

Conditional Independence Structures over Four Discrete Random Variables Revisited: Conditional Ingleton Inequalities

Milan Studený

dedicated to the memory of František Matúš

Abstract—The paper deals with linear information inequalities valid for entropy functions induced by discrete random variables. Specifically, the so-called *conditional Ingleton inequalities* are in the center of interest: these are valid under conditional independence assumptions on the inducing random variables. We discuss five inequalities of this particular type, four of which has appeared earlier in the literature. Besides the proof of the new fifth inequality, simpler proofs of (some of) former inequalities are presented. These five information inequalities are used to characterize all conditional independence structures induced by four discrete random variables.

Index Terms—entropy function, discrete random variables, conditional information inequalities, conditional independence, polymatroids.

I. INTRODUCTION

THE motivation for this paper is explained and its structure is described.

A. Motivation

The concept of *conditional independence* (CI) has been studied in probability theory [13, §25.3] and statistics [6], [24] for many years. This concept has a key theoretical role in probabilistic reasoning [27] and graphical statistical models [12]. This is because the implications between CI statements are interpreted in this context as substantial abstract properties of (= “axioms” for) the respective (probabilistic) conditional irrelevance relation. The first attempts to describe abstract properties of probabilistic CI in terms of (a finite number of) elementary CI implications occurred in the end of the 1970s [6], [32]. It was shown in the 1990s that probabilistic CI structures cannot be characterized by means of a finite number of CI implications of this kind [35] while some important substructures of probabilistic CI structures can be characterized in this way [16].

One of the goals motivated by this idea was to characterize CI structures induced by four discrete random variables. Note in this context that, for a theoretical reason, the CI structures over a fixed number of random variables can be characterized

by means of a finite number of such elementary CI implications but the number of these CI implications (= “axioms” for CI) grows rapidly with the number of random variables. The goal has been achieved in the end of 1990s by Matúš in a series of three papers [19], [20], [21]; the author of this article was a co-author of the first paper in the series. The final solution was the result of Matúš’s enormous efforts: it took him more than five years to reach his goal. Note in this context that the number of CI structures over four discrete random variables is very high, in fact, one has 18 478 standard such CI structures.

To prove the validity of elementary CI implications (= of “axioms” for CI) Matúš [20], [21] used a number of methods that he has developed. Some of the CI implications were derived as consequences of considerations within a wider framework of σ -algebras, some of them followed from the non-negativity of the Kullback-Leibler divergence of specially constructed probability distributions and a few of them were based on the characterization of CI in terms of factorization of probability density. In the last paper in the series two remaining CI implications were derived as consequences of conditional information inequalities. That last method was inspired by then recent paper by Zhang and Yeung [42] in which they revealed the first (non-Shannon) conditional information inequality; Matúš in [21] proved the second conditional inequality. Thus, one can say, with a little exaggeration, that each of the found CI implications from [20], [21] has its own specific proof. The interest in conditional information inequalities has been restored some years later when Kaced and Romashchenko [10] found other such inequalities and introduced the ways to classify them.

The source of motivation for this paper was the following simple question: could it be the case that all the CI implications that were revealed in case of four discrete random variables can be derived using only one procedure? The surprising answer is “yes”: it appears that all these CI implications can really be derived as consequences of conditional information inequalities valid for (entropy functions induced by) discrete random variables. These inequalities are special in a certain sense: they can be viewed as *conditional Ingleton inequalities* and only five of them are enough to cover all 19 necessary CI implications. Note in this context that there are also further valid CI implications/equivalences which, however, can be verified even easier. Another remark is that this paper, unlike the original series of papers [19], [20], [21], deals with standard CI structures, which means that the functional

M. Studený is with the Institute of Information Theory and Automation, Czech Academy of Sciences, Prague, CZ 18200 Czech Republic. (e-mail: studeny@utia.cas.cz)

Manuscript received December 9, 2020; revised August 1, 2021. Copyright ©2017 IEEE. Personal use of this material is permitted. However, permission to use this material for any other purposes must be obtained from the IEEE by sending a request to pubs-permissions@ieee.org.

dependences among the considered random variables are not taken into consideration. This is not a substantial difference because every augmented CI structure (= the one with functional dependence statements involved) can be viewed as an extension of a unique standard CI structure (= the one without functional dependences).

The contribution of this paper is a new (= the fifth) conditional Ingleton inequality, simpler proofs of two former such inequalities from [21], [10] and the derivation of all elementary CI implications over four discrete random variables using these five conditional Ingleton inequalities. For sake of completeness we also recall, or perhaps reinterpret, the proofs of two remaining inequalities so that the reader interested in the characterization of CI structures over four discrete random variables has a complete proof at disposal. Thus, altogether, we present a simpler proof of the characterization of CI structures over four variables than was the original one from [19], [20], [21]. There was also another conjectured conditional Ingleton inequality (= the sixth one), whose validity would not have been in contradiction with the validity of 19 above-mentioned elementary CI implications, but that one appeared not to be true. Thus, a counter-example to its validity is also given.

B. Structure of the paper

Basic concepts of the paper are introduced in Section II. We formally define the concepts of CI, entropy function, polymatroid, and Ingleton inequality there; we also recall a few fundamental facts used later. Section III then provides the reader with an overview of related former results; it can be viewed as a kind of extended introduction and can be skipped without losing understanding of the rest of the paper. Specifically, we recall the results on characterization of CI structures over 4 discrete random variables (in more details), on representations of polymatroids, and on information inequalities. Section IV is then devoted particularly to conditional Ingleton inequalities. We present 5 inequalities of this type there, whose proofs, however, are moved to Appendix (Section A). Additionally, five counter-examples to the (probabilistic) validity of the Ingleton inequality are given in Section IV and a few open tasks are formulated there. Section V then brings an elegant application of the results from Section IV: we characterize all (standard) CI structures induced by four discrete random variables there. In Conclusions (Section VI) we comment further potential applications of the presented results.

II. PRELIMINARIES

Throughout the paper a finite non-empty *basic set* N will be considered; its elements will index (= correspond to) discrete random variables. To avoid the trivial case we assume $|N| \geq 2$. Shortened notation for some subsets of N will often be used: union of two subsets $X, Y \subseteq N$ may be denoted by a juxtaposition of respective symbols: $XY := X \cup Y$. Analogously, the symbol for an element $i \in N$ will also serve to denote the respective singleton subset of N : $i := \{i\}$. The power set of N will be denoted by $\mathcal{P}(N) := \{S : S \subseteq N\}$.

A. Discrete random vector over a basic set

A *discrete random variable* is a measurable function ξ from a probability space $(\Omega, \mathcal{A}, \mathbf{P})$ to a non-empty finite set \mathbf{X} , called the *sample space* for ξ . The *density* (for ξ) is then a function p on \mathbf{X} defined by

$$p(x) := \mathbf{P}(\{\omega \in \Omega : \xi(\omega) = x\}) \quad \text{for } x \in \mathbf{X}.$$

Note that the probability space is only an auxiliary tool here, the object of interest is, in fact, the induced probability distribution on the sample space and this object is fully described by the density. Observe that p is a density (for a random variable with sample space \mathbf{X}) iff $p : \mathbf{X} \rightarrow [0, 1]$ and $\sum_{x \in \mathbf{X}} p(x) = 1$.

By a *discrete random vector* over N will be understood an indexed collection $\xi = [\xi_i]_{i \in N}$ of random variables on a shared probability space $(\Omega, \mathcal{A}, \mathbf{P})$ with each ξ_i taking values in its *individual* non-empty finite *sample space* \mathbf{X}_i .

Given such a random vector ξ over N , we introduce a symbol $\mathbf{X}_A := \prod_{i \in A} \mathbf{X}_i$ for any $\emptyset \neq A \subseteq N$, to denote the set of all possible *configurations* of values for the (random) sub-vector $\xi_A := [\xi_i]_{i \in A}$. Each sub-vector ξ_A of ξ can thus be interpreted as a random variable with sample space \mathbf{X}_A ; the random vector ξ itself can thus be viewed as a single random variable as well, with values in the *joint sample space* \mathbf{X}_N . Given a configuration $x \in \mathbf{X}_A$ and $i \in A$, the symbol x_i will denote the respective component of x , that is, $x = [x_i]_{i \in A}$, where $x_i \in \mathbf{X}_i$.

The *marginal density* for $A \subseteq N$ is defined by the formula

$$p_A(x) := \sum \{p(y) : y \in \mathbf{X}_N \text{ with } x_i = y_i \text{ for all } i \in A\},$$

whenever $x \in \mathbf{X}_N$.

We have intentionally introduced it as a function on \mathbf{X}_N depending on the components from A . The special cases are then the *joint density* p_N and the density p_\emptyset for the empty set, which is a constant function on \mathbf{X}_N taking the value 1. Nevertheless, if appropriate, one can view the marginal density p_A as a function on the respective marginal sample \mathbf{X}_A (provided $A \neq \emptyset$).

B. Probabilistic conditional independence

Probabilistic CI structure induced by a random vector ξ over N is a discrete mathematical structure describing stochastic independence (and dependence) relations among (random) sub-vectors of ξ . Having three subsets $X, Y, Z \subseteq N$ of the basic set we say that ξ_X is *conditionally independent* of ξ_Y given ξ_Z and write $\xi_X \perp\!\!\!\perp \xi_Y \mid \xi_Z$ if

$$\forall x \in \mathbf{X}_N \quad p_{XYZ}(x) \cdot p_Z(x) = p_{XZ}(x) \cdot p_{YZ}(x). \quad (1)$$

An alternative notation is $X \perp\!\!\!\perp Y \mid Z [\xi]$. The respective ordered triplet of sets will also be denoted by $(X, Y \mid Z)$; we use a bar to separate the third component interpreted as the conditioning variable set Z .

Note that the definition (1) works for any triplet of sets X, Y, Z although these three sets are typically assumed to be pairwise disjoint. The case $Z = \emptyset$ corresponds to classic (unconditional) stochastic independence, denoted also by

$\xi_X \perp\!\!\!\perp \xi_Y$, alternatively by $X \perp\!\!\!\perp Y \mid \xi$. The case $Y = X$ corresponds to functional dependence of ξ_X on ξ_Z : the reader can easily deduce from (1) that $\xi_X \perp\!\!\!\perp \xi_X \mid \xi_Z$ is equivalent to the existence of a function $f : \mathbf{X}_Z \rightarrow \mathbf{X}_X$ such that $\xi_X = f(\xi_Z)$.

There is a number of equivalent definitions of probabilistic CI, one of them in terms of *conditional density*, which is formally defined by the ratio

$$p_{X|Z}(x) := \frac{p_{XZ}(x)}{p_Z(x)} \quad \text{for } x \in \mathbf{X}_N \text{ such that } p_Z(x) > 0,$$

with disjoint $X, Z \subseteq N$. The reader can verify easily that, in case of pairwise disjoint $X, Y, Z \subseteq N$ with $X \neq \emptyset \neq Y$, one has $\xi_X \perp\!\!\!\perp \xi_Y \mid \xi_Z$ iff

$$p_{X|YZ}(x) = p_{X|Z}(x) \quad \text{for each } x \in \mathbf{X}_N \text{ with } p_{YZ}(x) > 0.$$

To say that in yet another way, one has $\xi_X \perp\!\!\!\perp \xi_Y \mid \xi_Z$ iff the conditional density $p_{X|YZ}(x)$ does not depend on the (value of a) sub-configuration for Y . In binary case, that is, in case $\mathbf{X}_i = \{0, 1\}$ for $i \in N$, the following *cross-product criterion* can be used: provided $|X| = 1 = |Y|$ and \tilde{p} is the marginal density for XYZ interpreted as a function on \mathbf{X}_{XYZ} then $\xi_X \perp\!\!\!\perp \xi_Y \mid \xi_Z$ iff

$$\tilde{p}(0, 0, z) \cdot \tilde{p}(1, 1, z) = \tilde{p}(0, 1, z) \cdot \tilde{p}(1, 0, z) \\ \text{for any configuration } z \in \mathbf{X}_Z \text{ for } Z.$$

Formally, the CI structure induced by a random vector ξ over N is a certain ternary relation on the power set $\mathcal{P}(N)$. Specifically, the *augmented CI structure* induced by a random vector ξ over N is

$$\{(X, Y|Z) \in \mathcal{P}(N) \times \mathcal{P}(N) \times \mathcal{P}(N) : \xi_X \perp\!\!\!\perp \xi_Y \mid \xi_Z\}.$$

The *standard CI structure* is the above ternary relation on $\mathcal{P}(N)$ confined to triplets of pairwise disjoint subsets of N as required traditionally in [27], [12]. Note that discrete probabilistic CI structures over N are naturally ordered by inclusion of involved independence triplets (for further details see Section II-H).

C. Conditional product of distributions

A discrete *probability distribution over N* is simply the distribution of a discrete random vector over N . Put it in another way: a discrete distribution P over N is specified by a collection of individual non-empty finite sample spaces \mathbf{X}_i , $i \in N$, and by its density $p : \mathbf{X}_N \rightarrow [0, 1]$ defined on the respective joint sample space. Given $\emptyset \neq A \subset N$, the *marginal* (distribution) of P for A can be introduced as the distribution of the random sub-vector ξ_A . Thus, it is a probability distribution over A with individual sample spaces \mathbf{X}_i , $i \in A$, inherited from P . The marginal density can be computed from the joint one by summing over configurations in $\mathbf{X}_{N \setminus A}$.

Given pairwise disjoint sets $A, B, C \subseteq N$ with $A \neq \emptyset \neq B$, we say that (discrete) probability distributions Q over AC and R over BC are *consonant* if the marginals of Q and R for C coincide, which involves the requirement that the individual sample spaces for $i \in C$ coincide. Given such a

pair of consonant distributions their *conditional product* is a (discrete) probability distribution P over ABC with individual sample spaces inherited from Q and R whose density p on \mathbf{X}_{ABC} is defined by the following formula:

$$p(a, b, c) := \begin{cases} \frac{q(a,c) \cdot r(b,c)}{r(c)} & \text{if } p(c) > 0, \\ 0 & \text{otherwise,} \end{cases}$$

where a, b, c belong to the respective marginal sample spaces and $q(a, c)$ denotes the value of the marginal density of Q for AC in the configuration $[a, c]$. Easy observations are that the marginals of the conditional product P are the given distributions Q and R and one, moreover, has $\xi_A \perp\!\!\!\perp \xi_B \mid \xi_C$ for any random vector ξ over ABC having the conditional product P as its distribution.

D. Semi-graphoids

In this paper we also deal with (standard) *abstract CI structures* over N which are simply ternary relations on $\mathcal{P}(N)$ (confined to triplets of pairwise disjoint sets). A convention is accepted that ordered triplets $(X, Y|Z)$ of sets involved in such ternary relations are interpreted as abstract independence statements, which is expressed by notation $X \perp\!\!\!\perp Y \mid Z$.

Abstract CI structures can be induced by various mathematical objects, not just by random vectors. Nevertheless, they typically comply with some basic formal properties of (= "axioms" for) conditional irrelevance relations which were already pinpointed in [6]. Thus, following to [27], we will say that a standard abstract CI structure over N is a *semi-graphoid* if it satisfies the next three conditions: given pairwise disjoint sets $X, Y, Z, U \subseteq N$, one has

$$\begin{aligned} \text{(S:0)} \quad & \emptyset \perp\!\!\!\perp Y \mid Z, \\ \text{(S:1)} \quad & X \perp\!\!\!\perp Y \mid Z \Leftrightarrow Y \perp\!\!\!\perp X \mid Z, \\ \text{(S:2)} \quad & X \perp\!\!\!\perp YZ \mid U \Leftrightarrow [X \perp\!\!\!\perp Y \mid ZU \ \& \ X \perp\!\!\!\perp Z \mid U]. \end{aligned}$$

One can analogously introduce semi-graphoids in context of augmented abstract CI structures: admit intersecting sets in (S:1) and (S:2) and replace (S:0) by

$$\bullet \quad X \subseteq Z \Rightarrow X \perp\!\!\!\perp Y \mid Z.$$

The fact that every probabilistic CI structure is a semi-graphoid easily follows from later observations (see Lemma 3 in Section II-F).

