



HAL
open science

How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma

Emirhan Gürpınar, Andrei Romashchenko

► **To cite this version:**

Emirhan Gürpınar, Andrei Romashchenko. How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma. ISIT 2019 - IEEE 1st International Symposium on Information Theory, Jul 2019, Paris, France. pp.1377-1381, 10.1109/ISIT.2019.8849309 . lirmm-01990325

HAL Id: lirmm-01990325

<https://hal-lirmm.ccsd.cnrs.fr/lirmm-01990325>

Submitted on 29 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

How to Use Undiscovered Information Inequalities: Direct Applications of the Copy Lemma

Emirhan Gürpınar
ENS de Lyon, France
Email: emirhan.gurpinar@ens-lyon.fr

Andrei Romashchenko
LIRMM, University of Montpellier, CNRS, France
on leave from IITP RAS
Email: andrei.romashchenko@lirmm.fr

Abstract—We discuss linear programming techniques that help to deduce corollaries of non classic inequalities for Shannon’s entropy. We focus on direct applications of the copy lemma. These applications involve implicitly some (known or unknown) non-classic universal inequalities for Shannon’s entropy, though we do not derive these inequalities explicitly. To reduce the computational complexity of these problems, we extensively use symmetry considerations.

We present two examples of usage of these techniques: we provide a reduced size formal inference of the best known bound for the Ingleton score (originally proven by Dougherty *et al.* with explicitly derived non Shannon type inequalities), and improve the lower bound for the optimal information ratio of the secret sharing scheme for an access structure based on the Vámos matroid.

I. INTRODUCTION

We can associate with an n -tuple of jointly distributed random variables its *entropy profile* that consists of the $2^n - 1$ values of Shannon’s entropy of each sub-tuple of the given tuple. We say that a point in $\mathbb{R}^{2^n - 1}$ is *entropic* if it represents the entropy profile of some distribution. The entropic points satisfy different information inequalities — the constraints that characterize the range of admissible entropies for jointly distributed variables. The most known and well understood information inequalities are so-called *Shannon-type inequalities* that are defined as linear combinations of several instances of the *basic inequality* $I(A : B|C) \geq 0$, where A, B, C are any subsets (possibly empty) of random variables.

In 1998 Z. Zhang and R.W. Yeung discovered the first example of an (unconditional) non Shannon-type information inequality, which was a linear inequality for entropies of a quadruple of random variables that cannot be represented as a combination of basic inequalities [4]. Now many other non Shannon-type information are known (including several infinite families of non Shannon-type information inequality), see, e.g., [6], [11], [17].

The works on non-Shannon type information inequalities are focused on the following fundamental question: can we prove some particular property for Shannon’s entropy (usually expressed as an equality or an inequality), assuming some specific constraints (which are also given as equalities and inequalities for Shannon’s entropy, including Shannon type and non Shannon type universal information inequalities). Not surprisingly, these arguments typically use the technique of linear programming: at the first stage, to derive new informa-

tion inequalities (and to prove that they are indeed new) and then, at the second stage, to apply the derived inequalities to some specific problem (e.g., in secret sharing, network coding, and so on). Many applications of this type involve heavy computations: the number of information inequalities in n random variables grows exponentially with n . It seems that in several problems the progress is stopped since the computational complexity of the corresponding linear programs is too high for the modern computers. So the question arises: can we reduce the computational complexity of the relevant problems of linear programming? In this paper we show that in some cases new progress can be made with a reasonable combination of previously known techniques.

Recently Farràs *et al.*, [26], observed that the two stages of the scheme mentioned above (deriving new information inequalities and applying them) can be merged in a unique problem of linear programming: in a specific application of information inequalities, instead of enumerating explicitly all known non-Shannon information inequalities, we can include in a linear program the *constraints* from which those inequalities are (or can be) derived. The *constraints* used in [26] were instances of the Ahlswede–Körner lemma, [7]. As a tool of inference of non Shannon type inequalities, the Ahlswede–Körner lemma is essentially equivalent to the Copy Lemma from [17] “cloning” one single random variable, see [20]. In this paper we use a technique similar to [26], but employing the *constraints* obtained from the Copy Lemma. This permits us to extend the technique: we apply the Copy Lemma to make “clones” of pairs of jointly distributed random variables (instead of copies of individual random variables used in [26]).

To reduce the dimension of the corresponding problem of linear programming, we use symmetries of the problems under consideration. Our usage of symmetries is similar to the ideas proposed in [24], where the authors suggested to use symmetries to reduce the complexity of computing the outer bounds on network coding capacity. For a study of the general problem of Shannon and non Shannon type inequalities for symmetric entropy points we refer the reader to [25].

To illustrate the power of this technique, we discuss two examples. In the first one we give a formal inference of the best known bound for the Ingleton score (originally proven in [17]), with only four auxiliary random variable and three applications of the Copy Lemma. The obtained computer-assistant proof is very fast, and the “formally checkable”

version of the proof can be reduced to a combination of 167 equalities and inequalities with rational coefficients. In our second example we improve the known lower bound for the optimal information ratio of the secret sharing schemes associated with the Vámos matroid (for the *access structure* denoted V_0).

Though the techniques used in this paper are rather simple, their combination proves to be fruitful. We believe that this approach can be used in other problems of information theory.

Notation:

We denote $[n] = \{1, \dots, n\}$. Given a tuple of jointly distributed random variable (X_1, \dots, X_n) and a set of indices $V = \{i_1, \dots, i_k\} \subset [n]$ we denote by $H(X_V)$ the Shannon entropy $H(X_{i_1}, \dots, X_{i_k})$. We fix an arbitrary order on non-empty subsets of the set of indices $[n]$ and assign to each distribution $\mathbf{X} = (X_1, \dots, X_n)$ its *entropy profile*, i.e., the vector of $2^n - 1$ entropies $H(X_V)$ (for all non-empty $V \subset [n]$).

We say that a point in the space $V_n = \mathbb{R}^{2^n - 1}$ is *entropic* if it represents the entropy profile of some distribution. Following [4], we denote by Γ_n^* the set of all entropic points. We denote by $\bar{\Gamma}_n^*$ the topological close Γ_n^* ; its elements are called *almost entropic*.

We use the standard abbreviations for linear combinations of coordinates in the entropy profile:

$$\begin{aligned} H(X_V|X_W) &:= H(X_{V \cup W}) - H(X_W) \\ I(X_V; X_W) &:= H(X_V) + H(X_W) - H(X_{V \cup W}) \\ I(X_V; X_W|X_U) &:= H(X_{U \cup V}) + H(X_{U \cup W}) \\ &\quad - H(X_{U \cup V \cup W}) - H(X_U). \end{aligned}$$

We extend this notation to almost entropic points.

II. COPY LEMMA

The following lemma was used (somewhat implicitly) in the very first proof of a non Shannon type inequality in [4], see also [18, Lemma 14.8]. The general version of this lemma appeared in [9] and [17]. In [17] it was presented explicitly, with a complete and detailed proof.

Lemma 1 (Copy Lemma): For every tuples of jointly distributed random variables (X, Y, Z) there exists a distribution (A, B, C, C') such that

- the distribution (A, B, C) coincides with the distribution of (X, Y, Z) ; the distribution of (A, C') coincides with the distribution of (X, Z) , and
- $I(C'; B, C|A) = 0$.

