Explicit Rate-Optimal Streaming Codes With Smaller Field Size

Myna Vajha, Vinayak Ramkumar, M. Nikhil Krishnan, Member, IEEE, and P. Vijay Kumar, Life Fellow, IEEE

Abstract—Streaming codes are a class of packet-level erasure codes that ensure packet recovery over a sliding window channel which allows either a burst erasure of size $b$ or a random erasures within any window of size $(\tau + 1)$ time units, under a strict decoding-delay constraint $\tau$. The field size over which streaming codes are constructed is an important factor in determining the implementation complexity. The best-known explicit rate-optimal streaming code, which covers all $\{a, b, \tau\}$ parameter choices, requires a field size of $q^b$, where $q \geq \tau + b - a$ is a prime power. In this work, we present an explicit rate-optimal streaming code over a field of size $q^2$, for prime power $q \geq \tau$. This is the smallest known field size for an explicit rate-optimal construction that takes into account all $\{a, b, \tau\}$ parameters. We achieve this by modifying the non-explicit code construction due to Krishnan et al., without changing the field size. We also present a generalization of our construction, which results in streaming codes over further smaller fields by trading off code rate.

Index Terms—Low-latency communication, streaming codes, packet-level FEC, random and burst erasures.

I. INTRODUCTION

E NABLING low-latency reliable communication for applications such as telesurgery, industrial automation, augmented reality and vehicular communication is a key target of advanced 5G communications systems. For instance, telesurgery camera flow requires a packet-loss rate less than $10^{-3}$ and an end-to-end latency below 150 ms [1]. One approach to combat the packet drops that are an inevitable part of any communication network is to employ feedback-based methods such as Automatic Repeat Request (ARQ). But such feedback-based schemes incur a three-way propagation delay (one-way delay from sender to receiver + one round-trip delay owing to feedback and re-transmission), making it challenging to meet low-latency requirements [2]. Using Forward Error Correction (FEC), which adds redundancy during transmissions, is an alternate approach. A naive FEC strategy involves blindly re-transmitting packets a predetermined number of times. This strategy, however, wastes resources and reduces throughput significantly. Although there are efficient FEC techniques such as Low-Density Parity Check (LDPC) codes [3] and digital fountain codes [4], [5], they often operate over large block lengths and are therefore better suited for non-interactive applications with less-stringent delay constraints [2].

Martinian and Sundberg [6] introduced the framework of streaming codes to construct packet-level erasure codes that achieve reliable, low-latency communication. The coding theoretic framework due to Martinian and Sundberg may be outlined as follows (a more formal description is provided later in Sec. II-A). The sender receives a sequence of message packets from some data source (one may find it convenient to imagine the on-the-fly arrival of an infinite “stream” of message packets at the sender). At time $t$, $t \in \{0, 1, \ldots\}$, the sender has access to the message packet $u(t) \in \mathbb{F}_q^k$. The sender adds redundancy by appending $n - k$ parity symbols to $u(t)$ to create a coded packet $\hat{u}(t) \in \mathbb{F}_q^m$, which it then transmits at time $t$. Naturally, the ratio $\frac{k}{n}$ is referred to as the rate of the code. The key characteristic that sets streaming codes apart from other packet-level erasure codes is the existence of a delay-constrained decoder (at the receiver), which is required to output an estimate $\hat{u}(t)$ of $u(t)$ by time $(t + \tau)$. Here, $\tau \geq 0$ signifies a decoding-delay constraint and is referred to as the delay parameter.

In communication networks, in addition to random packet losses, burst erasures also occur for a variety of reasons including poor quality wireless links and queuing issues [7]. Convolutional-code-based approaches, such as m-MDS codes [8], [9], are excellent in handling symbol-level random erasures. However, the use of conventional interleaving techniques to handle burst erasures in these symbol-level coding schemes results in extra delay. This may not be suitable for latency-sensitive applications. In contrast, the approach in [6], which is also followed in the current paper, is to design coding schemes directly for the packet erasure channel, with an explicit decoding-delay constraint as a design parameter.

In [6] and [10], streaming codes that allow perfect (delay-constrained) recovery of message packets (i.e., $\hat{u}(t) = u(t)$ for all $t$), in the presence of a burst erasure of size $b$, are...
provided. In [11], Badr et al. present a more general sliding window (SW) channel model that accommodates both burst and random erasures. The SW model has three parameters \( \{a, b, \tau\} \). As per the SW model, within any sliding window of \( w \) consecutive time slots, either a burst erasure of length at most \( b \) or else, at most \( a \) random erasures can occur.

In this paper, we are interested in constructing streaming codes for the SW channel model, i.e., they allow perfect recovery from erasure patterns as per the SW model. As it turns out (see [12]), when constructing such codes, we can, without loss of generality, set \( w = \tau + 1 \). To explicitly emphasize this simplification, from hereon, we will be referring to this modified SW model as the \( \{a, b, \tau\} \) Delay-Constrained Sliding Window (DCSW) channel model. We formally present the channel model in Sec. II-B. We will use the terminology \( \{a, b, \tau\} \) streaming code to denote any streaming code designed for the DCSW channel model.

In [11], an upper bound on the rate of an \( \{a, b, \tau\} \) streaming code is obtained, and a near-rate-optimal code over a finite field of size \( O(\tau^3) \) is presented. It is later shown in [13] and [14] that this rate is indeed achievable for all possible choices of parameters \( \{a, b, \tau\} \). The resultant optimal rate of an \( \{a, b, \tau\} \) streaming code is given by:

\[
R_{\text{opt}} = \frac{\tau + 1 - a}{\tau + 1 - a + b}.
\]

The rate-optimal codes presented in [13] and [14] require a finite field alphabet size that is exponential in \( \tau \). The paper [15] presents an explicit construction of rate-optimal codes that use maximum distance separable (MDS) and Gabidulin codes. However, the construction in [15] requires, again, a field size exponential in \( \tau \) and is confined to parameters \( \{a, b, \tau\} \) satisfying \( R_{\text{opt}} \geq \frac{1}{2} \). A non-explicit rate-optimal streaming code construction for all parameters, which requires a field \( \mathbb{F}_{q^2} \), with prime power \( q \geq \tau \), is presented in [12]. Subsequently, an explicit construction is provided in [16] requiring field size \( q^2 \), for prime power \( q \geq \tau + b - a \).

Explicit rate-optimal constructions having linear field size for some specific \( \{a, b, \tau\} \) parameter ranges are presented in [12], [17], and [18]. However, the one in [16] remains the smallest field size, explicit rate-optimal streaming code construction that covers all possible \( \{a, b, \tau\} \). Note that the field size required for the explicit code construction in [16] is larger than the field size requirement \( q^2; q \geq \tau \) of the non-explicit code in [12]. Streaming codes for variable packet lengths are explored in [19] and [20]. Various other models of erasure codes for streaming have been studied in the literature – for instance, see [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], and [31] and references therein. However, as noted earlier, in this paper we restrict our attention to the construction of \( \{a, b, \tau\} \) streaming codes.

A. Our Contributions

We present an explicit rate-optimal \( \{a, b, \tau\} \) streaming code construction for all parameters, which has the exact field size requirement \( q^2 \), with prime power \( q \geq \tau \), as that of the non-explicit code in [12]. We achieve the smallest known field size of an explicit rate-optimal \( \{a, b, \tau\} \) streaming code construction that holds for all \( \{a, b, \tau\} \) parameters. Our construction is inspired by the structure of the non-explicit code in [12]. As smaller field size constructions simplify implementation, we believe our construction would be of practical interest. Furthermore, we adhere to a modular design approach in the following sense. The parity-check (p-c) matrix of an MDS code with block length \( \tau + 1 \) and minimum distance \( a + 1 \) is one of the modules in our rate-optimal construction. The requirement \( q \geq \tau \) is applied to ensure the existence of such an MDS code. We note that the resulting code will still be an \( \{a, b, \tau\} \) streaming code even if the MDS p-c matrix is replaced with a p-c matrix of any linear block code with block length \( \tau + 1 \) and minimum distance at least \( a + 1 \). This way, although at the expense of rate-optimality, one may choose a \( q \ll \tau \). Thus, our construction also offers a framework to tradeoff rate versus field size.

B. Organization of the Paper

In Sec. II, we first formally present the definitions of streaming codes and the DCSW channel model. We then discuss the diagonal embedding framework for constructing streaming codes. The burst and random erasure recovery properties required of the embedded scalar codes are also enumerated. Sec. II ends with a discussion on the interplay between field size requirement and packet length of streaming codes. An explicit p-c matrix of a scalar code requiring field size \( q^2 \), where prime power \( q \geq \tau \), is presented in Sec. III. We illustrate how our scalar code satisfies the required burst and random erasure recovery properties with the help of an example in Sec. IV. In Sec. V, we provide a general proof for the random erasure recovery property. In Sec. VI, we demonstrate that the scalar code satisfies the burst erasure recovery property in general as well, assuming that a certain sub-matrix of the p-c matrix possesses certain properties. In Sec. VII, this assumption is proven to be valid. In Sec. VIII, we present a generalization of our construction resulting in streaming codes over further smaller fields by trading off rate.

C. Notation

For integers \( a \) and \( b \), the notation \([a : b]\) denotes the set \( \{a, a + 1, \ldots, b - 1, b\} \). Naturally, if \( a > b \), \([a : b]\) reduces to the null set \( \{\} \). Given two sets \( A, B \), we use \( A \setminus B \) for the set of all elements that are in \( A \), but not in \( B \). The number of elements in a set \( A \) is denoted by \(|A| \). Given a set of integers \( A \) and an integer \( z \), \( A + z \) denotes the set \( \{i + z : i \in A\} \).

The finite field with \( q \) elements is denoted by \( \mathbb{F}_q \), and \( \mathbb{F}_q^n \) is the \( n \)-dimensional vector space over \( \mathbb{F}_q \). Depending on the context, we will either interpret the vectors in \( \mathbb{F}_q^n \) as column vectors or row vectors. In particular, we will use underbar to specify column vectors. For instance, we will speak of a column vector \( v \in \mathbb{F}_q^n \). For a subset \( \mathcal{Y} \subseteq \mathbb{F}_q^n \), \( \langle \mathcal{Y} \rangle \) denotes the linear span of the elements in \( \mathcal{Y} \).

By \([n, k]\) scalar code, we mean a linear block code of block length \( n \) and dimension \( k \), i.e., a \( k \)-dimensional subspace.
of $\mathbb{F}_q^n$. If needed, $[n,k]_q$ notation is employed to explicitly specify the finite field size $q$. We will regard the elements of a code, i.e., codewords, as row vectors in $\mathbb{F}_q^n$. Codewords of $C$ will take the form $[c_0 \ c_1 \ \cdots \ c_{n-1}]$, where $c_j$'s are referred to as code symbols. The $[n,k,d_{\text{min}}]_q$ notation specifies that the Hamming distance between any two codewords is at least $d_{\text{min}}$.

Let $M$ be a $(k \times n)$ matrix, $I \subseteq [0 : k - 1]$ and $J \subseteq [0 : n - 1]$. Then, $M(I,J)$ denotes the $([I] \times [J])$ sub-matrix of $M$ comprises of rows with row-indices in $I$ and columns with column-indices in $J$. $M(I,:)$ is the $([I] \times n)$ sub-matrix of $M$ formed by rows indexed by $I$ and all columns. Similarly, $M(:,J)$ is the $(k \times [J])$ sub-matrix of $M$ formed by columns indexed by $J$ and all rows. For singleton sets, we follow the notation $M(i,J) = M([i],J)$, $M(I,j) = M(I,[j])$ and $M(i,j) = M([i],[j])$. We use $|M|$ to denote the determinant of $M$. The $(u \times u)$ identity matrix is denoted by $I_u$. We use $\mathbf{0}_{(u \times v)}$ for the $(u \times v)$ all-zero matrix and $\mathbf{1}_{(u \times v)}$ for the $(u \times v)$ all-one matrix. For brevity, we avoid mentioning size of the all-zero and all-one matrices if it is clear from the context.

II. BACKGROUND ON STREAMING CODES

A. General Streaming Codes

Streaming codes are packet-level erasure codes and have the following two defining characteristics: (i) a causal, convolutional encoder which allows on-the-fly encoding of message packets as they come in and (ii) a delay-constrained decoder.

B. Delay-Constrained Sliding Window (DCSW) Channel Model

For $t \in [0 : \infty]$, let $W_t$ denote the set of $t + \tau + 1$ consecutive time slots beginning from $t$, i.e., $W_t \triangleq [t : t + \tau]$. Consider an erasure pattern as given by $E \triangleq \{i \in [0 : \infty] | y(i) = \star\}$. An erasure pattern $E$ conforms to the $(a,b,\tau)$ DCSW channel model if it satisfies at least one of the following constraints for any given $t$:

- **Burst Erasure Constraint**: We have $E \cap W_t \subseteq [i : i + b - 1]$ for some $i \in W_t$. In other words, when restricted to $W_t$, the erasure pattern is bursty, which affects at most $b$ consecutive time slots.
- **Random Erasure Constraint**: We have $|E \cap W_t| \leq a$, i.e., when restricted to $W_t$, there can be at most $a$ erasures.

**Definition 1 ((a,b,τ) Streaming Code)**: Consider a streaming code $C$ for which there exists a sequence of decoding functions $\{\Phi_t\}_{t=0}^{\infty}$ such that:

$$\hat{u}(t) = \Phi_t(y(0), \cdots, y(t + \tau)),$$

for all $t$, whenever the erasure pattern conforms to the $(a,b,\tau)$ DCSW channel model. Then, $C$ will be referred to as an $(a,b,\tau)$ streaming code.

**Remark 1 (Constraints on Parameters (a,b,τ))**: As burst erasure of size $b$ is a special case of $b$ random erasures, we have $a \leq b$. Moreover, in the case of an $(a,b,\tau)$ streaming code, as the decoder needs to recover $u(t)$ by time $(t + \tau)$, it should be that $b \leq \tau$. If otherwise, due to causal encoding, a burst erasure affecting time slots $[t : t + \tau]$ will make it impossible for any decoder to recover $u(t)$ by time $(t + \tau)$.

