# Rate-Optimal Streaming Codes for Channels With Burst and Random Erasures

M. Nikhil Krishnan, Deeptanshu Shukla, and P. Vijay Kumar, *Fellow, IEEE*

***Abstract*— In this paper, we design erasure-correcting codes for channels with burst and random erasures, when a strict decoding delay constraint is in place. We consider the sliding-window-based packet erasure model proposed by Badr et al., where any time-window of width $w$ contains either up to $a$ random erasures or an erasure burst of length at most $b$. One needs to recover any erased packet with a strict decoding delay deadline of $\tau$, where erasures are as per the channel model. Presently existing rate-optimal constructions in the literature require, in general, a field-size which grows exponential in $\tau$, as long as $\frac{a}{\tau}$ remains a constant. In this work, we present a new rate-optimal code construction covering all channel and delay parameters, which requires an $O(\tau^2)$ field-size. As a special case, when $(b-a)=1$, we have a field-size linear in $\tau$. We also present two other constructions having linear field-size, under certain constraints on channel and decoding delay parameters. As a corollary, we obtain low field-size, rate-optimal convolutional codes for any given column distance and column span. Simulations indicate that the newly proposed streaming code constructions offer lower packet-loss probabilities compared to existing schemes, for selected instances of Gilbert-Elliott and Fritchman channels.**

***Index Terms*— Streaming codes, low latency, forward error correction (FEC), burst and random erasures, packet erasures, convolutional codes.**

## I. Introduction

RELIABLE communication at low-latency often comes up as an important requirement in the design of next-generation communication systems, including 5G, augmented reality and IoT. Low latency is particularly crucial for real-time multimedia applications, autonomous navigation and V2X (vehicle-to-everything) communications, 'working and playing' in the cloud, automation and remote management, tele-medicine and several other mission-critical scenarios [2]. A recent study [3] estimates that IP video traffic, a single use case of low-latency communication, will account for 82 percent of all consumer Internet traffic by 2021, up from 73 percent in 2016. The challenge of enabling delay-constrained communication is further exacerbated by issues arising out of noise, interference, fading, routing, mobility and reliability requirements. In order to ensure robust performance under such a wide range of operating conditions, networks provide for error detection, concealment and correction schemes at multiple layers. These error control strategies can be classified under two broad heads; retransmission strategies, like Automatic Repeat Request (ARQ) protocols, and channel coding or forward error correction (FEC). Choosing one of these error control strategies or a suitable hybrid of both of them is a critical design decision for any communication system.

### A. ARQ vs. FEC

Retransmission-based strategies, in general, add lower amount of redundancy compared to FEC, but incur an additional round-trip delay per retransmission. This might be acceptable for error control on a per hop basis, as in the link layer, but can significantly exceed latency requirements for long-distance communication. Retransmission also leads to more complicated protocols as the transmitter needs an acknowledgment from the receiver. If the message is received but its acknowledgment is lost, the sender will have to retransmit, wasting time and bandwidth. Retransmission-based error control is also not amenable to multicasting, a common data streaming scenario. Each client may miss different packets and retransmitting all of them may lead to a feedback implosion.

On the other hand, FEC is a more natural fit for low-latency applications. It incurs no round-trip delays, no acknowledgment issues and no feedback implosion during multicasting. Even in retransmission-based schemes like TCP, it is shown in [4], [5] that introducing FEC can lead to performance gains. But these advantages of FEC come at the cost of injecting redundancy. Hence the channel model and FEC parameters must be carefully calibrated to achieve optimal latency-redundancy tradeoff.

### B. Models for Handling Burst and Random Erasures

In end-to-end layers of the network, error control is mostly in the form of integrity checks such as checksums. These error detection features help the receiver infer if a packet has been received without any error. This can be naturally modeled by

Manuscript received March 15, 2019; revised October 27, 2019; accepted March 9, 2020. Date of publication March 25, 2020; date of current version July 14, 2020. The work of P. Vijay Kumar was supported in part by the J. C. Bose National Fellowship under Grant JCB/2017/000017 and in part by the NetApp University Research Fund under Grant SVCF-0002. This article was presented in part at the 2019 IEEE International Symposium on Information Theory (ISIT). *(Corresponding author: P. Vijay Kumar.)*

M. Nikhil Krishnan is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: nikhilkrishnan.m@gmail.com).

Deeptanshu Shukla is with Qualcomm, Bengaluru 560066, India (e-mail: deeptanshukla@gmail.com).

P. Vijay Kumar is with the Department of Electrical Communication Engineering, Indian Institute of Science, Bengaluru 560012, India, and also with the Department of Electrical and Computer Engineering, University of Southern California, Los Angeles, CA 90089 USA (e-mail: pvk1729@gmail.com).

Communicated by M. Schwartz, Associate Editor for Coding Techniques.

Color versions of one or more of the figures in this article are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2020.2983152

TABLE I

STREAMING CODE CONSTRUCTIONS FOR BURST/SLIDING-WINDOW-BASED ERASURE CHANNEL MODELS AND THEIR OPERATING REGIMES

| Streaming Code | Channel Model | Rate | Field Size | Rate-Optimal? | Explicit? |
|---|---|---|---|---|---|
| Maximally Short (MS) Codes [7] | Burst | $\frac{\tau}{\tau+b}$ | $O(\tau)$ | For $\tau \mod b = 1$ | Yes |
| Delay-Optimal Burst Erasure Codes [17] | Burst | " | $O(\tau)$ | Yes | Yes |
| MiDAS-m-MDS Codes [18] | Sliding-Window | $\frac{\tau-a}{\tau-a+b}$ | $\exp(\tau)$ | Near-optimal | Yes |
| MiDAS-interleaved Codes [18] | Sliding-Window | $\frac{\tau-a}{\tau-a+b}$ | $O(\tau^3)$ | Near-optimal | Yes |
| Embedded-Random Linear Codes [29] | Sliding-Window | $\frac{\tau-a+1}{\tau+b-a+1}$ | $\exp(\tau)$ | For $\frac{\tau-a+1}{\tau+b-a+1} = \frac{1}{2}$ | No |
| Random Convolutional Codes [19] | Sliding-Window | " | $\sim 2\binom{\tau+1}{a}$ | Yes | No |
| Construction A [20] | Sliding-Window | " | $O(\tau^2)$ | For $\tau \mod b \geq (b-a)$ or $b \mid \tau$ | Yes |
| Construction B [20] | Sliding-Window | " | $\sim (b-a)^{\tau+1}$ | Yes | Yes |
| Construction A (present paper) | Sliding-Window | " | $O(\tau^2)$ | Yes | No |
| Construction A (present paper) | Sliding-Window | " | $O(\tau)$ | For $(b-a)=1$ | No |
| Construction B (present paper) | Sliding-Window | " | $O(\tau)$ | For $(\tau+a+1) \geq 2b \geq 4a$ | Yes |
| Construction C (present paper) | Sliding-Window | " | $O(\frac{a}{b}\tau)$ | For $a \mid b \mid (\tau+1+b-a)$ | Yes |

an erasure channel. This model also incorporates packet drops due to other factors such as congestion, mis-routing and buffer overflows.

Measurements on real-world systems [6] indicate that erasures occur as isolated entities as well as in bursts. One means of modeling them is by using probabilistic channel models like Gilbert-Elliott (GE) and Fritchman Channels. However, such models are hard to analyze and even closed-form expressions for their capacities are not known. Thus, there is need for models rich enough to capture both isolated and burst erasures but simple enough to be tractable.

Another important consideration is to whether inject redundancy by introducing more packets per unit time (bandwidth expansion) or by increasing the packet size by adding redundancy within the packets (symbol expansion). In [7], the authors argue in favor of symbol expansion, as burst erasures often occur due to congestion in a network. Introducing more packets under such circumstances may lead to a congestion cycle [6] and degrade performance. Introducing new packets may also increase channel contention overhead [8]. Hence symbol expansion is often the preferred option. This leads to the question of what parities have to be added, i.e., what error-correcting code to be used. In response to these requirements, a new class of codes dedicated to transmitting packets over erasure channels under stringent decoding-delay constraints, named *streaming codes*, has emerged in recent years.

### C. A Brief History of Streaming Codes

While burst erasure correction has been studied for a very long time (for instance, see [9]–[15]), the problem of burst erasure correction under decoding delay constraints is relatively new and was first studied in [7]. Prior to this systematic study, off-the-shelf codes such as Reed-Solomon codes combined with heuristics like interleaving, mean burst loss length (MBL) and mean inter-loss distance (MILD) were employed for combating burst erasures in latency-critical applications [16]. In their model, Martinian and Sundberg [7] consider a channel which can introduce a burst erasure of length at most $b$. They incorporate latency-criticality in the model as a decoding delay constraint of $\tau$ packets, i.e., a packet transmitted at time $t$ must be recovered at the decoder by time $t+\tau$. The authors derive an upper bound on the rate of codes that can tolerate an erasure burst with delay at most $\tau$ and also obtain a family of rate-optimal codes for a wide range of parameters. The paper [17] provides a code construction which achieves the rate upper bound in [7] for all parameters $\{b, \tau\}$. The authors of [17] also introduce a *diagonal embedding technique* to design streaming codes using block codes as building blocks. In [18], a richer sliding-window-based erasure channel is proposed and analyzed, wherein any sliding-window of size $w$ can have either up to $a$ random erasures or an erasure burst of length at most $b$ (see Section III for a detailed explanation). The authors of [18] also derive an upper bound on the rate of streaming codes which can tolerate all the erasure patterns of the sliding-window channel model, with a delay of at most $\tau$. The works [19], [20] provide the first-known streaming codes that achieve the rate upper-bound in [18], for all feasible parameters. However except for a small range of parameters, the field-size requirements here are large; $> 2(\binom{\tau+1}{a} + \tau - b + 2)$ in [19] and $\sim (b-a)^{\tau+1}$ in [20]. In Table I, we provide a summary of streaming code constructions existing in the literature for these burst and sliding-window-based erasure channel models (including constructions from the present paper). Streaming codes have also been constructed for channels with unequal source-channel inter-arrival rates [18], multiplicative-matrix channels [21] and multiplexed communication scenarios with different decoding delays for different streams [22]. In [23], the authors consider

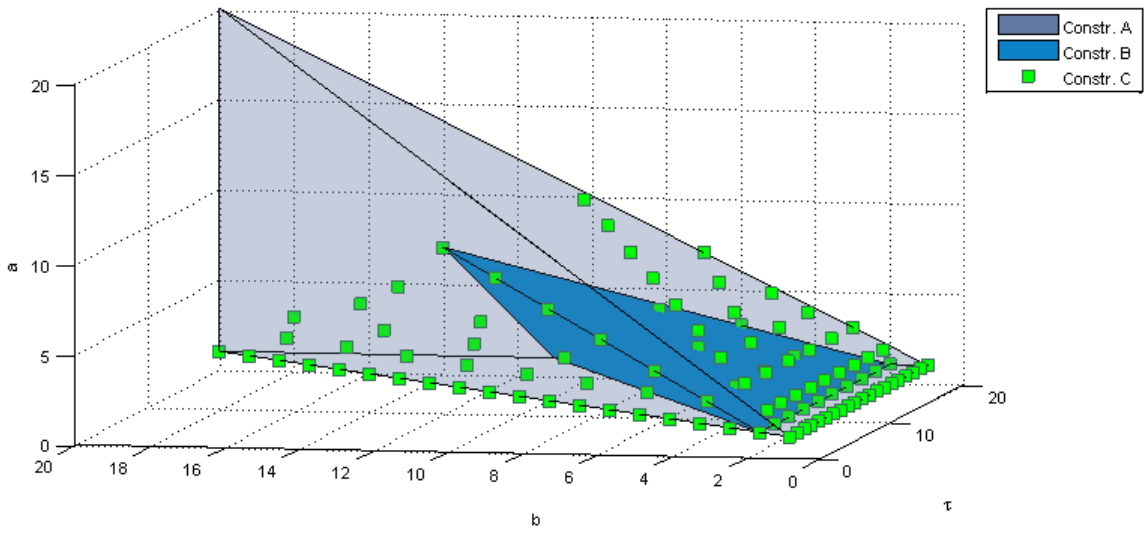



Fig. 1. Let $w = \tau + 1$. In the figure, we show all the valid parameter sets $\{a, b, \tau\}$ for Constructions A, B and C, where $a \leq b \leq \tau$, $\tau \leq 20$. Construction A covers the entire parameter range.

a setting for variable-size arrivals. Several other models for delay-constrained communication have been proposed and analyzed in works such as [24]–[28]. A comprehensive survey on streaming codes can be found in [8].

### *D. Contributions of the Present Paper*

We employ the diagonal embedding technique introduced in [17] to reduce the problem of designing streaming codes to that of constructing linear block codes with certain properties. We then translate these properties as some requirements on the parity-check (p-c) matrix (which is of size $b \times (\tau + b - a + 1)$) of the block code to be used for diagonal embedding. We provide three different families of code (p-c matrix) constructions, which will be referred to as Constructions A, B and C. All these block codes when used in conjunction with diagonal embedding, will result in rate-optimal streaming codes for the sliding-window-based erasure channel model.

Construction A works for all parameters $\{a, b, \tau, w\}$. The p-c matrix that we obtain in Construction A is not completely explicit. There are $(\tau + 1 - b)(b - a)$ entries of the p-c matrix which are not explicitly specified. An application of Combinatorial Nullstellensatz [30] guarantees that there exists an assignment of values to these entries so that the resultant p-c matrix satisfies the required properties. These entries however, can be easily determined via a greedy algorithm [31, Algorithm 1]. The remaining two constructions; Constructions B and C are explicit and cover a wide range of parameters. In terms of the field-size requirement, Construction A requires an $O(\tau^2)$ field-size, whereas the other two need a linear field-size. This is in contrast to the field-size requirements of currently existing rate-optimal streaming code constructions for the sliding-window-based channel model, which grow in general, exponential in $\tau$, once we fix the ratio $\frac{a}{\tau}$. In Fig. 1, we show all the valid parameters for the three constructions, when $\tau \leq 20$.

The rest of this paper is organized as follows; basic notation and some preliminary results regarding MDS codes are given in Section II. Section III describes the coding theoretic framework employed in this paper, the channel model and the technique of diagonal embedding, which reduces the design of streaming codes to that of block codes satisfying some specific conditions. In Sections IV and V, we present the three code constructions. In Section VI, by invoking results from [18], we discuss how the new code constructions imply the existence of rate-optimal convolutional codes for given column distance ($d_\tau$) and column span ($c_\tau$), which require a lower field-size, when compared to other rate-optimal convolutional code constructions in the literature. Section VII presents simulation results which indicate that the new streaming code constructions outperform existing streaming code constructions for some instances of GE and Fritchman channels.

## II. Punctured and Shortened Subcodes of an MDS Code

### *A. Notation*

For $m, n \in \mathbb{Z}$, let $[n] \triangleq \{i : 1 \leq i \leq n\}$ and $[m : n] \triangleq \{i : m \leq i \leq n\}$. The $n \times n$ identity matrix will be denoted by $I_n$. For a row vector $\underline{v}^T = [v_0 \; v_1 \; \ldots \; v_{n-1}] \in \mathbb{F}_q^n$, $\text{supp}(\underline{v}^T) \triangleq \{i : v_i \neq 0\}$. We write $m \mid n$ if $m$ divides $n$. Let $A \in \mathbb{F}_q^{m \times n}$, $\mathcal{I} \subseteq [0 : m-1]$, $\mathcal{J} \subseteq [0 : n-1]$. By $A(\mathcal{I}, \mathcal{J})$ we mean the $|\mathcal{I}| \times |\mathcal{J}|$ submatrix of $A$ obtained by selecting the rows indexed by $\mathcal{I}$ and columns indexed by $\mathcal{J}$. For $i \in [0 : m-1], j \in [0 : n-1]$, $A(i, :)$ and $A(:, j)$ will denote the $i$-th row and $j$-th column, respectively. Similarly, $A(\mathcal{I}, :)$ and $A(:, \mathcal{J})$ will denote the sub-matrices of $A$ obtained by selecting the rows in $\mathcal{I}$ and columns in $\mathcal{J}$, respectively. We will often use the alternative notation $\underline{a}_{\text{row},i}$ and $\underline{a}_i$ to denote the $i$-th row and $i$-th column of a matrix $A$, respectively. If $\mathcal{A} \subseteq [0 : n-1]$, then we will use $\mathcal{A}^c$ to denote the complement of $\mathcal{A}$ in $[0 : n-1]$, i.e., $\mathcal{A}^c \triangleq [0 : n-1] \setminus \mathcal{A}$. An $m \times n$ matrix $A$ is said to be *Cauchy-like*, if every square submatrix of $A$ is non-singular. The dual of an $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_q$, will be denoted by $\mathcal{C}^\perp$.

### B. Preliminaries

*Lemma 1 (Combinatorial Nullstellensatz [30]):* Consider a non-zero multivariate polynomial

$$f(x_1, x_2, \ldots, x_m) \in \mathbb{F}_q[x_1, x_2, \ldots, x_m].$$

Let the degree of the polynomial in the variable $x_i$ be $d_i$, for $1 \leq i \leq m$. If $|\mathbb{F}_q| > d_i$ for all $i \in [1:m]$, then there exists $(s_1, s_2, \ldots, s_m) \in \mathbb{F}_q^m$ such that $f(x_1 = s_1, x_2 = s_2, \ldots, x_m = s_m) \neq 0$.

*Definition 2 (Punctured Codes):* Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Given a subset $\mathcal{P}$ of $[0 : n-1]$, the code $\mathcal{C}$ *punctured on* the coordinates in $\mathcal{P}$, is the linear code of length $|\mathcal{P}^c| = n - |\mathcal{P}|$ obtained from $\mathcal{C}$ by deleting all the coordinates in $\mathcal{P}$. Equivalently, the code $\mathcal{C}$ punctured on the coordinates in $\mathcal{P}$ is the restriction of $\mathcal{C}$ to the coordinates in $\mathcal{P}^c$ and is denoted by $\mathcal{C}|_{\mathcal{P}^c}$. The punctured code (or restriction) $\mathcal{C}|_{\mathcal{P}^c}$ will also be referred to as $\mathcal{C}$ *punctured to* the coordinates in $\mathcal{P}^c$.

*Definition 3 (Shortened Codes):* Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$. Given a subset $\mathcal{P}$ of $[0 : n-1]$, consider first the subcode $\mathcal{C}^*$ given by:

$$\mathcal{C}^* = \{\underline{c}^T \triangleq (c_0\ c_1\ \ldots\ c_{n-1}) \in \mathcal{C} : c_i = 0\ \forall i \in \mathcal{P}\}.$$

Then by the phrase $\mathcal{C}$ *shortened on* the coordinates in $\mathcal{P}$, denoted by $\mathcal{C}^{\mathcal{P}^c}$, we will mean the linear code of length $n - |\mathcal{P}|$ obtained from $\mathcal{C}^*$ after puncturing on the coordinates given by $\mathcal{P}$. The code $\mathcal{C}^{\mathcal{P}^c}$ will also be referred to as the code $\mathcal{C}$ *shortened to* the coordinates in $\mathcal{P}^c$.

*Lemma 4 ([32, p. 17]):* Let $\mathcal{C}$ be an $[n, k]$ linear code over $\mathbb{F}_q$ and $\mathcal{P} \subseteq [0 : n-1]$. Then

$$(\mathcal{C}|_{\mathcal{P}})^{\perp} = (\mathcal{C}^{\perp})^{\mathcal{P}}.$$

An $m \times n$ matrix $A$ over a finite field $\mathbb{F}_q$, with $m \leq n$, will be referred to as an *MDS matrix* if any $m$ distinct columns of $A$ form a linearly independent set. Clearly, an MDS matrix $A$ can serve as the generator matrix of an $[n, m]$ MDS code.

*Lemma 5:* Let $\mathcal{C}_{\text{MDS}}$ denote an $[n, k]$ MDS code. Fix $l \in [k]$. Consider an $l \times n$ matrix $P$ whose $l$ rows $\{P(i,:)\}_{i=0}^{l-1}$ consist of $\ell$ linearly independent codewords $\{\underline{c}_i^T\}_{i=0}^{l-1}$ drawn from $\mathcal{C}_{\text{MDS}}$. Then if $|\cup_{i=0}^{l-1} \text{supp}(\underline{c}_i^T)| = n - k + l$, any choice of at most $l$ non-zero columns of $P$ forms a linearly independent set.

