A Note on Parity Check Matrices of Private Information Retrieval Codes

Koki Kazama Takahiro Yoshida

June 10, 2024

Abstract

A private information retrieval (PIR) is an information retrieval scheme that allows a user to retrieve messages from information databases while keeping secret which one the user wants to retrieve. Sun et al. formulated the download rate and showed that there is an upper limit to it (PIR capacity). Previous construction methods for a capacity-achieving linear PIR (CALPIR) are ad hoc. We show a suffiecient condition of a CALPIR using its extended parity check matrix.

The full version of this paper is in [1].

1 Introduction

A private information retrieval (PIR) is a scheme that allows a user to retrieve messages from an information database (DB) while keeping secret which one the user wants to retrieve (user's privacy). One scheme is for the user to download all information from all DBs. However, the communication efficiency of this scheme is low. We construct a PIR with high communication efficiency. Chor et al. first studied a PIR [2]. Since Sun et al. studied a PIR [3] using information theory and coding theory, numerous studies have followed Sun's study.

The scheme of a PIR [3] and this study is as follows: Multiple databases store multiple messages. First, the user generates queries and sends them to the DBs. Then, each DB generates responses based on the query and all messages and sends a response to the user. Lastly, the user decodes the message that the user wants to retrieve. Each DB independently tries to guess which message the user wants when receiving a query, while each DB cannot obtain any information about it.

Sun et al. [3] formulated the user's privacy and a download rate, which is the communication efficiency when a user receives responses from all DBs, using information theory and showed that there exists an upper limit (PIR capacity) to the download rate when we fix the numbers of the DBs and the messages. The representative construction methods for a PIR that achieves the capacity and whose response-generating function (encoder) and decoding function (decoder) are linear (capacity-achieving linear PIR, CALPIR) are the study by Sun et al. [3] and that by Tian et al. [4].

Our ultimate goal is to propose a systematic construction method for a large subclass of CALPIRs. We want such a subclass of PIRs because there must be a variety of evaluation criteria other than the download rate and reasonable PIRs that have advantages under these criteria other than the PIRs cited earlier. The construction methods in previous studies were ad hoc because describing the converse part of the proof of the PIR capacity using entropy did not clarify the conditions of the encoder and the decoder in the form of matrices.

As an intermediate step to our goal, this study shows a sufficient condition of a CALPIR by using its extended parity check matrix (EPCM) and, as a supplementary, a part of a construction method of the EPCM satisfying this condition. We explain the definition of EPCMs later. Using EPCMs make conditions for generator matrices of CALPIRs explicit since the parity check matrices decompose complex conditions that we want CALPIRs to satisfy into several simple conditions and each block row of the parity check matrices directly represents those conditions. Although several previous studies [5] [6] considered parity check matrices of PIRs, the policies differs from that of this study.

2 Reformulation of Previous Studies: The Capacity of PIRs

This section reformulates the previous studies of PIRs generally. Specifically, an encoder, a decoder and a decoder matrix are original to this study.

2.1 Definition of PIRs

We explain thedefinition of a PIR concerning [3] [4].

First, we define notations. $\mathbb{N} \coloneqq \{1, 2, 3, \dots\}$. $[m, n] \coloneqq \{ m, m+1, \dots, n \}$ and $[n] \coloneqq [1, n]$ for any $m, n \in \mathbb{N}$. All vectors are row vectors except specifically noted. $\boldsymbol{E}^\top$ denotes the transpose of a matrix $\boldsymbol{E}$. $\mathbb{F}_p$ is a finite field with p elements. $\mathbb{F}_p^{n \times m}$ denotes the set of all $n \times m$ matrices over $\mathbb{F}_p$, and $\mathbb{F}_p^n \coloneqq \mathbb{F}_p^{1 \times n}$. For any $\boldsymbol{a} = (a_1, \dots, a_n)$ and $A \subset [n]$, $i \in [n]$, we define $\boldsymbol{a}_A \coloneqq (a_i)_{i \in A}$ and $\boldsymbol{a}_i \coloneqq a_i = \boldsymbol{a}_{\{i\}}$. $\mathrm{Uni}(A)$ denotes the uniform distribution on a finite set A. $\boldsymbol{I}_n$ denotes the $n \times n$ identity matrix. The base of the logarithm in Shannon entropy H is p. $\sqcup$ denotes the direct sum of mutually exclusive sets.

Next, we define an information retrieval (IR) and a PIR.

Definition 2.1 ((replicated) PIR [3] [4] [7]) *Let $L_\mathrm{w}, L_\mathrm{a}, M, N, S$ be positive integers with $M, N \geq 2$. Let p be a prime power. Let $\boldsymbol{W} = (W_1, \dots, W_M)$ be a random variable vectors such that $W_1 = (W_{1,1}, \dots, W_{1,L_\mathrm{w}}), \dots, W_M = (W_{M,1}, \dots, W_{M,L_\mathrm{w}}) \overset{\text{i.i.d}}{\sim} \mathrm{Uni}\left(\mathbb{F}_p^{L_\mathrm{w}}\right)$. Let $\boldsymbol{S}(\sim \mathrm{Uni}([S]))$ be a random variable independent of $\boldsymbol{W}$. Let $\phi_n \colon \mathbb{N} \times \mathbb{F}_p^{L_\mathrm{w} M} \to \mathbb{F}_p^{L_\mathrm{a}}$ for $n \in [N]$, $\chi \colon [M] \times [S] \to \mathbb{N}^N$ and $\psi \colon [M] \times [S] \times \mathbb{F}_p^{L_\mathrm{a} N} \to \mathbb{F}_p^{L_\mathrm{w}}$ be functions. For any $\boldsymbol{q} = (q_1, \dots, q_N)$, we define $R(\boldsymbol{q}) \coloneqq \{ (n, q_n) \mid n \in [N] \}$.*

There are N DBs and each DB stores a local encoder ϕ, a local decoder ψ, and a message vector $\boldsymbol{W}$. M is the message length and L_{w} is the message symbol length. The user retrieves W_m by 3 phases, where $m(\in [M])$ is a desired index.

⟨Query Phase⟩ The user generates a query vector $(Q_1^{(m)}, \dots, Q_N^{(m)}) \coloneqq \chi(m, \boldsymbol{S})$ and send a query $Q_n^{(m)}$ to each DB $n \in [N]$.

⟨Answer Phase⟩ Each DBn sends a responce $A_{\left(n, Q_n^{(m)}\right)} \coloneqq \phi_n \left(Q_n^{(m)}, \boldsymbol{W} \right)$ to the user.

⟨Decoding Phase⟩ The user decodes W_m from m, S and the responce vector$\boldsymbol{A}_{R\left(\boldsymbol{Q}^{(m)}\right)} \coloneqq \left(\phi_n \left(Q_n^{(m)}, \boldsymbol{W} \right) \right)_{n \in [N]}$ using ψ. We define $\hat{W}_m$ as the decoding result of W_m, i.e.

$$\hat{W}_m \coloneqq \psi \left(m, \boldsymbol{S}, \left(\phi_n \left(\chi_n(m, \boldsymbol{S}), \boldsymbol{W} \right) \right)_{n \in [N]} \right), \tag{1}$$

where $\chi_n(m, \boldsymbol{S}) = Q_n^{(m)}$ is the n th entry of $\boldsymbol{Q}^{(m)}$ for $n \in [N]$. We define an information retrieval (IR) with the parameters $(M, N, L_{\mathrm{w}}, L_{\mathrm{a}}, p)$ as this protocol. Hereafter we omit "with the parameters $(M, N, L_{\mathrm{w}}, L_{\mathrm{a}}, p)$."

We define a decodable information retrieval (DIR) as an IR satisfies the (user's) decodaable constraint Eq.(2), i.e. $W_m = \hat{W}_m$. In other words,

$$\begin{aligned} &\forall m \in [M], \forall \boldsymbol{s} \in [S], \forall \boldsymbol{w} = (w_1, \dots, w_M) \in \mathbb{F}_p^{L_{\mathrm{w}} M}, \\ &w_m = \psi \left(m, \boldsymbol{s}, \left(\phi_n \left(\chi_n(m, \boldsymbol{s}), \boldsymbol{w} \right) \right)_{n \in [N]} \right). \end{aligned} \tag{2}$$

Moreover, we define a (replicated) private information retrieval (PIR) as an IR satisfying the (user's) decodaable constraint Eq.(2) and the (user's) privacy constraint Eq.(3).

$$\begin{aligned} &\forall m \in [M], \forall m' \in [M], \forall n \in [N], \forall q \in \mathbb{N}, \\ &\Pr \left(Q_n^{(m)} = q \right) = \Pr \left(Q_n^{(m')} = q \right). \end{aligned} \tag{3}$$

Remark 2.1 *In an IR, instead of sending $\boldsymbol{Q}^{(m)}$, the user may send $\left(\phi_n \left(Q_n^{(m)}, \cdot \right) \middle| n \in [N] \right)$.*

For simplicity, we assume Assumption2.1.

Assumption 2.1 *A function $\chi(m, \cdot)$ is injective for any $m \in [M]$. $\mathcal{Q}_n \coloneqq \left\{ q \in \mathbb{N} \middle| \Pr \left(Q_n^{(m)} = q \right) > 0 \right\} = \{ \chi_n(m, \boldsymbol{s}) \mid \boldsymbol{s} \in [S] \}$ does not depend on m for any IR.*

The first sentence in Assumption 2.1 shows that the last equaltion in Eq.(3) is equivalent to

$$\left| \left\{ (q_1, \dots, q_N) \in \boldsymbol{\mathcal{Q}}^{(m)} \middle| q_n = q \right\} \right| = \left| \left\{ (q_1, \dots, q_N) \in \boldsymbol{\mathcal{Q}}^{(m')} \middle| q_n = q \right\} \right| \tag{4}$$

where $\boldsymbol{\mathcal{Q}}^{(m)} \coloneqq \{ \chi(m, \boldsymbol{s}) \mid \boldsymbol{s} \in [S] \}$ (the m-th *query vector set*). This is a slight modification of Condition 11 in [8].

The second sentence in Assumption 2.1 is valid if an IR is a PIR.

Definition 2.2 (codeword) *We define a codeword of the IR as a random variable vector* $(\phi_n(q, \boldsymbol{W}))_{n\in[N],q\in\mathcal{Q}_n}$*.*

The idea of considering IRs as codes appeared in [7] [9] although codeword indices are different with this study.

Definition 2.3 (encoder, decoder) *For an IR, we define functions* $\Phi\colon \mathbb{F}_p^{L_\mathrm{w}M} \to \mathbb{F}_p^{L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|}$ *(encoder) and* $\Psi\colon [M]\times[S]\times\mathbb{F}_p^{L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|} \to \mathbb{F}_p^{L_\mathrm{w}MS}$ *(decoder) as*

$$\Phi(\boldsymbol{w}) \coloneqq (\phi_n(q,\boldsymbol{w}))_{n\in[N],q\in\mathcal{Q}_n}, \tag{5}$$

$$\Psi(\boldsymbol{a}) \coloneqq \left(\psi\left(m,\boldsymbol{s},\boldsymbol{a}_{R(\chi(m,\boldsymbol{s}))}\right)\right)_{m\in[M],\boldsymbol{s}\in[S]} \tag{6}$$

for any $\boldsymbol{w}\in\mathbb{F}_p^{L_\mathrm{w}M}$ *and* $\boldsymbol{a}\in\mathbb{F}_p^{L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|}$*.*

Then, Eq.(2) is equivalent to that for any $\boldsymbol{w}\in\mathbb{F}_p^{L_\mathrm{w}M}$,

$$\Psi(\Phi(\boldsymbol{w})) = (\underbrace{w_1,\dots,w_1}_{S},\dots,\underbrace{w_M,\dots,w_M}_{S}). \tag{7}$$

2.2 Linear PIR

We redefine a linear PIR (LPIR) concerning [4], [8].

