Toward the Minimal Set of Information Inequalities in Regenerating Codes: An Algebraic Approach

***Abstract*—The proof of information inequalities in the regenerating codes is often formulated as a linear programming (LP) problem. However, its constraint set typically contains numerous implicit equations and redundant inequalities, which obscure the problem structure and hinder efficient computation. In this paper, we address this issue by developing an algebraic methodology to systematically detect implicit equations and eliminate all the redundant constraints. Our approach establishes an equivalent minimal constraint set for the LP derived from the general $(n, n-1, n-1)$ regenerating codes for any n. This minimal set completely characterizes the constraint region of regenerating codes without any redundancy.**

I. Introduction

The study of the fundamental limits of information systems has been a central theme in information theory since its inception by Claude Shannon in 1948 [19]. Over time, an information-theoretic approach has been applied to analyze various systems, including coding for distributed data storage [4], [18], coded caching [15], private information retrieval [22], and straggler-resilient coded computation [12]. The quest to understand and characterize the fundamental limits of data storage systems has been a cornerstone of information theory. Regenerating codes, first introduced by Dimakis et al. [4], aim to address the trade-off between storage capacity and repair bandwidth in distributed systems. These codes ensure that data stored across multiple nodes can be reconstructed efficiently even in the event of node failures. Specifically, exact-repair regenerating codes hold practical importance as they enforce the stringent requirement that repaired nodes replicate the original data exactly, as opposed to merely serving equivalent functionality. For these reasons, exact-repair regenerating codes have received considerable attention recently [2], [18], [20], [23], [24], where the regenerated data need to be exactly the same as that stored in the failed node.

Traditionally, these fundamental limits—often expressed as outer bounds or converse bounds—have been derived analytically. This process involves constructing a sequence of steps using information inequalities and demands a deep understanding of the problem, proficiency with information-theoretic techniques, and significant human ingenuity. However, as information systems grow increasingly complex, this manual approach becomes less practical. To address these challenges, a computational approach has been proposed, yielding several notable results [3], [8], [13], [14], [21], [25]–[29], [31].

Despite these successes, the computational approach faces significant limitations. Its core idea is to frame the derivation of converse bounds as an optimization problem: joint entropies are treated as variables, while information inequalities and problem-specific constraints form a linear program (LP) [32]. By solving the LP and its dual, outer bounds and corresponding proofs can be obtained. However, the exponential growth in the number of Shannon-type information inequalities with respect to the number of random variables [33] poses a major challenge. For larger-scale problems, completing such computations becomes infeasible. Techniques like exploiting symmetry and implication relations can reduce the LP's scale, enabling some otherwise intractable cases to be computed [25], [27], [30]. Nevertheless, these methods cannot fully overcome the memory and computational barriers [36]. To address these hurdles, new techniques are urgently needed to break through the existing limitations in memory and computational efficiency.

For the (4, 3, 3) exact-repair regenerating code configuration, the complete characterization of its rate region provided a breakthrough in demonstrating a distinct and non-vanishing gap between the achievable trade-offs of functional-repair and exact-repair codes. This was achieved using a computational approach that extended Yeung's linear programming (LP) framework [32] for information inequalities. Subsequently, similar methods were adapted to analyze more complex configurations such as (5,4,4) codes [26], where layered code constructions were shown to achieve the outer bounds. Despite these advancements, conventional computational methods for deriving outer bounds face significant limitations, including exponential growth in complexity with the number of random variables involved. Alternative approaches, such as maximin problem reformulation and iterative procedures leveraging dual LPs, have been proposed to address these challenges. These methods not only alleviate memory and computational bottlenecks but also incorporate human intuition, such as leveraging potentially optimal code constructions, to enhance their effectiveness.

Recently, Chen and Tian [3] synthesized prior work and extended the computational approach to derive tighter outer bounds for larger-scale configurations, such as the (6, 5, 5) regenerating code problem. By combining symmetry reductions, optimized constraint selection, and advanced algorithms, they demonstrated significant improvements in scalability and bound tightness. These contributions provide valuable insights into the rate-region characterization of exact-repair regenerating codes and their implications for practical distributed storage systems.

Let p_X denote the probability distribution of a discrete random variable X. In information theory, the entropy (Shannon entropy) of X is defined by

$$H(X) = -\sum_{x} p_X(x) \log p_X(x).$$

The base of the logarithm is taken to be some convenient positive real number. When it is equal to 2, the unit of entropy is the bit. Likewise, the joint entropy of two random variables X and Y is defined by

$$H(X,Y) = -\sum_{x,y} p(X,Y)\log p_{XY}(x,y).$$

This definition is readily extendable to any finite number of random variables. All summations are assumed to be taken over the support of the underlying distribution. For example, for $H(X,Y)$ mentioned above, the summation is taken over all x and y such that $p_{XY}(x,y) > 0$.

In addition to entropy, the following information measures are also defined:

Conditional entropy

$$H(X|Y) = H(X,Y) - H(Y).$$

Mutual information

$$I(X;Y) = H(X) + H(Y) - H(X,Y).$$

Conditional mutual information

$$I(X;Y|Z) = H(X,Z) + H(Y,Z) - H(X,Y,Z) - H(Z).$$

Together with entropy, these information measures are collectively called Shannon's information measures. In fact, entropy, conditional entropy, and mutual information are all special cases of conditional mutual information. Note that all Shannon's information measures are linear combinations of entropies.

In this paper, an *information expression* refers to a function of Shannon's information measures involving a finite number of random variables. This expression can be written as a function of entropies, referred to as the *canonical form* of the information expression. The uniqueness of the canonical form was established for linear information expressions in [9] and later extended to more general information expressions in [32].

It is well known that all of Shannon's information measures are nonnegative. This property forms a set of inequalities called the *basic inequalities*. Information inequalities—whether unconstrained or constrained—that can be derived from the basic inequalities are referred to as *Shannon-type inequalities*. Most known information inequalities fall into this category. However, non-Shannon-type inequalities also exist, as first demonstrated in [37]. For a detailed discussion, see [33, Ch. 15].

In information theory, proving various information inequalities and identities involving Shannon's information measures is often required. These proofs are essential, particularly for establishing the converse of most coding theorems. However, proving an information inequality or identity involving more than a few random variables is often highly challenging.

To address this issue, a framework for linear information inequalities was introduced in [32]. Within this framework, the verification of Shannon-type inequalities can be formulated as a linear programming (LP) problem. Based on this idea, the *Information Theoretic Inequality Prover* (ITIP), a MATLAB-based software package, was developed [35]. Subsequently, different variations of ITIP have been developed. Instead of MATLAB, Xitip [16] uses a C-based linear programming solver, and it has been further developed into its web-based version, oXitip [17]. minitip [1] is a C-based version of ITIP that adopts a simplified syntax and has a user-friendly syntax checker. psitip [11] is a Python library that can verify unconstrained/constrained/existential entropy inequalities. It is a computer algebra system where random variables, expressions, and regions are objects that can be manipulated. AITIP [10] is a cloud-based platform that not only provides analytical proofs for Shannon-type inequalities but also give hints on constructing a smallest counterexample in case the inequality to be verified is not a Shannon-type inequality.

However, the LP-based approach is generally computationally inefficient as it does not exploit the special structure of the underlying LP. To address this limitation, Guo *et al.* [5] proposed a set of algorithms that can be implemented using symbolic computation. These algorithms enable procedures to reduce the original LP to a minimal size, making it easier to solve. This symbolic approach is computationally more efficient than solving the original LP directly. In the follow-up works [6], [7], Guo *et al.* built on the concepts from [5] to develop a new symbolic method that not only makes the LP reduction more efficient but, in many cases, proves the information inequality without requiring any LP solving.

Throughout this paper, all random variables are discrete. Unless otherwise specified, all information expressions involve some or all of the random variables $X_1, X_2, \ldots, X_n$. The value of n will be specified when necessary. Denote the set $\{1, 2, \ldots, n\}$ by $\mathcal{N}_n$, the set $\{0, 1, 2, \ldots\}$ by $\mathbb{N}_{\geq 0}$ and the set $\{1, 2, \ldots\}$ by $\mathbb{N}_{>0}$.