In what follows we abuse the notation and identify (A, B, C) with (X, Y, Z) . That is, we say that the initial distribution (X, Y, Z) can be extended¹ to the distribution (X, Y, Z, Z') , where (X, Z) and (X, Z') have isomorphic joint distributions, and $I(Z'; Y, Z|X) = 0$. Following [17], we say that Z' is a Y -copy of Z over X , denoted by

$$Z' := Y\text{-copy}(Z|X).$$

¹Formally speaking, such an “extension” may require a subdivision of the initial probabilistic space, so technically (A, B, C) and (X, Y, Z) are defined on different probabilistic spaces.

Note that Lemma 1 remains valid if X, Y, Z are not individual variables but tuples of variables.

F. Matúš and L. Csirmaz proposed several extensions and generalizations of the Copy Lemma (*polymatroid convolution*, *book extension*, *maximum entropy extension*, see, e.g., [12], [22], [23]). However, to the best of our knowledge, the “classic” version of the Copy Lemma is strong enough for all known proofs of non Shannon type inequalities

All known proofs of (unconditional) non Shannon type information inequalities can be presented in the following style: we start with a distribution (X_1, \dots, X_n) ; using the Copy Lemma we supplement to this distribution several new variable (Y_1, \dots, Y_k) ; then we enumerate the basic Shannon’s inequalities for the joint distribution $(X_1, \dots, X_n, Y_1, \dots, Y_k)$ and show that a combination of these inequalities (together with the constraints from the Copy Lemma) gives the desired new inequality for (X_1, \dots, X_n) (the entropy terms with new variable Y_j should be canceled). We refer the reader to [17] for many instances of this argument.

In what follows we use a very similar scheme of proof. The difference is that we superimpose constraints (equalities for the coordinates of the entropy profile of (X_1, \dots, X_n)) that are specific for the given specific problem. That is, in each application we prove a *conditional* non Shannon type inequality (which is valid only assuming some linear constraints for the entropy quantities). Each of these arguments can be theoretically translated in a more conventional style: we can at first prove some new unconditional non Shannon type inequalities, and then combine them with the given constraints and deduce the desired corollary. However, we do not need to reveal and formulate explicitly these unconditional inequalities hidden behind the proof.

III. SYMMETRIES

In this section we discuss a simple formalism of symmetry considerations that helps to reduce the dimension of a linear programs associated with problems concerning information inequalities (assuming that the problem has a particular symmetric structure). A similar formalism (action of permutations on multidimensional distributions and their entropy profiles, information inequalities for distributions with symmetric entropy profiles) was systematically studied in [25].

Let $\mathbf{X}^{(n)} = (X_1, \dots, X_n)$ be a joint distribution of n random variables. We denote by $\vec{H}(\mathbf{X})$ its *entropy profile*. Let $\pi : [n] \rightarrow [n]$ be a permutation of indices (an n -permutation). This permutation induces a natural transformation of the distribution \mathbf{X} ,

$$\mathbf{X} = (X_1, \dots, X_n) \xrightarrow{\pi} \hat{\mathbf{X}} := (X_{\pi(1)}, \dots, X_{\pi(n)}),$$

and therefore a transformation of the entropy profile

$$\vec{H}(\mathbf{X}) \xrightarrow{\pi} \vec{H}(\hat{\mathbf{X}}).$$

Example 1: If π is the transposition of indices 1 and 2, then the mapping defined above exchanges the entropy

values $H(X_1)$ and $H(X_2)$, the values $H(X_1, X_3)$ and $H(X_2, X_3)$, etc., and does not change the values $H(X_1, X_2)$, $H(X_1, X_2, X_3)$, etc.

Thus, every permutation of indices π induces a transformation of the set of all entropic points Γ_n^* . This transformation of the entropic points can be naturally extended to a linear transformation of the entire space V_n (defined by a suitable permutation of the coordinate axis). In what follows we denote this transformation by T_π . (Note that π is a permutation on n elements, while T_π is a transformation of the space of dimension $2^n - 1$.) In the usual algebraic terminology, we can say that we defined a representation of the symmetric group (the group of all n -permutations) by linear transformations of the set V_n .

We say that a point $\mathbf{x} \in V_n$ is π -invariant if $T_\pi(\mathbf{x}) = \mathbf{x}$. Similarly, we say that a set of points $S \subset V_n$ is π -invariant, if $T_\pi(\mathbf{x})$ is a permutation of points in S . For a subgroup G of n -permutations, we say that a point (or a subset) in V_n is G -invariant, if it is π -invariant for every $\pi \in G$.

We denote the set of G -invariant points in V_n by $\text{Inv}(G)$. In what follows we typically study linear and affine spaces that are G -invariant for some specific group of permutations G . Note that every G -invariant linear space in V_n contains the set $\text{Inv}(G)$ as a subspace.

The sets of all entropic and all almost entropic points (Γ_n^* and $\bar{\Gamma}_n^*$ respectively) are obviously π -invariant for every n -permutation π . For every group G of n -permutations, the intersections of Γ_n^* or $\bar{\Gamma}_n^*$ with any G -invariant set gives another G -invariant set. In what follows we discuss several simple examples of this type.

Example 2: Let L_{ent} be the set of points in Γ_4^* such that

$$\begin{cases} H(X_1|X_2, X_3) = 0, & H(X_1|X_2, X_4) = 0, \\ H(X_2|X_1, X_3) = 0, & H(X_2|X_1, X_4) = 0, \\ H(X_1, X_2, X_3, X_4) = 1. \end{cases}$$

Since L_{ent} is defined by affine conditions, it can be represented as the intersection of Γ_4^* with an affine subspace L (of co-dimension 5) in the entire space $V_4 = \mathbb{R}^{15}$. It is easy to see that this subspace L is invariant with respect to transpositions π_{12} and π_{34} (π_{12} exchanges the indices 1 and 2, and π_{12} exchanges the indices 3 and 4). Therefore, this subspace is G -invariant, where G is the subgroup of the symmetric group generated by the transpositions π_{12} and π_{34} (this subgroup consists of four permutations).

We say that a linear function

$$\mathcal{L} : \mathbb{R}^{2^n - 1} \rightarrow \mathbb{R}$$

is π -invariant, if $\mathcal{L}(T_\pi(\mathbf{x})) = \mathcal{L}(\mathbf{x})$ for all $\mathbf{x} \in \mathbb{R}^{2^n - 1}$. Similarly, for a subgroup of n -permutations G , we say that a linear function is G -invariant, if it is π -invariant for every $\pi \in G$.

Example 3: Ingleton's quantity $\text{Ing}(X_1, X_2, X_3, X_4)$ defined as

$$I(X_1; X_2|X_3) + I(X_1; X_2|X_4) + I(X_3 : X_4) - I(X_1; X_2)$$

can be extended to a linear function on the space $V_4 = \mathbb{R}^{15}$. This function is invariant with respect to the transposition of indices 1 and 2, to the transposition of indices 3 and 4, and with respect to the group (of size four) generated by these two transpositions.

Claim 1: Let $G = \{\pi_1, \dots, \pi_k\}$ be a subgroup of n -permutations, and let \mathbf{x} be a point in V_n . Then the center of mass of the points

$$T_{\pi_1}(\mathbf{x}), \dots, T_{\pi_k}(\mathbf{x}) \quad (1)$$

is G -invariant.

