The Ingleton inequality for random variables

Tobias Boege

Department of Mathematics KTH Royal Institute of Technology, Sweden

UiT The Arctic University of Norway 13 August 2024

Matroids

 Matroids are combinatorial structures which model "special position" relations in geometry.



Matroids

- Matroids are combinatorial structures which model "special position" relations in geometry.
 - For example the matroid of a set of points in the projective plane records which triples of points lie on a line.



Matroids

- Matroids are combinatorial structures which model "special position" relations in geometry.
 - For example the matroid of a set of points in the projective plane records which triples of points lie on a line.
- Non-realizability of matroids captures the (non-obvious) laws of projective geometry.















Entropy

Let X be a random variable taking finitely many values $\{1, \ldots, d\}$ with positive probabilities. Its *Shannon entropy* is

$$H(X) := \sum_{i=1}^{d} p(X = i) \log \frac{1}{p(X = i)}.$$

• *H* is continuous on $\Delta(d)$ and analytic on the interior.

Entropy

Let X be a random variable taking finitely many values $\{1, \ldots, d\}$ with positive probabilities. Its *Shannon entropy* is

$$H(X) := \sum_{i=1}^{d} p(X = i) \log \frac{1}{p(X = i)}.$$

- *H* is continuous on $\Delta(d)$ and analytic on the interior.
- A random vector $X \in \Delta(d_1, \ldots, d_n)$ is a random variable in $\Delta(\prod_{i=1}^n d_i)$, so the definition of H extends to vectors.
- ▶ The random vector $X = (X_1, ..., X_n)$ has 2^n marginal random vectors and we collect their entropies in an entropy profile $h_X : 2^{[n]} \to \mathbb{R}$.
 - ▶ For example (X, Y) has entropy profile $(0, H(X), H(Y), H(X, Y)) \in \mathbb{R}^4$.

Entropy as information



Figure: Entropy of a binary random variable X as a function of p = p(X = heads).

Let $\mathbf{H}_n^* \subseteq \mathbb{R}^{2^n}$ consist of all h_X where X is an *n*-variate discrete random vector. \mathbf{H}_n^* is the image of $\bigcup_{d_1=1}^{\infty} \cdots \bigcup_{d_n=1}^{\infty} \Delta(d_1, \ldots, d_n)$ under the transcendental map $X \mapsto h_X$.

Let $\mathbf{H}_n^* \subseteq \mathbb{R}^{2^n}$ consist of all h_X where X is an *n*-variate discrete random vector. \mathbf{H}_n^* is the image of $\bigcup_{d_1=1}^{\infty} \cdots \bigcup_{d_n=1}^{\infty} \Delta(d_1, \ldots, d_n)$ under the transcendental map $X \mapsto h_X$.

► H^{*}_n is a finite-dimensional space which captures special position information for all discrete random vectors of a fixed length (but unbounded state spaces).

Let $\mathbf{H}_n^* \subseteq \mathbb{R}^{2^n}$ consist of all h_X where X is an *n*-variate discrete random vector. \mathbf{H}_n^* is the image of $\bigcup_{d_1=1}^{\infty} \cdots \bigcup_{d_n=1}^{\infty} \Delta(d_1, \ldots, d_n)$ under the transcendental map $X \mapsto h_X$.

- ▶ \mathbf{H}_n^* is a finite-dimensional space which captures special position information for all discrete random vectors of a fixed length (but unbounded state spaces).
- ► Applications in cryptography, coding theory, engineering want to optimize linear functions over H^{*}_n.

Let $\mathbf{H}_n^* \subseteq \mathbb{R}^{2^n}$ consist of all h_X where X is an *n*-variate discrete random vector. \mathbf{H}_n^* is the image of $\bigcup_{d_1=1}^{\infty} \cdots \bigcup_{d_n=1}^{\infty} \Delta(d_1, \ldots, d_n)$ under the transcendental map $X \mapsto h_X$.

- ▶ \mathbf{H}_n^* is a finite-dimensional space which captures special position information for all discrete random vectors of a fixed length (but unbounded state spaces).
- ► Applications in cryptography, coding theory, engineering want to optimize linear functions over H^{*}_n.