**Remark 2**: It is fair to maintain the parameters $a, b$ proportionate to $\tau$ in practice. This is due to the fact that, in a real-world scenario, each packet is likely to encounter more "varieties" of erasure patterns across time slots $[t : t + \tau]$ as $\tau$ increases. In order to be resilient against such erasure patterns, it is hence desirable to increase $a$ and $b$ correspondingly in the DCSW model. Therefore, the field size requirement of $q^2, q \geq \tau + b - a$ in [16] may prove to be more stringent compared to the requirement $q^2, q \geq \tau$ in the current paper.

C. Streaming Codes Through Diagonal Embedding

Diagonal embedding, introduced in [10], is a framework for deriving a packet-level code from a scalar code. This

Markov models such as the Gilbert-Elliott (GE) model [32, 33] have widely been used to capture packet-loss patterns over various networks (e.g., see [34], [35], [36]). However, from the code design point-of-view, it is desirable to use deterministic channel models. In line with prior work, we adopt the SW channel model, which may be seen as a deterministic approximation of the GE model [37]. Under the GE model, there are two states – a "good" state and a "bad" state. In the good state, packets get erased with a small probability and in the bad state, the packet erasure probability is close to 1. Hence, the GE channel remaining in the bad state results in burst erasures whereas the good state leads to random erasures.

As noted earlier in Sec. I, after setting $w = \tau + 1$, the SW channel reduces to the DCSW channel model.
The packet-level code inherits the rate $\frac{k}{n}$ of the underlying scalar code $C$. Diagonal embedding of a scalar code of block length 6 is illustrated in Fig. 1.

### D. Properties Required of the Diagonally Embedded Scalar Code

Let $\delta = b - a$. In this paper, we employ the diagonal embedding technique to obtain an explicit rate-optimal $(a, b, \tau)$ streaming code construction. We will set $n = \tau + 1 - a + b = \tau + 1 + \delta$ and $k = \tau + 1 - a = n - b$, so that the rate of the packet-level code obtained through diagonal embedding matches the optimal rate given by (1). In order to show that the packet-level code constructed through the diagonal embedding of an $[n = \tau + 1 + \delta, k = n - b]$ scalar code $C$ is an $(a, b, \tau)$ streaming code, it is necessary and sufficient to show that the following erasure recovery properties hold for any codeword $[c_0, c_1, \cdots, c_{n-1}] \in C$.

1. **B1** For any $t \in [0 : \delta - 1]$, the code symbol $c_t$ should be recoverable using the set of code symbols $\{c_j \mid j \in [t + b : t + \tau] \cup \{c_j \mid j \in [0 : t - 1]\}$, i.e., $c_t$ can recover from the burst erasure involving $b$ code symbols $\{c_l \mid l \in [t : t + b - 1]\}$ by accessing $\tau + b - 1$ subsequent non-erased code symbols and $t$ previous code symbols.

2. **B2** For any $t \in [\delta : \tau + 1 + a]$, code symbols $\{c_j \mid j \in [t : t + b - 1]\}$ should be recoverable by accessing the remaining code symbols $\{c_j \mid j \notin [t : t + b - 1]\}$.

The properties B1 and B2 ensure burst erasure recovery under the delay constraint, whereas the properties R1 and R2 deal with random erasures under the delay constraint. We refer the reader to [12] for a detailed proof.

**Remark 3:** It follows from property B2 that, for $t = \tau + 1 - a$, the last $(n - k) = b$ code symbols $\{c_{k_1}, \ldots, c_{n-1}\}$ can be computed from the first $k$ code symbols $\{c_0, \ldots, c_{k-1}\}$. As the code dimension is $k$, property B2 thus guarantees that $C$ has a systematic generator matrix of the form $[I_k C]$.

### E. Parity Check Viewpoint of Desired Properties

Let $H = [h_0 \ h_1 \ \cdots \ h_{n-1}]$ be a $(b \times n)$ $p$-c matrix of the diagonally embedded $[n = \tau + 1 + \delta, k = n - b]$ scalar code $C$. For $t \in [0 : \delta - 1]$, let $H(t) = [h_0^{(t)} \ h_1^{(t)} \ \cdots \ h_{n-1}^{(t)}]$ be a $p$-c matrix of the punctured code obtained by deleting indices $[t + \tau - 1 + n - 1]$ of $C$. The erasure recovery properties enumerated previously in Sec. II-D can be translated into properties of these $p$-c matrices. We first state, without proof, a well-known result that is useful in deriving these properties.

**Lemma 1:** Let $H = [h_0 \ h_1 \ \cdots \ h_{n-1}]$ be a $p$-c matrix of an $[n, k]$ scalar code $C$, where $n = \tau + 1 + \delta$ and $k = n - b$. Let $\mathcal{E} \subseteq [0 : n - 1]$ with $i \in \mathcal{E}$ denote the set of erased code symbol indices. Then the $i$-th code symbol can be recovered from the non-erased code symbols if and only if $h_i \notin \{\langle h_j \mid j \in \mathcal{E} \setminus \{i\}\}$. 

---

**Fig. 1.** Packet-level code constructed by diagonal embedding of a scalar code of block length 6. Each diagonal is a codeword of the scalar code. Three such diagonally embedded codewords are shown in the figure using three different colors. Each column indicates a coded packet. Assume that the coded packet $\tilde{x}(0)$ is erased. If there is a delay constraint $\tau = 3$, then for recovery of code symbol $c_0$, one can not access code symbols $c_4$ and $c_5$. The technique has often been used in the streaming-code literature (for instance, see [12], [13], [14], [15], [16]). Let $C$ be an $[n, k]$ scalar code having a $k \times n$ systematic generator matrix of the form:

$$G = [I_k C].$$

i.e., the first $k$ code symbols are message symbols. Consider a packet-level code with the coded packet at time $t$ denoted by:

$$\tilde{x}(t) = [x_0(t) \ x_1(t) \ \cdots \ x_{n-1}(t)]^T.$$ 

We will say that the packet-level code is obtained by diagonal embedding of the scalar code $C$ if each length-$n$ row vector of the form:

$$[x_0(t) \ x_1(t + 1) \ \cdots \ x_{n-1}(t + n - 1)]$$

is a codeword in $C$, for all $t$. If the message packet at time $t$ is denoted by:

$$u(t) = [u_0(t) \ u_1(t) \ \cdots \ u_{k-1}(t)]^T,$$

the message vector corresponding to the codeword $[x_0(t) \ x_1(t + 1) \ \cdots \ x_{n-1}(t + n - 1)]$ is given by

$$[u_0(t) \ u_1(t + 1) \ \cdots \ u_{k-1}(t + k - 1)].$$

Thus, $x_i(t) = u_i(t)$ for $i \in [0 : k - 1]$ and

$$[x_k(t + k) \ \cdots \ x_{n-1}(t + n - 1)] = [u_0(t) \ u_1(t + 1) \ \cdots \ u_{k-1}(t + k - 1)]C.$$ 

The packet-level code inherits the rate $\frac{k}{n}$ of the underlying scalar code $C$. Diagonal embedding of a scalar code of block length 6 is illustrated in Fig. 1.
Using the above lemma, the required erasure recovery properties can be restated as follows [12]:

B1 For any \( t \in [0 : \delta - 1] \),
\[
\{ h^{(t)}_j | t + 1 \leq j \leq t + b - 1 \}.
\]

R1 For any \( t \in [0 : \delta - 1] \) and any set \( A \subseteq [t : t + \tau] \) with \( |A| = a \) and \( t \in A \),
\[
\{ h^{(t)}_j | j \in A \setminus \{t\} \}.
\]

B2 For any \( t \in [\delta : \tau + 1 - a] \), the set of \( b \) consecutive columns of \( H \) given by
\[
\{ h_j | t \leq j \leq t + b - 1 \}
\] should be linearly independent. Equivalently, \( H(:,[t : t+b-1]) \) should be invertible for all \( t \in [\delta : \tau+1-a] \).

R2 For any set \( A \subseteq [\delta : \tau + \delta] \) with \( |A| \leq a \), the set of columns
\[
\{ h_j | t \in A \}
\] should be linearly independent.

F. Encoder and Decoder Memory Under Diagonal Embedding

Although the streaming code definition in Section II-A does not place a finite memory requirement, it is a necessity in practice. Streaming codes constructed through diagonal embedding require only finite encoder and decoder memory.

During the encoding phase, computing the parity symbol \( x_{k+j}(t) \) would need access to the \( (t - (k + j)) \)-th packet as
\[
[x_0(t - k - j) \cdots x_{k+j}(t) \cdots x_{n-1}(t+n-k-j-1)] \in C,
\]
by the definition of diagonal embedding. As \( 0 \leq j \leq n-k-1 \), this implies that the memory needed for encoding a packet is \( k + (n - k - 1) = n - 1 \).

During the decoding of message packet \( u_i(t) \) at time \( t + \tau \), to recover the \( i \)-th message symbol \( u_i(t) \), the decoder may need access to the symbols \( \{u_0(t-i), \ldots, u_{i-1}(t-1)\} \) that have already been decoded. Since \( 0 \leq i \leq k - 1 \), it follows that the memory needed for decoding is \( t + \tau - (t + k - 1) = \tau + k - 1 \).

G. Field Size vs. Packet Length

The field size requirement and the packet length are closely related. By increasing the packet length, it is possible to obtain a small field size streaming code, as shown below.

Lemma 2: Let \( m \) be a positive integer. Suppose there exists an \((a,b,\tau)\) streaming code over \( \mathbb{F}_{Q^m} \), with packet length \( n \) and rate \( \frac{k}{n} \), constructed through diagonal embedding. Then, one can obtain an \((a,b,\tau)\) streaming code over \( \mathbb{F}_Q \) with packet length \( nm \) and the same rate \( \frac{k}{n} \).

Proof: Let \( C \) be an \([n,k]_{Q^m}\) code having a \((k \times n)\) systematic generator matrix. Any element of \( \mathbb{F}_{Q^m} \) can be represented as a row vector of length \( m \) over \( \mathbb{F}_Q \). Let \( C^{(m)} \) be a code of block length \( nm \) whose codewords are obtained by representing the code symbols of \( C \) as row vectors of length \( m \) over \( \mathbb{F}_Q \). In other words, for every codeword \([c_0, c_1, \cdots, c_{n-1}] \in C \), the new code \( C^{(m)} \) has a corresponding codeword of length \( nm \) such that the code symbols at indices \([im:im+m-1]\) are the \( m \) \( \mathbb{F}_Q \)-symbols representing \( c_i \), for all \( i \in [0 : n - 1] \). It is well-known that there exists a representation such that:

- \( C^{(m)} \) is an \([nm,km]_Q \) code with a \((km \times nm)\) systematic generator matrix and
- if \( C \) is capable of recovering code symbols with index in \( I \subseteq [0 : n - 1] \) using only code symbols with index in \( R \subseteq [0 : n - 1] \), then \( C^{(m)} \) is capable of recovering code symbols with index in \( U \subseteq \mathbb{E}[im : im + m - 1] \) using only code symbols with index in \( U \subseteq \mathbb{E}[im : im + m - 1] \).

We refer interested readers to [38] for an explicit description of such a representation and the resultant generator matrix for \( C^{(m)} \).

Suppose the \((a,b,\tau)\) streaming code over \( \mathbb{F}_{Q^m} \) is obtained by the diagonal embedding of \( C \). Now consider the packet-level code of packet length \( nm \), which is such that
\[
[x_0(t) x_1(t) \cdots x_{m-1}(t) x_m(t+1) \cdots x_{2m-1}(t+1) \cdots x_{(n-1)m}(t+n-1) \cdots x_{nm-1}(t+n-1)]
\]
is a codeword in \( C^{(m)} \), for all \( t \). It follows from the properties of \( C^{(m)} \) listed above that this packet-level code is an \((a,b,\tau)\) streaming code over \( \mathbb{F}_Q \), having rate \( \frac{km}{nm} = \frac{k}{n} \).

Since rate-optimal \((a,b,\tau)\) streaming code constructions based on diagonal embedding are known over finite fields of characteristic two (for instance, constructions in [12], [16]), it follows from Lemma 2 that rate-optimal binary streaming codes can be constructed for all valid \( \{a,b,\tau\} \) parameters, provided the packet length is allowed to be sufficiently large. Hence, the field size reduction problem for rate-optimal streaming codes is trivial if the allowed packet length is not bounded. On the other hand, Lemma 2 does not result in packet size reduction, as both codes in Lemma 2 have packet size equal to \( nm \log_2 Q \). Thus, reducing packet size is the non-trivial problem here. The field sizes of two streaming codes can hence be directly compared only if they have the same packet length.

In the streaming code literature, while specifying the field size of a construction, it is usually assumed (as can be seen in [12], [13], [14], [15], [16], [17], [18]) that the packet length \( n = O(\tau) \). More specifically, the rate-optimal quadratic field size constructions in [12] and [16], which are state of the art for general parameters, employ diagonal embedding with \( n = \tau + 1 - a + b \). If the parameters \( \{a,b,\tau\} \) are such that \( b \) and \( (\tau + 1 - a) \) are co-prime, then it follows from the optimal rate expression in (1) that the smallest possible packet length of a rate-optimal streaming code constructed via diagonal embedding is \( (\tau + 1 - a + b) \). In the current paper, we also use diagonal embedding with \( n = \tau + 1 - a + b \), and hence our field size comparison with the constructions in [12] and [16] makes sense.

III. MAIN CONSTRUCTION OF THE DIAGONALLY EMBEDDED SCALAR CODE

Our explicit, rate-optimal streaming code construction is based on the diagonal embedding of an \([n = \tau + 1 - a + b,\)
explicit constructions of $S$ and $1 + H$ previously. We construct the p-c matrix follows: 

$$D = \begin{pmatrix}
\[1 : \delta] \\
\[0 : \delta]
\end{pmatrix}
$$

$$P = \begin{pmatrix}
\[0 : \tau - 1]
\end{pmatrix}
$$

$$\tilde{W} = \begin{pmatrix}
\[0 : \tau]
\end{pmatrix}
$$

and will show in subsequent sections that $S$ satisfies the four erasure recovery properties listed in Sec. II-E. The p-c matrix construction requires the existence of two key matrices; (i) an $(a \times (\tau + 1 - a))$ matrix $S$ over $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$ such that any square sub-matrix of it is non-singular and (ii) a $(\delta \times (\tau - b))$ matrix $P$ over $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$ that satisfies certain criteria which we will soon present in Sec. III-B. We discuss the existence of explicit constructions of $S$ and $P$ in Sec. III-A and Sec. III-C, respectively.