Theorem I.1. [32] *Any Shannon's information measure can be expressed as a conic combination of the following two elemental forms of Shannon's information measures:*
i) $H(X_i|X_{\mathcal{N}_n - \{i\}})$
ii) $I(X_i;X_j|X_K)$*, where* $i \neq j$ *and* $K \subseteq \mathcal{N}_n - \{i,j\}$.

Example I.1. *For* $n = 3$*, we can write*

$$\begin{aligned} H(X_1|X_3) &= H(X_1|X_2,X_3) + I(X_1;X_2|X_3) \\ I(X_1;X_2,X_3) &= I(X_1;X_2) + I(X_1;X_3|X_2), \end{aligned}$$

where the RHSs above are elemental forms of Shannon's information measures.

The nonnegativity of the two elemental forms of Shannon's information measures forms a proper but equivalent subset of the set of basic inequalities. The inequalities in this smaller set are called the *elemental inequalities*. In [32], the minimality of the elemental inequalities is also proved. The total number of elemental inequalities is equal to $u \triangleq n + \binom{n}{2}2^{n-1}$.

Shannon's information measures, with conditional mutual information being the general form, can be expressed as a linear combination of joint entropies. For the random variables $X_1, X_2, \ldots, X_n$, there are a total of $2^n - 1$ joint entropies. By regarding the joint entropies as variables, the basic (elemental) inequalities become linear inequality constraints in $\mathbb{R}^{2^n-1}$. By the same token, the linear equality constraints on Shannon's information measures imposed by the problem under discussion become linear equality constraints in $\mathbb{R}^{2^n-1}$. This way, the problem of verifying a (linear) Shannon-type inequality can be formulated as a linear program (LP), which is described next.

Let $\mathbf{h}$ be the column (2^n-1)-vector of the joint entropies of $X_1, X_2, \ldots, X_n$. The set of elemental inequalities can be written as $\mathbf{Gh} \geq 0$, where $\mathbf{G}$ is an $u \times (2^n-1)$ matrix and $\mathbf{Gh} \geq 0$ means that all the entries of $\mathbf{Gh}$ are nonnegative. Likewise, linear constraints on the joint entropies can be written as $\mathbf{Qh} = 0$. When there is no constraint on the joint entropies, $\mathbf{Q}$ is assumed to contain zero rows. The following theorem enables a Shannon-type inequality to be verified by solving an LP.

Theorem I.2. [32] $\mathbf{b}^\top\mathbf{h} \geq 0$ *is a Shannon-type inequality under the constraint* $\mathbf{Qh} = 0$ *if and only if the minimum of the problem*

$$\textit{Minimize } \mathbf{b}^\top\mathbf{h}, \textit{ subject to } \mathbf{Gh} \geq 0 \textit{ and } \mathbf{Qh} = 0$$

is zero.

II. Problem reformulation

In this section, we will reformulate the inequality system generated from the $(n, n-1, n-1)$ regenerating code problem [25]. Assume that the distributed stored messages are denoted by the n variables $W_1, \ldots, W_n$. For any $1 \leq i \neq j \leq n$, the helper message sent from node i to node j is denoted as the variable S_{ij}. The helper messages $S_{ij}, j \neq i$ can be produced from the message W_i. For a specific node j, the stored message W_j can be repaired from the helper messages $S_{ij}, i \neq j$. These relations can be reflected in the following repair constraints, where $1 \leq i \neq j \leq n$:

$$\begin{cases} H(W_i) - H(W_i, \bigcup_{j \neq i} S_{ij}) = 0, & \text{(1a)} \\ H(\bigcup_{i \neq j} S_{ij}) - H(W_j, \bigcup_{i \neq j} S_{ij}) = 0, & \text{(1b)} \end{cases}$$

In this formulation, the collection $\{W_i, S_{ij} \mid 1 \leq i, j \leq n\}$ constitutes the set of random variables. Consequently, the $(n, n-1, n-1)$ regenerating code problem involves $N = n^2$ random variables. The form $H(X)$ for any subset $X \subseteq \{W_i, S_{ij} \mid 1 \leq i, j \leq n\}$ is defined as the *entropy variable* induced by X. For simplicity, we reformulate the random variables with the symbol "X" associated with the subscripts following the rules: $X_{i+n(i-1)} = W_i$ and $X_{j+n(i-1)} = S_{ij}$ for any $1 \leq i \neq j \leq n$. These replacements are more clear when we rearrange the variables in a $n \times n$ square table, shown in the following:

$$\begin{pmatrix} W_1 & S_{12} & \cdots & S_{1n} \\ S_{21} & W_2 & \cdots & S_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ S_{n1} & S_{n2} & \cdots & W_n \end{pmatrix}$$
$$\Downarrow$$
$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_{n+1} & X_{n+2} & \cdots & X_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ X_{n(n-1)+1} & X_{n(n-1)+2} & \cdots & X_{n^2} \end{pmatrix}$$

For a subset $\mathcal{A} \subseteq \mathcal{N}$, the notation $X_\mathcal{A}$ denotes the collection of random variables $\{X_i \mid i \in \mathcal{A}\}$. In the paper, when there is no ambiguity, we denote the entropy variable $H(X_\mathcal{A})$ by $H_\mathcal{A}$. By Theorem I.1, we obtain the basic constraints (elemental inequalities):

$$H(X_\mathcal{N}) - H(X_{\mathcal{N}\setminus\{i\}}) \geq 0, \quad \text{(2a)}$$
$$H(X_{i,\mathcal{A}}) + H(X_{j,\mathcal{A}}) - H(X_{i,j,\mathcal{A}}) - H(X_\mathcal{A}) \geq 0, \quad \text{(2b)}$$

for any $i, j \in \mathcal{N}$ and $\mathcal{A} \subseteq \mathcal{N} \setminus \{i, j\}$. This system consists of $N = 2^n - 1$ entropy variables and $N + 2^{N-2} \cdot \binom{N}{2} \sim O(2^{n^2} n^4)$ inequalities, possessing full permutation symmetry under any exchange of the variables. Denote by

- $\mathcal{D}_k = \{n(k-1)+k\}$ is the set consist of the k-th diagonal index,
- $\mathcal{R}_k = \{n(k-1)+1, n(k-1)+2, \ldots, nk\} \setminus \mathcal{D}_k$ consists of the indices in the k-row excluding the diagonal index,
- $\mathcal{C}_k = \{k, n+k, \ldots, n(n-1)+k\} \setminus \mathcal{D}_k$ consists of the indices in the k-column excluding the diagonal index.

Then, the constraint region, which is called *Initial System* in the following, of the $(n, n-1, n-1)$ regenerating code problem can be reformulated as (3):

$$\begin{cases} H_\mathcal{N} - H_{\mathcal{N}\setminus\{i\}} \geq 0, \ i \in \mathcal{N} & \text{(3a)} \\ H_{i,\mathcal{A}} + H_{j,\mathcal{A}} - H_{i,j,\mathcal{A}} - H_\mathcal{A} \geq 0, \ i, j \in \mathcal{N}, \\ \qquad \mathcal{A} \subseteq \mathcal{N} \setminus \{i, j\} & \text{(3b)} \\ H_{\mathcal{D}_k} = H_{\mathcal{D}_k \cup \mathcal{R}_k}, \ k \in \{1 \ldots n\} & \text{(3c)} \\ H_{\mathcal{C}_k} = H_{\mathcal{D}_k \cup \mathcal{C}_k}, \ k \in \{1 \ldots n\} & \text{(3d)} \end{cases}$$

Owing to the repair constraints defined in (3c) and (3d), (3) exhibits multiple implicit equations and redundant inequalities. The resolution of implicit equations leads to significant dimensionality reduction, and the removal of redundant inequalities further simplifies the system by decreasing the number of constraints. Our purpose is to provide a general formula for the minimal equivalent system, solving the implicit equations and removing all the redundant inequalities. This simplified system will help to improve the efficiency of solving the related problems in the regenerating code problem.

III. Equivalent minimal set

This section outlines the framework for system simplification and summarizes the main contributions of this work. In Section III-A, we present methods for detecting implicit equations. These equations establish equivalence relations among variables, which propagate throughout the inequality system. By solving these implicit equations, we achieve substantial dimensionality reduction, decreasing the system dimension from 2^{n^2} to $\sum_{i=0}^{n} \binom{n}{i} 2^{i(n-i)} (2^{n-i-1} - 1)^{n-i} \sim O(2^{n^2-n})$. In Section III-B, we develop criteria for identifying redundant inequalities, resulting in a Final System with substantially fewer constraints. The constraint count decreases from $O(2^{n^2} n^4)$ to $O(2^{n^2-n} n^4)$.