*Proof:* The basic idea here is to show that if a collection of $l$ independent codewords drawn from an $[n, k]$ MDS code share $k - l$ zeros in common, then the linear span of these $l$ codewords results in a shortened MDS code (after the $k - l$ coordinates containing the common zeros are deleted). More formally, it is known that shortening an $[n, k]$ MDS code on a set $\mathcal{S}$ of coordinates, where $\mathcal{S} \subseteq [0 : n-1]$, $|\mathcal{S}| = s$, $0 \leq s \leq k-1$, results in an $[n-s, k-s]$ MDS code. Let $\mathcal{A} \triangleq \cup_{i=0}^{l-1} \text{supp}(\underline{c}_i^T)$. Clearly span $< \underline{c}_0^T, \underline{c}_1^T, \cdots, \underline{c}_{l-1}^T >$, after removing the $k - l$ trivial zero coordinates corresponding to $\mathcal{A}^c$, is a subspace of the $[n-k+l, l]$ MDS code $\mathcal{C}_{\text{MDS}}^{\mathcal{A}}$ obtained by shortening $\mathcal{C}_{\text{MDS}}$ to $\mathcal{A}$. As $\text{rank}(P) = l$, the matrix $P$ (after removing the zero columns $\mathcal{A}^c$) is indeed a generator matrix for the shortened MDS code $\mathcal{C}_{\text{MDS}}^{\mathcal{A}}$ of dimension $l$. The lemma then follows. □

*Definition 6 (Zero-Band Generator Matrix of an MDS Code):* Consider an $[n, k]$ MDS code $\mathcal{C}_{\text{MDS}}$ over $\mathbb{F}_q$. A zero-band generator matrix (ZB generator matrix), say $Z$, corresponding to $\mathcal{C}_{\text{MDS}}$ is a $k \times n$ generator matrix of $\mathcal{C}_{\text{MDS}}$ that contains a diagonal band of $k-1$ consecutive zeros as shown below:

$$Z = \begin{bmatrix} * & 0 & 0 & \ldots & \ldots & 0 & * & * & * & \ldots & * & * & \ldots & * \\ * & * & 0 & \ldots & \ldots & 0 & 0 & * & * & \ldots & * & * & \ldots & * \\ * & * & * & 0 & \ldots & 0 & 0 & 0 & * & \ldots & * & * & \ldots & * \\ & & & \ddots & & & & & & \ddots & & & \ldots & * \\ * & * & * & \ldots & * & 0 & 0 & 0 & \ldots & 0 & * & * & \ldots & * \\ * & * & * & \ldots & * & * & 0 & 0 & \ldots & 0 & 0 & * & \ldots & * \end{bmatrix}.$$

More precisely, the $i$-th row of $Z$ (denoted by $\underline{z}_{\text{row},i}$), for $0 \leq i \leq k-1$, has a run of $k-1$ zeros spanning the coordinates $[i+1 : i+k-1] \pmod n$. Here each $*$ indicates a non-zero element in $\mathbb{F}_q$.

*Lemma 7:* Given an $[n, k]$ MDS code $\mathcal{C}_{\text{MDS}}$, there always exists a corresponding ZB generator matrix $Z$.

*Proof:* Let us choose the $i$-th row of $Z$ to be the non-zero codeword $\underline{c}_i^T \triangleq (c_{i,0}\ c_{i,1}\ \ldots\ c_{i,n-1}) \in \mathcal{C}_{\text{MDS}}$ such that $c_{i,j} = 0$ for $i+1 \leq j \leq i+k-1 \pmod n$. This can always be done since a codeword in an MDS code is uniquely specified by any set of $k$ coordinates and $k-1$ of them can be chosen to be zeros. Note that all the remaining $n-(k-1)$ coordinates of $\underline{c}_i^T$ are forced to be non-zero as $\mathcal{C}_{\text{MDS}}$ has minimum-distance and hence minimum Hamming weight, equal to $n-k+1$. The first $k$ columns of $Z$ then form a lower triangular matrix with non-zero entries along the diagonal. Hence $\text{rank}(Z) = k$ and $Z$ is a generator matrix for the MDS code. □

*Lemma 8:* Let $Z$ be a ZB generator matrix corresponding to an $[n, k]$ MDS code $\mathcal{C}_{\text{MDS}}$. Fix $i, j$ such that $0 \leq i \leq k-1$ and $1 \leq j \leq k-i$. Any choice of at most $j$ non-zero columns of the $j \times n$ matrix $Z(i : i+j-1, :)$ forms a linearly independent set.

*Proof:* The result follows from Lemma 5 by noting that the $j$ consecutive rows are linearly independent and that they have common zeros of size $k-j$ on the set of coordinates: $[i+j : i+k-1] \mod n$. □

*Lemma 9:* Consider an $[n, k]$ code $\mathcal{C}$. Let $H$ denote an $(n-k) \times n$ parity-check (p-c) matrix of $\mathcal{C}$, i.e., $\text{rank}(H) = n-k$ and $H\underline{c} = \underline{0}\ \forall \underline{c}^T \in \mathcal{C}$. Let the coordinates indexed by $\mathcal{E} \subseteq [0 : n-1]$ be erased from $\mathcal{C}$ and let $i \in \mathcal{E}$. Then the $i$-th code symbol in any codeword can be recovered from code symbols corresponding to the coordinates in $\mathcal{E}^c$ iff:

$$\underline{h}_i \notin \text{span}\left\langle \{\underline{h}_j\}_{j \in \mathcal{E} \setminus \{i\}} \right\rangle,$$

where $\underline{h}_j$ denotes the $j$-th column of $H$.

*Proof:* In order to make the paper self-contained, we present here a proof of this well-known result. First, we will prove the *if* part. Assume that the $i$-th code symbol of a codeword cannot be recovered from code symbols corresponding to the coordinates in $\mathcal{E}^c$, i.e., there exist two codewords $\underline{c}_1^T \triangleq (c_{1,0}\ c_{1,1}\ \ldots\ c_{1,n-1})$, $\underline{c}_2^T \triangleq (c_{2,0}\ c_{2,1}\ \ldots\ c_{2,n-1}) \in \mathcal{C}$ satisfying the property that $c_{1,m} = c_{2,m}\ \forall m \in \mathcal{E}^c$ and

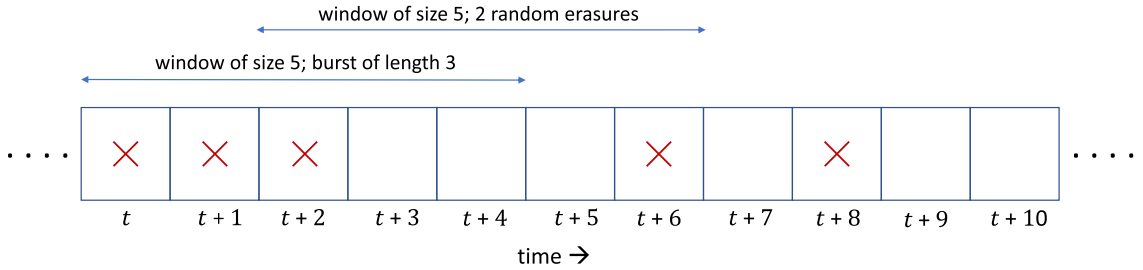



Fig. 2. An example channel realization under the SW channel model, for parameters $a = 2, b = 3, w = 5$. Here each $\times$ indicates an erasure.

$c_{1,i} \neq c_{2,i}$. As $H$ is a p-c matrix, we have:

$$\begin{aligned} \underline{0} &= \sum_{l=0}^{n-1} (c_{1,l} - c_{2,l})\underline{h}_l \\ &\overset{(a)}{=} \sum_{m \in \mathcal{E}} (c_{1,m} - c_{2,m})\underline{h}_m, \end{aligned} \tag{1}$$

where $(a)$ follows as $c_{1,m} = c_{2,m}\ \forall m \in \mathcal{E}^c$. From (1), we have $\underline{h}_i \in \text{span}\left\langle\ \{\underline{h}_j\}_{j \in \mathcal{E}\setminus\{i\}}\ \right\rangle$, as $c_{1,i} \neq c_{2,i}$. This completes the proof for the *if* part.

For the *only if* part, assume that $\underline{h}_i \in \text{span}\left\langle\ \{\underline{h}_j\}_{j \in \mathcal{E}\setminus\{i\}}\ \right\rangle$. Thus there exists a choice of $\{\lambda_m\}_{m \in \mathcal{E}} \subseteq \mathbb{F}_q$ with $\lambda_i \neq 0$ satisfying $\sum_{m \in \mathcal{E}} \lambda_m \underline{h}_m = \underline{0}$. Consider an arbitrary codeword $\underline{c}^T \in \mathcal{C}$ and let $\underline{c}_\lambda^T \triangleq (c_{\lambda,0}\ c_{\lambda,1}\ \ldots\ c_{\lambda,n-1}) \in \mathbb{F}_q^n$ be as follows:

$$c_{\lambda,l} = \begin{cases} c_l + \lambda_l, & \text{if } l \in \mathcal{E} \\ c_l, & \text{otherwise.} \end{cases}$$

As $\sum_{l=0}^{n-1} c_{\lambda,l}\underline{h}_l = \sum_{l=0}^{n-1} c_l \underline{h}_l + \sum_{m \in \mathcal{E}} \lambda_m \underline{h}_m = \underline{0} + \underline{0} = \underline{0}$, we have $\underline{c}_\lambda^T \in \mathcal{C}$. Clearly, $c_i \neq c_{\lambda,i}$ and $c_{m'} = c_{\lambda,m'}\ \forall m' \in \mathcal{E}^c$. Hence it is not possible to uniquely determine the $i$-th code symbol using the non-erased code symbols. This concludes the proof for the *only if* part. □

## III. A Coding Framework for Streaming Codes and the Sliding-Window Channel Model

### A. A Coding Framework for Streaming Codes

In this paper, we follow the packet-level FEC framework introduced by Martinian and Sundberg [7]. Let $k, n$ be integers such that $k < n$. The encoder $\mathbf{E}$ receives a *message packet* $\underline{s}(t) \in \mathbb{F}_q^k$,

$$\underline{s}(t) \triangleq [s_0(t)\ s_1(t)\ \ldots\ s_{k-1}(t)]^T, \quad t \in \{0, 1, 2, \ldots\},$$

at time $t$. The causal encoder $\mathbf{E}$ produces a *coded packet*:

$$\underline{x}(t) \triangleq \begin{bmatrix} \underline{s}(t) \\ \underline{p}(t) \end{bmatrix}$$

at time $t$, where the *parity packet* $\underline{p}(t) \triangleq [p_0(t)\ p_1(t)\ \ldots\ p_{n-k-1}(t)]^T \in \mathbb{F}_q^{n-k}$ is a function of message packets received till time $t$, i.e., $\{\underline{s}(0), \underline{s}(1), \ldots, \underline{s}(t)\}$. Between the encoder $\mathbf{E}$ and the decoder $\mathbf{D}$, there exists a channel which erases some of the transmitted coded packets. Let $\underline{y}(t)$ denote the received packet at time $t$. We have:

$$\underline{y}(t) = \begin{cases} *, & \text{if } \underline{x}(t) \text{ is erased,} \\ \underline{x}(t), & \text{otherwise.} \end{cases}$$

The delay-constrained decoder $\mathbf{D}$ with delay-parameter $\tau$ outputs the decoded message packet $\hat{\underline{s}}(t)$ by time $t + \tau$. Here $\hat{\underline{s}}(t)$, which is an estimate of the message packet $\underline{s}(t)$, is a function of received packets till time $t + \tau$, i.e., $\{\underline{y}(0), \underline{y}(1), \ldots, \underline{y}(t + \tau)\}$. In an ideal scenario, we would have $\hat{\underline{s}}(t) = \underline{s}(t)$. As $k$-length message packets are mapped to $n$-length coded packets at each time $t$, rate of the code $R$ is defined as $\frac{k}{n}$.

### B. Erasure-Channel Models

In [7], the authors propose a family of streaming codes that can tolerate a burst erasure of length $b$ with delay $\tau$. i.e., these codes enable recovery of message packet $\underline{s}(t)$ by time $t + \tau$, even when $\underline{y}(l) = *$ for $l \in [j : j + b - 1]$, where $t \in [j : j + b - 1], j \in \{0, 1, 2, \ldots\}$. At first glance this model might appear restricted to handling just a single erasure burst of length $b$ over all time. However because of the delay, this model forces the decoder to tolerate any number of bursts, as long as they are spaced apart by at least $\tau$ time units. Badr *et al.* [18] extend the burst-loss-based channel model introduced in [7] to include random erasures as well. The paper [18] introduces a sliding-window (SW) channel model with parameters $a$, $b$, $w$ in addition to the decoding delay parameter $\tau$. The model is as follows. Given any sliding-window of width $w$, the channel introduces either (i) a burst erasure of length at most $b$ or else, (ii) a total of at most $a$ random erasures (see Fig. 2). The SW model specializes to the burst-only model studied in [7], when $a = 1$ and $w = \tau + 1$. As explained below, the parameters $a, b, \tau, w$ are subject to certain constraints. We must have:

1) $a \leq b$, since if $a > b$, the burst-error requirement would be subsumed by the random-erasure requirement and rendered redundant,
2) $b \leq \tau$ in order to have non-zero rate when operating with a causal encoder,
3) $b < w$ to avoid admitting within the model, a never-ending continuous stream of erasures.

These constraints can be summarized in the form:

$$a \leq b \leq \min\{\tau, w - 1\}. \tag{2}$$

We will refer to $\{a, b, \tau, w\}$ as *the parameter set* of the Delay-Constrained SW (DC-SW) channel model [1]. We will assume

[1]The terminology "DC-SW channel model" clearly is an abuse of notation since the delay constraint is not part of the channel model, but rather a constraint placed on the decoder. We employ this terminology for the sake of convenience. This allows us to refer for example, to the set $\{a, b, \tau, w\}$ simply as the parameter set of the DC-SW channel.

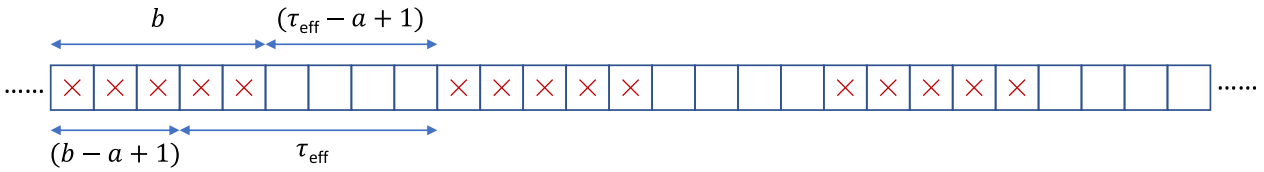



Fig. 3. A periodic erasure pattern with period $\tau_{\text{eff}} + \delta + 1$ for parameters $a = 3, b = 5, \tau_{\text{eff}} = 6$. Here each $\times$ indicates an erasure.

throughout the remainder of this paper that the parameter set satisfies the constraints laid out in (2).

Set $\delta \triangleq b - a$ and define the *effective time delay* parameter $\tau_{\text{eff}} \triangleq \min\{\tau, w-1\}$. The rate $R$ of a *streaming code* $\mathcal{C}_{\text{str}}$ which can faithfully recover all data with a delay not exceeding $\tau$, from all of the erasure patterns permitted under the DC-SW channel model, was shown in [18] to be upper bounded as below:

$$R \leq \frac{\tau_{\text{eff}} - a + 1}{\tau_{\text{eff}} + \delta + 1}. \tag{3}$$

The rate bound (3) can be derived from simply noting that any code which corrects all the erasure patterns permitted by the DC-SW channel needs to also recover from the periodic erasure pattern presented in Fig. 3. From an examination of this rate bound, one sees that the behavior with respect to $a$ and $b$ is asymmetrical. This might seem counter-intuitive since an MDS code which can recover from a burst of length $b$ (and having the least possible redundancy $b$ for a linear code), can in fact recover from $b$ random erasures. However, MDS codes cannot be directly employed in the current setting for the following reason. For simplicity, let $\tau_{\text{eff}} = \tau$. If the rate bound is achieved using a code with redundancy $b$, then the block length of the code must necessarily equal $\tau+\delta+1$. It can be shown that for an MDS code with block length $\tau + \delta + 1$ and dimension $\tau - a + 1$, the worst-case delay (in the presence of an erasure burst of length $b$) is $\tau + b - a \geq \tau$ with equality clearly iff $a = b$.

*Definition 10 (Rate-Optimal Streaming Code):* Given a DC-SW channel model with parameter set $\{a, b, \tau, w\}$, a streaming code $\mathcal{C}_{\text{str}}$ is said to be *rate-optimal* if the rate of the code meets the upper bound in (3) with equality and $\mathcal{C}_{\text{str}}$ permits recovery from all the erasure patterns as set by the DC-SW model.

### C. Relative Sizes of Window Length and Delay Parameters

Throughout the remainder of this paper, we assume $\tau_{\text{eff}} = \tau = w-1$. We provide here a justification for this assumption. Firstly, we note from the achievability results in [19], [20] that there exist rate-optimal constructions meeting (3) for all parameters $\{a, b, \tau, w\}$ satisfying $a \leq b \leq \tau = w - 1$.

Suppose one wants to design a rate-optimal code for the DC-SW channel with parameters $\{a, b, \tau, w > \tau+1\}$. Clearly, it is possible to construct a code without any rate penalty for a second DC-SW channel setting, where parameters $a, b, \tau$ are unchanged and $w = \tau + 1$. Here, the second channel setting is more stringent and permits many other erasure patterns in addition to those covered by the first setting. Hence instead of designing codes for parameters $\{a, b, \tau, w > \tau + 1\}$, one can consider designing codes for $\{a, b, \tau, w = \tau + 1\}$.

Now consider the remaining case of designing a rate-optimal code for the DC-SW channel with $\{a, b, \tau > w-1, w\}$. Again, without rate penalty, one can construct a code for a second, more stringent DC-SW channel setting, where parameters $a, b, w$ are unchanged and $\tau = w - 1$. It is straightforward to see that codes designed under the second setting offer a lower decoding delay.

Thus the parameter sets of the DC-SW channel model that we will focus on from here onward are of the form $\{a, b, \tau, w = \tau + 1\}$. We note that the authors of [18] also set $w \geq \tau + 1$, although employing a slightly different argument.

### D. An Equivalent Set of Conditions for Erasure Recovery

Given a DC-SW channel with parameter set $\{a, b, \tau, w\}$ and $w = \tau + 1$, it can be easily shown that a streaming code $\mathcal{C}_{\text{str}}$ recovers from all erasure patterns permissible under the DC-SW model iff the following conditions are true, for any $t \in \{0, 1, 2, \ldots\}$:

- J1. [*Burst Erasure Requirement*] $\mathcal{C}_{\text{str}}$ can guarantee recovery of $\underline{x}(t)$ with a delay of at most $\tau$ if $l$ consecutive coded packets $\underline{x}(j), \underline{x}(j+1), \ldots, \underline{x}(t), \ldots, \underline{x}(j+l-1)$ are erased, for any $j \in \{0, 1, 2, \ldots\}$ and $l \in [b]$ such that $t \in [j : j + l - 1]$.
- J2. [*Random Erasure Requirement]* $\mathcal{C}_{\text{str}}$ can guarantee recovery of $\underline{x}(t)$ with a delay of at most $\tau$ if coded packets $\{\underline{x}(j)\}_{j \in \mathcal{A}}$ are erased for any $\mathcal{A} \subseteq \{0, 1, 2, \ldots\}$ such that $|\mathcal{A}| \leq a$ and $t \in \mathcal{A}$.

### E. Convolutional Codes Derived From the Diagonal Embedding of a Block Code

The particular streaming code, which is a convolutional code, employed in the Martinian and Trott [17] scheme is constructed by embedding a block code in diagonal fashion (see Fig. 4). The same scheme has since been employed in [19], [20], [33] as it reduces the problem of designing a streaming code to that of carefully designing a block code that satisfies multiple constraints. We adopt the same approach in the present paper as well. Formally, the diagonal embedding scheme can be described as follows.