Theorem

 $\overline{\mathbf{H}_{n}^{*}}$ is a convex cone of dimension $2^{n} - 1$. Furthermore relint $(\overline{\mathbf{H}_{n}^{*}}) \subseteq \mathbf{H}_{n}^{*}$.

Let $\mathbf{H}_n^* \subseteq \mathbb{R}^{2^n}$ consist of all h_X where X is an *n*-variate discrete random vector. \mathbf{H}_n^* is the image of $\bigcup_{d_1=1}^{\infty} \cdots \bigcup_{d_n=1}^{\infty} \Delta(d_1, \ldots, d_n)$ under the transcendental map $X \mapsto h_X$.

- ▶ \mathbf{H}_n^* is a finite-dimensional space which captures special position information for all discrete random vectors of a fixed length (but unbounded state spaces).
- ► Applications in cryptography, coding theory, engineering want to optimize linear functions over H^{*}_n.

Theorem

 $\overline{\mathbf{H}_{n}^{*}}$ is a convex cone of dimension $2^{n} - 1$. Furthermore relint $(\overline{\mathbf{H}_{n}^{*}}) \subseteq \mathbf{H}_{n}^{*}$.

Elements of the dual cone (linear information inequalities) can give bounds for optimization problems.

Shannon inequalities

▶ A function $h: 2^N \to \mathbb{R}$ is a polymatroid if

►
$$h(\emptyset) = 0$$
,

- $h(I \mid K) := h(IK) h(K) \ge 0$ for disjoint I and K,
- ► $h(I:J | K) := h(IK) + h(JK) h(IJK) h(K) \ge 0$ for disjoint *I*, *J*, *K*.

Shannon inequalities

▶ A function $h: 2^N \to \mathbb{R}$ is a polymatroid if

►
$$h(\emptyset) = 0$$
,

- $h(I \mid K) \coloneqq h(IK) h(K) \ge 0$ for disjoint I and K,
- ► $h(I:J | K) := h(IK) + h(JK) h(IJK) h(K) \ge 0$ for disjoint *I*, *J*, *K*.
- The set P_N of polymatroids is a polyhedral cone in ℝ^{2^N} and P_N ⊇ H^{*}_N → ITIP.
 The information inequalities in the dual cone of P_N are the Shannon inequalities.

Shannon inequalities

▶ A function
$$h: 2^N \to \mathbb{R}$$
 is a polymatroid if

►
$$h(\emptyset) = 0$$
,

- $h(I \mid K) \coloneqq h(IK) h(K) \ge 0$ for disjoint I and K,
- ► $h(I:J | K) := h(IK) + h(JK) h(IJK) h(K) \ge 0$ for disjoint *I*, *J*, *K*.
- The set P_N of polymatroids is a polyhedral cone in ℝ^{2^N} and P_N ⊇ H^{*}_N → ITIP.
 The information inequalities in the dual cone of P_N are the Shannon inequalities.

Theorem ([Mat07])

 $\overline{\mathbf{H}_{N}^{*}}$ is not polyhedral for $|N| \geq 4$.

• GMM conjecture: $\overline{\mathbf{H}_N^*}$ is not semialgebraic for $|N| \ge 4$.

Information inequalities abound

Rule [43] Given:

and

Get:



Using: RS is copy of CD over ABSubstitutions: $A \ C \ R \ S$; $AD \ B \ R \ S$

Abbreviated Proof of (75): T: D-copy of A over BCRS. L1: -a.c. +c.d. +r.cd.a +c.s.a +b.d.s +a.bs.d +2a.cr.bs +a.bs.cr +d r abcs +d s abcr SL1: d.t.a +c.d.t +a.t.cd +c.r.t +a.t.cr +d.r.act +b.t.acdr +a.t.bs +c.s.at +b.t.acs +d.t.s +a.s.dt +b.d.ast +c.t.abds +a.r.bcst +r ad best +s ad bert +d t abers C2L1: 3t ad bers S: C-copy of A over BDR. 12: -2ac +2cd +abcr +2acbr +carb +abdr +4adbr +2a brd +2d bra +2r cd a +d rabe SL2: csh + ahcs + cds + ascd + dsabc + 3asbr + 3csbr+c rabs +d rs +a s dr +d rabs +d bras +c rads +b s acdr +2c s abdr +2d s abcr C2L2: 7s.ac.bdr R: D-copy of C over AB. S: cra +3crb +dra +7drb +cdr +2bracd +rabed +9c r abd +3d r abc C2. 16r cd ab