**Construction 1:** Let $\delta = b - a$, $q \geq \tau$ be a prime power and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Consider the matrices $S$ and $P$ as described previously. We construct the p-c matrix $H$ of an $[n = \tau + 1 + \delta, k = n - b]_{q^2}$ scalar code in a step-by-step manner as follows:

- Initialize $H$ to be the $(b \times (\tau + 1 + \delta))$ all-zero matrix,
- set $H([0 : \delta - 1], [0 : \delta - 1]) = \alpha I_3$,
- set $H([0 : \delta - 1], [b : \tau - 1]) = P$,
- set $H(0, \tau) = \alpha$,
- set $H([1 : \delta - 1], [\tau + 1 : \tau + \delta - 1]) = I_{3-1}$,
- set $H([\delta : b - 1], [0 : \tau - a]) = S$,
- set $H([\delta : b - 1], [\tau + 1 + a : \tau]) = I_a$ and
- set $H(b - 1, \tau + \delta) = 1$.

We use the notation:

$$H_T = H([0 : \delta - 1], :) \quad \text{and} \quad H_B = H([\delta : b - 1], :)$$

to indicate the top $\delta$ rows of the p-c matrix and the bottom $a$ rows of the p-c matrix, respectively. The top $\delta$ rows of the p-c matrix $H$ are given by:

$$H_T = \begin{pmatrix}
D_1 & Z_1 & P & D_2 & Z_2
\end{pmatrix}_{(\delta \times \delta)}$$

where $D_1, D_2$ are diagonal matrices and $Z_1, Z_2$ are zero matrices defined as shown below:

$$D_1 = \begin{pmatrix}
\alpha & & \\
& \alpha & \\
& & \alpha
\end{pmatrix}_{(\delta \times \delta)}$$

$$Z_1 = \begin{pmatrix}
0
\end{pmatrix}_{(\delta \times a)}$$

$$D_2 = \begin{pmatrix}
\alpha & 1 \\
& 1
\end{pmatrix}_{(\delta \times \delta)}$$

$$Z_2 = \begin{pmatrix}
0
\end{pmatrix}_{(\delta \times 1)}$$

The bottom $(b - \delta) = a$ rows of $H$ are given by:

$$H_B = \begin{pmatrix}
S & D_3 & Z_3 & E
\end{pmatrix}_{(a \times (\tau + 1 - a))}$$

where $D_3$ is a diagonal matrix and $Z_3$ is a zero matrix and $E$ is an identity vector defined as shown below:

$$D_3 = \begin{pmatrix}
1 & & \\
& 1 & \\
& & \ddots
\end{pmatrix}_{(a \times a)}$$

$$Z_3 = \begin{pmatrix}
0 \\
\vdots \\
0
\end{pmatrix}_{(a \times (\delta - 1))}$$

and $E = \begin{pmatrix}
0 \\
\vdots \\
1
\end{pmatrix}_{(a \times 1)}$.

See Fig. 2 for an illustration of the complete p-c matrix $H$.

**A. Full Superregular Matrices**

If $\hat{H} = [W I_a]$ is a p-c matrix of a $[\tau + 1, \tau + 1 - a]$ MDS code, then it is a well-known result [39, Ch. 11] that every square sub-matrix of $W$ is non-singular. Hence, we can choose $S = W$. Equivalently, $H([\delta : b - 1], [0 : \tau]) = H_B(:, [0 : \tau])$ is a p-c matrix of a $[\tau + 1, \tau + 1 - a]$ MDS code in systematic form.

Explicit constructions of $[n, k]_q$ MDS codes are known for $q \geq n - 1$. For instance, see the discussion on doubly extended Reed-Solomon codes in [39, Ch. 11]. Thus, a finite field of size $q \geq \tau$ suffices to explicitly construct the matrix $S$. This, in turn, results in a field size requirement of $q^2$, with prime power $q \geq \tau$, for the p-c matrix $H$ provided by Construction 1.

**Definition 2 (Full Superregular Matrices):** A matrix is said to be full superregular [40] if all its square sub-matrices are invertible. Hence, $S$ is a full superregular matrix. The full superregularity property of $S$ ensures that any collection of $a$ columns of $H_B(:, [0 : \tau]) = [S I_a]$ forms a linearly independent set.

**Remark 4:** In practical settings, finite fields with characteristic two is often preferred [41]. Since our construction works for any $q \geq \tau$, in particular, one may choose $q = 2^d$, for any $d \geq \lceil \log_2(\tau) \rceil$. It follows that the p-c matrix $H$ can be explicitly constructed over any finite field of size $2^d$, where $d \geq \lceil \log_2(\tau) \rceil$.

**B. Permissible Matrices**

In our p-c matrix description, the entries of $P$ are not specified. We show in Section V that the p-c matrix $H$ satisfies properties $R1$ and $R2$ irrespective of the assignment of $P$, provided the entries of $P$ are from $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$. In Section VI, it is shown that if $P$ possesses the following four properties, then $H$ satisfies $B1$ and $B2$ properties.

We use the notation:

$$\hat{P} = \begin{pmatrix}
0 \\
P
\end{pmatrix}_{(\delta \times a)}$$

to denote the $(\delta \times (\tau - \delta))$ matrix obtained from $P$ by augmenting $a$ all-zero columns in the beginning. We will refer to the matrix $P$ as a permissible matrix if it possesses the following four properties.
Fig. 2. \((b \times (\tau + 1 + \delta))\) parity check matrix \(H\).

- **Top-Left Property:** The \((\theta \times \theta)\) sub-matrix \(P([0 : \theta - 1], [0 : \theta - 1])\), obtained by selecting the first \(\theta\) rows and first \(\theta\) columns of \(P\), is non-singular, for all \(\theta \in [1 : \min\{\delta, \tau - b\}\).
- **Consecutive-Rows Property:** If \(\delta \geq \tau - b\), then the sub-matrix of \(P\) formed by any \(\tau - b\) consecutive rows should be non-singular, i.e., \(P([\ell : \ell + \tau - b - 1])\) is non-singular for all \(\ell \in [0 : \delta - \tau + b]\).
- **Consecutive-Columns Property:** If \(\tau - b \geq \delta\), then any \((\delta \times b)\) sub-matrix of \(P\) formed by \(b\) consecutive columns contains \(a\) all-zero columns and the remaining \(\delta\) columns of this sub-matrix are linearly independent. In other words, for all \(\ell \in [0 : \tau - b - \delta]\), \(P([\ell : \ell + b - 1])\) has \(a\) all-zero columns and rank \(\delta\).
- **Bottom-Right Property:** Let \(R_\theta\) be the \((\theta \times (\theta + a))\) sub-matrix of \(\hat{P}\) comprised of the last \(\theta\) rows and the last \(\theta + a\) columns of \(\hat{P}\), where \(\theta \in [1 : \min\{\delta, \tau - b\}\), i.e.,

\[
R_\theta = \hat{P}([\delta - \theta : \delta - 1], [\tau - \delta - \theta - a : \tau - \delta - 1]).
\]

Then, \(R_\theta\) contains \(a\) all-zero columns and the \(\theta\) other columns of \(R_\theta\) are linearly independent.

### C. Explicit Recursive \([0, 1]\) Construction of a Permissible Matrix

To complete the description of the explicit p-c matrix \(H\), it suffices to present an explicit \((\delta \times \tau - b)\) permissible matrix \(P\). We will now present a recursive construction of \(P\), which uses only ones and zeros.

**Definition 3:** For any positive integers \(u, v\) and \(a\), we recursively define the \((u \times v)\) matrix \(P_{u,v}^a\), as shown below:

\[
P_{u,v}^a = \begin{cases} 
I_u & u + a < v, \\
\begin{bmatrix} I_u & 0 \\
(0 \times (v-u))
\end{bmatrix} & u \leq v \leq u + a, \\
\begin{bmatrix} I_v & 0 \\
P_{u-v,v}^a 
\end{bmatrix} & v < u.
\end{cases}
\]

For example,

\[
P_{3,7}^2 = \begin{bmatrix} I_3 & 0 \\
(3 \times 2)
\end{bmatrix},
P_{3,2}^2 = \begin{bmatrix} I_2 \\
P_{1,2}^2
\end{bmatrix}
\text{ and } P_{1,2}^2 = [1, 0].
\]

Therefore we have:

\[
P_{3,7}^2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0
\end{bmatrix}
\text{. (5)}
\]

Given \(a, b, \tau\), we set \(P = P_{\delta, \tau - b}^a\). We note in the following lemma that this assignment results in a permissible matrix.

**Lemma 3:** The \((\delta \times (\tau - b))\) matrix \(P = P_{\delta, \tau - b}^a\) is a permissible matrix. i.e., it satisfies the four properties: top-left, consecutive-rows, consecutive-columns and bottom-right properties.

**Proof:** The proof is deferred to Sec. VII. \(\Box\)

Before we proceed to Theorem 1, which shows that the diagonal embedding of our scalar code leads to a rate-optimal streaming code, we provide some intuition for the recursive construction of \(P_{u,v}^a\), matrix. When \(v \geq u + a\), the recursion allows for a zero column among every \(u + a\) consecutive columns. This leads to \(\hat{P}\) possessing the consecutive-columns and bottom-right properties that require certain sub-matrices to have a zero columns. This, in turn, will ensure that the \((b \times b)\) sub-matrices of the p-c matrix \(H\) of interest for property \(B2\) can be made to have the block structure shown below:

\[
\begin{bmatrix} 0 & \hat{P} \\
\delta \times a & \delta \times \delta
\end{bmatrix}
\]

\[
\begin{bmatrix} \hat{S} \\
\delta \times a
\end{bmatrix}
\]

\[
\begin{bmatrix} X \\
\end{bmatrix}
\]

Here, \(\hat{P}\) is a \((\delta \times \delta)\) sub-matrix of \(\hat{P}\) that is invertible due to the consecutive-columns and bottom-right properties, and \(\hat{S}\) is an \((a \times a)\) sub-matrix of \([S \ D_3]\) matrix and hence invertible.

Regardless of the choice of \(u, v\), the top left portion of \(P_{u,v}^a\) consists of an identity matrix, which ensures the top-left property. The recursive expansion for the \(v < u\) case helps towards the consecutive-rows property. The proof of property \(B1\) employs the top-left and consecutive-rows properties to show invertibility of certain sub-matrices.
Theorem 1: Let $H$ be the $(b \times (\tau + 1 + \delta))$ p-c matrix described in Construction 1, where submatrices $S$ and $P$ are full superregular and permissible, respectively. Then, diagonal embedding of the $[\tau + 1 + \delta, \tau + 1 - a]$ scalar code with $H$ as a p-c matrix results in a rate-optimal $(a, b, \tau)$ streaming code. 

Proof: To prove the theorem, it suffices to show that $H$ satisfies the properties R1, R2, B1 and B2 outlined in Sec. II-E. The proofs for properties R1 and R2 are provided in Sec. V, and the proofs for properties B1 and B2 are in Sec. VI. We prove the theorem for an example case in Sec. IV. □

D. Example Constructions of Scalar Codes

Example 1: $(a = 3, b = 6, \tau = 8)$

Here $\delta = 3$, $\tau - b = 2$, $\tau + 1 - a = 6$ and $\tau + 1 + \delta = 12$. We choose $q = 2^3 \geq \tau$. Note that:

$$P_{3,2}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$ 

The p-c matrix $H$ of the $[n = 12, k = 6]_{2^6}$ scalar code in this case is given by:

$$H = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

where $S \in \mathbb{F}_{2^3}^{3 \times 6}$ and $\alpha \in \mathbb{F}_{2^3} \setminus \mathbb{F}_2$. We show in Sec. IV that this p-c matrix satisfies the properties R1, R2, B1 and B2.

Example 2: $(a = 2, b = 5, \tau = 12)$ Here $\delta = 3$, $\tau - b = 7$, $\tau + 1 - a = 11$ and $\tau + 1 + \delta = 16$. We choose $q = 13 \geq \tau$. Note that $P_{3,7}^2$ is as given in (5). The p-c matrix $H$ of the $[n = 16, k = 11]_{13^{13}}$ scalar code is given by:

$$H = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$ 

E. Connections to the Streaming Code Construction in [12]

The construction 1 in the paper is motivated by the non-explicit streaming code construction presented in [12]. In the following, we describe the construction in [12].

Constr (Prior Construction in [12]): Let $\delta = b - a$, $q \geq \tau$ be a prime power and $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Let the $(a \times (\tau + 1 - a))$ matrix $S$ over $\mathbb{F}_{q^2} \subseteq \mathbb{F}_q$ be a full superregular matrix. Let $H_{\text{n-e}}$ denote a p-c matrix of an $[n = \tau + 1 + \delta, k = n - b, \mathbb{F}_{q^2}]$ scalar code that is constructed in a step-by-step manner as follows:

- Initialize $H_{\text{n-e}}$ to be the $(b \times (\tau + 1 + \delta))$ all-zero matrix,
- set $H_{\text{n-e}}[0 : \delta - 1, [0 : \delta - 1]] = \alpha I_b$,
- set $H_{\text{n-e}}(i, j) = v_{i,j} \in \mathbb{F}_q$ for all $i \in [0 : \delta - 1]$ and $j \in [i + b : i + \tau]$,
- set $H_{\text{n-e}}(\delta : b - 1, [0 : a - 1]) = I_a$,
- set $H_{\text{n-e}}(\delta : b - 1, [a : \tau]) = S$ and
- set $H_{\text{n-e}}(\delta, \tau + \delta) = 1$.

It is shown in [12] that there exists an (non-explicit) assignment for variables $v_{i,j} \in \mathbb{F}_q$ for $i \in [0 : \delta - 1]$ and $j \in [i + b : i + \tau]$ such that $H_{\text{n-e}}$ satisfies the properties R1, R2, B1 and B2.