Let $\mathcal{C}$ be an $[n, k]$ code having a $k \times n$ systematic generator matrix $G = [I_k \ P]$, i.e., the first $k$ code symbols are message symbols. Set $r \triangleq n - k$. The parity symbols of the resultant systematic convolutional code after diagonally embedding $\mathcal{C}$ are given by:

$$\begin{aligned} &\big[p_0(t) \ p_1(t+1) \ \ldots \ p_{r-1}(t+r-1)\big] \\ &= \big[s_0(t-k) \ s_1(t-k+1) \ \ldots \ s_{k-1}(t-1)\big]P, \end{aligned} \tag{4}$$

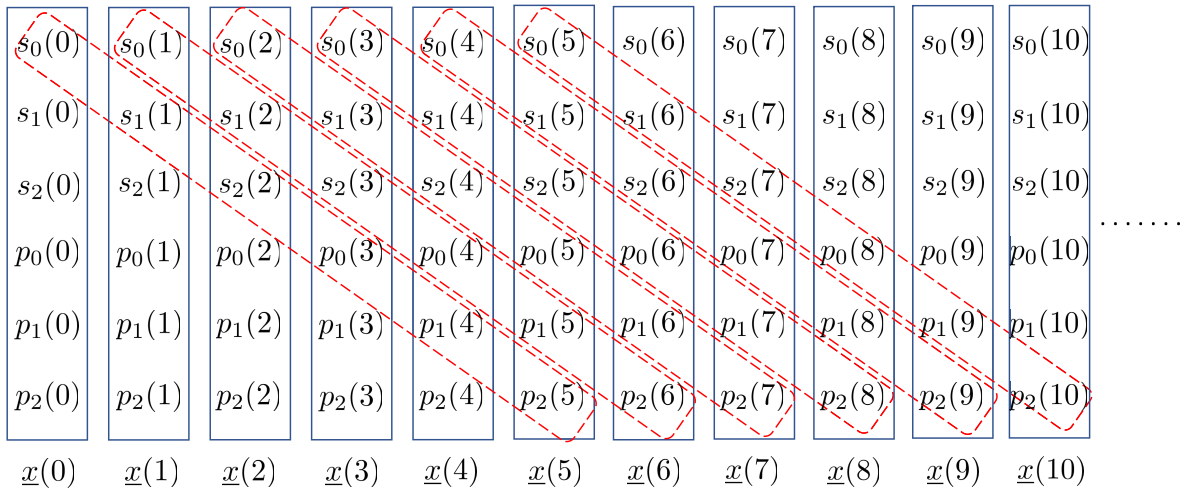



Fig. 4. The streaming code $\mathcal{C}_{\text{str}}$ obtained by diagonally embedding a $[6, 3]$ systematic block code $\mathcal{C}$. Each diagonal of the form $[s_0(t)\ s_1(t+1)\ s_2(t+2)\ p_0(t+3)\ p_1(t+4)\ p_2(t+5)]$ is a codeword in $\mathcal{C}$, where $t \in \mathbb{Z}$. The symbols $\{s_i(t)\}$ are raw message symbols belonging to the message packet $\underline{s}(t)$, whereas symbols $\{p_i(t)\}$ are parity symbols belonging to the parity packet $\underline{p}(t)$.

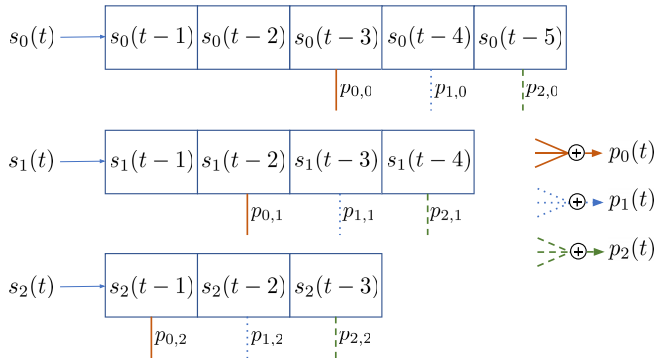



Fig. 5. An alternate representation of the streaming code $\mathcal{C}_{\text{str}}$ obtained by diagonally embedding a $[6, 3]$ block code $\mathcal{C}$ (see Fig. 4) using shift registers, to more clearly bring out its convolutional nature. Here $p_0(t) = p_{0,0}s_0(t-3) + p_{0,1}s_1(t-2) + p_{0,2}s_2(t-1)$ and so on.

for $t \in \mathbb{Z}$. Set $s_j(t) \triangleq 0$ when $t < 0$, for $0 \leq j \leq k-1$. We make the diagonal embedding technique explicit with the help of an example illustrated in Fig. 4, where $[n = 6, k = 3]$ and the submatrix $P$ is given by:

$$P = \begin{bmatrix} p_{0,0} & p_{1,0} & p_{2,0} \\ p_{0,1} & p_{1,1} & p_{2,1} \\ p_{0,2} & p_{1,2} & p_{2,2} \end{bmatrix}.$$

In order to bring out the convolutional nature of this encoder, we represent the encoding process in a more traditional manner using shift registers in Fig. 5.

In this paper, we follow the approach of building $\mathcal{C}_{\text{str}}$ via diagonal embedding a block code $\mathcal{C}$. Thus our aim is to construct, using the diagonal embedding technique, a streaming code $\mathcal{C}_{\text{str}}$ that can recover from any erasure pattern permissible under the DC-SW channel model. In the following, we discuss the requirements imposed on the block code $\mathcal{C}$.

*Example 11:* Consider the parameter set $\{a = 1, b = 3, \tau = 3, w = \tau + 1 = 4\}$. Our interest is in constructing a code $\mathcal{C}_{\text{str}}$ which can recover from all the erasure patterns permitted by the DC-SW channel model given these values of the parameters. Consider an $[n = 6, k = 3]$ block code $\mathcal{C}$ which is diagonally embedded to obtain $\mathcal{C}_{\text{str}}$. Note that the rate $R$ of the streaming code $\mathcal{C}_{\text{str}}$ is always equal to the rate of the block code used for diagonal embedding. In the present case, the rate $R = 0.5$, which meets (3) since here, $\delta = b - a = 2$ and hence:

$$R \leq \frac{\tau_{\text{eff}} - a + 1}{\tau_{\text{eff}} + \delta + 1} = \frac{3}{6} = \frac{1}{2}.$$

In Fig. 4 which corresponds to diagonally embedding a $[6, 3]$ code, assume coded packets $\underline{x}(5), \underline{x}(6), \underline{x}(7)$ are erased, i.e., there is a burst erasure of length $b = 3$ starting at time 5. Consider the recovery of $\underline{x}(5)$ with a delay of at most $\tau = 3$. In Table II, we list down various requirements to recover $\underline{x}(5)$, in terms of the symbols appearing in the streaming code $\mathcal{C}_{\text{str}}$ formed via diagonally embedding $\mathcal{C}$. Let $\underline{c}^T = (c_0\ c_1\ \ldots\ c_5)$ denote an arbitrary codeword in $\mathcal{C}$. In Table III, we translate the requirements presented in Table II to that on the code symbols $\{c_i\}_{i=0}^{5}$. To summarize, we have the condition on $\mathcal{C}$ that for all codewords $\underline{c}^T \in \mathcal{C}$, $c_i$ must be recoverable from $\{c_j : j \in [0 : i-1] \cup [i+3 : \min\{5, i+3\}]\}$. Note that here we considered the case where coded packet is erased as part of a burst erasure (see the packet-level recoverability requirement J1 in Section III-D). An analogous condition can be imposed on the block code $\mathcal{C}$ even for the case of random packet erasures (corresponds to the packet-level recoverability requirement J2 in Section III-D). We formally summarize in the following subsection the requirements on $\mathcal{C}$ so that the streaming code $\mathcal{C}_{\text{str}}$ ( formed via diagonally embedding $\mathcal{C}$) can recover any coded packet $\underline{x}(t)$ from a burst erasure of length $b$ or $a$ random erasures, with a delay constraint of $\tau$.

### *F. Requirements on the Block Code*

*Case (i)*: Let $\ell \in [0 : n-2-\tau]$ denote an erased coordinate. Owing to the delay constraint $\tau$, all the coordinates in $[\ell + \tau + 1 : n-1]$ are unavailable to the delay-constrained

TABLE II

ASSUME RECEIVED PACKETS $\underline{y}(5), \underline{y}(6), \underline{y}(7)$ ARE ERASED IN FIG. 4, I.E., A BURST ERASURE OF LENGTH 3. HERE WE STATE REQUIREMENTS TO RECOVER $\underline{x}(5)$ WITH A DELAY OF AT MOST $\tau = 3$, IN TERMS OF THE SYMBOLS APPEARING IN THE STREAMING CODE $\mathcal{C}_{\text{STR}}$

| Symbols to be recovered | Past known symbols | Erasure pattern | Symbols available (to the decoder) | Unavailable symbols (due to delay constraint) |
|---|---|---|---|---|
| $s_0(5)$ | - | $s_0(5), s_1(6), s_2(7)$ | $p_0(8)$ | $p_1(9), p_2(10)$ |
| $s_1(5)$ | $s_0(4)$ | $s_1(5), s_2(6), p_0(7)$ | $s_0(4), p_1(8)$ | $p_2(9)$ |
| $s_2(5)$ | $s_0(3), s_1(4)$ | $s_2(5), p_0(6), p_1(7)$ | $s_0(3), s_1(4), p_2(8)$ | - |
| $p_0(5)$ | $s_0(2), s_1(3), s_2(4)$ | $p_0(5), p_1(6), p_2(7)$ | $s_0(2), s_1(3), s_2(4)$ | - |
| $p_1(5)$ | $s_0(1), s_1(2), s_2(3), p_0(4)$ | $p_1(5), p_2(6)$ | $s_0(1), s_1(2), s_2(3), p_0(4)$ | - |
| $p_2(5)$ | $s_0(0), s_1(1), s_2(2), p_0(3), p_1(4)$ | $p_2(5)$ | $s_0(0), s_1(1), s_2(2), p_0(3), p_1(4)$ | - |

TABLE III

THE REQUIREMENTS IMPOSED ON THE CODE SYMBOLS OF THE DIAGONALLY-EMBEDDED BLOCK CODE $\mathcal{C}$ USED TO BUILD THE STREAMING CODE $\mathcal{C}_{\text{STR}}$

| Symbols to be recovered | Past known symbols | Erasure pattern | Symbols available (to the decoder) | Unavailable symbols (due to delay constraint) |
|---|---|---|---|---|
| $c_0$ | - | $c_0, c_1, c_2$ | $c_3$ | $c_4, c_5$ |
| $c_1$ | $c_0$ | $c_1, c_2, c_3$ | $c_0, c_4$ | $c_5$ |
| $c_2$ | $c_0, c_1$ | $c_2, c_3, c_4$ | $c_0, c_1, c_5$ | - |
| $c_3$ | $c_0, c_1, c_2$ | $c_3, c_4, c_5$ | $c_0, c_1, c_2$ | - |
| $c_4$ | $c_0, c_1, c_2, c_3$ | $c_4, c_5$ | $c_0, c_1, c_2, c_3$ | - |
| $c_5$ | $c_0, c_1, c_2, c_3, c_4$ | $c_5$ | $c_0, c_1, c_2, c_3, c_4$ | - |

decoder irrespective of whether some of these coordinates are erased or not. For any erased coordinate $i < \ell$, the $i$-th coordinate should be decodable by accessing code symbols up to the coordinate $(i+\tau) < (\ell+\tau)$. Hence during the decoding of $c_\ell$, all the symbols $c_0, \ldots, c_{\ell-1}$ can be assumed to be known. In summary, we have:

$$\underbrace{c_0, \cdots, c_{\ell-1}}_{\text{known}}, \quad \underbrace{c_\ell}_{\text{to be recovered}}, \quad \underbrace{c_{\ell+1}, \cdots, c_{\ell+\tau}}_{\text{all non-erased symbols accessible}}, \quad \underbrace{c_{\ell+\tau+1}, \cdots, c_{n-1}}_{\text{inaccessible, beyond delay constraint}}.$$

Let $\mathcal{K}$ denote the set of coordinates $[0 : \ell-1]$, $\mathcal{U}$ denote the set of coordinates $[\ell+\tau+1 : n-1]$ and $\mathcal{C}|_{\mathcal{U}^c}$ be the code obtained from $\mathcal{C}$ by puncturing on the coordinates in $\mathcal{U}$. Here one is faced with the task of decoding the code symbol $c_\ell$ using the code $\mathcal{C}|_{\mathcal{U}^c}$ when the code symbols $c_i, i \in \mathcal{K}$ are known and some of the code symbols among $c_i, i \in [\ell+1 : \ell+\tau]$ are possibly erased as per the DC-SW channel model. Let $H$ denote the p-c matrix of $\mathcal{C}$. The p-c matrix of $\mathcal{C}|_{\mathcal{U}^c}$ can be obtained as follows. We first identify a basis for the subspace of the row space of $H$ consisting of all the vectors having zeros in the coordinates making up $\mathcal{U}$. The required p-c matrix of $\mathcal{C}|_{\mathcal{U}^c}$ will then be formed using these basis vectors as its rows, after removing the trivial zero coordinates corresponding to $\mathcal{U}$. This is because, dual of a code punctured on $\mathcal{U}$ is the dual code shortened on $\mathcal{U}$ (see Lemma 4).

*Case (ii)*: Let $\ell \in [n-1-\tau : n-1]$ denote an erased coordinate. Here one is faced with the task of decoding the code symbol $c_\ell$ using the 'full' code $\mathcal{C}$, where code symbols $c_i, i \in \mathcal{K}$ are known and some of the symbols among $c_i, i \in [\ell+1 : n-1]$ are possibly erased as per the DC-SW channel model. The scenario is summarized as follows:

$$\underbrace{c_0, \cdots, c_{\ell-1}}_{\text{known}}, \quad \underbrace{c_\ell}_{\text{symbol to be recovered}}, \quad \underbrace{c_{\ell+1}, \cdots, c_{n-1}}_{\text{all the non-erased symbols are accessible}}.$$

### G. Consequent Requirements on the P-C Matrix $H$

Let $H$ be the p-c matrix of the code $\mathcal{C}$. For $0 \le \ell \le n-2-\tau$, let

$$H^{(\ell)} \triangleq \begin{bmatrix} \underline{h}_0^{(\ell)} & \cdots & \underline{h}_{\ell+\tau}^{(\ell)} \end{bmatrix}$$

denote a p-c matrix for the punctured code $\mathcal{C}|_{\mathcal{U}^c}$, where $\mathcal{U}^c \triangleq [0 : \ell+\tau]$. We will refer to $H^{(\ell)}$ as a *shortened p-c matrix* as dual of the punctured code $\mathcal{C}|_{\mathcal{U}^c}$ is the shortened dual code $(\mathcal{C}^\perp)^{\mathcal{U}^c}$ and the row space of $H^{(\ell)}$ is precisely $(\mathcal{C}^\perp)^{\mathcal{U}^c}$. Applying Lemma 9 and based on the observations in Section III-F, we have that the following conditions need to be satisfied by the p-c matrices $\{H^{(\ell)} \mid 0 \le \ell \le n-2-\tau\}$ and $H$:

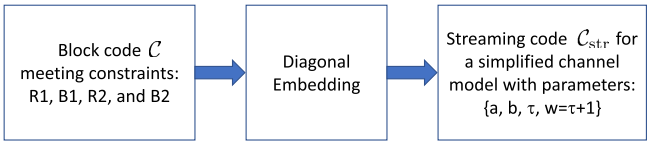



Fig. 6. The approach used in this paper to construct streaming codes for the DC-SW channel model.

1) **Condition B1** For $0 \leq \ell \leq n-2-\tau$, the $\ell$-th column, $\underline{h}_\ell^{(\ell)}$ of $H^{(\ell)}$ should be linearly independent of the set of $b-1$ columns
$$\left\{\underline{h}_j^{(\ell)} \mid \ell+1 \leq j \leq \ell+b-1\right\}.$$
2) **Condition B2** For $n-1-\tau \leq \ell \leq n-b$, the set
$$\left\{\underline{h}_j \mid \ell \leq j \leq \ell+b-1\right\}$$
of columns of $H$ should be linearly independent.
3) **Condition R1** For $0 \leq \ell \leq n-2-\tau$, the column $\underline{h}_\ell^{(\ell)}$ of $H^{(\ell)}$ should be linearly independent of any set of $a-1$ columns drawn from the set
$$\left\{\underline{h}_j^{(\ell)} \mid \ell+1 \leq j \leq \ell+\tau\right\}.$$
4) **Condition R2** Any set of $a$ columns from the set
$$\left\{\underline{h}_j \mid n-1-\tau \leq j \leq n-1\right\}$$
should be linearly independent.

*Remark 12:* In this paper, we aim to construct streaming codes for the DC-SW channel whose rates meet (3) with equality. Hence throughout the remainder of this paper, we choose the dimension $k$ of the block code $\mathcal{C}$ to be diagonally embedded, as $\tau-a+1$ and code length $n$ of $\mathcal{C}$ to be $\tau+\delta+1$. This way, the resultant convolutional code after diagonal embedding, $\mathcal{C}_{\text{str}}$ has a rate $R$ which meets the bound (3). We note in passing that if $gcd(\tau-a+1, b) = 1$, then such a construction will also have the least possible coded packet size $n$, i.e., will also be *packet-size-optimal*.

*Remark 13 (Systematicity):* As we choose dimension $k$ as $\tau-a+1$ and code length $n$ as $\tau+\delta+1$, we have $n-k=b$. Condition B2 ensures that, for the p-c matrix $H$ of size $b\times(\tau+\delta+1)$, the last $b$ columns are independent. Therefore $H$ can be expressed in the form $[H_1\ H_2]$, where the submatrix $H_1$ is of size $b\times k$ and the non-singular submatrix $H_2$ is of size $b\times b$. The generator matrix $G$ is then given by $[I_k\ P]$, where the $k\times b$ submatrix $P \triangleq -(H_2^{-1}H_1)^T$. This ensures that the first $k$ code symbols of the block code to be diagonally embedded are message symbols and thus aligns with the description of the diagonal-embedding-based encoder we illustrated in Fig. 4.

In Fig. 6, we summarize the approach used in this paper to construct streaming codes for the DC-SW channel model.

## IV. Quadratic Field-Size Construction A: for all Parameter Sets

In the present section and the next section, we will provide three different constructions for the diagonally-embedded block code $\mathcal{C}$ underlying the streaming code $\mathcal{C}_{\text{str}}$. We will simply refer to $\mathcal{C}$ as the block code. As the parameter $w=\tau+1$ is redundant, we consider the reduced parameter set $\{a,b,\tau\}$ for $\mathcal{C}$. As mentioned in Remark 12, our approach towards constructing a rate-optimal streaming code $\mathcal{C}_{\text{str}}$ whose rate matches with the upper bound in (3), is to construct a block code $\mathcal{C}$ with dimension, $k=\tau-a+1$ and code length, $n=\tau+1+\delta$. Under these choices of values for parameters $k,n$, since $n-k=\delta+a=b$, the p-c matrix will be of size $b\times n$.

The construction in the present section yields block codes for all parameters $\{a,b,\tau\}$. The required field-size in this construction, which we will refer to as Construction A, is $q^2$ where $q\geq\tau+1$. We describe the construction by successively refining or updating in four steps, our description of the p-c matrix $H$ of the code $\mathcal{C}$ over $\mathbb{F}_{q^2}$. We initialize $H$ to be the $b\times n$ all-zero matrix.

- *Step-a*: Set the $a\times(\tau+1)$ submatrix $H(\delta:b-1, 0:\tau)$ of $H$ to be the systematic generator matrix of an MDS code over $\mathbb{F}_q\subseteq\mathbb{F}_{q^2}$ that is of the form $[I_a\ C]$, where $C$ is an $a\times(\tau+1-a)$ Cauchy-like matrix. As $a+(\tau+1-a)=\tau+1\leq q$, there exists a Cauchy matrix of size $a\times(\tau+1-a)$ [34, Ch. 11], which may be chosen as $C$.
- *Step-b*: Set $H(0:\delta-1, 0:\delta-1)=\alpha I_\delta$, where $\alpha\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$.
- *Step-c*: If $\delta>0$, set $H(\delta,\tau+\delta)=1$ (any non-zero value in place of 1 would also work).
- *Step-d*: For $i\in[0:\delta-1]$, $j\in[b+i:\tau+i]$, set $H(i,j)=v_{i,j}$. Each $v_{i,j}$ here is a variable which will be assigned a carefully chosen value $a_{i,j}\in\mathbb{F}_q\subseteq\mathbb{F}_{q^2}$. The set of values $\{a_{i,j}\}$ are obtained as follows. Let $P_\ell \triangleq H(:,\ell:\ell+b-1)$, $\delta\leq\ell\leq\tau-a+1$. Consider the product of determinants $f\triangleq\prod_{\ell=\delta}^{\tau-a+1}\det(P_\ell)$. Here $f$ is a multivariate polynomial in the variables $\{v_{i,j}\}$. The set of values $\{a_{i,j}\}$ is found such that evaluating $f$ for $v_{i,j}=a_{i,j}\ \forall i,j$ results in a non-zero element in $\mathbb{F}_{q^2}$. As will be shown later in Lemma 16, since $q\geq\tau+1>\tau-b+2$[2], it is possible to obtain the desired set $\{a_{i,j}\}$. The following algorithm taken from [31] can be used to obtain $\{a_{i,j}\}$. This completes the p-c matrix $H$ construction.

