first studied the network error-correction problem in the single source scenario, and their scheme requires high (exponential in the network size) design complexity. Further works by [3] and [4] provided network error-correcting codes with design and implementation complexity that is low (*i.e.*, polynomial in size of the network parameters). The design of such robust network codes with "active nodes" (*i.e.* internal nodes using cryptographic schemes to detect packets modified by computationally bounded adversaries) has also been considered in the cryptographic setting (see for instance [5], [6]).

We consider the design of multisource network error-correcting codes that are resilient against worst-case network errors, *i.e.*, against errors injected by computationally unbounded adversaries. Naïve implementations of single source network error-correcting codes fail since such codes require the source to judiciously insert redundancy into the transmitted codeword; however, in the distributed source case this cannot be done. The work in [7] gave the capacity region for the multisource network error correction problem, but the achievability proof used codes with high decoding complexity.

The current paper gives the first construction of efficient decodable error-correction codes. For both coherent (when the network transform is known *a priori* to the receiver(s)) and non-coherent (when no such information is known *a priori* to the receiver(s)) cases our codes achieve the optimal rate-region demonstrated in [7] and have implementation complexity that is polynomial in the size of the network. Furthermore our codes are fully distributed in the sense that different sources require no knowledge of the data transmitted by their peers and end-to-end, *i.e.*, all nodes are oblivious to the adversaries present in the network and simply implement random linear network coding [8]. A remaining bottleneck is that the computational complexity of our codes increases exponentially with the number of sources. Thus the design of efficient schemes for a large number of sources is still open.

The remainder of this paper is organized as follows: In Section II we formulate the problem and introduce the mathematical preliminaries. In Section III we provide a code construction for the coherent case, *i.e.*, the receiver(s) knows the linear transform from each source induced by random linear network code. In Section IV we construct codes for the non-coherent case, where the receiver(s) has no information on the network transforms.

II. PRELIMINARIES

A. Model

We consider a delay-free network $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is the set of nodes and $\mathcal{E}$ is the set of edges. The capacity of each edge is normalized to be one symbol of $\mathbb{F}_p$ per unit time. Edges with non-unit capacity are modeled as parallel edges.

For notational convenience we restrict ourselves to the analysis of the situation where there are only two sources $\mathcal{S}_1, \mathcal{S}_2 \in \mathcal{V}$ transmitting information to one receiver $\mathcal{R} \in \mathcal{V}$, since the extension of our results to more sources and receivers is straightforward. The minimum cut capacity from source $\mathcal{S}_i$ to $\mathcal{R}$ is denoted by C_i for $i \in [1, 2]$, and the minimum cut capacity from both sources to the receiver is equal to C.

Within the network there is a hidden adversary trying to interfere with the transmission of information by observing all the transmissions in the network and injecting its own packets in any z links[1], that may be chosen as a function

---

[1]Note that since each transmitted symbol in the network is from a finite field, modifying symbol x to symbol y is equivalent to injecting/adding symbol $y - x$ into x.

of his complete knowledge of the network, the message, and the communication scheme.

The sources on the other hand know nothing about each other's transmitted information and the links compromised by the adversary. Their goal is to add redundancy into their transmitted packets so that they can achieve any rate-tuple (R_1, R_2) such that $R_1 \leq C_1 - 2z$, $R_2 \leq C_2 - 2z$, and $R_1 + R_2 \leq C - 2z$ (this is the rate region of the multi-source multicast problem proved in [7]). An example network and its rate region is shown in Figure 1.

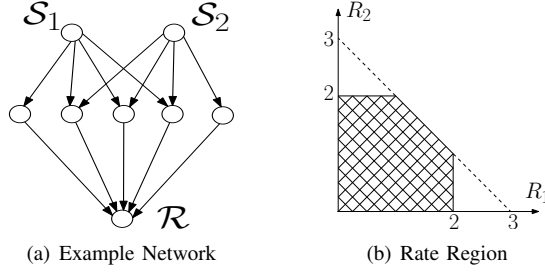(a) Example Network   (b) Rate Region

Fig. 1. An example network with two sources. The Network in Figure 1(a) has $C_1 = C_2 = 4$, $C = 5$ and the adversary can inject $z = 1$ error packet. The achievable rate region is shown in the dark region of Figure 1(b).

To simplify the discussion we show the code construction for rate-tuple (R_1, R_2) satisfying $R_1 \leq C_1 - 2z$, $R_2 \leq C_2 - 2z$, $R_1 + R_2 + 2z = C$ and exactly C edges reach the receiver $\mathcal{R}$ (if more do, redundant information can be discarded).