For $i \in [0 : \delta - 1]$, in the $i$-th row of $H_{\text{n-e}}$, there are $(b - 1)$ consecutive zeros at columns $[i + 1 : i + b - 1]$. However, this is not mandatory for the p-c matrix $H$ presented in Construction 1. The structure of the last $a$ rows has been altered in $H$ to allow for the possibility of a streaming code construction framework that trades off rate for field size reduction (see Construction 2). Random erasure properties R1, R2 for Construction 1 follow irrespective of the assignment of the $P$ matrix. However, the prior construction relies on the assignment of $v_{i,j}$ values to prove the random erasure properties.

F. Connections to the Streaming Code Construction in [42]

The recursive definition of $P_{u,v}^q$ can be viewed as a generalization of the recursive matrix definition in [42] that was used to construct rate-optimal binary streaming codes for the situation when only burst erasures are present, i.e., $a = 1$. The p-c matrix $H_{\text{n-e}}$ of the diagonally embedded scalar code in [42] is given by:

$$H_{\text{n-e}} = \begin{bmatrix} I_b & B_{b,\tau-b} & I_b \\ I_u & B_{u,v-u} & v > u, \\ I_v & B_{u-v,v} & v < u, \end{bmatrix}$$

where $B_{u,v} = \begin{bmatrix} I_u \\ I_v \end{bmatrix}$.

For the burst only scenario, we have $a = 1$ and $\delta = b - 1$. Therefore, the p-c matrix of Construction 1 is given by:

$$H = \begin{bmatrix} \alpha & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}.$$ 

It turns out that the construction can be simplified to a binary field construction for the burst only case by setting $a = 1$ and $H(b - 1, \tau) = 0$, as shown below:

$$\tilde{H} = \begin{bmatrix} I_{b-1} & 0 & P_{b-1,\tau-b}^1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$ 

For an example case, we will now show that the $(b \times (\tau - b))$ matrices $B_{b,\tau-b}$ and $P_{b-1,\tau-b}^1$ closely resemble constructions. Let $b = 5, \tau = 15$. Here, we have:

$$B_{5,10} = [I_5 I_5] \quad \text{and} \quad P_{4,10}^1 = [I_4 0 I_4 0].$$

It can be noted that by linearly combining the four rows of $P_{4,10}^1$ with the all-one row, we get $B_{5,5}$. This holds true in general when $a = 1$ and $b \mid \tau$.

IV. PROOF THAT EXAMPLE 1 YIELDS AN $(a = 3, b = 6, \tau = 8)$ STREAMING CODE

In this section, we show that the p-c matrix $H$ in (6) for parameters $(a = 3, b = 6, \tau = 8)$ satisfies the properties R1, R2, B1 and B2 outlined in Sec. II-E. Let $C$ denote the
have their elements drawn from $\mathbb{F}_{2^n}$.

We will first argue that random erasure properties R1 and R2 are satisfied.

### A. Random Erasure Recovery

1) **Property R1**: For $t \in [0 : 2]$, recall that $H^{(t)}$ (see Sec. II-E) is a $p$-c matrix of the punctured code obtained by deleting indices $[t + t + 1 : n - 1]$ of $C$. In order to obtain $H^{(t)}$ from $H$, we are interested in the subspace of vectors within the row-space of $H$, which has zero entries across columns $[t + t + 1 : n - 1]$. If the $i$-th row of $H$ has zero entries across columns $[t + t + 1 : n - 1]$, then $H(i, [0 : t + \tau])$ lies in the row space of $H^{(t)}$.

We initially consider the case of $t = 0$. It can be observed that rows $\{0, 3, 4\}$ of $H$ have zero entries across columns $[t + 1 : n - 1]$. Consider the matrix:

$$
\tilde{H}^{(0)} = H(\{0, 3, 4\}, [0 : \tau])
$$

where

$$
\tilde{H}^{(0)} = \begin{bmatrix}
\alpha & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 & 0 & 0 \\
0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
$$

Let $\tilde{h}^{(0)}_i$ denote the $i$-th column of $\tilde{H}^{(0)}$. As rows of $\tilde{H}^{(0)}$ lie in the row space of $H^{(0)}$, to prove property R1 for $t = 0$, it is sufficient to show that:

$$
\tilde{h}^{(0)} = \langle \{\tilde{h}^{(0)}_i \mid i \in A \setminus \{0\}\} \rangle,
$$

for all $A \subseteq [0 : 8]$ such that $0 \in A$ and $|A| \leq 3$. Assume to the contrary that there exists $j, l \in [1 : 8]$ such that:

$$
\tilde{h}^{(0)}_j = a_j \tilde{h}^{(0)}_l + a_l \tilde{h}^{(0)}_j.
$$

Let

$$
H' = \tilde{H}^{(0)}([1 : 2], :)
$$

where

$$
H' = \begin{bmatrix}
\alpha & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 & 0 & 0 \\
0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
\end{bmatrix}
$$

and $h''_i$ denote the $i$-th column of $H'$. From (8), it follows that:

$$
h''_0 = a_j h''_j + a_l h''_l.
$$

Note that any two non-zero columns of $H'$ are linearly independent by the definition of the matrix $S$. Hence, (9) holds, it should be that $\{j, l\} \subseteq [1 : 7]$. Moreover, $h''_j$ and $h''_l$ are independent and since all three columns vectors in (9) have their elements drawn from $\mathbb{F}_{2^n}$, we have $a_j, a_l \in \mathbb{F}_{2^n}$. This contradicts (8) as $H^{(0)}(0, 0) = \alpha \in \mathbb{F}_{2^n}$ and $H^{(0)}(0, i) \in \mathbb{F}_{2^n}$ for all $i \in [1 : 7]$. Hence, we have proved property R1 for $t = 0$.

To prove for $t = 1$, we look at the following sub-matrix of $H$:

$$
\tilde{H}^{(1)} = \begin{bmatrix}
0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
\alpha & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
\end{bmatrix}
$$

Observe that the rows of this matrix lie in the row space of $H^{(1)}$. Let $\tilde{h}^{(1)}_j$ denote the $j$-th column of $\tilde{H}^{(1)}$. It is sufficient to show that:

$$
\tilde{h}^{(1)}_1 \notin \langle \{\tilde{h}^{(1)}_j \mid j \in A \setminus \{1\}\} \rangle,
$$

for all $A \subseteq [1 : 9]$ with $|A| \leq 3$ and $1 \in A$. Any two non-zero columns of $\tilde{H}^{(1)}([1 : 2], :)$ are linearly independent. Now, since $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^3}$ and all other entries of $H^{(1)}$ are from $\mathbb{F}_{2^n}$, similar to the $t = 0$ case, it can be argued that (10) is true.

For the remaining case of $t = 2$, we consider the matrix:

$$
\tilde{H}^{(2)} = \begin{bmatrix}
0 & 0 & \alpha & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\alpha & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
\end{bmatrix}
$$

whose rows belong to the row space of $H^{(2)}$. Let $\tilde{h}^{(2)}_j$ denote the $j$-th column of $\tilde{H}^{(2)}$. Similar to the previous scenarios, it is sufficient to show that:

$$
\tilde{h}^{(2)}_1 \notin \langle \{\tilde{h}^{(2)}_j \mid j \in A \{2\}\} \rangle,
$$

for all $A \subseteq [2 : 10]$ with $|A| \leq 3$ and $2 \in A$. This, again, follows from the three facts that (i) any two non-zero columns of $\tilde{H}^{(2)}([1 : 2], :)$ are linearly independent, (ii) $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^3}$, and (iii) all other entries of $\tilde{H}^{(2)}$ lie in $\mathbb{F}_{2^n}$.

2) **Property R2**: We need to show that the set of columns $\{\tilde{h}^{(2)}_j \mid j \in A\}$ is linearly independent, for all $A \subseteq [3 : 11]$ with $|A| \leq 3$. Suppose to the contrary:

$$
\sum_{j \in A} a_j \tilde{h}^{(2)}_j = 0,
$$

for some such $A$ and $a_j \neq 0$ for some $j \in A$. Note that any collection of 3 distinct non-zero columns of the matrix:

$$
H_B = H([3 : 5], :)
$$

is linearly independent. Let $\tilde{h}''_j$ denote the $j$-th column of $H_B$. From (12), it follows that:

$$
\sum_{j \in A} a_j \tilde{h}''_j = 0.
$$

Let $A_1 = A \setminus \{9, 10\}$ and $A_2 = A \cap \{9, 10\}$. As $\tilde{h}''_j = \tilde{h}''_{10} = 0$, we can rewrite (13) as:

$$
\sum_{j \in A_1} a_j \tilde{h}''_j = 0.
$$

We first consider the case where $|\{8, 11\} \cap A| \leq 1$. In this case, as $\tilde{h}''_j$’s appearing in (14) are distinct, they are
independent. Hence, we have $a_j = 0$ for $j \in A_1$. Thus, (12) can be rewritten as:

$$\sum_{j \in A_2} a_j h_j = 0. \quad (15)$$

By inspecting the matrix $H$ in (7), it can be noted that $h_9$ and $h_{10}$ are linearly independent. Hence, from (15), it follows that $a_j = 0$ for $j \in A_2$. Thus, we have $a_j = 0$ for $j \in A$ and the assumption made in (12) is invalidated.

Now consider the remaining case where $\{8, 11\} \subseteq A$. From (7), it can be observed that columns $h_8$, $h_9$, $h_{10}$ and $h_{11}$ are linearly independent. Thus, for (12) to hold, it should be that one more element $\ell \in [3 : 7]$ is present in $A$ with $a_\ell \neq 0$. i.e., $A = \{\ell, 8, 11\}$, where $\ell \in [3 : 7]$ and $a_\ell \neq 0$. As $h_\ell^{\prime} = h_\ell|_1$, from (13), we have:

$$a_\ell h_\ell^{\prime} + (a_8 + a_{11}) h_8^{\prime} = 0. \quad (16)$$

Since $\ell \in [3 : 7]$, $h_\ell^{\prime}$ and $h_8^{\prime}$ form an independent set and from (16), it follows $a_\ell = 0$. This contradicts the assumption made in (12).

### B. Burst Erasure Recovery

For this example, unlike the general proof in Sec. VI, we present a direct proof that does not use the notion of permissible matrices.

1) Property B1: For any $t \in [0 : 2]$, we need to show that $h_7^{(t)} \notin \{h_j^{(t)} | j + 1 \leq j \leq t + 5\}$. For $t = 0$, we consider the row $H(0, :)$:

$$\begin{pmatrix} \alpha & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$  

As we have zero entries across columns $[\tau + 1 : n - 1]$, $H(0, [1 : \tau])$ lies in the row space of $H^{(0)}$. Since $H(0, 0) = \alpha \neq 0$ and $H(0, 1) = H(0, 2) = \cdots = H(0, 5) = 0$, it follows that $h_7^{(0)} \notin \{h_j^{(0)} | 1 \leq j \leq 5\}$.

For $t = 1$, we consider $H(1, [0 : 9])$:

$$\begin{pmatrix} 0 & \alpha & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

which lies in the row space of $H^{(1)}$. Since $H(1, 1) \neq 0$ and $H(1, 2) = H(1, 3) = \cdots = H(1, 6) = 0$, it follows that $h_7^{(1)} \notin \{h_j^{(1)} | 2 \leq j \leq 6\}$.

For the remaining case of $t = 2$, we consider the submatrix $H([0 : 2], [0 : 10])$:

$$\begin{pmatrix} \alpha & 0 & 0 & 0 & 0 & 1 & 0 & \alpha & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & \alpha & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

whose rows belong to the row space of $H^{(2)}$. By inspecting rows 0 and 2 of this matrix, it can be inferred that the vector:

$$(-\alpha & 0 & \alpha & 0 & 0 & 0 & 0 & 0 & -\alpha & 0 & 1)$$

lies in the row space of $H^{(2)}$. Now, applying similar arguments as in the cases of $t = 0$ and $t = 1$, it follows that $h_7^{(2)} \notin \{h_j^{(2)} | 3 \leq j \leq 7\}$.

2) Property B2: Here, we need to show that $H(\cdot, [t : t + 5])$ is invertible for all $t \in [3 : 6]$. Note that:

$$H(\cdot, [3 : 8]) = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \alpha \\ 0 & 0 & 0 & 0 & 1 \alpha \\ 0 & 0 & 0 & 0 & 1 \alpha \\ s_{0,3} & s_{0,4} & s_{0,5} & 1 & 0 \\ s_{1,3} & s_{1,4} & s_{1,5} & 0 & 0 \\ s_{2,3} & s_{2,4} & s_{2,5} & 0 & 1 \end{bmatrix}.$$  

Since $\alpha \in \mathbb{F}_2 \setminus \mathbb{F}_2^*$ and all other entries of $H(\cdot, [3 : 8])$ are from $\mathbb{F}_2^*$, it follows that $[H(\cdot, [3 : 8])] \neq 0$ if $|H([1 : 5], [3 : 7])| \neq 0$. Now, we observe that:

$$|H([1 : 5], [3 : 7])| = - \begin{bmatrix} s_{0,3} & s_{0,4} & s_{0,5} \\ s_{1,3} & s_{1,4} & s_{1,5} \\ s_{2,3} & s_{2,4} & s_{2,5} \end{bmatrix} \neq 0,$$

as any square sub-matrix of $S$ is invertible. Hence, $H(\cdot, [3 : 8])$ is invertible. Similar arguments can be used to prove the invertibility of the matrices $H(\cdot, [4 : 9])$, $H(\cdot, [5 : 10])$, and $H(\cdot, [6 : 11])$.

### V. Establishing Random Erasure Recovery for Construction 1

In this section, we show that the p-c matrix $H$ provided in Construction 1 satisfies the random erasure recovery properties R1 and R2.