In Fig. 7, we illustrate Construction A for parameters $\{a,b,\tau\}=\{5,8,12\}$.

*Remark 14:* For the trivial case $b=a$ and hence $\delta=0$, the p-c matrix $H$ of $\mathcal{C}$ takes the form $[I_a\ C]$. Thus $\mathcal{C}$ is a $[\tau+1,\tau-a+1]$ MDS code over $\mathbb{F}_q$. One can easily show that such an MDS code satisfies properties B1, B2, R1, R2 and therefore, results in a rate-optimal streaming code via diagonal embedding. Hence throughout the paper, we assume $\delta>0$.

*Lemma 15:* The multivariate polynomial $f$ in the variables $\{v_{i,j}\}$ is a non-zero polynomial.

*Proof:* We begin by noting that each $f_\ell\triangleq\det(P_\ell), \delta\leq\ell\leq\tau-a+1$ is a multivariate polynomial in a subset of variables drawn from $\{v_{i,j}\}$. Our goal here is to show that $f=\prod_{\ell=\delta}^{\tau-a+1}f_\ell$ is a non-zero polynomial, which is equivalent to showing that each component $f_\ell$ in the product is

[2]For the degenerate case of $b=a=1$, see Remark 14.

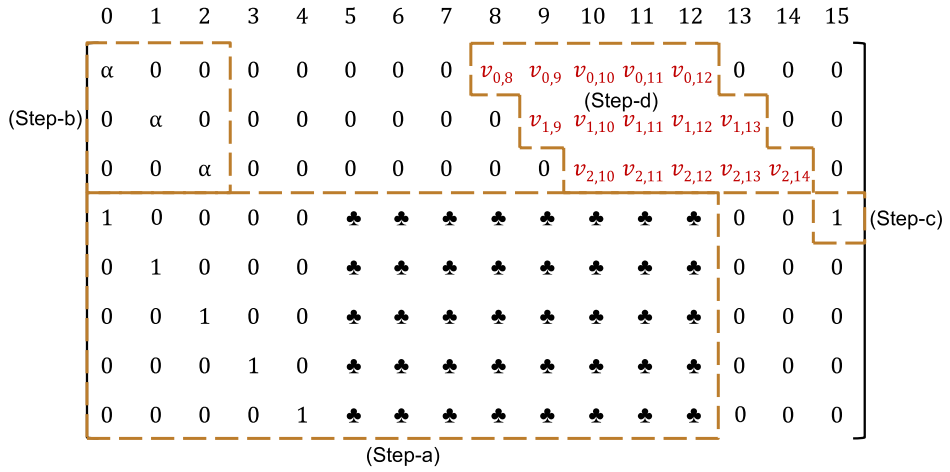



Fig. 7. The p-c matrix of an example code constructed using Construction A for the parameter set $\{a = 5, b = 8, \tau = 12\}$. Here we set $q = 2^4$ and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The submatrix $H(3:7, 5:12)$ is set to be a $5 \times 8$ Cauchy-like matrix $C$ whose entries (denoted by ♣) belong to $\mathbb{F}_q$. Each $v_{i,j}$ is a variable which is assigned a value $a_{i,j} \in \mathbb{F}_q$ obtained via Algorithm 1.

**Algorithm 1** Algorithm to Obtain Assignments $\{a_{i,j}\}$ for Variables $\{v_{i,j}\}$

**Input**: A non-zero multivariate polynomial $f$ over variables $\{v_{i,j}\}$

$g \leftarrow f$ // Initialising $g$ with the multivariate polynomial $f$

**for** $i \in [0 : \delta - 1]$ **do**

  **for** $j \in [b + i : \tau + i]$ **do**

    Find an $a_{i,j} \in \mathbb{F}_q$ such that $g|_{v_{i,j}=a_{i,j}}$ is a non-zero polynomial

    $g \leftarrow g|_{v_{i,j}=a_{i,j}}$ // Removing the variable $v_{i,j}$ from $g$ by setting $v_{i,j} = a_{i,j}$

**Output**: Set of values to be assigned: $\{a_{i,j}\}$

a non-zero polynomial. In order to prove that $f_\ell$ for a given $\ell \in [\delta : \tau - a + 1]$ is a non-zero polynomial, we will provide an explicit assignment specific to that value of $\ell$ to the variables $\{v_{i,j}\}$, for which $f_\ell$ evaluates to a non-zero element in $\mathbb{F}_{q^2}$.

When $\ell \in [\delta : \tau - a]$, for $0 \le i \le \delta - 1$ and $b + i \le j \le \tau + i$, we consider the assignment:

$$v_{i,j} = \begin{cases} 1, & \text{if } j = a + i + \ell, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

For $\ell \in [\delta : \tau - a]$, the $\ell$-specific assignment (5) results in $P_\ell$ taking the form shown in Fig. 8. In Fig. 8, the top-right $\delta \times \delta$ submatrix $P_{\ell,3} = I_\delta$ and hence is invertible. The bottom-left $a \times a$ submatrix $P_{\ell,2}$ is formed of $a$ columns of the MDS matrix $[I_a \ C]$ described in Step-a of the construction of $H$. Hence $P_{\ell,2}$ is also invertible. It follows that with respect to the assignment (5), $P_\ell$ is non-singular. Thus we have shown that for any $\ell \in [\delta : \tau - a]$, $f_\ell$ is a non-zero multivariate polynomial.

For the remaining case of $\ell = \tau - a + 1$, we consider the assignment:

$$v_{i,j} = \begin{cases} 1, & \text{if } j = \tau + i, \\ 0, & \text{otherwise,} \end{cases} \tag{6}$$

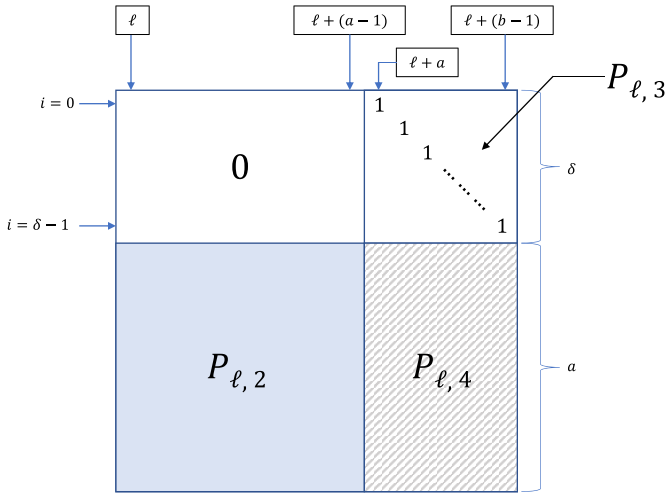



Fig. 8. This figure is relevant to the proof showing that $f$ is a non-zero polynomial. In this figure, we illustrate the structure of the matrix $P_\ell$ after the assignment (5). Here $P_{\ell,2}$ is an $a \times a$ submatrix of an $a \times (\tau + 1)$ MDS matrix and hence is invertible. It follows that $P_\ell$ is invertible.

where $0 \le i \le \delta - 1$ and $b + i \le j \le \tau + i$. This $\ell$-specific assignment results in $P_\ell$, where $\ell = \tau - a + 1$, taking the form shown in Fig. 9. In Fig. 9, $P_{\ell,2} \triangleq H(\delta + 1 : b - 1, \tau - a + 1 : \tau - 1)$ is an $(a - 1) \times (a - 1)$ submatrix of the MDS matrix $H(\delta + 1 : b - 1, 1 : \tau)$ of size $(a - 1) \times \tau$ and is hence invertible. The matrix $P_{\ell,3}$, as can be observed in Fig. 9, takes on the form $I_{\delta+1}$ with an extra non-zero element in the bottom left corner. Invertibility of the matrix $P_\ell$ can now be shown in a straightforward manner as follows. The last column of $P_\ell$ has a 1 in row $\delta$ and zeros elsewhere. We zero out all the other non-zero entries of the matrix $P_\ell$ in row $\delta$ by subtracting an appropriate scalar multiple of the last column. This will result in a matrix of the form:

$$\begin{bmatrix} [0] & Q_{\ell,3} \\ Q_{\ell,2} & Q_{\ell,4} \end{bmatrix},$$

where $Q_{\ell,2} = P_{\ell,2}$ and $Q_{\ell,3} = I_{\delta+1}$, both of which are invertible. This in turn proves that $P_\ell$ with the assignment (6) is invertible and hence $f_\ell$ is a non-zero polynomial. □

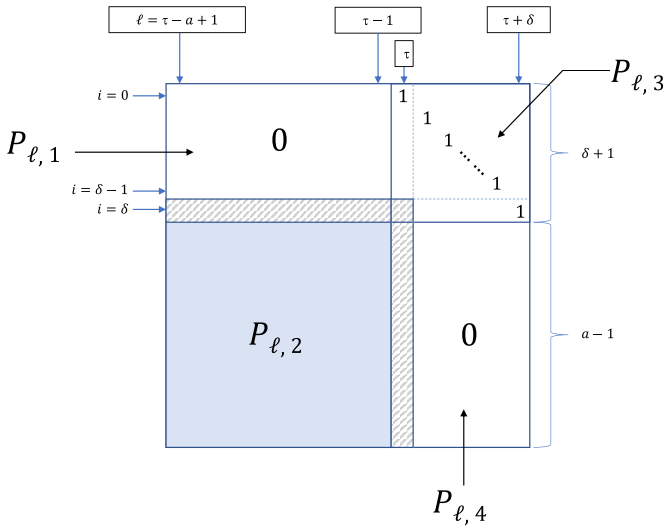



Fig. 9. This figure is relevant to the proof showing that $f$ is a non-zero polynomial. Let $\ell = \tau - a + 1$. In this figure, we illustrate the structure of $P_\ell$ after the assignment (6). Here $P_{\ell,2}$ is an $(a-1) \times (a-1)$ submatrix of the $(a-1) \times \tau$ MDS matrix $H(\delta + 1 : b - 1, 1 : \tau)$. It can be shown that $P_\ell$ is invertible.

*Lemma 16:* Let $0 \leq i \leq \delta - 1$ and $b + i \leq j \leq \tau + i$. There exists a set of values $\{a_{i,j}\} \subseteq \mathbb{F}_q$ such that $f$ evaluated at $v_{i,j} = a_{i,j}$ $\forall i, j$ yields a non-zero element in $\mathbb{F}_{q^2}$.

*Proof:* We begin by noting that each multivariate polynomial $f_\ell = \det(P_\ell)$ has a degree of at most 1 in each of the variables $\{v_{i,j}\}$. It follows that the product $\prod_{\ell=\delta}^{\tau-a+1} \det(P_\ell)$ is a multivariate polynomial that is of degree at most $(\tau - a + 1 - \delta) + 1 = \tau - b + 2$ in each variable. As $f$ is a non-zero polynomial (see Lemma 15) and the field-size $q \geq (\tau + 1) > (\tau - b + 2)$, we can apply the Combinatorial Nullstellensatz (see Lemma 1) to show that there exists an assignment of the variables over $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$ for which $f$ evaluates to a non-zero value. □

*Theorem 17:* The code $\mathcal{C}$ over $\mathbb{F}_{q^2}$ having p-c matrix $H$, when employed as the diagonally-embedded block code, will yield a rate-optimal streaming code $\mathcal{C}_{\text{str}}$.

*Proof:* Clearly, it suffices to show that with the assignment $v_{i,j} = a_{i,j}$ where $0 \leq i \leq \delta - 1$ and $b + i \leq j \leq \tau + i$, the p-c matrix $H$ satisfies the four conditions laid out in Section III-G. For $\ell \in [0 : \delta - 1]$, let $R_\ell \triangleq [0 : \ell] \cup [\delta + 1 : b - 1]$. For any $i$ from the set $R_\ell$, the $i$-th row $H(i, :)$ has a run of $\delta - \ell$ zeros across columns $[\ell + \tau + 1 : n - 1]$ (see Fig. 10 for an example). Hence $H(i, 0 : \ell + \tau)$ can be chosen to be a row of the shortened p-c matrix $H^{(\ell)}$. Condition B2 requires the last $b$ columns of $H$ to be independent and hence it can be shown that $H^{(\ell)}$ has precisely $b - \delta + \ell$ rows. As $|R_\ell| = b - \delta + \ell$, we choose $H^{(\ell)}$ as:

$$H^{(\ell)} = H(R_\ell, 0 : \ell + \tau).$$

- *Recovery from burst erasure of length at most $b$*:
  - Condition B1: For $\ell \in [0 : \delta - 1]$, the $\ell$-th row $\underline{h}_{\text{row},\ell}$ of the p-c matrix $H$ takes the form:

$$\underline{h}_{\text{row},\ell} = [\underbrace{0 \cdots 0}_{\ell \text{ symbols}} \ \alpha \ \underbrace{0 \cdots 0}_{(b-1)\text{symbols}} \ \triangle \cdots \triangle \ \underbrace{0 \cdots 0}_{\text{last } (\delta-\ell) \text{ symbols}} \ ],$$

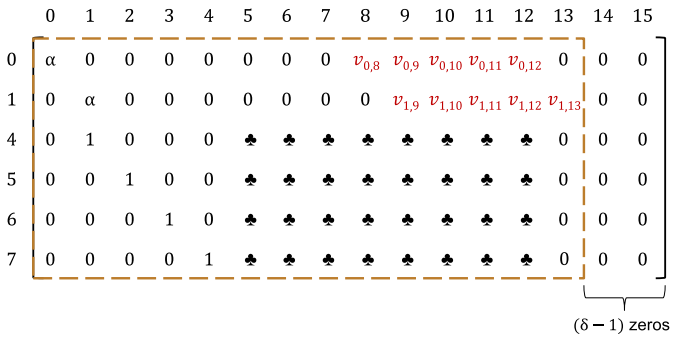



Fig. 10. Consider the p-c matrix $H$ given in Fig. 7. Let $\ell = 1$. All the rows $R_1 = [0 : 1] \cup [4 : 7]$ of $H$ have a run of zeros among the last $\delta - \ell = 2$ coordinates. The submatrix demarcated here in dashed lines is the shortened p-c matrix $H^{(1)}$.

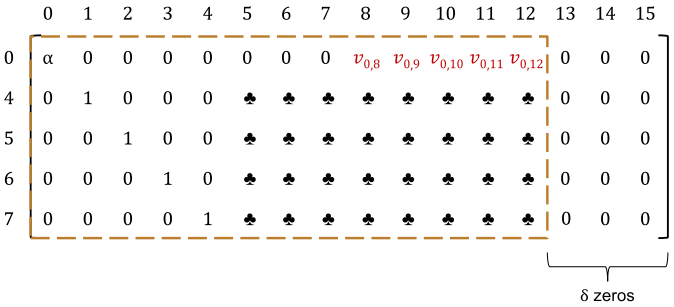



Fig. 11. Consider the p-c matrix $H$ given in Fig. 7. The submatrix demarcated here in dashed lines is the shortened p-c matrix $H^{(0)}$.

where $\triangle$'s denote field elements drawn from $\mathbb{F}_q$. As $\ell \in R_\ell$, the vector $\underline{h}_{\text{row},\ell}(:, 0 : \ell + \tau)$ is a row of $H^{(\ell)}$. As $\underline{h}_{\text{row},\ell}(:, \ell) = \alpha \neq 0$ and $\underline{h}_{\text{row},\ell}(:, i) = 0$ $\forall i \in [\ell + 1 : \ell + b - 1]$, condition B1 follows.

  - Condition B2: As $n = \tau + \delta + 1$ and $k = \tau - a + 1$, condition B2 is equivalent to the scenario that all the matrices $P_\ell$, $\delta \leq \ell \leq \tau - a + 1$ (with the assignment $v_{i,j} = a_{i,j}$) are non-singular. In other words $f = \prod_{\ell=\delta}^{\tau-a+1} \det(P_\ell)$ when evaluated at $v_{i,j} = a_{i,j}$ results in a non-zero value $\in \mathbb{F}_{q^2}$, which is true from the choice of $\{a_{i,j}\}$. Thus $H$ satisfies condition B2.

- *Recovery from at most $a$ random erasures*:
  - Condition R1: Fix $\ell \in [0 : \delta - 1]$. We divide the proof into two cases.
    - (*Case I*: $\ell = 0$): Let $R \triangleq [\delta + 1 : b - 1]$. As $R \subseteq R_0$, the $(a-1) \times (\tau + 1)$ matrix $H(R, 0 : \tau)$ consists of $a - 1$ rows of $H^{(0)}$ (e.g., see Fig. 11). It suffices to show that $H(R, 0 : \tau)$ satisfies condition R1. The matrix $H(R, 0 : \tau)$ has a zero-column at column 0 and rest of the columns of $H(R, 0 : \tau)$ form an $(a - 1) \times \tau$ MDS matrix (e.g., see Fig. 12). Hence R1 is satisfied for $\ell = 0$.
    - (*Case II*: $\ell \in [1 : \delta - 1]$): Let $S_\ell \triangleq \{\ell\} \cup [\delta + 1 : b - 1]$. As $S_\ell \subseteq R_\ell$, the matrix $H(S_\ell, 0 : \ell + \tau)$ consists of $a$ rows of $H^{(\ell)}$ (e.g., see Fig. 13). Similar to Case I, it suffices to show that $H(S_\ell, 0 : \ell + \tau)$ satisfies condition R1. In order to show this, we partition the matrix $H(S_\ell, 0 : \ell + \tau)$ in the

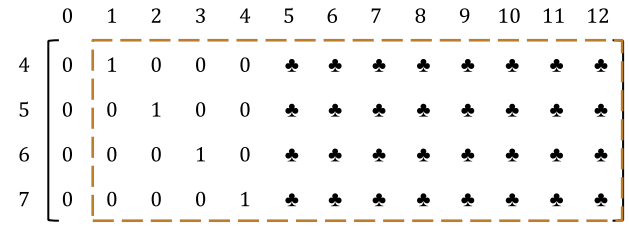


Fig. 12. An illustration of $H(R, 0:\tau)$ which consists of $a-1=4$ rows of $H^{(0)}$. The submatrix of size $4\times 12$ demarcated by dashed lines, is an MDS matrix.

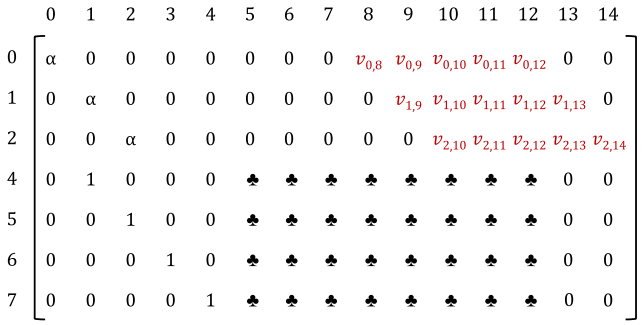


Fig. 13. The shortened p-c matrix $H^{(2)}$ for the p-c matrix given in Fig. 7.

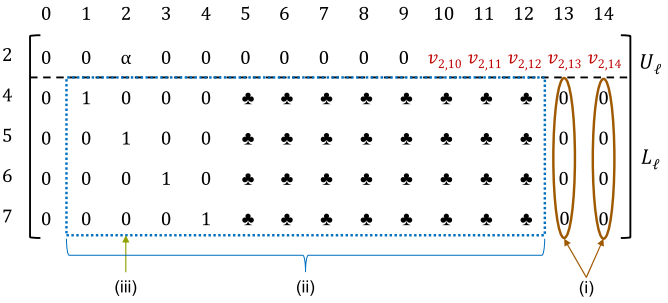


Fig. 14. Let $\ell=2$, $S_\ell=\{2\}\cup[4:7]$ for the p-c matrix given in Fig. 7. The matrix $H(S_\ell, 0:\ell+\tau)$ formed by $a$ rows of $H^{(2)}$ is partitioned into $U_\ell$ and $L_\ell$. Here the submatrix of $L_\ell$ demarcated by dotted lines is an MDS matrix.

following form:

$$\begin{bmatrix} U_\ell \\ L_\ell \end{bmatrix},$$

where $U_\ell \triangleq H(\ell, 0:\ell+\tau)$ and $L_\ell \triangleq H(\delta+1: b-1, 0:\ell+\tau)$ (see Fig. 14 for an example case of $\ell=2$). Note that $U_\ell = [U_{\ell,0}\ \ U_{\ell,1}\ \ \cdots\ \ U_{\ell,\ell+\tau}]$ is a row vector. An inspection of $L_\ell$ reveals the following facts:

(i) the $\ell$ columns $[1+\tau:\ell+\tau]$ of $L_\ell$ are all zero-columns; in other words, the entries of $H(\delta+1: b-1, 1+\tau:\ell+\tau)$ are all zero;

(ii) $L_\ell(:, 1:\tau)$ is an MDS matrix of size $(a-1)\times\tau$ over the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^2}$.