The semi-graphoid properties imply that one need not retain (information about) all CI statements in order to represent a CI structure. A triplet $(X, Y|Z)$ of pairwise disjoint subsets of N will be called *elementary* if $|X| = 1 = |Y|$. The point is that elementary triplets are enough to represent a semi-graphoid.

Lemma 1: Given a semi-graphoid over N (denoted using the symbol $\perp\!\!\!\perp$) and a triplet $(X, Y|Z)$ of pairwise disjoint subsets of N one has

$$X \perp\!\!\!\perp Y \mid Z \Leftrightarrow \tag{2}$$

$$\forall i \in X, j \in Y, K : Z \subseteq K \subseteq XYZ \setminus \{i, j\}, \quad i \perp\!\!\!\perp j \mid K.$$

Proof. We leave it to the reader to verify (2) by induction on the cardinality of XY . The induction premise follows immediately from (S:0) if $|XY| \leq 2$ while the induction step can be verified using (S:2). \square

Taking into consideration the symmetry property (S:1) one can deduce that to represent a standard semi-graphoid over N , $|N| = n$, in the memory of a computer it is enough to have $n \cdot (n-1) \cdot 2^{n-3}$ bits, each of which corresponds to a pair of mutually equivalent elementary triplets $(i, j|K)$ and $(j, i|K)$.

In the context of augmented abstract CI structures one has, however, to introduce additional (non-disjoint) elementary triplets $(i, i|N \setminus i)$ for $i \in N$; Lemma 1 can then be extended to that case as well.

E. Polymatroids

A central role in our exposition will have real set functions $h : \mathcal{P}(N) \rightarrow \mathbb{R}$. Given such a function h and sets $X, Y, Z \subseteq N$ we introduce a special shorthand

$$\Delta h(X, Y|Z) := h(XZ) + h(YZ) - h(XYZ) - h(Z) \quad (3)$$

to denote the corresponding *difference expression* for the ordered triplet $(X, Y|Z)$ of subsets of N . The symbol of the function h will sometimes be omitted; we will do so in situations when we wish to emphasize that (3) defines a functional $\Delta(X, Y|Z) : h \mapsto \Delta h(X, Y|Z)$ on $\mathbb{R}^{\mathcal{P}(N)}$. Typically, the considered triplet $(X, Y|Z)$ of subsets of N will be composed of pairwise disjoint sets and, in this case, it will be associated with an abstract CI statement $X \perp\!\!\!\perp Y | Z$.

The rank function of a *polymatroid* is a real set function $h : \mathcal{P}(N) \rightarrow \mathbb{R}$ which satisfies $h(\emptyset) = 0$ and $0 \leq \Delta h(X, Y|Z)$ for any triplet $X, Y, Z \subseteq N$ of subsets of the basic set. In case $I \subseteq J \subseteq N$ and $(X, Y|Z) = (J, J|I)$ one has $0 \leq \Delta h(J, J|I) = h(J) - h(I)$, which implies that every rank function h of a polymatroid is *non-decreasing*, and, therefore, non-negative. The requirement $0 \leq \Delta h(X, Y|Z)$ for any triplet $(X, Y|Z)$ of pairwise disjoint subsets of N then means that h is *submodular*, that is, $h(I) + h(J) \geq h(I \cup J) + h(I \cap J)$ for any $I, J \subseteq N$. Conversely, given three arbitrary sets $X, Y, Z \subseteq N$, the equality

$$\begin{aligned} \Delta(X, Y|Z) &= \\ &\Delta(A, BC|Z) + \Delta(B, C|AZ) + \Delta(C, C|ABZ) \\ &\text{with } A := X \setminus YZ, B := Y \setminus XZ, C := (X \cap Y) \setminus Z, \end{aligned}$$

allows one to show that any non-decreasing submodular function h satisfying $h(\emptyset) = 0$ defines a polymatroid; this relates our definition above to the common one from [8, § 2.2]. The concept itself can be viewed as a generalization of the concept of a matroid. Indeed, by [25, Corollary 1.3.4], an integer-valued set functions $h : \mathcal{P}(N) \rightarrow \mathbb{Z}$ is known to be a rank function of a *matroid* if it is non-decreasing, submodular and bounded by cardinality: if $I \subseteq N$ then $0 \leq h(I) \leq |I|$.

Polymatroids can also be assigned abstract CI structures. Specifically, given a rank function $h : \mathcal{P}(N) \rightarrow \mathbb{R}$ of a polymatroid (over N) we define

$$\begin{aligned} X \perp\!\!\!\perp Y | Z [h] &:= \Delta h(X, Y|Z) = 0 \\ &\text{for any triplet } (X, Y|Z) \text{ of subsets of } N. \end{aligned}$$

The following observation easily follows from the definition.

Lemma 2: The CI structure induced by a polymatroid is a semi-graphoid.

Proof. The fact $\Delta(\emptyset, Y|Z) = 0$ gives (S:0) while $\Delta(X, Y|Z) = \Delta(Y, X|Z)$ gives (S:1). Given a rank function $h : \mathcal{P}(N) \rightarrow \mathbb{R}$ of a polymatroid, the relation $\Delta h(X, YZ|U) = \Delta h(X, Y|ZU) + \Delta h(X, Z|U)$ together with non-negativity of the involved terms implies (S:2). \square

F. Entropy function

Given a discrete random variable ξ with a sample space \mathbf{X} , whose distribution is given by a density $p : \mathbf{X} \rightarrow [0, 1]$, its *entropy* $H(\xi)$ is given by the formula

$$H(\xi) := - \sum_{x \in \mathbf{X}: p(x) > 0} p(x) \cdot \ln(p(x)).$$

It is clearly a non-negative real number. Thus, every discrete random vector $\xi = [\xi_i]_{i \in N}$ can be assigned its *entropy function* $h_\xi : \mathcal{P}(N) \rightarrow [0, \infty)$ defined by

$$h_\xi(A) := H(\xi_A) \quad \text{for every } A \subseteq N.$$

Lemma 3: Given a discrete random vector ξ over N , the entropy function h_ξ is the rank function of a polymatroid. Moreover, for every ordered triplet $(X, Y|Z)$ of subsets of N one has

$$\xi_X \perp\!\!\!\perp \xi_Y | \xi_Z \Leftrightarrow \Delta h_\xi(X, Y|Z) = 0 \Leftrightarrow X \perp\!\!\!\perp Y | Z [h_\xi]. \quad (4)$$

In particular, the CI structure induced by ξ is a semi-graphoid.

Proof. Elementary information-theoretical inequalities, see [41, Appendix 14.A], imply that the entropy function h_ξ is a rank function of a polymatroid. The relation (4) then follows from the fact that the value $\Delta h_\xi(X, Y|Z)$ is exactly the so-called *conditional mutual information* between ξ_X and ξ_Y given ξ_Z . This quantity is known to vanish just in case of the validity of the CI statement; see [41, Theorem 2.34] or [38, Corollary 2.2]. The rest follows from Lemma 2. \square

Given discrete probability distributions Q and R on some sample space \mathbf{X} , with respective densities q and r , we say that Q is *absolutely continuous* with respect to R if $r(x) = 0$ implies $q(x) = 0$ for any $x \in \mathbf{X}$. We might alternatively say that R *dominates* Q or that Q is *dominated* by R . If this is the case then one can define the *Kullback-Leibler divergence* of Q with respect to R by the formula

$$D(Q \| R) := \sum_{x \in \mathbf{X}: q(x) > 0} q(x) \cdot \ln \frac{q(x)}{r(x)}.$$

Well-known facts are that $D(Q \| R) \geq 0$ and the equality holds iff $Q = R$ [41, Theorem 2.31]. Observe that, given a probability distribution P over N and pairwise disjoint sets $A, B, C \subseteq N$ with $A \neq \emptyset \neq B$, the conditional product \bar{P} of the marginals of P for AC and BC dominates the (original) distribution P . The Kullback-Leibler divergence $D(P \| \bar{P})$ is then the respective conditional mutual information.

G. Ingleton expression in different forms

Another important quantity exploited in this paper is the expression defining the so-called Ingleton inequality, discussed in more details in Section III-B. We are going to call that quantity (the) *Ingleton expression* and introduce a special symbol for it, following the notation from [19].

Given a real set functions $h : \mathcal{P}(N) \rightarrow \mathbb{R}$ and four *pairwise disjoint* subsets $X, Y, Z, U \subseteq N$ of the basic set N , we introduce another special shorthand

$$\begin{aligned} \square h(X, Y) &:= -h(XY) \\ &+ h(XZ) + h(XU) + h(YZ) + h(YU) + h(ZU) \\ &- h(Z) - h(U) - h(XZU) - h(YZU) \end{aligned} \quad (5)$$

to denote the respective Ingleton expression for $(X, Y|Z, U)$. Note that a more appropriate notation would be $\square h(X, Y|Z, U)$ because the expression (5) does depend on sets Z and U . Nevertheless, we will solely use this notation in a situation when the sets $X, Y, Z, U \subseteq N$ are fixed and no misunderstanding can occur. Observe that (5) is invariant relative to mutual exchanges $X \leftrightarrow Y$ and $Z \leftrightarrow U$. Like in case of the difference expression the symbol of the function h might be omitted in order to emphasize that (5) defines a functional $\square(X, Y) : h \mapsto \square h(X, Y|Z, U)$ on $\mathbb{R}^{\mathcal{P}(N)}$.

The point is that the expression (5) has a number of different forms, which were named, somewhat figuratively, “masks” in [19, § 4]. Note that only five “masks” were mentioned in [19, § 4] and are recalled in Lemma 4 below but thanks to the invariance of (5) relative to $X \leftrightarrow Y$ and $Z \leftrightarrow U$ one can recognize even 14 different forms of this expression. In fact, besides those 14 basic forms, there are further possible re-writings which have six difference terms.

Lemma 4: Given four pairwise disjoint subsets X, Y, Z, U of the basic set N the Ingleton expression defined in (5) has the following different forms:

$$\begin{aligned} \text{(M.1)} \quad \square(X, Y) &= \Delta(Z, U|X) + \Delta(Z, U|Y) + \Delta(X, Y|\emptyset) - \Delta(Z, U|\emptyset), \\ \text{(M.2)} \quad \square(X, Y) &= \Delta(Z, U|Y) + \Delta(X, Z|U) + \Delta(X, Y|\emptyset) - \Delta(X, Z|\emptyset), \\ \text{(M.3)} \quad \square(X, Y) &= \Delta(X, Y|Z) + \Delta(X, Z|U) + \Delta(Z, U|Y) - \Delta(X, Z|Y), \\ \text{(M.4)} \quad \square(X, Y) &= \Delta(X, Y|Z) + \Delta(X, Y|U) + \Delta(Z, U|XY) - \Delta(X, Y|ZU), \\ \text{(M.5)} \quad \square(X, Y) &= \Delta(X, Y|Z) + \Delta(X, Z|U) + \Delta(Z, U|XY) - \Delta(X, Z|YU). \end{aligned}$$

Proof. Easy verification of every form is left to the reader: substitute (3) into the right-hand side of it and, after canceling some terms, obtain (5). \square

H. Lattice of CI structures

A partially ordered set (\mathcal{Z}, \preceq) is called a *lattice* [2, § I.4] if every two-element subset of \mathcal{Z} has both the least upper bound, also named the supremum or the *join*, and the greatest lower bound, also named the infimum or the *meet*. A finite lattice is

necessarily *complete* which means that the requirement above holds for any subset of \mathcal{Z} . One of standard examples of a finite lattice is the *face-lattice* of a polyhedral cone [44, Theorem 2.7(v)]. A lattice (\mathcal{Z}, \preceq) is *anti-isomorphic* to a lattice (\mathcal{Z}', \preceq') if there is a one-to-one mapping ι from \mathcal{Z} onto \mathcal{Z}' which reverses the ordering: for $x, y \in \mathcal{Z}$, one has $x \preceq y$ iff $\iota(y) \preceq' \iota(x)$.

An element e in a lattice \mathcal{Z} is called *meet-irreducible* if it cannot be written as the infimum of two elements of \mathcal{Z} which are both different from e . In a finite lattice, every element can be written as the infimum of a set of meet-irreducible elements. Examples of meet-irreducible elements are the unique maximal element $\mathbf{1}$ in the lattice and its *sub-maximal* elements, called *co-atoms*. These are the elements $c \in \mathcal{Z}$ distinct from $\mathbf{1}$ such that the only elements $e \in \mathcal{Z}$ satisfying $c \preceq e$ are $e = c$ and $e = \mathbf{1}$. On the other hand, a finite lattice can have additional meet-irreducible elements besides those mentioned above.

Recall from Section II-B that discrete probabilistic CI structures over N are naturally ordered *by inclusion* (of involved ordered triplets of subsets of N). The point is that they form a complete lattice relative to this ordering. This is because the *intersection* of two discrete probabilistic CI structures over N is a discrete probabilistic CI structure over N , which fact follows from the following construction. Given densities $q : \mathbf{Y}_N \rightarrow [0, 1]$ and $r : \mathbf{Z}_N \rightarrow [0, 1]$ of discrete probability distributions Q and R over N one can put

$$p([y, z]) := q(y) \cdot r(z) \quad \text{for any } [y, z] \in \mathbf{Y}_N \times \mathbf{Z}_N,$$

which defines the density of a probability distribution P over N with individual sample spaces $\mathbf{X}_i := \mathbf{Y}_i \times \mathbf{Z}_i$ for any $i \in N$. The CI structure induced by P appears to be the intersection of CI structures induced by Q and R . The fact that CI structures are closed under intersection allows one to characterize them by means of meet-irreducible elements in the lattice of these structures.

III. OVERVIEW OF RELATED FORMER RESULTS

This section, recalling earlier findings relevant to the topic of study, can be skipped without losing understanding of the rest of the paper. To interpret geometrically some of the notions concepts from polyhedral geometry are used that are not defined here; definitions can be found in books on this topic [30], [44].

A. Representations of polymatroids

Matroid theory was introduced already in the 1930s [40] as an abstract theory of independence inspired by the concepts of independence emerging in linear algebra and other fields. There is a number of crypto-equivalent definitions of the concept of a matroid in sense that the equivalence is not apparent (at first glance) and some transitional constructions are needed; see [25] or [30, Chapter 39] for details. One of the equivalent definitions is in terms of the rank function (of a matroid) given in Section II-E. Some of the matroids are *linearly representable* over a field \mathbb{F} , which means that they

are defined through linear independence relationships within a finite collection of vectors from a linear space over \mathbb{F} .

The concept of a *polymatroid* was introduced by Edmonds [7] in the early 1970s as a certain bounded polyhedron in the space \mathbb{R}^N whose defining inequalities correspond to subsets of N . Tight upper bounds for the inequalities then define the values of the respective rank function, determining the polyhedron uniquely. The terminology was motivated by the fact that this concept generalizes the concept of an “independent set polytope” for a matroid [30, §40.2]. Later authors dealing with polymatroids [8, §2.2], however, found it to be more appropriate to define polymatroids in terms of their rank functions instead; we have done so in Section II-E as well. One can extend the concept of linear representability (from matroids) to polymatroids whose rank functions are integer-valued [8, p. 30].

One can distinguish different forms of probabilistic representability for a polymatroid; most of definitions below were inspired by Matúš [17], [22]. Let us say that a polymatroid over N with a rank function $h \in \mathbb{R}^{\mathcal{P}(N)}$ is

- *strongly probabilistically representable* if there exists a constant $c > 0$ and a discrete random vector ξ over N such that $c \cdot h(S) = h_\xi(S)$ for any $S \subseteq N$,
- (strongly) *asymptotically probabilistically representable* if there exists a constant $c > 0$ and a sequence of discrete random vectors ξ_n over N such that one has $c \cdot h(S) = \lim_{n \rightarrow \infty} h_{\xi_n}(S)$ for any $S \subseteq N$,
- *probabilistically representable* if there exists a discrete random vector ξ over N such that, for every triplet $(X, Y|Z)$ of subsets of N , one has

$$X \perp\!\!\!\perp Y | Z [h] \Leftrightarrow X \perp\!\!\!\perp Y | Z [\xi],$$

- *weakly probabilistically representable* if there exists a discrete random vector ξ over N such that, for every triplet $(X, Y|Z)$ of *pairwise disjoint* subsets of N ,

$$X \perp\!\!\!\perp Y | Z [h] \Leftrightarrow X \perp\!\!\!\perp Y | Z [\xi].$$

It is immediate that strong probabilistic representability implies the asymptotic one; by Lemma 3, it also implies the remaining weaker versions.