Definition 2.4 (a linear PIR [4] [8]) *We define a linear IR (LIR) as an IR such that there exists matrices* $\boldsymbol{G}_{(n,\chi_n(m,\boldsymbol{s}))}\in\mathbb{F}_p^{L_\mathrm{w}M\times L_\mathrm{a}}$ *(local generator matrix) and* $\boldsymbol{D}_{\boldsymbol{s},\cdot}^{(m)}\in\mathbb{F}_p^{L_\mathrm{w}\times NL_\mathrm{a}}$ *(local decoder matrix) such that* $\phi_n(\chi_n(m,\boldsymbol{s}),\boldsymbol{w}) = \boldsymbol{w}\boldsymbol{G}_{(n,\chi_n(m,\boldsymbol{s}))}$ *and* $\psi(m,\boldsymbol{s},\boldsymbol{a}') = \boldsymbol{a}'\left(\boldsymbol{D}_{\boldsymbol{s},\cdot}^{(m)}\right)^\top$ *for any* $n\in[N],\boldsymbol{s}\in[S],\boldsymbol{w}\in\mathbb{F}_p^{L_\mathrm{w}M},\boldsymbol{a}'\in\mathbb{F}_p^{L_\mathrm{a}N}$*. A DIR and PIR which are also LIRs are referred to as a linear DIR (LDIR) and linear PIR (LPIR), respectively.*

Definition 2.5 (generator matrix [4], decoder matrix [8]) *For an LIR, there exist a matrix* $\boldsymbol{G}\in\mathbb{F}_p^{L_\mathrm{w}M\times L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|}$ *(generator matrix) and a matrix* $\tilde{\boldsymbol{D}}\in\mathbb{F}_p^{L_\mathrm{w}MS\times L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|}$ *(decoder matrix) such that for any* $\boldsymbol{w}\in\mathbb{F}_p^{L_\mathrm{w}M}$ *and* $\boldsymbol{a}\in\mathbb{F}_p^{L_\mathrm{a}\sum_{n\in[N]}|\mathcal{Q}_n|}$*, it holds that* $\Phi(\boldsymbol{w}) = \boldsymbol{w}\boldsymbol{G}$ *and* $\Psi(\boldsymbol{a}) = \boldsymbol{a}\tilde{\boldsymbol{D}}^\top$*.*

We construct the generator matrix from the local generator matrices and the decoder matrix from the local decoding matrices.

$$\boldsymbol{G} \coloneqq \begin{pmatrix} \boldsymbol{G}_{(1,1)}^{(1)} & \cdots & \boldsymbol{G}_{(1,|\mathcal{Q}_1|)}^{(1)} & \cdots & \boldsymbol{G}_{(N,1)}^{(1)} & \cdots & \boldsymbol{G}_{(N,|\mathcal{Q}_N|)}^{(1)} \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ \boldsymbol{G}_{(1,1)}^{(M)} & \cdots & \boldsymbol{G}_{(1,|\mathcal{Q}_1|)}^{(M)} & \cdots & \boldsymbol{G}_{(N,1)}^{(M)} & \cdots & \boldsymbol{G}_{(N,|\mathcal{Q}_N|)}^{(M)} \end{pmatrix}, \tag{8}$$

where $\boldsymbol{G}^{(m)}_{(n,q)} \in \mathbb{F}_p^{L_{\mathrm{w}} \times L_{\mathrm{a}}}$ for any $m \in [M], n \in [N], q \in \mathcal{Q}_n$. Each block column is

$$\boldsymbol{G}_{(n,q)} \coloneqq \begin{pmatrix} \boldsymbol{G}^{(1)}_{(n,q)} \\ \vdots \\ \boldsymbol{G}^{(M)}_{(n,q)} \end{pmatrix}$$

and each block row is

$$\boldsymbol{G}^{(m)} \coloneqq \begin{pmatrix} \boldsymbol{G}^{(m)}_{(1,1)} & \dots & \boldsymbol{G}^{(m)}_{(N,|\mathcal{Q}_N|)} \end{pmatrix}.$$

We define $\boldsymbol{G}_{R(\boldsymbol{q})} \coloneqq \left(\boldsymbol{G}_{(n,q_n)}\right)_{n\in[N]}$ for any $\boldsymbol{q} = (q_1, \dots, q_N) \in \boldsymbol{\mathcal{Q}}^{(m)}$. We devide $\boldsymbol{D}^{(m)}_{\boldsymbol{s},\cdot} = \begin{pmatrix} \boldsymbol{D}^{(m)}_{\boldsymbol{s},1} & \dots & \boldsymbol{D}^{(m)}_{\boldsymbol{s},N} \end{pmatrix}$ so that $\boldsymbol{D}^{(m)}_{\boldsymbol{s},n} \in \mathbb{F}_p^{L_{\mathrm{w}} \times L_{\mathrm{a}}}$. Moreover, we define

$$\tilde{\boldsymbol{D}} = \begin{pmatrix} \tilde{\boldsymbol{D}}^{(1)} \\ \vdots \\ \tilde{\boldsymbol{D}}^{(M)} \end{pmatrix}, \ \tilde{\boldsymbol{D}}^{(m)} = \begin{pmatrix} \tilde{\boldsymbol{D}}^{(m)}_{1,\cdot} \\ \vdots \\ \tilde{\boldsymbol{D}}^{(m)}_{S,\cdot} \end{pmatrix} \tag{9}$$

$$\tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},\cdot} = \begin{pmatrix} \tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(1,1)} & \dots & \tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(1,|\mathcal{Q}_1|)} & \dots & \tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(N,1)} & \dots & \tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(N,|\mathcal{Q}_N|)} \end{pmatrix} \tag{10}$$

$$\mathbb{F}_p^{L_{\mathrm{w}} \times L_{\mathrm{a}}} \ni \tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(n,q)} \coloneqq \begin{cases} \boldsymbol{D}^{(m)}_{\boldsymbol{s},n} \text{ if } q = \chi_n(m, \boldsymbol{s}) \\ \boldsymbol{0}_{L_{\mathrm{w}} \times L_{\mathrm{a}}} \text{ otherwise.} \end{cases} \tag{11}$$

Remark 2.2 *Similary as Remark 2.2, in an LIR, instead of sending $\boldsymbol{Q}^{(m)}$, the user may send $\boldsymbol{G}_{R(\boldsymbol{Q}^{(m)})}$.*

Lemma 2.1 (decoding of an LIR) *We define $\boldsymbol{J} \in \mathbb{F}_p^{L_{\mathrm{w}}MS \times L_{\mathrm{w}}M}$ as the transpose of a matrix in Eq.*(12)*, where $\boldsymbol{0} \in \mathbb{F}_p^{L_{\mathrm{w}} \times L_{\mathrm{w}}}$.*

$$\begin{array}{c} \left(\begin{array}{ccccccc} \boldsymbol{I}_{L_{\mathrm{w}}} & \dots & \boldsymbol{I}_{L_{\mathrm{w}}} & \dots & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \dots & \boldsymbol{0} & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \dots & \boldsymbol{0} & \dots & \boldsymbol{I}_{L_{\mathrm{w}}} & \dots & \boldsymbol{I}_{L_{\mathrm{w}}} \end{array}\right) \left.\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right\} L_{\mathrm{w}}M \\ \underbrace{\hphantom{\boldsymbol{I}_{L_{\mathrm{w}}} \dots \boldsymbol{I}_{L_{\mathrm{w}}}}}_{L_{\mathrm{w}}S} \qquad \qquad \underbrace{\hphantom{\boldsymbol{I}_{L_{\mathrm{w}}} \dots \boldsymbol{I}_{L_{\mathrm{w}}}}}_{L_{\mathrm{w}}S} \end{array} \tag{12}$$

Then for an LIR, Eq. (7) *is equivalent to*

$$\tilde{\boldsymbol{G}} \begin{pmatrix} -\boldsymbol{J} & \tilde{\boldsymbol{D}} \end{pmatrix}^{\top} = \boldsymbol{0}_{L_{\mathrm{w}}M \times L_{\mathrm{w}}MS}, \tag{13}$$

where $\tilde{\boldsymbol{G}} \coloneqq (\boldsymbol{I}_{L_{\mathrm{w}}M}, \boldsymbol{G})$ and $\boldsymbol{G}$ is a generator matrix.

This lemma is a modification of Propositon 9 in [8].

Proof *We define* $\boldsymbol{L}^{(m)} := \begin{pmatrix} \boldsymbol{0}_{(m-1)L_{\mathrm{w}} \times L_{\mathrm{w}}} \\ \boldsymbol{I}_{L_{\mathrm{w}}} \\ \boldsymbol{0}_{(M-m)L_{\mathrm{w}} \times L_{\mathrm{w}}} \end{pmatrix}$ *For an LIR, Eq.*(2) *is equivalent to that* $\boldsymbol{w}\boldsymbol{G}_{R(\chi(m,\boldsymbol{s}))} \left(\boldsymbol{D}^{(m)}_{\boldsymbol{s},\cdot}\right)^{\top} = w_m$ *for any* $\boldsymbol{w}, m, \boldsymbol{s}$*. This equation is equivalent to* $\boldsymbol{G}_{R(\chi(m,\boldsymbol{s}))} \left(\boldsymbol{D}^{(m)}_{\boldsymbol{s},\cdot}\right)^{\top} = \boldsymbol{L}^{(m)}$*. Thus, for an LIR, Eq.* (7) *is equivalent to* $\boldsymbol{G}\tilde{\boldsymbol{D}}^{\top} = \boldsymbol{J}^{\top}$*.* □

Hereafter we define $\boldsymbol{P} := \begin{pmatrix} -\boldsymbol{J} & \tilde{\boldsymbol{D}} \end{pmatrix}$.

2.3 Rate and the PIR Capacity

The communication efficiency of an IR (not necessarily an LPIR) is the (download) rate. We do not discuss upload cost.

Definition 2.6 (rate [3]) *We define the rate of an IR as*

$$\mathrm{rate}_{\mathrm{I}} := \min_{m \in [M]} \frac{L_{\mathrm{w}}}{\mathrm{H}\left(\boldsymbol{A}^{(m)} | \boldsymbol{Q}^{(m)}\right)}. \tag{14}$$

It holds that $\mathrm{rate}_{\mathrm{I}} = \min_{m \in [M]} \frac{L_{\mathrm{w}} S}{\sum_{\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}} \mathrm{H}\left(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}\right)}$.

Proposition 2.1 (Capacity [3]) *We fix a finite field* $\mathbb{F}_p$ *and integers* $M, N \geq 2$*. For any PIR, it holds that*

$$\mathrm{rate}_{\mathrm{I}} \leq \mathrm{C} := \left(1 - \frac{1}{N}\right) / \left(1 - \frac{1}{N^M}\right). \tag{15}$$

We define the PIR capacity as the R.H.S. of this iniquality. There exist $L_{\mathrm{w}}, L_{\mathrm{a}} \in \mathbb{N}$ *and an LPIR that achieves equality in the iniquality* (15) *(Capacity-Achieving LPIR, CALPIR).*

The proof of the converse part is in Appendix A.1 in [1].

Hereafter we fix the values of M, N and p. Condition 10 in [8] showed several capacity-achieving conditions of LPIRs.

3 This Study: Conditions of A Capacity-Achieving Linear PIR

We explain the conditions under which LPIR is always correctly decodable (Eq. (13)) and achieves the PIR capacity using its extended parity check matrix (EPCM). We already showed the user's privacy condition in Eq.(4).