Proof: It is easy to see that the set of points (1) is π -invariant for each $\pi \in G$. Therefore, the center of mass of this set is also G -invariant. ■

Lemma 2: Let $G = \{\pi_1, \dots, \pi_k\}$ be a subgroup of n -permutations, L be a G -invariant convex set in V_n , and $\mathcal{F} : V_n \rightarrow \mathbb{R}$ be a G -invariant linear function. Then

$$\inf_{\mathbf{x} \in L} \mathcal{F}(\mathbf{x}) = \inf_{\mathbf{y} \in L \cap \text{Inv}(G)} \mathcal{F}(\mathbf{y}).$$

Proof: It is enough to prove that for every $\mathbf{x} \in L$ there exists a $\mathbf{y} \in L \cap \text{Inv}(G)$ such that

$$\mathcal{F}(\mathbf{x}) = \mathcal{F}(\mathbf{y}).$$

To this end we take the points

$$T_{\pi_1}(\mathbf{x}), \dots, T_{\pi_k}(\mathbf{x})$$

and define \mathbf{y} as the center of mass of these k points. Since L is G -invariant, each point $T_{\pi_i}(\mathbf{x})$ belongs to L . From convexity of L it follows that \mathbf{y} also belongs to L , and Claim 1 implies that \mathbf{y} belongs to $\text{Inv}(G)$. Thus, the constructed point belongs to $L \cap \text{Inv}(G)$.

On the other hand, from G -invariance of \mathcal{F} it follows that

$$\mathcal{F}(T_{\pi_1}(\mathbf{x})) = \dots = \mathcal{F}(T_{\pi_k}(\mathbf{x})). \quad (2)$$

Since \mathcal{F} is linear, we conclude that \mathcal{F} at the center of mass of $T_{\pi_i}(\mathbf{x})$ is equal to the same values as the points in (2), and the lemma is proven. ■

Example 4: Assume we are looking for the minimum of $\text{Ing}(X_1, X_2, X_3, X_4)$ (see Example 3) on the set of *almost entropic* points (points in $\bar{\Gamma}_4^*$) that satisfy the linear constraints

$$\begin{cases} H(X_1|X_2, X_3) = 0, & H(X_1|X_2, X_4) = 0, \\ H(X_2|X_1, X_3) = 0, & H(X_2|X_1, X_4) = 0, \\ H(X_1, X_2, X_3, X_4) = 1. \end{cases}$$

(see Example 2). We define G as the group of permutations generated by two transpositions π_{12} and π_{34} that exchange the indices (1, 2) and (3, 4) respectively.

We claim that the required extremal value of $\text{Ing}(X_1, X_2, X_3, X_4)$ is achieved at some G -invariant point. Indeed, the given constraints define in V_4 a G -invariant affine subspace. The intersection of this subspace with the convex cone $\bar{\Gamma}_4^*$ is a G -invariant convex set. On the other hand, Ingleton's quantity $\text{Ing}(X_1, X_2, X_3, X_4)$ is a G -invariant linear function. Therefore, we can apply Lemma 2 and conclude that desired extremum is achieved at some point in $\text{Inv}(G)$.

IV. THE STANDARD BENCHMARK: BOUNDS FOR INGLETON'S QUANTITY

It is widely believed that one of the most interesting questions on the structure of $\bar{\Gamma}_4^*$ is the question on the Ingleton's quantity: what is the worst possible violation of Ingleton's inequality

$$\text{Ing}(A, B, C, D) \geq 0. \quad (3)$$

This inequality is true for *linearly representable* entropic points but for some other entropic points it is violated (see [5]). The question is how far below 0 can go the *Ingleton score*

$$\frac{\text{Ing}(A, B, C, D)}{H(A, B, C, D)}$$

(here we use the terminology from [17]). From the Shannon type inequalities it follows only that this score is greater than $-1/4$. The first non Shannon type inequality from [4] implies that this score is greater than $-1/6$. The best bound was discovered by Dougherty *et al.*:

Theorem 1 (originally proven in [17]): For every quadruple of jointly distributed random variables (A, B, C, D)

$$\frac{\text{Ing}(A, B, C, D)}{H(A, B, C, D)} \geq -3/19.$$

We show that this bound can be derived with only three applications of the Copy Lemma (with four new variables), with the help of symmetry considerations from the previous section. This approach gives a pretty simple way to confirm the ratio $-3/19 \approx -0.15789$ with the help of a computer, and provides a reasonably short “formally checkable” proof (a linear combination of 167 simple equalities and inequalities with rational coefficients, see Appendix).

Sketch of the proof: Our goal is to find the minimal value of the Ingleton score (3) for entropic points. It is equivalent to the minimal value of $\text{Ing}(A, B, X, Y)$ for *almost* entropic points satisfying the normalization condition $H(A, B, C, D) = 1$.

The objective function $\text{Ing}(A, B, C, D)$ and the normalization constraint are invariant with respect to the transpositions $\pi_{A,B}$ and $\pi_{C,D}$ that exchange the variables A, B and C, D respectively. Therefore, we can apply Lemma 2 and conclude that the required minimal value can be found in the space of points that are $\pi_{A,B}$ - and $\pi_{C,D}$ -invariant.

The invariance means that we can restrict ourselves to the points in $\bar{\Gamma}_4^*$ such that

$$\begin{cases} H(A) = H(B), H(A, C, D) = H(B, C, D), \\ H(A, C) = H(B, C), H(A, D) = H(B, D), \\ H(C) = H(D), H(A, B, C) = H(A, B, D), \\ H(A, C) = H(A, D), H(B, C) = H(B, D). \end{cases} \quad (4)$$

The crucial part of the proof is, of course, the Copy Lemma. We use the trick² from [17, proof of Ineq. 33, p. 19] and define

²It is remarkable that Ineq. 33. from [17] (even together with the symmetry constraints) does not imply Theorem 1. There is no contradiction: the instances of the Copy Lemma used in this proof imply besides Ineq. 33. several other non Shannon type inequalities, and only together these inequalities imply the required bound for the Ingleton score.

four new random variables R, S, T, U :

$$\begin{cases} (R, S) & := \emptyset\text{-copy}(B, D|A, C), \\ T & := (D, R)\text{-copy}(C|A, B, S), \\ U & := D\text{-copy}(B|A, C, R, S, T). \end{cases} \quad (5)$$

Technically, this means that we take the conditions (equalities) from the Copy Lemma (Lemma 1) that determine the entropies of the introduced variables and the properties of conditional independence for each instance of the Copy Lemma.

At last, we add to the normalization condition $H(A, B, C, D) = 1$ and the constraints (4) and (5) the Shannon type inequalities for A, B, C, D, R, S, T, U . Thus, we obtain a linear program for the $2^8 - 1 = 255$ variables (corresponding to the coordinates of the the entropy profile of (A, B, C, D, R, S, T, U)) with the objective function

$$\text{Ing}(A, B, C, D) \rightarrow \min$$

This problem is easily for the standard linear programming solvers (we made experiments with the solvers [27]–[29]). We can extract from the dual solution of this linear program a rational combination of inequalities that gives the desired bound (without floating point arithmetics nor rounding). We present this “formally checkable” proof in Appendix. ■

V. SECRET SHARING SCHEMES ON THE VÁMOS MATROID

The notion of a *secret sharing scheme* was introduced by Shamir [2] and Blakley [1]. Nowadays, secret sharing is an important component of many cryptographic protocols. We refer the reader to [15] for an excellent survey of secret sharing and its applications.

