Entropy and matroids

František Matúš

Institute of Information Theory and Automation
Academy of Sciences of the Czech Republic
matus@utia.cas.cz

First Workshop on Entropy and Information Inequalities

Hong Kong, April 15-17, 2013

$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$ ... a ground set

$N = \{1, 2, 3, 4, 5, 6\}$ ... a ground set

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

... a matrix
with entries in a field
and columns labeled by N

$N = \{1, 2, 3, 4, 5, 6\}$ ... a ground set

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

... a matrix
with entries in a field
and columns labeled by N

for each set of labels, e.g. $I = \{3, 5, 6\} \subseteq N$,

$N = \{1, 2, 3, 4, 5, 6\}$ ... a ground set

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

... a matrix
with entries in a field
and columns labeled by N

for each set of labels, e.g. $I = \{3, 5, 6\} \subseteq N$,

record the rank of the I-submatrix, e.g. of $A_I = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

$N = \{1, 2, 3, 4, 5, 6\}$ ... a ground set

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

... a matrix
with entries in a field
and columns labeled by N

for each set of labels, e.g. $I = \{3, 5, 6\} \subseteq N$,

record the rank of the I-submatrix, e.g. of $A_I = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

(may depend on an underlying field)

$N = \{1\,,\,2\,,\,3\,,\,4\,,\,5\,,\,6\}$ … a ground set

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

… a matrix
with entries in a field
and columns labeled by N

for each set of labels, e.g. $I = \{3\,,\,5\,,\,6\} \subseteq N$,

record the rank of the I-submatrix, e.g. of $A_I = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

(may depend on an underlying field)

collect basic properties of the ranks of all A_I submatrices

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and
rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and
rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$

$$r(I) \leqslant |I| \text{ for } I \subseteq N.$$

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$

$$r(I) \leqslant |I| \text{ for } I \subseteq N.$$

The matroid is linear over a field $\mathbb{F}$ if a matrix A exists such that $r(I) = \mathrm{rank}_{\mathbb{F}}(A_I)$ for all $I \subseteq N$.

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$

$$r(I) \leqslant |I| \text{ for } I \subseteq N.$$

The matroid is linear over a field $\mathbb{F}$ if a matrix A exists such that $r(I) = \mathrm{rank}_{\mathbb{F}}(A_I)$ for all $I \subseteq N$.

going back to 1936, today > 10000 papers

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and
rank function $r\colon I \mapsto \{0, 1, \dots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$

$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$

$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$

$$r(I) \leqslant |I| \text{ for } I \subseteq N.$$

The matroid is linear over a field $\mathbb{F}$ if a matrix A exists such that
$r(I) = \mathrm{rank}_{\mathbb{F}}(A_I)$ for all $I \subseteq N$.

going back to 1936, today > 10000 papers

several textbooks (Welsh, Recski, Oxley)

Definition (Matroid I)

(N, r) is a matroid, with a ground set N and rank function $r\colon I \mapsto \{0, 1, \ldots\}$, $I \subseteq N$, if

$$r(\emptyset) = 0$$
$$r(I) \leqslant r(J) \quad \text{for } I \subseteq J \subseteq N$$
$$r(I) + r(J) \geqslant r(I \cup J) + r(I \cap J) \quad \text{for } I, J \subseteq N$$
$$r(I) \leqslant |I| \text{ for } I \subseteq N.$$

The matroid is linear over a field $\mathbb{F}$ if a matrix A exists such that $r(I) = \mathrm{rank}_{\mathbb{F}}(A_I)$ for all $I \subseteq N$.

going back to 1936, today > 10000 papers

several textbooks (Welsh, Recski, Oxley)

crossroad of combinatorics, algebra and finite geometry

the matroid admits a number of equivalent ‘crypto’ definitions

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

the matroid admits a number of equivalent ‘crypto’ definitions

$$N = \{1\ , 2\ , 3\ , 4\ , 5\ , 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

the matroid admits a number of equivalent ‘crypto’ definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1, 2, 3\}$, $\{1\}$, ..., $\{4, 5, 6\}$.