Randall Dougherty, Chris Freiling, and Kenneth Zeger. *Non-Shannon Information Inequalities in Four Random Variables*. 2011. arXiv: 1104.3602v1 [cs.IT]

Information-theoretical "special position" properties of discrete random variables can be formulated in terms of linear functionals on the entropy profile h_X :

Information-theoretical "special position" properties of discrete random variables can be formulated in terms of linear functionals on the entropy profile h_X :

Rank condition	Matroid concept	Information theory concept
h(i) = 0	loop	constant random variable
$h(N) = h(i) + h(N \setminus i)$	coloop	max. private information

Information-theoretical "special position" properties of discrete random variables can be formulated in terms of linear functionals on the entropy profile h_X :

Rank condition	Matroid concept	Information theory concept
h(i) = 0	loop	constant random variable
$h(N) = h(i) + h(N \setminus i)$	coloop	max. private information
h(iK) = h(K)	closure operator	functional dependence
$h(K) = \sum_{k \in K} h(k)$	independent set	total independence
h(iK) + h(jK) = h(K) + h(ijK)	modular pair	conditional independence

Information-theoretical "special position" properties of discrete random variables can be formulated in terms of linear functionals on the entropy profile h_X :

Rank condition	Matroid concept	Information theory concept
h(i) = 0	loop	constant random variable
$h(N) = h(i) + h(N \setminus i)$	coloop	max. private information
h(iK) = h(K)	closure operator	functional dependence
$h(K) = \sum_{k \in K} h(k)$	independent set	total independence
h(iK) + h(jK) = h(K) + h(ijK)	modular pair	conditional independence

All of these are **linear** in *h*. Even though entropy is a transcendental function, many of these conditions are **polynomial** in the probabilities \rightarrow algebraic statistics.

$$I(A, B | C, D) := h(A, C) + h(B, C) + h(A, D) + h(B, D) + h(C, D) - h(A, B) - h(C) - h(D) - h(A, C, D) - h(B, C, D) \ge 0.$$

► Let A, B, C, D be subspaces in a finite-dimensional vector space. Then the Ingleton inequality holds for h = dim (the matroid setting):

$$I(A, B | C, D) := h(A, C) + h(B, C) + h(A, D) + h(B, D) + h(C, D) - h(A, B) - h(C) - h(D) - h(A, C, D) - h(B, C, D) \ge 0.$$

▶ The Ingleton inequality fails in general for $h = h_X$ (the entropic setting) but certain special position assumptions do make it true, e.g.,

$$\begin{split} \mathbb{I}(A,B \mid C,D) &:= h(A,C) + h(B,C) + h(A,D) + h(B,D) + h(C,D) - \\ h(A,B) - h(C) - h(D) - h(A,C,D) - h(B,C,D) \geq 0. \end{split}$$

- ▶ The Ingleton inequality fails in general for $h = h_X$ (the entropic setting) but certain special position assumptions do make it true, e.g.,
 - ▶ If $C \perp D$ then $I(A, B \mid C, D) \ge 0$.

$$\begin{split} I(A,B \mid C,D) &:= h(A,C) + h(B,C) + h(A,D) + h(B,D) + h(C,D) - \\ h(A,B) - h(C) - h(D) - h(A,C,D) - h(B,C,D) \geq 0. \end{split}$$

- ▶ The Ingleton inequality fails in general for $h = h_X$ (the entropic setting) but certain special position assumptions do make it true, e.g.,
 - ▶ If $C \perp D$ then $I(A, B \mid C, D) \ge 0$.
 - ▶ If $A \perp \!\!\!\perp C \mid D$ and $A \perp \!\!\!\perp D \mid C$ then $I(A, B \mid C, D) \ge 0$.