A classic result by Matúš [15, Theorem 2] says that every *matroid* which is *linearly representable* over a *finite* field \mathbb{F} is also strongly probabilistically representable; that particular construction of his was based on the assumption of the finiteness of the field \mathbb{F} . The same method can be used to show that this implication holds also for (integer-valued) polymatroids [26, Theorem 1.6.2]. Note in this context that it follows from [25, Corollary 6.8.13] that any matroid which is linearly representable over a field is also linearly representable over a finite field. Therefore, the assumption that the field \mathbb{F} is finite can be omitted.

There is also a concept of (finite) *group representability* of a polymatroid over N , defined in [41, §16.2], and any polymatroid which has a group representation is strongly probabilistically representable [4].

To give geometric interpretation to probabilistic representability concepts let us recall a few basic facts on the

cone $\mathcal{H}(N)$ of rank functions $h \in \mathbb{R}^{\mathcal{P}(N)}$ of polymatroids over N . It is a pointed polyhedral cone and its facets are given by inequalities $\Delta h(i, j|K) \geq 0$ for distinct $i, j \in N$, $K \subseteq N \setminus \{i, j\}$, and by inequalities $\Delta h(i, i|N \setminus i) \geq 0$ for $i \in N$. This means that the facets of the cone correspond to elementary triplets for representation of an augmented abstract CI structure; see Section II-D. In particular, every *face* F of $\mathcal{H}(N)$ can be identified with an *augmented abstract CI structure*, determined by the list of elementary triplets for facets containing F .

The facets of $\mathcal{H}(N)$ specified by equalities $\Delta h(i, i|N \setminus i) = 0$ for $i \in N$ are quite large. In fact, there is only one extreme ray of $\mathcal{H}(N)$ not contained in such a facet, which is the zero-one indicator $v^{\uparrow i}$ of supersets of $\{i\}$. Let us say that a polymatroid over N is *tight* if its rank function h satisfies $\Delta h(i, i|N \setminus i) = 0$ for any $i \in N$. Thus, the set $\hat{\mathcal{H}}(N)$ of rank functions of tight polymatroids over N is a face of $\mathcal{H}(N)$ whose extreme rays are the extreme rays of $\mathcal{H}(N)$ with the exception of $|N|$ rays generated by $v^{\uparrow i}$ for $i \in N$. This is because every $h \in \mathcal{H}(N)$ can be assigned its tightened version $\hat{h} \in \hat{\mathcal{H}}(N)$ defined by $\hat{h}(S) := h(S) - \sum_{i \in N} \Delta h(i, i|N \setminus i) \cdot v^{\uparrow i}(S)$ for $S \subseteq N$. The facets of $\hat{\mathcal{H}}(N)$ are given by inequalities $\Delta h(i, j|K) \geq 0$ for distinct $i, j \in N$, $K \subseteq N \setminus \{i, j\}$ and, thus, correspond to elementary triplets for representation of a standard abstract CI structure; see Section II-D. In particular, every *face* of $\hat{\mathcal{H}}(N)$ can be identified with a *standard abstract CI structure*.

The first two concepts of probabilistic representability of a polymatroid with a rank function h concern the *ray generated by* h . The strong representability means that the relative interior of that ray contains an entropy function; the asymptotic representability means that it contains a limit of entropy functions. The probabilistic representability concerns the *face of* $\mathcal{H}(N)$ *generated by* h , which is the least face F of $\mathcal{H}(N)$ containing h . It is the requirement that the relative interior of F contains an entropy function. The weak probabilistic representability concerns the *face* \hat{F} of $\hat{\mathcal{H}}(N)$ *generated by* \hat{h} , the tightened version of h . It is the requirement that the relative interior of the face \hat{F} contains a tightened version of an entropy function.

Remark 1: The reader may be interested in a question what are the extreme rays of the cone $\mathcal{H}(N)$. As explained above, this question is equivalent to the task what are the extreme rays of $\hat{\mathcal{H}}(N)$. It follows from the fact that $\mathcal{H}(N)$ is defined by inequalities with rational coefficients that every extreme ray of $\mathcal{H}(N)$ is generated by an integer-valued rank function. There is a way to recognize the extremity in $\mathcal{H}(N)$. Each function $h \in \mathcal{H}(N)$ can be identified with its *base polyhedron* $B(h)$ [8, §2.2]. Note in this context that the base polyhedron $B(h)$ is *not* the original “polymatroid” polyhedron introduced by Edmonds [7], which is named the *independence polyhedron* in [8, §2.2]: the relation is that $B(h)$ is a certain face of the latter polyhedron. In a 2016 paper [39] an easy criterion was given which allows one to test on basis of $B(h)$ whether the function h generates an extreme ray of $\mathcal{H}(N)$. Specifically, it leads to solving a certain simple linear equation system determined by (the vertices of) $B(h)$. Note, however, that the paper [39] is

primarily devoted to supermodular functions, which are mirror images of submodular functions. The point is that the cone $\hat{\mathcal{H}}(N)$ of rank functions for tight polymatroids is isomorphic to the cone of (suitably) standardized supermodular functions. The class of base polyhedra for polymatroids then coincides with the class of polytopes that are known as “cores” of supermodular (= convex) games. The same class of polytopes is also known as the class of *generalized permutohedra* [29].

B. CI structures over four discrete variables

Here we describe in more detail the methodological approach from [19], [20], [21]. The basic idea was the embedding $\xi \mapsto h_\xi$ of discrete random vectors over N into the cone $\mathcal{H}(N)$; see Section II-F.

The starting conjecture (of two of us), which holds in case $|N| = 3$, was that every $h \in \mathcal{H}(N)$ is a multiple of some entropy function. To verify that it would be enough, thanks to the construction in Section II-H, to find, for every extreme ray R of $\mathcal{H}(N)$, a discrete random vector ξ over N with h_ξ generating R . Matúš found the extreme rays of $\mathcal{H}(N)$ in case $|N| = 4$ in a previous paper of his [18, §5]: there are 41 of them and they break into 11 permutational types.

We found the desired probabilistic constructions for 10 permutational types [19, §5] and were stuck with the last permutational type containing 6 rays. Note in this context that all these 35 rays, for which we found the constructions, are generated by integer-valued rank functions linearly representable over finite fields. Thus, the existence of their (strong) probabilistic representations could also be derived from results on linearly representable polymatroids [15], [26] mentioned in Section III-A. In the Appendix, Section B, we give 9 of these constructions, namely those for tight polymatroids.

The breakthrough was an observation by Matúš that the last permutational type is not strongly probabilistically representable [17, §7]. The motivational source for that observation was his perception that the rank function

$$h_{xy}(S) := \begin{cases} 0 & \text{for } S = \emptyset, \\ 4 & \text{for } S = xy \text{ and } S = N, \\ |S| + 1 & \text{for other } S \subseteq N, \end{cases}$$

where $\{x, y\} \subset N$, $|N| = 4$, generating a ray of the last type, can be obtained by coarsening from the rank function of the simplest *non-linear matroid*, the so-called *Vámos cube*, defined on an 8-element basic set. The observation from [17, Lemma 1] that h_{xy} has no strong probabilistic representation was based on a derived CI property which involves functional dependences; therefore, it does not exclude the (pertinent) existence of a weak probabilistic representation for h_{xy} . The conclusion that h_{xy} has no weak probabilistic representation, however, follows from standard CI implications found in [36, §5] on basis of [17, Lemma 1].

Another argument for linear non-representability of h_{xy} is that it does not satisfy the *Ingleton inequality* $\square h_{xy}(x, y) \geq 0$. This special inequality was published in 1971: Ingleton [9] showed that the rank function of any linearly representable *matroid* over N , $|N| = 4$, must comply with it. An interesting geometric observation [19, Lemma 4.1] is that the sub-cone

of $\mathcal{H}(N)$ demarcated by adding six versions of Ingleton inequality has 35 extreme rays, namely those rays of $\mathcal{H}(N)$ for which the probabilistic representation was found. This led us to a revised conjecture that the sub-cone defined by adding Ingleton inequalities to those for $\mathcal{H}(N)$ determines all probabilistic CI structures over N , that is, probabilistic and linear representability coincide in case of 4 variables.

The revised conjecture appeared not to be true: we found four examples of probability distributions whose induced entropy functions do not satisfy the Ingleton inequality; see Examples 1-4 in Section IV-B. Thus, we got examples of probabilistically representable polymatroids that are not linearly representable. Matúš then continued in his laborious analysis of numerous remaining cases of “un-decided” abstract CI structures. He obtained them on basis of a more detailed geometric analysis of the cone $\mathcal{H}(N)$ from [19, §6]. He found many additional CI implications in the next paper [20] by combining various methods but stuck in 1995 with a couple of undecided cases. A breakthrough came in 1997 when Zhang and Yeung [42] published their first conditional information inequality. Matúš found out that he is able to settle one of his remaining cases by deriving a CI implication as a consequence of their inequality. Moreover, in [21, Proposition 2.1] he proved the second conditional information inequality and solved the last case by deriving the last CI implication.

C. Information inequalities

In 1998 Zhang and Yeung [43] found the first unconstrained linear inequality for the entropy function which is not implied by the inequalities defining $\mathcal{H}(N)$ and showed that the set of limits of entropy functions is closed convex cone. Thus, they gave the first negative response to a general question raised by Pippenger [28] in 1986: what are the “laws of information theory”, specifically whether classic Shannon inequalities characterize entropy functions. In 2007 then Matúš [23] showed that the cone of limits of entropy functions is not polyhedral if $|N| \geq 4$, which means there is an infinite number of unconstrained information inequalities (= linear inequalities valid for entropy functions).

The interest in conditional (= constrained) information inequalities has been restored in the 2010s when Kaced and Romashchenko [10] started to study these inequalities from a theoretical point of view. Besides the proofs of several new inequalities they proposed to classify these inequalities. Some of the conditional information inequalities can be derived from unconstrained ones, which means they are essentially unconstrained. Kaced and Romashchenko, however, showed that two former conditional information inequalities from [42], [21] and their own new inequalities are *essentially conditional*, which means they cannot be derived from unconstrained linear information inequalities.

They also introduced more detailed classification of essentially conditional inequalities: some of them hold solely for entropy functions and some of them hold even for limits of entropy functions. By a special evidence technique they showed that most of (their) new inequalities are valid for limits of entropy functions. On the other hand, they gave examples

that two discussed essentially conditional inequalities need not hold for limits of entropy functions; the first conditional information inequality [42] is one of them.

IV. CONDITIONAL INGLETON INEQUALITIES

In this section we present sufficient conditions in terms of CI for the validity of Ingleton inequality, give a few counter-examples to its general probabilistic validity and raise related open questions.

A. Sufficient conditions

Our main theoretical result offers five conditions ensuring the validity of Ingleton inequality; to fix the context we consider the case $\square(X, Y) \geq 0$.

Theorem 1: Given the entropy function h induced by a discrete random vector over N , the next implications hold:

- [1cI] $\Delta h(X, Y|\emptyset) = 0 = \Delta h(X, Y|Z) \Rightarrow \square h(X, Y) \geq 0$,
- [2cI] $\Delta h(X, Y|Z) = 0 = \Delta h(Y, U|Z) \Rightarrow \square h(X, Y) \geq 0$,
- [3cI] $\Delta h(X, Z|U) = 0 = \Delta h(X, U|Z) \Rightarrow \square h(X, Y) \geq 0$,
- [4cI] $\Delta h(X, Z|U) = 0 = \Delta h(Z, U|X) \Rightarrow \square h(X, Y) \geq 0$,
- [5cI] $\Delta h(X, Z|U) = 0 = \Delta h(Y, Z|U) \Rightarrow \square h(X, Y) \geq 0$.

Proof. This shown in the Appendix, Section A. \square

Because of the symmetry of the expression $\square h(X, Y)$ with respect to $X \leftrightarrow Y$ and $Z \leftrightarrow U$ the conditional Ingleton inequalities from Theorem 1 have altogether 14 possible forms; the inequalities [2cI] and [4cI] have four possible permuted versions while [1cI], [3cI], and [5cI] only two of them.

B. Counter-examples

To show that the premises for Ingleton inequality $\square h(X, Y) \geq 0$ in Theorem 1 are minimal possible ones one needs counter-examples to its general validity. Four of them are based on constructions of probability distributions having certain special CI structure; analogous constructions were formerly given in [20], [21], [37].

The first counter-example is loosely related to (M.1) form of $\square(X, Y)$.

Example 1: There exists a discrete random vector such that

$$[X \perp\!\!\!\perp Y | \emptyset \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | Y \ \& \ Z \perp\!\!\!\perp U | XY] \\ \not\Rightarrow \square(X, Y) \geq 0.$$

Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p : \begin{array}{ll} x & y & z & u \\ (0, 0, 0, 0) & \mapsto & 1/4 \\ (0, 1, 0, 1) & \mapsto & 1/4 \\ (1, 0, 0, 1) & \mapsto & 1/4 \\ (1, 1, 1, 1) & \mapsto & 1/4 \end{array}$$

with zero values for other configurations. The reader can easily check the validity of above CI statements. Using (M.1) in Lemma 4 one has $\square(X, Y) = -\Delta(Z, U|\emptyset) < 0$ because

$Z \not\perp\!\!\!\perp U | \emptyset$. The induced CI structure over N has 6 permutably equivalent versions.

The second counter-example is based on (M.2) form of the Ingleton expression $\square(X, Y)$.

Example 2: There exists a discrete random vector such that

$$[X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y \ \& \ Z \perp\!\!\!\perp U | XY] \\ \not\Rightarrow \square(X, Y) \geq 0.$$

To this end we put $N = \{x, y, z, u\}$ and define the density p of a binary random vector over N as follows:

$$p : \begin{array}{ll} x & y & z & u \\ (0, 0, 0, 0) & \mapsto & 1/4 \\ (0, 1, 1, 0) & \mapsto & 1/4 \\ (1, 0, 0, 1) & \mapsto & 1/4 \\ (1, 1, 0, 0) & \mapsto & 1/8 \\ (1, 1, 1, 0) & \mapsto & 1/8 \end{array}$$

with zero values for other configurations. The reader can check directly the validity of above CI statements. Using (M.2) in Lemma 4 one has $\square(X, Y) = -\Delta(X, Z|\emptyset) < 0$ because $X \not\perp\!\!\!\perp Z | \emptyset$. The induced CI structure over N has 24 permutably equivalent versions.

The third counter-example is related to (M.3) and (M.5) forms of $\square(X, Y)$.

Example 3: There exists a discrete random vector such that

$$[X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y \ \& \ Z \perp\!\!\!\perp U | XY] \\ \not\Rightarrow \square(X, Y) \geq 0.$$

We put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p : \begin{array}{ll} x & y & z & u \\ (0, 0, 0, 1) & \mapsto & 2/7 \\ (0, 0, 1, 1) & \mapsto & 1/7 \\ (0, 1, 1, 1) & \mapsto & 1/7 \\ (1, 0, 0, 1) & \mapsto & 1/7 \\ (1, 0, 1, 1) & \mapsto & 1/7 \\ (1, 1, 1, 0) & \mapsto & 1/7 \end{array}$$

with zero values for other configurations. The reader can directly verify the validity of above CI statements. Using (M.3) in Lemma 4 one has $\square(X, Y) = -\Delta(X, Z|Y) < 0$ as $X \not\perp\!\!\!\perp Z | Y$; by (M.5), alternatively, one has $\square(X, Y) = -\Delta(X, Z|YU) < 0$ since $X \not\perp\!\!\!\perp Z | YU$. The induced CI structure over N has 24 permutably equivalent versions.

The fourth counter-example is loosely related to (M.4) form of the Ingleton expression $\square(X, Y)$.