Definition 3.1 (extended parity check matrix of an LIR) *We fix an LIR and a generator matrix* $\boldsymbol{G}$ *of this LIR. We define an extended generator matrix*

(EGM) of $\boldsymbol{G}$ *as* $\tilde{\boldsymbol{G}} \coloneqq (\boldsymbol{I}_{L_{\mathrm{w}}M}, \boldsymbol{G})$*. We define an extended parity check matrix (EPCM) of* $\boldsymbol{G}$ *as* $\tilde{\boldsymbol{H}} \in \mathbb{F}_p^{h \times (L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n| + L_{\mathrm{w}}M)}$ *such that*

$$\begin{cases} \mathrm{rank}\tilde{\boldsymbol{H}} & = L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n| \,, \\ \tilde{\boldsymbol{G}}\tilde{\boldsymbol{H}}^\top & = \boldsymbol{0}_{L_{\mathrm{w}}M \times h}, \end{cases} \tag{16}$$

where h *is a certain integer such that* $h \geq L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n|$*.*

3.1 Conditions of Decoding

Definition 3.2 *When two matrices* $\boldsymbol{A}, \boldsymbol{B}$ *are transferred to each other by a row basis transformation, the matrices* $\boldsymbol{A}, \boldsymbol{B}$ *are said to be equivalent and this is denoted by* $\boldsymbol{A} \sim \boldsymbol{B}$*.*

Lemma 3.1 *For a matrix* $\tilde{\boldsymbol{H}} \in \mathbb{F}_p^{h \times (L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n| + L_{\mathrm{w}}M)}$*, Eq.*(17) *is equivalent to Eq.* (16)*.*

$$\tilde{\boldsymbol{H}} \sim \begin{pmatrix} \boldsymbol{G}^\top & -\boldsymbol{I}_{L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n|} \\ \boldsymbol{0} & \boldsymbol{0} \end{pmatrix}. \tag{17}$$

Hereafter we focus on a construction method for $\tilde{\boldsymbol{H}}$ *satisfying Eq.*(17) *and the decoder matrix* $\tilde{\boldsymbol{D}}$*.*

Lemma 3.2 *For an IR, the LIR is a LDIR if and only if the EPCM* $\tilde{\boldsymbol{H}}$ *satisfies Condition 3.1.*

Condition 3.1 *There exist* $h' \geq 0$, $\tilde{\boldsymbol{H}}' \in \mathbb{F}_p^{h' \times (L_{\mathrm{w}}M + L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n|)}$, $\tilde{\boldsymbol{D}} \in \mathbb{F}_p^{L_{\mathrm{w}}M \times L_{\mathrm{a}} \sum_{n\in[N]} |\mathcal{Q}_n|}$ *and* $\boldsymbol{G} \in \mathbb{F}_p^{L_{\mathrm{w}}M \times L_{\mathrm{a}} \sum_n |\mathcal{Q}_n|}$ *satisfying* $\tilde{\boldsymbol{H}} = \begin{pmatrix} \boldsymbol{P} \\ \tilde{\boldsymbol{H}}' \end{pmatrix}$, $\boldsymbol{P} = \begin{pmatrix} -\boldsymbol{J} & \tilde{\boldsymbol{D}} \end{pmatrix}$*, Eq.*(17)*, and for any* $n, m, \boldsymbol{s}$*, if* $q \neq \chi_n(m, \boldsymbol{s})$*,* $\tilde{\boldsymbol{D}}^{(m)}_{\boldsymbol{s},(n,q)} = \boldsymbol{0}_{L_{\mathrm{w}} \times L_{\mathrm{a}}}$*.*

Theorem 3.1 *If there exists a function* χ *and a matrix* $\tilde{\boldsymbol{H}}$ *satisfying Condition 3.1, we can construct an LDIR whose generator matrix is* $\boldsymbol{G}$ *in Condition 3.1. Moreover, if they satisfy Eq.*(4)*, the LIR is an LPIR.*

3.2 Conditions of Achieving the PIR Capacity

This subsection discuss the capacity-achieving conditions using its extended parity check matrix. Specifically, we discuss the rest $\tilde{\boldsymbol{H}}'$ in Condition 3.1. We first prepare lemmas and notations. We define $\boldsymbol{L}^I \coloneqq \big(\boldsymbol{L}^{(m)} | m \in I\big) \in \mathbb{F}_p^{L_{\mathrm{w}}M \times |I| L_{\mathrm{w}}}$. It is obvious that $\boldsymbol{L}^{[M]} = \boldsymbol{I}_{L_{\mathrm{w}}M}$.

Lemma 3.3 *An LPIR achieves the PIR capacity if and only if the LPIR satisfies Condition 3.2.*

Condition 3.2 (Capacity-Achieving Conditions Using its Generator Matrix) *(1) For any $m \in [M], \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}, n, n' \in [N]$,*

$$\begin{aligned} &\operatorname{rank}\left(\boldsymbol{L}^{(m)}, \boldsymbol{G}_{(n,q_n)}, \boldsymbol{G}_{(n',q_{n'})}\right) - \operatorname{rank}\left(\boldsymbol{L}^{(m)}, \boldsymbol{G}_{(n,q_n)}\right) \\ &= 0 \end{aligned} \tag{18}$$

(2) For any $m \in [M], \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}, I \subset [M] \setminus \{m\}$ with $I \neq \emptyset$,

$$\begin{aligned} &\operatorname{rank}\left(\boldsymbol{L}^{\boldsymbol{I}}, \boldsymbol{G}_{R(\boldsymbol{q})}\right) - |I| L_{\mathrm{w}} \\ &= \sum_{n \in [N]} \left(\operatorname{rank}\left(\boldsymbol{L}^{\boldsymbol{I}}, \boldsymbol{G}_{(n,q_n)}\right) - |I| L_{\mathrm{w}}\right). \end{aligned} \tag{19}$$

(3) $\sum_{\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(1)}} \operatorname{rank} \boldsymbol{G}_{R(\boldsymbol{q})} = \cdots = \sum_{\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(M)}} \operatorname{rank} \boldsymbol{G}_{R(\boldsymbol{q})}$,

The proof is in Appendix A.2 in [1].

Condition 3.2 is equivalent to Condition 10 in [8]. On the other hand, Condition 3.2 is slightly different from Conditions P1,P2,P3 in [4] because the definitions of the rate are different.

Hereafter we rewrite (1), (2) and (3) of Condition 3.2 by the EPCM $\tilde{\boldsymbol{H}}$ instead of $\boldsymbol{G}$, respectively.

First, we focus on (1) of Condition 3.2. In the next lemma, the matrix $\boldsymbol{K}$ is divided into block matrices. $M + \sum_{n \in [N]} |\mathcal{Q}_n|$ blocks. $\tilde{\boldsymbol{K}}$ is divided into the $M + \sum_{n \in [N]} |\mathcal{Q}_n|$ block columns. In the first M block columns, denote the set of all indices of the block columns as $[M]$ and denote the set of all indices of the columns as $[M] \times [L_{\mathrm{w}}]$. In the second $\sum_{n \in [N]} |\mathcal{Q}_n|$ block columns, denote the set of all indices in the block column as $\mathcal{NQ} := \{\, (n, q) \mid n \in [N], q \in \mathcal{Q}_n \,\} = \bigcup_{n \in [N]} \{n\} \times \mathcal{Q}_n$ and denote the set of all indices in the column as $\mathcal{NQ} \times [L_{\mathrm{a}}]$. $[M] \times [L_{\mathrm{w}}]$ and $\mathcal{NQ} \times [L_{\mathrm{a}}]$ are mutually exclusive. Let each block matrix in the first M block columns be an $L_{\mathrm{a}} \times L_{\mathrm{w}}$ matrix. Let each block matrix in the next $\sum_{n \in [N]} |\mathcal{Q}_n|$ block columns be an $L_{\mathrm{a}} \times L_{\mathrm{w}}$ matrix.

Lemma 3.4 *(1) of Condition 3.2 is a necessary and sufficient condition for the following condition.*

Condition 3.3 *$\tilde{\boldsymbol{H}}'$ in Condition 3.1 has the form of $\tilde{\boldsymbol{H}}' = \begin{pmatrix} \boldsymbol{K} \\ \vdots \end{pmatrix}$, where $\boldsymbol{K}$ has the form in Fig. 1. We abbriviate $A := \sum_{n \in [N]} |\mathcal{Q}_n|$, $C := (M-1)A(A-1)$ in Fig. 1. Each $\tilde{\boldsymbol{H}}_{i,j}$ is a block matrix.*

Proof *(1) of Condition 3.2 is equivalent to that for any $m, n, n, \boldsymbol{q}$, each column of $\boldsymbol{G}_{(n',q_{n'})}$ is a linear combination of all columns of $\boldsymbol{L}^{(m)}, \boldsymbol{G}_{(n,q_n)}, \boldsymbol{G}_{(n',q_{n'})}$. This is equivalent to $\tilde{\boldsymbol{G}} \boldsymbol{K}^\top = \boldsymbol{0}$.* □

Next, we focus on (2) of Condition 3.2. In the next lemmas, not only $\tilde{\boldsymbol{H}}$, but also the EGM $\tilde{\boldsymbol{G}}$ is divided into $M + \sum_{n \in [N]} |\mathcal{Q}_n|$ block columns as in $\tilde{\boldsymbol{H}}$. We define the set of all block column indices and the set of all column indices in the same way as for $\tilde{\boldsymbol{H}}$. We prepare notations.

$$
\begin{array}{c}
\left(\begin{array}{cccccccccc}
\tilde{\boldsymbol{H}}_{1,1} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} & \tilde{\boldsymbol{H}}_{1,M+2} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\
\tilde{\boldsymbol{H}}_{2,1} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} & \mathbf{0} & \tilde{\boldsymbol{H}}_{2,M+3} & \cdots & \mathbf{0} & \mathbf{0} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\tilde{\boldsymbol{H}}_{A-1,1} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \tilde{\boldsymbol{H}}_{A-1,M+A} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\tilde{\boldsymbol{H}}_{(A-1)^2+1,1} & \mathbf{0} & \cdots & \mathbf{0} & \tilde{\boldsymbol{H}}_{(A-1)^2+1,M+1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} \\
\tilde{\boldsymbol{H}}_{(A-1)^2+2,1} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \tilde{\boldsymbol{H}}_{(A-1)^2+2,M+2} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\tilde{\boldsymbol{H}}_{A(A-1),1} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{A(A-1),M+A-1} & \boldsymbol{I} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+1,M} & \boldsymbol{I} & \tilde{\boldsymbol{H}}_{C+1,M+2} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+2,M} & \boldsymbol{I} & \mathbf{0} & \tilde{\boldsymbol{H}}_{C+2,M+3} & \cdots & \mathbf{0} & \mathbf{0} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+A,M} & \boldsymbol{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \tilde{\boldsymbol{H}}_{C+A,M+A} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+(A-1)^2+1,M} & \tilde{\boldsymbol{H}}_{C+(A-1)^2+1,M+1} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+(A-1)^2+2,M} & \mathbf{0} & \tilde{\boldsymbol{H}}_{C+(A-1)^2+2,M+2} & \mathbf{0} & \cdots & \mathbf{0} & \boldsymbol{I} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+A(A-1),M} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \tilde{\boldsymbol{H}}_{C+A(A-1),M+A-1} & \boldsymbol{I}
\end{array}\right) \\
\underbrace{\hphantom{\tilde{\boldsymbol{H}}_{(A-1)^2+1,1}\;\mathbf{0}\;\cdots\;\tilde{\boldsymbol{H}}_{C+(A-1)^2+1,M}}}_{M\ \text{block columns}}\quad\underbrace{\hphantom{\tilde{\boldsymbol{H}}_{C+(A-1)^2+1,M+1}\;\tilde{\boldsymbol{H}}_{C+(A-1)^2+2,M+2}\;\mathbf{0}\;\cdots\;\tilde{\boldsymbol{H}}_{C+A(A-1),M+A-1}\;\boldsymbol{I}}}_{A\ \text{block columns}}
\end{array}
$$

Figure 1: The figure of $\boldsymbol{K}$

Definition 3.3 *Let $\boldsymbol{G}_{(n,q)} = (\boldsymbol{g}_{(n,q),1}, \ldots, \boldsymbol{g}_{(n,q),L_{\mathrm{a}}})$ be the column vector representation of a submatrix $\boldsymbol{G}_{(n,q)}$ of the generator matrix $\boldsymbol{G}$ of an LPIR. Let $\boldsymbol{l}_i$ be the i th column of $\boldsymbol{L}^{[M]}$ for any $i \in [M] \times [L_{\mathrm{w}}]$, i.e. $\boldsymbol{L}^{[M]} = \{\, \boldsymbol{l}_i \mid i \in [M] \times [L_{\mathrm{w}}] \,\}$. We fix a function $B(\cdot,\cdot)\colon 2^{[M]} \times 2^{\mathcal{N}\mathcal{Q}} \to 2^{\mathcal{N}\mathcal{Q} \times [L_{\mathrm{a}}]}$; $(I, R) \mapsto B(I, R)$ satisfying the following conditions.*

(1) The union set of a set $\{\, \boldsymbol{l}_i \mid i \in I \times [L_{\mathrm{w}}] \,\}$ of the columns of $\boldsymbol{G}_R$ and a set $\left\{\, \boldsymbol{g}_{(n,q),j} \;\middle|\; ((n, q), j) \in B\,(I, R) \,\right\}$ of the columns of $\boldsymbol{G}_R$ is a basis of a linear code generated by all columns of a matrix $\left(\boldsymbol{L}^I, \boldsymbol{G}_R\right)$ for any $I \subset [M]$ and $R \subset \mathcal{N}\mathcal{Q}$.