#### A. Proof of Property R1

Fix $t \in [0 : \delta - 1]$. Let $A \subseteq [t : t + \tau]$ with $|A| \leq \alpha$ and $t \in A$. In terms of the p-c matrix, the requirement (see Sec. II-E) is that:

$$h_\ell^{(t)} \notin \{h_j^{(t)} | j \in A \setminus \{t\}\}.$$  

Let $\tilde{H}^{(t)}$ be some matrix whose rows lie in the row space of $H^{(t)}$. Let $\tilde{h}_j^{(t)}$ denote the j-th column of $\tilde{H}^{(t)}$. It is sufficient to show that there exists such an $\tilde{H}^{(t)}$ so that:

$$\tilde{h}_j^{(t)} \notin \{\tilde{h}_j^{(t)} | j \in A \setminus \{t\}\}.$$  

Towards constructing $\tilde{H}^{(t)}$, consider the following two sub-matrices of $H$:

$$H(t, :) = \begin{bmatrix} 0 & \cdots & 0 \\ 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{bmatrix}$$

and

$$H([\delta : b - 2], :) = \begin{bmatrix} \cdots & \cdots & \cdots & \cdots \\ (a - 1) \times (\tau + 1 - a) & I_{(a - 1)} & 0 \\ (a - 1) \times (\delta + 1) \end{bmatrix}.$$  

In (18), *’s denote the entries of row $t$ of $P$. However, in this proof of property R1 (and in the subsequent proof of property R2), the specific structure of $P$ does not play any role and we only use the fact that *’s belong to the subfield $\mathbb{F}_q \subseteq \mathbb{F}_{q^2}$.
We use the $\diamond$ symbol in (18) as a placeholder for either $\alpha$ (if $t = 0$) or else, 1 (if $t \in [1 : \delta - 1]$). The matrix $S'$ in (19) is a sub-matrix of the full superregular matrix $S$ (defined as part of the p-c matrix $H$ presented earlier in Sec. III) and hence is a full superregular matrix by itself. Let $R_t \triangleq \{t\} \cup \{\delta : b - 2\}$. It can be inferred from (18) and (19) that the last ($\delta - t$) columns of the sub-matrix $H(R_t, :)$ are all zero columns. Hence, rows of $H(R_t, [0 : t + \tau])$ belong to the row space of $H(t)$ and we set

$$\tilde{H}(t) = H(R_t, [0 : t + \tau]).$$

In Fig. 3, an illustration of the structure of $\tilde{H}(t)$ is provided. Now, to prove (17), assume the contrary statement that:

$$\sum_{j \in A \setminus \{t\}} a_j \tilde{h}_j = 0. \quad (20)$$

For convenience of notation, let $\tilde{h}_j'$ denote the $j$-th column of $H([\delta : b - 2], :)$. If one restricts the attention to rows $[\delta : b - 2]$ of $H$, it follows from (20) that:

$$\tilde{h}_j' = \sum_{j \in A \setminus \{t\}} a_j \tilde{h}_j'. \quad (21)$$

It can be inferred from (19) that the initial $\tau$ columns $\{\tilde{h}_j' \mid i \in [0 : \tau - 1]\}$ are non-zero and all other $\tilde{h}_j'$'s are zero column vectors. Moreover, any $(\alpha - 1)$ non-zero columns are linearly independent. In particular, as $t \in [0 : \delta - 1]$, the column vector $\tilde{h}_j'$ is non-zero. Together with the fact that $|A| \leq \alpha$, for (21) to be true, it should be that $\{\tilde{h}_j' \mid j \in A \setminus \{t\}\}$ is an independent set consisting of $|A \setminus \{t\}| = \alpha - 1$ elements. Furthermore, as columns $\{\tilde{h}_j' \mid i \in [\tau : \tau + \delta]\}$ are zero columns, $A \subseteq [t : \tau - 1]$. We now observe that all the column vectors appearing in (21) are over $F_q \subseteq F_{q^2}$. From the independence of the column vectors on the RHS of (21), it now follows that $\{a_j \mid j \in A \setminus \{t\}\} \subseteq F_q \subseteq F_{q^2}$. We will now revisit (20) and observe that the first element of the column vector on the LHS of (20) is $\alpha \in F_{q^2} \setminus F_q$ whereas the first element of each column vector on the RHS belongs to $F_q$. Since $\{a_j \mid j \in A \setminus \{t\}\} \subseteq F_q$, the assumption made in (20) is now invalidated. This completes our proof of property R1.

### B. Proof of Property R2

We need to show that for any $A \subseteq [\delta : \tau + \delta]$ with $|A| \leq a$, the set of columns $\{\tilde{h}_j \mid j \in A\}$ is linearly independent. Assume to the contrary that there exists an $A$ and coefficients $\{a_j \mid j \in A\}$ (with $a_j \neq 0$ for some $j$) such that:

$$\sum_{j \in A} a_j \tilde{h}_j = 0. \quad (22)$$

We will divide the proof into two cases.

**Case-1:** Here we consider the scenario that $|A \cap \{\tau, \tau + \delta\}| \leq 1$, i.e., $\{\tau, \tau + \delta\}$ are not present together in $A$. Consider the matrix $H_B = H([\delta : b - 1], :)$ which takes the form:

$$\begin{bmatrix}
\begin{array}{c|c|c}
|a| & I & 0 \\
\hline
S & 0 & 0 \\
\end{array}
\end{bmatrix} \quad (23)$$

Let $h''_i$ denote the column $i$ of $H_B$. Clearly, from (22), we now have:

$$\sum_{j \in A} a_j h''_j = 0. \quad (24)$$

We will now partition $A$ into two sets $A_1 \triangleq A \setminus \{\tau + 1 : \tau + \delta - 1\}$ and $A_2 \triangleq A \cap \{\tau + 1 : \tau + \delta - 1\}$. As $h''_j = 0$ for all $j \in A_2$, we can rewrite (24) as:

$$\sum_{j \in A_1} a_j h''_j = 0. \quad (25)$$

It can be observed from (23) that any set of $a$ non-zero columns (without any column repeated) of $H_B$ form an independent set. As $|A \cap \{\tau, \tau + \delta\}| \leq 1$, we do not have any repeating non-zero columns among $\{h''_j \mid j \in A\}$. As $|A_1| \leq |A| \leq a$ and since $\{h''_j \mid j \in A_1\}$ consists of all the non-zero columns among $\{h''_j \mid j \in A\}$, clearly, $\{h''_j \mid j \in A_1\}$ should form an independent set. From (25), it follows that $a_j = 0$ for all $j \in A_1$. As a result, we will now rewrite (22) as:

$$\sum_{j \in A_2} a_j \tilde{h}_j = 0. \quad (26)$$
Consider the sub-matrix $H(:, [\tau : \delta + \tau])$ consisting of the last $\delta + 1$ columns of $H$, which takes the form:

$$
\begin{bmatrix}
\alpha & 0 & \cdots & 0 & 0 \\
0 & \vdots & \ddots & \vdots & \vdots \\
0 & \vdots & \ddots & 0 & 0 \\
0 & 0 & \cdots & 0 & 1 \\
\end{bmatrix}
$$

It can be observed that these $\delta + 1$ columns, namely $\{h_j | j \in \{\tau : \delta + \tau\}\}$, form an independent set. As $A_2 \subseteq \{\tau + 1 : \tau + \delta - 1\} \subseteq \{\tau : \tau + \delta\}$, it follows that the columns $\{h_j | j \in A_2\}$ are linearly independent and hence (26) implies that $a_j = 0$ for all $j \in A_2$. Hence, in summary, we have $a_j = 0$ for all $j \in A$, which contradicts our assumption that $a_j \neq 0$ for some $j \in A$.

**Case-2:** Here we consider the remaining scenario of $|A \cap \{\tau, \tau + \delta\}| = 2$. As in case-1, we will begin with the contrary assumption that there exists a set of coefficients $\{a_j | j \in A\}$, not all of them zero, satisfying (22). We will now restrict our attention to the rows $[\delta : b - 1]$ of $H$ (see the matrix in (23)).

Recall our definitions of $A_1, A_2$ introduced in the proof of case-1. From (25), we have:

$$
0 = \sum_{j \in A_1} a_j h'_j = \left( \sum_{j \in A_1 \setminus \{\tau, \tau + \delta\}} a_j h'_j \right) + (a_{\tau} + a_{\tau + \delta}) h''_r.
$$

(27)

Here we used the fact that $h''_r = h''_{\tau + \delta}$. As $\{h'_j | j \in A_1 \setminus \{\tau, \tau + \delta\}\}$ form a linearly independent set, from (27), it follows that $a_j = 0$ for $j \in A_1 \setminus \{\tau, \tau + \delta\}$. As a result, we can now rewrite (22) as:

$$
\sum_{j \in A_2} a_j h'_j + a_{\tau} h''_r + a_{\tau + \delta} h''_{\tau + \delta} = 0.
$$

As $A_2 \subseteq \{\tau + 1 : \tau + \delta - 1\}$ and since the set of $\delta + 1$ consecutive columns $\{h_j | \tau \leq i \leq \tau + \delta\}$ is linearly independent (shown earlier in the proof of case 1), it should be that $a_j = 0$ for $j \in A_2 \cup \{\tau, \tau + \delta\}$. This contradicts our initial assumption that $a_j \neq 0$ for some $j \in A$ and hence completes the proof.

**VI. Establishing Burst Erasure Recovery for Construction 1**

We will now show that Construction 1 satisfies the burst erasure recovery properties $B1, B2$ by assuming that the $(\delta \times (\tau - b))$ matrix $P = P_{\delta, \tau - b}$ is a permissible matrix, as stated in Lemma 3. The proof of Lemma 3 appears in Sec. VII.

**A. Proof of Property $B1$**

In property $B1$, we are interested in the recovery of code symbol $c_t$, where $t \in [0 : \delta - 1]$, from a burst erasure confined to $[t : t + b - 1]$ by accessing the non-erased code symbols having index $\leq t + \tau$. In terms of the columns of $H^{(t)}$, the equivalent requirement (see Sec. II-E) is that:

$$
\hat{h}_{\tau}^{(t)} \notin \{h_j^{(t)} | t + 1 \leq j \leq t + b - 1\},
$$

Let $\hat{H}^{(t)}$ be some matrix whose rows lie in the row space of $H^{(t)}$. Let $\hat{h}_{\tau}^{(t)}$ denote the $\tau$-th column of $\hat{H}^{(t)}$. It is sufficient to show that for all $t \in [0 : \delta - 1]$ there exists a $\hat{H}^{(t)}$ such that:

$$
\hat{h}_{\tau}^{(t)} \notin \{h_j^{(t)} | t + 1 \leq j \leq t + b - 1\}.
$$

(29)

We observe that $H([0 : t], :)$ takes the form:

$$
\begin{bmatrix}
\alpha I_{t+1} & 0_{(t+1) \times (\delta-1)} & 0_{(t+1) \times \alpha} & P([0 : t], :) & 0_{(t+1) \times (\alpha - 1)} & 0_{(t+1) \times (\delta - \alpha)}
\end{bmatrix},
$$

where $D_{2} = D_{2}([0 : t], [0 : t])$ (see (2) for the definition of the $(\delta \times \delta)$ diagonal matrix $D_{2}$). The last $(\delta - t)$ columns of $H([0 : t], :)$ are all zero columns and hence rows of $H([0 : t], [0 : t + \tau])$ belong to the row space of $H^{(t)}$. We choose

$$
\hat{H}^{(t)} = H([0 : t], [0 : t + \tau]).
$$

We will now show that this choice of $\hat{H}^{(t)}$ satisfies (29).

1) $t = 0$: Here, the matrix of interest is:

$$
\hat{H}^{(0)} = H(0, [0 : \tau]) = \alpha \begin{bmatrix}
0 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & 0 \\
\end{bmatrix}
$$

where *'s denote the entries of $P$. Clearly, (29) is true for this case as $H(0, 0) \neq 0$ and $H(0, j) = 0$, for all $j \in [1 : b - 1]$.

2) $t \in [1 : \min(\tau - b, \delta - 1)]$: In this case, we have:

$$
\hat{H}^{(t)}(\tau, [t : t + b - 1]) = H([0 : t], [t : t + b - 1])
$$

$$
= \begin{bmatrix}
0 & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & 0 \\
\end{bmatrix}
$$

$$
\alpha
$$

We illustrate this $(t + 1) \times b$ matrix in Fig. 4. Observe that:

$$
\hat{h}_{\tau}^{(t)} = \begin{cases}
0 & j \in [t + 1 : b - 1], \\
P([0 : t], j - b) & j \in [b : t + b - 1].
\end{cases}
$$
Hence to prove (29), we only need to show that:

\[
\begin{pmatrix}
0 \\
\vdots \\
0
\end{pmatrix}
\notin \{P(0 : t), b - b | b \leq j \leq t + b - 1\}.
\]  
(30)

By the top-left property, the \((t \times t)\) matrix \(P([0 : t], [0 : t - 1])\) is invertible. As a result, there does not exist a non-trivial linear combination of the columns of \(P([0 : t], [0 : t - 1])\) which yields a column vector having zeros in the first \(t\) rows and hence (30) is true.

We have now covered all the B1 scenarios when \(\tau - b \geq \delta - 1\). For the case when \(\tau - b < \delta - 1\), we need to prove the recoverability of \(c_t\) for \(t \in [\tau - b + 1 : \delta - 1]\).

3) \(t \in [\tau - b + 1 : \delta - 1]\): Since \(t \geq \tau - b + 1\), the \((t + 1) \times b\) matrix \(\hat{H}(t)(\cdot, [t : t + b - 1])\) involves some columns from \(D_2\). We have:

\[
\hat{H}(t)(\cdot, [t : t + b - 1]) = \begin{bmatrix}
0 \\
\vdots \\
0
\end{bmatrix} P([0 : t], \cdot) \begin{bmatrix}
\sum_{j=0}^{(t+1) \times (b-1)} \delta \\
0
\end{bmatrix}
\]

where \(D = D_2([0 : t - \tau + b - 1], [0 : t - \tau + b - 1])\). We illustrate the structure of \(\hat{H}(t)(\cdot, [t : t + b - 1])\) in Fig. 5.

Since \(L_j^{(t)} = 0\) for all \(j \in [t + 1 : b - 1]\), to prove (29), it suffices to show that:

\[
\begin{pmatrix}
0 \\
\vdots \\
0
\end{pmatrix} \notin \{L_j^{(t)} | b \leq j \leq t + b - 1\}.
\]  
(31)

From the consecutive-rows property, we have that the \((\tau - b) \times (\tau - b)\) matrix \(P([t - \tau + b : t - 1], \cdot)\) is invertible. The \((t - \tau + b) \times (t - \tau + b)\) matrix \(D\) is a diagonal matrix with all its entries non-zero and is thus invertible. Note that \(\hat{H}(t)([t - \tau + b : t - 1], [\tau : t + b - 1])\) is an all zero matrix. It follows that \(\hat{H}(t)([0 : t - 1], [b : t + b - 1])\) is an invertible matrix. Thus, there does not exist a non-trivial linear combination of the columns of \(\hat{H}(t)([0 : t - 1], [b : t + b - 1])\) which yields a column vector having zeros in the first \(t\) rows and hence (31) is true.

