Constructing $(h, k+1)$ cooperative MSR codes with sub-packetization $(h+1)2^{\lceil n/2 \rceil}$

Zihao Zhang, Guodong Li and Sihuang Hu
School of Cyber Science and Technology, Shandong University, Qingdao, China
Email: {zihaozhang, guodongli}@mail.sdu.edu.cn, husihuang@sdu.edu.cn

***Abstract*—THIS PAPER IS ELIGIBLE FOR THE STUDENT PAPER AWARD. We address the multi-node failure repair challenges for MDS array codes. Presently, two primary models are employed for multi-node repairs: the centralized model where all failed nodes are restored in a singular data center, and the cooperative model where failed nodes acquire data from auxiliary nodes and collaborate amongst themselves for the repair process. This paper focuses on the cooperative model, and we provide explicit constructions of optimal MDS codes with $d = k+1$ helper nodes under this model. The sub-packetization level of our new codes is $(h+1)2^{\lceil n/2 \rceil}$ where h is the number of failed nodes and n is the code length. This improves upon recent constructions given by Liu *et. al.* (IEEE Transactions on Information Theory, Vol. 69, 2023).**

I. Introduction

Erasure codes are widely used in current distributed storage systems, where they enhance data robustness by adding redundancy to tolerant data node failures. Common erasure codes include maximum distance separable (MDS) codes and locally repairable codes (LRC). Particularly, MDS codes have garnered significant attention because they provide the maximum failure tolerance for a given amount of storage overhead.

An (n, k, ℓ) array code has k information coordinates and $r = n - k$ parity check coordinates, where each coordinate is a vector in $\mathbb{F}_q^\ell$ for some finite field $\mathbb{F}_q$. Formally, an (linear) (n, k, ℓ) array code $\mathcal{C}$ can be defined by its parity check equations, i.e.,

$$\mathcal{C} = \{(C_0, \ldots, C_{n-1}) : H_0C_0 + \cdots + H_{n-1}C_{n-1} = \mathbf{0}\},$$

where each C_i is a column vector of length ℓ over $\mathbb{F}_q$, and each H_i is a $r\ell \times \ell$ matrix over $\mathbb{F}_q$. We call $\mathcal{C}$ an MDS array code if any r out of its n coordinates can be recovered from the other k coordinates. To be specific, let $\mathcal{F} = \{i_1, i_2, \ldots, i_r\} \subset [n]$ be the collection of indices of r failed nodes, we have

$$\sum_{i\in\mathcal{F}} H_iC_i = -\sum_{i\in[n]\setminus\mathcal{F}} H_iC_i,$$

where we use $[n]$ to denote the set $\{0, 1, \ldots, n-1\}$. Thus, we know that r coordinates $C_i, i \in \mathcal{F}$ can be recovered from the other k coordinates $C_i, i \in [n] \setminus \mathcal{F}$ if and only if the square matrix $[H_{i_1} \quad H_{i_2} \quad \ldots \quad H_{i_r}]$ is invertible. Equivalently, we say a set of n matrices $H_0, H_1, \ldots, H_{n-1}$ in $\mathbb{F}_q^{r\ell\times\ell}$ defines an (n, k, ℓ) MDS array code if

$$[H_{i_1} \quad H_{i_2} \quad \cdots \quad H_{i_r}] \text{ is invertible } \forall\ \{i_1, i_2, \ldots, i_r\} \subset [n].$$

Research partially funded by National Key R&D Program of China under Grant No. 2021YFA1001000, National Natural Science Foundation of China under Grant No. 12001322 and 12231014, a Taishan scholar program of Shandong Province, and CCF-Huawei Populus Grove Fund.

With the emergence of large-scale distributed storage systems, the notion of *repair bandwidth* was introduced to measure the efficiency of recovering the erasure of a single codeword coordinate. The seminal work by Dimakis *et. al.* [1] pointed out that we can repair a single failed node by smaller repair bandwidths than the trivial MDS repair scheme. More precisely, for an (n, k, ℓ) MDS array code, the optimal repair bandwidth for a single node failure by downloading data from $d \geq k$ helper nodes is

$$\frac{d\ell}{d-k+1}. \tag{1}$$

We call an (n, k, ℓ) MDS array code minimum storage regenerating (MSR) code with repair degree d if it achieves the lower bound (1) for the repair of any single erased coordinate from any d out of $n-1$ remaining coordinates. Please see [2]–[11] and references therein for the constructions and studies of MSR codes.

MSR codes can efficiently recover a single failed node using the smallest possible bandwidth. Naturally, new variants of MSR codes are adopted to handle the case when $h > 1$ nodes fail simultaneously. Under the centralized-repair, a single repair center downloads helper data from d helper nodes and uses this data to produce h replacement nodes (please see [12]–[22] and references therein). Another scheme of repairing multiple failed nodes simultaneously is cooperative-repair, where failed nodes acquire data from auxiliary nodes and collaborate amongst themselves for the repair process. Notably, the cooperative model has demonstrated greater robustness compared to its centralized counterpart, being able to deduce a corresponding centralized model under equivalent parameters. Please refer to [23]–[30] and references therein for the results on cooperative MSR codes.

This paper primarily focuses on the cooperative model, and all subsequent references to repair bandwidth and cut-set bounds are made within this context.

Theorem 1. *(Cut-set bound[23]) For an (n, k, ℓ) MDS array code, the optimal repair bandwidth for h failed nodes by*

downloading information from d helper nodes under the cooperative repair scheme is

$$\frac{h(d+h-1)\ell}{d-k+h}. \tag{2}$$

We say that an (n,k,ℓ) MDS array code $\mathcal{C}$ is an (h,d)-MSR code under the cooperative model if any h failed nodes can be recovered from any other d helper nodes with total bandwidth achieving the lower bound (2).

A. Previous works on cooperative MSR codes

In [27], Ye and Barg provided an explicit construction for cooperative MSR codes with all admissible parameters. The sub-packetization level of the construction in [27] is given by $((d-k)^{h-1}(d-k+h))^{\binom{n}{h}}$. In [28], Zhang *et al.* introduced a construction with optimal access property, where $\ell=(d-k+h)^{\binom{n}{h}}$. Subsequently, in the work of Ye [29], the sub-packetization was further reduced to $(d-k+h)(d-k+1)^n$. More recently, Liu's work [30] achieved even lower sub-packetization for the case $d=k+1$: the sub-packetization of the new construction is $o2^n$ where o is the largest odd number such that $o \mid 2^n$.

Codes	Sub-packetization ℓ	Restrictions
Ye and Barg 2019 [27]	$((d-k)^{h-1}m)^{\binom{n}{h}}$	
Zhang *et al.* 2020 [28]	$m^{\binom{n}{h}}$	
Ye 2020 [29]	ms^n	
Liu *et al.* 2023 [30]	os^n	$d=k+1$
This paper	$ms^{\lfloor n/2 \rfloor}$	$d=k+1$

TABLE I
SUB-PACKETIZATIONS AND RESTRICTIONS OF DIFFERENT CONSTRUCTIONS OF (h,d)-COOPERATIVE MSR CODES, WHERE $s=d-k+1$, $m=d-k+h$ AND o IS THE LARGEST ODD NUMBER SATISFYING $o \mid m$.

B. Our contributions.

In this paper, we present a construction of cooperative MSR codes with $d=k+1$ and $\ell=(h+1)2^{\lceil n/2 \rceil}$. Our approach is inspired by the construction of MSR codes in [11], which introduced a method to design parity check sub-matrices using the so-called kernel matrices and blow-up map. In this work, we first introduce new kernel matrices and then blow up them to construct new $(1,k+1)$-MSR codes. Then, similarly as [29], we replicate the $(1,k+1)$-MSR code $h+1$ times obtaining an $(h,k+1)$-MSR code. The optimal repair scheme is guaranteed by the suitably chosen cooperative pairing matrices. Our results can be generalized to construct (h,d) cooperative MSR codes with sub-packetization $(d-k+h)(d-k+1)^{n/2}$, and we leave this for future work.

All the omitted proofs in this paper can be seen in our long paper [31].

II. PRELIMINARIES

Let $\mathbb{F}_q$ be a finite field with order q. For a positive integer m, we define $[m]:=(0,1,\cdots,m-1)$. For an integer a, we define

$$a+[m]:=(a+x : x\in[m]),$$

and we denote the vector $x_{[m]}$ over $\mathbb{F}_q$ as $(x_j : j\in[m])$. Let $\mathbf{I}_m$ be the $m\times m$ identity matrix over $\mathbb{F}_q$. For an element $x\in\mathbb{F}_q$, and a positive integer t, we define a column vector of length t as

$$L^{(t)}(x):=\begin{bmatrix}1\\ x\\ x^2\\ \vdots\\ x^{t-1}\end{bmatrix}.$$

Assume that s,t are two positive integers. For each $i\in[s^t]$, we write

$$i=\sum_{z\in[t]} i_z s^z,\ i_z\in[s].$$

Here we use i_z to denote the z-th digit in the t digits base-s expansion of i.