(2) $B(I, \emptyset) \coloneqq \emptyset$ for any $I \subset [M]$.

(3) For any $I \subset [M]$ and $R \subset \mathcal{N}\mathcal{Q}$, it holds that $B\,(I, R) \subset R \times [L_a]$.

(4) We exclusively partition a set $R \subset \mathcal{N}\mathcal{Q}$ into $R = R_1 \sqcup R_2$ satisfying $R_1, R_2 \neq \emptyset$. Then for any $I \subset [M]$, it holds that $B\,(I, R) \subset B\,(I, R_1) \cup B\,(I, R_2)$.

(5) For any $I_2 \subset I_1 \subset [M]$ and $R \subset \mathcal{N}\mathcal{Q}$, it holds that $B\,(I_2, R) \subset B\,(I_1, R)$.

For an LPIR, the function $B(\cdot,\cdot)$ satisfying the above is not necessarily uniquely determined. We fix any one of them.

Before discussing (2) of Condition 3.2, we discuss the fact that $\{\, \boldsymbol{l}_i \mid i \in I \times [L_{\mathrm{w}}] \,\} \cup \left\{\, \boldsymbol{g}_{(n,q),j} \;\middle|\; ((n, q), j) \in B(I, R(\boldsymbol{q})) \,\right\}$ is a basis by the following two lemmas.

Lemma 3.5 *All column vectors in* $\{\, \boldsymbol{l}_i \mid i \in I \times [L_{\mathrm{w}}] \,\} \cup \{\, \boldsymbol{g}_{(n,q),j} \bigm| ((n,q),j) \in B(I, R(\boldsymbol{q})) \,\}$ *generate each column vector in* $\{\, \boldsymbol{g}_{(n,q),j} \bigm| ((n,q),j) \in R \times [L_{\mathrm{w}}] \setminus B(I, R(\boldsymbol{q})) \,\}$ *if and only if Condition 3.4 holds.*

Condition 3.4 $\tilde{\boldsymbol{H}}'$ *in Condition 3.1 has the form of* $\tilde{\boldsymbol{H}}' = \begin{pmatrix} \boldsymbol{K} \\ \boldsymbol{B} \\ \vdots \end{pmatrix}$, *where* $\boldsymbol{K}$ *is in Condition 3.3.* $\boldsymbol{B}$ *is a submatrix that collects matrices of the forms shown in Fig. 2 and 3 for all* $m \in [M], \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$, *where* $I := [M] \setminus \{m\}$. *The blue areas in the figures represent parts of rows, and their values may be different for each area.*

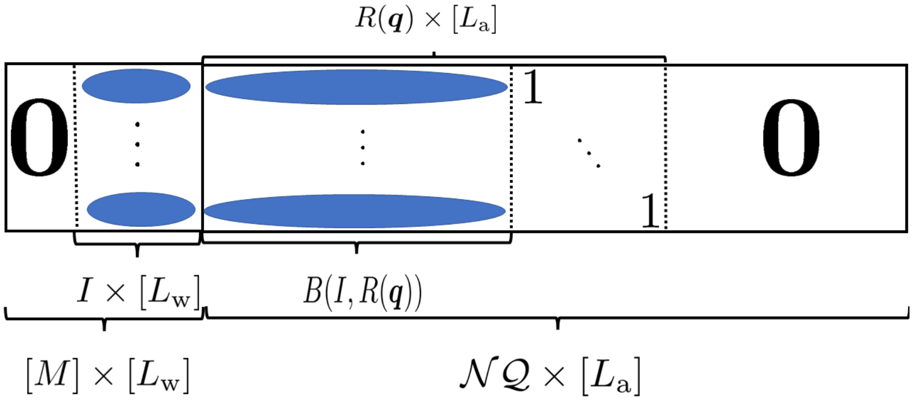

$R(\boldsymbol{q}) \times [L_{\mathrm{a}}]$
$\mathbf{0}$
1
1
$\mathbf{0}$
$I \times [L_{\mathrm{w}}]$
$B(I, R(\boldsymbol{q}))$
$[M] \times [L_{\mathrm{w}}]$
$\mathcal{NQ} \times [L_{\mathrm{a}}]$

Figure 2: one of the block rows of $\boldsymbol{B}$

The proof of Lemma 3.5 is in Appendix A.3 in [1].

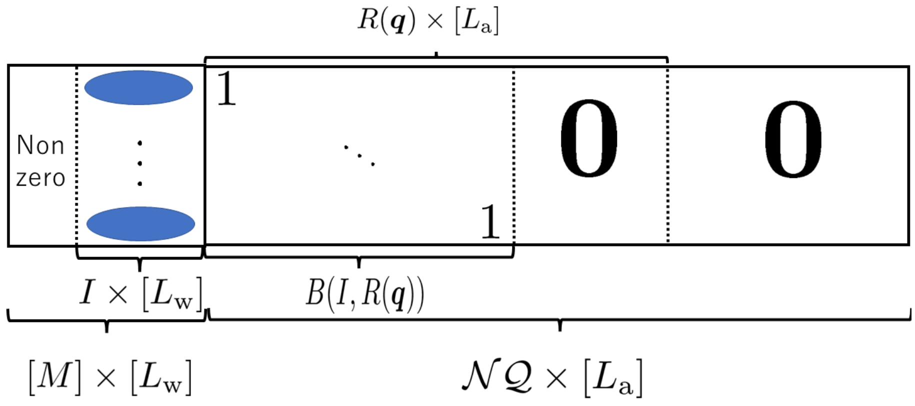
Lemma 3.6 *All vectors in* $\{\, \boldsymbol{l}_i \mid i \in I \times [L_{\mathrm{w}}] \,\} \cup \{\, \boldsymbol{g}_{(n,q),j} \bigm| ((n,q),j) \in B(I, R(\boldsymbol{q})) \,\}$ *are linearly independent if Condition 3.5 holds.*

Condition 3.5 *For any* $m \in [M]$,$\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$, $I \subset [M] \setminus \{m\}$, *the following conditions hold.*

(1) No vector is generated whose support is a subset of $(I \times [L_{\mathrm{w}}]) \sqcup B\,(I, R\,(\boldsymbol{q}))$ *by all rows of the EPCM* $\tilde{\boldsymbol{H}}$.

(2) Let $I \neq \emptyset$. *For any* $n \in [N]$, *no vector is generated whose support is a subset of* $(I \times [L_{\mathrm{w}}]) \sqcup B\,(I, \{(n, q_n)\})$ *by all rows of the EPCM* $\tilde{\boldsymbol{H}}$.

(3) No vector is generated whose support is a subset of $[M] \times [L_{\mathrm{w}}]$ *by all rows of the EPCM* $\tilde{\boldsymbol{H}}$.



$R(\boldsymbol{q}) \times [L_{\mathrm{a}}]$
Non zero
1
1
0
0
$I \times [L_{\mathrm{w}}]$
$B(I, R(\boldsymbol{q}))$
$[M] \times [L_{\mathrm{w}}]$
$\mathcal{N}\mathcal{Q} \times [L_{\mathrm{a}}]$

Figure 3: one of the block rows of $\boldsymbol{B}$

Proof *(1) holds because for any $m, I, \boldsymbol{q}$, all columns of the union of the sets $\{ \boldsymbol{l}_i \mid i \in I \times [L_{\mathrm{w}}] \}$ and $\left\{ \boldsymbol{g}_{(n,q),j} \,\middle|\, ((n,q),j) \in B(I, R(\boldsymbol{q})) \right\}$ are linearly independent. The proof of (2) is similar. (3) holds because the submatrix corresponding to the index set in the EGM $\boldsymbol{G}$ is $\boldsymbol{I}_{L_{\mathrm{w}}M}$.* □

We discuss (2) of Condition 3.2.

Lemma 3.7 *(2) of Condition 3.2 is a necessary and sufficient condition for the following condition.*

Condition 3.6 *For any $m \in [M], \boldsymbol{q} = (q_1, \ldots, q_N) \in \boldsymbol{\mathcal{Q}}^{(m)}, I \subset [M] \setminus \{m\}$ with $I \neq \emptyset$,*

$$B(I, R(\boldsymbol{q})) = \bigsqcup_{n \in [N]} B(I, \{ (n, q_n) \}) . \tag{20}$$

Proof *Assume that (2) of Condition 3.2 holds. We show that Eq.(20) holds. From (4) of Definition 3.3, it holds that $B(I, R(\boldsymbol{q})) \subset \bigcup_{n \in [N]} B(I, \{ (n, q_n) \})$. Moreover,*

$$\begin{aligned} 0 &= \operatorname{rank}\left(\boldsymbol{L}^I, \boldsymbol{G}_{(1,q_1),\ldots,(N,q_N)}\right) - \sum_{n \in [N]} \operatorname{rank}\left(\boldsymbol{L}^I, \boldsymbol{G}_{(n,q_n)}\right) \\ &\quad + (N-1)|I|L_{\mathrm{w}} & (21) \\ &= |I|L_{\mathrm{w}} + |B(I, R(\boldsymbol{q}))| - \sum_{n \in [N]} \left(|I|L_{\mathrm{w}} + |B(I, \{ (n, q_n) \})|\right) \\ &\quad + (N-1)|I|L_{\mathrm{w}} & (22) \end{aligned}$$

$$= \left|B\left(I, R\left(\boldsymbol{q}\right)\right)\right| - \sum_{n\in[N]} \left|B\left(I, \left\{\, \left(n, q_n\right)\, \right\}\right)\right|. \tag{23}$$

Therefore, Eq.(20) *holds.*
The converse is obvious from the above equations. □

From this lemma, Condition 3.4 can be replaced by the following condition.