The aim of *perfect secret sharing* is to distribute a *secret value* among a set of parties in such a way that only the *qualified sets* of parties can recover the secret value; the non-qualified sets should have no information about the secret. The family of qualified sets of parties is called the *access structure* of the scheme. This family of sets must be monotone (a superset of a qualified set is also qualified).

The *information ratio* of a secret sharing schemes is the maximal ratio between the size (the entropy) of a share and the size (the entropy) of the secret. The optimization of this parameter is the central problem of secret sharing. This question was extensively studied for several families of access structures. The main technique for proving lower bounds on complexity of secret sharing schemes is nowadays the linear programming applied to the constraints formulated in terms of classic and non-classic information inequalities, see [19].

In what follows we apply our technique (the Copy Lemma combined with symmetry considerations and linear programming) to one of the classic access structures — the access structure defined on the Vámos matroid (more technically, one of two access structures that can be defined on the Vámos matroid). We skip the general motivation (the Vámos matroid is particularly interesting as a simple example of a non-representable matroid, see [15] for details) and formulate directly the problem of the information ratio for this access

structure in terms of Shannon's entropy of the involved random variables.

We define an access structure with parties $\{1, \dots, 7\}$. The minimal qualified sets are the 3-sets $\{1, 2, 3\}$, $\{1, 4, 5\}$ and all 4-sets not containing them, with three exceptions $\{2, 3, 4, 5\}$, $\{2, 3, 6, 7\}$, $\{4, 5, 4, 7\}$. We deal with jointly distributed random variables (S_0, \dots, S_7) , where S_0 is the secret and S_1, \dots, S_7 are the shares given to the seven parties involved in the scheme. We require that

- (i) for every minimal qualified set V listed above $H(S_0|S_V) = 0$;
- (ii) if $V \subset \{1, \dots, 7\}$ includes no minimal qualified set, then $H(S_0|S_V) = H(S_0)$.

Under these constraints, we are looking for the extremal value

$$\frac{\max\{H(S_1), \dots, H(S_7)\}}{H(S_0)} \rightarrow \inf$$

Since the set of almost-entropic points is a closed convex cone, we can add the normalization $H(S_0) = 1$ and rewrite the objective function as

$$\max\{H(S_1), \dots, H(S_7)\} \rightarrow \min \quad (6)$$

It is known that the required minimum is not greater than $4/3$, [14]. The history of improvements of the lower bound for this problem is presented in the table:

| | |
|------------|--|
| [3], 1992 | > 1 |
| [8], 2006 | $\geq 1 + \Omega(1/\sqrt{k})$ for a secret of size k |
| [13], 2008 | $\geq 11/10$ |
| [16], 2011 | $\geq 9/8 = 1.125$ |
| [21], 2013 | $\geq 67/59 \approx 1.135593$ |
| [26], 2018 | $\geq 33/29 \approx 1.137931$ |
| this paper | $\geq 561/491 \approx 1.142566$ |

Notice that the objective function, the normalization condition $H(S_0) = 1$, and the linear constraints in (i) and (ii) above are invariant with respect to the permutation that

- swap the indices 2 and 3,
- swap the indices 4 and 5,
- swap the indices 6 and 7,
- swap the pairs (2, 3) and (4, 5).

Therefore we can apply Lemma 2 and reduce the problem to those almost entropic points that satisfy the symmetries defined above.

We denote

$$V := (S_0, S_1) \text{ and } W := (S_6, S_7)$$

and define four new variables by applying twice the Copy Lemma:

- let (V', W') be an (S_0, S_1, S_6, S_7) -copy of (V, W) over (S_2, S_3, S_4, S_5) ;
- let (V'', W'') be an $(S_0, S_1, S_6, S_7, V', W')$ -copy of (V, W) over (S_2, S_3, S_4, S_5) .

Remark 1: Each instance of the Copy Lemma includes the property of *conditional independence*. In the construction

described above we have two applications of the Copy Lemma, and therefore two independence conditions:

$$\begin{aligned} I(V', W'; S_0, S_1, S_6, S_7 | S_2, S_3, S_4, S_5) &= 0 \\ I(V'', W''; S_0, S_1, S_6, S_7, V', W' | S_2, S_3, S_4, S_5) &= 0. \end{aligned}$$

These two conditions can be merged in one (more symmetric) constraint

$$\begin{aligned} H(S_0, S_1, S_6, S_7, V', V'', W', W'' | S_2, S_3, S_4, S_5) &= \\ = H(S_0, S_1, S_6, S_7 | S_2, S_3, S_4, S_5) &+ \\ + H(V', W' | S_2, S_3, S_4, S_5) &+ \\ + H(V'', W'' | S_2, S_3, S_4, S_5). \end{aligned}$$

Thus, we obtain a linear program with the following constraints:

- the conditions (i) and (ii) that define the access structure of the secret sharing scheme,
- the normalization $H(S_0) = 1$,
- the equalities that follow from the symmetry of the access structure,
- the conditions of the two instances of the Copy Lemma,
- and the Shannon type inequalities for twelve random variables $(S_0, \dots, S_7, V', V'', W', W'')$ (i.e., for $2^{12} - 1$ coordinates of their entropy profile).

The goal is to optimize the objective function (6).

Remark 2: We do not need to include in the linear program the variables V and W and their entropies — these two variables are used only as a notation in the Copy Lemma.

With a help of a computer (we used the solvers [27]–[29]) we find the optimal solution of this linear program: it is equal to $561/491$. Thus we establish the following statement.

Theorem 2: The optimal information rate of the secret sharing scheme for the access structure V_0 on the Vámos matroid is not less than $561/491 = 1.142566 \dots$

Remark 3: The standard linear programming solvers use the floating point arithmetic, and we should keep in mind the rounding errors. Our linear program contains only constraints with integer coefficients, so the values of the variables for the optimal solution of this linear program (the primal and the dual) can be taken rational. These rational values can be found by exact computing, without rounding. To compute the exact solution of a linear program we use the rational linear programming solver `QSOPT_EX`, see [10], [27].

The found exact dual solutions (rational linear combinations of constraints) for this linear program consist of more than 10^3 equalities and inequalities. The found rational linear combinations of equalities and inequalities provide a formal mathematical proof of Theorem 2, though such a proof hardly can be called “human-readable.”

Computing the exact solution of a linear program is rather time consuming. If we only need a *lower bound* for the optimal solution, it is enough to find a feasible solution of the dual problem that approximates (well enough) the optimal solution. Such an approximation can be found much faster than the exact ration solution, with more conventional floating point LP solvers.

Remark 4: The linear program constructed in this section would have the same optimal value if we omit the symmetry conditions (note that, unlike the previous section, in the proof of Theorem 2 the Copy Lemma is applied in symmetric settings). However, these symmetry conditions are not useless. In our experiments with exact computations, the symmetry constraints help to find a rational solution of the dual problem with smaller denominators. Also, in several experiments with floating point solvers, the symmetry constraints make the computation (or approximation) of the optimal solution faster. However, this is not a universal rule: in some experiments the symmetry constraints make the computation only slower — it depends on the used linear programming algorithm and on the chosen scaling of the objective function and of the constraints.