Example 4: There exists a discrete random vector such that

$$[X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Y | U \ \& \ Z \perp\!\!\!\perp U | X \\ \ \& \ Z \perp\!\!\!\perp U | Y \ \& \ Z \perp\!\!\!\perp U | XY] \not\Rightarrow \square(X, Y) \geq 0.$$

To this end we put $N = \{x, y, z, u\}$ and define the density p of a binary random vector over N as follows:

$$p : \begin{array}{ll} x & y & z & u \\ (0, 0, 0, 0) & \mapsto & 2/7 \\ (0, 1, 0, 0) & \mapsto & 1/7 \\ (0, 1, 1, 0) & \mapsto & 1/7 \\ (1, 0, 0, 0) & \mapsto & 1/7 \\ (1, 0, 0, 1) & \mapsto & 1/7 \\ (1, 1, 0, 0) & \mapsto & 1/7 \end{array}$$

with zero values for other configurations. The reader can directly verify the validity of above CI statements. Using (M.4) in Lemma 4 one has $\square(X, Y) = -\Delta(X, Y|ZU) < 0$ because $X \perp\!\!\!\perp Y | ZU$. The induced CI structure over N has 6 permutably equivalent versions.

The preceding examples allow one to get the following.

Corollary 5: The premises of all the implications from Theorem 1 are minimal.

Proof. No single premise $\Delta h(A, B|C) = 0$ there implies $\square h(X, Y) \geq 0$. \square

An important addition to Theorem 1 is the following claim (see later Remark 2).

Example 5: There exists a discrete random vector such that

$$[X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp U | Z] \not\Rightarrow \square(X, Y) \geq 0.$$

To show that we put $N = \{x, y, z, u\}$ and define the density p of a binary random vector over N as follows:

$x \ y \ z \ u$	$p :$		
(0, 0, 0, 0)	\mapsto	18/64	
(0, 1, 0, 0)	\mapsto	3/64	
(0, 1, 0, 1)	\mapsto	1/64	
(0, 1, 1, 0)	\mapsto	7/64	
(0, 1, 1, 1)	\mapsto	3/64	
(1, 0, 0, 0)	\mapsto	3/64	
(1, 0, 0, 1)	\mapsto	7/64	
(1, 0, 1, 0)	\mapsto	1/64	
(1, 0, 1, 1)	\mapsto	3/64	
(1, 1, 1, 1)	\mapsto	18/64	

with zero values for other configurations. It is easy to compute the respective marginal densities for XZU and YZU :

$x \ z \ u$	\mapsto	$y \ z \ u$	\mapsto	
(0, 0, 0)	\mapsto	21/64	\mapsto	21/64
(0, 0, 1)	\mapsto	1/64	\mapsto	7/64
(0, 1, 0)	\mapsto	7/64	\mapsto	1/64
(0, 1, 1)	\mapsto	3/64	\mapsto	3/64
(1, 0, 0)	\mapsto	3/64	\mapsto	3/64
(1, 0, 1)	\mapsto	7/64	\mapsto	1/64
(1, 1, 0)	\mapsto	1/64	\mapsto	7/64
(1, 1, 1)	\mapsto	21/64	\mapsto	21/64

and observe that $X \perp\!\!\!\perp Z | U$ and $Y \perp\!\!\!\perp U | Z$ (using the cross-product criterion). The goal is to show that the induced entropy function h satisfies $\square h(X, Y) < 0$. Note that two-dimensional marginals have a special form P_α with a density

$$p_\alpha : \begin{array}{ll} (0, 0) & \mapsto \frac{1}{4} \cdot (1 + \alpha) \\ (0, 1) & \mapsto \frac{1}{4} \cdot (1 - \alpha) \\ (1, 0) & \mapsto \frac{1}{4} \cdot (1 - \alpha) \\ (1, 1) & \mapsto \frac{1}{4} \cdot (1 + \alpha) \end{array} \quad \text{for some } \alpha \in [0, 1].$$

Specifically, one has $\alpha_{xy} = 1/8$, $\alpha_{xz} = \alpha_{yu} = 3/8$ and $\alpha_{zu} = 1/2$. Observe that the mutual information for the distribution P_α is as follows:

$$I(\alpha) := \frac{1}{2} \cdot [(1 + \alpha) \cdot \ln(1 + \alpha) + (1 - \alpha) \cdot \ln(1 - \alpha)].$$

In particular, $\Delta h(X, Y|\emptyset) = I(1/8)$, $\Delta h(X, Z|\emptyset) = \Delta h(Y, U|\emptyset) = I(3/8)$ and $\Delta h(Z, U|\emptyset) = I(1/2)$. This allows one to write the (16)-multiple of the Ingleton expression in the following form:

$$\begin{aligned} 16 \cdot \square h(X, Y) &\stackrel{(5)}{=} \underbrace{16 \cdot \Delta h(X, Z|U)}_{=0} + \underbrace{16 \cdot \Delta h(Y, U|Z)}_{=0} \\ &\quad + 16 \cdot \Delta h(X, Y|\emptyset) + 16 \cdot \Delta h(Z, U|\emptyset) \\ &\quad - 16 \cdot \Delta h(X, Z|\emptyset) - 16 \cdot \Delta h(Y, U|\emptyset) \\ &= 16 \cdot [I(1/8) + I(1/2) - 2 \cdot I(3/8)] \\ &= 9 \cdot \ln \frac{9}{8} + 7 \cdot \ln \frac{7}{8} + 12 \cdot \ln \frac{3}{2} + 4 \cdot \ln \frac{1}{2} \\ &\quad - 22 \cdot \ln \frac{11}{8} - 10 \cdot \ln \frac{5}{8} \\ &= 32 \cdot \ln(2) + 30 \cdot \ln(3) - 10 \cdot \ln(5) \\ &\quad + 7 \cdot \ln(7) - 22 \cdot \ln(11) \\ &\doteq -0.0876256 < 0. \end{aligned}$$

Hence, $\square h(X, Y) < 0$, which concludes the arguments. Note that the induced CI structure involves only 2 non-trivial statements $X \perp\!\!\!\perp Z | U$ and $Y \perp\!\!\!\perp U | Z$.

C. Remaining open tasks

First, let us recall the considerations leading to Theorem 1.

Remark 2: The simple question at the beginning was which CI assumptions imply the validity of Ingleton inequality $\square(X, Y) \geq 0$. Clearly, by Lemma 4, there are 14 single CI statements implying its validity, namely the ones whose respective terms are with “minus” in one of the 14 basic forms of the Ingleton expression. Thus, other possible CI assumptions for $\square(X, Y) \geq 0$ are subsets of the 10-element set of remaining CI statements composed of X, Y, Z, U .

The constructions from Examples 1-4 were known formerly [20], [21], [37]; these appear to be maximal CI assumptions which *do not imply* $\square(X, Y) \geq 0$. This led to the task to determine the minimal subsets of the above 10-element set of CI statements that are *not contained* in one of those non-implicators. These are 2-element sets falling into 6 permutational types (relative to $X \leftrightarrow Y$ and $Z \leftrightarrow U$). Five of them, reported in Theorem 1, appeared to imply $\square(X, Y) \geq 0$, while the sixth type not, as shown by Example 5.

Thus, Example 5 can be viewed as a counter-example to probabilistic validity of the sixth potential conditional Ingleton inequality. Nevertheless, it does not exclude its existence. Therefore, we ask the following.

Open question 1: Is there a set \mathcal{X} of CI statements such that $\{X \perp\!\!\!\perp Z | U, Y \perp\!\!\!\perp U | Z\} \subset \mathcal{X}$ and

$$\mathcal{X} \subseteq \{X \perp\!\!\!\perp Y | \emptyset, X \perp\!\!\!\perp Z | U, Y \perp\!\!\!\perp U | Z, Z \perp\!\!\!\perp U | XY\}$$

which implies the validity of $\square(X, Y) \geq 0$?

Note in this context that it follows from Theorem 1 and Example 5 that these are all the remaining potential CI implicators for $\square(X, Y) \geq 0$. Another couple of open problems is inspired by concepts and results from [10].

Open question 2: Is the new inequality [5cI] from Theorem 1 essentially conditional? Which of the inequalities [1cI]-[5cI] are valid for functions that are limits of entropy functions induced by discrete random vectors?

Remark that, by results from [10], the inequalities [1cI]-[4cI] are essentially conditional and [3cI]-[4cI] hold for limits of entropy functions.

V. CONDITIONAL INDEPENDENCE STRUCTURES REVISITED

In this section we apply the previously presented results to characterize (abstract properties of) CI structures induced by four discrete random variables.

A. CI equivalences

There are properties of (discrete) probabilistic CI structures which follow solely from the basic fact that every entropy function is a polymatroid (see Lemma 3). These properties can be viewed as two-way CI implications where one set of CI statements implies another set of CI statements and conversely.

Corollary 6: Every (standard) abstract CI structure over N induced by the rank function of a polymatroid is a semi-graphoid which complies with the following five conditions: given pairwise disjoint sets $X, Y, Z, U \subseteq N$, one has

$$\begin{aligned}
 \text{(E:1)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ X \perp\!\!\!\perp U | Y] \\
 \Leftrightarrow & [X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp Z | Y \ \& \ X \perp\!\!\!\perp U | Z], \\
 \text{(E:2)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp U | Y \ \& \ Y \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | X] \\
 \Leftrightarrow & [X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp U | Z \ \& \ Y \perp\!\!\!\perp Z | X \ \& \ Z \perp\!\!\!\perp U | Y], \\
 \text{(E:3)} \quad & [X \perp\!\!\!\perp Y | ZU \ \& \ X \perp\!\!\!\perp Z | \emptyset \ \& \ Y \perp\!\!\!\perp U | \emptyset \ \& \ Z \perp\!\!\!\perp U | XY] \\
 \Leftrightarrow & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | YU \ \& \ Y \perp\!\!\!\perp U | XZ \ \& \ Z \perp\!\!\!\perp U | \emptyset], \\
 \text{(E:4)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | ZU \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | Y] \\
 \Leftrightarrow & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Y | U \ \& \ Z \perp\!\!\!\perp U | \emptyset \ \& \ Z \perp\!\!\!\perp U | XY], \\
 \text{(E:5)} \quad & [X \perp\!\!\!\perp Y | ZU \ \& \ X \perp\!\!\!\perp U | Y \ \& \ Y \perp\!\!\!\perp Z | \emptyset \ \& \ Z \perp\!\!\!\perp U | X] \\
 \Leftrightarrow & [X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp U | YZ \ \& \ Y \perp\!\!\!\perp Z | X \ \& \ Z \perp\!\!\!\perp U | \emptyset].
 \end{aligned}$$

In particular, every (standard) probabilistic CI structure satisfies (E:1)-(E:5).

Proof. Lemma 2 says that the induced CI structure is a semi-graphoid. To verify the implication \Rightarrow in (E:1), write for a rank function $h : \mathcal{P}(N) \rightarrow \mathbb{R}$:

$$\begin{aligned}
 0 &= \Delta h(X, Y|Z) + \Delta h(X, Z|U) + \Delta h(X, U|Y) \\
 &= +h(XY) + h(XZ) + h(XU) \\
 &\quad + h(YZ) + h(YU) + h(ZU) \\
 &\quad - h(Y) - h(Z) - h(U) \\
 &\quad - h(XYZ) - h(XYU) - h(XZU) \\
 &= \Delta h(X, Y|U) + \Delta h(X, Z|Y) + \Delta h(X, U|Z)
 \end{aligned}$$

and deduce from non-negativity of involved difference terms that they have to vanish. The opposite implication \Leftarrow in (E:1) and also all other implications in (E:2)-(E:5) can be verified in an analogous way; this is left to the reader. The last claim then easily follows from the equivalence (4) in Lemma 3. \square

The CI equivalences from Corollary 6, including the properties defining a semi-graphoid, appear to be all CI equivalences which effectively apply in case four random variables. Note, however, that one can derive many further valid CI equivalences in the same way in case five and more discrete variables; one can even use computers for this purpose [3].

Remark 3: This is to commemorate the occurrence of the properties from Corollary 6 in the literature. The condition (E:4) appeared as (A.3) in [34] as the first ever CI property which does not follow from semi-graphoid axioms. The conditions (E:1)-(E:5) were all formulated in [36] as properties (A.3)-(A.7) of the so-called ‘‘structural’’ semi-graphoids discussed there; note that one can show using [38, § 5.3] that ‘‘structural’’ semi-graphoids coincide with standard CI structures induced by polymatroids. On the other hand, the conditions (E:1)-(E:5) were not mentioned in [19], [20], [21]; they are, however, implicit in the concept of a ‘‘semi-matroid’’ defined there, which concept corresponds to an augmented CI structure induced by a polymatroid.

B. CI implications

Here we apply the conditional Ingleton inequalities from Theorem 1 to derive CI implications valid for discrete random vectors.

Corollary 7: Every (standard) probabilistic CI structure induced by a discrete random vector over N complies with the following 19 conditions: given pairwise disjoint sets $X, Y, Z, U \subseteq N$, one has

$$\begin{aligned}
 \text{(I:1)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | Z \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow Z \perp\!\!\!\perp U | \emptyset, \\
 \text{(I:2)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow Z \perp\!\!\!\perp XU | \emptyset, \\
 \text{(I:3)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | \emptyset, \\
 \text{(I:4)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | U \ \& \ X \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp ZU | \emptyset, \\
 \text{(I:5)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | \emptyset, \\
 \text{(I:6)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | \emptyset, \\
 \text{(I:7)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp YZ | \emptyset, \\
 \text{(I:8)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | Y, \\
 \text{(I:9)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | Y, \\
 \text{(I:10)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ X \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | Y, \\
 \text{(I:11)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | Y, \\
 \text{(I:12)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | Y] \\
 & \Rightarrow X \perp\!\!\!\perp Z | Y, \\
 \text{(I:13)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Y | U \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp Y | ZU, \\
 \text{(I:14)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Y | U \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp YZ | U,
 \end{aligned}$$

$$\begin{aligned}
 \text{(I:15)} \quad & [X \perp\!\!\!\perp Y | \emptyset \ \& \ X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp Z | YU, \\
 \text{(I:16)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp Z | YU, \\
 \text{(I:17)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ X \perp\!\!\!\perp U | Z \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp Z | YU, \\
 \text{(I:18)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | X \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow X \perp\!\!\!\perp Z | YU, \\
 \text{(I:19)} \quad & [X \perp\!\!\!\perp Y | Z \ \& \ X \perp\!\!\!\perp Z | U \ \& \ Y \perp\!\!\!\perp Z | U \ \& \ Z \perp\!\!\!\perp U | XY] \\
 & \Rightarrow Z \perp\!\!\!\perp XY | U.
 \end{aligned}$$

Proof. In this proof, we will use, besides five conditional Ingleton inequalities from Theorem 1 in their basic forms [1cI], [2cI], ..., [5cI] written there, also alternative versions of two of them, namely

$$\begin{aligned}
 \text{[cI2]} \quad & \Delta h(X, Y|U) = 0 = \Delta h(X, Z|U) \Rightarrow \square h(X, Y) \geq 0, \\
 \text{[cI4]} \quad & \Delta h(Y, U|Z) = 0 = \Delta h(Z, U|Y) \Rightarrow \square h(X, Y) \geq 0,
 \end{aligned}$$

which can be obtained from [2cI] and [4cI] by the exchange $[X, Z] \leftrightarrow [Y, U]$. Each of 19 considered CI implications is derived from one of these 7 (versions of) conditional Ingleton inequalities using one of 5 forms (M.1), (M.2), ..., (M.5) of the Ingleton expression from Lemma 4.