Condition 3.7 *$\tilde{\boldsymbol{H}}'$ in Condition 3.1 has the form of $\tilde{\boldsymbol{H}}' = \begin{pmatrix} \boldsymbol{K} \\ \boldsymbol{B} \\ \vdots \end{pmatrix}$, where $\boldsymbol{K}$ is in Condition 3.3. $\boldsymbol{B}$ is a submatrix that collects matrices of the forms shown in Fig. 7 and 6 for all $m \in [M], n \in [N], q \in \mathcal{Q}_n$, where $I \coloneqq [M] \setminus \{m\}$. The blue areas in the figures represent parts of rows, and their values may be different for each area.*

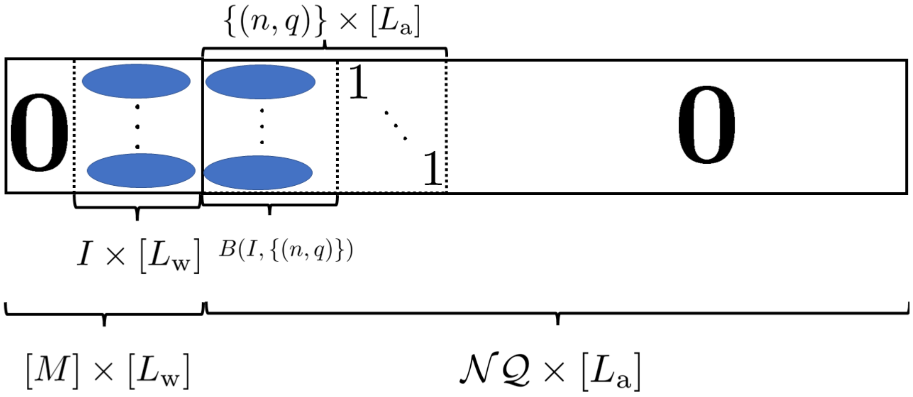

$\{(n,q)\} \times [L_{\mathrm{a}}]$
$\mathbf{0}$
1
1
$\mathbf{0}$
$I \times [L_{\mathrm{w}}]$
$B(I, \{(n,q)\})$
$[M] \times [L_{\mathrm{w}}]$
$\mathcal{NQ} \times [L_{\mathrm{a}}]$

Figure 4: one of the block rows of $\boldsymbol{B}$

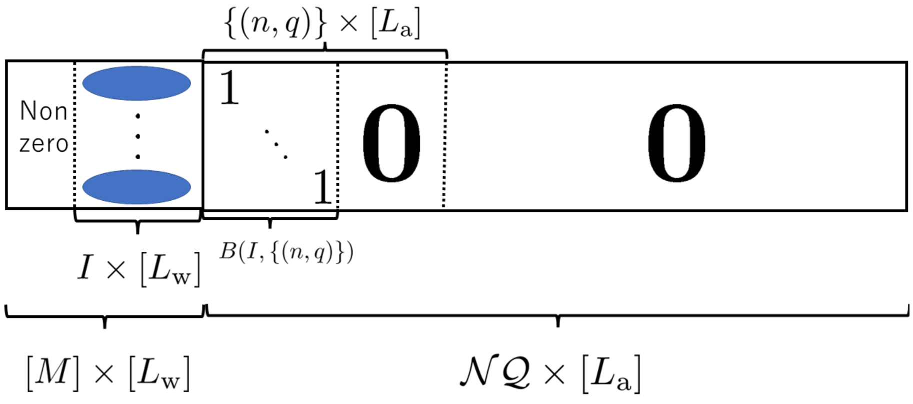
At last, we focus on (3) of Condition 3.2.

Lemma 3.8 *(3) of Condition 3.2 is a necessary and sufficient condition for the following condition.*

Condition 3.8

$$\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \left|B\left(\emptyset, R\left(\boldsymbol{q}\right)\right)\right| = \cdots = \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(M)}} \left|B\left(\emptyset, R\left(\boldsymbol{q}\right)\right)\right| \tag{24}$$

Proof *$B\left(\emptyset, R\left(\boldsymbol{q}\right)\right)$ is the set of all indices of the basis of the linear code generated by all columns of $\boldsymbol{G}_{R(\boldsymbol{q})}$.*□



$\{(n,q)\} \times [L_{\mathrm{a}}]$
Non zero
1
1
$\mathbf{0}$
$\mathbf{0}$
$B(I, \{(n,q)\})$
$I \times [L_{\mathrm{w}}]$
$[M] \times [L_{\mathrm{w}}]$
$\mathcal{NQ} \times [L_{\mathrm{a}}]$

Figure 5: one of the block rows of $\boldsymbol{B}$

Theorem 3.2 *If there exists a function* χ*, a function* B *and a matrix* $\tilde{\boldsymbol{H}} = \begin{pmatrix} \boldsymbol{P} \\ \tilde{\boldsymbol{H}}' \end{pmatrix}$*, where* $\tilde{\boldsymbol{H}}' = \begin{pmatrix} \boldsymbol{K} \\ \boldsymbol{B} \\ \boldsymbol{C} \end{pmatrix}$ *and* $\boldsymbol{C} \in \mathbb{F}_p^{h'' \times (L_{\mathrm{a}} \sum_{n \in [N]} |\mathcal{Q}_n| + L_{\mathrm{w}} M)}$ *for some* $h'' \geq 0$*, satisfying from Conditions 3.1, 3.3, 3.5, 3.6, 3.7 and 3.8, we can construct a CALPIR whose generator matrix is* $\boldsymbol{G}$ *in Condition 3.1.*

This theorem makes the condition for the generating matrix $\boldsymbol{G}$ to construct a large subclass of CALPIRs more explicit than Condition 3.2.

4 Construction Method for its Extended Parity Check Matrix

Finally, as a part of the construction of a CALPIR, we describe a construction method for the submatrix $\boldsymbol{C}$ of the EPCM $\tilde{\boldsymbol{H}}$ in Theorem 3.2. We do not discuss specific construction methods for other elements of $\tilde{\boldsymbol{H}}$. We assume that $b := \operatorname{rank} \begin{pmatrix} \boldsymbol{P} \\ \boldsymbol{K} \\ \boldsymbol{B} \end{pmatrix} \leq L_{\mathrm{a}} \sum_{n \in [N]} |\mathcal{Q}_n|$. Since the EPCM $\tilde{\boldsymbol{H}}$ only needs to satisfy Condition 3.1, we can make $\boldsymbol{C}$ as $\boldsymbol{C} = (\mathbf{0}, \boldsymbol{C}')$, where a certain matrix $\boldsymbol{C}'$ has $L_{\mathrm{a}} \sum_{n \in [N]} |\mathcal{Q}_n|$ columns and satisfies $\operatorname{rank}\boldsymbol{C}' = L_{\mathrm{a}} \sum_{n \in [N]} |\mathcal{Q}_n| - b$.

If you want to add other conditions to the CALPIR, about the upload cost for example, add block rows corresponding to that condition to the EPCM $\tilde{\boldsymbol{H}}$ under the constraint that the assumptions in Theorem 3.2 are satisfied.

5 Conclusion

We show a sufficient condition of a CALPIR (Theorem 3.2) by using its EPCM and a construction method for $\boldsymbol{C}$ to propose a systematic construction method for a subclass of CALPIRs. The future work is to propose a more specific construction method for the EPCM $\tilde{\boldsymbol{H}}$.

A Apendix : Proofs

A.1 The Proof of the Iniquality (15)

Proof

$$\frac{L_{\mathrm{w}}}{\mathrm{r}_{\mathrm{I}}} = \max_{m\in[M]} \mathrm{H}\left(\boldsymbol{A}^{(m)}|\boldsymbol{Q}^{(m)}\right) \tag{25}$$

$$\overset{\text{(a)}}{\geq} \mathrm{H}\left(\boldsymbol{A}^{(1)}|\boldsymbol{Q}^{(1)}\right) \tag{26}$$

$$= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{Q}^{(1)})}|\boldsymbol{Q}^{(1)}=\boldsymbol{q}) \tag{27}$$

$$= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}) \tag{28}$$

$$= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\left(\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|W_1)+\mathrm{H}(W_1)\right) \tag{29}$$

$$= L_{\mathrm{w}} + \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|W_1). \tag{30}$$

For any $m\in[2,M]$*,*

$$\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m-1)}} \Pr(\boldsymbol{Q}^{(m-1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[m-1]}) \tag{31}$$

$$\overset{\text{(b)}}{\geq} \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m-1)}} \Pr(\boldsymbol{Q}^{(m-1)}=\boldsymbol{q})\frac{1}{N} \times \sum_{n\in[N]} \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_{[m-1]}) \tag{32}$$

$$= \frac{1}{N}\sum_{n\in[N]}\sum_{q\in\mathcal{Q}_n}\left(\sum_{\substack{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m-1)}\\ q_n=q}} \Pr(\boldsymbol{Q}^{(m-1)}=\boldsymbol{q})\right) \times \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q)}|\boldsymbol{W}_{[m-1]}) \tag{33}$$

$$= \frac{1}{N}\sum_{n\in[N]}\sum_{q\in\mathcal{Q}_n}\left(\sum_{\substack{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}\\ q_n=q}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\right) \times \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q)}|\boldsymbol{W}_{[m-1]}) \quad \because \textit{Privacy constraint} \tag{34}$$

$$= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\frac{1}{N}\sum_{n\in[N]} \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_{[m-1]}) \tag{35}$$

$$\overset{\text{(c)}}{\geq} \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\frac{1}{N}\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[m-1]}) \tag{36}$$

$$= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \frac{1}{N}\Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\left(\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[m]})+\mathrm{H}(W_m)\right) \tag{37}$$

$$= \frac{L_{\mathrm{w}}}{N}+\frac{1}{N}\left(\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr\left(\boldsymbol{Q}^{(m)}=\boldsymbol{q}\right)\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[m]})\right). \tag{38}$$

Thus

$$\begin{aligned}
\frac{L_{\mathrm{w}}}{\mathrm{r_I}} &\geq L_{\mathrm{w}} + \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|W_1)\\
&\geq L_{\mathrm{w}}\left(1+\frac{1}{N}\right)\\
&\quad + \frac{1}{N}\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(2)}} \Pr(\boldsymbol{Q}^{(2)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[2]})\\
&\dots\\
&\geq L_{\mathrm{w}}\left(1+\frac{1}{N}+\cdots+\frac{1}{N^{M-2}}\right)+\frac{1}{N^{M-2}}\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(M-1)}}\\
&\quad \times \Pr(\boldsymbol{Q}^{(M-1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[M-1]})\\
&\geq L_{\mathrm{w}}\left(1+\frac{1}{N}+\cdots+\frac{1}{N^{M-2}}+\frac{1}{N^{M-1}}\right)+\frac{1}{N^{M-1}}\\
&\quad \times \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(M)}} \Pr\left(\boldsymbol{Q}^{(M)}=\boldsymbol{q}\right)\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_{[M]})\\
&= L_{\mathrm{w}}\left(1+\frac{1}{N}+\cdots+\frac{1}{N^{M-1}}\right).
\end{aligned}$$

□

A.2 The Proof of Lemma 3.3

Proof $\overset{(a)}{\geq}$, $\overset{(b)}{\geq}$ *and* $\overset{(c)}{\geq}$ *in Appendix A.1 shows that a PIR achieves the PIR capacity if and only if*[1] *the below conditions* (1), (2) *and* (3) *hold.*

(1) For any $m \in [M], \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}, n, n' \in [N]$,

$$\mathrm{H}(\Phi(\boldsymbol{W})_{(n',q_{n'})}, \Phi(\boldsymbol{W})_{(n,q_n)}, W_m) = \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}, W_m) \tag{39}$$

(2) For any $m \in [M], \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}, I \subset [M]\setminus\{m\}$ *with* $I \neq \emptyset$,

$$\mathrm{H}\left(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_I\right) = \sum_{n\in[N]} \mathrm{H}\left(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_I\right). \tag{40}$$

[1] We can replace Eq.(40) with $\mathrm{H}\left(\Phi(\boldsymbol{W})_{(1,q_1)},\dots,\Phi(\boldsymbol{W})_{(N,q_N)},\boldsymbol{W}_I\right) - \mathrm{H}\left(\boldsymbol{W}_I\right) = \sum_{n\in[N]}\mathrm{H}\left((\Phi(\boldsymbol{W})_{(n,q_n)},\boldsymbol{W}_I) - \mathrm{H}\left(\boldsymbol{W}_I\right)\right)$ and Eq.(39) with $\mathrm{H}\left(\Phi(\boldsymbol{W})_{(n,q_n)},\Phi(\boldsymbol{W})_{(n',q_{n'})},W_m\right) - \mathrm{H}\left(\Phi(\boldsymbol{W})_{(n',q_{n'})},W_m\right) = 0.$

(3)

$$\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(1)}} \mathrm{H}\left(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}\right) = \cdots = \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(M)}} \mathrm{H}\left(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}\right). \tag{41}$$

The conditions that the equalilties hold in $\overset{\text{(a)}}{\geq}$, $\overset{\text{(b)}}{\geq}$ *and* $\overset{\text{(c)}}{\geq}$ *correspond to the above conditions* (3), (1) *and* (2) *respectively. We show this fact.*

First, we focus on $\overset{\text{(a)}}{\geq}$. *Since the desired symbol* m *can arbitrarily change its value due to its symmetry, the equality holds in* $\overset{\text{(a)}}{\geq}$ *if and only if*

$$\mathrm{H}\left(\boldsymbol{A}^{(1)}|\boldsymbol{Q}^{(1)}\right) = \cdots = \mathrm{H}\left(\boldsymbol{A}^{(M)}|\boldsymbol{Q}^{(M)}\right). \tag{42}$$

Since

$$\mathrm{H}\left(\boldsymbol{A}^{(m)}|\boldsymbol{Q}^{(m)}\right) = \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(1)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}) = \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \frac{1}{S}\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}),$$

we can write Eq. (42) *as Eq.*(41).