B. Random linear network coding

In this paper, we consider the following well-known distributed random linear coding scheme [8].

Sources: The source $\mathcal{S}_i$ arranges the data into a $C_i \times \ell$ *message matrix* M_i over $\mathbb{F}_p$ (here the *packet-length* ℓ is a network design parameter). For $i \in [1, 2]$ source $\mathcal{S}_i$ then takes independent and uniformly random linear combinations over $\mathbb{F}_p$ of the rows of M_i to generate respectively the packets transmitted on each outgoing edge.

Network nodes: Each internal node similarly takes uniformly random linear combinations of the packets on incoming edges to generate packets transmitted on outgoing edges.

Receiver: The receiver $\mathcal{R}$ constructs the $C \times \ell$ matrix Y over $\mathbb{F}_p$ by treating the received packets as consecutive length-ℓ row vectors of Y (recall that exactly C edges reach $\mathcal{R}$). In the case that no error happen in the network, the network's internal linear operations induce linear transforms between M_i and Y as

$$Y = T_1 M_1 + T_2 M_2, \tag{1}$$

where T_i is the overall transform matrix from $\mathcal{S}_i$ to $\mathcal{R}$.

C. Finite field extension

In the analysis below denote by $\mathbb{F}_p^{m \times n}$ the set of all $m \times n$ matrices with elements from $\mathbb{F}_p$. The identity matrix with dimension $m \times m$ is denoted by I_m, and the zero matrix of any dimensions is denoted by O. The dimension of the zero

matrix will be clear from the context stated. For the clarity of notation vectors are in bold-face (*e.g.* $\mathbf{A}$).

Before we continue to the analysis of the encoding and decoding process it is useful to introduce some concepts from the theory of finite field. Every finite field $\mathbb{F}_p$, where p is a prime or a power of a prime, can be algebraically extended[2] [9] to a larger finite field $\mathbb{F}_q$, where $q = p^n$ for any positive integer n. Note that $\mathbb{F}_q$ includes $\mathbb{F}_p$ as a subfield thus any matrix $A \in \mathbb{F}_p^{m \times \ell}$ is also a matrix in $\mathbb{F}_q^{m \times \ell}$. Hence throughout the paper matrix multiplication over different fields (one over the base field and the other from the extended field) is allowed and computed over the extended field.

There is a bijective mapping between $\mathbb{F}_p^{m \times n}$ and $\mathbb{F}_q^m$ defined as follows:

- For each $A \in \mathbb{F}_p^{m \times n}$, the folded version of A is a vector $\mathbf{A}^f$ in $\mathbb{F}_q^m$ given by $A\mathbf{a}^{\mathrm{T}}$ where $\mathbf{a} = \{a_1, \ldots, a_n\}$ is a basis of the extension field $\mathbb{F}_q$ with respect to $\mathbb{F}_p$. Here we treat the ith row of A as a single element in $\mathbb{F}_q$ to obtain the ith element of A^f. For instance let $A = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ be a matrix in $\mathbb{F}_2^{2 \times 2}$. Then the operation of folding it into $\mathbb{F}_4^2$ gives $\mathbf{A}^f = \begin{bmatrix} (1,0) \\ (1,1) \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \end{bmatrix} \in \mathbb{F}_4^2$ (where $2 \equiv x$ and $3 \equiv x + 1 \mod (x^2 + x + 1)$ [9]).

- For each $\mathbf{B} \in \mathbb{F}_q^m$, the unfolded version of $\mathbf{B}$ is a matrix B^u in $\mathbb{F}_p^{m \times n}$. Here we treat the ith element of $\mathbf{B}$ as a row in $\mathbb{F}_p^{1 \times n}$ to obtain the ith row of B^u. For instance let $\mathbf{B} = \begin{bmatrix} 2 \\ 3 \end{bmatrix}$ be a vector in $\mathbb{F}_4^2$. Then the operation of unfolding it into $\mathbb{F}_2^{2 \times 2}$ gives $B^u = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

We can also extend these operations to include more general scenarios. Specifically any matrix $A \in \mathbb{F}_p^{m \times \ell n}$ can be written as a concatenation of matrices $A = [A_1 \ldots A_\ell]$, where $A_i \in F_p^{m \times n}$. The folding operation is defined as follows: $A^f = [\mathbf{A}_1^f \ldots \mathbf{A}_\ell^f]$. Similarly the unfolding operation u can be applied to a number of submatrices of a large matrix, e.g., $[\mathbf{A}_1^f \ldots \mathbf{A}_\ell^f]^u = [(\mathbf{A}_1^f)^u \ldots (\mathbf{A}_\ell^f)^u] = [A_1 \ldots A_\ell]$.