A. Implicit equations

Example III.1 illustrates an example of deriving implicit equations from (3).

Example III.1 (Implicit Equations)**.** *Consider the case where $n = 3$. Let $\mathcal{N}$ denote the full index set $\{1, 2, \ldots, 9\}$. Starting with subsets $\mathcal{A}_1 = \{1, 2\}$ and $\mathcal{B}_1 = \{1\}$, we successively append the elements $4, 5, 6, 7, 8, 9$ to $\mathcal{A}_1$ and rename the resulting subsets as $\mathcal{A}_i$ for $2 \le i \le 7$. Similarly, we successively append the elements $3, 4, 5, 6, 7, 8, 9$ to $\mathcal{B}_1$ and rename the resulting subsets as $\mathcal{B}_i$ for $2 \le i \le 8$.*

$$\begin{cases} H_{\mathcal{A}_i \cup \{3\}} + H_{\mathcal{A}_{i+1}} - H_{\mathcal{A}_{i+1} \cup \{3\}} - H_{\mathcal{A}_i} \ge 0, \text{ for } 1 \le i \le 6, \\ H_{\mathcal{N}} - H_{\mathcal{A}_6} \ge 0 \end{cases} \tag{4}$$

$$\begin{cases} H_{\mathcal{B}_i \cup \{2\}} + H_{\mathcal{B}_{i+1}} - H_{\mathcal{B}_{i+1} \cup \{2\}} - H_{\mathcal{B}_i} \ge 0, \text{ for } 1 \le i \le 7, \\ H_{\mathcal{N}} - H_{\mathcal{B}_8} \ge 0 \end{cases} \tag{5}$$

Adding the inequalities in (4) *and* (5) *yields $H_{1,2,3} - H_{1,2} \ge 0$ and $H_{1,2} - H_1 \ge 0$, respectively. This further implies $H_{1,2,3} - H_1 \ge 0$, which is an inherent property of the entropy variables. Note that* (3) *contains an explicit equation $H_{\mathcal{D}_1 \cup \mathcal{R}_1} - H_{\mathcal{D}_1} = H_{1,2,3} - H_1 = 0$. Thus, all inequalities in* (4) *and* (5) *that imply $H_{1,2,3} - H_{1,2} \ge 0$ are in fact implicit equations.*

The implicit equations establish equivalences among the variables, which consequently propagate to the entire inequality system. An example of the equivalence is shown in Example III.2.

Example III.2 (Equivalence among variables and inequality system)**.** *In Example III.1, the following equivalence relations among entropy variables can be established:*

$$\begin{cases} H_1 = H_{1,2} = H_{1,3} = H_{1,2,3}, \\ H_{1,4} = H_{1,2,4} = H_{1,3,4} = H_{1,2,3,4}, \\ H_{1,7} = H_{1,2,7} = H_{1,3,7} = H_{1,2,3,7}, \\ H_{1,4,7} = H_{1,2,4,7} = H_{1,3,4,7} = H_{1,2,3,4,7}. \end{cases}$$

To simplify, the entropy variables $H_{\mathcal{C}}$ (resp. $H_{\mathcal{C} \cup \{4\}}$, $H_{\mathcal{C} \cup \{7\}}$, $H_{\mathcal{C} \cup \{4,7\}}$) are equivalent when $\mathcal{C}$ takes values from the set $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$. Thus, $H_{\mathcal{C} \cup \{4\}} + H_{\mathcal{C} \cup \{7\}} - H_{\mathcal{C} \cup \{4,7\}} - H_{\mathcal{C}} \ge 0$ represents the equivalent inequalities. Similarly, we can derive $H_{4,7} = H_{\mathcal{C} \cup \{4,7\}}$ for any $\mathcal{C}$ belonging to the set $\{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$.

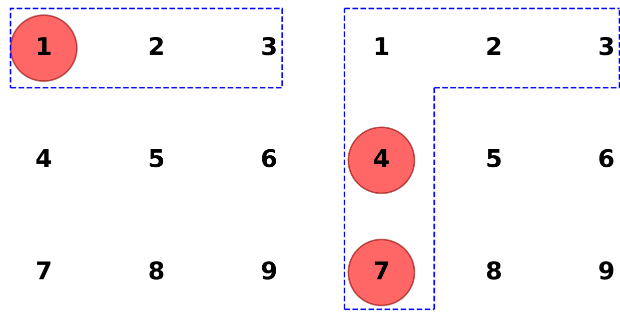
In fact, the equivalent relations, as well as the simplification of (3), heavily rely on the index set of the entropy variables. We give the definitions of *closed set* and *closure* for the index set, which enables us to generalize the equivalence relations via Theorem III.1.

Definition III.1 (Closed Set and Closure)**.** *A given subset $\mathcal{A} \subseteq \mathcal{N}$ is called a* ***closed set*** *if $\mathcal{A}$ satisfies the following two conditions:*

1) *if $\mathcal{D}_k \subseteq \mathcal{A}$ for some k, then $\mathcal{R}_k \subseteq \mathcal{A}$;*
2) *if $\mathcal{C}_k \subseteq \mathcal{A}$ for some k, then $\mathcal{D}_k \cup \mathcal{R}_k \subseteq \mathcal{A}$.*

The minimal closed set containing $\mathcal{A}$, denoted by $\overline{\mathcal{A}}$, is called the ***closure*** *of $\mathcal{A}$.*

According to Definition III.1, we give out two criteria for constructing the closure of a given set $\mathcal{A}$, which is illustrated in Fig. 1:



(a) Row Criterion (R)   (b) Column Criterion (C)

Fig. 1: Row and Column Criteria for Constructing Closed Sets

(R) if $\mathcal{D}_k \subseteq \mathcal{A}$ for some k, then add $\mathcal{R}_k$ into $\mathcal{A}$ (Fig. 1a);
(C) if $\mathcal{C}_k \subseteq \mathcal{A}$ for some k, then add $\mathcal{D}_k \cup \mathcal{R}_k$ into $\mathcal{A}$ (Fig. 1b).

Example III.3 illustrates some of the closures that appear in Examples III.1 and III.2. Furthermore, Example III.4 depicts the detailed process of constructing the closure.

Example III.3 (Closure for index set)**.** *We list part of the closures appeared in Example III.2 here:*

$$\overline{\{1\}} = \overline{\{1, 2\}} = \overline{\{1, 3\}} = \{1, 2, 3\},$$
$$\overline{\{1, 4\}} = \overline{\{1, 2, 4\}} = \overline{\{1, 3, 4\}} = \{1, 2, 3, 4\},$$
$$\overline{\{4, 7\}} = \overline{\{1, 4, 7\}} = \overline{\{1, 2, 4, 7\}} = \overline{\{1, 3, 4, 7\}} = \{1, 2, 3, 4, 7\}$$

Example III.4 (Construction of Closure)**.** *Let $n = 4$ and $\mathcal{A} = \{1, 7, 15\}$ be the initial set. Starting with the diagonal element $\mathcal{D}_1 = \{1\}$, we add the first row $\mathcal{R}_1 = \{2, 3, 4\}$ to the set. This triggers the addition of the third column, $\mathcal{C}_3 = \{3, 7, 15\}$, due to the newly included element 3. The process continues iteratively until closure is reached, yielding $\overline{\mathcal{A}} = \{1, 2, 3, 4, 7, 9, 10, 11, 12, 15\}$.*

Given a closed set $\mathcal{A}$ and an element i, the closure $\overline{\{i\} \cup \mathcal{A}}$ is constructed by an iterative process that alternates between the row criterion (R) and the column criterion (C). The process begins with the row criterion (R) if i is a diagonal element; otherwise, the column criterion (C) applies first. Note that the application of either the row criterion (R) or the column criterion (C) results in the addition of some row(s) to the current set. Let $\mathsf{RowIndexList}(i, \mathcal{A})$ denote the list of row indices added during the iterative construction of the closure $\overline{\{i\} \cup \mathcal{A}}$. For instance, with $i = 1$ and $\mathcal{A} = \{7, 15\}$, we have $\mathsf{RowIndexList}(1, \{7, 15\}) = [1, 3]$, meaning rows 1 and 3 are added in the process. Then, for a given closed set $\mathcal{A}$ and an element i, the closure can be expressed explicitly as

$$\overline{\{i\} \cup \mathcal{A}} = \mathcal{A} \cup \bigcup_{k \in \mathsf{RowIndexList}(i, \mathcal{A})} (\mathcal{D}_k \cup \mathcal{R}_k). \tag{6}$$

It is easy to verify the properties for closed sets and closures shown in Property III.1.