$$\begin{split} \mathsf{I}(A,B \mid C,D) &:= h(A,C) + h(B,C) + h(A,D) + h(B,D) + h(C,D) - \\ h(A,B) - h(C) - h(D) - h(A,C,D) - h(B,C,D) \geq 0. \end{split}$$

- ▶ The Ingleton inequality fails in general for $h = h_X$ (the entropic setting) but certain special position assumptions do make it true, e.g.,
 - ▶ If $C \perp D$ then $I(A, B \mid C, D) \ge 0$.
 - ▶ If $A \perp \!\!\!\perp C \mid D$ and $A \perp \!\!\!\perp D \mid C$ then $I(A, B \mid C, D) \ge 0$.
 - ▶ ...

► Let A, B, C, D be subspaces in a finite-dimensional vector space. Then the Ingleton inequality holds for h = dim (the matroid setting):

$$I(A, B | C, D) := h(A, C) + h(B, C) + h(A, D) + h(B, D) + h(C, D) - h(A, B) - h(C) - h(D) - h(A, C, D) - h(B, C, D) \ge 0.$$

▶ The Ingleton inequality fails in general for $h = h_X$ (the entropic setting) but certain special position assumptions do make it true, e.g.,

▶ If
$$C \perp D$$
 then $I(A, B \mid C, D) \ge 0$.

- ▶ If $A \perp \!\!\!\perp C \mid D$ and $A \perp \!\!\!\perp D \mid C$ then $I(A, B \mid C, D) \ge 0$.
- ▶ ...

These are conditional linear information inequalities and they can sometimes tell apart honest boundary parts of \mathbf{H}_n^* from fake boundary parts on $\overline{\mathbf{H}_n^*}$.

Since I(A, B | C, D) is symmetric in A ↔ B and C ↔ D, there are only six different versions of I ≥ 0 on four random variables modulo 𝔅₄.

- Since I(A, B | C, D) is symmetric in A ↔ B and C ↔ D, there are only six different versions of I ≥ 0 on four random variables modulo 𝔅₄.
- \blacktriangleright The Shannon cone P_4 decomposes into seven cones:
 - One where all Ingleton inequalities are satisfied: it is contained in $\overline{\mathbf{H}_{4}^{*}}$.

- Since I(A, B | C, D) is symmetric in A ↔ B and C ↔ D, there are only six different versions of I ≥ 0 on four random variables modulo 𝔅₄.
- ▶ The Shannon cone P_4 decomposes into seven cones:
 - One where all Ingleton inequalities are satisfied: it is contained in $\overline{\mathbf{H}_{4}^{*}}$.
 - Six linearly isomorphic copies of the cone $J_4 := P_4 \cap \{I(A, B \mid C, D) < 0\}$.

- Since I(A, B | C, D) is symmetric in A ↔ B and C ↔ D, there are only six different versions of I ≥ 0 on four random variables modulo 𝔅₄.
- ▶ The Shannon cone P_4 decomposes into seven cones:
 - One where all Ingleton inequalities are satisfied: it is contained in $\overline{\mathbf{H}_{4}^{*}}$.
 - Six linearly isomorphic copies of the cone $J_4 := P_4 \cap \{I(A, B \mid C, D) < 0\}$.
- ► J₄ is simplicial and its facets are induced by conditional independence functionals and the Ingleton functional.

Conditional Ingleton inequalities

Theorem ([KR13] & [Stu21] & [Boe23])

Up to symmetry there are precisely ten minimal sets of conditional independence assumptions on four random variables which ensure $I \ge 0$.

Check out \geq https://mathrepo.mis.mpg.de/ConditionalIngleton/ \leq for non-linear algebra and numerical optimization techniques used in part of the proof.

Conditional Ingleton inequalities

Theorem ([KR13] & [Stu21] & [Boe23])

Up to symmetry there are precisely ten minimal sets of conditional independence assumptions on four random variables which ensure $I \ge 0$.