To simplify notations, we need the following matrix operator $\boxtimes$ and blow-up map introduced in [11].

Definition 1. *For a matrix A and an $m\times n$ block matrix B written as*

$$B=\begin{bmatrix}B_{0,0} & \cdots & B_{0,n-1}\\ \vdots & \ddots & \vdots\\ B_{m-1,0} & \cdots & B_{m-1,n-1}\end{bmatrix},$$

we define

$$A\boxtimes B:=\begin{bmatrix}A\otimes B_{0,0} & \cdots & A\otimes B_{0,n-1}\\ \vdots & \ddots & \vdots\\ A\otimes B_{m-1,0} & \cdots & A\otimes B_{m-1,n-1}\end{bmatrix},$$

where $\otimes$ is the Kronecker product. Note that the result $A\boxtimes B$ is dependent on how the rows and columns of B are partitioned, and we will specify the partition every time we use this notation. If every block entry $B_{i,j}$ is a scalar over $\mathbb{F}_q$, we have $A\boxtimes B=B\otimes A$.

Throughout this paper, when we say that B is an $m\times n$ block matrix, we always assume that B is uniformly partitioned, i.e. each block entry of B is the same size.

Definition 2 (Blow-up)**.** *Let t be a positive integer. For any $a\in[t]$, we* blow up *an $s\times s$ block matrix K to get an $s^t\times s^t$ block matrix via*

$$\Phi_{t,a}(K)=\mathbf{I}_{s^{t-a-1}}\otimes(\mathbf{I}_{s^a}\boxtimes K).$$

The following lemma shows the relationship between K and its blown-up matrix $\Phi_{t,a}(K)$.

Lemma 2. *For $i,j\in[s^t]$, the block entry of $\Phi_{t,a}(K)$ at the ith block row and jth block column*

$$\Phi_{t,a}(K)(i,j)=\begin{cases}K(i_a,j_a) & \text{if } i_z=j_z\ \forall z\in[t]\setminus\{a\}\\ \mathbf{O} & \text{otherwise,}\end{cases}$$

where $K(i_a,j_a)$ is the block entry of K at the i_ath block row and j_ath block column.

The following properties of blown-up matrices will be used for the repair scheme of our codes.

Lemma 3. *Let A, B and C be three $s \times s$ block matrices. If*

$$(\mathbf{I}_s \otimes A)(\mathbf{I}_s \boxtimes B) = (\mathbf{I}_s \boxtimes B)(\mathbf{I}_s \otimes C)^{[1]}$$

then for any positive integer t and $a_0 \neq a_1 \in [t]$,

$$\Phi_{t,a_0}(A)\Phi_{t,a_1}(B) = \Phi_{t,a_1}(B)\Phi_{t,a_0}(C).$$

The following result can be obtained easily by the mixed-product property of the Kronecker product, and we omit its proof.

Lemma 4. *Let A and B be two $s \times s$ block matrices. Then for any positive integer t and $a \in [t]$, we have*

$$\Phi_{t,a}(A)\Phi_{t,a}(B) = \Phi_{t,a}(AB)$$

if AB is a valid matrix product.

III. Code construction and MDS property

Given code length n, dimension k, repair degree d, and the number of failed nodes h such that

$$k + 1 \leq d \leq n - h,$$

we use $r = n - k$ to denote the redundancy of our code, and set $s = d - k + 1$. In this section, we construct an $(n, k, \ell = (h+1)2^{\lceil n/2 \rceil})$ cooperative MSR code with repair degree $d = k + 1$ for any fixed number of failed nodes h. Hence $s = d - k + 1 = 2$. Without loss of generality, we always assume that $2|n$. Then $\ell = (h+1)2^{n/2}$ and we write $\tilde{\ell} = 2^{n/2}$. The codeword $(C_0, C_1, \cdots, C_{n-1})$ of the (n, k, ℓ) array code is divided into $n/2$ groups of size 2. We use $a \in [n/2], b \in [2]$ to denote the group's and the node's index within its group, respectively. In other words, group a consists of the two nodes C_{2a} and C_{2a+1}.

To begin with, we select $2n$ distinct elements $\lambda_{[2n]}$ and two distinct elements γ_0, γ_1 from $\mathbb{F}_q$. We first define the following *kernel map*

$$\mathcal{K}^{(t)} : \mathbb{F}_q^2 \to \mathbb{F}_q^{2t \times 2},$$

which maps $x_{[2]}$ to the following 2×2 block matrix

$$\mathcal{K}^{(t)}(x_{[2]}) = \begin{bmatrix} L^{(t)}(x_0) & L^{(t)}(x_1) \\ L^{(t)}(x_0) & L^{(t)}(x_1) \end{bmatrix}. \tag{3}$$

Besides, we introduce the *cooperative pairing* matrices

$$V_0 = \begin{bmatrix} 1 & \gamma_0 \\ \gamma_0 & 1 \end{bmatrix}, \ V_1 = \begin{bmatrix} 1 & \gamma_1 \\ \gamma_1 & 1 \end{bmatrix},$$

and

$$U_0 = \begin{bmatrix} 1 & -\gamma_1 \\ -\gamma_1 & 1 \end{bmatrix}, \ U_1 = \begin{bmatrix} 1 & -\gamma_0 \\ -\gamma_0 & 1 \end{bmatrix}.$$

Claim 5. *For any $b \in [2]$, we can directly check that*

$$U_b V_b = \begin{bmatrix} 1 - \gamma_0\gamma_1 & \gamma_b - \gamma_{b\oplus 1} \\ \gamma_b - \gamma_{b\oplus 1} & 1 - \gamma_0\gamma_1 \end{bmatrix},$$

$$U_b V_{b\oplus 1} = \begin{bmatrix} 1 - \gamma_{b\oplus 1}^2 & \\ & 1 - \gamma_{b\oplus 1}^2 \end{bmatrix}.$$

Here we use the symbol "$\oplus$" to represent the addition in $\mathbb{F}_2$. These cooperative pairing matrices will play a pivotal role in our cooperative repair scheme of Section IV. Now, we are ready to define the following *kernel matrices*. For $a \in [n/2], b \in [2]$ and a positive integer t, we define

$$\begin{aligned} K_{a,b}^{(t)} &= \left(V_b \otimes \mathbf{1}^{(t)}\right) \odot \ \mathcal{K}^{(t)}(\lambda_{4a+2b+[2]}) \\ &= \begin{bmatrix} L^{(t)}(\lambda_{4a+2b}) & \gamma_b L^{(t)}(\lambda_{4a+2b+1}) \\ \gamma_b L^{(t)}(\lambda_{4a+2b}) & L^{(t)}(\lambda_{4a+2b+1}) \end{bmatrix}, \end{aligned}$$

where $\odot$ is the Hadamard (element-wise) product of two matrices. Then, for a non-empty subset $B \subseteq [2]$, we define the following matrix

$$K_{a,B}^{(t)} = [K_{a,b}^{(t)} : b \in B].$$

Next, we blow up the kernel matrix to get

$$M_{a,b}^{(t)} = \Phi_{\frac{n}{2},a}(K_{a,b}^{(t)}) = \mathbf{I}_{s^{\frac{n}{2}-a-1}} \otimes (\mathbf{I}_{s^a} \boxtimes K_{a,b}^{(t)}).$$

Similarly, we define $M_{a,B}^{(t)}$ by the same way as that of $K_{a,B}^{(t)}$. Following that, we define

$$f(x_{[4]}, \gamma_{[2]}) = \det \begin{bmatrix} L_0^{(2)} & \gamma_0 L_1^{(2)} & L_2^{(2)} & \gamma_1 L_3^{(2)} \\ \gamma_0 L_0^{(2)} & L_1^{(2)} & \gamma_1 L_2^{(2)} & L_3^{(2)} \end{bmatrix}$$

where $L_i^{(2)} = L^{(2)}(x_i)$ and

$$g(\gamma_0, \gamma_1) = (\gamma_0^2 - 1)(\gamma_1^2 - 1)(\gamma_0\gamma_1 - 1).$$

To guarantee the MDS property and the optimal repair scheme, we further require the elements $\lambda_{[2n]}, \gamma_0, \gamma_1$ to satisfy

$$g(\gamma_0, \gamma_1) \cdot \Pi_{a \in [n/2]} f(\lambda_{4a+[4]}, \gamma_{[2]}) \neq 0. \tag{4}$$

The existence of such elements in some linear field is guaranteed by the following result.