In the paper *double algebraic extensions* are considered. More precisely let $\mathbb{F}_Q$ be an algebraic extension from $\mathbb{F}_q$, where $Q = q^N = p^{nN}$ for any positive integer N. Table I summarize the notation of the fields considered.

TABLE I
SUMMARY OF FILED NOTATIONS

Field	$\mathbb{F}_p$	$\mathbb{F}_q$	$\mathbb{F}_Q$
Size	p	$q = p^n$	$Q = q^N$

Note: Of the three fields $\mathbb{F}_p$, $\mathbb{F}_q$ and $\mathbb{F}_Q$ defined above, two or sometimes all three appear simultaneously in the same equation. To avoid confusion, unless otherwise specified, the superscript f for folding is from $\mathbb{F}_p$ to $\mathbb{F}_q$, and the superscript u for unfolding is from $\mathbb{F}_q$ (or $\mathbb{F}_Q$) to $\mathbb{F}_p$.

[2]Let $\mathbb{F}_p[x]$ be the set of all polynomials over $\mathbb{F}_p$ and $f(x) \in \mathbb{F}_p[x]$ be an irreducible polynomial of degree n. Then $\mathbb{F}_p[x]/f(x)$ defines an algebraic extension field $\mathbb{F}_{p^n}$ by a homomorphism mapping [9].

D. Row-space distance

For any two matrices $B_1 \in \mathbb{F}_p^{m_1 \times n}$ and $B_2 \in \mathbb{F}_p^{m_2 \times n}$ let $\mathcal{B}_1$ be the subspace spanned by the rows of B_1 and $\mathcal{B}_2$ be the subspace spanned by the rows of B_2. The *row-space distance* of B_1 and B_2 is defined as $d_S(B_1, B_2) = dim(span(\mathcal{B}_1 \cup \mathcal{B}_2)) - dim(span(\mathcal{B}_1 \cap \mathcal{B}_2))$. Row-space distance is a metric and satisfies the triangle inequality [10].

If $m_1 = m_2 = m$, the following proposition is direct consequence of Corollary 3 in [4]:

Proposition 1. $d_S(B_1, B_2) \leq 2 \, rank(B_1 - B_2)$.

E. Gabidulin codes

Gabidulin in [11] introduced a class of error correcting codes over $\mathbb{F}_p^{m \times n}$. Let $\mathbf{X} \in \mathbb{F}_q^R$ be the information vector, $G \in \mathbb{F}_q^{m \times R}$ be the generator matrix, $(G\mathbf{X})^u \in \mathbb{F}_p^{m \times n}$ be the transmitted matrix, $Z \in \mathbb{F}_p^{m \times n}$ be the error matrix, and $(G\mathbf{X})^u + Z \in \mathbb{F}_p^{m \times n}$ be the received matrix. Then decoding is possible if and only if $rank(Z) \leq \lfloor \frac{d}{2} \rfloor$, where $d = m - R + 1$ is the minimum distance of the code.

The work of [4] utilizes the results of [11] to obtain network error-correcting codes with the following properties:

Theorem 1 (Theorem 11 in [4]). *Let Z can be expressed as $Z = \sum_{i \in [1,\tau]} \mathbf{L}_i \mathbf{E}_i$, such that:*

- *For each $i \in [1, \tau]$, $\mathbf{L}_i \in \mathbb{F}_p^{m \times 1}$ and $\mathbf{E}_i \in \mathbb{F}_p^{1 \times n}$;*
- *For each $i \in [1, \mu]$, $\mathbf{L}_i$ is known a priori by the receiver;*
- *For each $i \in [\mu + 1, \mu + \delta]$, $\mathbf{E}_i$ is known a priori by the receiver;*
- *$2\tau - \mu - \delta \leq d - 1$,*

using Gabidulin codes the receiver can decode $\mathbf{X}$ with at most $\mathcal{O}(mn)$ operations over $\mathbb{F}_q$.

Thus when $\mu = \delta = 0$, Theorem 1 reduces to the basic case where the receiver has no *priori* knowledge about Z.