Property III.1 (Closure Properties)**.** *Let $\mathcal{A}, \mathcal{B} \subseteq \mathcal{N}$ be arbitrary subsets, and let $i, j \in \mathcal{N}$. The closure operation satisfies the following:*

1) *If $\mathcal{A}$ and $\mathcal{B}$ are closed, so is their intersection $\mathcal{A} \cap \mathcal{B}$.*
2) *If $\mathcal{A} \subseteq \mathcal{B}$, then $\overline{\mathcal{A}} \subseteq \overline{\mathcal{B}}$.*

3) *We have* $\{i\} \cup \mathcal{A} \subseteq \{i\} \cup \overline{\mathcal{A}} \subseteq \overline{\{i\} \cup \overline{\mathcal{A}}} = \overline{\{i\} \cup \mathcal{A}}$.
4) *If* $\mathcal{A}$ *is a closed set, and* $i, j \notin \mathcal{A}$ *with* $i \neq j$, *we have*

$$\overline{\{i\} \cup \mathcal{A}} \cap \overline{\{j\} \cup \mathcal{A}} = \begin{cases} \overline{\{i\} \cup \mathcal{A}}, & \text{if } i \in \overline{\{j\} \cup \mathcal{A}}; \\ \overline{\{j\} \cup \mathcal{A}}, & \text{if } j \in \overline{\{i\} \cup \mathcal{A}}; \\ \mathcal{A}, & \text{otherwise}. \end{cases} \quad (7)$$

Proof. The first three properties follow directly from the definition. We now prove the fourth property.

Since $\mathcal{A}$ is closed, we have $\mathcal{A} = \overline{\mathcal{A}} \subseteq \overline{\{i\} \cup \mathcal{A}} \cap \overline{\{j\} \cup \mathcal{A}}$. Suppose $i \in \overline{\{j\} \cup \mathcal{A}}$. By the monotonicity of closure, $\overline{\{i\} \cup \mathcal{A}} \subseteq \overline{\{j\} \cup \mathcal{A}}$, and hence $\overline{\{i\} \cup \mathcal{A}} \cap \overline{\{j\} \cup \mathcal{A}} = \overline{\{i\} \cup \mathcal{A}}$. The case $j \in \overline{\{i\} \cup \mathcal{A}}$ is symmetric, yielding $\overline{\{i\} \cup \mathcal{A}} \cap \overline{\{j\} \cup \mathcal{A}} = \overline{\{j\} \cup \mathcal{A}}$.

Now let us consider the case when $i \notin \overline{\{j\} \cup \mathcal{A}}$ and $j \notin \overline{\{i\} \cup \mathcal{A}}$. Assume, for contradiction, that there exists a common row index $k \in \mathsf{RowIndexList}(i, \mathcal{A}) \cap \mathsf{RowIndexList}(j, \mathcal{A})$.

If i is the k-th diagonal element, then $i \in \mathcal{D}_k \subseteq (\mathcal{D}_k \cup \mathcal{R}_k) \subseteq \overline{\{j\} \cup \mathcal{A}}$, contradicting $i \notin \overline{\{j\} \cup \mathcal{A}}$. Similarly, j cannot be the k-th diagonal element. Therefore, the k-th row is added via a column criterion in both closures. Consequently, $\mathcal{C}_k \subseteq \overline{\{i\} \cup \mathcal{A}}$ and $\mathcal{C}_k \subseteq \overline{\{j\} \cup \mathcal{A}}$. Moreover, we have $i, j \notin \mathcal{C}_k$.

Let l_i and l_j denote the respective row indices of i and j. In constructing $\overline{\{i\} \cup \mathcal{A}}$, the set $\mathcal{D}_k \cup \mathcal{R}_k$ is added because the element at (l_i, k) is introduced. Here we know that the element at (l_i, k) is not contained in $\mathcal{A}$ and all other elements of $\mathcal{C}_k$ were already in $\mathcal{A}$ or added earlier. If the element at (l_j, k) were also added during this construction, then $\mathcal{D}_{l_j} \cup \mathcal{R}_{l_j} \subseteq \overline{\{i\} \cup \mathcal{A}}$, implying $j \in \overline{\{i\} \cup \mathcal{A}}$, a contradiction. Hence, (l_j, k) must have been in $\mathcal{A}$ from the start. Therefore, from the construction of $\overline{\{i\} \cup \mathcal{A}}$, we deduce that the element at (l_i, k) is not in $\mathcal{A}$, whereas the element at (l_j, k) must be in $\mathcal{A}$. By a symmetric argument from the construction of $\overline{\{j\} \cup \mathcal{A}}$, we deduce the opposite: the element at (l_j, k) is not in $\mathcal{A}$, while the one at (l_i, k) must be in $\mathcal{A}$. These two conclusions are mutually exclusive, constituting a contradiction.

Hence, our initial assumption was false; there can be no common row index k. This proves that $\mathsf{RowIndexList}(i, \mathcal{A}) \cap \mathsf{RowIndexList}(j, \mathcal{A}) = \emptyset$. Therefore, $\overline{\{i\} \cup \mathcal{A}} \cap \overline{\{j\} \cup \mathcal{A}} = \mathcal{A}$ follows immediately. □

Property III.2 demonstrates several fundamental properties that are satisfied by entropy variables.

Property III.2 (Entropy Variables)**.** *For all entropy variables* $H_{\mathcal{A}}, \mathcal{A} \subseteq \mathcal{N}$,

1) *For* $\mathcal{I}, \mathcal{J}, \mathcal{A} \subseteq \mathcal{N}$ *and do not intersect with each other,* $\mathcal{I}, \mathcal{J} \neq \emptyset$, *then* $H_{\mathcal{I} \cup \mathcal{A}} + H_{\mathcal{J} \cup \mathcal{A}} - H_{\mathcal{I} \cup \mathcal{J} \cup \mathcal{A}} - H_{\mathcal{A}} \geq 0$
2) *For* $\mathcal{A} \subseteq \mathcal{A}'$, $H_{\mathcal{A}} \leq H_{\mathcal{A}'}$. *Therefore, if* $H_{\mathcal{A}} = H_{\mathcal{A}'}$, $\forall \mathcal{A} \subseteq \mathcal{K} \subseteq \mathcal{A}'$, $H_{\mathcal{A}} = H_{\mathcal{K}} = H_{\mathcal{A}'}$

Note that in the existing examples, the entropy variables whose index set having the same closure are equivalent. Actually, this is true for variables with arbitrary index sets. Lemma III.1 shows that two entropy variables are equivalent whenever the index set of one can be obtained from that of the other by applying the row criterion (R).

Lemma III.1. *For any subset* $\mathcal{A} \subseteq \mathcal{N}$, *if* $\mathcal{D}_k \subseteq \mathcal{A}$ *for some* k, *then we have* $H_{\mathcal{A}} = H_{\mathcal{A} \cup \mathcal{R}_k}$.

Proof. If $\mathcal{A} \subseteq \mathcal{D}_k \cup \mathcal{R}_k$, then $\mathcal{D}_k \subseteq \mathcal{A} \subseteq \mathcal{A} \cup \mathcal{R}_k \subseteq \mathcal{D}_k \cup \mathcal{R}_k$, the conclusion follows immediately according to (3c) and Property III.2.