Lemma 6. *If $q \geq 2n$, then in $\mathbb{F}_q$ we can always find these distinct elements $\lambda_{[2n]}$ and distinct elements $\gamma_{[2]}$ satisfy (4).*

From now let $\mathbb{F}_q$ be a finite field with order $q \geq 2n$. Then by Lemma 6 we can select $2n$ distinct elements $\lambda_{[2n]}$ and two distinct elements $\gamma_{[2]}$ satisfying (4) from $\mathbb{F}_q$. Now we write $L_i^{(t)} = L^{(t)}(\lambda_i)$. Then we have the following.

Lemma 7. *Suppose that $a \in [n/2]$, $B \subseteq [2]$ is a non-empty set of size t. For any integer $m > t$, there exists an $\tilde{\ell}m \times \tilde{\ell}m$ matrix V such that:*

(i)

$$V M_{a,B}^{(m)} = \begin{bmatrix} M_{a,B}^{(t)} \\ \mathbf{O} \end{bmatrix}$$

where $\mathbf{O}$ is the $\tilde{\ell}(m-t) \times \tilde{\ell}t$ all-zero matrix.

(ii) *For any $c \in [n/2] \setminus \{a\}, d \in [2]$,*

$$V M_{c,d}^{(m)} = \begin{bmatrix} M_{c,d}^{(t)} \\ \widehat{M}_{c,d}^{(m-t)} \end{bmatrix}$$

[1] This condition is equivalent to $\Phi_{2,0}(A)\Phi_{2,1}(B) = \Phi_{2,1}(B)\Phi_{2,0}(C)$.

where $\widehat{M}_{c,d}^{(m-t)}$ *is an* $\tilde{\ell}(m-t)\times\tilde{\ell}$ *matrix which is column equivalent to* $M_{c,d}^{(m-t)}$.

(iii) *For any* $\lambda_i,\lambda_j\notin\{\lambda_{4a+2B+[2]}\}$,

$$V(\mathbf{I}_{\tilde{\ell}/2}\boxtimes \mathrm{blkdiag}(L_i^{(m)},L_j^{(m)}) = \begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2}\boxtimes \mathrm{blkdiag}(L_i^{(t)},L_j^{(t)}) \\ (\mathbf{I}_{\tilde{\ell}/2}\boxtimes \mathrm{blkdiag}(L_i^{(m-t)},L_j^{(m-t)})Q \end{bmatrix}$$

where Q *is an* $\tilde{\ell}\times\tilde{\ell}$ *invertible matrix.*

Since the proof of this lemma is exactly the same as that of [11, Lemma 3], we omit its detail.

Before giving the construction of our cooperative MSR code, we define an intermediate $(n,k,\tilde{\ell})$ array code

$$\tilde{\mathcal{C}}=\{(\tilde{C}_0,\ldots,\tilde{C}_{n-1})|\sum_{i\in[n]}\tilde{H}_i\tilde{C}_i=\mathbf{0},\tilde{C}_i\in\mathbb{F}_q^{\tilde{\ell}}\},\quad(5)$$

where $\tilde{H}_{2a+b}=M_{a,b}^{(r)}$ for $a\in[n/2],b\in[2]$.

Lemma 8. *For any* z *distinct integers* $a_0,a_1,\cdots,a_{z-1}\in[n/2]$ *and any* z *non-empty subsets* $B_0,B_1,\cdots,B_{z-1}\subseteq[2]$ *satisfying* $|B_0|+|B_1|+\cdots+|B_{z-1}|=m\le r$, *we have*

$$\det\left(\begin{bmatrix}M_{a_0,B_0}^{(m)} & M_{a_1,B_1}^{(m)} & \cdots & M_{a_{z-1},B_{z-1}}^{(m)}\end{bmatrix}\right)\neq 0.$$

Note that if we set $m=r$ in Lemma 8, then we obtain the MDS property of the array code (5).

Remark 1. *The* $(n,k,\tilde{\ell})$ *MDS array code* $\tilde{\mathcal{C}}$ *in* (5) *is in fact an MSR code with repair degree* $d=k+1$. *This can be proved similarly by the method of [11].*

Finally, we give the construction of our cooperative MSR code as

$$\mathcal{C}=\{(C_0,\ldots,C_{n-1})|\sum_{i\in[n]}H_iC_i=\mathbf{0},C_i\in\mathbb{F}_q^{\ell}\}\quad(6)$$

where $H_i=\mathbf{I}_{h+1}\otimes\tilde{H}_i$ for $i\in[n]$. In other words, we replicate the $(1,k+1)$-MSR code $\tilde{\mathcal{C}}$ $h+1$ times obtaining an $(h,k+1)$-MSR code.

Theorem 9. *The code* $\mathcal{C}$ *in* (6) *is an* (n,k,ℓ) *MDS array code.*

Proof. This follows directly from the fact that $\tilde{\mathcal{C}}$ is an MDS array code and $H_i=\mathbf{I}_{h+1}\otimes\tilde{H}_i$ for $i\in[n]$. □

IV. Repair scheme for any h failed nodes

In this section, we describe the cooperative repair scheme of $\mathcal{C}$ defined in (6). Let $\mathcal{F}=\{i_0,i_1,\cdots,i_{h-1}\}\subset[n]$ be the indices of the h failed nodes, where $i_0<i_1<\cdots<i_{h-1}$. This naturally induces a bijective map $\mathcal{I}_{\mathcal{F}}:\mathcal{F}\to[h]$ which maps i_z to z for $z\in[h]$. For simplicity, we write $\hat{i}=\mathcal{I}_{\mathcal{F}}(i)$ for $i\in\mathcal{F}$. Let $\mathcal{H}\subset[n]\backslash\mathcal{F}$ be the collection of the indices of d helper nodes.

For $a\in[n/2],g\in[2]$, we first introduce the following $\tilde{\ell}/2\times\tilde{\ell}$ row-selection matrix

$$R_{a,g}=\mathbf{I}_{2^{n/2-a-1}}\otimes\boldsymbol{e}_g\otimes\mathbf{I}_{2^a}$$

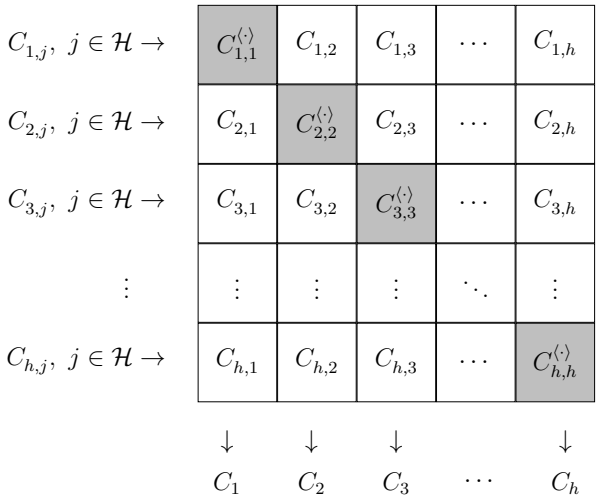

Fig. 1. The repair scheme of our cooperative MSR codes. Without loosing of generality, we assume that $\mathcal{F}=\{1,2,\ldots,h\}$, and $\mathcal{H}\subseteq[n]\backslash\mathcal{F}$. For each $i\in\mathcal{F}$, we have $C_{i,i}^{\langle g\rangle}=D_{i,i}^{\langle g\rangle}C_i,g\in[2]$, and $C_{i,j}=D_{i,j}C_j,j\in[n]\backslash\{i\}$. Here, for each $i\in\mathcal{F}$, we use $C_{i,i}^{\langle\cdot\rangle}$ to denote the two nodes $C_{i,i}^{\langle 0\rangle}$ and $C_{i,i}^{\langle 1\rangle}$. All the off-diagonal nodes at the ith column will be transmitted to node C_i.

where $\boldsymbol{e}_g$ is the g-th row of $\mathbf{I}_2$. Multiplying an $\tilde{\ell}\times\tilde{\ell}$ matrix M from the left by $R_{a,g}$ is equivalent to selecting those rows in M whose indices i satisfying that $i_a=g$. We can verify that

$$\sum_{g\in[2]}R_{a,g}^TR_{a,g}=\mathbf{I}_{\tilde{l}}.\quad(7)$$

Then, for $a\in[n/2]$, $g\in[2]$ and $z\in[h]$, we define the following $2\times(h+1)$ block matrix

$$S_{a,g,z}(i,j)=\begin{cases}R_{a,i\oplus g} & \text{if } j=i \text{ or } j=z+2\\ \mathbf{O} & \text{otherwise,}\end{cases}\quad(8)$$

where $i\in[2]$, $j\in[h+1]$. Note that for $z=h-1$, the case $j=z+2$ is impossible.

For any $i\in\mathcal{F}$, we define the following *repair matrix*

$$\mathcal{R}_i^{\mathcal{F}}=S_{\lfloor\frac{i}{2}\rfloor,0,\hat{i}}(\mathbf{I}_{h+1}\otimes\Phi_{\frac{n}{2},\lfloor\frac{i}{2}\rfloor}(U_{i \bmod 2})).$$

We also set the following notations.