III. COHERENT NETWORK ERROR-CORRECTING CODES

Coherent here means the receiver $\mathcal{R}$ knows the linear transforms from both $\mathcal{S}_1$ and $\mathcal{S}_2$, *i.e.*, $\mathcal{R}$ knows T_1 and T_2 defined in equation (1). For instance, it is possible T_1 and T_2 to be inferred by network communications before the adversary enters the network and corrupts information. Alternatively, if centralized designed network coding is used [12], T_1 and T_2 is assumed to be known by the receiver.

While the non-coherent codes we propose are more general than the coherent codes, the description of the latter is simpler, and hence we first describe them. Under the coherent assumption the goal of the section is to construct a code attaining any rate-tuple (R_1, R_2) in the rate region for our communication scenario (see section II-A for details).

A. Encoding

Each source $\mathcal{S}_i$, $i \in [1, 2]$, has information to deliver to destination $\mathcal{R}$ and organizes this information into batches of R_i packets. Each packet is a concatenation of $\ell = knN$ symbols from the finite field $\mathbb{F}_p$, where $n = R_1 + 2z$ and

$N = R_2 + 2z$ and k is a code design parameter. For simplicity we will analyze the transmission of a single batch of packets.

The way sources encode their information packets is through the use of Gabidulin codes (see Section II-E for details). More precisely the information of $\mathcal{S}_1$ is a matrix $X_1 \in \mathbb{F}_q^{R_1 \times kN}$, where $\mathbb{F}_q$ is an algebraic extension of $\mathbb{F}_p$ and $q = p^n$ (see Section II-C for details). Before transmission X_1 is multiplied with a generator matrix, $G_1 \in \mathbb{F}_q^{n \times R_1}$, creating $G_1 X_1 \in \mathbb{F}_q^{n \times (kN)}$ whose unfolded version $M_1 = (G_1 X_1)^u$ is a matrix in $\mathbb{F}_p^{n \times \ell}$ that is transmitted through the network using the random linear network coding defined in Section II-B.

The information of $\mathcal{S}_2$ is a matrix $X_2 \in \mathbb{F}_Q^{R_2 \times k}$, where $\mathbb{F}_Q$ is an algebraic extension of $\mathbb{F}_q$ and $Q = q^N = p^{nN}$. Before transmission X_2 is multiplied with a generator matrix, $G_2 \in \mathbb{F}_Q^{N \times R_2}$, creating $G_2 X_2 \in \mathbb{F}_Q^{N \times k}$ whose unfolded version $M_2 = (G_2 X_2)^u$ over $\mathbb{F}_p$ is a matrix in $\mathbb{F}_p^{N \times \ell}$ that is transmitted through the network using the random linear network coding defined in Section II-B.

Both G_1 and G_2 are chosen as generator matrices for Gabidulin codes and have the capability of correcting errors of rank at most z over $\mathbb{F}_p$ and $\mathbb{F}_q$ respectively.

B. Decoding

The packets reaching receiver $\mathcal{R}$ can be expressed as

$$Y = T_1 M_1 + T_2 M_2 + E, \quad (2)$$

where $Y \in \mathbb{F}_p^{C \times \ell}$ is the matrix formed by the packets received by $\mathcal{R}$, $T_1 \in \mathbb{F}_p^{C \times n}$, $T_2 \in \mathbb{F}_p^{C \times N}$ are the linear transform matrices from $\mathcal{S}_1$ and $\mathcal{S}_2$ to the receiver $\mathcal{R}$, and $E \in \mathbb{F}_p^{C \times \ell}$ is the error matrix induced at the receiver. Note that $rank(E) \leq z$ since the adversary can inject only z error packets [3].

Folding equation (2) into $\mathbb{F}_q$ results in:

$$Y^f = [T_1 G_1 \quad T_2] \begin{bmatrix} X_1 \\ M_2^f \end{bmatrix} + E^f, \quad (3)$$

where E^f has rank at most equal to z according to Lemma 1.

Lemma 1. *Folding a matrix does not increase its rank.*

Proof: Let matrix $H \in \mathbb{F}_p^{m \times kn}$ has $rank(H) = r$. Thus $H = WZ$, where $Z \in \mathbb{F}_p^{r \times kn}$ is of full row rank and $W \in \mathbb{F}_p^{m \times r}$ is of full column rank. After the folding operation H becomes $H^f = WZ^f$ and therefore $rank(H^f) \leq r$. $\quad \square$

Let $D = [\, T_1 G_1 \quad T_2 \,]$. Since $R_1 + N = R_1 + R_2 + 2z = C$ (see Section II-A for details), D is a $C \times C$ square matrix.