(iii) the $\ell$-th column of the matrix $L_\ell$ is within the MDS matrix $L_\ell(:, 1:\tau)$ since $\ell\in[1:\delta-1]$ and $\tau\geq b>\delta$.

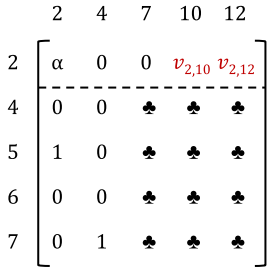


Fig. 15. Let $\ell=2, A_\ell=\{2,4,7,10,12\}$. Here any 4 columns of the $4\times 5$ submatrix indexed by rows $[4:7]$ form an independent set. The linear combination shown in (8) would then imply that the choice of coefficients $\{a_4, a_7, a_{10}, a_{12}\}$ is unique, with all the coefficients drawn from $\mathbb{F}_q\backslash\{0\}$. However $\alpha\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $\{v_{2,10}, v_{2,12}\}\subseteq\mathbb{F}_q$. Hence we arrive at a contradiction to (7).

In Fig. 14, we illustrate these facts with respect to an example.

Now assume contrary to the condition R1, that there exists a set of $a$ coordinates, $A_\ell\subseteq[\ell:\ell+\tau]$, with $|A_\ell|=a$ and $\ell\in A_\ell$ such that $\underline{h}_\ell^{(\ell)}$ lies in the span of columns $\{\underline{h}_i^{(\ell)}\mid i\in A_\ell\setminus\{\ell\}\}$, i.e.,

$$\underline{h}_\ell^{(\ell)} = \sum_{i\in A_\ell\setminus\{\ell\}} a_i \underline{h}_i^{(\ell)}, \tag{7}$$

where $a_i\in\mathbb{F}_{q^2}$. Equation (7) implies the following:

$$L_\ell(:,\ell) = \sum_{i\in A_\ell\setminus\{\ell\}} a_i L_\ell(:,i), \tag{8}$$

$$U_{\ell,\ell} = \sum_{i\in A_\ell\setminus\{\ell\}} a_i U_{\ell,i}. \tag{9}$$

As $A_\ell\subseteq[\ell:\ell+\tau]$ by assumption, (i), (ii) and (iii) would then imply that in order for (8) to happen, $A_\ell\subseteq[\ell:\tau]$ and the coefficients $\{a_i\}$ are uniquely determined, must be all-non-zero and must all belong to the subfield $\mathbb{F}_q$. Now consider the equation (9). We have $U_{\ell,\ell}=\alpha\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $U_{\ell,i}\in\mathbb{F}_q$ for $i\neq\ell$. Together with the constraint imposed by (8) that $\{a_i\}\subseteq\mathbb{F}_q$, we have $LHS\in\mathbb{F}_{q^2}\setminus\mathbb{F}_q$ and $RHS\in\mathbb{F}_q$ for (9). This clearly contradicts (7). Thus our assumption as to the existence of $A_\ell$ is invalid, which proves that $H$ satisfies the condition R1. In Fig. 15, we consider an example case where $\ell=2$ and $A_\ell=\{2,4,7,10,12\}$.

– Condition R2: Let $S\triangleq[\delta:b-1]$. We make the following three observations:

1) The columns $\{H(S,i)\mid i\in[\tau+1:\tau+\delta-1]\}$ are all-zero columns.
2) The matrix formed using the remaining columns of $H(S,\delta:n-1)$, i.e., $H(S,[\delta:n-1]\backslash[\tau+1:\tau+\delta-1])$, is an MDS matrix of size $a\times(a+(\tau-b)+2)$.
3) The collection of columns $\{\underline{h}_j\mid j\in[\tau+1:\tau+\delta-1]\}$ forms a linearly independent set as required by condition B2, since it is a subset of

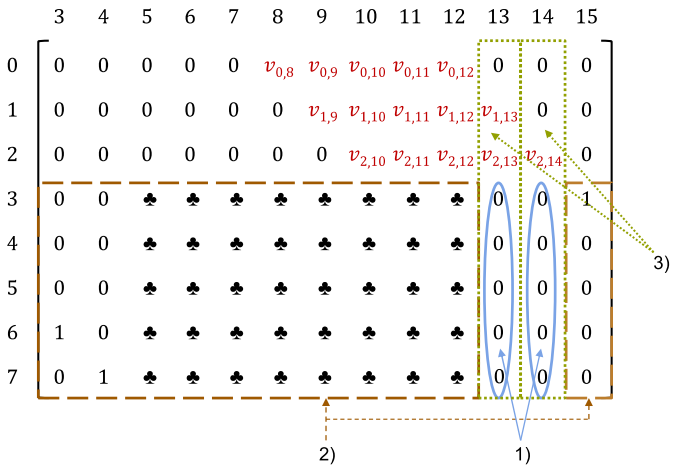



Fig. 16. An illustration of $H(:, \delta : n-1)$ for the p-c matrix given in Fig. 7. In the figure, the three observations we make in the proof of condition R2 are identified.

the larger linearly independent set of $b$ columns, $\{\underline{h}_j \mid j \in [\tau - a + 1 : \tau + \delta]\}$.

In Fig. 16, we illustrate these observations with the help of an example. In order to establish Condition R2, assume there exists a set $A_\ell \subseteq [\delta : n-1]$ with $|A_\ell| \leq a$ such that:

$$\sum_{i \in A_\ell} a_i \underline{h}_i = 0, \tag{10}$$

where the $\{a_i\}$ are all $\neq 0$. From the observations 1) and 2) above, we have that $A_\ell$ cannot contain any of the columns in $[\delta : n-1] \setminus [\tau + 1 : \tau + \delta - 1]$. However on the other hand, observation 3) states that the remaining columns form an independent set. Hence (10) is not feasible and thus condition R2 is satisfied.

□

*Remark 18 ($O(\tau)$ Field-Size Construction for $\delta = 1$):* If $\delta = 1$, the property $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ will not be used in the proof of Theorem 17. Hence for the case of $\delta = 1$, $\alpha$ may be chosen to be a non-zero element drawn from $\mathbb{F}_q$. This results in a code $\mathcal{C}$ over $\mathbb{F}_q$.

## V. Linear Field-Size Constructions for Specific Parameter Regimes

### A. Construction B: for $\delta \geq a$ and $\tau + 1 \geq b + \delta$

Here we provide a second construction (which we will refer to as Construction B), which is explicit and furthermore, requires a field-size $q$ that is linear in $\tau$. More specifically, the construction works for all parameters $\{a, b, \tau\}$ satisfying:

- $\tau + 1 \geq b + \delta$, $\delta \geq a$ and $q \geq \tau + 1$.

As in the other two constructions A and C, we assume that the block code length, $n = \tau + 1 + \delta$ and dimension, $k = \tau - a + 1$. Again, we describe the construction by successively refining in four steps, our description of the p-c matrix $H$ of the code $\mathcal{C}$ over $\mathbb{F}_q$. We initialize $H$ to be the $b \times n$ all-zero matrix.

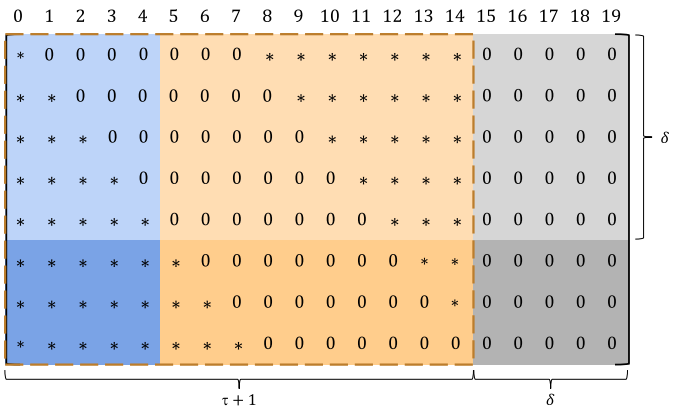



Fig. 17. $H$ after Step-a for parameters $\{a, b, \tau\} = \{3, 8, 14\}$. The submatrix $H(:, 0 : 14)$ (demarcated by dashed lines) is a ZB generator matrix $G_{\text{MDS}}$ corresponding to a $[15, 8]$ MDS code.

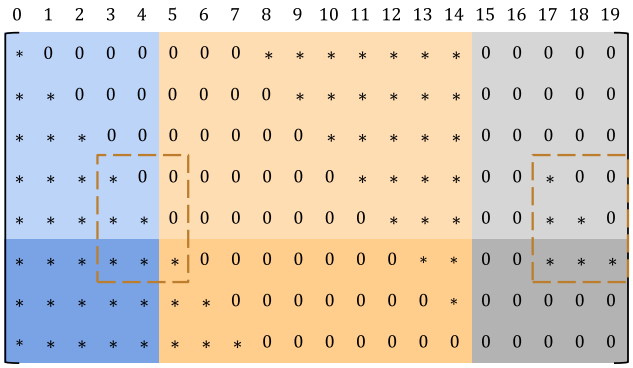


Fig. 18. $H$ after Step-b for parameters $\{a, b, \tau\} = \{3, 8, 14\}$. Here we replicate a portion of the p-c matrix.

- Step-a: Let $G_{\text{MDS}}$ be a ZB generator matrix corresponding to a $[\tau + 1, b]$ MDS code, say $\mathcal{C}_{\text{MDS}}$, over $\mathbb{F}_q$. We update $H$ by setting $H(:, 0 : \tau) = G_{\text{MDS}}$. As $q \geq \tau + 1$, the existence of such a matrix $G_{\text{MDS}}$ is guaranteed.
- Step-b: Next, we update $H$ by setting $H(a : \delta, \tau + a : \tau + \delta) = H(a : \delta, a : \delta)$ (elements of the submatrix on the RHS are already defined in Step-a).
- *Step-c*: For $1 \leq j \leq a - 1$, we set $H(b - j, \tau + j) = 1$ (any non-zero value in place of 1 would also work).
- *Step-d*: In the final update, we replace $H(\delta : b - 1, 0 : b - 1)$ with an $a \times b$ Cauchy-like matrix $C$. As $a + b \leq \delta + b \leq \tau + 1 \leq q$, we are guaranteed the existence of such a Cauchy-like matrix $C$.

In Fig. 17–20, we illustrate the four steps involved in the construction of $H$ for parameters $\{a, b, \tau\} = \{3, 8, 14\}$.

*Theorem 19:* The code $\mathcal{C}$ over $\mathbb{F}_q$ having p-c matrix $H$ based on Construction B, when employed as the diagonally-embedded block code, will yield a rate-optimal streaming code $\mathcal{C}_{\text{str}}$.

*Proof:* Clearly, it suffices to show that $H$ meets all the four conditions; B1, B2, R1 and R2 described in Section III-G. The proof is deferred to Appendix I. □

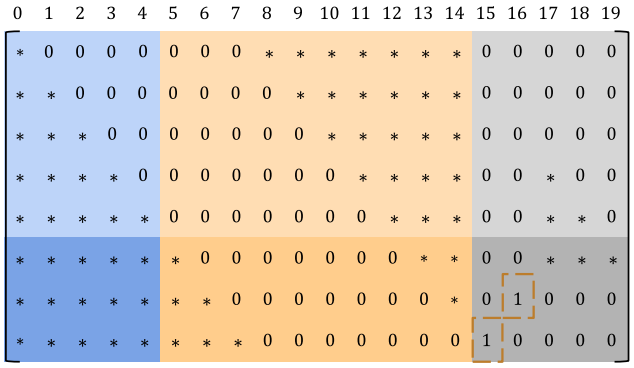



Fig. 19. $H$ after Step-c for parameters $\{a, b, \tau\} = \{3, 8, 14\}$. Here we replace some of the 0's with 1's.

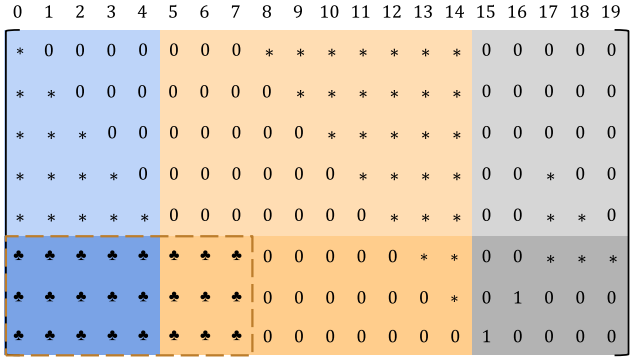



Fig. 20. $H$ after Step-d for parameters $\{a, b, \tau\} = \{3, 8, 14\}$. In Step-d, we set the demarcated section of $H$ to be a Cauchy-like matrix. Here ♣'s denote entries of the Cauchy-like matrix.

### B. Construction C: Interleaving MDS Codes

In this section, we present a second linear field-size construction, Construction C, obtained by simply interleaving MDS codes. The construction requires parameters $\{a, b, \tau\}$ to satisfy:

- $a \mid b \mid \tau - a + 1$ and $q \geq \frac{a}{b}(\tau + \delta + 1)$.

As always, $n = \tau + \delta + 1$, and thus we have $b \mid n$ as well. Let $\gamma \triangleq \frac{b}{a}$, $\beta \triangleq \frac{n}{b}$. In terms of $\gamma, \beta$ and $a$, one can express $\tau$ and $\delta$ as: $\tau = (\beta-1)\gamma a + a - 1$ and $\delta = (\gamma-1)a$, respectively. The construction is over a field $\mathbb{F}_q$, of size $q$ satisfying: $q \geq a\beta$. The description below of Construction C is, again, in terms of the p-c matrix $H$:

- Let $G_{\text{MDS}}$ denote the generator matrix of an $[a\beta, a]$ MDS code $\mathcal{C}_{\text{MDS}}$ over $\mathbb{F}_q$. Clearly, as $q \geq a\beta$, the required generator matrix $G_{\text{MDS}}$ of the MDS code can be found.
- For $0 \leq i \leq \beta - 1$, group the $a$ adjacent columns $[ia : (i+1)a - 1]$ of $G_{\text{MDS}}$ to form the matrix $G^{(i)}_{\text{MDS}}$. Thus we have $G_{\text{MDS}} = [G^{(0)}_{\text{MDS}}\ G^{(1)}_{\text{MDS}}\ \ldots\ G^{(\beta-1)}_{\text{MDS}}]$. Here, without loss of generality, one can assume that $G^{(\beta-1)}_{\text{MDS}} = I_a$.
- The p-c matrix $H$ of the code is then built up using the matrices $\left\{G^{(i)}_{\text{MDS}}\right\}$ as shown in Fig. 21.

*Example 20:* Let parameters $\{a, b, \tau\} = \{2, 6, 13\}$. Thus we have $\gamma = 3, \beta = 3, n = 18, \delta = 4$. Let $G_{\text{MDS}}$ be as follows:

$$G_{\text{MDS}} = \left[\begin{array}{cc|cc|cc} g_{0,0} & g_{0,1} & g_{0,2} & g_{0,3} & 1 & 0 \\ g_{1,0} & g_{1,1} & g_{1,2} & g_{1,3} & 0 & 1 \end{array}\right].$$

The p-c matrix $H$ associated to Construction C is as given in Fig. 22.

*Theorem 21:* The code $\mathcal{C}$ over $\mathbb{F}_q$ having p-c matrix $H$ based on Construction C, when employed as the diagonally-embedded block code, will yield a rate-optimal streaming code $\mathcal{C}_{\text{str}}$.

*Proof:* Clearly, as in the case of previous constructions, it suffices to show that $H$ satisfies all the four conditions; B1, B2, R1 and R2. As we take $G^{(\beta-1)}_{\text{MDS}}$ to be $I_a$, all the rows in the range $[0 : a+\ell-1]$ of $H$ have a run of $\delta-\ell$ zeros amongst the last $\delta - \ell$ columns $[\tau + \ell + 1 : \tau + \delta]$. Hence we choose $H^{(\ell)}$ as:

$$H^{(\ell)} = H(0 : a + \ell - 1, 0 : \ell + \tau).$$

- *Recovery from burst erasure of length at most $b$*:
  - Condition B1: Let $0 \leq \ell \leq (\gamma - 1)a - 1 \triangleq \delta - 1$. Partition the p-c matrix into $\gamma$ submatrices as follows:

$$H = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_{(\gamma-1)} \end{bmatrix},$$

    where $H_i \triangleq H(ia : ia + a - 1, :)$, $0 \leq i \leq \gamma - 1$ (see Fig. 23). Clearly, the $\beta a$ non-zero columns within an $H_i$ correspond to the $\beta a$ columns of $G_{\text{MDS}}$. Fix $\ell \in [0 : \delta - 1]$. Let $\ell = \mu a + \nu$, for some $\mu, \nu$ such that $0 \leq \mu \leq \gamma - 2$ and $0 \leq \nu \leq a - 1$. It can be verified that the matrix $H_\mu(:, 0 : \ell + \tau)$ consists of $a$ rows of $H^{(\ell)}$. We further note that any consecutive set of $b$ coordinates involve precisely $a$ non-zero columns of $H_i$ for any $i \in [0 : \gamma - 1]$. Moreover, these $a$ non-zero columns which correspond to each $H_i$ form an independent set as they are columns of an MDS matrix $G_{\text{MDS}}$. It follows that $H_\mu(:, \ell)$ (which is a non-zero column of $H_\mu$) is linearly independent of the set of $b - 1$ columns (only $a - 1$ of them are non-zero columns):

$$\{H_\mu(:, j) \mid \ell + 1 \leq j \leq \ell + b - 1\},$$

    which implies condition B1.
  - Condition B2: Let $\ell \in [\delta : \tau - a + 1]$. Consider any set of $b$ consecutive coordinates $[\ell : \ell + b - 1]$, which are erased. Here, again, we note that any consecutive set of $b$ coordinates, $[\ell : \ell + b - 1]$, involve precisely $a$ non-zero coordinates of any $H_i$, $0 \leq i \leq \gamma - 1$ and all these $a$ non-zero columns of each $H_i$ form an independent set. Hence it follows that

$$\left\{\underline{h}_j \mid \ell \leq j \leq \ell + b - 1\right\}$$

    form an independent set (condition B2).
- *Recovery from at most $a$ random erasures*:
  - Condition R1: Let $\ell \in [0 : \delta - 1]$ and recall the definition of $\mu, \nu$ such that: $\ell = a\mu + \nu$, where $0 \leq \mu \leq \gamma - 2$ and $0 \leq \nu \leq a - 1$. As seen in the condition B1 case, $H_\mu(:, 0 : \ell + \tau)$ consists of $a$ rows of $H^{(\ell)}$. Also, we have already seen that $H_\mu(:, \ell)$ is a non-zero

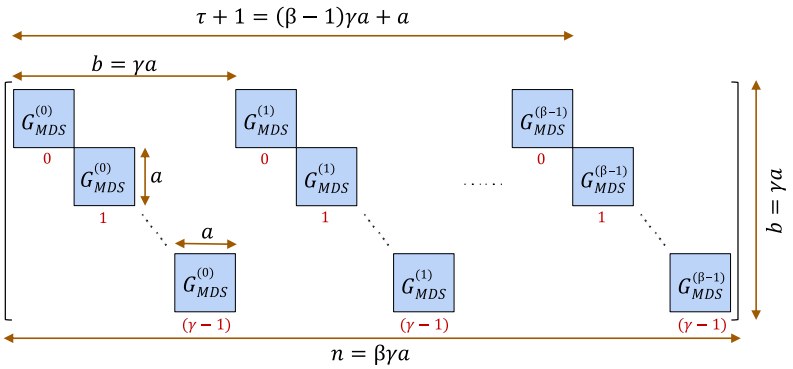



Fig. 21. The p-c matrix associated to Construction C. Here $G_{\text{MDS}} = [G^{(0)}_{\text{MDS}}\ G^{(1)}_{\text{MDS}}\ \ldots\ G^{(\beta-1)}_{\text{MDS}}]$ is the generator matrix of an $[a\beta, a]$ MDS code $\mathcal{C}_{\text{MDS}}$. From this, the interleaved MDS nature of the construction is apparent.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $g_{0,0}$ | $g_{0,1}$ | 0 | 0 | 0 | 0 | $g_{0,2}$ | $g_{0,3}$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| | $g_{1,0}$ | $g_{1,1}$ | 0 | 0 | 0 | 0 | $g_{1,2}$ | $g_{1,3}$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| | 0 | 0 | $g_{0,0}$ | $g_{0,1}$ | 0 | 0 | 0 | 0 | $g_{0,2}$ | $g_{0,3}$ | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| | 0 | 0 | $g_{1,0}$ | $g_{1,1}$ | 0 | 0 | 0 | 0 | $g_{1,2}$ | $g_{1,3}$ | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| | 0 | 0 | 0 | 0 | $g_{0,0}$ | $g_{0,1}$ | 0 | 0 | 0 | 0 | $g_{0,2}$ | $g_{0,3}$ | 0 | 0 | 0 | 0 | 1 | 0 |
| | 0 | 0 | 0 | 0 | $g_{1,0}$ | $g_{1,1}$ | 0 | 0 | 0 | 0 | $g_{1,2}$ | $g_{1,3}$ | 0 | 0 | 0 | 0 | 0 | 1 |

Fig. 22. $H$ corresponding to the Example 20. Here $\{a = 2, b = 6, \tau = 13\}$.

column and any $a$ non-zero columns of $H_\mu$ form an independent set. Clearly this implies condition R1.