Check out \geq https://mathrepo.mis.mpg.de/ConditionalIngleton/ \leq for non-linear algebra and numerical optimization techniques used in part of the proof.

Corollary

On four discrete random variables there are precisely 18 478 realizable conditional independence structures. (Combinatorial laws of information theory)

Conditional Ingleton inequalities

Theorem ([KR13] & [Stu21] & [Boe23])

Up to symmetry there are precisely ten minimal sets of conditional independence assumptions on four random variables which ensure $I \ge 0$.

Check out \geq https://mathrepo.mis.mpg.de/ConditionalIngleton/ \leq for non-linear algebra and numerical optimization techniques used in part of the proof.

Corollary

On four discrete random variables there are precisely 18 478 realizable conditional independence structures. (Combinatorial laws of information theory)

Problem

Which of these laws holds on $\overline{\mathbf{H}_{4}^{*}}$? (Some do, some don't ...)

Problem

Find/sample positive points from conditional independence varieties.

Problem

Find/sample positive points from conditional independence varieties.

Problem (Gómez–Mejía–Montoya) Is $[A \perp C \mid D] \land [A \perp D \mid C] \land [B \perp C \mid D] \land [B \perp D \mid C] \implies I(A, B \mid C, D) \ge 0$ essentially conditional?

Problem

Find/sample positive points from conditional independence varieties.

Problem (Gómez–Mejía–Montoya) Is $[A \perp C \mid D] \land [A \perp D \mid C] \land [B \perp C \mid D] \land [B \perp D \mid C] \implies I(A, B \mid C, D) \ge 0$ essentially conditional?

Problem

Find a description of the boundary of H_3^* .



Problem

Find/sample positive points from conditional independence varieties.

Problem (Gómez–Mejía–Montoya) Is $[A \perp C \mid D] \land [A \perp D \mid C] \land [B \perp C \mid D] \land [B \perp D \mid C] \implies I(A, B \mid C, D) \ge 0$ essentially conditional?

Problem

Find a description of the boundary of \mathbf{H}_{3}^{*} .



Problem

Find/sample positive points from conditional independence varieties.

Problem (Gómez–Mejía–Montoya) Is $[A \perp C \mid D] \land [A \perp D \mid C] \land [B \perp C \mid D] \land [B \perp D \mid C] \implies I(A, B \mid C, D) \ge 0$ essentially conditional?

Problem Find a description of the boundary of H₃. Thank you!

References

- [Boe23] Tobias Boege. "No Eleventh Conditional Ingleton Inequality". In: *Experimental Mathematics* (2023). DOI: 10.1080/10586458.2023.2294827.
- [DFZ11] Randall Dougherty, Chris Freiling, and Kenneth Zeger. Non-Shannon Information Inequalities in Four Random Variables. 2011. arXiv: 1104.3602v1 [cs.IT].
- [KR13] Tarik Kaced and Andrei Romashchenko. "Conditional information inequalities for entropic and almost entropic points". In: IEEE Trans. Inf. Theory 59.11 (2013), pp. 7149–7167. ISSN: 0018-9448. DOI: 10.1109/TIT.2013.2274614.
- [Mat06] Frantisek Matús. "Piecewise linear conditional information inequality". In: IEEE Trans. Inf. Theory 52.1 (2006), pp. 236–238. ISSN: 0018-9448. DOI: 10.1109/TIT.2005.860438.
- [Mat07] František Matúš. "Infinitely many information inequalities". In: *Proc. IEEE ISIT 2007*. 2007, pp. 41–44.
- [MS95] František Matúš and Milan Studený. "Conditional independences among four random variables. I". In: Combin. Probab. Comput. 4.3 (1995), pp. 269–278. DOI: 10.1017/S0963548300001644.
- [Stu21] Milan Studený. "Conditional independence structures over four discrete random variables revisited: conditional ingleton inequalities". In: IEEE Trans. Inf. Theory 67.11 (2021), pp. 7030–7049. ISSN: 0018-9448. DOI: 10.1109/TIT.2021.3104250.