Lemma 2. *Matrix $D \in \mathbb{F}_q^{C \times C}$ is invertible with probability at least $1 - |\mathcal{E}|/p$.*

Proof: Let $\mathcal{X}$ be the set of random variables over $\mathbb{F}_p$ comprised of the local coding coefficients used in the random linear network code. Thus the determinant of D is a polynomial $\mathbf{f}(\mathcal{X})$ over $\mathbb{F}_q$ of degree at most $|\mathcal{E}|$ (see Theorem 1 in [8] for details). Since the variables $\mathcal{X}$ in $\mathbf{f}(\mathcal{X})$ are evaluated over $\mathbb{F}_p$, $\mathbf{f}(\mathcal{X})$ is equivalent to a vector of polynomials $(f_1(\mathcal{X}), f_2(\mathcal{X}), \ldots, f_n(\mathcal{X}))$, where $f_i(\mathcal{X}) \in \mathbb{F}_p[\mathcal{X}]$ is a polynomial over $\mathbb{F}_p$ with variables in $\mathcal{X}$. Note that $f_i(\mathcal{X})$ also

has degree no more than $|\mathcal{E}|$ for each $i \in [1, n]$. Thus once we prove that there exists an evaluation of $\mathcal{X}$ such that $\mathbf{f}$ is a nonzero vector over $\mathbb{F}_p$, we can show D is invertible with probability at least $1 - |\mathcal{E}|/p$ by Schwartz-Zippel lemma [13].

Since $R_1 + N = C$ (see Section II-A for details) and $R_1 \leq C_1$ and $N \leq C_2$, there exist $R_1 + N$ edge-disjoint-paths: $\mathcal{P}_1^1, \mathcal{P}_2^1, \ldots, \mathcal{P}_{R_1}^1$ from s_1 to r and $\mathcal{P}_1^2, \mathcal{P}_2^2, \ldots, \mathcal{P}_N^2$ from s_2 to r. The variables in $\mathcal{X}$ are evaluated in the following manner:

1). Let O be the zero matrix in $F_q^{n \times N}$. We choose the variables in $\mathcal{X}$ so that the R_1 independent rows of $[G_1, O] \in \mathbb{F}_q^{n \times C}$ correspond to routing information from s_1 to R via $\mathcal{P}_1^1, \ldots, \mathcal{P}_{R_1}^1$.

2). Let $\{\mathbf{u}_{R_1+1}, \mathbf{u}_{R_1+2}, \ldots, \mathbf{u}_C\}$ be N distinct rows of the identity matrix in $\mathbb{F}_q^{C \times C}$ such that for each $i \in [1, N]$, $\mathbf{u}_{R_1+i}$ has the element 1 located at position $R_1 + i$. Then these N vectors correspond to routing information from s_2 to r via $\mathcal{P}_1^2, \mathcal{P}_2^2, \ldots, \mathcal{P}_N^2$.

Under such evaluations of the variables in $\mathcal{X}$, matrix D equals $\begin{bmatrix} G_1' & O \\ O & I_N \end{bmatrix}$, where $G_1' \in \mathbb{F}_q^{R_1 \times R_1}$ consists of the R_1 independent rows of G_1. Hence $\mathbf{f}$ is non-zero. Using the Schwartz-Zippel Lemma $\mathbf{f} \neq 0$ and thus D is invertible with probability at least $1 - |\mathcal{E}|/p$ over the choices of $\mathcal{X}$. $\square$

Hence, by multiplying Equation (3) by D^{-1} the receiver gets $D^{-1}Y^f = \begin{bmatrix} X_1 \\ M_2^f \end{bmatrix} + D^{-1}E^f$. The last $N = R_2 + 2z$ rows of $D^{-1}Y^f$ are $(D^{-1}Y^f)_d = M_2^f + (D^{-1}E^f)_d$, where the subscript d stands for the last N rows of each matrix.

Note: To show why $\mathcal{S}_2$ uses a generator matrix G_2 over a double-extended field $\mathbb{F}_Q = \mathbb{F}_{q^N} = \mathbb{F}_{p^{nN}}$, consider what happens if instead it uses $\mathbb{F}_Q = \mathbb{F}_q$. In this case the matrix $M_2^f + (D^{-1}E^f)_d$ is indeed of the form required for successful decoding of Gabidulin codes as long as $(D^{-1}E^f)_d^u$ has rank less than z over $\mathbb{F}_p$. But this is not generally the case since D^{-1} belongs to $\mathbb{F}_q$ but not $\mathbb{F}_p$. Therefore although E^f and consequently $D^{-1}E^f$ have rank less than z over $\mathbb{F}_q$, the rank of $(D^{-1}E^f)_d^u$ might increase over $\mathbb{F}_p$.