VI. CONCLUSION

When we derive balanced information inequalities, the technique of the Copy Lemma with “clones” of *individual* random variables is equivalent to the technique of the Ahlswede–Körner lemma, see [20]. In this paper we used the Copy Lemma in a stronger form, making “clones” of *pairs* of correlated variables. In the proofs of Theorem 1 and Theorem 2 it was crucial that we can “duplicate” in one shot a pair of correlated random variables, not only a single random variable.

The Ahlswede–Körner lemma used in [26] has a clear intuitive meaning: it can be interpreted in terms of extraction of the *common information*, see [7] and [6]. It would be interesting to find a structural property of the probability distribution that would give an intuitive explanation of the efficiency of the Copy Lemma with *two* (or more) copied variables.

REFERENCES

- [1] G. R. Blakley, Safeguarding cryptographic keys. *AFIPS Conference Proceedings 48*, (1979) 313-317.
- [2] A. Shamir, How to share a secret. *Commun. of the ACM*, (1979) 22, 612-613.
- [3] P. D. Seymour, On secret-sharing matroids. *J. of Combinatorial Theory, Series B*, 56:69–73, 1992.
- [4] Z. Zhang and R. W. Yeung, On characterization of entropy function via information inequalities. *IEEE Transactions on Information Theory*, 44(4), (1998) 1440-1452.
- [5] D. Hammer, A. Romashchenko, A. Shen, and N. Vereshchagin, Inequalities for Shannon entropy and Kolmogorov complexity. *Journal of Computer and System Sciences*, (2000) 60(2), 442-464.
- [6] K. Makarychev, Yu. Makarychev, A. Romashchenko, and N. Vereshchagin, A new class of non-Shannon-type inequalities for entropies. *Communications in Information and Systems*, (2002) 2(2), 147-166.
- [7] R. Ahlswede and J. Körner, On common information and related characteristics of correlated information sources, in *General Theory of Information Transfer and Combinatorics*, (2006) 664-677. Springer.
- [8] A. Beimel and N. Livne, On matroids and non-ideal secret sharing. In Proc. *Theory of Cryptography Conference*, (2006) 482-501.
- [9] R. Dougherty, C. Freiling, and K. Zeger, Six new non-Shannon information inequalities. In Proc. *IEEE International Symposium on Information Theory*, (2006) 233-236.
- [10] D. G. Espinoza, *On linear programming, integer programming and cutting planes*. PhD thesis, Georgia Institute of Technology. 2006.
- [11] F. Matúš, Infinitely many information inequalities. In Proc. *IEEE International Symposium on Information Theory*, 2007, 41-44.
- [12] F. Matúš, Adhesivity of polymatroids. *Discrete Mathematics*, (2007) 307(21), 2464-2477.
- [13] A. Beimel, N. Livne, C. Padró, Matroids Can Be Far From Ideal Secret Sharing. *Theory of Cryptography*, (2008) 194-212.
- [14] J. Martí-Farré, and C. Padró, On secret sharing schemes, matroids and polymatroids. *J. Math. Cryptol.* (2010) 4, 95-120.
- [15] A. Beimel, Secret-Sharing Schemes: A Survey. In Proc. *International Conference on Coding and Cryptology 2011*. LNCS, vol. 6639, (2011) 11-46.
- [16] J. R. Metcalf-Burton, Improved upper bounds for the information rates of the secret sharing schemes induced by the Vámos matroid. *Discrete Math.* (2011) 311, 651-662.
- [17] R. Dougherty, C. Freiling, and K. Zeger, Non-Shannon information inequalities in four random variables. (2011) arXiv:1104.3602.
- [18] R. W. Yeung, A first course in information theory. (2012) Springer Science & Business Media.
- [19] C. Padró, L. Vázquez, A. Yang, Finding Lower Bounds on the Complexity of Secret Sharing Schemes by Linear Programming. *Discrete Applied Mathematics*, (2013) 161, 1072-1084.
- [20] T. Kaced, Equivalence of two proof techniques for non-Shannon-type inequalities. In Proc. *IEEE International Symposium on Information Theory*, 2013, 236-240.
- [21] M. Gharahi, On the Complexity of Perfect Secret Sharing Schemes. Ph.D. Thesis (in Persian), Iran Univ. of Science and Technology (2013).
- [22] L. Csirmaz, Book Inequalities. *IEEE Trans. Information Theory*, (2014) 60(11), 6811-6818.
- [23] F. Matúš, and L. Csirmaz, Entropy region and convolution. *IEEE Trans. Inf. Theory*, (2016) 62(11), 6007-6018.
- [24] J. Apte and J. M. Walsh, Symmetry in network coding. In Proc. *IEEE International Symposium on Information Theory*, (2015) 376-380.
- [25] Q. Chen and R. W. Yeung, Partition-symmetrical entropy functions. *IEEE Transactions on Information Theory*, (2016) 62(10), 5385-5402.
- [26] O. Farràs, T. Kaced, S. Martín, and C. Padró, Improving the linear programming technique in the search for lower bounds in secret sharing. In Proc. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2018, 597-621.
- [27] QSOPT_EX: an exact linear programming solver. The authors of the solver are David Applegate, William Cook, Sanjeeb Dash, and Daniel Espinoza. The code is distributed under GNU GPL v2.1. Website of the project: <https://www.math.uwaterloo.ca/~bico/qsopt/ex/> A fork of QSOPT_EX on GitHub: <https://github.com/jonls/qsopt-ex>
- [28] GNU Linear Programming Kit, developed by Andrew O. Makhorn. The code is distributed under GNU GPL v3. Website of the project: www.gnu.org/software/glpk/
- [29] Gurobi Optimizer: a proprietary optimization solver for mathematical programming. Website: <http://www.gurobi.com/>

APPENDIX

In what follows we present a list of 167 equalities and inequalities. An integer linear combination of these inequalities implies Theorem 1.

Definition of the standard information quantities:

with a factor of 4503:
 $H(A) + H(B) - H(A, B) - I(A; B) = 0$
 with a factor of -4503:
 $H(AC) + H(B, C) - H(A, B, C) - H(C) - I(A; B|C) = 0$
 with a factor of -4503:
 $H(A, D) + H(B, D) - H(A, B, D) - H(D) - I(A; B|D) = 0$
 with a factor of -4503:
 $H(C) + H(D) - H(C, D) - I(C; D) = 0$

Symmetries between A and B and between C and D:

with a factor of 948:
 $H(A) - H(B) = 0$
 with a factor of -2370:
 $H(A, C) - H(B, C) = 0$
 with a factor of 1389:
 $H(A, C, D) - H(B, C, D) = 0$
 with a factor of 711:
 $H(C) - H(D) = 0$
 with a factor of -2844:
 $H(B, C) - H(B, D) = 0$
 with a factor of 1859:
 $H(A, B, C) - H(A, B, D) = 0$