### B. Proof of Property B2

Here, we need to show that the \((b \times b)\) sub-matrices \(H(:, [t : t + b - 1]) \mid t \in [\delta : \tau - a + 1]\) are all invertible.

1) \(t \in [\delta : \tau - b]\): Recall the definition of \(\hat{P}\) presented in Sec. III-B. For \(t \in [\delta : \tau - b]\), we have:

\[
H(:, [t : t + b - 1]) = \begin{bmatrix}
\hat{P}([0 : \delta - 1], [t - \delta : t + b - 1 - \delta]) \\
H([\delta : b - 1], [t : t + b - 1])
\end{bmatrix}
\]

From the consecutive-columns property defined in Sec. III-B, there exists an \(a\)-element set \(A \subseteq [t - \delta : t + b - 1 - \delta]\) such that \(\hat{P}([0 : \delta - 1], A) = 0\) and \(\hat{P}([0 : \delta - 1], [t - \delta : t + b - 1 - \delta] \setminus A)\) is invertible. The determinant of \(H(:, [t : t + b - 1])\) is therefore given by:

\[
\pm|\hat{P}(:, [t - \delta : t + b - 1 - \delta] \setminus A)||H([\delta : b - 1], A + \delta)| \neq 0.
\]

This follows as \(H([\delta : b - 1], [0 : \tau])\) is a \(p\)-c matrix of a \([\tau + 1, \tau + a] \times MDS\) code and hence any \(a\) columns of \(H([\delta : b - 1], [0 : \tau])\) are linearly independent.

2) \(t \in [\max(\tau - b + 1, \delta), \tau - a]\): The \((b \times b)\) sub-matrix \(H(:, [t : t + b - 1])\) for this case is as shown below:

\[
\begin{bmatrix}
\hat{P}([0 : \delta - 1], [t - \delta : \tau - \delta - 1]) \\
H([\delta : b - 1], [t : \tau])
\end{bmatrix} = \begin{bmatrix}
\alpha & 0 \cdots 0 \\
0 & I_{t+b-\tau-1}
\end{bmatrix}
\]

Let \(\theta = (\tau - t - a)\). The \((b \times b)\) matrix \(H(:, [t : t + b - 1])\) is invertible if the \(((\theta + a) \times (\theta + a))\) sub-matrix \(M_\theta\) shown below is invertible.

\[
\hat{M}_\theta = \begin{bmatrix}
R_\theta \\
H([\delta : b - 1], [t : \tau - 1])
\end{bmatrix}
\]

where \(R_\theta = \hat{P}([\delta - \theta : \delta - 1], [\tau - b - \theta : \tau - \delta - 1])\) is the \((\theta \times (\theta + a))\) bottom right submatrix of \(\hat{P}\) as defined in Sec. III-B. This can be argued as follows. Let \(J_t \triangleq \{0\} \cup [t + b - \tau : b - 1]\). Since

\[
H([1 : t + b - \tau - 1], [\tau + 1 : t + b - 1]) = I_{t+b-\tau-1}
\]

and

\[
H(J_t, [\tau + 1 : t + b - 1]) = 0,
\]

it is clear that \(H(:, [t : t + b - 1])\) is invertible if the \(((\theta + a + 1) \times (\theta + a + 1))\) matrix \(H(J_t, [t : \tau])\) is invertible. Note that \(H(J_t, [t : \tau])\) takes the form:

\[
H(J_t, [t : \tau]) = \begin{bmatrix}
* & \cdots & * & \alpha \\
* & \cdots & * & *
\end{bmatrix}
\]
where $* \times$ is used as a placeholder for the elements in the row and column containing $\alpha$. All entries of $H(J_1 \{t : \tau \})$ except $\alpha$ are from $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q \setminus \mathbb{F}_q$. The determinant of $H(J_1 \{t : \tau \})$ can thus be written as:

$$|H(J_1 \{t : \tau \})| = \pm \alpha |\tilde{\mathcal{M}}_0| + x$$

where $x \in \mathbb{F}_q$, and hence

$$|H(J_1 \{t : \tau \})| \neq 0 \text{ if } |\tilde{\mathcal{M}}_0| \neq 0.$$

We will now show that $\tilde{\mathcal{M}}_0$ is invertible using the bottom-right property defined in Sec. III-B. From the bottom-right property, there is an $a$-element set $\mathcal{A} \subseteq \{0 : \theta + a - 1\}$ such that $R_{\theta}(\{0 : \theta - 1\}, \mathcal{A}) = 0$ and $R_{\theta}(\{0 : \theta - 1\}, \{0 : \theta + a - 1\} \setminus \mathcal{A})$ is invertible. Moreover, any $a$ columns of the sub-matrix $H(\{\delta : b - 1\}, \{0 : \tau \})$ are linearly independent. Therefore:

$$(\tilde{\mathcal{M}}_0) = \pm |R_{\theta}(\{0 : \theta - 1\}, \{0 : \theta + a - 1\} \setminus \mathcal{A})||H(\{\delta : b - 1\}, \mathcal{A} + \theta)\| \neq 0.$$

3) $t = \tau - a + 1$: The $(b \times b)$ sub-matrix formed by the last $b$ columns of $H$ takes the form:

$$H(:, [\tau + 1 - a : \tau + \delta]) = \begin{bmatrix} X & 0 & \cdots & 0 \\ \vdots & I_{a} & \cdots & 0 \\ 0 & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

where $X$ is some matrix. Observe that

- $H([0 : \delta - 1] \cup \{b - 1\}, [\tau : \tau + \delta])$ is an invertible matrix,
- $H([\delta : b - 2], [\tau : \tau + \delta])$ is a zero matrix, and
- $H([\delta : b - 2], [\tau + 1 - a : \tau - 1]) = I_{a-1}.$

It follows that $H(:, [\tau + 1 - a : \tau + \delta])$ is invertible.

VII. PROOF THAT RECURSIVE $\{0, 1\}$ CONSTRUCTION YIELDS A PERMISCELLAIRE MATRIX

In this section, we prove that the $\delta \times (\tau - b)$ matrix $P = P_{\delta, \tau-b}^u$ is a permisscribible matrix by showing that it satisfies the four properties listed in Sec. III-B. Before proving the general case, we first show an example.

Example 4: ($a = 2, b = 5, \tau = 12$)

For parameters $\delta = 3, \tau - b = 7$ and $a = 2$, we have:

$$P = P_{3,7}^2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

By attaching two all-zero columns at the beginning, we get:

$$\hat{P} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}.$$ 

1) Top-Left Property: For this example, top-left property requires that $P([0 : \theta - 1], [0 : \theta - 1])$ is invertible for all $\theta \in [1 : 3]$. Clearly, this is true since:

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

are all invertible.

2) Consecutive-Rows Property: Since $\delta = 3 < \tau - b = 7$, the consecutive-rows property can be ignored for this example.

3) Consecutive-Columns Property: This property can be verified by observing that all the following $(3 \times 5)$ sub-matrices of $P$ have 2 all-zero columns and the remaining 3 columns form a $(3 \times 3)$ invertible matrix:

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$ 

4) Bottom-Right Property: Here, we have:

$$R_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}, R_2 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{bmatrix}. $$

It can be easily verified that for each $R_{\theta}$, we have $a$ zero columns and the remaining $\theta$ columns are linearly independent.

Now, we will present the proof for the general case. Let:

$$\tilde{P}_{u,v}^a = \begin{bmatrix} 0 & P_{u,v}^a \end{bmatrix}.$$ 

A. Top-Left Property

To show the top-left property, it suffices to set $u = \delta$ and $v = \tau - b$ in the Lemma 4 below.

Lemma 4: The $(\theta \times \theta)$ matrix $P_{u,v}^a([0 : \theta - 1], [0 : \theta - 1])$ is non-singular for all $\theta \in [1 : \min\{u, v\}].$

Proof: From the definition of $P_{u,v}^a$, it can be seen that:

$$P_{u,v}^a([0 : \theta - 1], [0 : \theta - 1]) = I_{\theta},$$

which is non-singular.

B. Consecutive-Rows Property

Setting $u = \delta$ and $v = \tau - b$ in the Lemma 5 below yields the consecutive-rows property.

Lemma 5: If $v \leq u$, then the sub-matrices formed by any $v$ consecutive rows of $P_{u,v}^a$ are non-singular.

Proof: Let $u = xv + y$, where $0 \leq y < v$ and $x \geq 1$. Then, $P_{u,v}^a$ has the following form:

$$P_{u,v}^a = \begin{bmatrix} I_y \\ \vdots \\ I_y \end{bmatrix} P_{y,v}^a([0 : y - 1], [y : y - 1]).$$

It follows that any $u$ consecutive rows are linearly independent in the above matrix.

We use this lemma in the proof of the bottom-right property as well.
C. Consecutive-Columns Property

Setting \( u = \delta \) and \( v = \tau - b \) in Lemma 6 results in the consecutive-columns property.

**Lemma 6:** Suppose \( u \geq v \). Pick any collection of \( u+a \) consecutive columns of \( \hat{\mathcal{P}}^a_{u,v} \). There must be \( a \) all-zero columns among them and the remaining \( u \) columns form an \((u \times u)\) invertible matrix.

**Proof:** Let \( v + a = x(u + a) + y \), where \( 0 \leq y < u + a \) and \( x \geq 1 \). If \( y \leq a \), then

\[
\hat{\mathcal{P}}^a_{u,v} = \begin{bmatrix}
0_{(u \times a)} & I_u & 0_{(u \times a)} & \cdots & 0_{(u \times a)} & I_u & 0_{(u \times a)}
\end{bmatrix}.
\]

If \( a < y < u + a \), then:

\[
\hat{\mathcal{P}}^a_{u,v} = \begin{bmatrix}
0_{(u \times a)} & I_u & 0_{(u \times a)} & \cdots & 0_{(u \times a)} & I_u & P^a_{u,y-a}
\end{bmatrix}
\]

with

\[
P^a_{u,y-a} = \begin{bmatrix}
I_{y-a} \\
P^a_{u-y+a,y-a}
\end{bmatrix}.
\]

In both cases, it can be seen that among any \( u + a \) consecutive columns, there are \( a \) all-zero columns and the remaining \( u \) columns are linearly independent. □

D. Bottom-Right Property

Setting \( u = \delta \) and \( v = \tau - b \) in Lemma 7 results in the bottom-right property.

**Lemma 7:** For all \( \theta \in [1 : \min\{u, v\}] \), let

\[
R^a_{u,v,\theta} = \hat{\mathcal{P}}^a_{u,v}([u - \theta : u - 1], [v - \theta : v + a - 1]).
\]

Then, \( R^a_{u,v,\theta} \) contains \( a \) all-zero columns and the \( \theta \) remaining columns of \( R^a_{u,v,\theta} \) are linearly independent.

**Proof:** Suppose \( u \leq v \leq u + a \). In this scenario, we have:

\[
\hat{\mathcal{P}}^a_{u,v} = \begin{bmatrix}
0_{(u \times a)} & I_u & 0_{(u \times (v-u))}
\end{bmatrix}.
\]

It can be verified that in the \( R^a_{u,v,\theta} \) matrix formed by picking the bottom right \((\theta \times (\theta + a))\) sub-matrix of \( \hat{\mathcal{P}}^a_{u,v} \), there are \( a \) all-zero columns and the remaining \( \theta \) columns form an invertible matrix. Thus, Lemma 7 is true when \( u \leq v \leq u + a \). We prove the lemma for the rest of the parameter ranges by induction.

**Induction Assumption:** Suppose that for all \( \theta \in [1 : \min\{u', v'\}] \), \( R^a_{u',v',\theta} \) contains \( a \) all-zero columns and the remaining \( \theta \) columns are linearly independent, provided \( (u', v') \) are such that:

- either \( u' < u \) and \( v' = v \), or
- \( u' = u \) and \( v' < v \).

**Base Case:** To prove Lemma 7, it suffices to show that \( R^a_{u,v,\theta} \) satisfies the requirements of Lemma 7, if the induction assumption is true. The recursion in the definition of \( \hat{\mathcal{P}}^a_{u,v} \) always ends in the base case of \( u \leq v \leq u + a \). We have already proved that \( R^a_{u,v,\theta} \) possesses the required properties for the base case.

**Induction Step:** We divide the proof into \( v > u + a \) and \( v < u \) cases based on the expansion of \( R^a_{u,v,\theta} \).

1) \( v > u + a \): Here, we have:

\[
\hat{\mathcal{P}}^a_{u,v} = \begin{bmatrix}
0_{(u \times a)} & I_u & 0_{(u \times (v-u))}
\end{bmatrix}.
\]

In this case, \( \min\{u, v\} = u \), and so we need to consider \( \theta \in [1 : u] \). If \( \theta \leq u - a \), then \( R^a_{u,v,\theta} \) is contained inside \( \hat{\mathcal{P}}^a_{u,v-u-a} \) and hence:

\[
R^a_{u,v,\theta} = R^a_{u,v-u-a,\theta}.
\]

By the induction assumption, the lemma is true for this case.