If source $\mathcal{S}_2$ uses a generator matrix G_2 defined over $\mathbb{F}_Q = \mathbb{F}_{q^N}$ that is able to correct rank z errors over $\mathbb{F}_q$, we can prove the main result in this section as follows.

Theorem 2. *A coherent receiver $\mathcal{R}$ can efficiently decode both X_1 and X_2 correctly with probability at least $1 - 2|\mathcal{E}|/p$.*

Proof: First, according to Lemma 2 matrix D is invertible with probability at least $1 - |\mathcal{E}|/p$. Since G_2 is able to correct rank z errors over $\mathbb{F}_q$, using $(D^{-1}Y^f)_d = M_2^f + (D^{-1}E^f)_d$, $\mathcal{R}$ can execute the Gabidulin decoding algorithm and get X_2.

Second, once X_2 is known T_2M_2 is subtracted from Y to result in $T_1M_1 + E$. Since T_1 is left invertible with probability at least $1 - |\mathcal{E}|/p$ (by [14]), $\mathcal{R}$ can multiply $T_1M_1 + E$ with the left inverse of T_1 giving $M_1 + T_1^{-1}E$. Since $\text{rank}(T_1^{-1}E) \leq z$ over base field $\mathbb{F}_p$, the execution of the Gabidulin decoding algorithm results in X_1. In the end the overall probability of correct decoding is at least $1 - 2|\mathcal{E}|/p$. $\square$

C. Complexity discussion

Since the computational complexity of the coherent network error-correcting codes here is that same as those of the non-coherent codes shown later, we delay the discussion until Section IV-C.

IV. NON-COHERENT ERROR CORRECTION

In the non-coherent case it is assumed that receiver $\mathcal{R}$ does not know the network transform matrices T_1 and T_2 of the two sources prior to communication in the presence of the adversary. Assuming a non-coherent receiver the goal of this section is to construct codes attaining any rate-tuple (R_1, R_2) in the rate region for our communication scenario (see section II-A for details).

A. Encoding

In the scenario where the receiver $\mathcal{R}$ does not know T_1 and T_2 *a priori* the two sources append headers on their transmitted packets to convey information about T_1 and T_2 to the receiver. Thus source $\mathcal{S}_1$ constructs message matrix $[I_n \quad O \quad M_1]$ with the zero matrix O having dimensions $n \times N$, and source $\mathcal{S}_2$ constructs a message matrix $[O \quad I_N \quad M_2]$ with the zero matrix O having dimension $N \times n$. The identity and zero matrices have elements from $\mathbb{F}_p$ and the M_1, M_2 matrices in $\mathbb{F}_p^{C \times \ell}$ have the same definitions as in Section III-A.

B. Decoding

The two message matrices are transmitted to the receiver $\mathcal{R}$ through the network with the use of random linear network code and therefore the receiver gets:

$$Y = [Y_1 \quad Y_2 \quad Y_3] = [T_1 \quad T_2 \quad A] + E, \quad (4)$$

where $A = T_1M_1 + T_2M_2 \in \mathbb{F}_p^{C \times \ell}$ and $E \in \mathbb{F}_p^{C \times (n+N+m)}$ has rank no more than z over field $\mathbb{F}_p$. Let $E = [E_1 \quad E_2 \quad E_3]$, where $E_1 \in \mathbb{F}_p^{C \times n}$ and $E_2 \in \mathbb{F}_p^{C \times N}$ and $E_3 \in \mathbb{F}_p^{C \times \ell}$. As in the decoding scheme in Section III the receiver $\mathcal{R}$ first decodes X_2 and then X_1.

Stage 1: Decoding X_2:
Let $Y_a = [Y_1G_1 \quad Y_2 \quad Y_3^f]$ be a matrix in $\mathbb{F}_q^{C \times (R_1+N+kN)}$. To be precise:

$$Y_a = [T_1G_1 \quad T_2 \quad A^f] + [E_1G_1 \quad E_2 \quad E_3^f]. \quad (5)$$

Receiver $\mathcal{R}$ uses invertible row operations over $\mathbb{F}_q$ to transform Y_a into a row-reduced echelon matrix $[T_{RRE} \quad M_{RRE}]$ that has the same row space as Y_a, where T_{RRE} has $C = R_1 + N$ columns and M_{RRE} has kN columns. Then the following propositions are from the results[3] proved in [4]:

Proposition 2. 1) *The matrix $[T_{RRE} \quad M_{RRE}]$ takes the form $[T_{RRE} \quad M_{RRE}] = \begin{bmatrix} I_C + \hat{L}U_\mu^T & r \\ O & \hat{E} \end{bmatrix}$, where $U_\mu \in \mathbb{F}_q^{C \times \mu}$ comprises of μ distinct columns of the $C \times C$ identity matrix such that $U_\mu^T r = 0$ and $U_\mu^T \hat{L} = -I_\mu$. In*

---

[3] 1) is from Proposition 7, 2) from Theorem 9, and 3) from Proposition 10 in [4].

particular, $\hat{L}$ in $\mathbb{F}_q^{C \times \mu}$ is the "error-location matrix", r in $\mathbb{F}_q^{C \times kN}$ is the "message matrix", and $\hat{E}$ in $\mathbb{F}_q^{\delta \times kN}$ is the "known error value" (and its rank is denoted δ).

2) *Let $X = \begin{bmatrix} X_1 \\ M_2^f \end{bmatrix}$ and $e = r - X$ and $\tau = \mathrm{rank} \begin{bmatrix} \hat{L} & e \\ 0 & \hat{E} \end{bmatrix}$. Then $2\tau - \mu - \delta$ is no more than $d_S([T_{RRE} \quad M_{RRE}], [I_C \quad X])$, i.e., the row-space distance between $[T_{RRE} \quad M_{RRE}]$ and $[I_C \quad X]$.*

3) *There exist τ column vectors $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_\tau \in \mathbb{F}_q^C$ and τ row vectors $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_\tau \in \mathbb{F}_q^{1 \times kN}$ such that $e = \sum_{i \in [1,\tau]} \mathbf{L}_i \mathbf{E}_i$. In particular, $\mathbf{L}_1, \mathbf{L}_2, \ldots, \mathbf{L}_\mu$ are the columns of $\hat{L}$, and $\mathbf{E}_{\mu+1}, \mathbf{E}_{\mu+2}, \ldots, \mathbf{E}_{\mu+\delta}$ are the rows of $\hat{E}$.*

Recall that the subscripte d stands for the last N rows of any matrix/vector. Then we show the following for our scheme.

Lemma 3. *1) Matrix $e_d = r_d - M_2^f$ can be expressed as $e_d = \sum_{i \in 1,2,\ldots,\tau} (\mathbf{L}_i)_d \mathbf{E}_i$, where $(\mathbf{L}_1)_d, (\mathbf{L}_2)_d, \ldots, (\mathbf{L}_\mu)_d$ are the columns of $\hat{L}_d$ and $\mathbf{E}_{\mu+1}, \mathbf{E}_{\mu+2}, \ldots, \mathbf{E}_{\mu+\delta}$ are the rows of $\hat{E}$.*

2) *With probability at least $1 - |\mathcal{E}|/p$,*

$$2\tau - \mu - \delta \leq 2z$$

Proof: 1) It is a direct corollary from Proposition 2.3.

2) Using Proposition 2.2 it suffices to prove with probability at least $1 - |\mathcal{E}|/p$, $d_S([T_{RRE} \quad M_{RRE}], [I_C \quad X]) \leq 2z$.

As shown in the proof of Lemma 1, the columns of E_3^f are in the column space of E_3 (and then of E) over $\mathbb{F}_q$. Thus $[E_1 \quad E_2 \quad E_3^f]$ and therefore $[E_1 G_1 \quad E_2 \quad E_3^f]$ has rank at most equal to z over $\mathbb{F}_q$. Using Proposition 1 and Equation (5), $d_S(Y_a, [T_1 G_1 \quad T_2 \quad A^f])$ is no more than $2z$.

Since $d_S([T_{RRE} \quad M_{RRE}], Y_a) = 0$, we have $d_S([T_{RRE} \quad M_{RRE}], [T_1 G_1 \quad T_2 \quad A^f]) \leq 2z$.

Using Lemma 2, matrix D is invertible with probability at least $1 - |\mathcal{E}|/p$, so $[I_C \quad X]$ has zero row-space distance from $[D \quad DX] = [T_1 G_1 \quad T_2 \quad A^f]$. Thus $d_S([T_{RRE} \quad M_{RRE}], [I_C \quad X]) \leq 2z$. $\square$

In the end combining Lemma 3 and Theorem 1 the receiver $\mathcal{R}$ can take $(\hat{L}_d, \hat{E}, r)$ as the input for the Gabidulin decoding algorithm and decode X_2 correctly.