Next, we focus on $\overset{\text{(b)}}{\geq}$. *Since the desired symbol* m *can arbitrarily change its value due to its symmetry, the equality holds in* $\overset{\text{(b)}}{\geq}$ *if and only if for any* $m \in [M]$ *and* $I \subset [M]$ *satisfing* $m \in I$ *and* $|I| \leq M-1$,

$$\begin{aligned}&\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_I)\\ &= \sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q})\frac{1}{N}\sum_{n\in[N]} \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_I).\end{aligned} \tag{43}$$

Clearly we can omit the constraint $|I| \leq M-1$.

Since we can write Eq.(43) *as*

$$\sum_{\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)}=\boldsymbol{q}) \sum_{n\in[N]} \left(\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_I) - \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_I)\right) = 0 \tag{44}$$

and $\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|\boldsymbol{W}_I) \geq \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|\boldsymbol{W}_I)$, *the equality holds in* $\overset{\text{(b)}}{\geq}$ *if and only if for any* $m \in [M]$, $(m \in)I \subset [M]$, $n \in [N]$ *and* $\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$,

$$\mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})}|W_I) = \mathrm{H}(\Phi(\boldsymbol{W})_{(n,q_n)}|W_I). \tag{45}$$

This is equivalent to that for any $m \in [M]$, $(m \in)I \subset [M]$, $n, n' \in [N]$ *and* $\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$,

$$\mathrm{H}(\Phi(\boldsymbol{W})_{(n',q_{n'})}|\Phi(\boldsymbol{W})_{(n,q_n)}, W_I) = 0. \tag{46}$$

This is equivalent to that for any $m \in [M]$, $n, n' \in [N]$ and $\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$,

$$\mathrm{H}(\Phi(\boldsymbol{W})_{(n', q_{n'})} | \Phi(\boldsymbol{W})_{(n, q_n)}, W_m) = 0. \tag{47}$$

We can write this equation as Eq.(39).

At last, we focus on $\overset{\text{(c)}}{\geq}$. Since the desired symbol m can arbitrarily change its value due to its symmetry, the equality holds in $\overset{\text{(c)}}{\geq}$ if and only if for any $m \in [M]$ and $(\emptyset \neq) I \subset [M]$,

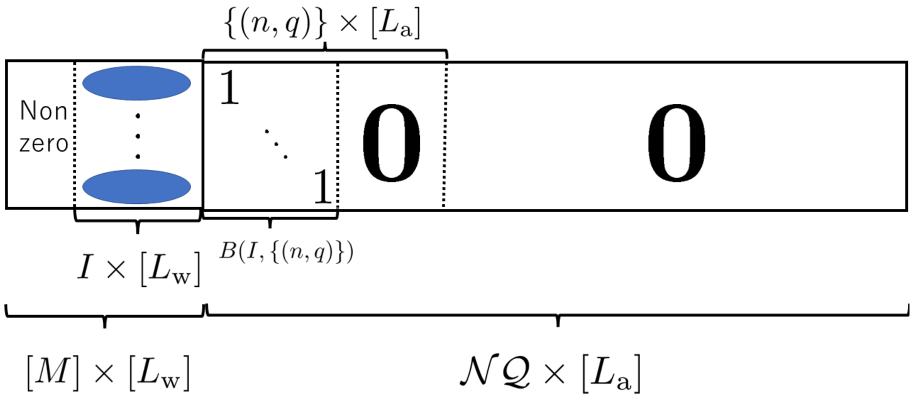
$$\begin{aligned} &\sum_{\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)} = \boldsymbol{q}) \sum_{n \in [N]} \mathrm{H}(\Phi(\boldsymbol{W})_{(n, q_n)} | \boldsymbol{W}_I) \\ = &\sum_{\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}} \Pr(\boldsymbol{Q}^{(m)} = \boldsymbol{q}) \mathrm{H}(\Phi(\boldsymbol{W})_{R(\boldsymbol{q})} | \boldsymbol{W}_I) \end{aligned} \tag{48}$$

This is equivalent to the above condition (2).

The above conditions (1), (2) and (3) are equivalent to Condition 3.2 in an LIR.□

A.3 The Proof of Lemma 3.5

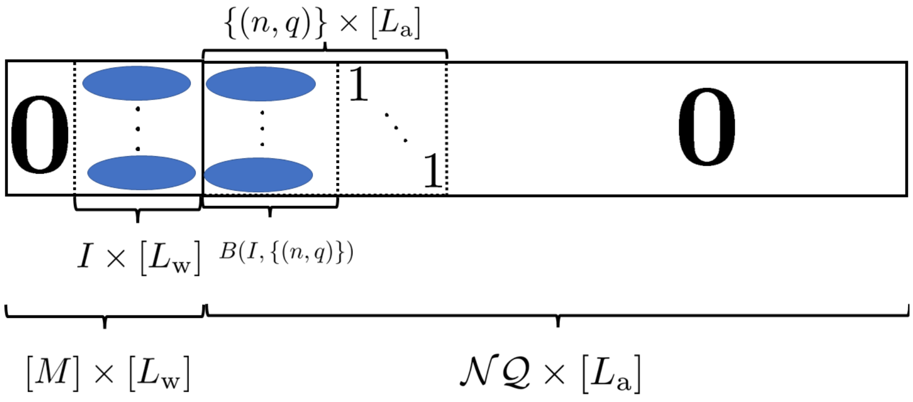
Proof *We focus on Fig.7,6,2 and 3.*



$\{(n,q)\} \times [L_\mathrm{a}]$
Non zero
1
1
0
0
$I \times [L_\mathrm{w}]$
$B(I, \{(n,q)\})$
$[M] \times [L_\mathrm{w}]$
$\mathcal{N}\mathcal{Q} \times [L_\mathrm{a}]$

Figure 6: A part of block rows of the EPCM $\tilde{\boldsymbol{H}}$

We set $m \in [M]$, $I \subset [M] \setminus \{m\}$,$\boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}$. Since the union of two sets $\{\, \boldsymbol{l}_i \mid i \in I \times [L_\mathrm{w}] \,\}$ and $\left\{\, \boldsymbol{g}_{(n'', q''), i} \,\middle|\, ((n'', q''), i) \in B\,(I, R(\boldsymbol{q}))\,\right\}$ generates the other columns of the matrix $\left(\boldsymbol{L}^I, \boldsymbol{G}_{R(\boldsymbol{q})}\right)$, a part of the rows of $\tilde{\boldsymbol{H}}$ form the $(L_\mathrm{a}|R(\boldsymbol{q})| - B(I, R(\boldsymbol{q}))) \times (L_\mathrm{w} M + \sum_{n \in [N]} |\mathcal{Q}_n|\, L_\mathrm{a})$ matrix in Fig.2, where the



$\{(n,q)\}\times[L_\mathrm{a}]$
$\mathbf{0}$
1
1
$\mathbf{0}$
$I\times[L_\mathrm{w}]$
$B(I,\{(n,q)\})$
$[M]\times[L_\mathrm{w}]$
$\mathcal{N}\mathcal{Q}\times[L_\mathrm{a}]$

Figure 7: A part of block rows of the EPCM $\tilde{\boldsymbol{H}}$

left $\mathbf{0}$ *is an* $(L_\mathrm{a}|R(\boldsymbol{q})|-B(I,R(\boldsymbol{q})))\times(L_\mathrm{w}M-|I|\,L_\mathrm{w})$ *zero matrix and the right* $\mathbf{0}$ *is an* $(L_\mathrm{a}|R(\boldsymbol{q})|-B(I,R(\boldsymbol{q})))\times(-1+\sum_{n\in[N]}|\mathcal{Q}_n|)L_\mathrm{a}$ *zero matrix. The blue area in the figures canbe all zero rows.*

Moreover, since all vectors in the union of $\left\{\, \boldsymbol{g}_{(n'',q''),i} \;\middle|\; ((n'',q''),i)\in B\,(I,R(\boldsymbol{q}))\,\right\}$ *and the set of all columns of* $\boldsymbol{L}^I$ *are linearly independent and all columns of* $\boldsymbol{L}$ *generate* $\left\{\, \boldsymbol{g}_{(n'',q''),i} \;\middle|\; ((n'',q''),i)\in B\,(I,R(\boldsymbol{q}))\,\right\}$*, a part of the rows of* $\tilde{\boldsymbol{H}}$ *form the* $|B(I,R(\boldsymbol{q}))|\times(L_\mathrm{w}M+\sum_{n\in[N]}|\mathcal{Q}_n|\,L_\mathrm{a})$ *matrix in Fig.3.*

We set $m\in[M]$*,* $(\emptyset\neq)I\subset[M]\setminus\{m\}$ *,*$\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)},n\in[N]$*. Similarly as before, a part of rows of* $\tilde{\boldsymbol{H}}$ *form the matrix in Fig.7,6.*

We define $\boldsymbol{B}'$ *as a submatrix of* $\tilde{\boldsymbol{H}}$ *formed by collecting matrices in Fig.7,6 for all* $m\in[M],I\subset[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}$ *and matrices in Fig. 2,3 for all* $m\in[M],\emptyset\neq I\subset[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)},n\in[N]$*.*

We show that row transformation of this and removing the zero matrix yields a matrix $\boldsymbol{B}$*. We fix* $R\subset\left(\bigcup_{n\in[N]}\{n\}\times\mathcal{Q}_n\right)\times[L_\mathrm{a}]$ *and move* $I\subset[M]$*. When we arrange the matrices in Fig.8 constructed from* $B(I,R)$ *in the order of inclusion of* I*, the matrices form as Fig.9.*

Thus, by row reduction, the submatrices constructed by collecting all matrices in the form of Fig.7 for all $m\in[M],I\subset[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}$ *is removed by the submatrix constructed by collecting all matrices in the form of Fig.7 for all* $m\in[M],I\coloneqq[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}$*. The same thing holds for Fig.2. Moreover, the same things hold for Fig.6,3. Thus, we only have to consider the submatrix* $\boldsymbol{B}''$ *of the matrix* $\boldsymbol{B}'$*, where* $\boldsymbol{B}''$ *is the matrix constructed from the matrices in the form of Fig.7,6 for all* $m\in[M],I\coloneqq[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)},n\in[N]$ *and the matrices in the form of Fig.2,3 for all* $m\in[M],I\coloneqq[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}$*.*

By row reduction, for any $m\in[M],I\coloneqq[M]\setminus\{m\},\boldsymbol{q}\in\boldsymbol{\mathcal{Q}}^{(m)}$*, the matrices*