Now consider any \( \theta \in [v - u - a + 1 : u] \) and let \( x = \theta - (v - u - a) \geq 1 \). In this case, \( R^a_{u,v,\theta} \) involves \( x \) columns to the left of \( \hat{\mathcal{P}}^a_{u,v-u-a} \). An illustration of the structure of \( R^a_{u,v,\theta} \) is provided in Fig. 6. We first note that:

\[
R^a_{u,v,\theta}([0 : \theta - 1], [x : x + a - 1]) = 0_{(\theta \times a)}.
\]

Thus, \( R^a_{u,v,\theta} \) has \( a \) all-zero columns. Now, inspecting the remaining \( \theta \) columns indexed by \([0 : x - 1] \cup [x + a : \theta + a - 1]\), it can be inferred that:

\[
R^a_{u,v,\theta}([0 : \theta - x - 1], [0 : x - 1]) = 0_{(\theta-x) \times x} \quad \text{and}
\]

\[
R^a_{u,v,\theta}([\theta - x : \theta - 1], [0 : x - 1]) = I_x.
\]

Consider the \((\theta-x) \times (\theta-x)\) matrix \( M \) defined as follows:

\[
M = R^a_{u,v,\theta}([0 : \theta - x - 1], [x + a : \theta + a - 1]).
\]

It follows from the structure of \( R^a_{u,v,\theta} \) that if \( M \) is invertible then the \((\theta \times \theta)\) matrix \( R^a_{u,v,\theta}([0 : \theta - 1], [0 : x - 1] \cup [x + a : \theta + a - 1]) \) is invertible. By definition,

\[
M = P^a_{u,v-u-a}([u - \theta : u - x - 1], :).
\]

Therefore, \( M \) is a square matrix formed by \((\theta-x) = (u-u-a)\) consecutive rows of \( P^a_{u,v-u-a} \). It follows from Lemma 5 that \( M \) is invertible.
Construction 1, is a p-c matrix of \( H \tau \alpha \):
\[
\begin{bmatrix}
0 & I \\
\hat{M} & \hat{X}
\end{bmatrix}
\]

Fig. 7. Structure of \( R_{u,v}^a \) when \( v < u \) and \( y = \theta - (u - v) \geq 1 \). Here \( \hat{X} \) is some \( (\theta - y) \times y \) matrix.

2) \( v < u \): For this case, we have:
\[
\hat{P}_{u,v}^a = \begin{bmatrix}
0 & \hat{I}_v \\
\hat{P}_{u-v,v}^a & \hat{I}_v
\end{bmatrix}
\]

Since \( v < u \), \( \min\{u,v\} = v \), and so \( \theta \in [1 : v] \). If \( \theta \leq u - v \), then \( R_{u,v,\theta} \) is contained in \( R_{u-v,v}^a \) and hence:
\[
R_{u,v,\theta}^a = R_{u-v,v,\theta}^a.
\]

It follows from the induction assumption that the lemma holds for this case. Now consider any \( \theta \in [u - v + 1 : v] \) and let \( y = \theta - (u - v) \geq 1 \). In Fig. 7, we provide an illustration of the structure of \( R_{u,v,\theta}^a \). It can be easily verified that:
\[
R_{u,v,\theta}^a([0 : y - 1],[0 : \theta + a - y - 1]) = \begin{bmatrix} 0 \end{bmatrix}_{y \times (\theta + a - y)} \quad \text{and} \quad R_{u,v,\theta}^a([0 : y - 1],[\theta + a - y : \theta + a - 1]) = \hat{I}_y.
\]

Consider the \((\theta - y) \times (\theta + a - y)\) matrix \( \hat{M} \) defined as follows:
\[
\hat{M} = R_{u,v,\theta}^a([y : \theta - 1],[0 : \theta + a - y - 1])
\]

We note that \( \hat{M} \) is formed by \( (\theta + a - y) = (u - v + a) \) consecutive columns of \( R_{u-v,v}^a \). By Lemma 6, \( \hat{M} \) has \( a \) all-zero columns and the remaining \((u - v)\) columns form an invertible matrix. It follows that \( R_{u,v,\theta}^a \) has \( a \) all-zero columns and the other \((u - v + y) = \theta\) columns of \( R_{u,v,\theta}^a \) are linearly independent.

### Table I

| (a, b, \( \tau \)) | r | R | \( R_{\text{opt}}^a \) | \( q^2 \) | \( q^2_\alpha \) |
|---------------------|---|---|-------------------|---|---|
| (2.4, 6)            | 3 | 0.4444 | 0.5555 | 4 | 49 | 64 |
| (2.4, 12)           | 4 | 0.6 | 0.7333 | 4 | 169 | 256 |
| (2.4, 12)           | 3 | 0.6666 | 0.7333 | 16 | 169 | 256 |
| (2.6, 30)           | 5 | 0.7428 | 0.8285 | 4 | 961 | 1296 |
| (2.6, 30)           | 4 | 0.7714 | 0.8285 | 9 | 961 | 1296 |
| (2.6, 30)           | 3 | 0.8 | 0.8285 | 25 | 961 | 1296 |
| (3.1, 11)           | 5 | 0.5 | 0.6428 | 4 | 121 | 169 |
| (3.1, 11)           | 4 | 0.5714 | 0.6428 | 16 | 121 | 169 |
| (3.6, 16)           | 6 | 0.55 | 0.7 | 4 | 256 | 361 |
| (3.6, 16)           | 5 | 0.6 | 0.7 | 9 | 256 | 361 |
| (4.6, 13)           | 6 | 0.65 | 0.7 | 16 | 256 | 361 |
| (4.6, 13)           | 5 | 0.5625 | 0.625 | 49 | 169 | 256 |
| (4.8, 45)           | 11 | 0.7 | 0.84 | 4 | 2209 | 2401 |
| (4.8, 45)           | 8 | 0.76 | 0.84 | 16 | 2209 | 2401 |
| (4.8, 45)           | 6 | 0.8 | 0.84 | 64 | 2209 | 2401 |

### VIII. Sub-Optimal Construction With Further Reduced Field Size

As noted earlier in Section III-A, the \( a \times (\tau + 1) \) submatrix \( H([\delta : b - 1],[0 : \tau]) \) of the p-c matrix \( H \) given by Construction 1, is a p-c matrix of a \([\tau + 1, \tau + 1 - a] \) MDS code. The property of MDS code used in our proof is that any collection of \( a \) columns of \( H([\delta : b - 1],[0 : \tau]) \) forms a linearly independent set. Suppose there exists \([\tau + 1, \tau + 1 - r, d_{\min} \geq a + 1]_q \) scalar code \( C \). Since \( d_{\min} \geq a + 1 \), any set of \( a \) columns of a p-c matrix of \( C \) will also form a linearly independent set. Using this p-c matrix instead of that of an MDS code, we will now construct a p-c matrix of a new \([\tau + 1 - a + b, \tau + 1 - r]_q \) scalar code. Diagonal embedding of this new code results in an \((a, b, \tau)\) streaming code over \( \mathbb{F}_q \) of rate \( R = \frac{\tau + 1 - r}{\tau + 1 - a + b} \), as stated in Theorem 2.

Construction 2: Let \([U I_y] \in \mathbb{F}_q^{\times \tau + 1} \) be a p-c matrix of an \([\tau + 1, \tau + 1 - r, d_{\min} \geq a + 1]_q \) scalar code \( C \). Let \( b = a, \delta \in \mathbb{F}_q^* \setminus \mathbb{F}_q \) and \( P_{\tau + b}^a \) be the permissible matrix given in Definition 3. We construct a p-c matrix \( H_C \) of an \([n = \tau + 1 + \delta, k = n - (\delta + r)]_q ^2 \) scalar code in a step-by-step manner:

- Initialize \( H_C \) to be the \((\delta + r) \times (\tau + 1 + \delta)\) all-zero matrix.
- Set \( H_C([0 : \delta - 1],[0 : \delta - 1]) = \alpha I_\delta \).
- Set \( H_C([0 : \delta - 1],[b : \tau - 1]) = P_{\delta,\tau-b}^a \).
- Set \( H_C(0, \tau) = \alpha \).
- Set \( H_C([1 : \delta - 1],[\tau + 1 : \tau + \delta - 1]) = I_{\delta - 1} \).
- Set \( H_C([\delta : \delta + r - 1],[0 : \tau - r]) = U \).
- Set \( H_C([\delta : \delta + r - 1],[\tau + 1 : r + 1]) = I_r \) and \( H_C(\delta + r - 1, \tau + \delta) = 1 \).

The top \( \delta \) rows of the p-c matrix \( H_C \) are given by:

\[
H_C([0 : \delta - 1],: ) = \begin{bmatrix} D_1 & Z_1 \end{bmatrix}_{\delta \times \delta} \begin{bmatrix} Z_1 \end{bmatrix}_{\delta \times \alpha} \begin{bmatrix} P \end{bmatrix}_{\delta \times (\delta - b)} \begin{bmatrix} D_2 \end{bmatrix}_{\delta \times \delta} \begin{bmatrix} Z_2 \end{bmatrix}_{\delta \times 1},
\]

where \( D_1, D_2 \) are diagonal matrices, \( P = P_{\delta,\tau-b}^a \) and \( Z_1, Z_2 \) are zero matrices as defined in (2). The bottom \( r \) rows...
of $H_C$ are as shown below:

$$H_C(\delta : \delta + r - 1, \cdot ) = \begin{bmatrix}
U_{(r \times (\tau + 1 - r))} & \tilde{D}_3_{(r \times r)} & \tilde{Z}_3_{(r \times (\delta - 1))} & \tilde{E}_{(r \times 1)}
\end{bmatrix},$$

where $\tilde{D}_3$ is a diagonal matrix and $\tilde{Z}_3$ is a zero matrix and $\tilde{E}$ is an identity vector defined as shown below:

$$\tilde{D}_3 = \begin{bmatrix}
1 & 1 & \ldots & 1
\end{bmatrix}_{(r \times r)},$$

$$\tilde{Z}_3 = \begin{bmatrix}
0 \\
\vdots \\
0 \\
1
\end{bmatrix}_{r \times (\delta - 1)}$$

and $\tilde{E} = \begin{bmatrix}
0 \\
\vdots \\
0 \\
1
\end{bmatrix}_{r \times 1}.$ (32)

If $C$ is an MDS code, then this p-c matrix is the same as that given by Construction 1.

**Theorem 2:** Diagonal embedding of the $[\tau + 1 + \delta, \tau + 1 - r]$ scalar code with $H_C$ as a p-c matrix results in an $(a, b, \tau)$ streaming code.

**Proof:** See Appendix I. $\Box$

1) **An Example:** For any finite field $\mathbb{F}_Q$, there exists the $[Q^2 + Q + 1, Q^2 + Q - 2, d_{\min} = 3]_Q$ Hamming code. Using Construction 2, one can obtain $(a = 2, b, \tau = Q^2 + Q)$ streaming codes over $\mathbb{F}_{Q^2}$ of rate $\frac{2 \delta - 2}{2 \tau + 2}$, which is close to the optimal rate $\frac{\tau - 1}{\tau - 1 + \tau}$. Thus, we have a family of $O(\tau)$ field size near-rate-optimizing streaming codes for $a = 2$.

In Table I, we compare the rate $R$ of some example streaming codes (obtained via Construction 2) with the optimal rate $R_{opt}$. From the code tables in [43], we pick the smallest $r$ such that a $[\tau + 1 + \delta, \tau + 1 - r]$ code with $d_{\min} \geq a + 1$ exists. We also compare the field size requirements of Construction 2, our rate-optimal code (Construction 1) and the previously best-known rate-optimal explicit code in [16].

**APPENDIX I**

**Proof of Theorem 2**

1) **Properties Required of the Scalar Code:** To show that the packet-level code constructed through diagonal embedding of the $[n = \tau + 1 + \delta, k = \tau + 1 - r]$ scalar code $C'$ (whose p-c matrix is given by Construction 2) is an $(a, b, \tau)$ streaming code, it suffices to show that the following properties hold for any codeword $[c_0, c_1, \ldots, c_{n-1}] \in C'$.

**S** \{ $c_t \mid 0 \leq t \leq \tau - r$ \} is an information set, thereby guaranteeing systematic encoding.

**B1** Any code symbol $c_t$ with $t \in [0 : \delta - 1]$ should be recoverable by accessing code symbols in the set $\{c_j \mid t + b \leq j \leq t + \delta + t \} \cup \{c_j \mid j < t\}$.

**B2** For any $t \in [\delta : \tau + 1 - a]$, code symbols $\{c_j \mid j \in [t : t + b - 1]\}$ should be recoverable by accessing remaining code symbols $\{c_j \mid j \notin [t : t + b - 1]\}$.

**R1** Any code symbol $c_t$ with $t \in [0 : \delta - 1]$ can be recovered using code symbols in the set $\{c_j \mid j \in [t : t + \tau] \} \cup \{c_j \mid j < t\}$, for all $A \subseteq [t : t + \tau]$ such that $t \in A$ and $|A| = a$.

**R2** For any set $A \subseteq [\delta : \tau + \delta]$ with $|A| = a$, code symbols $\{c_j \mid j \in A\}$ should be recoverable by accessing the remaining code symbols $\{c_j \mid j \notin A\}$.

We remark that the properties B1, B2, R1 and R2 described here are the same as those stated in Sec II-D.