The derivations are in terms of the entropy function h of a discrete random vector over $XYZU$ satisfying the premises of the respective CI implications. To describe them briefly we use special schematic records. Specifically, the record

$$\text{(I:1)} \quad \underbrace{\overbrace{(X, Y|\emptyset)} + \overbrace{(X, Y|Z)} + \underline{(Z, U|X)} + \underline{(Z, U|Y)}}_{\text{(M.1)} \quad (Z, U|\emptyset)}$$

will be used to encode the following reasoning for (I:1). Its premise means vanishing of four difference terms, encoded as the starting ones in the record:

$$\begin{aligned}
 \Delta h(X, Y|\emptyset) = 0, \quad \Delta h(X, Y|Z) = 0, \\
 \Delta h(Z, U|X) = 0, \quad \Delta h(Z, U|Y) = 0,
 \end{aligned}$$

and the goal is to verify vanishing the remaining difference term in the record, which is $\Delta h(Z, U|\emptyset) = 0$ in this case. One can use [1cI] inequality, which assumes vanishing two terms $\Delta h(X, Y|\emptyset) = 0 = \Delta h(X, Y|Z)$, indicated by overbracing them in the record, and says that $\square h(X, Y) \geq 0$. Then we use the (M.1) form of the Ingleton expression $\square h(X, Y)$, which step is indicated by underlining in the record. Since the underlined terms vanish the Ingleton inequality takes the form $-\Delta h(Z, U|\emptyset) = \square h(X, Y) \geq 0$. Nevertheless, the remaining difference term $\Delta h(Z, U|\emptyset)$ is non-negative and must vanish.

The procedure to verify (I:2) is analogous, but uses [4cI] instead,

$$\text{(I:2)} \quad \underbrace{\overbrace{(X, Y|\emptyset)} + \overbrace{(X, Z|U)} + \underline{\overbrace{(Z, U|X)}} + \underline{(Z, U|Y)}}_{\text{(M.1)} \quad (Z, U|\emptyset)}$$

with little extension: using the formula $\Delta(Z, U|\emptyset) + \Delta(X, Z|U) = \Delta h(Z, XU|\emptyset)$ yields a stronger conclusion $Z \perp\!\!\!\perp XU | \emptyset$.

The next bunch of CI implications is based on (M.2) form:

$$\begin{aligned}
 \text{(I:3)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[1cI2]}} + \overbrace{(X, Y|U)} + \underbrace{\overbrace{(X, Z|U)} + \underline{(Z, U|Y)}}_{\text{(M.2)} \quad (X, Z|\emptyset)} \\
 \text{(I:4)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[3cI]}} + \overbrace{(X, Z|U)} + \underbrace{\overbrace{(X, U|Z)} + \underline{(Z, U|Y)}}_{\text{(M.2)} \quad (X, Z|\emptyset)} \\
 \text{(I:5)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[cI4]}} + \underline{(X, Z|U)} + \underbrace{\overbrace{(Y, U|Z)} + \underline{\overbrace{(Z, U|Y)}}}_{\text{(M.2)} \quad (X, Z|\emptyset)} \\
 \text{(I:6)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[5cI]}} + \overbrace{(X, Z|U)} + \underbrace{\overbrace{(Y, Z|U)} + \underline{(Z, U|Y)}}_{\text{(M.2)} \quad (X, Z|\emptyset)}
 \end{aligned}$$

with an extension for (I:4): the formula $\Delta(X, Z|\emptyset) + \Delta(X, U|Z) = \Delta(X, ZU|\emptyset)$ yields a stronger conclusion $X \perp\!\!\!\perp ZU | \emptyset$.

Another groups of CI implications is based on (M.3) form:

$$\begin{aligned}
 \text{(I:7)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[1cI]}} + \overbrace{(X, Y|Z)} + \underbrace{\underline{(X, Z|U)} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)} \\
 \text{(I:8)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[2cI]}} + \underline{(X, Z|U)} + \underbrace{\overbrace{(Y, U|Z)} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)} \\
 \text{(I:9)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[cI2]}} + \overbrace{(X, Y|U)} + \underbrace{\underline{\overbrace{(X, Z|U)}} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)} \\
 \text{(I:10)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[3cI]}} + \overbrace{(X, Z|U)} + \underbrace{\overbrace{(X, U|Z)} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)} \\
 \text{(I:11)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[4cI]}} + \overbrace{(X, Z|U)} + \underbrace{\underline{\overbrace{(Z, U|X)}} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)} \\
 \text{(I:12)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[5cI]}} + \overbrace{(X, Z|U)} + \underbrace{\overbrace{(Y, Z|U)} + \underline{(Z, U|Y)}}_{\text{(M.3)} \quad (X, Z|Y)}
 \end{aligned}$$

with an extension for (I:7): $\Delta(X, Z|Y) + \Delta(X, Y|\emptyset) = \Delta(X, YZ|\emptyset)$ yields a stronger conclusion $X \perp\!\!\!\perp YZ | \emptyset$.

Two of CI implications are based on (M.4) form:

$$\begin{aligned}
 \text{(I:13)} \quad \underbrace{\overbrace{(X, Y|\emptyset)}}_{\text{[1cI]}} + \overbrace{(X, Y|Z)} + \underline{\overbrace{(X, Y|U)}} + \underline{\overbrace{(Z, U|XY)}}_{\text{(M.4)} \quad (X, Y|ZU)} \\
 \text{(I:14)} \quad \underbrace{\overbrace{(X, Y|Z)}}_{\text{[cI2]}} + \overbrace{(X, Y|U)} + \underline{\overbrace{(X, Z|U)}} + \underline{\overbrace{(Z, U|XY)}}_{\text{(M.4)} \quad (X, Y|ZU)}
 \end{aligned}$$

with an extension for (I:14): $\Delta(X, Y|ZU) + \Delta(X, Z|U) = \Delta(X, YZ|U)$ yields a stronger conclusion $X \perp\!\!\!\perp YZ | U$.

The last bunch of CI implications is based on (M.5) form:

$$(I:15) \quad \widehat{[1cl]} \quad \overbrace{(X, Y|\emptyset)} + \overbrace{(X, Y|Z)} + \overbrace{(X, Z|U)} + \overbrace{(Z, U|XY)} \\ \stackrel{(M.5)}{=} (X, Z|YU)$$

$$(I:16) \quad \widehat{[2cl]} \quad \overbrace{(X, Y|Z)} + \overbrace{(X, Z|U)} + \overbrace{(Y, U|Z)} + \overbrace{(Z, U|XY)} \\ \stackrel{(M.5)}{=} (X, Z|YU)$$

$$(I:17) \quad \widehat{[3cl]} \quad \overbrace{(X, Y|Z)} + \overbrace{(X, Z|U)} + \overbrace{(X, U|Z)} + \overbrace{(Z, U|XY)} \\ \stackrel{(M.5)}{=} (X, Z|YU)$$

$$(I:18) \quad \widehat{[4cl]} \quad \overbrace{(X, Y|Z)} + \overbrace{(X, Z|U)} + \overbrace{(Z, U|X)} + \overbrace{(Z, U|XY)} \\ \stackrel{(M.5)}{=} (X, Z|YU)$$

$$(I:19) \quad \widehat{[5cl]} \quad \overbrace{(X, Y|Z)} + \overbrace{(X, Z|U)} + \overbrace{(Y, Z|U)} + \overbrace{(Z, U|XY)} \\ \stackrel{(M.5)}{=} (X, Z|YU)$$

with an extension for (I:19): $\Delta(X, Z|YU) + \Delta(Y, Z|U) = \Delta(Z, XY|U)$ yields a stronger conclusion $Z \perp\!\!\!\perp XY | U$. \square

In the proof above we have derived each CI implication by combining two CI assumptions that imply Ingleton inequality with a suitable form of the Ingleton expression. Note in this context that such a combination need not be unique, some of those CI implications may have two alternative derivations which use different combinations of these two things.

The reader willing to commemorate former occurrence of the properties from Corollary 7 can find detailed information in the Appendix, Section C.

C. Sub-maximal CI structures

The largest CI structure over N is the one induced by a random vector over N whose components are stochastically independent random variables. In this section we discuss *sub-maximal CI structures* induced by 4 discrete random variables (see Section II-H for definitions). These appear to be closely related to the cone (of rank functions) of polymatroids satisfying all six versions of Ingleton inequality. More specifically, it was observed in [19, Lemma 4.1] that, in case $|N| = 4$, this pointed cone has 35 extreme rays falling into 10 permutational types. In our context of standard CI structures, however, one can limit the attention to the sub-cone of that cone specified by additional requirements $\Delta(i, i|N \setminus i) = 0$ for $i \in N$; this leads to excluding 4 extreme rays of 1 permutational type.

The polymatroids generating the extreme rays of the sub-cone mentioned above are linearly representable, and, therefore, by utilizing the results from [26], can be shown to be probabilistically representable. The induced CI structures then appear to be sub-maximal CI structures induced by 4 discrete random variables. To give the reader a complete picture we list representatives of 9 permutational types of these CI structures in the Appendix, Section B.

D. Overview: two complementary characterizations

In this section we summarize our findings on (standard) CI structures induced by 4 discrete random variables. Since these structures are semi-graphoids it follows from the facts in Section II-D that they can be identified with subsets of a

24-element set of (pairs of mutually equivalent) elementary triplets $(i, j|K)$ over N , $|N| = 4$ (see Lemma 1). Note in this context that the result of computations made in connection with [36] was that the number of (standard) semi-graphoids over N , $|N| = 4$, is 26 424. An even tighter upper approximation is the set of “structural” semi-graphoids over N (see Remark 3); their number is 22 108 [36]. The number of CI structures induced by 4 discrete random variables is, however, only 18 478, which is the result of computations made in connection with [31].

The class of CI structures is a lattice because the intersection of two CI structures is a CI structure (see Section II-H). This fact leads to two mutually complementary ways to characterize the CI structures, namely

- in terms of irreducible CI structures, and
- in terms of CI implications.

The first option is straightforward: to characterize CI structures over N , $|N| = 4$, it is enough to provide the list (of permutational types) of meet-irreducible CI structures over N . These appear to be

- the full CI structure (induced by independent random variables),
- the sub-maximal CI structures (= the co-atoms of the lattice), which are described in the Appendix, Section B,
- remaining meet-irreducible CI structures, which are just those presented in Examples 1-4 from Section IV-B.

Note that the irreducible CI structures of the third kind correspond to counter-examples to probabilistic validity of Ingleton inequality. Thus, altogether one has 92 irreducible discrete probabilistic CI structures over N , $|N| = 4$, and they break into 14 permutational types.

The second option is to describe minimal sets \mathcal{X} of (elementary) triplets over N that *are not* CI structures. Every such a set has uniquely determined CI closure: the fact that the intersection of CI structures is a CI structure implies the existence of the least CI structure \mathcal{Y} (over N) containing \mathcal{X} . One can interpret this as the claim that \mathcal{X} probabilistically implies $\mathcal{Y} \setminus \mathcal{X}$. Therefore, the above mentioned minimal sets \mathcal{X} correspond to CI implications/equivalences. One can distinguish three kinds of these CI properties in case $|N| = 4$:

- the semi-graphoid properties (S:0)-(S:2) in Section II-D,
- the CI equivalences (E:1)-(E:5) from Corollary 6,
- the CI implications (I:1)-(I:19) from Corollary 7.

Thus, altogether, one can recognize 27 abstract CI properties characterizing CI structures induced by 4 discrete random variables. The fact that both ways of description determine the same class of 18 478 (standard) abstract CI structures over N , $|N| = 4$, was verified by means of a computer [31].

VI. CONCLUSIONS

The principal message of the paper is that CI inference problem (for discrete probability distributions) can be solved in an elegant way by applying special conditional information inequalities. This was testified in case of four random variables and the question is whether the idea is applicable in general, for a higher number of random variables.

A new conditional Ingleton inequality was revealed in this paper and this leads to a few natural open tasks formulated in Section IV-C. Note in this context that conditional information inequalities have applications outside information theory. For example, (more general) conditional information inequalities can be used to obtain bounds for information ratios in the area of secure sharing (schemes) [1, § 3.2.6], have some group-theoretical counter-parts [1, § 3.2.4] and also counter-parts in context of Kolmogorov complexity [10, § 7]. One can even find surprising combinatorial applications for conditional Ingleton inequalities [11].

This paper has not dealt with augmented CI structures involving functional dependence statements. For this reason, the conditional Ingleton inequalities which have functional dependence premises allowed, as for example (I3) in [10], have been omitted. These inequalities can, however, possibly be used to derive (further) CI implications for the augmented probabilistic CI structures. Thus, one of future potential research directions is to (try to) characterize augmented CI structures induced by 4 discrete random variables by means of conditional information inequalities allowing functional dependence premises.

The interest in (algorithmic aspects of) constraints on entropy functions has recently been amplified in the context of database theory [1]. An interesting result from that paper, related to our topic of study, says that the CI inference problem (with a bounded number of variables) belongs to one of primitive class of decidable problems [1, Theorem 8]. The results presented in this paper support that claim from [1] and raise the hope in characterizing CI inference for a higher number of discrete random variables.

APPENDIX A PROOFS OF INEQUALITIES

We prove all five conditional Ingleton inequalities from Section IV here.

A. The first inequality

The first conditional Ingleton inequality appeared as [42, Theorem 3] but it was not immediately clear from its original formulation that it is, in fact, the Ingleton inequality. For sake of completeness we present a modified version of the original proof from [42, Section II]; it seems to be the simplest possible proof of this inequality from a methodological point of view.

Proposition 1: The first conditional Ingleton inequality is valid for any (discrete) entropy function h :

$$[1cI] \quad \Delta h(X, Y|\emptyset) = 0 = \Delta h(X, Y|Z) \Rightarrow \square h(X, Y) \geq 0.$$

Proof. Let P be a discrete probability distribution over $XYZU$ that satisfies both $X \perp\!\!\!\perp Y | \emptyset [P]$ and $X \perp\!\!\!\perp Y | Z [P]$, which is equivalent to the assumption that the entropy function h of P satisfies $\Delta h(X, Y|\emptyset) = 0 = \Delta h(X, Y|Z)$. We are going to show $\square h(X, Y) \geq 0$.

Let Q be the conditional product of marginals P_{XZU} and P_{YZU} (see Section II-C) and \bar{h} the entropy function of Q . Thus, P and Q have the same marginals for XZU and YZU while one has, moreover, $X \perp\!\!\!\perp Y | ZU [Q]$. The next step is to

define a probability distribution R over $XYZU$ which shares the (joint) sample space with P and Q . Specifically, its density r is given by

$$r(x, y, z, u) := \begin{cases} \frac{p(x, z) \cdot p(x, u) \cdot p(y, z) \cdot p(y, u)}{p(x) \cdot p(y) \cdot p(z) \cdot p(u)} & \text{if } p(x) \cdot p(y) \cdot p(z) \cdot p(u) > 0, \\ 0 & \text{otherwise,} \end{cases}$$

where x, y, z, u belong to the respective individual sample spaces and $p(x, z)$ denotes the value of the marginal density of P for XZ in the configuration $[x, z]$. Note that, in the definition of r , one can replace the used marginal densities $p(*)$ of P by the respective marginal densities $\bar{p}(*)$ of Q because they coincide. Our CI assumptions imply that r is a probability density:

$$\begin{aligned} & \sum_{x, y, z, u} r(x, y, z, u) \\ &= \sum_{x, y, z, u: p(x), \dots, p(u) > 0} \frac{p(x, z) \cdot p(x, u) \cdot p(y, z) \cdot p(y, u)}{p(x) \cdot p(y) \cdot p(z) \cdot p(u)} \\ & \stackrel{X \perp\!\!\!\perp Y | Z [P]}{=} \sum_{x, y, z, u: p(x), \dots, p(u) > 0} \frac{p(x, y, z) \cdot p(x, u) \cdot p(y, u)}{p(x) \cdot p(y) \cdot p(u)} \\ &= \sum_{x, y, u: p(x), p(y), p(u) > 0} \frac{p(x, u) \cdot p(y, u)}{p(x) \cdot p(y) \cdot p(u)} \cdot \underbrace{\sum_{z: p(z) > 0} p(x, y, z)}_{p(x, y)} \\ &= \sum_{x, y, u: p(x), p(y), p(u) > 0} \frac{p(x, u) \cdot p(y, u) \cdot p(x, y)}{p(x) \cdot p(y) \cdot p(u)} \\ & \stackrel{X \perp\!\!\!\perp Y | \emptyset [P]}{=} \sum_{x, y, u: p(x), p(y), p(u) > 0} \frac{p(x, u) \cdot p(y, u)}{p(u)} \\ &= \sum_{x, u: p(x), p(u) > 0} \frac{p(x, u)}{p(u)} \cdot \underbrace{\sum_{y: p(y) > 0} p(y, u)}_{p(u)} \\ &= \sum_{x, u: p(x), p(u) > 0} p(x, u) = 1. \end{aligned}$$