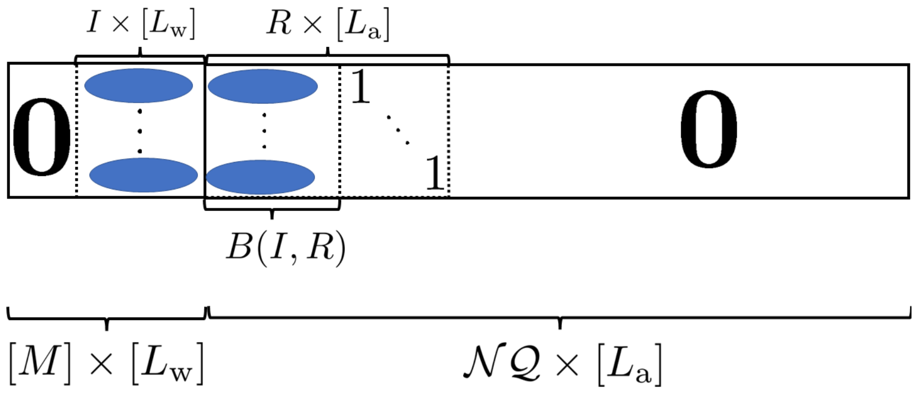

$I \times [L_{\mathrm{w}}]$
$R \times [L_{\mathrm{a}}]$
$\mathbf{0}$
1
1
$\mathbf{0}$
$B(I, R)$
$[M] \times [L_{\mathrm{w}}]$
$\mathcal{NQ} \times [L_{\mathrm{a}}]$

Figure 8: A part of block rows of the EPCM $\tilde{\boldsymbol{H}}$

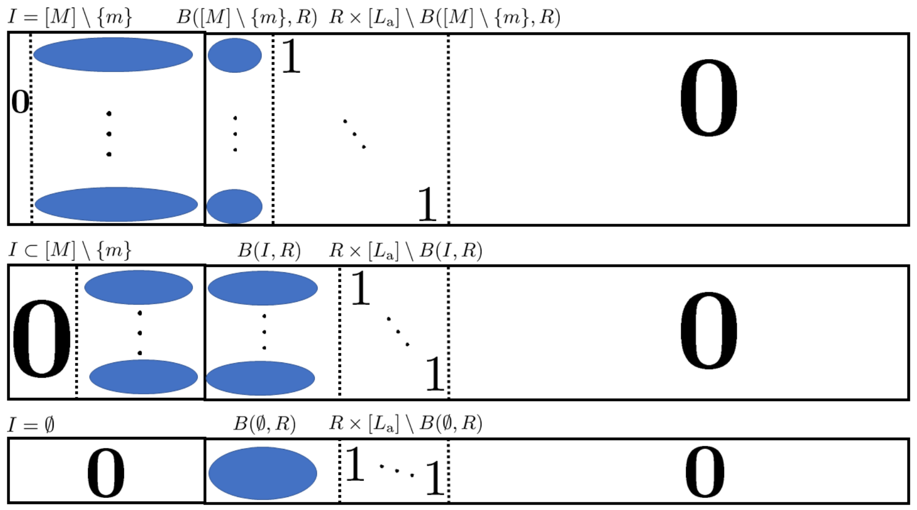

$I = [M] \setminus \{m\}$
$B([M] \setminus \{m\}, R)$
$R \times [L_{\mathrm{a}}] \setminus B([M] \setminus \{m\}, R)$
$\mathbf{0}$
1
1
$\mathbf{0}$
$I \subset [M] \setminus \{m\}$
$B(I, R)$
$R \times [L_{\mathrm{a}}] \setminus B(I, R)$
$\mathbf{0}$
1
1
$\mathbf{0}$
$I = \emptyset$
$B(\emptyset, R)$
$R \times [L_{\mathrm{a}}] \setminus B(\emptyset, R)$
$\mathbf{0}$
1
1
$\mathbf{0}$

Figure 9: A part of block rows of the EPCM $\tilde{\boldsymbol{H}}$

in the form of Fig.7,6 for all $n \in [N]$ are deleted by the submatrix constructed from the matrices in the form of Fig.2,3 deleted by row reduction.

We explain that, by row reduction, the matrix in the form of Fig.7 for all $n \in [N]$ are deleted by the submatrix constructed from the matrices in the form of Fig.2. Simplifying the latter by the former, the latter becomes the matrix in the form of Fig.10. However, all rows of this matrix are zeros due to the conditions. Thus $\boldsymbol{B}''$ becomes the submatrix $\boldsymbol{B}$ constructed from the matrices in the form of Fig.2,3 for all $m \in [M], I \coloneqq [M] \setminus \{m\}, \boldsymbol{q} \in \boldsymbol{\mathcal{Q}}^{(m)}, n \in [N]$. Similarly, we can show that the matrices in the form of Fig.6 for all $n \in [N]$ are deleted by the submatrix constructed from the matrices in the form of Fig.3.

Thus a part of the EPCM is in the form of $\boldsymbol{B}$. □

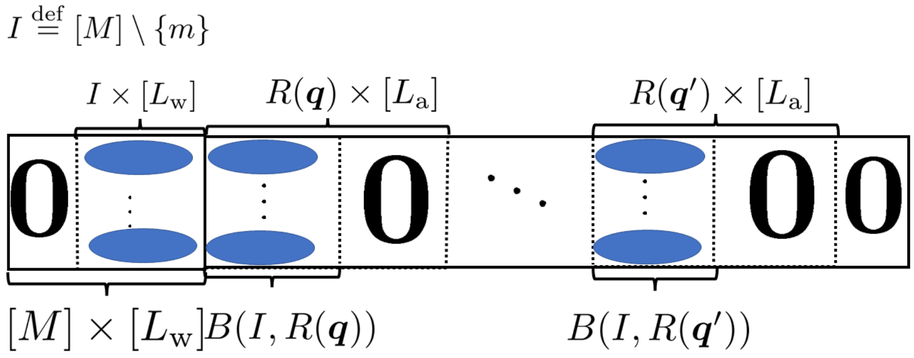

$I \overset{\text{def}}{=} [M] \setminus \{m\}$
$I \times [L_{\text{w}}]$
$R(\boldsymbol{q}) \times [L_{\text{a}}]$
$R(\boldsymbol{q}') \times [L_{\text{a}}]$
$\mathbf{0}$
$\mathbf{0}$
$\mathbf{0}$
$\mathbf{0}$
$[M] \times [L_{\text{w}}]$
$B(I, R(\boldsymbol{q}))$
$B(I, R(\boldsymbol{q}'))$

Figure 10: A part of block rows of the EPCM $\tilde{\boldsymbol{H}}$

B Apendix : Examples

B.1 Numerical Examples

Example B.1 (CALPIR [4]) *We set the parameters as follows.*

- *M, N are positive integers. $F \coloneqq N^M, L_{\text{w}} \coloneqq N-1, L_{\text{a}} \coloneqq 1$.*
- *$\boldsymbol{W} = (W_1, \ldots, W_M) = (W_{1,1}, \ldots, W_{1,N-1}, \ldots, W_{M,1}, \ldots, W_{M,N-1})$. We set $W_{m,N} = 0$ for $m \in [M]$.*
- *$\mathbb{F}_p$ is a finite field.*
- *$\boldsymbol{S} = (S_1, \ldots, S_{M-1})$ is a random variable vector uniformly distributed on $[N]^{M-1}$.*

- $\mathcal{Q} = [N]^M$.
- *The query is*

$$Q_n^{(m)} = \left(Q_{n,1}^{(m)}, \ldots, Q_{n,m-1}^{(m)}, Q_{n,m}^{(m)}, Q_{n,m+1}^{(m)}, \ldots, Q_{n,M}^{(m)}\right) \tag{49}$$

$$\coloneqq \left(S_1, \ldots, S_{m-1}, \left(n - \sum_{j=1}^{M-1} S_j\right) \mod N, S_m, S_{m+1}, \ldots, S_{M-1}\right) \in [N]^{M-1}. \tag{50}$$

$A \mod N (\in [N])$ denotes the remainder when divided by N. Hereafter we omit $\mod N$. We set $W_{m,N} \coloneqq 0$ for $m \in [M]$. There exists between a bijection $Q_n^{(m)}$ and $\boldsymbol{S}$ for any m, n.

- *The responce is*

$$\phi(n, q_n, \boldsymbol{W}) \coloneqq W_{1,s_1} + \cdots + W_{m-1,s_{m-1}} + W_{m,\left(n - \sum_{j=1}^{M-1} s_j\right)} + W_{m+1,s_m} + \cdots + W_{M,s_{M-1}} \tag{51}$$

where $\boldsymbol{s} = (s_1, \ldots, s_{M-1})$ is a random key.

$$\phi_{\mathrm{TSC}}(n, q_n, \boldsymbol{W}) \coloneqq W_{1,q_{n,1}} + \cdots + W_{M,q_{n,M}} = \boldsymbol{W} \underbrace{\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}}_{=: \boldsymbol{G}_{\mathrm{TSC},(n,q_n)} \in \mathbb{F}_p^{M(N-1)\times 1}} . \tag{52}$$

where $q_n = (q_{n,1}, \ldots, q_{n,M}) \in \mathcal{Q} = [N]^M$ (query to DB n).

$\boldsymbol{G}_{\mathrm{TSC},(n,q_n)}$ does not depend on n. We represent $N-1$ as -1 and N as 0 for simplicity.

- *The decoder is $\boldsymbol{q} = (q_1, \ldots, q_N) = (q_{1,1}, \ldots, q_{1,M}, \ldots, q_{N,1}, \ldots, q_{N,M}) \in \mathcal{Q}^N = \left([N]^M\right)^N$, $\boldsymbol{a} = (a_1, \ldots, a_N) \in \left(\mathbb{F}_p^{L_{\mathrm{a}}}\right)^N = \left(\mathbb{F}_p^1\right)^N$.*

When we represent this with a random key $\boldsymbol{s} = (s_1, \ldots, s_{M-1})$, the decoder is

$$\psi_{\mathrm{TSC}}\left(m, \boldsymbol{a}, \boldsymbol{q}\right) \coloneqq \left(a_{1+\sum_{j=1}^{M-1} s_j} - a_{\sum_{j=1}^{M-1} s_j}, \ldots, a_{N-1+\sum_{j=1}^{M-1} s_j} - a_{\sum_{j=1}^{M-1} s_j}\right) \tag{53}$$

Otherwise

$$\psi_{\mathrm{TSC}}\left(m,\boldsymbol{a},\boldsymbol{q}\right) \coloneqq \left(a_{2-q_{1,m}} - a_{1-q_{1,m}}, \dots, a_{N-q_{1,m}} - a_{1-q_{1,m}}\right) \tag{54}$$

$$= \boldsymbol{a} \underbrace{\begin{pmatrix} -1 & -1 & \dots & -1 \\ 1 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}}_{=: \left(\boldsymbol{D}^{(m)}_{\mathrm{TSC},i\cdot}\right)^{\top} \in \mathbb{F}_p^{N\times(N-1)}} \tag{55}$$

Example B.2 (Example of [4] when $M = 3, N = 2$) *We set $F = N^M = 8, L_{\mathrm{w}} = N - 1 = 1, L_{\mathrm{a}} = 1$ and*

$$\boldsymbol{W} = (W_{m,l})_{m\in[M],l\in[L_{\mathrm{w}}]} = (W_{1,1}, W_{2,1}, W_{3,1}) \in \left(\mathbb{F}_p^{L_{\mathrm{w}}}\right)^M = \left(\mathbb{F}_p^1\right)^3. \tag{56}$$

We set $\boldsymbol{S} = (s_1, s_2) \in [2]^2 = [N]^{M-1}$.