– Condition R2: As any $a$ non-zero columns of $H_i$, $0 \leq i \leq \gamma - 1$ form an independent set, it follows that any $a$ columns of $H$ form an independent set. Hence condition R2 is satisfied.

□

## VI. Rate-Optimal Convolutional Codes for Given Column Distance and Column Span

In [19], the authors observe that the rate-optimal streaming codes (which are convolutional codes) they construct for the DC-SW channel, are also rate-optimal convolutional codes with respect to column span and column distance. Here we extend this observation to the constructions presented in this paper.

Consider a rate $\frac{k}{n}$ convolutional code with memory $m$. The relation between input vectors $\{\underline{s}(t)\}$ and $\{\underline{x}(t)\}$ is given by:

$$\underline{x}^T(t) = \sum_{i=0}^{m} \underline{s}^T(t-i) G_i^{\text{conv}}, \tag{11}$$

where $\underline{s}(t) \in \mathbb{F}_q^{k\times 1}$, $\underline{x}(t) \in \mathbb{F}_q^{n\times 1}$, $G_i^{\text{conv}} \in \mathbb{F}_q^{k\times n}$ and $\underline{s}(j) \triangleq \underline{0}$ for $j < 0$. We borrow the following definitions from [18], [19]:

Column distance,

$$d_\tau \triangleq \min\{\text{wt}(\underline{x}(0), \underline{x}(1), \ldots, \underline{x}(\tau)) : \underline{s}(0) \neq \underline{0}\},$$

Column span,

$$c_\tau \triangleq \min\{\text{span}(\underline{x}(0), \underline{x}(1), \ldots, \underline{x}(\tau)) : \underline{s}(0) \neq \underline{0}\},$$

where $\text{wt}(\underline{x}(0), \underline{x}(1) \ldots, \underline{x}(\tau))$ is the number of non-zero vectors in $\{\underline{x}(i)\}_{i=0}^{\tau}$ and $\text{span}(\underline{x}(0), \underline{x}(1) \ldots, \underline{x}(\tau)) = \max\{i \in [0:\tau] \mid \underline{x}(i) \neq \underline{0}\} - \min\{i \in [0:\tau] \mid \underline{x}(i) \neq \underline{0}\} + 1$. Clearly, $d_\tau \leq c_\tau \leq \tau + 1$.

It is shown in [18] that a convolutional code with column distance, $d_\tau$ and column span, $c_\tau$ is a streaming code which can correct, with a delay $\tau$, all the erasure patterns of the DC-SW channel having parameters $\{a = d_\tau - 1, b = c_\tau - 1, \tau, w = \tau + 1\}$. Thus, from (3), it follows that:

$$\frac{k}{n} \leq \frac{\tau - d_\tau + 2}{\tau - d_\tau + c_\tau + 1}. \tag{12}$$

Conversely, for a streaming code (which also is a convolutional code, as in the case of our constructions) which can recover with a delay $\tau$ from all the erasure patterns of the $\{a, b, \tau, w = \tau + 1\}$ DC-SW channel, it is shown in [18] that $d_\tau \geq a+1$ and $c_\tau \geq b+1$. Thus, for the rate-optimal streaming codes obtained via diagonally embedding Construction A, B or C, we have:

$$\begin{aligned} \frac{k}{n} &= \frac{\tau - a + 1}{\tau - a + 1 + b} \\ &\geq \frac{\tau - d_\tau + 2}{\tau - d_\tau + 2 + b} \\ &\geq \frac{\tau - d_\tau + 2}{\tau - d_\tau + c_\tau + 1} \end{aligned} \tag{13}$$

A convolutional code having column distance, $d_\tau$ and column span, $c_\tau$ is defined to be rate-optimal, if it satisfies (12) with equality. The following theorem is a direct consequence of Theorem 17 and inequalities (12), (13).

*Theorem 22:* For any $d_\tau, c_\tau$ and $\tau$ such that $d_\tau \leq c_\tau \leq \tau + 1$, there exists a rate-optimal convolutional code $\mathcal{C}_{\text{str}}$ with column distance $d_\tau$ and column span $c_\tau$, over $O(\tau^2)$ field-size.

## VII. Numerical Evaluation

In this section, we study the performance of two of our proposed diagonally-embedded constructions (A and C), the random convolutional code appearing in [19], the rate-optimal burst erasure correcting code of [17] and a diagonally-embedded MDS code. Constructions A, C and the random convolutional code have parameters $\{a, b, \tau\} = \{4, 8, 11\}$. The optimal burst erasure correcting code has parameters $\{b, \tau\} = \{11, 11\}$ and the MDS code has parameters $[n = 12, k = 6]$. Note that, with the chosen parameters, the code rate, $R = 0.5$

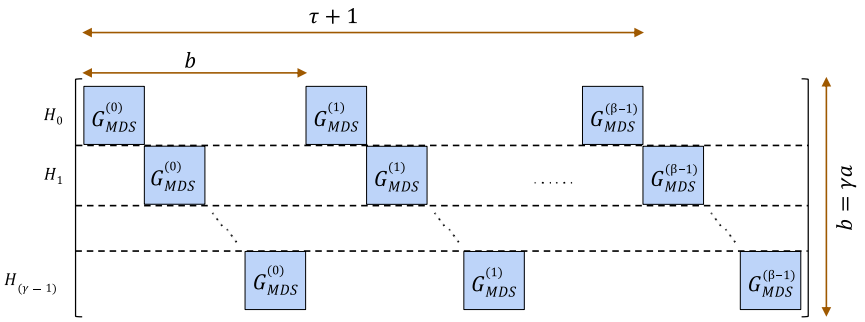



Fig. 23. Figure showing the partition of the p-c matrix shown in Fig. 21.

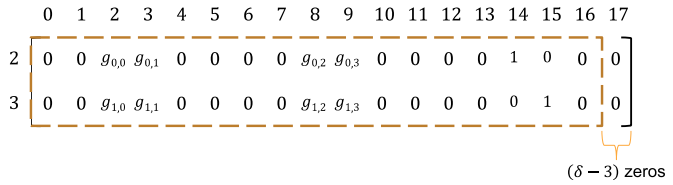



Fig. 24. Consider the Example 20. Let $\ell = 3$. The submatrix $H(2:3, 0:16)$ demarcated by dashed lines consists of $a = 2$ rows of $H^{(3)}$. Clearly column 3 of this submatrix is independent of the next $b - 1 = 5$ columns $[4:8]$. This proves that $H^{(3)}$ satisfies condition B1.

and delay parameter, $\tau = 11$ are the same for all the five code constructions. With regard to the field-size requirements, Construction A, random convolutional code and Construction C are over $\mathbb{F}_{2^8}$, $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^3}$, respectively. The MDS code is over $\mathbb{F}_{2^4}$ and as $R = 0.5$, the burst erasure correcting code turns out to be a repetition-code-based scheme needing just $\mathbb{F}_2$. The simulations are performed over Gilbert-Elliott and Fritchman channels. Each data point is a result of $10^8$ simulations. Note that the parameters $\{a, b, \tau\} = \{4, 8, 11\}$ that we have chosen, lie outside the permitted parameter ranges for Construction B.

### A. The Gilbert-Elliott Channel

The Gilbert-Elliott (GE) channel is a Markov model consisting of a good state and a bad state. The model is characterized by the tuple $(\alpha, \beta, \epsilon)$. Here $\alpha$ and $\beta$ are the transition probabilities from the good state to the bad state and vice versa, respectively. In the good state, a packet is lost with probability $\epsilon$, i.e., the channel behaves as a binary erasure channel with erasure probability $\epsilon$. All packets transmitted while the channel is in the bad state, are lost.

We perform simulations over GE channels with $\alpha = 5 \times 10^{-4}, \beta = 0.5$ and $\epsilon$ varying from 0.001 to 0.04. Fig. 25 illustrates the performance of all the five coding schemes. As expected, the burst-erasure correcting code performs the best for very low $\epsilon$ ($< 0.003$), when the channel behavior is dominated by burst erasures. On the other end of the spectrum, the MDS code starts outperforming all the other codes when $\epsilon$ is large enough and random erasures become the dominant factor. In the intermediate range, despite smaller field-size requirements, Construction A and Construction C perform better than the random convolutional code.

### B. The Fritchman Channel

The Fritchman Channel is a generalization of the two-state GE model. It is characterized by parameters $(\alpha, \beta, \epsilon, M)$. It consists of one good state $G$ and $M$ bad states, $E_1, \ldots, E_M$. In the good state, the channel behaves as a Binary Erasure Channel with erasure probability $\epsilon$. All the packets transmitted while the channel is in any bad state, are lost with probability 1. Transitions between these states are governed by the following 3 rules:

1) If the channel is in the good state $G$, it will remain in the same state with probability $1 - \alpha$, or transition to $E_1$ with probability $\alpha$, in the next time slot.
2) If the channel is in a state $E_l, l \in [M - 1]$, it will remain in the same state with probability $1 - \beta$, or transition to $E_{l+1}$ with probability $\beta$, in the next time slot.
3) If the channel is in state $E_M$, it will remain in the same state with probability $1 - \beta$, or transition to $G$ with probability $\beta$, in the next time slot.

Figure 26 shows the state transition probabilities for a Fritchman channel with $M = 4$. Note that the GE channel is a special case of Fritchman channel, where $M = 1$. We perform simulations over Fritchman channels with $\alpha = 10^{-4}, \beta = 0.75, M = 4$ and $\epsilon$ varying from 0.004 to 0.05. Fig. 27 illustrates the performance of these coding schemes, where the trends are similar to that of the GE channel.

*Remark 23:* As Construction A and the random convolutional code are not completely explicit, these simulations have been done on particular realizations of these constructions. The complete set of Matlab codes used for these simulations, are available at: `https://github.com/deeptanshu04/StreamingCodes`.

## APPENDIX I
## PROOF OF THEOREM 19 (CONSTRUCTION B)

For $\ell \in [0 : \delta - 1]$ and $R' \triangleq [0 : a - 1]$, let:

$$R'_\ell \triangleq \begin{cases} R' \cup [b - \ell : b - 1], & \text{if } \ell \in [0 : a - 1] \\ R' \cup [\delta + 1 : b - 1] \cup [a : \ell] & \text{otherwise.} \end{cases} \tag{14}$$

For every $i \in R'_\ell$, the $i$-th row $H(i, :)$ has a run of $\delta - \ell$ zeros across columns $[\ell + \tau + 1 : n - 1]$ (see Fig. 28 for an example). Hence $H(i, 0 : \ell + \tau)$ can be chosen to be a row of

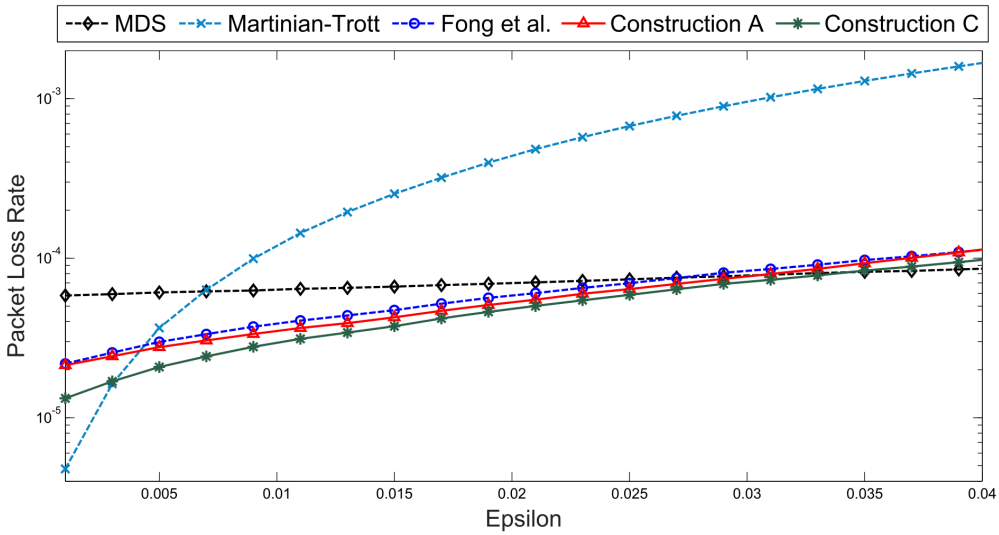



Fig. 25. We consider the GE channel with parameters $\alpha = 5 \times 10^{-4}, \beta = 0.5$ and $\epsilon$ varying from 0.001 to 0.04. The packet-loss probabilities of five coding schemes having rate, $R = 0.5$ and delay parameter, $\tau = 11$, are plotted; a diagonally-embedded $[12, 6]$ MDS code, Martinian-Trott code [17] for burst erasures having parameters $\{b = 11, \tau = 11\}$, Fong et al. code [19] for parameters $\{a, b, \tau\} = \{4, 8, 11\}$ and two codes from the present paper; Constructions A and C, again, for parameters $\{a, b, \tau\} = \{4, 8, 11\}$.

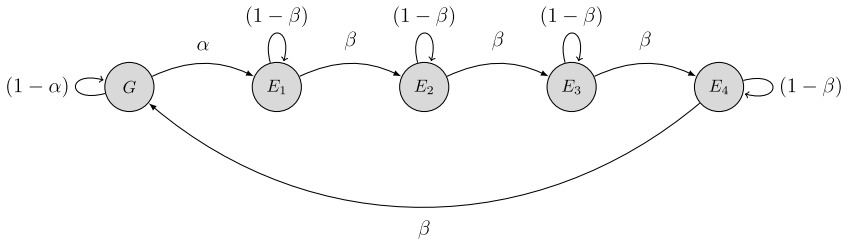



Fig. 26. State transition diagram for the Fritchman channel with $M = 4$ bad states.

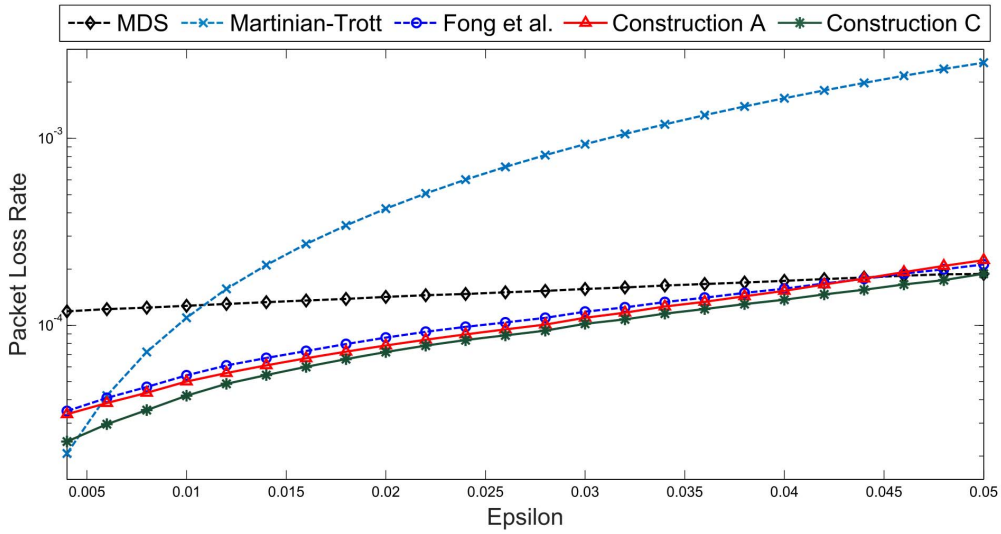



Fig. 27. Here we consider the Fritchman channel with 5 states, which is a generalization of the GE channel. The channel parameters are $\alpha = 10^{-4}$, $\beta = 0.75$, $M = 4$ and $\epsilon$ varying from 0.004 to 0.05. The five code constructions that are being compared are the same as that we use in the case of GE channel.

the shortened p-c matrix $H^{(\ell)}$. As argued earlier in the case of Construction A, Condition B2 requires the last $b$ columns of $H$ to be independent and thus it can be shown that $H^{(\ell)}$ has precisely $b - \delta + \ell$ rows. As $|R'_\ell| = b - \delta + \ell$, we choose $H^{(\ell)}$ as:

$$H^{(\ell)} = H(R'_\ell, 0 : \ell + \tau).$$

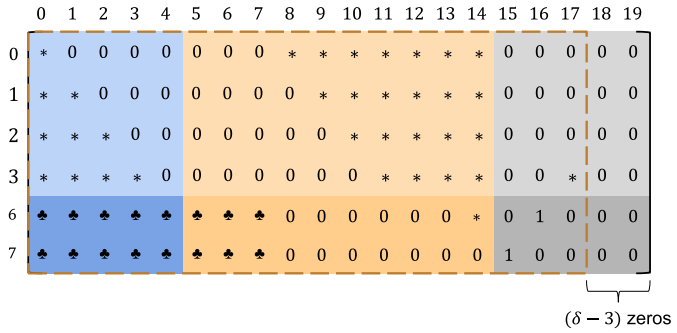



Fig. 28. Let $\ell = 3$. The submatrix $H(R'_\ell, :)$ for the p-c matrix $H$ given in Fig. 20. Here $R'_\ell = [0:2] \cup [6:7] \cup \{3\}$. The submatrix demarcated here in dashed lines is the shortened p-c matrix $H^{(3)}$.

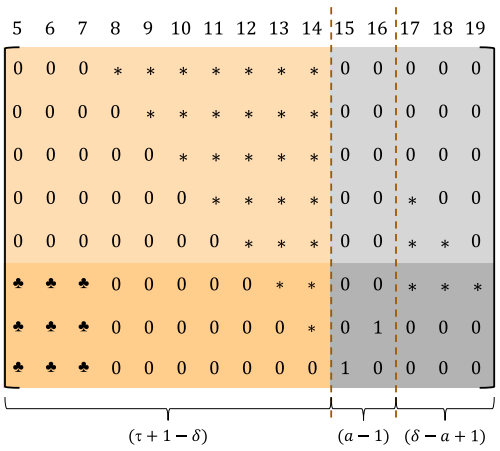



Fig. 29. Consider the p-c matrix given in Fig. 20. The $8 \times 15$ matrix $H(:, 5:19)$ is partitioned into three regions; $H(:, 5:14)$, $H(:, 15:16)$ and $H(:, 17:19)$.