Conditions from the Copy Lemma:

with a factor of -5260:
 $H(A, C, R, S) + H(A, B, C, D) - H(A, B, C, D, R, S) - H(A, C) = 0$
 with a factor of 948:
 $H(R) - H(B) = 0$
 with a factor of 948:
 $H(R, S) - H(B, D) = 0$
 with a factor of -948:
 $H(A, R) - H(A, B) = 0$
 with a factor of -3792:
 $H(A, S) - H(A, D) = 0$
 with a factor of 948:
 $H(A, R, S) - H(A, B, D) = 0$
 with a factor of -948:
 $H(C, R) - H(B, C) = 0$
 with a factor of 2873:
 $H(C, S) - H(C, D) = 0$
 with a factor of -1925:
 $H(C, R, S) - H(B, C, D) = 0$
 with a factor of 1385:
 $H(A, C, R) - H(A, B, C) = 0$
 with a factor of 919:
 $H(A, C, S) - H(A, C, D) = 0$
 with a factor of 1488:
 $H(A, C, R, S) - H(A, B, C, D) = 0$
 with a factor of -3555:
 $H(A, B, S, T) + H(A, B, C, D, R, S) - H(A, B, C, D, R, S, T) - H(A, B, S) = 0$
 with a factor of 474:
 $H(T) - H(C) = 0$
 with a factor of 948:
 $H(S, T) - H(C, S) = 0$
 with a factor of -1613:
 $H(A, T) - H(A, C) = 0$
 with a factor of -2133:
 $H(B, T) - H(B, C) = 0$
 with a factor of -520:
 $H(A, S, T) - H(A, C, S) = 0$
 with a factor of -46:
 $H(A, B, T) - H(A, B, C) = 0$
 with a factor of 2890:
 $H(A, B, S, T) - H(A, B, C, S) = 0$
 with a factor of -3855:
 $H(A, C, R, S, T, U) + H(A, B, C, D, R, S, T) - H(A, B, C, D, R, S, T, U) = 0$
 with a factor of 1896:
 $H(U) - H(B) = 0$
 with a factor of -1659:
 $H(T, U) - H(B, T) = 0$
 with a factor of 46:
 $H(A, U) - H(A, B) = 0$
 with a factor of -1555:
 $H(C, U) - H(B, C) = 0$
 with a factor of 341:
 $H(R, T, U) - H(B, R, T) = 0$
 with a factor of -46:
 $H(A, T, U) - H(A, B, T) = 0$
 with a factor of 607:
 $H(C, T, U) - H(B, C, T) = 0$
 with a factor of -341:
 $H(A, R, U) - H(A, B, R) = 0$
 with a factor of -341:
 $H(C, R, U) - H(B, C, R) = 0$
 with a factor of -46:
 $H(A, S, U) - H(A, B, S) = 0$
 with a factor of 46:
 $H(C, S, U) - H(B, C, S) = 0$
 with a factor of 191:
 $H(A, C, U) - H(A, B, C) = 0$
 with a factor of -46:
 $H(C, R, S, U) - H(B, C, R, S) = 0$
 with a factor of -667:
 $H(A, C, S, U) - H(A, B, C, S) = 0$
 with a factor of -428:
 $H(A, S, T, U) - H(A, B, S, T) = 0$
 with a factor of -266:
 $H(A, C, T, U) - H(A, B, C, T) = 0$
 with a factor of 817:
 $H(A, C, R, U) - H(A, B, C, R) = 0$
 with a factor of 114:
 $H(A, C, S, T, U) - H(A, B, C, S, T) = 0$

with a factor of 1337:
 $H(A, C, R, S, T, U) - H(A, B, C, R, S, T) = 0$

Shannon type inequalities:

with a factor of 711:
 $H(C) + H(D) - H(C, D) \geq 0$
 with a factor of 549:
 $H(A, B, C, D, S, U) - H(B, C, D, S, U) \geq 0$
 with a factor of 195:
 $H(A, B, C, D, S, T, U) - H(B, C, D, S, T, U) \geq 0$
 with a factor of 678:
 $H(A, B, C, D, S, T, U) - H(A, C, D, S, T, U) \geq 0$
 with a factor of 136:
 $H(A, B, C, D, S) - H(A, B, D, S) \geq 0$
 with a factor of 849:
 $H(A, B, C, D, S, T, U) - H(A, B, D, S, T, U) \geq 0$
 with a factor of 437:
 $H(A, C, D, R, S, U) - H(A, C, D, R, U) \geq 0$
 with a factor of 341:
 $H(A, R, T) + H(B, R, T) - H(A, B, R, T) - H(R, T) \geq 0$
 with a factor of 46:
 $H(A, D, U) + H(B, D, U) - H(A, B, D, U) - H(D, U) \geq 0$
 with a factor of 474:
 $H(A, D, T) + H(B, D, T) - H(A, B, D, T) - H(D, T) \geq 0$
 with a factor of 191:
 $H(A, D, S, U) + H(B, D, S, U) - H(A, B, D, S, U) - H(D, S, U) \geq 0$
 with a factor of 370:
 $H(A, C, T) + H(B, C, T) - H(A, B, C, T) - H(C, T) \geq 0$
 with a factor of 208:
 $H(A, C, D, R, S, U) + H(B, C, D, R, S, U) - H(A, B, C, D, R, S, U) - H(C, D, R, S, U) \geq 0$
 with a factor of 341:
 $H(A, R, U) + H(C, R, U) - H(A, C, R, U) - H(R, U) \geq 0$
 with a factor of 607:
 $H(A, R, T) + H(C, R, T) - H(A, C, R, T) - H(R, T) \geq 0$
 with a factor of 191:
 $H(A, B, S, T, U) + H(B, C, S, T, U) - H(A, B, C, S, T, U) - H(B, S, T, U) \geq 0$
 with a factor of 46:
 $H(A, B, R, S, U) + H(B, C, R, S, U) - H(A, B, C, R, S, U) - H(B, R, S, U) \geq 0$
 with a factor of 948:
 $H(A, S, T) + H(R, S, T) - H(A, R, S, T) - H(S, T) \geq 0$
 with a factor of 208:
 $H(A, C, D, S) + H(C, D, R, S) - H(A, C, D, R, S) - H(C, D, S) \geq 0$
 with a factor of 46:
 $H(A, B, S, U) + H(B, R, S, U) - H(A, B, R, S, U) - H(B, S, U) \geq 0$
 with a factor of 744:
 $H(A, B, C, D) + H(B, C, D, R) - H(A, B, C, D, R) - H(B, C, D) \geq 0$
 with a factor of 927:
 $H(A, B, C, D, S) + H(B, C, D, R, S) - H(A, B, C, D, R, S) - H(B, C, D, S) \geq 0$
 with a factor of 744:
 $H(A, B, C, D, R, T) + H(B, C, D, R, S, T) - H(A, B, C, D, R, S, T) - H(B, C, D, R, T) \geq 0$
 with a factor of 266:
 $H(A, D, U) + H(D, T, U) - H(A, D, T, U) - H(D, U) \geq 0$
 with a factor of 237:
 $H(A, B, C, D, U) + H(B, C, D, T, U) - H(A, B, C, D, T, U) - H(B, C, D, U) \geq 0$
 with a factor of 403:
 $H(A, B, C, D, R) + H(B, C, D, R, T) - H(A, B, C, D, R, T) - H(B, C, D, R) \geq 0$
 with a factor of 100:
 $H(A, C, D) + H(C, D, U) - H(A, C, D, U) - H(C, D) \geq 0$
 with a factor of 208:
 $H(A, C, D, S, T) + H(C, D, S, T, U) - H(A, C, D, S, T, U) - H(C, D, S, T) \geq 0$
 with a factor of 208:
 $H(A, C, D, R, S) + H(C, D, R, S, U) - H(A, C, D, R, S, U) - H(C, D, R, S) \geq 0$
 with a factor of 744:
 $H(A, B, C, D, S) + H(B, C, D, S, U) - H(A, B, C, D, S, U) - H(B, C, D, S) \geq 0$
 with a factor of 195:
 $H(A, B, C, D, R, S, T) + H(B, C, D, R, S, T, U) - H(A, B, C, D, R, S, T, U) - H(B, C, D, R, S, T) \geq 0$
 with a factor of 341:
 $H(B, C) + H(C, R) - H(B, C, R) - H(C) \geq 0$
 with a factor of 1925:
 $H(B, C, S) + H(C, R, S) - H(B, C, R, S) - H(C, S) \geq 0$
 with a factor of 46:
 $H(B, C, S, U) + H(C, R, S, U) - H(B, C, R, S, U) - H(C, S, U) \geq 0$
 with a factor of 403:
 $H(A, B, C, D, U) + H(A, C, D, R, U) - H(A, B, C, D, R, U) - H(A, C, D, U) \geq 0$
 with a factor of 778:
 $H(A, B, C, D, S) + H(A, C, D, R, S) - H(A, B, C, D, R, S) - H(A, C, D, S) \geq 0$
 with a factor of 191:
 $H(B, D, U) + H(D, S, U) - H(B, D, S, U) - H(D, U) \geq 0$
 with a factor of 208:
 $H(B, C, D, T) + H(C, D, S, T) - H(B, C, D, S, T) - H(C, D, T) \geq 0$
 with a factor of 3601:
 $H(A, B) + H(A, S) - H(A, B, S) - H(A) \geq 0$
 with a factor of 46:
 $H(A, B, U) + H(A, S, U) - H(A, B, S, U) - H(A, U) \geq 0$
 with a factor of 476:
 $H(A, B, C, R, U) + H(A, C, R, S, U) - H(A, B, C, R, S, U) - H(A, C, R, U) \geq 0$
 with a factor of 362:
 $H(A, B, C, D) + H(A, C, D, S) - H(A, B, C, D, S) - H(A, C, D) \geq 0$
 with a factor of 744:
 $H(A, B, C, D, R, U) + H(A, C, D, R, S, U) - H(A, B, C, D, R, S, U) - H(A, C, D, R, U) \geq 0$
 with a factor of 208:
 $H(B, C, D) + H(C, D, T) - H(B, C, D, T) - H(C, D) \geq 0$
 with a factor of 1181:
 $H(A, B, C, D, R, S, U) + H(A, C, D, R, S, T, U) - H(A, B, C, D, R, S, T, U) - H(A, C, D, R, S, U) \geq 0$
 with a factor of 237:
 $H(B, C, T) + H(C, T, U) - H(B, C, T, U) - H(C, T) \geq 0$
 with a factor of 403:
 $H(B, C, D, R) + H(C, D, R, U) - H(B, C, D, R, U) - H(C, D, R) \geq 0$
 with a factor of 237:
 $H(A, B, S, T) + H(A, S, T, U) - H(A, B, S, T, U) - H(A, S, T) \geq 0$
 with a factor of 963:
 $H(A, B, C, S, T) + H(A, C, S, T, U) - H(A, B, C, S, T, U) - H(A, C, S, T) \geq 0$
 with a factor of 1337:
 $H(A, B, C, R, S, T) + H(A, C, R, S, T, U) - H(A, B, C, R, S, T, U) - H(A, C, R, S, T) \geq 0$