(1) For $g\in[2]$,

$$H_{i,i}^{\langle g\rangle}=(\mathcal{R}_i^{\mathcal{F}}\otimes\mathbf{I}_r)H_iS_{\lfloor\frac{i}{2}\rfloor,g,h-1}^T,$$
$$D_{i,i}^{\langle g\rangle}=S_{\lfloor\frac{i}{2}\rfloor,g,\hat{i}},$$
$$C_{i,i}^{\langle g\rangle}=D_{i,i}^{\langle g\rangle}C_i.$$

(2) For $j\in[n]\setminus\{i\}$ and $\lfloor\frac{j}{2}\rfloor=\lfloor\frac{i}{2}\rfloor$,

$$H_{i,j}=(\mathcal{R}_i^{\mathcal{F}}\otimes\mathbf{I}_r)H_jS_{\lfloor\frac{i}{2}\rfloor,0,h-1}^T,$$
$$D_{i,j}=S_{\lfloor\frac{i}{2}\rfloor,0,\hat{i}},$$
$$C_{i,j}=D_{i,j}C_j.$$

Algorithm 1: $\texttt{repair}(\mathcal{F},\mathcal{H})$

Input: Two subsets $\mathcal{F},\mathcal{H}\subseteq[n]$ of size $[\mathcal{F}]=h,|\mathcal{H}|=d$ and $\mathcal{F}\cap\mathcal{H}=\emptyset$, which collect the indices of failed nodes and the indices of helper nodes respectively.

Output: The repaired nodes $\{C_i, i\in\mathcal{F}\}$

1 **for** $i\in\mathcal{F}$ **do**
2 **for** $j\in\mathcal{H}$ **do**
3 Node j computes $C_{i,j}=D_{i,j}C_j$
4 Node j **transmits** $C_{i,j}$ to node i
5 Node i computes
$$\{C_{i,i}^{\langle g\rangle}, g\in[2], C_{i,j}, j\in\mathcal{F}\setminus\{i\}\}$$
from the received data $\{C_{i,j}, j\in\mathcal{H}\}$ ▷ Lemma 10
6 **for** $i\in\mathcal{F}$ **do**
7 **for** $j\in\mathcal{F}\setminus\{i\}$ **do**
8 Node j **transmits** $C_{j,i}$ to node i
9 Node i repairs C_i from
$$\{C_{i,i}^{\langle g\rangle}, g\in[2], C_{j,i}, j\in\mathcal{F}\setminus\{i\}\}$$
▷ Lemma 11
10 **return** $\{C_i, i\in\mathcal{F}\}$

(3) For $j\in[n]\setminus\{i\}$ and $\lfloor\frac{j}{2}\rfloor\neq\lfloor\frac{i}{2}\rfloor$,

$$H_{i,j}=(S_{\lfloor\frac{i}{2}\rfloor,0,\hat{i}}\otimes\mathbf{I}_r)H_jS^T_{\lfloor\frac{i}{2}\rfloor,0,h-1},$$
$$D_{i,j}=\mathcal{R}_i^{\mathcal{F}},$$
$$C_{i,j}=D_{i,j}C_j.$$

Lemma 10. *For each $i\in\mathcal{F}$, the $n+1$ matrices*

$$H_{i,0},\ \cdots,\ H_{i,i-1},\ H_{i,i}^{\langle 0\rangle},\ H_{i,i}^{\langle 1\rangle},\ H_{i,i+1},\ \cdots,\ H_{i,n-1}$$

define an $(n+1,k+1,\tilde{\ell})$ MDS array code. And for every codeword $(C_0,\ldots,C_{n-1})\in\mathcal{C}$ the corresponding vector $(C_{i,0},\cdots,C_{i,i-1},C_{i,i}^{\langle 0\rangle},C_{i,i}^{\langle 1\rangle},C_{i,i+1},\cdots,C_{i,n-1})$ satisfies

$$\sum_{g\in[2]}H_{i,i}^{\langle g\rangle}C_{i,i}^{\langle g\rangle}+\sum_{j\in[n]\setminus\{i\}}H_{i,j}C_{i,j}=\mathbf{0}.$$

Lemma 11. *The $\ell\times\ell$ matrix formed by vertically joining the $h+1$ matrices $D_{i,i}^{\langle g\rangle}, g\in[2], D_{j,i}, j\in\mathcal{F}\setminus\{i\}$, is invertible.*

Repair scheme. We use $i\in\mathcal{F}$ to denote the index of each failed node, while using $j\in[n]\setminus\{i\}$ to denote the indices of the left nodes. We illustrate the repair scheme in Fig. 1 and provide the complete steps in Algorithm 1. The repair process is divided into the following two steps.

(1) For each $i\in\mathcal{F}$, the following steps are executed: Firstly, each helper node j ($j\in\mathcal{H}$) calculates a vector $C_{i,j}=D_{i,j}C_j$ of length $\tilde{\ell}$ and sends it to node i. Then, by Lemma 10, node i can use the received data $\{C_{i,j}, j\in\mathcal{H}\}$ to compute the $h+1$ vectors of length $\tilde{\ell}$, $\{C_{i,i}^{\langle g\rangle}, g\in[2], C_{i,j}, j\in\mathcal{F}\setminus\{i\}\}$. These operations correspond to every row in Fig. 1 and Line 1-5 in Algorithm 1.

(2) For each $i\in\mathcal{F}$, node i can be repaired by the following steps: First, for each $j\in\mathcal{F}\setminus\{i\}$, node j transmits the of length-$\tilde{\ell}$ column vector $C_{j,i}$ computed in step (1) to node i. Recall that

$$C_{i,i}^{\langle g\rangle}=D_{i,i}^{\langle g\rangle}C_i, g\in[2], C_{j,i}=D_{j,i}C_i, j\in\mathcal{F}\setminus\{i\}.$$

By Lemma 11, C_i can be recovered from $C_{i,i}^{\langle 0\rangle}$, $C_{i,i}^{\langle 1\rangle}$ and the received data $\{C_{j,i}, j\in\mathcal{F}\setminus\{i\}\}$ from other failed nodes. These steps correspond to every column in Fig. 1 and Line 6-9 in Algorithm 1.

It is easy to check that the repair scheme achieves the lower bound of repair bandwidth in Theorem 1. Specifically, the length of each intermediate vector computed during the repair process is $\tilde{\ell}=\ell/(d-k+h)$, and the steps that occupy bandwidth only occur in Line 4 and Line 8 of Algorithm 1. It can be easily calculated that the bandwidth consumed during the repair process is

$$\frac{hd\ell}{d-k+h}+\frac{h(h-1)\ell}{d-k+h}.$$

Here, the left side represents the bandwidth occupied by the transmission from helper nodes to the failed nodes, while the right side represents the bandwidth occupied by the data transmission between failed nodes.

References

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4539–4551, 2010.

[2] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the MSR and mbr points via a product-matrix construction," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.

[3] I. Tamo, Z. Wang, and J. Bruck, "Zigzag codes: MDS array codes with optimal rebuilding," *IEEE Transactions on Information Theory*, vol. 59, no. 3, pp. 1597–1616, 2013.

[4] I. Tamo, Z. Wang, and J. Bruck, "Access versus bandwidth in codes for storage," *IEEE Transactions on Information Theory*, vol. 60, no. 4, pp. 2028–2037, 2014.

[5] M. Ye and A. Barg, "Explicit constructions of high-rate MDS array codes with optimal repair bandwidth," *IEEE Transactions on Information Theory*, vol. 63, no. 4, pp. 2001–2014, 2017.

[6] B. Sasidharan, M. Vajha, and P. V. Kumar, "An explicit, coupled-layer construction of a high-rate MSR code with low sub-packetization level, small field size and $d<(n-1)$," in *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 2048–2052, 2017.

[7] M. Ye and A. Barg, "Explicit constructions of optimal-access MDS codes with nearly optimal sub-packetization," *IEEE Transactions on Information Theory*, vol. 63, no. 10, pp. 6307–6317, 2017.

[8] I. Tamo, M. Ye, and A. Barg, "Optimal repair of reed-solomon codes: Achieving the cut-set bound," in *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 216–227, 2017.

[9] J. Li, X. Tang, and C. Tian, "A generic transformation to enable optimal repair in MDS codes for distributed storage systems," *IEEE Transactions on Information Theory*, vol. 64, no. 9, pp. 6257–6267, 2018.

[10] S. B. Balaji and P. V. Kumar, "A tight lower bound on the sub-packetization level of optimal-access MSR and MDS codes," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 2381–2385, 2018.

[11] G. Li, N. Wang, S. Hu, and M. Ye, "MSR codes with linear field size and smallest sub-packetization for any number of helper nodes," *arXiv preprint arXiv:2303.10467*, 2023.