Stage 2: Decoding X_1:

From equation (4) the receiver $\mathcal{R}$ gets $Y = [T_1 + E_1 \quad T_2 + E_2 \quad A + E_3]$. The receiver $\mathcal{R}$ computes $(T_2 + E_2)M_2$ and then it subtracts matrix $[O \quad (T_2 + E_2) \quad (T_2 + E_2)M_2]$ from Y. The resulting matrix has N zero columns in the middle (column $n+1$ to column $n+N$). Disregarding these we get:

$$Y' = [T_1 \quad T_1 M_1] + [E_1 \quad E_3 - E_2 M_2].$$

The new error matrix $E' = [E_1 \quad E_3 - E_2 M_2]$ has rank at most z over $\mathbb{F}_p$ since the columns of E' are simply linear combinations of columns of E whose rank is at most z. Therefore the problem degenerates into a single source problem and receiver $\mathcal{R}$ can decode X_1 with probability at

least $1 - |\mathcal{E}|/p$ by following the approach in [4].

Summarizing the above decoding scheme for X_1 and X_2, we have the main result in the section.

Theorem 3. *A non-coherent receiver $\mathcal{R}$ can efficiently decode both X_1 and X_2 correctly with probability at least $1 - 2|\mathcal{E}|/p$.*

C. Complexity discussion

The paper consider the technique of double field-extension to design double-access network codes robust against network errors. The technique has not been considered before in the literature, and makes achieving the rate-region proved in [7] computationally tractable.

For both coherent and non-coherent cases the computational complexity of Gabidulin encoding and decoding of two source messages is dominated by the decoding of X_2, which requires $\mathcal{O}(C \ell n N \log(nN))$ operations over $\mathbb{F}_p$ (see [4]).

To generalize our technique to more sources, consider a network with s sources $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_s$. Let R_i be the rate of $\mathcal{S}_i$ and $n_i = R_i + 2z$ for each $i \in [1, s]$. A straightforward generalization uses the multiple field-extension technique so that $\mathcal{S}_i$ uses the generator matrix over finite field of size $p^{n_1 n_2 \ldots n_i}$. In the end the packet length must be at least $n_g = n_1 n_2 \ldots n_s$, resulting in a decoding complexity $\mathcal{O}(C n_g^2 \log(n_g))$ increasing exponentially in the number of sources s. Thus the multiple field-extension technique works in polynomial time only for a fixed number of sources.

REFERENCES

[1] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, July 2000.

[2] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. of 2002 IEEE Information Theory Workshop (ITW)*, 2002.

[3] S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, and M. Médard, "Resilient network coding in the presence of byzantine adversaries," in *Proc. IEEE INFOCOM 2007*, 2007.

[4] D. Silva, F. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 3951–3967, Sept. 2008.

[5] C. Gkantsidis and P. Rodriguez, "Cooperative security for network coding file distribution," in *Proc. of the 25th IEEE INFOCOM*, 2006.

[6] D. Charles, K. Jain, and K. Lauter, "Signatures for network coding," in *Proc. of the Fortieth Annual Conference on Information Sciences and Systems*, 2006.

[7] S. Vyetrenko, T. Ho, M. Effros, J. Kliewer, and E. Erez, "Rate regions for coherent and noncoherent multisource network error correction," in *Proc. of ISIT 2009*, 2009.

[8] T. Ho, M. Medard, J. Shi, M. Effros, and D. R. Karger, "On randomized network coding," in *Proc. of Allerton 2003*, 2003.

[9] M. Artin, *Algebra*. New Jersey: Prentice Hall, 1991.

[10] R. Kötter and F. R. Kschischang, "Coding for errors and erasures in random network coding," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 3579–3591, Aug. 2008.

[11] E. M. Gabidulin, "Theory of codes with maximum rank distance," *Probl. Peredachi Inf.*, vol. 21, no. 1, pp. 3–16, 1985.

[12] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. Tolhuizen, "Polynomial time algorithms for multicast network code construction," *IEEE Transactions on Information Theory*, vol. 51, no. 6, pp. 1973–1982, 2003.

[13] M. Agrawa and S. Biswas, "Primality and identity testing via chinese remaindering," *Journal of the ACM*, 2003.

[14] P. A. Chou, Y. Wu, and K. Jain, "Practical network coding," in *Proc. of Allerton 2003*, 2003.