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1,2,3\}$, $\{1\}$, ..., $\{4,5,6\}$.

collect basic properties of the independent sets

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1, 2, 3\}$, $\{1\}$, ..., $\{4, 5, 6\}$.

collect basic properties of the independent sets

Definition (Matroid II)

$(N, \mathcal{I})$ is a matroid, with a ground set N and family of $\mathcal{I} \subseteq 2^N$ of independent sets if

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1,2,3\}$, $\{1\}$, ..., $\{4,5,6\}$.

collect basic properties of the independent sets

Definition (Matroid II)

$(N, \mathcal{I})$ is a matroid, with a ground set N and family of $\mathcal{I} \subseteq 2^N$ of independent sets if

$\emptyset \in \mathcal{I}$

the matroid admits a number of equivalent ‘crypto’ definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1,2,3\}$, $\{1\}$, ..., $\{4,5,6\}$.

collect basic properties of the independent sets

Definition (Matroid II)

$(N, \mathcal{I})$ is a matroid, with a ground set N and family of $\mathcal{I} \subseteq 2^N$ of independent sets if

$\emptyset \in \mathcal{I}$

$I \subseteq J \subseteq N$ and $J \in \mathcal{I}$ implies $I \in \mathcal{I}$

the matroid admits a number of equivalent 'crypto' definitions

$$N = \{1\ ,\ 2\ ,\ 3\ ,\ 4\ ,\ 5\ ,\ 6\}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

record all sets $I \subseteq N$ such that A_I has independent columns

call them independent, e.g. $\{1,2,3\}$, $\{1\}$, ..., $\{4,5,6\}$.

collect basic properties of the independent sets

Definition (Matroid II)

$(N, \mathcal{I})$ is a matroid, with a ground set N and family of $\mathcal{I} \subseteq 2^N$ of independent sets if

$\emptyset \in \mathcal{I}$

$I \subseteq J \subseteq N$ and $J \in \mathcal{I}$ implies $I \in \mathcal{I}$

for $K \subseteq N$ all $I \subseteq K$ maximal in $\mathcal{I}$ have the same cardinality.

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

sets in $2^N \setminus \mathcal{I}$ are dependent

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

sets in $2^N \setminus \mathcal{I}$ are dependent

minimal dependent set is a circuit C

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

sets in $2^N \setminus \mathcal{I}$ are dependent

minimal dependent set is a circuit C

$F \subseteq N$ is a flat if $r(F) < r(F \cup i)$ for all $i \in N \setminus F$

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

sets in $2^N \setminus \mathcal{I}$ are dependent

minimal dependent set is a circuit C

$F \subseteq N$ is a flat if $r(F) < r(F \cup i)$ for all $i \in N \setminus F$

four more axiom systems

'Thm': 'one-to-one correspondence' between $(N, \mathcal{I})$ and (N, r)

maximal independent set is a base B

sets in $2^N \setminus \mathcal{I}$ are dependent

minimal dependent set is a circuit C

$F \subseteq N$ is a flat if $r(F) < r(F \cup i)$ for all $i \in N \setminus F$

four more axiom systems

many theorems on one-to-one correspondences

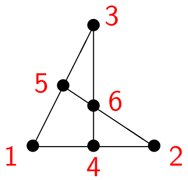
sometimes a matroid can be described by a point configuration

sometimes a matroid can be described by a point configuration

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

sometimes a matroid can be described by a point configuration

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$



$r(I)$ ... affine dimension of I
B base ... three points not collinear
C circuit ... $\{1, 2, 4\}$, $\{1, 4, 5, 6\}$, etc.