Otherwise, let $\mathcal{I} = \mathcal{A} \backslash (\mathcal{D}_k \cup \mathcal{R}_k)$. By Property III.2, we have $H_{\mathcal{I} \cup \mathcal{D}_k} + H_{\mathcal{D}_k \cup \mathcal{R}_k} - H_{\mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k} - H_{\mathcal{D}_k} \geq 0$. Since $H_{\mathcal{D}_k} = H_{\mathcal{D}_k \cup \mathcal{R}_k}$, the inequality simplifies to $H_{\mathcal{I} \cup \mathcal{D}_k} \geq H_{\mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k}$. On the other hand, because $\mathcal{I} \cup \mathcal{D}_k \subseteq \mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k$, we have the reverse entropy inequality $H_{\mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k} \geq H_{\mathcal{I} \cup \mathcal{D}_k}$. Thus the two entropies coincide: $H_{\mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k} = H_{\mathcal{I} \cup \mathcal{D}_k}$. Now note that $\mathcal{I} \cup \mathcal{D}_k \cup \mathcal{R}_k = \mathcal{A} \cup \mathcal{R}_k$, $\mathcal{I} \cup \mathcal{D}_k = \mathcal{A} \setminus \mathcal{R}_k$, and that $\mathcal{A} \setminus \mathcal{R}_k \subseteq \mathcal{A} \subseteq \mathcal{A} \cup \mathcal{R}_k$. Applying Property III.2 again yields $H_{\mathcal{A}} = H_{\mathcal{A} \cup \mathcal{R}_k}$. □

Substituting $\mathcal{D}_k$ with $\mathcal{C}_k$ and $\mathcal{R}_k$ with $\mathcal{D}_k$ in Lemma III.1 and its proof, we will conclude the following lemma which shows that two entropy variables are equivalent whenever the index set of one can be obtained from that of the other by applying the column criterion (C).

Lemma III.2. *For any subset* $\mathcal{A} \subseteq \mathcal{N}$, *if* $\mathcal{C}_k \subseteq \mathcal{A}$ *for some* k, *then we have* $H_{\mathcal{A}} = H_{\mathcal{A} \cup \mathcal{D}_k} = H_{\mathcal{A} \cup \mathcal{D}_k \cup \mathcal{R}_k}$.

Lemmas III.1 and III.2 directly yield Theorem III.1. Building upon this result, Theorem III.2 furnishes further implicit equations for the system (3).

Theorem III.1. *For any subset* $\mathcal{A} \subseteq \mathcal{N}$, *the entropy satisfies* $H_{\mathcal{A}} = H_{\overline{\mathcal{A}}}$, *where* $\overline{\mathcal{A}}$ *denotes the closure of* $\mathcal{A}$.

Theorem III.2 (Implicit Equations)**.** *In* (3)*, the entropy equivalence relations are as follows:*

1) *for any* $i \in \mathcal{N}$, *the entropy satisfies* $H_{\mathcal{N}} = H_{\overline{\mathcal{N} \setminus \{i\}}}$.
2) *for any index set* $\mathcal{A}$ *and* $i, j \notin \mathcal{A}$, *if* $i \in \overline{\mathcal{A}}$ *or* $j \in \overline{\mathcal{A}}$,*the entropy satisfies* $H_{i,\mathcal{A}} + H_{j,\mathcal{A}} - H_{i,j,\mathcal{A}} - H_{\mathcal{A}} = 0$.

Proof. For the first statement, note that $\overline{\mathcal{N} \setminus \{i\}} = \mathcal{N}$ for every $i \in \mathcal{N}$. The conclusion then follows directly from Theorem III.1.

For the second statement, we treat the case $i \in \overline{\mathcal{A}}$. Since $\mathcal{A} \subseteq \{i\} \cup \mathcal{A} \subseteq \overline{\mathcal{A}}$ and $H_{\mathcal{A}} = H_{\overline{\mathcal{A}}}$, Property III.2 yields $H_{\{i\} \cup \mathcal{A}} = H_{\mathcal{A}}$. Similarly, because $\{j\} \cup \mathcal{A} \subseteq \{i, j\} \cup \mathcal{A} \subseteq \{j\} \cup \overline{\mathcal{A}} \subseteq \overline{\{j\} \cup \mathcal{A}}$ and $H_{\{j\} \cup \mathcal{A}} = H_{\overline{\{j\} \cup \mathcal{A}}}$, we obtain $H_{\{j\} \cup \mathcal{A}} = H_{\{i,j\} \cup \mathcal{A}}$. Consequently, $H_{\{i\} \cup \mathcal{A}} + H_{\{j\} \cup \mathcal{A}} - H_{\{i,j\} \cup \mathcal{A}} - H_{\mathcal{A}} = 0$, which completes the proof of the second statement. □

Theorem III.2 finds the implicit equations in (3). Indeed, we find that the remaining inequalities in this system are not implicit equations.

Theorem III.3. *For any index set* $\mathcal{A}$ *and* $i, j \notin \overline{\mathcal{A}}$, *the inequality* $H_{i,\mathcal{A}} + H_{j,\mathcal{A}} - H_{i,j,\mathcal{A}} - H_{\mathcal{A}} \geq 0$ *is not an implicit equation in* (3).

Proof. For any fixed index set $\mathcal{A}$, we prove this conclusion by assigning special values for the entropy variables, such that the strict inequality are valid. Let

$$H_{\mathcal{K}}=\begin{cases}0, \text{ if } \mathcal{K}=\emptyset\\ 1, \text{ if } \emptyset\neq\mathcal{K}\subseteq\overline{\mathcal{A}}\\ 2, \text{ if } \mathcal{K}\nsubseteq\overline{\mathcal{A}}\end{cases}$$

Since $\{i,j\}\cap\overline{\mathcal{A}}$, we know that $\overline{\mathcal{A}}\neq\mathcal{N}$ and $\mathcal{N}\setminus\{i'\}\nsubseteq\overline{\mathcal{A}}$ for any i'. Therefore, $H_{\mathcal{N}}=H_{\mathcal{N}\setminus\{i'\}}=2$. The inequalities (3a), which are implicit equations are satisfied. If $\mathcal{D}_k\subseteq\overline{\mathcal{A}}$, we have $\mathcal{D}_k\cup\mathcal{R}_k\subseteq\overline{\mathcal{A}}$. Therefore, $H_{\mathcal{D}_k}=H_{\mathcal{D}_k\cup\mathcal{R}_k}=1$. Otherwise, $H_{\mathcal{D}_k}=H_{\mathcal{D}_k\cup\mathcal{R}_k}=2$. The Equation (3c) follows immediately. Similarly, (3d) follows too.

Next, we consider (3b) for a given index set $\mathcal{K}$ and $i',j'\notin\mathcal{K}$. We have for any $\ell\in\mathcal{N}$,

$$H_{\ell,\mathcal{K}}=\begin{cases}1, & \text{if } \ell\in\overline{\mathcal{A}} \text{ and } \mathcal{K}\subseteq\overline{\mathcal{A}}\\ 2, & \text{if } \ell\notin\overline{\mathcal{A}} \text{ or } \mathcal{K}\nsubseteq\overline{\mathcal{A}}\end{cases}$$

Then, we have $H_{i',\mathcal{K}}+H_{j',\mathcal{K}}-H_{i',j',\mathcal{K}}-H_{\mathcal{K}}=$

$$\begin{cases}1, \text{ if } i',j'\notin\overline{\mathcal{A}} \text{ and } \emptyset\neq\mathcal{K}\subseteq\overline{\mathcal{A}}\\ 1, \text{ if } \{i',j'\}\cap\overline{\mathcal{A}}\neq\emptyset \text{ and } \mathcal{K}=\emptyset\\ 2, \text{ if } i',j'\notin\overline{\mathcal{A}} \text{ and } \mathcal{K}=\emptyset\\ 0, \text{ otherwise}\end{cases}$$

Therefore, (3b) are valid under this evaluation.

Note that when $\mathcal{A}\neq\emptyset$, the case for $i,j,\mathcal{A}$ coincides with the first case, otherwise coincides with the third case based on the choices for i and j. We can conclude that $H_{i,\mathcal{A}}+H_{j,\mathcal{A}}-H_{i,j,\mathcal{A}}-H_{\mathcal{A}}>0$, which is a strict inequality. □

From Theorem III.1, all the entropy variables can be substituted by the one with the corresponding closures. That is, the constraints in (3) is equivalent to the one that we substitute all the index sets with the corresponding closures. In this case, (3a), (3c) and (3d) will be trivial equations. The second type of implicit equations described in Theorem III.2 and the inequalities described in Theorem III.3 are disjoint and contains all the cases of (3b). After solving the equations, we are left the inequalities shown in Theorem III.3. With the equivalent relation shown in Theorem III.1, we can simplify the Initial System (3) as the following *Eliminated System* (8), where $\mathcal{CS}$ is the collection of all the closed sets:

$$\begin{aligned}\{H_{\overline{i,\mathcal{A}}}+H_{\overline{j,\mathcal{A}}}-H_{\overline{i,j,\mathcal{A}}}-H_{\mathcal{A}}\geq 0 \mid&\\ \text{for any } \mathcal{A}\in\mathcal{CS} \text{ and } i,j\notin\mathcal{A}\}&\end{aligned}\tag{8}$$

Lemma III.3. *For a fixed n, the number of closed sets is $\mathsf{num\_CS}$, where*

$$\mathsf{num\_CS}=\sum_{k=0}^{n}\binom{n}{k}2^{k(n-k)}(2^{n-k-1}-1)^{n-k}\sim O(2^{n^2-n}).$$

Proof. From (6) we know that a closed set consists of some full rows together with additional elements that do not form complete rows. Due to the column criterion (C), the possible number of full rows ranges from 0 to n, excluding $n-1$. In what follows, we count the number of closed sets according to the number of full rows they contain.