The definition of R also implies that Q is absolutely continuous with respect to R because $r(x, y, z, u) = 0$ implies $p(x, z) \cdot p(x, u) \cdot p(y, z) \cdot p(y, u) = 0$ and, hence, $\bar{p}(x, y, z, u) = 0$, where \bar{p} is the density of Q . It remains to verify that $\square h(X, Y) = D(Q \| R)$ to which goal we use $X \perp\!\!\!\perp Y | \emptyset [P]$

and $X \perp\!\!\!\perp Y | ZU [Q]$:

$$\begin{aligned}
 \square h(X, Y) &\stackrel{(M.1)}{=} \Delta h(Z, U|X) + \Delta h(Z, U|Y) \\
 &\quad + \underbrace{\Delta h(X, Y|\emptyset) - \Delta h(Z, U|\emptyset)}_{=0} \\
 &= \Delta \bar{h}(Z, U|X) + \Delta \bar{h}(Z, U|Y) - \Delta \bar{h}(Z, U|\emptyset) \\
 &= -\bar{h}(XZU) - \bar{h}(YZU) + \bar{h}(ZU) \\
 &\quad + \bar{h}(XZ) + \bar{h}(XU) + \bar{h}(YZ) + \bar{h}(YU) \\
 &\quad - \bar{h}(X) - \bar{h}(Y) - \bar{h}(Z) - \bar{h}(U) \\
 &= \sum_{x,y,z,u: \bar{p}(x,y,z,u) > 0} \bar{p}(x, y, z, u) \cdot \ln \frac{\bar{p}(x,z,u) \cdot \bar{p}(y,z,u)}{\bar{p}(z,u)} \\
 &\quad \frac{\bar{p}(x,z) \cdot \bar{p}(x,u) \cdot \bar{p}(y,z) \cdot \bar{p}(y,u)}{\bar{p}(x) \cdot \bar{p}(y) \cdot \bar{p}(z) \cdot \bar{p}(u)} \\
 &= \sum_{x,y,z,u: \bar{p}(x,y,z,u) > 0} \bar{p}(x, y, z, u) \cdot \ln \frac{\bar{p}(x, y, z, u)}{r(x, y, z, u)} \\
 &= D(Q \| R) \geq 0.
 \end{aligned}$$

Thus, the non-negativity of the Kullback-Leibler divergence implies the claim. \square

B. The second inequality

The second conditional Ingleton inequality appeared in [21, § 2]. Specifically, the proof of Proposition 2.1 in [21] contained both a hint to verify the first inequality from [42] and the arguments for the second inequality. We believe that our proof of the second inequality is much simpler than the original one.

Proposition 2: The second conditional Ingleton inequality is valid for any (discrete) entropy function h :

$$[2cI] \quad \Delta h(X, Y|Z) = 0 = \Delta h(Y, U|Z) \Rightarrow \square h(X, Y) \geq 0.$$

Proof. Let P be a probability distribution over $XYZU$ that satisfies both $X \perp\!\!\!\perp Y | Z [P]$ and $Y \perp\!\!\!\perp U | Z [P]$, which is equivalent to the assumption that the entropy function h of P satisfies $\Delta h(X, Y|Z) = 0 = \Delta h(Y, U|Z)$. We are going to show $\square h(X, Y) \geq 0$.

Let Q be the conditional product of marginals P_{YZ} and P_{XZU} and \bar{h} the entropy function of Q . Thus, P and Q have the same marginals for YZ and XZU while one, moreover, has $Y \perp\!\!\!\perp XU | Z [Q]$. Hence, $Y \perp\!\!\!\perp U | Z [Q]$ and the facts $P_{YZ} = Q_{YZ}$, $P_{ZU} = Q_{ZU}$ and $Y \perp\!\!\!\perp U | Z [P]$ imply $P_{YZU} = Q_{YZU}$. One can analogously derive $P_{XYZ} = Q_{XYZ}$ (exchange U and X). In particular, P and Q have the same marginals for XZU , YZU , and XY and it follows from the definition (5) of the Ingleton expression that $\square h(X, Y) = \square \bar{h}(X, Y)$. Therefore, it is enough to show $\square \bar{h}(X, Y) \geq 0$.

Nonetheless, $Y \perp\!\!\!\perp XU | Z [Q]$ implies $Y \perp\!\!\!\perp X | ZU [Q]$, which is equivalent to $\Delta \bar{h}(X, Y|ZU) = 0$. Analogously, $\Delta \bar{h}(X, Y|Z) = 0$ can be observed, although this particular observation is not necessary to draw our conclusion. Thus, one of the forms of the Ingleton expression from Lemma 4

$$\begin{aligned}
 \square \bar{h}(X, Y) &\stackrel{(M.4)}{=} \underbrace{\Delta \bar{h}(X, Y|Z)}_{=0} + \Delta \bar{h}(X, Y|U) \\
 &\quad + \Delta \bar{h}(Z, U|XY) - \underbrace{\Delta \bar{h}(X, Y|ZU)}_{=0} \\
 &= \Delta \bar{h}(X, Y|U) + \Delta \bar{h}(Z, U|XY)
 \end{aligned}$$

together with Shannon inequalities for \bar{h} imply that $\square \bar{h}(X, Y) \geq 0$. \square

C. The third inequality

A number of CI implications has been derived in [20, § 2] by a special technique of transforming the implication problem into a wider framework of σ -algebras and applying a special CI property for σ -algebras based on a construction of a certain “intersection” σ -algebra for two given σ -algebras. The idea behind this method is that random variables on a probability space $(\Omega, \mathcal{A}, \mathbf{P})$ can be identified with their induced sub- σ -algebras of \mathcal{A} ; yet another interpretation is possible in case of a finite Ω when the σ -algebras correspond to partitions of Ω .

In our case of finitely many discrete random variables, the construction of the “intersection” σ -algebra corresponds to a construction of a certain random variable on basis of two given random variables. The above special CI property for σ -algebras can equivalently be expressed as the property of the constructed random variable, which is formally done in the next Lemma 8. Note that this auxiliary result has already been formulated both in [10, Lemma 1] and in [14, Lemma 4], where it was named a “double Markov property”. Nevertheless, the result itself was known much earlier: it was already formulated in the form of an exercise under title “double Markovity” in [5, § 3.4, exercise 25].

Lemma 8: Every discrete random vector ξ over ABC satisfying $\xi_A \perp\!\!\!\perp \xi_B | \xi_C$ and $\xi_A \perp\!\!\!\perp \xi_C | \xi_B$ can be extended by a discrete random variable ξ_W to a random vector over $ABCW$ in which ξ_W is functionally dependent both on ξ_B and on ξ_C and, moreover, one has $\xi_A \perp\!\!\!\perp \xi_{BC} | \xi_W$.

Proof. Assume without loss of generality $A, B, C \neq \emptyset$ for otherwise one can take any constant random variable in place of ξ_W . Let P be the distribution of ξ on a joint finite sample space $A \times B \times C$ and p its density with strictly positive one-dimensional marginal densities on A , B , and C . Consider the support set $L := \{(b, c) \in B \times C : p_{BC}(b, c) > 0\}$ of the marginal distribution of P for BC equipped with a binary relation \sim defined by

$$(b, c) \sim (b', c') := [b = b' \text{ or } c = c']$$

and introduce an equivalence \approx on L as the transitive closure of \sim . Then the quotient set W of L by \approx (= the collection of equivalence classes for \approx) will be the individual sample space for ξ_W . Define the density \tilde{p} of the extended random vector over $ABCW$ as follows: given $(a, b, c, w) \in A \times B \times C \times W$,

$$\tilde{p}(a, b, c, w) := \begin{cases} p(a, b, c) & \text{if } p(a, b, c) > 0 \\ & \text{and } w \text{ contains } (b, c), \\ 0 & \text{otherwise.} \end{cases}$$

Given $b \in B$, the definition of \approx implies that all pairs $(b, c) \in L$ belong to the same equivalence class w of \approx . Thus, ξ_W functionally depends on ξ_B and an analogous argument implies that ξ_W functionally depends on ξ_C .

Realize that P can be viewed as a distribution on $A \times L$ and one can consider the conditional density

$$p_{A|BC}(a | b, c) := \frac{p(a, b, c)}{p(b, c)} \text{ defined for } a \in A \text{ and } (b, c) \in L.$$

The assumption $\xi_A \perp\!\!\!\perp \xi_B \mid \xi_C$ implies

$$p_{A|BC}(a|b, c) = \frac{p(a, c)}{p(c)} = p_{A|BC}(a|b', c)$$

whenever $a \in A$ and $(b, c), (b', c) \in L$. Analogously, the assumption $\xi_A \perp\!\!\!\perp \xi_C \mid \xi_B$ gives

$$p_{A|BC}(a|b, c) = p_{A|BC}(a|b, c')$$

whenever $a \in A$ and $(b, c), (b, c') \in L$. Hence, $p_{A|BC}(*|b, c) = p_{A|BC}(*|b', c')$ whenever $(b, c) \sim (b', c')$ and, by transitivity argument, $p_{A|BC}$ is constant on equivalence classes of \approx . Thus, having fixed an equivalence class $w \in W$, the conditional density $p_{A|BC}(*|b, c)$ does not depend on the choice of $(b, c) \in w \subseteq L$, which implies $\xi_A \perp\!\!\!\perp \xi_{BC} \mid \xi_W$. \square

The random variable ξ_W from the above proof is, in fact, defined by some equivalence \approx on $L \subseteq B \times C$. The particular definition of \approx from our proof corresponds to the construction of the ‘‘intersection’’ σ -algebra for σ -algebras induced by ξ_B and ξ_C ; note that it solely depends on the marginal of P on BC . Thus, our construction is universal relative to ξ_A in sense that one gets $\xi_A \perp\!\!\!\perp \xi_{BC} \mid \xi_W$ for *arbitrary* ξ_A satisfying $\xi_A \perp\!\!\!\perp \xi_B \mid \xi_C$ and $\xi_A \perp\!\!\!\perp \xi_C \mid \xi_B$.

Note in this context that the proof of an analogous result in [10, Appendix IX] was based on a slightly different, perhaps formally shorter, construction of an equivalence on L , which construction was, however, depending on the considered random variable ξ_A . Thus, its specific form was determined by the marginal of P on ABC . In particular, the equivalence on L from [10, Appendix IX] can be shown to be a coarsening of \approx from our proof of Lemma 8.

We now apply Lemma 8 to prove the third conditional Ingleton inequality which appeared in [10] as $(\mathcal{I}4')$. In fact, two proofs of this inequality were given there. The basic proof of it was more complicated because the goal was to prove that it is valid for any function which is a limit of (discrete) entropy functions. The second ‘‘direct’’ proof from [10, § III.C] was simpler because of easier task to prove that the inequality holds for entropy functions only. That simpler proof was based on an analogous idea as our proof below but it was different in technical details. We believe that our reasoning is more transparent.

Proposition 3: The third conditional Ingleton inequality is valid for any (discrete) entropy function h :

$$[3c1] \quad \Delta h(X, Z|U)=0 = \Delta h(X, U|Z) \Rightarrow \square h(X, Y) \geq 0.$$

Proof. Let P be a probability distribution over $XYZU$ that satisfies both $X \perp\!\!\!\perp Z \mid U [P]$ and $X \perp\!\!\!\perp U \mid Z [P]$, which is equivalent to the assumption that the entropy function h of P satisfies $\Delta h(X, Z|U) = 0 = \Delta h(X, U|Z)$. We are going to show $\square h(X, Y) \geq 0$.

We apply Lemma 8 to a random vector ξ over XZU having P_{XZU} as its distribution with $A := X$, $B := Z$ and $C := U$. It says there is an extended discrete random vector $\tilde{\xi}$ over $XZUW$ with a distribution \tilde{P} (having P_{XZU} as a marginal) such that the variable ξ_W functionally depends both on ξ_Z and on ξ_U and, moreover, $\xi_X \perp\!\!\!\perp \xi_{ZU} \mid \xi_W$. Let us introduce the

conditional product \hat{P} of distributions \tilde{P} over $XZUW$ and P over $XYZU$, that is, define an extended random vector $\hat{\xi}$ over $XYZUW$. By the construction, its entropy function \hat{h} is an extension of the entropy function h of P , one has $X \perp\!\!\!\perp ZU \mid W [\hat{P}]$ and $\hat{\xi}_W$ functionally depends both on $\hat{\xi}_Z$ and on $\hat{\xi}_U$.

To verify the conclusion we utilize the dependences $\hat{\xi}_W \leftarrow \hat{\xi}_Z$ and $\hat{\xi}_W \leftarrow \hat{\xi}_U$, which imply that $\hat{h}(T) = \hat{h}(TW)$ for any T containing either Z or U , the fact that the entropy function is non-decreasing, which gives $\hat{h}(XY) \leq \hat{h}(XYW)$, and $X \perp\!\!\!\perp Z \mid W [\hat{P}]$, which gives $\Delta \hat{h}(X, Z|W) = 0$:

$$\begin{aligned} \square h(X, Y) &\stackrel{(M.2)}{=} \Delta h(Z, U|Y) + \underbrace{\Delta h(X, Z|U)}_{=0} \\ &\quad + \Delta h(X, Y|\emptyset) - \Delta h(X, Z|\emptyset) \\ &= \Delta \hat{h}(Z, U|Y) + \Delta \hat{h}(X, Y|\emptyset) - \Delta \hat{h}(X, Z|\emptyset) \\ &= \hat{h}(YZ) + \hat{h}(YU) - \hat{h}(YZU) - \hat{h}(XY) \\ &\quad - \hat{h}(Z) + \hat{h}(XZ) \\ &= \hat{h}(YZW) + \hat{h}(YUW) - \hat{h}(YZUW) - \hat{h}(XY) \\ &\quad - \hat{h}(ZW) + \hat{h}(XZW) \\ &\geq \hat{h}(YZW) + \hat{h}(YUW) - \hat{h}(YZUW) - \hat{h}(XYW) \\ &\quad - \hat{h}(ZW) + \hat{h}(XZW) \\ &= \Delta \hat{h}(Z, U|YW) + \Delta \hat{h}(X, Y|W) - \underbrace{\Delta \hat{h}(X, Z|W)}_{=0} \\ &= \Delta \hat{h}(Z, U|YW) + \Delta \hat{h}(X, Y|W) \geq 0. \end{aligned}$$

Thus, the Shannon's inequalities for \hat{h} imply the desired conclusion. \square

D. The fourth inequality

Here we use an analogous method to verify the fourth conditional Ingleton inequality which appeared as $(\mathcal{I}5')$ in [10]. Its original proof was more intricate because the task was to prove its validity for functions which are limits of entropy functions. Our proof below is based on different simpler arguments.

Proposition 4: The fourth conditional Ingleton inequality is valid for any (discrete) entropy function h :

$$[4c1] \quad \Delta h(X, Z|U)=0 = \Delta h(Z, U|X) \Rightarrow \square h(X, Y) \geq 0.$$

Proof. Let P be a probability distribution over $XYZU$ that satisfies both $Z \perp\!\!\!\perp X \mid U [P]$ and $Z \perp\!\!\!\perp U \mid X [P]$, which is equivalent to the assumption that the entropy function h of P satisfies $\Delta h(X, Z|U) = 0 = \Delta h(Z, U|X)$. We are going to show $\square h(X, Y) \geq 0$.

We apply Lemma 8 to a random vector ξ over XZU having P_{XZU} as its distribution with $A := Z$, $B := X$ and $C := U$. It says there is an extended discrete random vector $\tilde{\xi}$ over $XZUW$ with a distribution \tilde{P} (having P_{XZU} as a marginal) such that the variable ξ_W functionally depends both on ξ_X and on ξ_U and, moreover, $\xi_Z \perp\!\!\!\perp \xi_{XU} \mid \xi_W$. Take the conditional product \hat{P} of distributions \tilde{P} over $XZUW$ and P over $XYZU$, that is, define an extended random vector $\hat{\xi}$ over $XYZUW$. Because of the construction, its entropy function \hat{h} is an extension of the entropy function h of P , one has

$Z \perp\!\!\!\perp XU | W [\hat{P}]$ and $\hat{\xi}_W$ functionally depends both on $\hat{\xi}_X$ and on $\hat{\xi}_U$.