[12] V. R. Cadambe, S. A. Jafar, H. Maleki, K. Ramchandran, and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2974–2987, 2013.

[13] A. S. Rawat, O. O. Koyluoglu, and S. Vishwanath, "Centralized repair of multiple node failures with applications to communication efficient secret sharing," *IEEE Transactions on Information Theory*, vol. 64, no. 12, pp. 7529–7550, 2018.

[14] Z. Wang, I. Tamo, and J. Bruck, "Optimal rebuilding of multiple erasures in MDS codes," *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1084–1101, 2017.

[15] M. Zorgui and Z. Wang, "Centralized multi-node repair for minimum storage regenerating codes," in *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 2213–2217, 2017.

[16] I. Tamo, M. Ye, and A. Barg, "The repair problem for reed–solomon codes: Optimal repair of single and multiple erasures with almost optimal node size," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2673–2695, 2019.

[17] M. Zorgui and Z. Wang, "On the achievability region of regenerating codes for multiple erasures," in *2018 IEEE International Symposium on Information Theory (ISIT)*, pp. 2067–2071, 2018.

[18] N. Mital, K. Kralevska, C. Ling, and D. Gündüz, "Practical functional regenerating codes for broadcast repair of multiple nodes," in *2019 IEEE International Symposium on Information Theory (ISIT)*, pp. 221–225, 2019.

[19] R. Li, J. Lin, and P. P. Lee, "Enabling concurrent failure recovery for regenerating-coding-based storage systems: From theory to practice," *IEEE Transactions on Computers*, vol. 64, no. 7, pp. 1898–1911, 2015.

[20] H. Dau, I. M. Duursma, H. M. Kiah, and O. Milenkovic, "Repairing reed-solomon codes with multiple erasures," *IEEE Transactions on Information Theory*, vol. 64, no. 10, pp. 6567–6582, 2018.

[21] J. Mardia, B. Bartan, and M. Wootters, "Repairing multiple failures for scalar MDS codes," *IEEE Transactions on Information Theory*, vol. 65, no. 5, pp. 2661–2672, 2019.

[22] S. Li, M. Gadouleau, J. Wang, and D. Zheng, "A new centralized multi-node repair scheme of MSR codes with error-correcting capability," *arXiv preprint arXiv:2309.15668*, 2023.

[23] K. W. Shum and Y. Hu, "Cooperative regenerating codes," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7229–7258, 2013.

[24] A.-M. Kermarrec, N. Le Scouarnec, and G. Straub, "Repairing multiple failures with coordinated and adaptive regenerating codes," in *2011 International Symposium on Networking Coding*, pp. 1–6, 2011.

[25] J. Li and B. Li, "Cooperative repair with minimum-storage regenerating codes for distributed storage," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, pp. 316–324, 2014.

[26] K. W. Shum and J. Chen, "Cooperative repair of multiple node failures in distributed storage systems," *Int. J. Inf. Coding Theory*, vol. 3, p. 299–323, jan 2016.

[27] M. Ye and A. Barg, "Cooperative repair: Constructions of optimal MDS codes for all admissible parameters," *IEEE Transactions on Information Theory*, vol. 65, no. 3, pp. 1639–1656, 2019.

[28] Y. Zhang, Z. Zhang, and L. Wang, "Explicit constructions of optimal-access MSCR codes for all parameters," *IEEE Communications Letters*, vol. 24, no. 5, pp. 941–945, 2020.

[29] M. Ye, "New constructions of cooperative MSR codes: Reducing node size to $\exp(o(n))$," *IEEE Transactions on Information Theory*, vol. 66, no. 12, pp. 7457–7464, 2020.

[30] Y. Liu, H. Cai, and X. Tang, "A new cooperative repair scheme with $k+1$ helper nodes for (n,k) hadamard MSR codes with small sub-packetization," *IEEE Transactions on Information Theory*, vol. 69, no. 5, pp. 2820–2829, 2023.

[31] Z. Zhang, G. Li, and S. Hu, "Constructing $(h, k+1)$ cooperative MSR codes with sub-packetization $(h+1)2^{\lceil n/2 \rceil}$," *Github: https://github.com/HzzQAQ/cooperative-msr*, 2024.

Appendix A
Proof of Lemma 2

We prove this lemma by induction. It is easy to see that the conclusion holds for the case $t = 1$. Now assume that the conclusion holds for some positive integer t and any $a \in [t]$, that is,

$$\Phi_{t,a}(K)(i,j) = \begin{cases} K(i_a, j_a) & \text{if } i_z = j_z \ \forall z \in [t] \setminus \{a\} \\ \mathbf{O} & \text{otherwise,} \end{cases} \tag{9}$$

where $i, j \in [s^t]$.

We proceed to prove the case $t+1$. If $a = t$ then $\Phi_{t+1,t}(K) = \mathbf{I}_{s^t} \boxtimes K$, and we can verify that

$$\Phi_{t+1,t}(K)(i,j) = \begin{cases} K(i_t, j_t) & \text{if } i_z = j_z \ \forall z \in [t] \\ \mathbf{O} & \text{otherwise,} \end{cases}$$

where $i, j \in [s^{t+1}]$. If $0 \le a \le t-1$, then by definition $\Phi_{t+1,a}(K) = \mathbf{I}_s \otimes \Phi_{t,a}(K)$. By (9) we get

$$\Phi_{t+1,a}(K)(i,j) = \begin{cases} K(i_a, j_a) & \text{if } i_z = j_z \ \forall z \in [t+1] \setminus \{a\} \\ \mathbf{O} & \text{otherwise,} \end{cases}$$

where $i, j \in [s^{t+1}]$. This concludes the proof.

Appendix B
Proof of Lemma 3

By Lemma 2, we have

$$\Phi_{t,a_0}(A)(u,v) = \begin{cases} A(u_{a_0}, v_{a_0}) & \text{if } u_i = v_i, \forall i \in [t]\backslash\{a_0\} \\ \mathbf{O} & \text{otherwise,} \end{cases}$$

$$\Phi_{t,a_1}(B)(u,v) = \begin{cases} B(u_{a_1}, v_{a_1}) & \text{if } u_i = v_i, \forall i \in [t]\backslash\{a_1\} \\ \mathbf{O} & \text{otherwise,} \end{cases}$$

and

$$\Phi_{t,a_0}(C)(u,v) = \begin{cases} C(u_{a_0}, v_{a_0}) & \text{if } u_i = v_i, \forall i \in [t]\backslash\{a_0\} \\ \mathbf{O} & \text{otherwise,} \end{cases}$$

where $u, v \in [s^t]$. We also regard $\Phi_{t,a_0}(A)\Phi_{t,a_1}(B)$ and $\Phi_{t,a_1}(B)\Phi_{t,a_0}(C)$ as $s^t \times s^t$ block matrices. Note that $a_0 \neq a_1$. Then by the above we can verify that

$$\begin{aligned} &[\Phi_{t,a_0}(A)\Phi_{t,a_1}(B)](u,v) \\ &= \sum_{w \in [s^t]} \Phi_{t,a_0}(A)(u,w)\Phi_{t,a_1}(B)(w,v) \\ &= \begin{cases} A(u_{a_0}, v_{a_0})B(u_{a_1}, v_{a_1}) & \text{if } u_i = v_i, \forall i \in [t]\backslash\{a_0, a_1\} \\ \mathbf{O} & \text{otherwise,} \end{cases} \end{aligned}$$

and

$$\begin{aligned} &[\Phi_{t,a_1}(B)\Phi_{t,a_0}(C)](u,v) \\ &= \begin{cases} B(u_{a_1}, v_{a_1})C(u_{a_0}, v_{a_0}) & \text{if } u_i = v_i, \forall i \in [t]\backslash\{a_0, a_1\} \\ \mathbf{O} & \text{otherwise.} \end{cases} \end{aligned}$$

Now we can see that

$$\Phi_{t,a_0}(A)\Phi_{t,a_1}(B) = \Phi_{t,a_1}(B)\Phi_{t,a_0}(C)$$

if and only if for any $(i_0, j_0), (i_1, j_1) \in [s]^2$,

$$A(i_0, j_0)B(i_1, j_1) = B(i_1, j_1)C(i_0, j_0).$$

The latter is equivalent to

$$(\mathbf{I}_s \otimes A)(\mathbf{I}_s \boxtimes B) = (\mathbf{I}_s \boxtimes B)(\mathbf{I}_s \otimes C).$$

This concludes our proof.