For a fixed integer k with $0\leq k\leq n$, there are $\binom{n}{k}$ ways to choose k full rows. Without loss of generality, we may consider the first k rows, which we denote by

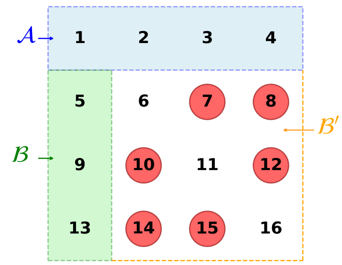


Fig. 2: Structure of a closed set.

$$\mathcal{A}=\{\mathcal{R}_t\cup\mathcal{D}_t \mid 1\leq t\leq k\}.$$

Let $N_{\mathcal{A}}$ be the number of closed index sets that contain $\mathcal{A}$ but contain no other full rows. Then the total number of closed sets does not exceed $\sum_{k=0}^{n}\binom{n}{k}N_{\mathcal{A}}$. Now, we give an upper bound for $N_{\mathcal{A}}$.

Denote by $\mathcal{I}=\{t\mid 1\leq t\leq k\}$ the set of indices of the k full rows, and let $\mathcal{I}'=\{t\mid k+1\leq t\leq n\}$ be its complement. We split the remaining $n-k$ rows into two blocks:

- the columns whose indices belong to $\mathcal{I}$, denoted by $\mathcal{B}$;
- the columns whose indices belong to $\mathcal{I}'$, denoted by $\mathcal{B}'$.

Figure 2 illustrates this partition for the case $n=4,\ k=1$. With this division we state two claims:

Claim 1. *There are exactly $N_{\mathcal{B}}=2^{k(n-k)}$ closed sets that contain $\mathcal{A}$ and are contained in $\mathcal{A}\cup\mathcal{B}$.*

Claim 2. *There are $N_{\mathcal{B}'}=(2^{n-k-1}-1)^{n-k}$ closed sets that contain $\mathcal{A}$ and are contained in $\mathcal{A}\cup\mathcal{B}'$.*

Consequently, the number of closed sets containing $\mathcal{A}$ equals $N_{\mathcal{A}}=N_{\mathcal{B}}N_{\mathcal{B}'}$. Hence the total number of closed sets is bounded above by

$$\sum_{k=0}^{n}\binom{n}{k}2^{k(n-k)}(2^{n-k-1}-1)^{n-k}.$$

Proof of Claim 1. Let $\mathcal{B}_1$ be an arbitrary subset of $\mathcal{B}$. Since $\mathcal{B}_1$ contains no diagonal elements, the row criterion (R) is never activated when computing the closure $\overline{\mathcal{A}\cup\mathcal{B}_1}$. If the column criterion (C) is triggered, any rows added must already lie in $\mathcal{A}$. Thus $\mathcal{A}\cup\mathcal{B}_1$ is always a closed set. Because $\mathcal{B}$ contains $k(n-k)$ elements, there are $2^{k(n-k)}$ possible choices for $\mathcal{B}_1$, proving the claim.

Proof of Claim 2. Let $\mathcal{B}_2$ be a subset of $\mathcal{B}'$. If we require $\mathcal{A}\cup\mathcal{B}_2$ to be closed and to contain no full rows with indices in $\mathcal{I}'$, two conditions must be satisfied:

1) $\mathcal{D}_t\nsubseteq\mathcal{B}_2$ for every $t\in\mathcal{I}'$,
2) each column of $\mathcal{B}_2$ contains at most $n-k-2$ elements.

Note that $\mathcal{B}'$ consists of $n-k$ columns, each containing $n-k$ elements. For a single column of $\mathcal{B}_2$, the number of admissible subsets satisfying the two conditions above is $2^{n-k-1}-1$. Hence, over all $n-k$ columns, we obtain $N_{\mathcal{B}'}=(2^{n-k-1}-1)^{n-k}$ choices for $\mathcal{B}_2$, which establishes the claim. □

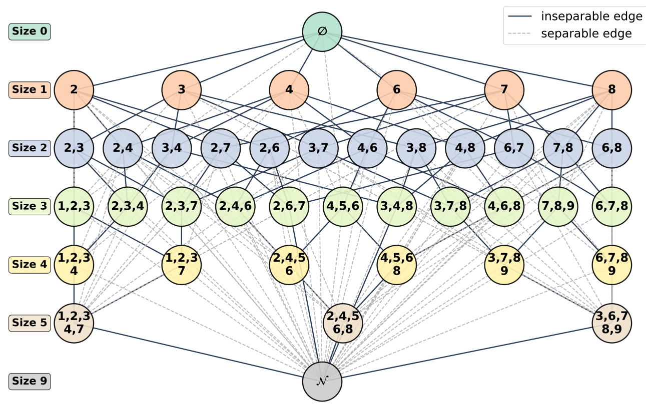


Fig. 3: Illustration of connections among entropy variable index sets in (9).

The number of entropy variables in (8) coincides with the number of closures in $\mathcal{N}$, which is shown in Lemma III.3. This greatly simplifies (3) on the number of entropy variables. Since there are at most n^2 choices for i and j in (8), the number of constraints there can be bounded by $\textsf{num\_ES} = \textsf{num\_CS} \cdot \binom{n^2}{2} \sim O(2^{n^2-n}n^4)$. Obviously, (8) still contains large amount of redundant inequalities. In the next subsection, we focus on identify all the redundant constraints in (8) and establish an equivalent minimal set.

B. Redundant inequalities

System (8) can be reformulated as (9) in terms of number of entropy variables, where $\mathcal{A}$ ranges over all closed sets, and $i, j \notin \mathcal{A}$ satisfy $\overline{\{i,\mathcal{A}\}} \not\subseteq \overline{\{j,\mathcal{A}\}}$ and $\overline{\{j,\mathcal{A}\}} \not\subseteq \overline{\{i,\mathcal{A}\}}$:

$$\begin{cases} H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0 & \text{(9a)} \\ H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0 & \text{(9b)} \end{cases}$$

Example III.5 shows three classical types of redundant inequalities.

Example III.5 (Redundant Inequalities)**.** *In* (9)*, we have:*

1) *the inequality* $H_{7,8,9} + H_2 - H_{\mathcal{N}} - H_{\emptyset} \geq 0$ *is redundant due to the existence of* $H_2 + H_8 - H_{2,4,5,6,8} - H_{\emptyset} \geq 0$ *and* $H_{2,4,5,6,8} + H_{7,8,9} - H_{\mathcal{N}} - H_8 \geq 0$.
2) *the inequality* $H_{1,2,3,4} - H_{2,4} \geq 0$ *is redundant due to the existence of* $H_{1,2,3,4} - H_{2,3,4} \geq 0$ *and* $H_{2,3,4} - H_{2,4} \geq 0$.
3) *the inequality* $H_2 - H_{\emptyset} \geq 0$ *is redundant due to the existence of* $H_2 + H_4 - H_{2,4} - H_{\emptyset} \geq 0$ *and* $H_{2,4} - H_4 \geq 0$.

Note that the index sets of entropy variables in each inequality exhibit close relationships that can be represented as a graph structure (Fig. 3). We treat each closed set as a *node*. An *edge* $\mathcal{A} \to \mathcal{B}$ exists between nodes $\mathcal{A}$ and $\mathcal{B}$ if and only if $\mathcal{B} = \overline{\mathcal{A} \cup \{i\}}$ for some element i. It is called *inseparable* if it constitutes the unique directed path from $\mathcal{A}$ to $\mathcal{B}$. Otherwise, it is called *separable*.