- *Recovery from burst erasure of length at most b*:
  - Condition B1: For $\ell \in [0 : \delta - 1]$, the $\ell$-th row $\underline{h}_{\text{row},\ell}$ of the p-c matrix $H$ takes the form:

$$\underline{h}_{\text{row},\ell} = [\underbrace{\triangle \cdots \triangle}_{\ell \text{ symbols}} * \quad \underbrace{0 \cdots 0}_{(b-1) \text{ symbols}} \quad \triangle \cdots \triangle \quad \underbrace{0 \cdots 0}_{\text{last } (\delta - \ell) \text{ symbols}} \quad ],$$

    where $\triangle$'s indicate elements over $\mathbb{F}_q$ and $*$ indicates a non-zero element over $\mathbb{F}_q$. As $\ell \in R'_\ell$, $\underline{h}_{\text{row},\ell}(0, 0 : \ell + \tau)$ is a row of $H^{(\ell)}$. Similar to the corresponding case appearing in the proof of Theorem 17, using the structure of $\underline{h}_{\text{row},\ell}$, now one can argue that $H$ satisfies condition B1.
  - Condition B2: For $\delta \leq \ell \leq \tau - a + 1$, let $P_\ell$ denote the $b \times b$ square submatrix of $H$ corresponding to the column set $[\ell : \ell + b - 1]$ as in Construction A, i.e.,

$$P_\ell \triangleq H(:, [\ell : \ell + b - 1]).$$

    Condition B2 is equivalent to the scenario that all matrices $\{P_\ell\}$ are invertible. Consider the partition of $H(:, \delta : \delta + \tau)$ into three regions; $H(:, \delta : \tau)$, $H(:, 1 + \tau : a - 1 + \tau)$ and $H(:, a + \tau : \delta + \tau)$ (see Fig. 29). Based on where $P_\ell$, for a given $\ell$, is placed with respect to these three regions, we have five cases that need to be checked. Let $B_\ell \triangleq [\ell : \ell + b - 1]$.
    - (*Case I*: $B_\ell \subseteq [\delta : \tau]$ and $\ell \leq b$): In words, this is the scenario where $P_\ell$ is contained within $H(:, \delta : \tau)$ and $P_\ell$ contains the column $\underline{h}_b$. Here, it can be observed that $P_\ell$ takes the form:

$$P_\ell = \begin{bmatrix} P_{\ell,1} & P_{\ell,3} \\ P_{\ell,2} & [0] \end{bmatrix}, \tag{15}$$

      where $P_{\ell,3} \triangleq H(0 : \ell - 1, b : \ell + b - 1)$ and $P_{\ell,2} \triangleq H(\ell : b - 1, \ell : b - 1)$. Recall the ZB generator matrix $G_{\text{MDS}}$ used in Step-a of the construction. The $\ell \times \ell$ upper triangular matrix $P_{\ell,3}$ consists of $\ell$ non-zero columns chosen from $G_{\text{MDS}}(0 : \ell - 1, :)$ and hence is invertible (see Lemma 8). $P_{\ell,2}$ is invertible as it is a square submatrix of the Cauchy-like matrix $H(\delta : b - 1, 0 : b - 1)$. From the invertibility of $P_{\ell,2}$ and $P_{\ell,3}$, it follows that $P_\ell$ is invertible. In Fig. 30, we illustrate case I when $\ell = 5, 6$ for the p-c matrix shown in Fig. 20.
    - (*Case II*: $B_\ell \subseteq [\delta : \tau]$ and $\ell \geq b$): Note that this scenario arises only if $b + (b - 1) \leq \tau$. In this case, $P_\ell$ consists of $b$ columns of $G_{\text{MDS}}$ and hence is invertible. For the example p-c matrix in Fig. 20 that we have been using, we have $b = 8$ and $\tau = 14$, and hence case II will not

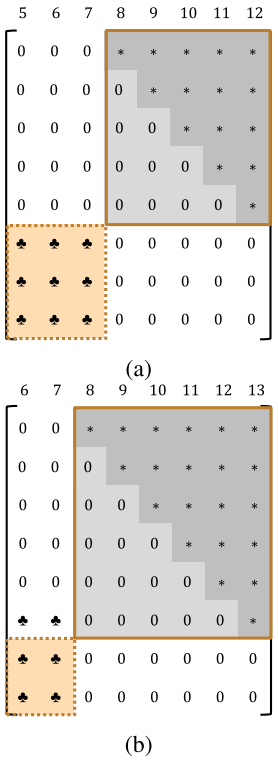



Fig. 30. Two $b \times b$ square submatrices of the p-c matrix in Fig. 20. The submatrices demarcated by dotted lines in (a) and (b) are invertible, as they are square submatrices of the Cauchy-like matrix $H(5:7, 0:7)$. The $5 \times 5$ submatrix shown in (a) using solid lines is invertible as it consists of 5 non-zero columns chosen from 5 adjacent rows of the ZB generator matrix $G_{\text{MDS}}$ used in Step-a. Similarly, the $6 \times 6$ matrix marked in (b) is invertible as it consists of 6 non-zero columns chosen from 6 adjacent rows of $G_{\text{MDS}}$.

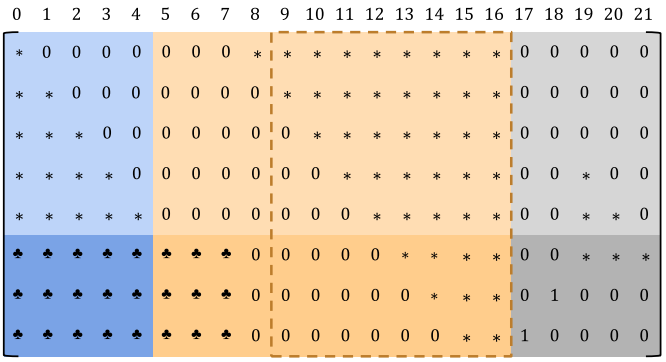



Fig. 31. An example p-c matrix $H$ for parameters $\{a, b, \tau\} = \{3, 8, 16\}$. The submatrix $P_9$ demarcated by dashed lines consists of 8 columns of the $8 \times 17$ MDS matrix $G_{\text{MDS}}$ introduced in Step-a. Hence $P_9$ is invertible.

be encountered. In order to specifically illustrate this case, we consider an example p-c matrix for parameters $\{a = 3, b = 8, \tau = 16\}$ in Fig. 31.

- (*Case III*: $B_\ell \not\subseteq [\delta : \tau]$, $B_\ell \subseteq [\delta : a - 1 + \tau]$ and $\ell \leq b$): This corresponds to the scenario where $P_\ell$ includes some columns from $H(:, 1 + \tau : a - 1 + \tau)$ but not any columns from $H(:, a + \tau : \delta + \tau)$ and also column $\underline{h}_b$ is present in the matrix $P_\ell$. Here $P_\ell$ takes the form shown in Figure 32a. By changing the ordering of columns from $\{\ell, (\ell+1), \ldots, b, \ldots, \tau, (1+\tau) \ldots, (\ell+b-1)\}$ to $\{(1+\tau), \ldots, (\ell+b-1), \ell, \ldots, b, \ldots, \tau\}$, as shown in Fig. 32b, we obtain a column-permuted $P_\ell$ of the form (15). Here $P_{\ell,2} \triangleq [H(\tau - b + 1 : b - 1, 1 + \tau : \ell + b - 1)\ H(\tau - b + 1 : b - 1, \ell : b - 1)]$, as can be seen from Fig. 32b, is an invertible matrix. Similar to case I, $P_{\ell,3} \triangleq H(0 : \tau - b, b : \tau)$ is an upper triangular matrix and is invertible as it consists of $\tau - b + 1$ non-zero columns chosen from $\tau - b + 1$ adjacent rows of the ZB generator matrix $G_{\text{MDS}}$. Hence $P_\ell$ is invertible.
- (*Case IV*: $B_\ell \not\subseteq [\delta : \tau]$, $B_\ell \subseteq [\delta : a - 1 + \tau]$ and $\ell \geq b$): For this case, $P_\ell$ takes the form:

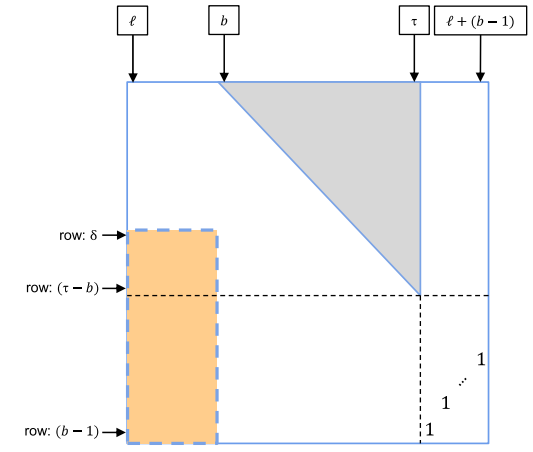
$$P_\ell \ = \ \begin{bmatrix} P_{\ell,1} & [0] \\ P_{\ell,2} & P_{\ell,4} \end{bmatrix},$$

where $P_{\ell,1} \triangleq H(0 : \tau - \ell, \ell : \tau)$ and $P_{\ell,4} \triangleq H(\tau - \ell + 1 : b - 1, 1 + \tau : \ell + b - 1)$ are invertible matrices as can be seen from Fig. 33 (see Fig. 34 for an example). Hence $P_\ell$ is invertible.

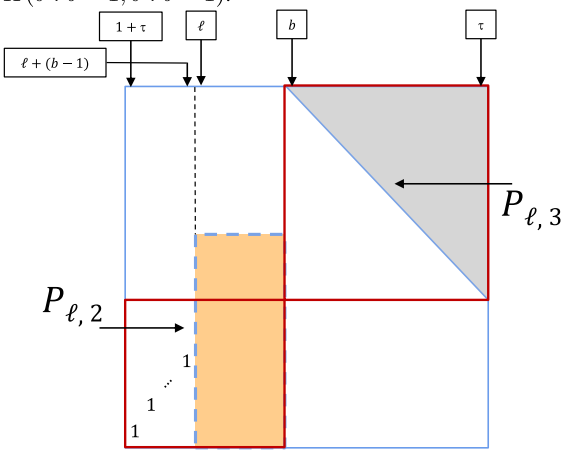
- (*Case V*: $B_\ell \not\subseteq [\delta : a - 1 + \tau]$): Clearly this corresponds to the scenario where $P_\ell$ includes some columns from $[a + \tau : \delta + \tau]$ and hence:

$$\ell + b - 1 \geq a + \tau. \tag{16}$$

Consider the ZB generator matrix $G_{\text{MDS}}$ of size $b \times (\tau+1)$ used in Step-a. In the following, with the help of three observations, we show that $b$ distinct columns of $G_{\text{MDS}}$ lie in the column space of $P_\ell$. As any $b$ columns of $G_{\text{MDS}}$ form an independent set, this would imply that $P_\ell$ is invertible.




(a) As $(\tau + 1) \geq (b + \delta)$, the matrix $H(\tau - b + 1 : b-1, \ell : b-1)$ is a submatrix of the Cauchy-like matrix $H(\delta : b - 1, \delta : b - 1)$.




(b) An illustration of the column-permuted $P_\ell$. Here $P_{\ell,2}$ is invertible, as its columns consist of standard basis vectors and columns of the Cauchy-like matrix $H(\tau - b + 1 : b - 1, \ell : b - 1)$.

Fig. 32. An illustration of $P_\ell$ for case III.

As $\ell$ ranges from $\delta$ to $\tau - a + 1$, using (16), one can infer that the columns $\{\underline{h}_i \mid 1 + \tau \leq i \leq a - 1 + \tau\}$ are part of $P_\ell$. As these $a - 1$ columns are standard basis vectors covering the last $a - 1$ rows, and the independent set of columns $\{G_{\text{MDS}}(:, i) \mid \delta + 1 \leq i \leq b - 1\}$ have non-zero entries only in the last $a - 1$ rows, we make the following observation:
(i) The space spanned by column vectors

$$\{\underline{h}_i \mid 1 + \tau \leq i \leq a - 1 + \tau\}$$

and

$$\{G_{\text{MDS}}(:, i) \mid \delta + 1 \leq i \leq b - 1\}$$

is the same (see Fig. 35).
Recall the constraint $\tau + 1 \geq b + \delta$ placed on the construction. Together with (16), we have: $\ell \geq (a + \tau) - (b - 1) = (\tau + 1) - \delta \geq b$. As columns $[b : \tau]$ of $H$ are unchanged after Step-a, we also have:

$$\underline{h}_j = G_{\text{MDS}}(:, j),$$

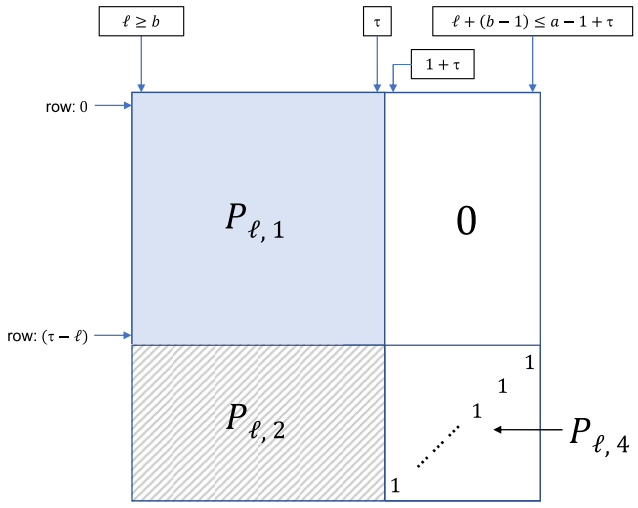



Fig. 33. In this figure, we illustrate the structure of $P_\ell$, for case IV. Here $P_{\ell,1}$ is a $(\tau-\ell+1)\times(\tau-\ell+1)$ submatrix consisting of $\tau-\ell+1$ non-zero columns from the first $\tau-\ell+1$ rows of the ZB generator matrix $G_{\text{MDS}}$. Hence $P_{\ell,1}$ is invertible. The matrix $P_{\ell,4}$ is clearly invertible and hence invertibility of $P_\ell$ follows.

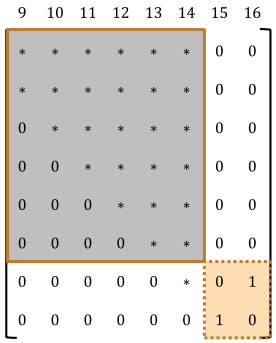



Fig. 34. Let $\ell = 9$. In the figure, we illustrate the matrix $P_\ell$ corresponding to the p-c matrix given in Fig. 20. The two submatrices demarcated by solid and dotted lines, are both invertible.

where $b \leq j \leq \tau$. Hence we make a second observation:

(ii) As $\ell \geq b$, the columns $\{\underline{h}_i \mid \ell \leq i \leq \tau\}$ of $P_\ell$ are columns of the MDS matrix $G_{\text{MDS}}$, where $\underline{h}_i = G_{\text{MDS}}(:, i)$.

Now consider the remaining columns $\{\underline{h}_i \mid a+\tau \leq i \leq \ell+b-1\}$ of $P_\ell$. From Step-b, it follows that columns $G_{\text{MDS}}(:, i-\tau)$ and $\underline{h}_i$ are identical except at the last $a-1$ rows, where $a+\tau \leq i \leq \ell+b-1$. As the standard basis corresponding to these last $a-1$ rows are part of the columns of $P_\ell$, we make a third observation as follows:

(iii) The columns $\{G_{\text{MDS}}(:, j) \mid j \in [a : \ell+b-1-\tau]\}$ lie in the span of $\{\underline{h}_i \mid 1+\tau \leq i \leq \ell+b-1\}$.

Together observations (i), (ii) and (iii) imply that columns $[a : \ell+b-1-\tau] \cup [\delta+1 : b-1] \cup [\ell : \tau]$ of $G_{\text{MDS}}$ lie in the column space of $P_\ell$. As $(\ell+b-1)-\tau \leq (n-1)-\tau = (\tau+\delta)-\tau = \delta$, clearly these are $b$ distinct columns of the $b\times(\tau+1)$ MDS matrix $G_{\text{MDS}}$. This implies that $P_\ell$ has rank $b$ and hence is invertible.

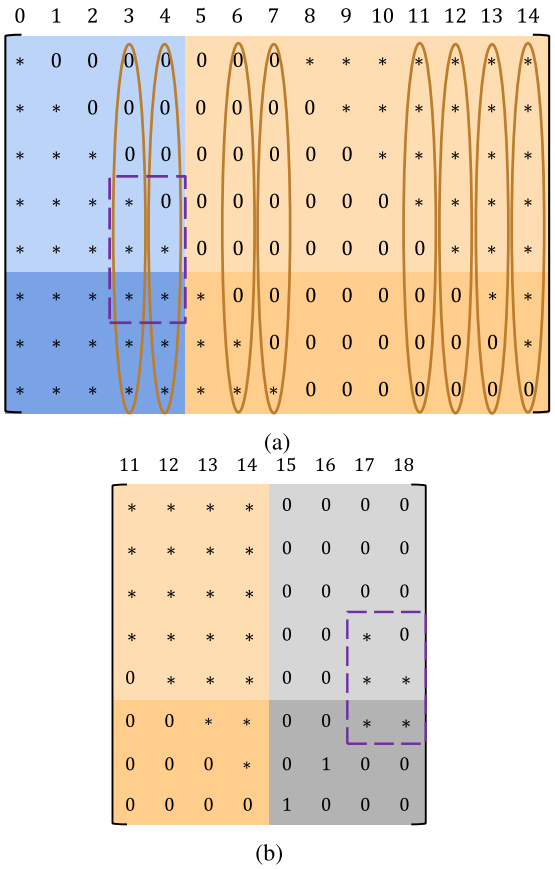



Fig. 35. An illustration of the three observations that we make in the proof of case V. (a) The ZB generator matrix $G_{\text{MDS}}$ corresponding to the p-c matrix shown in Fig. 20. (b) The submatrix $P_{11} \triangleq H(:, 11:18)$. We make the following three observations; (i) The column space of $G_{\text{MDS}}(:, [6:7])$ and $H(:, [15:16])$ is the same. (ii) $G_{\text{MDS}}(:, i) = \underline{h}_i$ for $11 \leq i \leq 14$. (iii) Columns $G_{\text{MDS}}(:, 3)$ and $G_{\text{MDS}}(:, 4)$ lie in the column space of $H(:, [15:18])$. Hence columns $[3:4] \cup [6:7] \cup [11:14]$ of $G_{\text{MDS}}$ lie in the column space of $P_{11}$. This implies that $P_{11}$ is invertible.

- *Recovery from at most $a$ random erasures*:
  - Condition R1: We divide the proof of condition R1 into two cases. Recall the definition of $R'_\ell$ in (14).
    - (*Case I*: $\ell \in [0 : a-1]$): Consider the rows $R' \triangleq [0 : a-1] \subseteq R'_\ell$ of $H$. Let $U_\ell \triangleq H(R', 0 : \ell+\tau)$, which consists of $a$ rows of $H^{(\ell)}$. It can be verified that the columns $\mathcal{I} \triangleq [a : b-1] \cup [1+\tau : \ell+\tau]$ of $U_\ell$ are zero columns. If we exclude the zero-columns $[1+\tau : \ell+\tau]$ of $U_\ell$, the submatrix $U_\ell(:, 0:\tau)$ is formed by $a$ consecutive rows of a ZB generator matrix corresponding to a $[\tau+1, b]$ MDS code. Hence applying Lemma 8, we have that any set of at most $a$ non-zero columns of $U_\ell$ forms an independent set. As $H(R', \ell) \triangleq U_\ell(:, \ell)$ is a non-zero column of $U_\ell$, it follows that condition R1 is satisfied for $\ell \in [0 : a-1]$. In Fig. 36, we consider the example of $\ell = 2$ with respect to the p-c matrix given in Fig. 20. Note that this proof idea does not extend to the case $\ell \in [a : \delta-1]$, as $U_\ell(:, \ell)$ is a zero-column for this range of $\ell$.
    - (*Case II*: $\ell \in [a : \delta-1]$): Consider the set of rows $S_\ell \triangleq R' \cup \{\ell\} \cup [\delta+1 : b-1] \subseteq R'_\ell$. Partition the

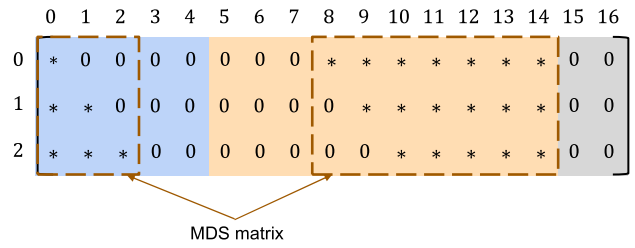



Fig. 36. Here $\ell = 2, R' = [0:2]$. In the figure, the submatrix $U_\ell \triangleq H(R', 0:16)$ is shown, which corresponds to the p-c matrix given in Fig. 20. The columns of $U_\ell$ indexed by $\mathcal{I} \triangleq [3:7] \cup [15:16]$ are zero columns. Any collection of at most 3 non-zero columns forms an independent set. In other words, $U_\ell(:, [0:2] \cup [8:14])$ is an MDS matrix. As a result, column 2 cannot lie in the span of any set of at most 2 other columns.