$$Q_1^{(1)} = (1 - (s_1 + s_2), s_1, s_2) \in \mathcal{Q} = [2]^3,$$

$$Q_2^{(1)} = (2 - (s_1 + s_2), s_1, s_2) \in \mathcal{Q} = [2]^3,$$

$$Q_1^{(2)} = (s_1, 1 - (s_1 + s_2), s_2) \in \mathcal{Q} = [2]^3$$

$$Q_2^{(2)} = (s_1, 2 - (s_1 + s_2), s_2) \in \mathcal{Q} = [2]^3,$$

$$Q_1^{(3)} = (s_1, s_2, 1 - (s_1 + s_2)) \in \mathcal{Q} = [2]^3,$$

$$Q_2^{(3)} = (s_1, s_2, 2 - (s_1 + s_2)) \in \mathcal{Q} = [2]^3.$$

For example, if $n = 1, q = (101)$, then $\phi_{\mathrm{TSC}}(n, q, \boldsymbol{W}) = (W_{1,1}, W_{2,1}, W_{3,1}) \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$. Moreover, if $m = 1, \boldsymbol{q} = ((100), (000))$, $\boldsymbol{a} = (a_1, a_2)$, then $\psi_{\mathrm{TSC}}(m, \boldsymbol{q}, \boldsymbol{a}) = (a_1, a_2) \begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Example B.3 ($\boldsymbol{G}_{\mathrm{TSC}}, \tilde{\boldsymbol{D}}_{\mathrm{TSC}}$ in Example B.2)

-
$$\begin{aligned} &\Big(\ \phi_{\mathrm{TSC}}(1,000,\boldsymbol{W}), \phi_{\mathrm{TSC}}(1,001,\boldsymbol{W}), \phi_{\mathrm{TSC}}(1,010,\boldsymbol{W}), \phi_{\mathrm{TSC}}(1,011,\boldsymbol{W}), \phi_{\mathrm{TSC}}(1,100,\boldsymbol{W}), \phi_{\mathrm{TSC}}(1,10 \\ &= \Big(\ W_{1,1}, W_{2,1}, W_{3,1}\ \Big) \underbrace{\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{=: \boldsymbol{G}_{\mathrm{TSC}}} \end{aligned} \tag{57}$$

-
$$\tilde{\boldsymbol{D}}_{\mathrm{TSC}}^{\top} \coloneqq \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Then

$$\boldsymbol{G}_{\mathrm{TSC}}\tilde{\boldsymbol{D}}_{\mathrm{TSC}}^{\top} = \boldsymbol{J}^{\top} \coloneqq \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{58}$$

For example, if $m = 1$ and $s_1 = s_2 = 0$, it bholds that $\boldsymbol{Q}^{(1)} = ((100), (000))$. Then

$$(W_{1,1}, W_{2,1}, W_{3,1}) \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{59}$$

$$= (W_{1,1}, W_{1,2}, W_{1,3}) \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = W_{1,1}.$$

Example B.4 ($\tilde{\boldsymbol{G}}_{\mathrm{TSC}}, \tilde{\boldsymbol{H}}_{\mathrm{TSC}}$ in Example B.2)

- $$\tilde{\boldsymbol{G}}_{\mathrm{TSC}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{60}$$

  The generator matrix $\boldsymbol{G}_{\mathrm{TSC}}$ is formed by from the 4 th column to 19 th column.

- $\tilde{\boldsymbol{H}}_{\mathrm{TSC}} \in \mathbb{F}_p^{\sum_{n\in[N]}|\mathcal{Q}_n|L_{\mathrm{a}} \times (L_{\mathrm{w}}M + \sum_{n\in[N]}|\mathcal{Q}_n|L_{\mathrm{a}})} = \mathbb{F}_p^{16\times 19}$ *is* $(\boldsymbol{G}_{\mathrm{TSC}}^{\top}, -\boldsymbol{I}_{16\times 16})$.

Example B.5 (the EPCM using $(-\boldsymbol{J}, \tilde{\boldsymbol{D}})$ in Example B.2) *If $N = 2, M = 3$, when we add $\tilde{\boldsymbol{H}}'$ for the bottom 8 lines to the matrix $(-\boldsymbol{J}, \tilde{\boldsymbol{D}})$ in Example B.2, the matrix is as follows. This is the EPCM $\tilde{\boldsymbol{H}}$ of the PIR.*

$$\begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{61}$$

Example B.6 ($\boldsymbol{K}$ in Example B.2 ($M = 3, N = 2$)) *For each DB$n \neq n' \in [N] = [2]$ and a random key $\boldsymbol{s} = (s_1, \ldots, s_{M-1}) \in [N]^{M-1} = [2]^{3-1}$, the query $Q_n^{(m)} \in [N]^M = [2]^3$ to DB n is*

$$Q_n^{(m)} = (s_1, \ldots, s_{m-1}, n - \sum s_i, s_m, \ldots, s_{M-1}). \tag{62}$$

Here we set from $\mathcal{Q}_1$ to $\mathcal{Q}_N = \mathcal{Q}_2$ as $[N]^M = [2]^3$. Moreover, the responce $A_{(n,Q_n^{(m)})} \in \mathbb{F}_p^{L_{\mathrm{a}}} = \mathbb{F}_p^1$ is, for a message vector $\boldsymbol{w} = (w_{1,1}, \ldots, w_{1,N-1}, w_{2,1}, \ldots, w_{2,N-1}, \ldots) =$

$(w_{1,1}, w_{2,1}, w_{3,1})$,

$$A_{(n,Q_n^{(m)})} = w_{1,s_1} + \cdots + w_{m-1,s_{m-1}} + w_{m,n-\sum s_i} + w_{m+1,s_m} + \cdots + w_{M,s_{M-1}} \tag{63}$$

where, for any $m \in [M] = [3]$, we set $w_{m,N} = w_{m,2} \coloneqq 0$. Then it holds that

$$\begin{aligned} & W_{m,n'-\sum s_i} - W_{m,n-\sum s_i} \\ & + A_{(n,\underbrace{(s_1,\ldots,s_{m-1},n-\sum s_i,s_m,\ldots,s_{M-1})}_{=Q_n^{(m)}})} \\ & - A_{(n',\underbrace{(s_1,\ldots,s_{m-1},n'-\sum s_i,s_m,\ldots,s_{M-1})}_{=Q_{n'}^{(m)}})} \\ & = 0. \end{aligned} \tag{64}$$

Therefore $\boldsymbol{K} \in \mathbb{F}_p^{L_{\mathrm{a}} \sum_{m\in[M]} \left|\boldsymbol{\mathcal{Q}}^{(m)}\right| N(N-1) \times (L_{\mathrm{w}} M + \sum_{n\in[N]} |\mathcal{Q}_n| L_{\mathrm{a}})} = \mathbb{F}_p^{MN^{M-1}N(N-1)\times(M(N-1)+N^M N)} = \mathbb{F}_p^{24\times 19}$ is as follows.

$$\begin{pmatrix}
-1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix} \tag{65}$$

Example B.7 ($\boldsymbol{B}$ in Example B.2 ($M = 3, N = 2, L_{\mathrm{a}} = 1$)) *We set the function $B(\cdot,\cdot)$ as follows*[2]*.*

- *If* $m = 1$ *(*$I = [M] \setminus \{m\} = \{2, 3\}$*),*
  - $B(I, \{(1, 100)\}) = \{(1, 100)\}$, $B(I, \{(2, 000)\}) = \emptyset$
  - $B(I, \{(1, 001)\}) = \emptyset$, $B(I, \{(2, 101)\}) = \{(2, 101)\}$
  - $B(I, \{(1, 010)\}) = \emptyset$, $B(I, \{(2, 110)\}) = \{(2, 110)\}$
  - $B(I, \{(1, 111)\}) = \{(1, 111)\}$, $B(I, \{(2, 011)\}) = \emptyset$
- *If* $m = 2$ *(*$I = [M] \setminus \{m\} = \{1, 3\}$*),*
  - $B(I, \{(1, 010)\}) = \{(1, 010)\}$, $B(I, \{(2, 000)\}) = \emptyset$
  - $B(I, \{(1, 001)\}) = \emptyset$, $B(I, \{(2, 011)\}) = \{(2, 011)\}$
  - $B(I, \{(1, 100)\}) = \emptyset$, $B(I, \{(2, 110)\}) = \{(2, 110)\}$
  - $B(I, \{(1, 111)\}) = \{(1, 111)\}$, $B(I, \{(2, 101)\}) = \emptyset$
- *If* $m = 3$ *(*$I = [M] \setminus \{m\} = \{1, 2\}$*),*
  - $B(I, \{(1, 001)\}) = \{(1, 001)\}$, $B(I, \{(2, 000)\}) = \emptyset$
  - $B(I, \{(1, 010)\}) = \emptyset$, $B(I, \{(2, 011)\}) = \{(2, 011)\}$
  - $B(I, \{(1, 100)\}) = \emptyset$, $B(I, \{(2, 101)\}) = \{(2, 101)\}$
  - $B(I, \{(1, 111)\}) = \{(1, 111)\}$, $B(I, \{(2, 110)\}) = \emptyset$

Then $\boldsymbol{B} \in \mathbb{F}_p^{12 \times 19}$ *is as follows.*

$$\begin{pmatrix}
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix} \tag{66}$$

Example B.8 (a part of the EPCM in Example B.2 ($M = 3, N = 2$)) $\begin{pmatrix} -\boldsymbol{J} & \tilde{\boldsymbol{D}} \\ \boldsymbol{K}_{[M]} & \boldsymbol{K}_{[M+1, M+\sum_{n \in [N]} |\mathcal{Q}_n|]} \\ \boldsymbol{B}_{[M]} & \boldsymbol{B}_{[M+1, M+\sum_{n \in [N]} |\mathcal{Q}_n|]} \end{pmatrix}$ *is as follows.*

[2] Actually, we need to determine more, but this is good enough to determine the matrix $\boldsymbol{B}$.

$$
\begin{pmatrix}
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\[1em]
-1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\[1em]
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}
\tag{67}
$$

References

[1] K. Kazama and T Yoshida. A note on parity check matrix of private information retrieval code. `https://x.gd/kEJ58`, 2024.

[2] Benny Chor, Eyal Kushilevitz, Oded Goldreich, and Madhu Sudan. Private information retrieval. *J. ACM*, Vol. 45, No. 6, pp. 965–981, November 1998.

[3] H. Sun and S. A. Jafar. The capacity of private information retrieval. *IEEE Transactions on Information Theory*, Vol. 63, No. 7, pp. 4075–4088, 2017.

[4] C. Tian, H. Sun, and J. Chen. Capacity-achieving private information retrieval codes with optimal message size and upload cost. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, May 2019.

[5] Siddhartha Kumar, Hsuan-Yin Lin, Eirik Rosnes, and Alexandre Graell i Amat. Achieving private information retrieval capacity in distributed storage using an arbitrary linear code. *CoRR*, Vol. abs/1712.03898, , 2017.

[6] Ragnar Freij-Hollanti, Oliver W. Gnilke, Camilla Hollanti, Anna-Lena Horlemann-Trautmann, David A. Karpuk, and Ivo Kubjas. t-private information retrieval schemes using transitive codes. *CoRR*, Vol. abs/1712.02850, , 2017.

[7] Hua Sun and Syed Ali Jafar. On the capacity of locally decodable codes. *IEEE Transactions on Information Theory*, Vol. 66, No. 10, pp. 6566–6579, 2020.

[8] U. Imazu, K. Kazama, and T. Matsushima. A proposal of the construction algorithm of private information retrieval systems with high efficiency (in japanese). *Proceedings of Japan Industrial Management Association Annual Conference 2021 Spring*, pp. 367–370, May 2021.

[9] K. Kazama, A. Kamatsuka, T. Yoshida, and T. Matsushima. A note on a relationship between smooth locally decodable codes and private information retrieval. In *2020 International Symposium on Information Theory and Its Applications (ISITA)*, pp. 259–263, 2020.