with a factor of 578:
 $H(A, B, C, D, T) + H(A, C, D, T, U) - H(A, B, C, D, T, U) - H(A, C, D, T) \geq 0$
with a factor of 778:
 $H(A, B, C, D, R) + H(A, C, D, R, U) - H(A, B, C, D, R, U) - H(A, C, D, R) \geq 0$
with a factor of 711:
 $H(C, U) + H(D, U) - H(C, D, U) - H(U) \geq 0$
with a factor of 237:
 $H(B, C, U) + H(B, S, U) - H(B, C, S, U) - H(B, U) \geq 0$
with a factor of 46:
 $H(A, B, C, T, U) + H(A, B, S, T, U) - H(A, B, C, S, T, U) - H(A, B, T, U) \geq 0$
with a factor of 31065:
 $H(A, B, C, D, U) + H(A, B, D, S, U) - H(A, B, C, D, S, U) - H(A, B, D, U) \geq 0$
with a factor of 849:
 $H(A, B, C, D, T) + H(A, B, D, S, T) - H(A, B, C, D, S, T) - H(A, B, D, T) \geq 0$
with a factor of 80180:
 $H(C, U) + H(T, U) - H(C, T, U) - H(U) \geq 0$
with a factor of 208:
 $H(C, D, U) + H(D, T, U) - H(C, D, T, U) - H(D, U) \geq 0$
with a factor of 191:
 $H(B, C, S, U) + H(B, S, T, U) - H(B, C, S, T, U) - H(B, S, U) \geq 0$
with a factor of 948:
 $H(A, C, R, S) + H(A, R, S, T) - H(A, C, R, S, T) - H(A, R, S) \geq 0$
with a factor of 312:
 $H(A, C, D, U) + H(A, D, T, U) - H(A, C, D, T, U) - H(A, D, U) \geq 0$
with a factor of 191:
 $H(A, C, D, S, U) + H(A, D, S, T, U) - H(A, C, D, S, T, U) - H(A, D, S, U) \geq 0$
with a factor of 1323:
 $H(A, B, C, D) + H(A, B, D, T) - H(A, B, C, D, T) - H(A, B, D) \geq 0$
with a factor of 46:
 $H(A, B, C, D, U) + H(A, B, D, T, U) - H(A, B, C, D, T, U) - H(A, B, D, U) \geq 0$
with a factor of 341:
 $H(A, B, C, D, R) + H(A, B, D, R, T) - H(A, B, C, D, R, T) - H(A, B, D, R) \geq 0$
with a factor of 198:
 $H(A, B, C, D) + H(A, B, D, U) - H(A, B, C, D, U) - H(A, B, D) \geq 0$
with a factor of 39:
 $H(A, B, C, D, R) + H(A, B, D, R, U) - H(A, B, C, D, R, U) - H(A, B, D, R) \geq 0$
with a factor of 849:
 $H(A, B, C, D, R, S, T) + H(A, B, D, R, S, T, U) - H(A, B, C, D, R, S, T, U) - H(A, B, D, R, S, T) \geq 0$
with a factor of 1879:
 $H(B, C, D, S) + H(B, C, R, S) - H(B, C, D, R, S) - H(B, C, S) \geq 0$
with a factor of 1181:
 $H(A, C, D, S, T, U) + H(A, C, R, S, T, U) - H(A, C, D, R, S, T, U) - H(A, C, S, T, U) \geq 0$
with a factor of 817:
 $H(A, B, C, D) + H(A, B, C, R) - H(A, B, C, D, R) - H(A, B, C) \geq 0$
with a factor of 861:
 $H(A, B, C, D, T, U) + H(A, B, C, R, T, U) - H(A, B, C, D, R, T, U) - H(A, B, C, T, U) \geq 0$
with a factor of 522:
 $H(A, B, C, D, S, U) + H(A, B, C, R, S, U) - H(A, B, C, D, R, S, U) - H(A, B, C, S, U) \geq 0$
with a factor of 191:
 $H(A, D) + H(A, S) - H(A, D, S) - H(A) \geq 0$
with a factor of 191:
 $H(A, C, D, U) + H(A, C, S, U) - H(A, C, D, S, U) - H(A, C, U) \geq 0$
with a factor of 104:
 $H(A, C, D, T, U) + H(A, C, S, T, U) - H(A, C, D, S, T, U) - H(A, C, T, U) \geq 0$
with a factor of 778:
 $H(A, C, D, R) + H(A, C, R, S) - H(A, C, D, R, S) - H(A, C, R) \geq 0$
with a factor of 3096:
 $H(A, B, C, D) + H(A, B, C, S) - H(A, B, C, D, S) - H(A, B, C) \geq 0$
with a factor of 1337:
 $H(A, B, C, D, R, T, U) + H(A, B, C, R, S, T, U) - H(A, B, C, D, R, S, T, U) - H(A, B, C, R, T, U) \geq 0$
with a factor of 474:
 $H(B, D) + H(B, T) - H(B, D, T) - H(B) \geq 0$
with a factor of 237:
 $H(B, C, D, U) + H(B, C, T, U) - H(B, C, D, T, U) - H(B, C, U) \geq 0$
with a factor of 711:
 $H(A, D) + H(A, T) - H(A, D, T) - H(A) \geq 0$
with a factor of 46:
 $H(A, B, D, U) + H(A, B, T, U) - H(A, B, D, T, U) - H(A, B, U) \geq 0$
with a factor of 341:
 $H(A, B, D, R) + H(A, B, R, T) - H(A, B, D, R, T) - H(A, B, R) \geq 0$
with a factor of 104:
 $H(A, B, C, D) + H(A, B, C, T) - H(A, B, C, D, T) - H(A, B, C) \geq 0$
with a factor of 873:
 $H(A, B, C, D, S) + H(A, B, C, S, T) - H(A, B, C, D, S, T) - H(A, B, C, S) \geq 0$
with a factor of 769:
 $H(A, B, C, D, R, U) + H(A, B, C, R, T, U) - H(A, B, C, D, R, T, U) - H(A, B, C, R, U) \geq 0$
with a factor of 474:
 $H(D, T) + H(T, U) - H(D, T, U) - H(T) \geq 0$