2) **Proof of Properties:** Here we will show that the scalar code $C'$ with $H_C$ as p-c matrix satisfies all the properties given above. Since the $[\tau + 1, \tau + 1 - r]$ code $C$ has $d_{\min} \geq a + 1$, any set of $a$ columns of $H_C([\delta : \delta + r - 1], [0 : \tau])$ will form a linearly independent set. We will use this fact multiple times in our proof.

a) **Property S:** To prove this property, it is sufficient to show that the $(\delta + r) \times (\delta + r)$ sub-matrix $H_C(:, [\tau + 1 - r : \tau + \delta])$ is invertible. This sub-matrix has the following structure:

$$\begin{bmatrix}
X & 0 & \cdots & 0 \\
\alpha & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
I_{(\delta - 1)} & 0 & \cdots & 0 \\
I_r & 0 & \cdots & 0
\end{bmatrix},$$

where $X$ is some $\delta \times (r - 1)$ matrix. It is easy to see that $|H_C(:, [\tau + 1 - r : \tau + \delta])| \neq 0$.

b) **Property B1:** The first $\delta$ rows of the p-c matrix are identical for constructions 1 and 2. The proof of property B1 depends only on these $\delta$ rows. Thus, property B1 follows using the same arguments as given in Sec VI-A.

c) **Property B2:** Here, we need to show that the columns of $H_C(:, [t : t + b - 1])$ form a linearly independent set, for all $t \in [\delta : \tau + a - 1]$. For $t \in [\tau + 1 - r : \tau + 1 - a]$, this follows from Property S proved above. For $t \in [\delta : \tau - b]$, we have:

$$H_C(:, [t : t + b - 1]) = \begin{bmatrix}
\hat{P}(:, [t - \delta : t + b - 1 - \delta]) \\
H_C([\delta : \delta + r - 1], [t : t + b - 1])
\end{bmatrix}.$$

From the consecutive-columns property, there exists an $a$-element set $A \subseteq [\delta : t + b - 1 - \delta]$ such that $\hat{P}(:, A) = 0$ and $\hat{P}(:, [t - \delta : t + b - 1 - \delta] \setminus A)$ is invertible. Also, any $a$ columns of $H_C([\delta : \delta + r - 1], [t : t + b - 1])$ are linearly independent. Therefore, by column permutation of $H_C(:, [t : t + b - 1])$ we can obtain a matrix of the form:

$$\begin{bmatrix}
0 \\
\delta \times a \\
\delta \times \delta \\
H'_{r \times a} \\
H''_{r \times \delta}
\end{bmatrix},$$

where $X$ is an invertible matrix and columns of $H'$ are linearly independent. It follows that the columns of $H_C(:, [t : t + b - 1])$ are linearly independent in this case. Now we consider
Let $\theta = (\tau - t - a)$. Consider the following $(\theta + r) \times (\theta + a)$ matrix:

$$M_{\theta} = \begin{bmatrix}
    \mathbf{R}_\theta \\
    \mathbf{H}_C([\delta : \delta + r - 1], [t : \tau - 1])
\end{bmatrix},$$

where $R_{\theta} = \hat{P}([\delta - \theta : \delta - 1], [\tau - b - \theta : \tau - \delta - 1])$. From the bottom-right property, there exists an $a$-element set $A \subseteq [0 : \theta + a - 1]$ such that $R_{\theta}([0 : \theta - 1], A) = 0$ and $R_{\theta}([0 : \theta - 1], [0 : \theta + a - 1])$ is invertible. Any set of a columns of $H_{C}([\delta : \delta + r - 1], [t : \tau - 1])$ is linearly independent. It easily follows along the lines of the argument for the previous case that columns of $M_{\theta}$ are linearly independent. It can be easily seen from the structure of $H_{C}([t : t + b - 1])$ that columns of this matrix form a linearly independent set if columns of the $(\theta + r + 1) \times (\theta + a + 1)$ matrix $M'_{\theta}$ shown below are linearly independent:

$$M'_{\theta} = \begin{bmatrix}
    \alpha & \cdots & \alpha \\
    & \cdots \\
    & & \cdots
\end{bmatrix},$$

where $\alpha$ is an element drawn from $\mathbb{F}_q$. Suppose the last column of $M'_{\theta}$ can be obtained as a linear combination of the other columns of $M'_{\theta}$ with coefficients $\{a_j \mid j \in [0 : \theta + a - 1]\}$. We note that there exists an invertible $(\theta + a) \times (\theta + a)$ sub-matrix of $M_{\theta}$ and that the entries of $M_{\theta}$ are also from $\mathbb{F}_q$. Hence, $\{a_j\} \subseteq \mathbb{F}_q$. However, as $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, it cannot be obtained as a linear combination of the other entries in the first row if $\{a_j\} \subseteq \mathbb{F}_q$. This results in a contradiction, thereby proving that the columns of $M'_{\theta}$ are linearly independent.

**Property R1:** Let $H_{C}(\theta) = [h_{1}(\theta) \ h_{2}(\theta) \ \cdots \ h_{t}(\theta)]$ be a $t \times \frac{\theta + a}{2}$-matrix of the code obtained by restricting $H_{C}$ to the indices $[0 : t + \tau]$. Fix $t \in [0 : \theta - 1]$ and $A \subseteq [t : t + \tau]$, where $|A| \leq a$ and $t \in A$. To prove property R1, we need to show that $h_{j}(\theta) \notin \{h_{j}(\theta) \mid j \in A \setminus \{t\}\}$. Consider the following two sub-matrices of $H_{C}$:

$$H_{C}(t, :) = \begin{bmatrix}
    0 \cdots 0 & \alpha & 0 \cdots 0 & \cdots & 0
\end{bmatrix}_{t \times (\theta + a - 1)}$$

and

$$H_{C}(\theta, :) = \begin{bmatrix}
    1 \cdots 1 & 0
\end{bmatrix}_{1 \times (\theta + a)}$$

and

$$H_{C}(\delta : \delta + r - 2, :) = \begin{bmatrix}
    U' \\
    (r-1) \times (r+1)
\end{bmatrix}_{(r-1) \times (r+1)}$$

Here, $*$’s denote the entries of row $t$ of $P$ and these symbols belong to $\mathbb{F}_{q} \subseteq \mathbb{F}_{q^2}$.

Let $\mathcal{A}_1 \triangleq \mathbb{A} \setminus \tau, \mathcal{A}_2 \triangleq \mathcal{A}_1 \setminus \mathcal{A}_1$. Consider the matrix $H'' \triangleq H_{C}([\delta : \delta + r - 2], :)$. This takes the form:

$$\begin{bmatrix}
    U & 1 & 0 \\
    1 & \cdots \\
    0 & \cdots & 1
\end{bmatrix}_{r \times (r+1)}$$

As $[U \ I_r]$ is a $t \times \frac{\theta + a}{2}$-matrix of $C$ which has $d_{\min} \geq a + 1$, any set of $a$ non-zero, non-repeating columns of $H''$ form an independent set. We use $h_{j}'$ to denote the column $j$ of $H''$. As $h_{j}' = 0$ for all $j \in \mathcal{A}_2$, we have:

$$\sum_{j \in \mathcal{A}_1} a_j h_{j}' = 0.$$
\{h_j'' \mid j \in A\}_1 \}. It follows that \{h_j'' \mid j \in A_1\} is an independent set and hence from (34) we have \(a_j = 0\) for all \(j \in A_1\). As a result, we can now rewrite (33) as:

\[
\sum_{j \in A_2} a_j h_j = 0. \tag{35}
\]

Now, we note that the columns of \(H \in \{0 : \delta+r-1\} \mid \tau : \tau + \delta \} \) are linearly independent (by design). As \(A_2 \subseteq \{\tau + 1 : \tau + \delta - 1 \} \subseteq \{\tau : \tau + \delta \} \), it follows that the columns \(\{h_j \mid j \in A_2\}_1 \) are linearly independent and hence (35) implies that \(a_j = 0\) for all \(j \in A_2\). Hence, in summary, we have \(a_j = 0\) for all \(j \in A\), which contradicts our assumption that \(a_j \neq 0\) for some \(j \in A\).

Now we consider the remaining case of \(|A \cap \{\tau, \tau + \delta\}| = 2\). Here also, we begin with the contrary assumption that there exists an \(A\) and a set of coefficients \(\{a_j \mid j \in A\}_1\), not all of them zero, satisfying (33). From (33), we have:

\[
0 = \sum_{j \in A_1 \setminus \{\tau, \tau + \delta\}} a_j h_j'' + (a_\tau + a_{\tau + 1}) h_{\tau + 1}.
\]

Here we used the fact that \(h_j'' = h_{\tau + 1}'\). As \(\{h_j \mid j \in A_1 \setminus \{\tau, \tau + \delta\}\}_1 \) form a linearly independent set, it follows that \(a_j = 0\) for \(j \in A_1 \setminus \{\tau, \tau + \delta\}\). As a result, we can now rewrite (33) as:

\[
\sum_{j \in A_2} a_j h_j + a_\tau h_{\tau} + a_{\tau + 1} h_{\tau + 1} = 0.
\]

As \(A_2 \subseteq \{\tau + 1 : \tau + \delta - 1\} \) and since the set of \(\delta + 1\) consecutive columns \(\{h_j \mid \tau \leq i \leq \tau + \delta\}_1 \) is linearly independent, it should be that \(a_j = 0\) for \(j \in A_2 \cup \{\tau, \tau + \delta\} \). This contradicts our initial assumption that \(a_j \neq 0\) for some \(j \in A\) and hence completes the proof.

References

[1] 5G Services Innovation, 5G Amer., 2019.
[2] 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. 14, no. 2, pp. 35–52, May 2017.
[3] R. Gallager, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. 8, no. 1, pp. 21–28, Jan. 1962.
[4] M. Luby, "LT codes," in Proc. IEEE Symp. Found. Comput. Sci., Nov. 2002, pp. 271–280.
[5] A. Shokrollahi, "Raptor codes," IEEE Trans. Inform. Theory, vol. 52, no. 6, pp. 1951–1957, Jun. 2006.
[6] E. Martinian and C.-E.-W. Sundberg, "Burst erasure correction codes with low decoding delay," IEEE Trans. Inform. Theory, vol. 50, no. 10, pp. 2489–2502, Oct. 2004.
[7] Y. J. Liang, J.-G. Apostolopoulos, and B. Girod, "Analysis of packet loss for compressed video: Effect of burst losses and correlation between error frames," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 7, pp. 861–874, Jul. 2008.
[8] E. M. Gabidulin, "Convolutional codes over large alphabets," in Proc. Int. Workshop Algebr. Combinat. Coding Theory, IEEE, 1988, pp. 80–84.
[9] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache, "Strongly-MDS convolutional codes," IEEE Trans. Inform. Theory, vol. 52, no. 2, pp. 584–598, Feb. 2006.
[10] E. Martinian and M. Trott, "Delay-optimal burst erasure code construction," in Proc. IEEE Int. Symp. Inform. Theory, Jun. 2007, pp. 1006–1010.
[11] A. Badr, P. Patil, A. Khisti, W.-T. Tan, and J. Apostolopoulos, "Layered constructions for low-delay streaming codes," IEEE Trans. Inform. Theory, vol. 63, no. 1, pp. 111–141, Jan. 2017.
[12] M. N. Krishnan, D. Shukla, and P. V. Kumar, "Rate-optimal streaming codes for channels with burst and random erasures," IEEE Trans. Inform. Theory, vol. 66, no. 8, pp. 4869–4891, Aug. 2020.
[38] M. Luby and D. Zuckerman, “An XOR-based erasure-resilient coding scheme,” Tech. Rep., 1995.
[39] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, vol. 16. Amsterdam, The Netherlands: Elsevier, 1977.
[40] P. J. Almeida, D. Napp, and R. Pinto, “Superregular matrices and applications to convolutional codes,” Linear Algebra Appl., vol. 499, pp. 1–25, Jun. 2016.
[41] J. S. Plank, K. M. Greenan, and E. L. Miller, “A complete treatment of software implementations of finite field arithmetic for erasure coding applications,” Univ. Tennessee, Knoxville, TN, USA, Tech. Rep. UT-CS-13-717, Oct. 2013.
[42] H. D. L. Hollmann and L. M. G. M. Tolhuizen, “Optimal codes for correcting a single (wrap-around) burst of erasures,” IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4361–4364, Sep. 2008.
[43] M. Grassl. Bounds on the Minimum Distance of Linear Codes and Quantum Codes. accessed: Nov. 13, 2022. [Online]. Available: http://www.codetables.de

Myna Vajha received the bachelor’s degree from the Indian Institute of Technology Kharagpur (IIT Kharagpur), the master’s degree from the University of Southern California (USC), and the Ph.D. degree from the Indian Institute of Science (IISc), Bengaluru. She was a Systems Architect with Ericsson, San Jose. She is currently with Qualcomm, Bengaluru, with a focus on Wi-Fi physical layer algorithms. Her current research interests include wireless communications, coding theory, and information theory, with applications to distributed storage systems, low latency streaming, and privacy.

Vinayak Ramkumar received the B.Tech. degree in electronics and communication engineering from the National Institute of Technology Calicut in 2015 and the M.Sc. (Engg.) and Ph.D. degrees in electrical communication engineering from the Indian Institute of Science, Bengaluru, in 2017 and 2023, respectively. He is currently a Post-Doctoral Fellow with the Department of Electrical Engineering-Systems, Tel Aviv University. His research interests include coded computation, codes for distributed storage, coding for low-latency communication, and information-theoretic privacy.

M. Nikhil Krishnan (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Amrita School of Engineering, Amritapuri Campus, in 2011, and the M.E. degree in telecommunications and the Ph.D. degree in electrical communication engineering from the Indian Institute of Science, Bengaluru, in 2013 and 2019, respectively. He was a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Toronto, from 2019 to 2021. From 2021 to 2022, he was an Assistant Professor with the International Institute of Information Technology Bengaluru. He is currently a DST-INSPIRE Faculty Fellow with the Department of Electrical Engineering, Indian Institute of Technology Palakkad. His research interests include coding for low-latency communication, coding for distributed storage, and coded computation.

P. Vijay Kumar (Life Fellow, IEEE) received the B.Tech. and M.Tech. degrees in electrical engineering from the Indian Institute of Technology Kharagpur (IIT Kharagpur) and the Ph.D. degree in electrical engineering from the University of Southern California (USC) in 1983. From 1983 to 2003, he was a Faculty Member of the Department of Electrical Engineering-Systems, USC. From 2003 to 2021, he was a Professor with the Indian Institute of Science, Bengaluru (IISc Bengaluru), where he is currently an Honorary Professor. From 2010 to 2017, he was an Adjunct Research Professor with USC, where he was a Visiting Professor from 2018 to 2020. A pseudorandom sequence family designed in a 1996 paper coauthored by him formed the short scrambling code of the 3G WCDMA cellular standard. The I4Z family of spreading codes co-designed by him will be incorporated by ISRO into the new civilian L1 signal of the NavIC satellite navigation system. He was a Plenary Speaker at ISIT 2014. His current research interests include codes for low-latency communication, codes for distributed storage, and low-correlation sequences for navigation satellite systems. He is a fellow of the INAE, IAS, and INSA Indian academies. He was on the Board of Governors of the IEEE Information Theory (IT) Society from 2013 to 2015. He was a recipient of the 1995 IEEE Information Theory Society Prize-Paper Award and the IEEE Data Storage Best Paper Award in 2011 and 2012. He received the USC School of Engineering’s Senior Research Award in 1994, the Rustum Choksi Award for Excellence in Research in Engineering from IISc in 2013, and the 2017 J. C. Bose National Fellowship Award. He was the TPC Co-Chair of ISIT 2015 and the Chair of the IT Society Conference Committee from 2019 to 2021.