Fig. 3 depicts the connections among entropy variable index sets in (9), which is a reformulation of (8). Note that among the four nodes in (9a), the node $\overline{\{i,j,\mathcal{A}\}}$ is completely determined by the other three: $\mathcal{A}$, $\overline{\{i,\mathcal{A}\}}$, and $\overline{\{j,\mathcal{A}\}}$. Similarly, the edges $\overline{\{i,\mathcal{A}\}} \to \overline{\{i,j,\mathcal{A}\}}$ and $\overline{\{j,\mathcal{A}\}} \to \overline{\{i,j,\mathcal{A}\}}$ can be deduced from the two edges $\mathcal{A} \to \overline{\{i,\mathcal{A}\}}$ and $\mathcal{A} \to \overline{\{j,\mathcal{A}\}}$. Consequently, Fig. 3 displays only these two fundamental edges with respect to (9a), rather than all four. Dashed lines represent separable edges, while solid lines denote inseparable ones. Equation (9b) consists of two nodes connected by a single edge $\mathcal{A} \to \overline{\{i,\mathcal{A}\}}$, corresponding to an individual edge in Fig. 3. For each inequality, we designate the node with the fewest elements as the *initial node*.

Consider the three redundant inequalities from Example III.5. In Fig. 3, we observe that the edge $\emptyset \to \{7,8,9\} = \overline{\{9\}}$ in the first inequality is separable, as an alternative directed path $\emptyset \to \{7\} \to \{7,8\} \to \overline{\{7,8,9\}}$ exists. Similarly, the edge $\{2,4\} \to \{1,2,3,4\} = \overline{\{1,2,4\}}$ in the second inequality due to the existence of another path $\{2,4\} \to \{2,3,4\} \to \{1,2,3,4\}$. The third inequality contains the inseparable edge $\emptyset \to \{2\}$, but notably, its initial node $\emptyset$ also gives rise to another inseparable edge $\emptyset \to \{4\}$.

In fact, these observations admit generalization, providing criteria for identifying redundant inequalities within (9), as established in Theorem III.4.

Theorem III.4 (Redundancy Identification)**.** *Based on the edge separability originating from initial nodes $\mathcal{A}$, we have*

1) *Inequality* (9a) $H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ *is redundant when* $\mathcal{A} \to \overline{i,\mathcal{A}}$ *or* $\mathcal{A} \to \overline{j,\mathcal{A}}$ *is separable.*
2) *Inequality* (9b) $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ *is redundant when* $\mathcal{A} \to \overline{i,\mathcal{A}}$ *is separable.*
3) *When* $\mathcal{A} \to \overline{i,\mathcal{A}}$ *is inseparable,* (9b) $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ *is redundant when there exists another inseparable edge starting from* $\mathcal{A}$.

Proof. Without loss of generality, suppose that $\mathcal{A} \to \overline{i,\mathcal{A}}$ is separable. Then, there exists an inseparable edge $\mathcal{A} \to \overline{k,\mathcal{A}}$ for some $k \in \mathcal{N} \setminus \mathcal{A}$ such that $\overline{k,\mathcal{A}} \subsetneq \overline{i,\mathcal{A}}$. Note that $\overline{i,k,\mathcal{A}} = \overline{i,\mathcal{A}}$, $\overline{i,j,k,\mathcal{A}} = \overline{i,j,\mathcal{A}}$. Adding the inequalities $H_{\overline{k,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{k,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ and $H_{\overline{j,k,\mathcal{A}}} + H_{\overline{i,k,\mathcal{A}}} - H_{\overline{i,j,k,\mathcal{A}}} - H_{\overline{k,\mathcal{A}}} \geq 0$, we will obtain $H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$. Therefore, the latter is redundant. The first statement is proved.

When $\mathcal{A} \to \overline{i,\mathcal{A}}$ is separable, there exists an inseparable edge $\mathcal{A} \to \overline{k,\mathcal{A}}$ for some $k \in \mathcal{N} \setminus \mathcal{A}$ such that $\overline{k,\mathcal{A}} \subsetneq \overline{i,\mathcal{A}}$. Note that the inequality $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ is actually degenerated from $H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ for some $j \in \mathcal{N} \setminus \mathcal{A}$ and $\overline{i,\mathcal{A}} \subseteq \overline{j,\mathcal{A}}$. We have $\overline{i,\mathcal{A}} = \overline{i,k,\mathcal{A}} \subseteq \overline{j,k,\mathcal{A}}$. Therefore, $H_{\overline{k,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ and $H_{\overline{i,\mathcal{A}}} - H_{\overline{k,\mathcal{A}}} \geq 0$ are both contained in the type (9b). Adding them together, we will obtain $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$, which shows the redundancy. The second statement is proved.

Suppose that there is another inseparable edge $\mathcal{A} \to \overline{k,\mathcal{A}}$ for some $k \neq i$. Note that the inequality $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ is actually degenerated from $H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ for some $j \in \mathcal{N} \setminus \mathcal{A}$ and $\overline{i,\mathcal{A}} \subseteq \overline{j,\mathcal{A}}$. Since $\overline{i,k,\mathcal{A}} \subseteq \overline{j,k,\mathcal{A}}$, $H_{\overline{i,k,\mathcal{A}}} - H_{\overline{k,\mathcal{A}}} \geq 0$ is contained in the type (9b). Added by the inequality $H_{\overline{i,\mathcal{A}}} + H_{\overline{k,\mathcal{A}}} - H_{\overline{i,k,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$, we will obtain $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ which shows the redundancy. The last statement is proved. ☐

Theorem III.4 provides sufficient conditions for identifying redundant inequalities. It asserts that an inequality is certainly

TABLE I: Comparison between the Initial, Eliminated and Final System

n	Variable		Inequalities		
	Initial	Final	Initial	Eliminated	Final
2	16	2	28	1	1
3	512	40	4,617	414	89
4	65,536	3,362	1,966,096	123,446	40,391
5	33,554,432	969,376	2,516,582,425	94,163,710	39,000,979

redundant if a separable edge originates from its initial node. Additionally, for inequalities in (9b), redundancy also occurs when the initial node has two or more outgoing edges. Removing the redundant ones, we obtain the simplified *Final System*:

$$H_{\mathcal{P}} + H_{\mathcal{Q}} - H_{\overline{\mathcal{P} \cup \mathcal{Q}}} - H_{\mathcal{A}} \geq 0, \tag{10}$$

where $\mathcal{A}$ is an arbitrary closed set. The edges $\mathcal{A} \rightarrow \mathcal{P}$ and $\mathcal{A} \rightarrow \mathcal{Q}$ range over:

- Any two distinct inseparable edges originating from $\mathcal{A}$, when $\mathcal{A}$ has multiple inseparable edges;
- The same inseparable edge taken twice, when $\mathcal{A}$ has only one inseparable edge. That is, $\mathcal{P} = \mathcal{Q}$.

Note that an inequality in (10) is redundant if and only if it can be expressed as a nonnegative combination of other inequalities in the system. From such a combination, one can deduce the existence of an alternative directed path from the initial node $\mathcal{A}$ to either $\overline{\{i, \mathcal{A}\}}$ or $\overline{\{j, \mathcal{A}\}}$. Graphically, this implies that at least one of the corresponding edges, $\mathcal{A} \rightarrow \overline{\{i, \mathcal{A}\}}$ or $\mathcal{A} \rightarrow \overline{\{j, \mathcal{A}\}}$, must be *separable*. This establishes a direct link between redundancy in (10) and edge separability in its graphical representation. Therefore, the conditions given in Theorem III.4 for identifying separable edges are both sufficient and necessary for detecting redundant inequalities. Consequently, the system (10) is guaranteed to be *minimal* (i.e., free of any redundant constraints). Finally, Theorem III.5 summarizes the complete criteria for constructing this equivalent minimal system from the Initial System.