Appendix C
Proof of Lemma 6

By $k+1 \le d \le n-h$, we have $n \ge k+1+h \ge 4$ because of $k \ge 2$ and $h \ge 1$. Let ω be a primitive element of $\mathbb{F}_q$ with $q \ge 2n \ge 8$. Then we set $\lambda_0 = 0$, $\lambda_i = \omega^{i-1}$ for $1 \le i \le 2n-1$, $\gamma_0 = 0$, and only γ_1 is unassigned. We substitute these values and can compute that

$$\begin{aligned} g(\gamma_{[2]}) &= \gamma_1^2 - 1, \\ f(\lambda_{[4]}, \gamma_{[2]}) &= \det \begin{bmatrix} 1 & 0 & 1 & \gamma_1 \\ 0 & 0 & \omega & \gamma_1\omega^2 \\ 0 & 1 & \gamma_1 & 1 \\ 0 & 1 & \gamma_1\omega & \omega^2 \end{bmatrix} \\ &= \omega(\omega-1)(\omega\gamma_1^2 - \omega - 1), \\ f(\lambda_{4+[4]}, \gamma_{[2]}) &= \det \begin{bmatrix} 1 & 0 & 1 & \gamma_1 \\ \omega^3 & 0 & \omega^5 & \gamma_1\omega^6 \\ 0 & 1 & \gamma_1 & 1 \\ 0 & \omega^4 & \gamma_1\omega^5 & \omega^6 \end{bmatrix} \\ &= (\omega-1)^2\omega^7(\omega^2\gamma_1^2 + \omega\gamma_1^2 - \omega^2 + \gamma_1^2 - 2\omega - 1), \end{aligned}$$

and

$$f(\lambda_{4a+[4]}, \gamma_{[2]}) = \omega^{8a-8} f(\lambda_{4+[4]}, \gamma_{[2]}), \ 1 \le a \le n/2 - 1.$$

Write $F(\gamma_1) = \gamma_1 g(\gamma_{[2]}) f(\lambda_{[4]}, \gamma_{[2]}) f(\lambda_{4+[4]}, \gamma_{[2]})$. Note that the condition (4) is euivalent to $F(\gamma_1) \neq 0$. We see that $F(\gamma_1)$ is a nonzero polynomial in γ_1 with degree at most 7. As $q \ge 8$ we can find a nonzero element in $\mathbb{F}_q$ such that $F(\gamma_1)$ is nonzero, and we assign it to γ_1. This concludes our proof.

Appendix D
Proof of Lemma 8

We prove it by induction on the positive integer z. If $z = 1$, since all the λ_i satisfying (4), we have $\det(M_{a_0,B_0}^{[B_0]}) \neq 0$.

For the inductive hypothesis, we assume that the conclusion holds for an arbitrary positive integer z.

For the case of $z+1$, we have $|B_0| + |B_1| + \cdots + |B_z| = m$. We write $t = |B_0|$. As M_{a_0,B_0} is invertible and all the ns elements λ_{ns} are distinct, according to Lemma 7, there exist $\tilde{\ell}m \times \tilde{\ell}m$ matrix V such that

$$\begin{aligned} &\det(V[M_{a_0,B_0}^{(m)} \ \ M_{a_1,B_1}^{(m)} \ \ \cdots \ \ M_{a_z,B_z}^{(m)}]) \\ &= \det \begin{bmatrix} M_{a_0,B_0}^{(t)} & M_{a_1,B_1}^{(t)} & \cdots & M_{a_z,B_z}^{(t)} \\ \mathbf{O} & \widehat{M}_{a_1,B_1}^{(m-t)} & \cdots & \widehat{M}_{a_z,B_z}^{(m-t)} \end{bmatrix} \\ &= \det\left(M_{a_0,B_0}^{(t)}\right) \det\left([\widehat{M}_{a_1,B_1}^{(m-t)} \ \ \cdots \ \ \widehat{M}_{a_z,B_z}^{(m-t)}]\right) \end{aligned} \tag{10}$$

and each $\widehat{M}^{(m-t)}_{a_i,B_i}$ is column equivalent to $M^{(m-t)}_{a_i,B_i}$. Note that $|B_1|+\cdots+|B_z| = m-t$. By the induction hypothesis, the matrix

$$[M^{(m-t)}_{a_1,B_1} \quad M^{(m-t)}_{a_2,B_2} \quad \cdots \quad M^{(m-t)}_{a_z,B_z}]$$

is invertible. It means that the matrix

$$[\widehat{M}^{(m-t)}_{a_1,B_1} \quad \widehat{M}^{(m-t)}_{a_2,B_2} \quad \cdots \quad \widehat{M}^{(m-t)}_{a_z,B_z}]$$

is also invertible. By (10), we know

$$\det([M^{(m)}_{a_0,B_0} \quad M^{(m)}_{a_1,B_1} \quad \cdots \quad M^{(m)}_{a_z,B_z}]) \neq 0.$$

Appendix E
Proof of Lemma 10

The proof of Lemma 10 is divided into the following two lemmas.

Lemma 12. *For each $i \in \mathcal{F}$, the $n+1$ matrices of size $r\tilde{\ell} \times \tilde{\ell}$,*

$$H_{i,0}, \ldots, H_{i,i-1}, H^{\langle 0\rangle}_{i,i}, H^{\langle 1\rangle}_{i,i}, H_{i,i+1}, \ldots, H_{i,n-1}$$

defines an $(n+1, k+1, \tilde{\ell})$ MDS array code.

Lemma 13. *For $(C_0, \ldots, C_{n-1}) \in \mathcal{C}$, we have*

$$(R^{\mathcal{F}}_i \otimes I_r)(\sum_{j\in[n]} H_j C_j)$$
$$= \sum_{g\in[2]} H^{\langle g\rangle}_{i,i} C^{\langle g\rangle}_{i,i} + \sum_{j\in[n]\setminus\{i\}} H_{i,j} C_{i,j} = \mathbf{0}.$$

Here, Lemma 12 proves the first part of Lemma 10 while Lemma 13 proves the second part of Lemma 10. Combining these two lemmas, we complete our proof.

We first need the following technical lemma. The proof of it is exactly the same as that of [11, Lemma 4], and so we omit its proof. Let

$$K = \begin{bmatrix} K_{0,0} & K_{0,1} \\ K_{1,0} & K_{1,1} \end{bmatrix}$$

be a 2×2 block matrix in which each block entry is a column vector of length r.

Lemma 14. *For any $a, c \in [n/2]$, $b, z \in [2]$, we have*

(i) If $c = a$,

$$(R_{a,b} \otimes \mathbf{I}_r)\Phi_{\frac{n}{2},c}(K)R_{a,z} = \mathbf{I}_{2^{\tilde{c}}} \otimes K_{b,z}.$$

(ii) If $c \neq a$,

$$(R_{a,b} \otimes \mathbf{I}_r)\Phi_{\frac{n}{2},c}(K)R_{a,z} = \begin{cases} \Phi_{\frac{n}{2}-1,\tilde{c}}(K) & \text{if } b = z \\ \mathbf{O} & \text{otherwise.} \end{cases}$$

Here

$$\tilde{c} = \begin{cases} c & \text{if } c < a \\ c-1 & \text{if } c > a \\ \frac{n}{2}-1 & \text{if } c = a. \end{cases}$$

The following result follows directly from the above.

Lemma 15. *For $a, c \in [n/2]$, and $z \in [h]$, we have*

$$(S_{a,0,z} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},c}(K))S^T_{a,g,h-1}$$
$$= \begin{cases} \Phi_{\frac{n}{2},\tilde{c}}(\text{blkdiag}(K_{0,g}, K_{1,g\oplus 1})) & \text{if } a = c, \\ \Phi_{\frac{n}{2},\tilde{c}}(K) & \text{if } a \neq c, g = 0, \\ \mathbf{O} & \text{if } a \neq c, g \neq 0, \end{cases}$$

where $\tilde{c}$ is defined the same as Lemma 14.