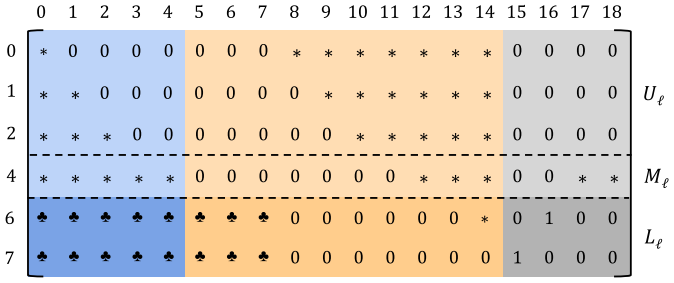



Fig. 37. Here $\ell = 4$. In the figure, the submatrix $H(S_\ell, 0:\ell+\tau)$ which corresponds to the p-c matrix shown in Fig. 20, is partitioned into $U_\ell$, $M_\ell$ and $L_\ell$.

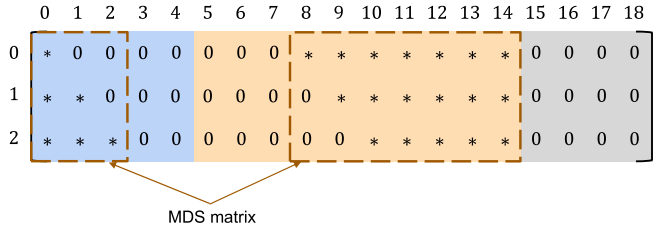



Fig. 38. Here $\ell = 4, \mathcal{I} = [3:7] \cup [15:18]$. In the figure, we illustrate the submatrix $U_4$ which corresponds to Fig. 37. Any collection of at most 3 non-zero columns forms an independent set. Thus, in order to satisfy (18), $A_4 \subseteq [4:18]$ cannot include any of the coordinates $[0:18] \setminus \mathcal{I}$. Hence $A_4 \subseteq [4:7] \cup [15:18]$.

matrix $H(S_\ell, 0:\ell+\tau)$ in the following form:

$$\begin{bmatrix} U_\ell \\ M_\ell \\ L_\ell \end{bmatrix},$$

where $U_\ell$ is as defined in case I, $M_\ell \triangleq H(\ell, 0:\ell+\tau)$ and $L_\ell \triangleq H(\delta+1:b-1, 0:\ell+\tau)$ (see Fig. 37 for an example case of $\ell = 4$). Note that the matrix $H(S_\ell, 0:\ell+\tau)$ consists of $2a$ rows of $H^{(\ell)}$ and that $M_\ell = [M_{\ell,0} \;\; M_{\ell,1} \;\; \cdots \;\; M_{\ell,\ell+\tau}]$ is a row vector.

In Fig. 38, we illustrate this for $\ell = 4$, with respect to the p-c matrix given in Fig. 20.

Now, contrary to the condition R1, assume there exists a set $A_\ell \subseteq [\ell : \ell+\tau]$ with $|A_\ell| \leq a$ and

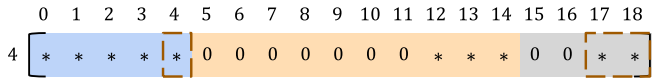


Fig. 39. Here $\ell = 4$. In the figure, we illustrate the submatrix $M_4$ which corresponds to Fig. 37. From (21), we have $A_4 \subseteq [4:7] \cup [15:18]$. Here we have identified the non-zero entries among the coordinates $[4:7] \cup [15:18]$ to be $M_{4,4}, M_{4,17}$ and $M_{4,18}$. Hence in order to satisfy (19), we require at least one of the coordinates from $[17:18]$ to be in $A_4$.

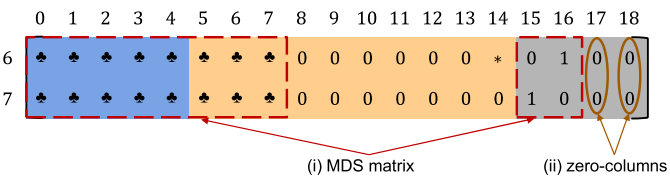



Fig. 40. Here $\ell = 4$. In the figure, we illustrate the submatrix $L_4$ which corresponds to Fig. 37. From (21), we have $A_4 \subseteq [4:7] \cup [15:18]$ and from (19), we require at least one of the coordinates from $[17:18]$ to be in $A_4$. However as $L_4(:, 17)$ and $L_4(:, 18)$ are zero-columns, and $L_4(:, [0:7] \cup [15:16])$ is an MDS matrix, (20) would result in a dependency across at most 2 columns of this MDS matrix, which is a contradiction.

$\ell \in A_\ell$ such that:

$$\underline{h}_\ell^{(\ell)} = \sum_{i \in A_\ell \setminus \{\ell\}} a_i \underline{h}_i^{(\ell)}, \tag{17}$$

where $\{a_i\}$ are all non-zero. Equation (17) implies the following:

$$U_\ell(:, \ell) = \sum_{i \in A_\ell \setminus \{\ell\}} a_i U_\ell(:, i), \tag{18}$$

$$M_{\ell,\ell} = \sum_{i \in A_\ell \setminus \{\ell\}} a_i M_{\ell,i}, \tag{19}$$

and

$$L_\ell(:, \ell) = \sum_{i \in A_\ell \setminus \{\ell\}} a_i L_\ell(:, i). \tag{20}$$

As seen in case I, we have a set of zero columns for $U_\ell$ at the columns indexed by $\mathcal{I} = [a : b-1] \cup [1+\tau : \ell+\tau]$ and any collection of at most $a$ non-zero columns of $U_\ell$ forms an independent set. Thus in order for (18) to hold, $A_\ell$ cannot include any of the non-zero coordinates of $U_\ell$. Thus we have:

$$A_\ell \subseteq [\ell : b-1] \cup [1+\tau : \ell+\tau]. \tag{21}$$

Now consider (19). As $M_{\ell,\ell} \triangleq H(\ell, \ell) \neq 0$, for (19) to hold, we need at least a single coordinate $i \in A_\ell \setminus \{\ell\}$ such that $M_{\ell,i} \triangleq H(\ell, i) \neq 0$. Because of the constraint (21), it can be inferred from the p-c matrix structure that, the only way this can be true is by including at least one coordinate from $[a+\tau : \ell+\tau]$ in $A_\ell$ (for instance, see Fig. 39).

We will turn our attention to (20) now. We make the following observations on $L_\ell$.

(i) $L_\ell(:, [0 : b-1] \cup [1+\tau : a-1+\tau])$ is an $(a-1) \times (b+a-1)$ MDS matrix. Also, as

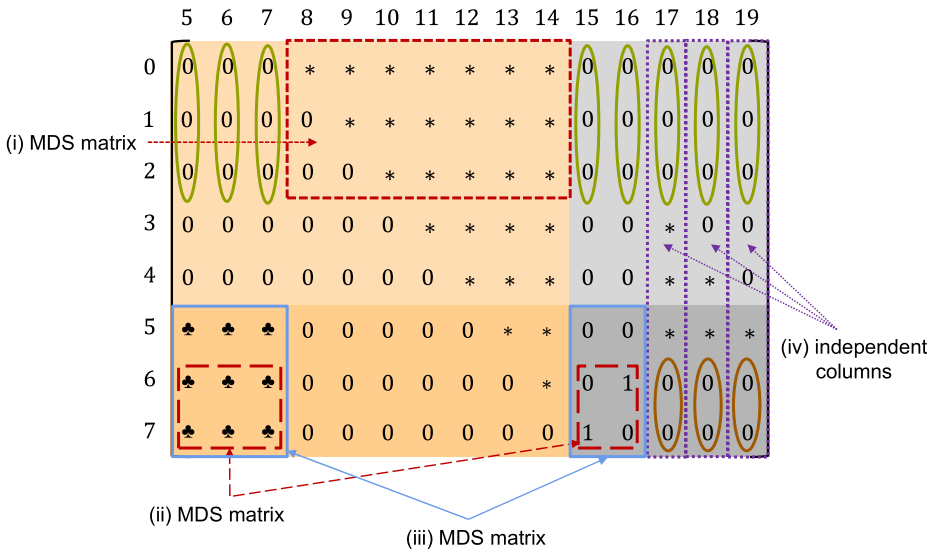



Fig. 41. In this figure, we identify observations (i)-(iv) with respect to the submatrix $H(:, 5:19)$, which corresponds to the p-c matrix in Fig. 37.

$\ell \in [a : \delta - 1]$ and $\delta < b$, $L_\ell(:, \ell)$ is a column of this MDS matrix.

(ii) The columns of $L_\ell$ indexed by $[a + \tau : \ell + \tau]$ are all zero-columns.

In Fig. 40, we identify these observations for the case $\ell = 4$ (with respect to the p-c matrix given in Fig. 20).

Now consider the set $[\ell : b - 1] \cup [1 + \tau : \ell + \tau]$ appearing in (21). Consider the partition of this set into $A_{\ell,1} \triangleq [\ell : b - 1] \cup [1 + \tau : a - 1 + \tau]$ and $A_{\ell,2} \triangleq [a + \tau : \ell + \tau]$. By observation (i), all the columns of $L_\ell$ chosen from $A_{\ell,1}$, are columns of the MDS matrix described in observation (i). From observation (i), we also have $L_\ell(:, \ell)$ is a column of this MDS matrix. Similarly, using observation (ii), we have that all columns of $L_\ell$ chosen from $A_{\ell,2}$, are zero-columns. As noted earlier, (19) requires at least one coordinate from $A_{\ell,2}$ to be present in $A_\ell$. If we include a coordinate from $A_{\ell,2}$ (zero-column of $L_\ell$) in $A_\ell$, (20) will result in a dependency involving at most $a-1$ columns of the MDS matrix $L_\ell(:, [0 : b-1] \cup [\tau+1 : \tau+a-1])$. Clearly, this is a contradiction (see 40, for an example). Thus our assumption on the existence of $A_\ell$ is not valid, and hence $H$ satisfies condition R1 for $\ell \in [a : \delta - 1]$.

– Condition R2: Assume there exists a set $A_\ell \subseteq [\delta : n - 1]$ with $|A_\ell| \leq a$ such that:

$$\sum_{i \in A_\ell} a_i \underline{h}_i = 0, \tag{22}$$

where $\{a_i\}$ are all non-zero. Let $R' \triangleq [0 : a-1]$, $S \triangleq [\delta : b-1]$, $S' \triangleq [\delta+1 : b-1]$. We make the following observations:

(i) Consider the submatrix $H(R', \delta : \tau+\delta)$. All except the columns given by $\{H(R', j) \mid j \in [b : \tau]\}$ are zero columns. Also, $H(R', b : \tau)$ is an $a \times (\tau - b + 1)$ MDS matrix.

(ii) $H(S', [\delta : \tau+a-1] \setminus [b : \tau])$ is a $(a-1) \times (2a-1)$ MDS matrix and all the columns $\{H(S', i) \mid i \in [\tau + a : \tau + \delta]\}$ are zero-columns.

(iii) $H(S, [\delta : \tau + a - 1] \setminus [b : \tau])$ is a $a \times (2a - 1)$ MDS matrix.

(iv) The collection of columns $\{\underline{h}_j \mid j \in [\tau + a : \tau + \delta]\}$ forms a linearly independent set as required by condition B2, since it is a subset of the larger linearly independent set of $b$ columns, $\{\underline{h}_j \mid j \in [\tau - a + 1 : \tau + \delta]\}$.

We illustrate these observations with respect to an example in Fig. 41. From (i), we have that none of the columns from $[b : \tau]$ can be a part of $A_\ell$. Thus we have $A_\ell \subseteq [\delta : b - 1] \cup [\tau + 1 : \tau + \delta]$. Using observation (ii), we claim that $A_\ell$ cannot simultaneously contain coordinates from both $[\delta : b-1] \cup [\tau+1 : \tau+a-1]$ and $[\tau + a : \tau + \delta]$. This is so because if not, we will have a linear dependency amongst at most $a-1$ columns of the MDS matrix $H(S', [\delta : \tau + a - 1] \setminus [b : \tau])$, which clearly is not possible. Thus we have either:

$$A_\ell \subseteq [\delta : \tau + a - 1] \setminus [b : \tau] \tag{23}$$

or

$$A_\ell \subseteq [\tau + a : \tau + \delta]. \tag{24}$$

However observations (iii) and (iv), respectively, imply that (23) and (24) are not possible. This contradicts our assumption on the existence of $A_\ell$ and property R2 follows.

## REFERENCES

[1] M. N. Krishnan, D. Shukla, and P. V. Kumar, "A quadratic field-size rate-optimal streaming code for channels with burst and random erasures," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2019, pp. 852–856.

[2] ITU-R. (2015). IMT Vision—Framework and overall objectives of the future development of IMT for 2020 and beyond. [Online]. Available: http://www.itu.int/dms_pubrec/itu-r/rec/m/r-rec-m.2083-0-201509-i!!pdf-e.pdf

[3] Cisco, "Cisco visual networking index: Forecast and methodology, 2016–2021," White Paper, 2017.
[4] T. Anker, R. Cohen, and D. Dolev, "Transport layer end-to-end error correcting," School Comput. Sci. Eng., Hebrew Univ., Jerusalem, Israel, Tech. Rep., 2004.
[5] O. Tickoo, V. Subramanian, S. Kalyanaraman, and K. K. Ramakrishnan, "LT-TCP: End-to-end framework to improve TCP performance over networks with lossy channels," in *Proc. Int. Workshop Qual. Service*, 2005, pp. 81–93.
[6] C. Yu, Y. Xu, B. Liu, and Y. Liu, "'Can you SEE me now?' A measurement study of mobile video calls," in *Proc. INFOCOM*, Apr./May 2014, pp. 1456–1464.
[7] E. Martinian and C.-E.-W. Sundberg, "Burst erasure correction codes with low decoding delay," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2494–2502, Oct. 2004.
[8] A. Badr, A. Khisti, W.-T. Tan, and J. Apostolopoulos, "Perfecting protection for interactive multimedia: A survey of forward error correction for low-delay interactive applications," *IEEE Signal Process. Mag.*, vol. 34, no. 2, pp. 95–113, Mar. 2017.
[9] G. Forney, "Burst-correcting codes for the classic bursty channel," *IEEE Trans. Commun. Technol.*, vol. 19, no. 5, pp. 772–781, Oct. 1971.
[10] J. Massey, "Implementation of burst-correcting convolutional codes," *IEEE Trans. Inf. Theory*, vol. 11, no. 3, pp. 416–422, Jul. 1965.
[11] S. Lin and D. J. Costello, *Error Control Coding: Fundamentals and Applications*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1983.
[12] N. Abramson, "A class of systematic codes for non-independent errors," *IEEE Trans. Inf. Theory*, vol. 5, no. 4, pp. 150–157, Dec. 1959.
[13] P. Fire, "A class of multiple-error-correcting binary codes for non-independent errors," Sylvania Reconnaissance Syst. Lab., Mountain View, CA, USA, Sylvania Rep. RSL-E-2, 1959.
[14] P. G. Farrell and S. J. Hopkins, "Burst-error-correcting array codes," *Radio Electron. Eng.*, vol. 52, no. 4, pp. 188–192, 1982.
[15] S. Johnson, "Burst erasure correcting LDPC codes," *IEEE Trans. Commun.*, vol. 57, no. 3, pp. 641–652, Mar. 2009.
[16] A. Nafaa, T. Taleb, and L. Murphy, "Forward error correction strategies for media streaming over wireless networks," *IEEE Commun. Mag.*, vol. 46, no. 1, pp. 72–79, Jan. 2008.
[17] E. Martinian and M. Trott, "Delay-optimal burst erasure code construction," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 1006–1010.
[18] A. Badr, P. Patil, A. Khisti, W.-T. Tan, and J. Apostolopoulos, "Layered constructions for low-delay streaming codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 111–141, Jan. 2017.
[19] S. L. Fong, A. Khisti, B. Li, W.-T. Tan, X. Zhu, and J. Apostolopoulos, "Optimal streaming codes for channels with burst and arbitrary erasures," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4274–4292, Jul. 2019.
[20] M. N. Krishnan and P. V. Kumar, "Rate-optimal streaming codes for channels with burst and isolated erasures," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 1809–1813.
[21] R. Mahmood, A. Badr, and A. Khisti, "Streaming codes for multiplicative-matrix channels with burst rank loss," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5296–5311, Jul. 2018.
[22] A. Badr, D. Lui, A. Khisti, W.-T. Tan, X. Zhu, and J. Apostolopoulos, "Multiplexed coding for multiple streams with different decoding delays," *IEEE Trans. Inf. Theory*, vol. 64, no. 6, pp. 4365–4378, Jun. 2018.
[23] M. Rudow and K. V. Rashmi, "Streaming codes for variable-size arrivals," in *Proc. 56th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2018, pp. 733–740.
[24] D. Leong and T. Ho, "Erasure coding for real-time streaming," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2012, pp. 289–293.
[25] D. Leong, A. Qureshi, and T. Ho, "On coding for real-time streaming under packet erasures," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2013, pp. 1012–1016.
[26] O. F. Tekin, T. Ho, H. Yao, and S. Jaggi, "On erasure correction coding for streaming," in *Proc. Inf. Theory Appl. Workshop*, Feb. 2012, pp. 221–226.
[27] N. Adler and Y. Cassuto, "Burst-erasure correcting codes with optimal average delay," *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 2848–2865, May 2017.
[28] D. Malak, M. Medard, and E. M. Yeh, "Tiny codes for guaranteeable delay," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 809–825, Apr. 2019.
[29] A. Badr, A. Khisti, W.-T. Tan, and J. Apostolopoulos, "Streaming codes for channels with burst and isolated erasures," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2850–2858.
[30] N. Alon, "Combinatorial nullstellensatz," *Combinatorics, Probab. Comput.*, vol. 8, nos. 1–2, pp. 7–29, 1999.
[31] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE/ACM Trans. Netw.*, vol. 11, no. 5, pp. 782–795, Oct. 2003.
[32] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2003.
[33] A. Badr, A. Khisti, W.-T. Tan, and J. Apostolopoulos, "Robust streaming erasure codes using MDS constituent codes," in *Proc. 13th Can. Workshop Inf. Theory*, Jun. 2013, pp. 158–163.
[34] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1981.

**M. Nikhil Krishnan** received the B.Tech. degree in electronics and communication engineering from the Amrita School of Engineering, Amritapuri Campus, Kerala, in 2011, and the M.E. degree in telecommunications and the Ph.D. degree in electrical communication engineering from the Indian Institute of Science (IISc), Bengaluru, in 2013 and 2019, respectively. He is currently a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto. His current research interests include coding for low-latency communication, coding for distributed storage, and coded computation. He was a co-recipient of the Qualcomm Innovation Fellowship India, in 2019. He is a coauthor of an article selected as a finalist for the IEEE Jack Keil Wolf ISIT Student Paper Award, in 2019.

**Deeptanshu Shukla** received the B.Tech. degree in electrical engineering from the Indian Institute of Technology, Delhi, and the M.Tech. degree in electrical communication engineering from the Indian Institute of Science, Bengaluru. He is currently working with Qualcomm India Pvt., Ltd., as an Engineer. His research interests include coding theory and information-theoretic secure computation.

**P. Vijay Kumar** (Fellow, IEEE) received the B.Tech. degree from IIT Kharagpur, the M.Tech. degree from IIT Kanpur, and the Ph.D. degree from USC in 1983, all in electrical engineering. From 1983 to 2003, he was on the faculty of the EE-Systems Department, USC. Since 2003, he has been on the faculty of IISc Bengaluru. He currently holds the position of a Visiting Professor at USC. His current research interests include codes for distributed storage, codes for low-latency communication, and coded computation. He is a Fellow of the INAE, IAS, and INSA academies. He was a recipient of the 1995 IEEE Information Theory Society Prize-Paper Award and the IEEE Data Storage Best Paper Award of 2011/2012. A pseudorandom sequence family designed in a 1996 paper coauthored by him now forms the short scrambling code of the 3G WCDMA cellular standard. He received the USC School of Engineering Senior Research Award in 1994, the Rustum Choksi Award for Excellence in Research in Engineering in 2013 at IISc, and the period of 2017 to 2022 the J. C. Bose National Fellowship awarded by the Department of Science and Technology. He was on the Board of Governors of the IEEE Information Theory (IT) Society from 2013 to 2015, was a Plenary Speaker at ISIT 2014, the TPC Co-Chair of ISIT 2015. Since 2019, he has been the Chair of the IT Society Conference Committee.