To verify the inequality we use the dependences $\hat{\xi}_W \leftarrow \hat{\xi}_X$ and $\hat{\xi}_W \leftarrow \hat{\xi}_U$, which imply that $\hat{h}(T) = \hat{h}(TW)$ for any T containing either X or U , and $Z \perp\!\!\!\perp X | W [\hat{P}]$, which gives $\Delta \hat{h}(Z, X|W) = 0$:

$$\begin{aligned} \square h(X, Y) &\stackrel{(M.2)}{=} \Delta h(Z, U|Y) + \underbrace{\Delta h(X, Z|U)}_{=0} \\ &\quad + \Delta h(X, Y|\emptyset) - \Delta h(X, Z|\emptyset) \\ &= \Delta \hat{h}(Z, U|Y) + \Delta \hat{h}(X, Y|\emptyset) - \Delta \hat{h}(X, Z|\emptyset) \\ &= \hat{h}(YZ) + \hat{h}(YU) - \hat{h}(YZU) - \hat{h}(XY) \\ &\quad - \hat{h}(Z) + \hat{h}(XZ) \\ &= \hat{h}(YZ) + \hat{h}(YUW) - \hat{h}(YZUW) - \hat{h}(XYW) \\ &\quad - \hat{h}(Z) + \hat{h}(XZW) \\ &= \hat{h}(YUW) - \hat{h}(YZUW) - \hat{h}(XYW) + \hat{h}(YZ) \\ &\quad - \hat{h}(Z) + \hat{h}(XZW) \\ &= \Delta \hat{h}(Z, U|YW) + \Delta \hat{h}(X, Y|W) \\ &\quad + \Delta \hat{h}(Y, W|Z) - \underbrace{\Delta \hat{h}(Z, X|W)}_{=0} \\ &= \Delta \hat{h}(Z, U|YW) + \Delta \hat{h}(X, Y|W) + \Delta \hat{h}(Y, W|Z) \geq 0. \end{aligned}$$

Thus, the Shannon's inequalities for \hat{h} imply the desired conclusion. \square

E. The fifth inequality

Here we give the proof of the fifth conditional Ingleton inequality which is methodologically similar to the proof of the second inequality.

Proposition 5: The fifth conditional Ingleton inequality is valid for any (discrete) entropy function h :

$$[5cI] \quad \Delta h(X, Z|U) = 0 = \Delta h(Y, Z|U) \Rightarrow \square h(X, Y) \geq 0.$$

Proof. Let P be a probability distribution over $XYZU$ that satisfies both $Z \perp\!\!\!\perp X | U [P]$ and $Z \perp\!\!\!\perp Y | U [P]$, which is equivalent to the assumption that the entropy function h of P satisfies $\Delta h(X, Z|U) = 0 = \Delta h(Y, Z|U)$. We are going to show $\square h(X, Y) \geq 0$.

Let Q be the conditional product of marginals P_{XYU} and P_{ZU} and \bar{h} the entropy function of Q . Thus, P and Q have the same marginals for XYU and ZU while one, moreover, has $Z \perp\!\!\!\perp XY | U [Q]$. Hence, $Z \perp\!\!\!\perp X | U [Q]$ and the facts $P_{ZU} = Q_{ZU}$, $P_{XU} = Q_{XU}$ and $Z \perp\!\!\!\perp X | U [P]$ imply $P_{XZU} = Q_{XZU}$. Analogously, $P_{YZU} = Q_{YZU}$ (exchange X and Y). In particular, P and Q have the same marginals for XZU , YZU , and XY and it follows from the definition (5) of the Ingleton expression that $\square h(X, Y) = \square \bar{h}(X, Y)$. Therefore, it is enough to show $\square \bar{h}(X, Y) \geq 0$.

Nonetheless, $Z \perp\!\!\!\perp XY | U [Q]$ implies $Z \perp\!\!\!\perp X | YU [Q]$, which is equivalent to $\Delta \bar{h}(X, Z|YU) = 0$. Analogously, $\Delta \bar{h}(X, Z|U) = 0$ can be observed, although this particular

observation is not necessary to draw our conclusion. Thus, one of the forms of the Ingleton expression from Lemma 4

$$\begin{aligned} \square \bar{h}(X, Y) &\stackrel{(M.5)}{=} \Delta \bar{h}(X, Y|Z) + \underbrace{\Delta \bar{h}(X, Z|U)}_{=0} \\ &\quad + \Delta \bar{h}(Z, U|XY) - \underbrace{\Delta \bar{h}(X, Z|YU)}_{=0} \\ &= \Delta \bar{h}(X, Y|Z) + \Delta \bar{h}(Z, U|XY) \end{aligned}$$

together with Shannon inequalities for \bar{h} imply that $\square \bar{h}(X, Y) \geq 0$. \square

APPENDIX B SUB-MAXIMAL CI STRUCTURES

This is to recall basic constructions of discrete probability distributions over N , $|N| = 4$.

[I.]: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x \ y \ z \ u \\ (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}) \mapsto 1/2 \\ (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) \mapsto 1/2 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min \{ |S \cap \{x, y\}|, 1 \} \quad \text{for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 1 over $\{x, y\}$. The induced CI structure involves 20 (pairs of) elementary CI statements:

$$\begin{aligned} x \perp\!\!\!\perp z | \emptyset, \quad x \perp\!\!\!\perp u | \emptyset, \quad y \perp\!\!\!\perp z | \emptyset, \quad y \perp\!\!\!\perp u | \emptyset, \quad z \perp\!\!\!\perp u | \emptyset, \\ x \perp\!\!\!\perp z | y, \quad x \perp\!\!\!\perp z | u, \quad x \perp\!\!\!\perp u | y, \quad x \perp\!\!\!\perp u | z, \\ y \perp\!\!\!\perp z | x, \quad y \perp\!\!\!\perp z | u, \quad y \perp\!\!\!\perp u | x, \quad y \perp\!\!\!\perp u | z, \\ z \perp\!\!\!\perp u | x, \quad z \perp\!\!\!\perp u | y, \\ x \perp\!\!\!\perp z | yu, \quad x \perp\!\!\!\perp u | yz, \quad y \perp\!\!\!\perp z | xu, \quad y \perp\!\!\!\perp u | xz, \quad z \perp\!\!\!\perp u | xy. \end{aligned}$$

It has 6 permutably equivalent versions.

[II.]: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x \ y \ z \ u \\ (\mathbf{0}, \mathbf{0}, \mathbf{0}, \mathbf{0}) \mapsto 1/2 \\ (\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{0}) \mapsto 1/2 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min \{ |S \cap \{x, y, z\}|, 1 \} \quad \text{for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 1 over $\{x, y, z\}$. The induced CI structure involves 18 (pairs of) elementary CI statements:

$$\begin{aligned} x \perp\!\!\!\perp u | \emptyset, \quad y \perp\!\!\!\perp u | \emptyset, \quad z \perp\!\!\!\perp u | \emptyset, \\ x \perp\!\!\!\perp y | z, \quad x \perp\!\!\!\perp z | y, \quad x \perp\!\!\!\perp u | y, \quad x \perp\!\!\!\perp u | z, \\ y \perp\!\!\!\perp z | x, \quad y \perp\!\!\!\perp u | x, \quad y \perp\!\!\!\perp u | z, \quad z \perp\!\!\!\perp u | x, \quad z \perp\!\!\!\perp u | y, \\ x \perp\!\!\!\perp y | zu, \quad x \perp\!\!\!\perp z | yu, \quad x \perp\!\!\!\perp u | yz, \\ y \perp\!\!\!\perp z | xu, \quad y \perp\!\!\!\perp u | xz, \quad z \perp\!\!\!\perp u | xy. \end{aligned}$$

It has 4 permutably equivalent versions.

III.: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x y z u \\ (0, 0, 0, 0) \mapsto 1/2 \\ (1, 1, 1, 1) \mapsto 1/2 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min\{|S|, 1\} \text{ for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 1 over N . The induced CI structure involves 18 (pairs of) elementary CI statements:

$$\begin{array}{l} x \perp\!\!\!\perp y | z, x \perp\!\!\!\perp y | u, x \perp\!\!\!\perp z | y, x \perp\!\!\!\perp z | u, \\ x \perp\!\!\!\perp u | y, x \perp\!\!\!\perp u | z, y \perp\!\!\!\perp z | x, y \perp\!\!\!\perp z | u, \\ y \perp\!\!\!\perp u | x, y \perp\!\!\!\perp u | z, z \perp\!\!\!\perp u | x, z \perp\!\!\!\perp u | y, \\ x \perp\!\!\!\perp y | zu, x \perp\!\!\!\perp z | yu, x \perp\!\!\!\perp u | yz, \\ y \perp\!\!\!\perp z | xu, y \perp\!\!\!\perp u | xz, z \perp\!\!\!\perp u | xy. \end{array}$$

It has only 1 permutably equivalent version.

IV.: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x y z u \\ (0, 0, 0, 0) \mapsto 1/4 \\ (0, 1, 1, 0) \mapsto 1/4 \\ (1, 0, 1, 0) \mapsto 1/4 \\ (1, 1, 0, 0) \mapsto 1/4 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min\{|S \cap \{x, y, z\}|, 2\} \text{ for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 2 over $\{x, y, z\}$. The induced CI structure involves 18 (pairs of) elementary CI statements:

$$\begin{array}{l} x \perp\!\!\!\perp y | \emptyset, x \perp\!\!\!\perp z | \emptyset, x \perp\!\!\!\perp u | \emptyset, \\ y \perp\!\!\!\perp z | \emptyset, y \perp\!\!\!\perp u | \emptyset, z \perp\!\!\!\perp u | \emptyset, \\ x \perp\!\!\!\perp y | u, x \perp\!\!\!\perp z | u, x \perp\!\!\!\perp u | y, x \perp\!\!\!\perp u | z, \\ y \perp\!\!\!\perp z | u, y \perp\!\!\!\perp u | x, y \perp\!\!\!\perp u | z, z \perp\!\!\!\perp u | x, z \perp\!\!\!\perp u | y, \\ x \perp\!\!\!\perp u | yz, y \perp\!\!\!\perp u | xz, z \perp\!\!\!\perp u | xy. \end{array}$$

It has 4 permutably equivalent versions.

V.: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x y z u \\ (0, 0, 0, 0) \mapsto 1/8 \\ (0, 0, 1, 1) \mapsto 1/8 \\ (0, 1, 0, 1) \mapsto 1/8 \\ (0, 1, 1, 0) \mapsto 1/8 \\ (1, 0, 0, 1) \mapsto 1/8 \\ (1, 0, 1, 0) \mapsto 1/8 \\ (1, 1, 0, 0) \mapsto 1/8 \\ (1, 1, 1, 1) \mapsto 1/8 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min\{|S|, 3\} \text{ for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 3 over N . The induced CI structure involves 18 (pairs of) elementary CI statements:

$$\begin{array}{l} x \perp\!\!\!\perp y | \emptyset, x \perp\!\!\!\perp z | \emptyset, x \perp\!\!\!\perp u | \emptyset, \\ y \perp\!\!\!\perp z | \emptyset, y \perp\!\!\!\perp u | \emptyset, z \perp\!\!\!\perp u | \emptyset, \\ x \perp\!\!\!\perp y | z, x \perp\!\!\!\perp y | u, x \perp\!\!\!\perp z | y, x \perp\!\!\!\perp z | u, \\ x \perp\!\!\!\perp u | y, x \perp\!\!\!\perp u | z, y \perp\!\!\!\perp z | x, y \perp\!\!\!\perp z | u, \\ y \perp\!\!\!\perp u | x, y \perp\!\!\!\perp u | z, z \perp\!\!\!\perp u | x, z \perp\!\!\!\perp u | y. \end{array}$$

It has only 1 permutably equivalent version.

VI.: Put $N = \{x, y, z, u\}$ and define the density p of a binary random vector:

$$p: \begin{array}{l} x y z u \\ (0, 0, 0, 0) \mapsto 1/4 \\ (0, 0, 1, 1) \mapsto 1/4 \\ (1, 1, 0, 1) \mapsto 1/4 \\ (1, 1, 1, 0) \mapsto 1/4 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \begin{cases} 1 & \text{if } S = \{x, y\}, \\ \min\{|S|, 2\} & \text{otherwise,} \end{cases} \text{ for any } S \subseteq N.$$

Note that it corresponds to a (non-uniform) matroid over N . The induced CI structure involves 14 (pairs of) elementary CI statements:

$$\begin{array}{l} x \perp\!\!\!\perp z | \emptyset, x \perp\!\!\!\perp u | \emptyset, y \perp\!\!\!\perp z | \emptyset, y \perp\!\!\!\perp u | \emptyset, z \perp\!\!\!\perp u | \emptyset, \\ x \perp\!\!\!\perp z | y, x \perp\!\!\!\perp u | y, y \perp\!\!\!\perp z | x, y \perp\!\!\!\perp u | x, \\ x \perp\!\!\!\perp y | zu, x \perp\!\!\!\perp z | yu, x \perp\!\!\!\perp u | yz, y \perp\!\!\!\perp z | xu, y \perp\!\!\!\perp u | xz. \end{array}$$

It has 6 permutably equivalent versions.

VII.: Put $N = \{x, y, z, u\}$ and define the density of a ternary random vector:

$$p: \begin{array}{l} x y z u \\ (0, 0, 0, 0) \mapsto 1/9 \\ (0, 1, 1, 1) \mapsto 1/9 \\ (0, 2, 2, 2) \mapsto 1/9 \\ (1, 0, 1, 2) \mapsto 1/9 \\ (1, 1, 2, 0) \mapsto 1/9 \\ (1, 2, 0, 1) \mapsto 1/9 \\ (2, 0, 2, 1) \mapsto 1/9 \\ (2, 1, 0, 2) \mapsto 1/9 \\ (2, 2, 1, 0) \mapsto 1/9 \end{array}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \min\{|S|, 2\} \text{ for any } S \subseteq N.$$

Note it corresponds to the uniform matroid of rank 2 over N . The induced CI structure involves 12 (pairs of) elementary CI statements:

$$\begin{aligned} & x \perp\!\!\!\perp y \mid \emptyset, \quad x \perp\!\!\!\perp z \mid \emptyset, \quad x \perp\!\!\!\perp u \mid \emptyset, \\ & y \perp\!\!\!\perp z \mid \emptyset, \quad y \perp\!\!\!\perp u \mid \emptyset, \quad z \perp\!\!\!\perp u \mid \emptyset, \\ & x \perp\!\!\!\perp y \mid zu, \quad x \perp\!\!\!\perp z \mid yu, \quad x \perp\!\!\!\perp u \mid yz, \\ & y \perp\!\!\!\perp z \mid xu, \quad y \perp\!\!\!\perp u \mid xz, \quad z \perp\!\!\!\perp u \mid xy. \end{aligned}$$

It has only 1 permutably equivalent version.

VIII.: Put $N = \{x, y, z, u\}$ and define the density p of a random vector, whose components are binary except for ξ_x which has 4 allowed values:

$$\begin{aligned} & \begin{array}{ccc} & x & y & z & u \\ p : & (0, 0, 0, 0) & \mapsto & 1/4 \\ & (1, 0, 1, 1) & \mapsto & 1/4 \\ & (2, 1, 0, 1) & \mapsto & 1/4 \\ & (3, 1, 1, 0) & \mapsto & 1/4 \end{array} \end{aligned}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \begin{cases} 2 & \text{for } S = \{x\}, \\ \min\{|S|, 2\} & \text{if } S \neq \{x\}, \end{cases} \quad \text{for } S \subseteq N.$$

Note that it does not correspond to a matroid. The induced CI structure involves 12 (pairs of) elementary CI statements:

$$\begin{aligned} & y \perp\!\!\!\perp z \mid \emptyset, \quad y \perp\!\!\!\perp u \mid \emptyset, \quad z \perp\!\!\!\perp u \mid \emptyset, \\ & y \perp\!\!\!\perp z \mid x, \quad y \perp\!\!\!\perp u \mid x, \quad z \perp\!\!\!\perp u \mid x, \\ & x \perp\!\!\!\perp y \mid zu, \quad x \perp\!\!\!\perp z \mid yu, \quad x \perp\!\!\!\perp u \mid yz, \\ & y \perp\!\!\!\perp z \mid xu, \quad y \perp\!\!\!\perp u \mid xz, \quad z \perp\!\!\!\perp u \mid xy. \end{aligned}$$

It has 4 permutably equivalent versions.