Proof. We can compute that

$$(S_{a,0,z} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},c}(K))S^T_{a,g,h-1}$$
$$= \begin{bmatrix} (R_{a,0} \otimes \mathbf{I}_r)\Phi_{\frac{n}{2},c}(K)R_{a,g} & \\ & (R_{a,1} \otimes \mathbf{I}_r)\Phi_{\frac{n}{2},c}(K)R_{a,g\oplus 1}) \end{bmatrix}.$$

The rest follows directly from Lemma 14. □

A. Proof of Lemma 12

To begin with, we must calculate the structure of the $n+1$ matrices

$$H_{i,0}, \cdots, H_{i,i-1}, H^{\langle 0\rangle}_{i,i}, H^{\langle 1\rangle}_{i,i}, H_{i,i+1}, \cdots, H_{i,n-1}. \tag{11}$$

For all $j \in [n]$, let

$$\widetilde{\lfloor \frac{j}{2} \rfloor} = \begin{cases} \lfloor \frac{j}{2} \rfloor & \text{if } \lfloor \frac{j}{2} \rfloor < a \\ \lfloor \frac{n}{2} \rfloor - 1 & \text{if } \lfloor \frac{j}{2} \rfloor = a \\ \lfloor \frac{j}{2} \rfloor - 1 & \text{if } \lfloor \frac{j}{2} \rfloor > a. \end{cases}$$

(1) For any $g \in [2]$, by Lemma 4, we have

$$H^{\langle g\rangle}_{i,i} = (\mathcal{R}^{\mathcal{F}}_i \otimes \mathbf{I}_r)H_i S^T_{a,g,h-1}$$
$$= (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K))S^T_{a,g,h-1}$$

where $K = (U_b \otimes \mathbf{I}_r)K^{(r)}_{a,b}$. Then we can compute that

$$K = (U_b \otimes \mathbf{I}_r)\left(V_b \otimes \mathbf{1}^{(r)}\right) \odot \mathcal{K}^{(r)}_b(\lambda_{2i+[2]})$$
$$= \left(U_b V_b \otimes \mathbf{1}^{(r)}\right) \odot \mathcal{K}^{(r)}_b(\lambda_{2i+[2]})$$
$$= \begin{bmatrix} (1-\gamma_0\gamma_1)L^{(r)}_{2i} & (\gamma_b - \gamma_{b\oplus 1})L^{(t)}_{2i+1} \\ (\gamma_b - \gamma_{b\oplus 1})L^{(r)}_{2i} & (1-\gamma_0\gamma_1)L^{(r)}_{2i+1} \end{bmatrix},$$

where $L^{(r)}_i = L^{(r)}(\lambda_i)$. Using Lemma 15, we can compute that

$$\begin{aligned} H^{\langle 0\rangle}_{i,i} &= (1-\gamma_0\gamma_1)\Phi_{\frac{n}{2},\widetilde{\lfloor \frac{i}{2} \rfloor}}(\text{blkdiag}(L_{2i}, L_{2i+1})), \\ H^{\langle 1\rangle}_{i,i} &= (\gamma_b - \gamma_{b\oplus 1})\Phi_{\frac{n}{2},\widetilde{\lfloor \frac{i}{2} \rfloor}}(\text{blkdiag}(L_{2i+1}, L_{2i})). \end{aligned} \tag{12}$$

(2) For $j \in [n] \setminus \{i\}$ and $\lfloor \frac{j}{2} \rfloor = a$, we have $j = 2a + (b \oplus 1)$ and

$$H_{i,j} = (\mathcal{R}^{\mathcal{F}}_i \otimes \mathbf{I}_r)H_j S^T_{a,0,h-1}$$
$$= (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K))S^T_{a,0,h-1}$$

where $K = (U_b \otimes \mathbf{I}_r)K^{(r)}_{a,b\oplus 1}$. Then we can compute that

$$K = (U_b \otimes \mathbf{I}_r)\left(V_{b\oplus 1} \otimes \mathbf{1}^{(r)}\right) \odot \mathcal{K}^{(r)}_{b\oplus 1}(\lambda_{2j+[2]})$$
$$= \left(U_b V_{b\oplus 1} \otimes \mathbf{1}^{(r)}\right) \odot \mathcal{K}^{(r)}_{b\oplus 1}(\lambda_{2j+[2]})$$
$$= \begin{bmatrix} (1-\gamma^2_{b\oplus 1})L^{(r)}_{2j} & \\ & (1-\gamma^2_{b\oplus 1})L^{(r)}_{2j+1} \end{bmatrix},$$

where $L_i^{(r)} = L^{(r)}(\lambda_i)$. Using Lemma 15, we can compute that

$$H_{i,j} = (1-\gamma_{b\oplus 1}^2)\Phi_{\frac{n}{2},\widetilde{\lfloor \frac{j}{2} \rfloor}}(\text{blkdiag}(L_{2j}, L_{2j+1})). \quad (13)$$

(3) For $j \in [n] \setminus \{i\}$ and $\lfloor \frac{j}{2} \rfloor \neq a$,

$$\begin{aligned} H_{i,j} =& (S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j S_{a,0,h-1}^T \\ =& (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},\lfloor \frac{j}{2} \rfloor}(K)) S_{a,0,h-1}^T. \end{aligned}$$

where $K = K^{(r)}_{\lfloor \frac{j}{2} \rfloor, j \bmod 2}$. And by Lemma 15, we can directly compute that

$$H_{i,j} = \Phi_{\frac{n}{2},\widetilde{\lfloor \frac{j}{2} \rfloor}}(K^{(r)}_{\lfloor \frac{j}{2} \rfloor, j \bmod 2}). \quad (14)$$

From (12)-(14) we can observe that the structure of $n+1$ matrices defined in (11) is similar to that of parity check sub-matrices of (5). Using Lemma 7 and the same approach as in Lemma 8, we can prove Lemma 12.

B. Proof of Lemma 13

Firstly, for $z \in [h]$, we define an $(h+1) \times (h+1)$ block matrix

$$Q_z(i,j) = \begin{cases} \mathbf{I}_{\tilde{\ell}} & \text{if } i = j \in [h+1]\backslash[2] \\ -\mathbf{I}_{\tilde{\ell}} & \text{if } i \in [2],\ j = z+2 \\ \mathbf{O} & \text{otherwise,} \end{cases} \quad (15)$$

and we can see that Q_z is an $\ell \times \ell$ matrix. Furthermore, we have the following two lemmas, which can be proved directly by (7), (8) and (15).

Lemma 16. *For any $a \in [n/2]$ and $z \in [h]$,*

$$\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,z} + Q_z = \mathbf{I}_\ell. \quad (16)$$

Lemma 17. *For any $z \in [h]$, $a \in [n/2]$ and $r\tilde{\ell} \times \tilde{\ell}$ matrix M, we have*

$$(S_{a,0,z} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes M) Q_z = \mathbf{O}.$$

For each $i \in \mathcal{F}$, we write $i = 2a + b$, where $a \in [n/2]$ and $b \in [2]$. We also write $E_{a,b} = \mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(U_b)$, and $R_i^{\mathcal{F}} = S_{a,0,\hat{i}} E_{a,b}$. Further, we have

$$\begin{aligned} & (R_i^{\mathcal{F}} \otimes \mathbf{I}_r)(\sum_{j\in[n]} H_j C_j) && (17) \\ =& \sum_{j\in[n]} (R_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j C_j && (18) \\ =& \sum_{j\in[n]} (R_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j (\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}}) C_j && (19) \\ =& \sum_{g\in[2]} H_{i,i}^{\langle g\rangle} C_{i,i}^{\langle g\rangle} + \sum_{j\in[n]\backslash\{i\}} H_{i,j} C_{i,j} && (20) \\ =& \mathbf{0}. && (21) \end{aligned}$$

Using (16) with $z = \hat{i}$, we can get (19) from (18). Then we divide the derivation process from (19) to (20) into three cases:

1) If $j = i$,

$$\begin{aligned} & (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r)(\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}}) C_i \\ =& \sum_{g\in[2]} \left[(\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_i S_{a,g,h-1}^T\right](S_{a,g,\hat{i}} C_i) \\ & + (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_i Q_{\hat{i}} C_i \\ =& \sum_{g\in[2]} \left[(S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) S_{a,g,h-1}^T\right](S_{a,g,\hat{i}} C_i) \\ & + (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) Q_{\hat{i}} C_i \end{aligned}$$

where $K = (U_b \otimes \mathbf{I}_r) K_{a,b}^{(r)}$. By Lemma 17, we have

$$(S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) Q_{\hat{i}} = \mathbf{O}.$$

Therefore, by the definition of $H_{i,i}^{\langle g\rangle}, C_{i,i}^{\langle g\rangle}$ for $g \in [2]$, we have

$$\begin{aligned} & (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_i (\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}}) C_i \\ =& \sum_{g\in[2]} \left[(\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_i S_{a,g,h-1}^T\right](S_{a,g,\hat{i}} C_i) \\ =& \sum_{g\in[2]} H_{i,i}^{\langle g\rangle} C_{i,i}^{\langle g\rangle}, \end{aligned}$$

2) For $j \in [n]\backslash\{i\}$ and $\lfloor j/2 \rfloor = a$, The same as in above, we have

$$\begin{aligned} & (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j (\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}}) C_j \\ =& \sum_{g\in[2]} \left[(S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) S_{a,g,h-1}^T\right](S_{a,g,\hat{i}} C_j) \\ & + (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) Q_{\hat{i}} C_j \end{aligned}$$

where $K = (U_b \otimes \mathbf{I}_r) K_{a,b\oplus 1}^{(r)}$.By Lemma 17, we have

$$(S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) Q_{\hat{i}} = \mathbf{O}.$$