Theorem III.5 (Minimal System)**.** *Based on the edge separability originating from initial nodes $\mathcal{A}$, we have*

1) *Inequality* (9a) $H_{\overline{i,\mathcal{A}}} + H_{\overline{j,\mathcal{A}}} - H_{\overline{i,j,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ *is irredundant if and only if both edges* $\mathcal{A} \rightarrow \overline{i, \mathcal{A}}$ *and* $\mathcal{A} \rightarrow \overline{j, \mathcal{A}}$ *are inseparable.*
2) *Inequality* (9b) $H_{\overline{i,\mathcal{A}}} - H_{\mathcal{A}} \geq 0$ *is irredundant if and only if the edge* $\mathcal{A} \rightarrow \overline{i, \mathcal{A}}$ *is the only inseparable edge originating from* $\mathcal{A}$*.*

Fig. 3 clearly demonstrates that applying Theorem III.4 to remove redundant inequalities substantially reduces the number of constraints. This is demonstrated in Table I. Table I compares the counts of variables and constraints across three systems, the Initial System, the Eliminated System, and the Final System for $n \in \{2, 3, 4, 5\}$.

IV. Conclusion

In this paper, we establish an equivalent minimal set for the constraint region of the $(n, n-1, n-1)$ regenerating code problem via an algebraic approach. We first extract implicit equations to reveal equivalence relations among entropy variables, thereby reducing dimensionality. Then, we provide necessary and sufficient conditions for identifying redundant inequalities, leading to the final minimal set. Our method is general and applicable for any parameter n. Although the problem involves $N = n^2$ random variables, resulting in $2^{n^2} - 1$ entropy variables, the algebraic framework developed here offers a novel perspective for proving information inequalities in more general symmetric settings with arbitrary N.

References

[1] L. Csirmaz (2016), A MINimal Information Theoretic Inequality Prover (Minitip). [Online]. Available: https://github.com/lcsirmaz/minitip

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

[3] W. Chen, C. Tian, "A New Approach to Compute Information Theoretic Outer Bounds and Its Application to Regenerating Codes". arXiv:2205.01612, 2022.

[4] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inform. Theory*, vol. 56, pp. 4539-4551, Sept 2010.

[5] L. Guo, R. W. Yeung and X. -S. Gao, "Proving Information Inequalities and Identities with Symbolic Computation," in IEEE Transactions on Information Theory, doi: 10.1109/TIT.2023.3263178.

[6] L. Guo, R. W. Yeung and X. -S. Gao, "Proving Information Inequalities by Gaussian Elimination," 2024 IEEE International Symposium on Information Theory (ISIT), Athens, Greece, 2024, pp. 3172-3177.

[7] L. Guo, R. W. Yeung and X. -S. Gao, "Proving Information Inequalities by Gaussian Elimination," arXiv preprint, arXiv:2401.14916, 2024.

[8] T. Guo, R. Zhou, and C. Tian, "New results on the storage-retrieval tradeoff in private information retrieval systems," IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 403–414, 2021.

[9] T. S. Han, "A uniqueness of Shannon's information distance and related non-negativity problems," *J. Comb., Info., and Syst. Sci.*, 6: 320-321, 1981.

[10] S.-W. Ho, L. Ling, C. W. Tan, and R. W. Yeung, "Proving and disproving information inequalities: Theory and scalable algorithms," *IEEE Trans. Inf. Theory*, vol. 66, no. 9, pp. 5522-536, Sep. 2020.

[11] C. T. Li (2020), Python Symbolic Information Theoretic Inequality Prover (psitip). [Online]. Available: https://github.com/cheuktingli/

[12] K. Lee, M. Lam, R. Pedarsani, D. Papailiopoulos, and K. Ramchandran, "Speeding up distributed machine learning using codes," IEEE Transactions on Information Theory, vol. 64, no. 3, pp. 1514–1529, 2017.

[13] C. Li, S. Weber, and J. M. Walsh, "Multilevel diversity coding systems: Rate regions, codes, computation, & forbidden minors," IEEE Trans. on Information Theory, vol. 63, no. 1, pp. 230–251, Jan. 2017.

[14] Z. Li and H. Sun, "Conditional disclosure of secrets: A noise and signal alignment approach," arXiv preprint arXiv:2002.05691, 2020.

[15] M. A. Maddah-Ali and U. Niesen, "Fundamental limits of caching," IEEE Trans. on Information Theory, vol. 60, no. 5, pp. 2856–2867, May 2014.

[16] R. Pulikkoonattu and S. Diggavi (2006), Xitip, ITIP-Based C Program Software Package. [Online]. Available: http://xitip.epfl.ch

[17] N. Rathenakar, S. Diggavi, T. Gläle, E. Perron, R. Pulikkoonattu, R. W. Yeung, and Y.-O. Yan (2020), Online X-Information Theoretic Inequalities Prover (oXitip). [Online]. Available: http://www.oxitip.com

[18] 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 Trans. Inf. Theory, vol. 57, no. 8, pp. 5227-5239, Aug. 2011.

[19] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379–423, 623–656, Jul. Oct. 1948.

[20] B. Sasidharan, N. Prakash, M. N. Krishnan, M. Vajha, K. Senthoor, P. V. Kumar, "Outer bounds on the storage-repair bandwidth trade-off of exact-repair regenerating codes," *International Journal of Information and Coding Theory*, vol. 3, no. 4, pp: 255-298, 2016.

[21] S. Shao, J. G/'omez-Vilardeb/'o, K. Zhang, and C. Tian, "On the fundamental limits of coded caching systems with restricted demand types," IEEE Transactions on Communications, vol. 69, no. 2, pp. 863–873, 2020.

[22] H. Sun and S. A. Jafar, “The capacity of private information retrieval,” IEEE Transactions on Information Theory, vol. 63, no. 7, pp. 4075–4088, Jul. 2017.

[23] N. B. Shah, K. V. Rashmi, P. V. Kumar and K. Ramchandran, “Distributed storage codes with repair-by-transfer and non-achievability of interior points on the storage-bandwidth tradeoff,” IEEE Trans. Inf. Theory, vol. 58, no. 3, pp. 1837-1852, Mar. 2012.

[24] N. B. Shah, K. V. Rashmi, P. V. Kumar and K. Ramchandran, “Interference alignment in regenerating codes for distributed storage: necessity and code constructions,” IEEE Trans. Inf. Theory, vol. 58, no. 4, pp. 2134-2158, Apr. 2012

[25] C. Tian, “Characterizing the rate region of the (4, 3, 3) exact-repair regenerating codes,” *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 5, pp: 967-975, 2014.

[26] C. Tian, “A note on the rate region of exact-repair regenerating codes”. arXiv:1503.00011, Mar. 2015.

[27] Tian, “Symmetry, outer bounds, and code constructions: A computer-aided investigation on the fundamental limits of caching,” Entropy, vol. 20, no. 8, p. 603, 2018.

[28] C. Tian, “On the storage cost of private information retrieval,” IEEE Transactions on Information Theory, vol. 66, no. 12, pp. 7539–7549, 2020.

[29] C. Tian and T. Liu, “Multilevel diversity coding with regeneration,” IEEE Trans. on Information Theory, vol. 62, no. 9, pp. 4833–4847, Sep. 2016.

[30] C. Tian, J. Plank, B. Hurst, and R. Zhou, “Computational techniques for investigating information theoretic limits of information systems,” Information, vol. 12, no. 2, p. 82, 2021.

[31] C. Tian, H. Sun, and J. Chen, “A Shannon-theoretic approach to the storage-retrieval tradeoff in PIR systems,” in 2018 IEEE International Symposium on Information Theory (ISIT), 2018, pp. 1904–1908.

[32] R. W. Yeung, “A framework for linear information inequalities,” *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1924-1934, Nov. 1997.

[33] R. W. Yeung, *Information Theory and Network Coding*. New York, NY, USA: Springer, 2008.

[34] R. W. Yeung and C. T. Li, “Machine-Proving of Entropy Inequalities,” IEEE BITS the Information Theory Magazine, vol. 1, no. 1, pp. 12-22, 1 Sept. 2021.

[35] R. W. Yeung and Y.-O. Yan (1996), Information Theoretic Inequality Prover (ITIP), MATLAB Program Software Package. [Online]. Available: http://home.ie.cuhk.edu.hk/ ITIP

[36] K. Zhang and C. Tian, “On the symmetry reduction of information inequalities,” IEEE Transactions on Communications, vol. 66, no. 6, pp. 2396–2408, Jun. 2018.

[37] Z. Zhang and R. W. Yeung, “On characterization of entropy function via information inequalities,” *IEEE Trans. Inf. Theory*, vol. 44, pp. 1440-1452, July 1998.