IX.: Put $N = \{x, y, z, u\}$ and define the density p of a random vector, whose components are binary except for ξ_u which has 4 allowed values:

$$\begin{aligned} & \begin{array}{ccc} & x & y & z & u \\ p : & (0, 0, 0, 0) & \mapsto & 1/8 \\ & (0, 0, 1, 1) & \mapsto & 1/8 \\ & (0, 1, 0, 2) & \mapsto & 1/8 \\ & (0, 1, 1, 3) & \mapsto & 1/8 \\ & (1, 0, 0, 3) & \mapsto & 1/8 \\ & (1, 0, 1, 2) & \mapsto & 1/8 \\ & (1, 1, 0, 1) & \mapsto & 1/8 \\ & (1, 1, 1, 0) & \mapsto & 1/8 \end{array} \end{aligned}$$

with zero values for other configurations. It provides (strong) probabilistic representation of a polymatroid over N with the following integer-valued rank function:

$$h(S) := \begin{cases} |S| & \text{if } u \notin S, \\ \min\{|S| + 1, 3\} & \text{if } u \in S, \end{cases} \quad \text{for } S \subseteq N.$$

Note that it does not correspond to a matroid. The induced CI structure involves 12 (pairs of) elementary CI statements:

$$\begin{aligned} & x \perp\!\!\!\perp y \mid \emptyset, \quad x \perp\!\!\!\perp z \mid \emptyset, \quad x \perp\!\!\!\perp u \mid \emptyset, \\ & y \perp\!\!\!\perp z \mid \emptyset, \quad y \perp\!\!\!\perp u \mid \emptyset, \quad z \perp\!\!\!\perp u \mid \emptyset, \\ & x \perp\!\!\!\perp y \mid z, \quad x \perp\!\!\!\perp z \mid y, \quad y \perp\!\!\!\perp z \mid x, \\ & x \perp\!\!\!\perp y \mid zu, \quad x \perp\!\!\!\perp z \mid yu, \quad y \perp\!\!\!\perp z \mid xu. \end{aligned}$$

It has 4 permutably equivalent versions.

APPENDIX C

FORMER VERSIONS OF CI PROPERTIES

This is to commemorate former occurrence of the properties from Corollary 7 in the literature. One of them was proved in [33] and two of them formulated without proofs in [36]. The (original) proofs of all these properties were then published in [20], [21]; nevertheless, the CI implications were not formulated there as explicitly as in this paper and their proofs were encrypted as parts of composite proofs for compound propositions. On the other hand, all the properties were formulated explicitly in a conference contribution [37] (without proofs), two of them in the form of open questions (= conjectures). Here we recall the (main) ideas of the original proofs from [20], [21].

- The implication (I:1) was proved in [20, Proposition 3.1, 1st part] with $[X, Y, Z, U] = [1, 2, 3, 4]$. The argument there was similar to the proof of the first conditional information inequality [1cI]: the CI assumptions allow one to construct a certain probability distribution on ZU which dominates the marginal distribution on ZU and the non-negativity of the respective Kullback-Leibler divergence implies its vanishing, meaning $Z \perp\!\!\!\perp U$. The implication also appeared as (D.2) in [37]: $[X, Y, Z, U] = [C, D, A, B]$.
- The implication (I:2) first appeared as (B.1) in [36, § 5]; it was also reported in [37] as (B.1) with substitution $[X, Y, Z, U] = [C, D, B, A]$. The claim was then proved in [20, Proposition 2.1,(1)] with substitution $[X, Y, Z, U] = [1, 2, 3, 4]$. The argument there was the transformation to a wider framework of σ -algebras and applying a special CI property within this framework (see Section A-C).
- The implication (I:3) was proved in [20, Proposition 3.1, 2nd part] with $[X, Y, Z, U] = [2, 1, 4, 3]$. The argument there was some calculation with heedful cancellation terms (allowed by CI assumptions) and using some alternative definitions of CI. The property (I:3) also appeared as (D.3) in [37] with substitution $[X, Y, Z, U] = [B, D, A, C]$.
- The implication (I:4) first appeared as (B.2) in [36, § 5] and was also reported in [37] as (B.2) with substitution $[X, Y, Z, U] = [B, D, A, C]$. The claim was proved in [20, Proposition 2.1,(2)] with $[X, Y, Z, U] = [2, 1, 4, 3]$. The argument there was the same as in case of (I:2).
- The implication (I:5) was proved in [20, Proposition 2.1,(3)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [2, 1, 4, 3]$ there. The property

- also appeared as (B.3) in [37] with $[X, Y, Z, U] = [B, D, A, C]$.
- The implication (I:6) was proved in [20, Proposition 2.1,(4)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [2, 1, 4, 3]$ there. The property also appeared as (B.4) in [37] with $[X, Y, Z, U] = [B, D, A, C]$.
 - The implication (I:7) was proved in [20, Proposition 3.1, 3rd part] with $[X, Y, Z, U] = [2, 1, 4, 3]$. The argument there was analogous as in case of (I:3). The property appeared as (D.4) in [37]: $[X, Y, Z, U] = [B, D, A, C]$.
 - The implication (I:8) was proved in [20, Proposition 2.1,(8)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.8) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
 - The implication (I:9) was proved in [20, Proposition 3.1, 4th part] with $[X, Y, Z, U] = [1, 2, 3, 4]$. The argument there was similar to the one in case of (I:1): the CI assumptions allow one to construct a probability distribution on XYZ dominated by the marginal distribution on XYZ and the non-negativity of the respective Kullback-Leibler divergence forces that it vanishes, which gives $X \perp\!\!\!\perp Y | Z$. The property also appeared as (C.3) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
 - The implication (I:10) was proved in [20, Proposition 2.1,(5)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.5) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
 - The implication (I:11) was proved in [20, Proposition 2.1,(6)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.6) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
 - The implication (I:12) was proved in [20, Proposition 2.1,(7)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.7) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
 - The implication (I:13) first appeared in [33] and its elegant proof there was based on an equivalent definition of CI in terms of factorization of the density. The proof from [20, Proposition 4.1, 1st part] was based on the same argument with $[X, Y, Z, U] = [1, 2, 3, 4]$. The implication (I:13) also appeared as (D.1) in [37] where $[X, Y, Z, U] = [A, B, C, D]$.
 - The implication (I:14) was proved in [20, Proposition 4.1, 2nd part] with $[X, Y, Z, U] = [1, 2, 3, 4]$; the argument there was the uniqueness principle for factorizable distributions with coinciding marginals. The implication also appeared as (C.1) in [37] with $[X, Y, Z, U] = [A, B, C, D]$.
 - The implication (I:15) was derived in [21, § 2] as a consequence of the inequality [1cI] from [21, Proposition 2.1] in the text below that claim; take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as an open question a) in [37] with $[X, Y, Z, U] = [A, D, B, C]$.
 - The implication (I:16) was derived in [21, § 2] as a consequence of the inequality [2cI] from [21, Proposition 2.1] in the text below that claim; take $[X, Y, Z, U] =$

$[1, 2, 3, 4]$. The property also appeared as an open question b) in [37] with $[X, Y, Z, U] = [A, D, B, C]$.

- The implication (I:17) was proved in [20, Proposition 2.1,(9)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.9) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
- The implication (I:18) was proved in [20, Proposition 2.1,(10)] using the same arguments as in case of (I:2); take $[X, Y, Z, U] = [1, 2, 3, 4]$. The property also appeared as (B.10) in [37] with $[X, Y, Z, U] = [A, C, B, D]$.
- The implication (I:19) was proved in [20, Proposition 4.1, 3rd part] with $[X, Y, Z, U] = [1, 2, 3, 4]$; the argument there was the uniqueness principle for factorizable distributions with coinciding supports. The implication also appeared as (C.2) in [37] with $[X, Y, Z, U] = [B, C, A, D]$.

ACKNOWLEDGMENT

The research of the author is supported from GAČR project 19-04579S. This particular research theme follows up the cooperation with my deceased colleague Fero Matuš and I am indebted to him for the fruitful discussion on this topic we had over the former years. My thanks also go to Tobias Boege, who reminded me that every linearly representable matroid is representable over a finite field. Finally, I am indebted to László Csirmaz, Tarik Kaced, and anonymous reviewers for reading the manuscript and giving me their valuable comments.

REFERENCES

- [1] B. Abo Khamis, P. G. Kolaitis, H. Q. Ngo, D. Suci, "Decision problems in information theory," in *Proceedings of the 47th International Colloquium on Automata, Languages and Programming (ICALP 2020)*, pp. 106:1–106:20.
- [2] G. Birkhoff, *Lattice Theory*. Third edition, American Mathematical Society, Colloquium Publications 25, Providence 1995.
- [3] R. Bouckaert, R. Hemmecke, S. Lindner, M. Studený, "Efficient algorithms for conditional independence inference," *Journal of Machine Learning Research* 11 (2010), 3453–3479.
- [4] T. H. Chen, R. W. Yeung, "On a relation between information inequalities and group theory," *IEEE Transactions on Information Theory* 48 (2002), 1992–1995.
- [5] I. Csizár, J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Second impression, Akadémiai Kiadó, Budapest 1986.
- [6] A. P. Dawid, "Conditional independence in statistical theory," *Journal of the Royal Statistical Society B* 41(1) (1979), 1–31.
- [7] J. Edmonds, "Submodular functions, matroids, and certain polyhedra," in *Combinatorial Structures and their Applications*, Gordon and Breach, 1970, pp. 69–87.
- [8] S. Fujishige, *Submodular Functions and Optimization*. Second edition, Elsevier, Amsterdam 2005.
- [9] A. W. Ingleton, "Conditions for representability and transversality of matroids," in *Lecture Notes in Computer Science* 211, Springer, 1971, pp. 62–67.
- [10] T. Kaced, A. Romashchenko, "Conditional information inequalities for entropic and almost entropic points," *IEEE Transactions on Information Theory* 59(11) (2013), 7149–7167.
- [11] T. Kaced, A. Romashchenko, N. Vereshchagin, "A conditional information inequality and its combinatorial applications," *IEEE Transactions on Information Theory* 64(5) (2018), 3610–3615.
- [12] S. L. Lauritzen, *Graphical Models*. Clarendon Press, Oxford 1996.
- [13] M. Loève, *Probability Theory, Foundations, Random Sequences*. Van Nostrand, Toronto 1955.

- [14] K. Makarychev, Y. Makarychev, A. Romashchenko, N. Vereshchagin, "A new class of non-Shannon-type inequalities for entropies," *Communications in Information and Systems* 2(2) (2002), 147–166.
- [15] F. Matúš, "Ascending and descending conditional independence relations," in *Transactions of the 11th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes, volume B*, Academia, Prague 1992, pp. 189–200.
- [16] F. Matúš, "Stochastic independence, algebraic independence and abstract connectedness," *Theoretical Computer Science* 134 (1994), 455–471.
- [17] F. Matúš, "Probabilistic conditional independence structures and matroid theory: background," *International Journal of General Systems* 22 (1994), 185–196.
- [18] F. Matúš, "Extreme convex set functions with many non-negative differences," *Discrete Mathematics* 135 (1994), 177–191.
- [19] F. Matúš, M. Studený, "Conditional independences among four random variables I," *Combinatorics, Probability and Computing* 4 (1995), 269–278.
- [20] F. Matúš, "Conditional independences among four random variables II," *Combinatorics, Probability and Computing* 4 (1995), 407–417.
- [21] F. Matúš, "Conditional independences among four random variables III: final conclusion," *Combinatorics, Probability and Computing* 8 (1999), 269–276.
- [22] F. Matúš, "Two constructions on limits of entropy functions," *IEEE Transactions on Information Theory* 53 (2007) 320–330.
- [23] F. Matúš, "Infinitely many information inequalities," in *Proceedings of the IEEE International Symposium on Information Theory, Nice 2007*, pp. 41–44.
- [24] M. Mouchart, J. M. Rolin, "A note on conditional independence with statistical applications," *Statistica* 44 (1984), 557–584.
- [25] J. G. Oxley, *Matroid Theory*. Second edition, Oxford University Press, New York 2011.
- [26] C. Padro, "Lecture Notes in Secrete Sharing," Cryptology E-print Archive, Report 2012/674.
- [27] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan Kaufmann, San Francisco 1988.
- [28] N. Pippenger, "What are the laws of information theory," in *1986 Special Problems on Communication and Computation Conference*, pp. 3–5.
- [29] A. Postnikov, V. Reiner, L. Williams, "Faces of generalized permutohedra," *Documenta Mathematica* 13 (2008), 207–273.
- [30] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency, volume B*. Springer, 2003.
- [31] P. Šimeček, "Independence models," (in Czech), PhD thesis, Charles University, Prague, Czech Republic, 2007.
- [32] W. Spohn, "Stochastic independence, causal independence and shieldability," *Journal of Philosophical Logic* 9(1) (1980), 73–99.
- [33] W. Spohn, "On the properties of conditional independence," in *Patrick Suppes: Scientific Philosopher* (P. Humphreys ed.), Kluwer, Dordrecht 1994, pp. 173–196.
- [34] M. Studený, "Multiinformation and the problem of characterization of conditional independence relations," *Problems of Control and Information Theory* 18(1) (1989), 3–16.
- [35] M. Studený, "Conditional independence relations have no finite complete characterization," in *Transactions of the 11th Prague Conference on Information Theory, Statistical Decision Functions and Random Processes, volume B*, Academia, Prague 1992, pp. 377–396.
- [36] M. Studený, "Structural semigraphoids," *International Journal of General Systems* 22 (1994), 207–217.
- [37] M. Studený, P. Boček, "CI-models arising among 4 random variables," in *Proceedings of the 3rd Workshop on Uncertainty Processing in Expert Systems (WUPES'94)*, September 11–15, 1994, pp. 268–282.
- [38] M. Studený, *Probabilistic Conditional Independence Structures*. Springer, London 2005.
- [39] M. Studený, T. Kroupa, "Core-based criterion for extreme supermodular functions," *Discrete Applied Mathematics* 206 (2016), 122–151.
- [40] H. Whitney, "On the abstract properties of linear dependence," *American Journal of Mathematics* 57(3) (1935), 509–533.
- [41] R. W. Yeung, *Information Theory and Network Coding*. Springer, New York 2008.
- [42] Z. Zhang, R. W. Yeung, "A non-Shannon-type conditional inequality of information quantities," *IEEE Transactions on Information Theory* 43 (1997), 1982–1986.
- [43] Z. Zhang, R. W. Yeung, "On characterization of entropy function via information inequalities," *IEEE Transactions on Information Theory* 44 (1998), 1440–1450.
- [44] G. M. Ziegler, *Lectures on Polytopes*. Springer, New York 1995.



Milan Studený was born in Mariánské Lázně, Czechoslovakia, in 1957. He received his RNDr. degree (M.Sc. level) in mathematical analysis from Charles University, Faculty of Mathematics and Physics, Prague, in 1981 and his CSc. degree (Ph.D. level) in theoretical cybernetics from Czechoslovak Academy of Sciences, Prague, in 1986.

From 1986, he has been with the Institute of Information Theory and Automation, the Czech Academy of Sciences, Prague. In 2001 he got his DrSc. degree in mathematical informatics and theoretical cybernetics (academic professor level) from Czech Academy of Sciences, Prague. His research interests include formal properties of conditional independence (both in probabilistic and non-probabilistic context), algebraic properties of entropy, information-theoretical measures of conditional dependence, marginal problem, and graphical statistical models. He is also interested in application of the methods of polyhedral geometry, algebra, optimization theory, and statistics in this context; thus, his research interests also touch the areas of algebraic statistics and cooperative game theory. He has published about 40 peer reviewed journal papers and more than 40 conference papers or book chapters on the topics of his research interest. He is an author of a 2005 monograph entitled *Probabilistic Conditional Independence Structures*.