We can compute that

$$K = \begin{bmatrix} (1-\gamma_{b\oplus 1}^2) L_{2j}^{(r)} & \\ & (1-\gamma_{b\oplus 1}^2) L_{2j+1}^{(r)} \end{bmatrix},$$

then by Lemma 15 we can get

$$\begin{aligned} & (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j S_{a,g,h-1}^T \\ =& (S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},a}(K)) S_{a,1,h-1}^T \\ =& \mathbf{O}. \end{aligned}$$

then by the definition of $H_{i,j}, C_{i,j}$, we can conclude that

$$\begin{aligned} & (\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j (\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}}) C_j \\ =& \left[(\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j S_{a,0,h-1}^T\right](S_{a,0,\hat{i}} C_j) \\ =& H_{i,j} C_{i,j}. \end{aligned}$$

3) For $j \in [n]\backslash\{i\}$ and $\lfloor j/2 \rfloor \neq a$. Using Lemma 3 directly, we have

$$(E_{a,b} \otimes \mathbf{I}_r) H_j \mathbf{I}_\ell = H_j \mathbf{I}_\ell E_{a,b},$$

then

$$
\begin{aligned}
&(\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j \Big(\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}} \Big) C_j \\
=&(S_{a,0,\hat{i}} \otimes \mathbf{I}_r)(E_{a,b} \otimes \mathbf{I}_r) H_j \Big(\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}} \Big) C_j \\
=&(S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j \Big(\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}} \Big) E_{a,b} C_j \\
=&\sum_{g\in[2]} \left[(S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j S_{a,g,h-1}^T \right] (S_{a,g,\hat{i}} E_{a,b} C_j) \\
&+ (S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j Q_{\hat{i}} E_{a,b} C_j.
\end{aligned}
$$

Because $H_j = \left(\mathbf{I}_{h+1} \otimes \Phi_{\frac{n}{2},\lfloor \frac{j}{2} \rfloor} (K^{(r)}_{\lfloor \frac{j}{2} \rfloor, j \bmod 2}) \right)$, using Lemma 15 and Lemma 17, we have

i. $(S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j S_{a,1,h-1}^T = \mathbf{O}$
ii. $(S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j Q_{\hat{i}} = \mathbf{O}$

Therefore, by the definition of $H_{i,j}, C_{i,j}$, we have

$$
\begin{aligned}
&(\mathcal{R}_i^{\mathcal{F}} \otimes \mathbf{I}_r) H_j \Big(\sum_{g\in[2]} S_{a,g,h-1}^T S_{a,g,\hat{i}} + Q_{\hat{i}} \Big) C_j \\
=&\left[(S_{a,0,\hat{i}} \otimes \mathbf{I}_r) H_j S_{a,0,h-1}^T \right] (S_{a,0,\hat{i}} E_{a,b} C_j) \\
=&H_{i,j} C_{i,j}.
\end{aligned}
$$

Appendix F
Proof of Lemma 11

For any $i, j \in \mathcal{F}$, we write $i = 2a + b$ where $a \in [n/2]$ and $b \in [2]$. We define

$$
P_{j,i} = \begin{cases}
\begin{bmatrix} R_{\lfloor \frac{j}{2} \rfloor,0} \\ R_{\lfloor \frac{j}{2} \rfloor,1} \end{bmatrix} & \text{if } \lfloor \tfrac{j}{2} \rfloor = a, \\
\begin{bmatrix} R_{\lfloor \frac{j}{2} \rfloor,0} \\ R_{\lfloor \frac{j}{2} \rfloor,1} \end{bmatrix} \Phi_{\frac{n}{2},\lfloor \frac{j}{2} \rfloor}(U_{j \bmod 2}) & \text{if } \lfloor \tfrac{j}{2} \rfloor \neq a,
\end{cases}
$$

which is an invertible matrix.

We also define $E_z = \mathbf{I}_{\tilde{\ell}} \boxtimes e_z$ where e_z is the z-th row of $\mathbf{I}_{h+1}$ and regarded as a $1 \times (h+1)$ block matrix. We will split the proof into two cases.

Case 1: $\hat{i} \in [h-1]$

We can see

$$
D_{i,i}^{\langle 0 \rangle} = \begin{bmatrix} R_{a,0} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}
\quad \begin{matrix} \\ \downarrow \\ (\hat{i}+2)\text{-th block column} \end{matrix}
$$

$$
D_{i,i}^{\langle 1 \rangle} = \begin{bmatrix} R_{a,1} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}
$$

By performing operations on the rows of the matrices, we can get

$$
\begin{aligned}
M_0 &= \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 0 \rangle} + \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 1 \rangle} \right) \\
&= \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \begin{bmatrix} R_{a,0} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} \\ R_{a,1} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&= E_0 + E_{\hat{i}+2}. \qquad (22)
\end{aligned}
$$

$$
\begin{aligned}
M_1 &= \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \end{bmatrix} D_{i,i}^{\langle 0 \rangle} + \begin{bmatrix} \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 1 \rangle} \right) \\
&= \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \begin{bmatrix} \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&= \begin{bmatrix} \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&= E_1 + E_{\hat{i}+2}. \qquad (23)
\end{aligned}
$$

Let $k \in \mathcal{F}$ with $\hat{k} = h-1$, then we can check that

$$
\begin{aligned}
E_{\hat{i}+2} &= P_{k,i}^{-1} \left(\begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} P_{k,i} M_0 + \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \end{bmatrix} P_{k,i} M_1 - D_{k,i} \right) \\
&= \begin{bmatrix} \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&\qquad\qquad\qquad\qquad \uparrow \\
&\qquad (\hat{i}+2)\text{-th block column}
\end{aligned}
$$

and we have

$$
\begin{aligned}
E_0 &= M_0 - E_{\hat{i}+2} = \begin{bmatrix} \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
E_1 &= M_1 - E_{\hat{i}+2} = \begin{bmatrix} \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \cdots & \mathbf{O} \end{bmatrix}.
\end{aligned}
$$

In the end, for any $j \in \mathcal{F} \backslash \{i, k\}$, (i.e. $\hat{j} \neq h-1, \hat{i}$), we have

$$
\begin{aligned}
E_{\hat{j}+2} &= P_{j,i}^{-1} \left(D_{j,i} - \begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} P_{j,i} E_0 - \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \end{bmatrix} P_{j,i} E_1 \right) \\
&= \begin{bmatrix} \mathbf{O} & \cdots & \mathbf{O} & \mathbf{I}_{\tilde{\ell}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix} \\
&\qquad\qquad\qquad\qquad \uparrow \\
&\qquad (\hat{j}+2)\text{-th block column}
\end{aligned}
$$

Therefore, we can obtain all E_z for $z \in [h+1]$ by using the row operators mentioned above. This implies that the $\ell \times \ell$ matrix formed by vertically joining the $h+1$ matrices, which includes $D_{i,i}^{\langle g \rangle}, g \in [2], D_{j,i}, j \in \mathcal{F} \backslash \{i\}$, is invertible for all $i \in \mathcal{F}$ satisfying $\hat{i} \in [h-1]$.

Case 2: $\hat{i} = h-1$

In this case, we can see

$$
D_{i,i}^{\langle 0 \rangle} = \begin{bmatrix} R_{a,0} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & R_{a,1} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}
$$

$$
D_{i,i}^{\langle 1 \rangle} = \begin{bmatrix} R_{a,1} & \mathbf{O} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & R_{a,0} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}
$$

As same as case 1, we can get

$$
E_0 = \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 0 \rangle} + \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 1 \rangle} \right)
$$

$$
E_1 = \begin{bmatrix} R_{a,0} \\ R_{a,1} \end{bmatrix}^{-1} \left(\begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \end{bmatrix} D_{i,i}^{\langle 0 \rangle} + \begin{bmatrix} \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} D_{i,i}^{\langle 1 \rangle} \right).
$$

And then for all $j \in \mathcal{F} \backslash \{i\}$, we have

$$
E_{\hat{j}+2} = P_{j,i}^{-1} \left(D_{j,i} - \begin{bmatrix} \mathbf{I}_{\tilde{\ell}/2} & \mathbf{O} \\ \mathbf{O} & \mathbf{O} \end{bmatrix} P_{j,i} E_0 - \begin{bmatrix} \mathbf{O} & \mathbf{O} \\ \mathbf{O} & \mathbf{I}_{\tilde{\ell}/2} \end{bmatrix} P_{j,i} E_1 \right)
$$

$$= \begin{bmatrix} \mathbf{O} & \cdots & \mathbf{O} & \underset{\substack{\uparrow \\ (\hat{j}+2)\text{-th block column}}}{\mathbf{I}_{\tilde{\ell}}} & \mathbf{O} & \cdots & \mathbf{O} \end{bmatrix}.$$

As the result, we get all E_z for $z \in [h+1]$ again, which means the $\ell \times \ell$ matrix formed by vertically joining the $h+1$ matrices $D_{i,i}^{\langle g \rangle}, g \in [2], D_{j,i}, j \in \mathcal{F} \backslash \{i\}$, is invertible for $\hat{i} = h-1$.