with a factor of 237:
 $H(B, D) + H(B, U) - H(B, D, U) - H(B) \geq 0$
with a factor of 46:
 $H(A, D, T) + H(A, T, U) - H(A, D, T, U) - H(A, T) \geq 0$
with a factor of 191:
 $H(A, D, S, T) + H(A, S, T, U) - H(A, D, S, T, U) - H(A, S, T) \geq 0$
with a factor of 370:
 $H(A, C, D, T) + H(A, C, T, U) - H(A, C, D, T, U) - H(A, C, T) \geq 0$
with a factor of 815:
 $H(A, B, C, D) + H(A, B, C, U) - H(A, B, C, D, U) - H(A, B, C) \geq 0$
with a factor of 1722:
 $H(A, B, C, D, S, T) + H(A, B, C, S, T, U) - H(A, B, C, D, S, T, U) - H(A, B, C, S, T) \geq 0$
with a factor of 341:
 $H(R, U) + H(T, U) - H(R, T, U) - H(U) \geq 0$
with a factor of 607:
 $H(C, R) + H(C, T) - H(C, R, T) - H(C) \geq 0$
with a factor of 208:
 $H(B, C, D, R, S) + H(B, C, D, S, T) - H(B, C, D, R, S, T) - H(B, C, D, S) \geq 0$
with a factor of 195:
 $B, C, D, R, S, U) + H(B, C, D, S, T, U) - H(B, C, D, R, S, T, U) - H(B, C, D, S, U) \geq 0$
with a factor of 948:
 $H(A, R) + H(A, T) - H(A, R, T) - H(A) \geq 0$
with a factor of 963:
 $H(A, C, R, S) + H(A, C, S, T) - H(A, C, R, S, T) - H(A, C, S) \geq 0$
with a factor of 293:
 $H(A, B, C, R, U) + H(A, B, C, T, U) - H(A, B, C, R, T, U) - H(A, B, C, U) \geq 0$
with a factor of 476:
 $H(C, D, R) + H(C, D, U) - H(C, D, R, U) - H(C, D) \geq 0$
with a factor of 476:
 $H(A, C, R, S) + H(A, C, S, U) - H(A, C, R, S, U) - H(A, C, S) \geq 0$
with a factor of 39:
 $H(A, B, D, R) + H(A, B, D, U) - H(A, B, D, R, U) - H(A, B, D) \geq 0$
with a factor of 849:
 $A, B, D, R, S, T) + H(A, B, D, S, T, U) - H(A, B, D, R, S, T, U) - H(A, B, D, R, S, T) \geq 0$
with a factor of 948:
 $H(R, S) + H(R, T) - H(R, S, T) - H(R) \geq 0$
with a factor of 208:
 $H(C, D, S) + H(C, D, T) - H(C, D, S, T) - H(C, D) \geq 0$
with a factor of 341:
 $H(B, C, D, R, S) + H(B, C, D, R, T) - H(B, C, D, R, S, T) - H(B, C, D, R) \geq 0$
with a factor of 191:
 $H(A, D, S) + H(A, D, T) - H(A, D, S, T) - H(A, D) \geq 0$
with a factor of 607:
 $H(A, C, R, S) + H(A, C, R, T) - H(A, C, R, S, T) - H(A, C, R) \geq 0$
with a factor of 208:
 $H(A, C, D, S) + H(A, C, D, T) - H(A, C, D, S, T) - H(A, C, D) \geq 0$
with a factor of 522:
 $H(A, B, C, S, U) + H(A, B, C, T, U) - H(A, B, C, S, T, U) - H(A, B, C, U) \geq 0$
with a factor of 293:
 $H(A, B, C, D, R, S, U) + H(A, B, C, D, R, T, U) - H(A, B, C, D, R, S, T, U) - H(A, B, C, D, R, U) \geq 0$
with a factor of 208:
 $H(C, D, S, T) + H(C, D, T, U) - H(C, D, S, T, U) - H(C, D, T) \geq 0$
with a factor of 403:
 $H(B, C, D, R, S) + H(B, C, D, R, U) - H(B, C, D, R, S, U) - H(B, C, D, R) \geq 0$
with a factor of 136:
 $H(A, B, D, S) + H(A, B, D, U) - H(A, B, D, S, U) - H(A, B, D) \geq 0$

The sum of these equalities and inequalities (with the specified factors) is equal to

$$4503[I(A; B|C) + I(A; B|D) + I(C; D) - I(A; B)] + 711H(A, B, C, D) \geq 0,$$

which is equivalent to

$$I(A; B|C) + I(A; B|D) + I(C; D) - I(A; B) + (3/19)H(A, B, C, D) \geq 0.$$

Therefore,

$$\frac{I(A; B|C) + I(A; B|D) + I(C; D) - I(A; B)}{H(A, B, C, D)} \geq -3/19.$$