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{cc} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} & \begin{matrix} a \\ b \\ c \\ d \end{matrix} \end{array}$$

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{c c} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} & \begin{array}{c} a \\ b \\ c \\ d \end{array} \end{array}$$

A and B have the same row spaces (codes) over $\mathrm{GF}(2)$,

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{cc} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} & \begin{array}{c} a \\ b \\ c \\ d \end{array} \end{array}$$

A and B have the same row spaces (codes) over $\mathrm{GF}(2)$,

hence induce the same matroid

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{c} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} a \\ b \\ c \\ d \end{array}$$

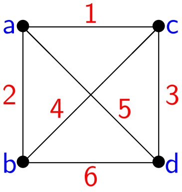
A and B have the same row spaces (codes) over $\mathrm{GF}(2)$,
hence induce the same matroid

the matroid is graphical because B is an incidence matrix of K_4

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{cc} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} & \begin{array}{c} a \\ b \\ c \\ d \end{array} \end{array}$$

A and B have the same row spaces (codes) over $\mathrm{GF}(2)$,
hence induce the same matroid

the matroid is graphical because B is an incidence matrix of K_4

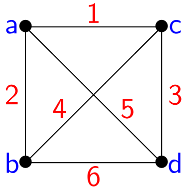


B base ... edges of a spanning tree
C circuit ... edges of a minimal cycle

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} \quad B = \begin{array}{cc} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} & \begin{array}{c} a \\ b \\ c \\ d \end{array} \end{array}$$

A and B have the same row spaces (codes) over $\mathrm{GF}(2)$,
hence induce the same matroid

the matroid is graphical because B is an incidence matrix of K_4



B base ... edges of a spanning tree
C circuit ... edges of a minimal cycle

matroids ... vertexless graphs

ξ ... random variable with outcomes $x_1, \ldots, x_m$

ξ … random variable with outcomes $x_1, \ldots, x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

ξ ... random variable with outcomes $x_1, ..., x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

Shannon entropy $H(\xi) = -p_1 \ln p_1 - \ldots - p_m \ln p_m$

ξ ... random variable with outcomes $x_1, ..., x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

Shannon entropy $H(\xi) = -p_1 \ln p_1 - \ldots - p_m \ln p_m$

... amount of uncertainty in ξ

ξ ... random variable with outcomes $x_1, ..., x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

Shannon entropy $H(\xi) = -p_1 \ln p_1 - \ldots - p_m \ln p_m$

... amount of uncertainty in ξ

between 0 and $\ln m$

ξ ... random variable with outcomes $x_1, ..., x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

Shannon entropy $H(\xi) = -p_1 \ln p_1 - \ldots - p_m \ln p_m$

... amount of uncertainty in ξ

between 0 and $\ln m$

$H(\xi) = 0$ iff all but one $p_1, \ldots, p_m$ equal zero

ξ ... random variable with outcomes $x_1, ..., x_m$

governed by $p_1, \ldots, p_m$, nonnegative, summing to 1

Shannon entropy $H(\xi) = -p_1 \ln p_1 - \ldots - p_m \ln p_m$

... amount of uncertainty in ξ

between 0 and $\ln m$

$H(\xi) = 0 \quad$ iff $\quad$ all but one $p_1, \ldots, p_m$ equal zero

$H(\xi) = \ln m \quad$ iff $\quad p_1 = \ldots = p_m = \frac{1}{m}$

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$$N = \{1\ ,\ 2\ ,\ 3\}\quad P$$

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1, 2, 3\}$ P

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels, e.g. $I = \{1\}$ P^I

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1, 2, 3\}$ P

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels,
keep the corresponding columns

e.g. $I = \{1\}$ P^I

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels, e.g. $I = \{1\}$ $\quad P^I$

keep the corresponding columns

erase row repetitions but add probabilities

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|l} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels,

keep the corresponding columns

erase row repetitions but add probabilities

e.g. $I = \{1\}\quad P^I$

$$\begin{array}{c|l} 0 & p_{000} + p_{011} \\ 1 & p_{101} + p_{110} \end{array}$$

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1\ ,\ 2\ ,\ 3\}$ P

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels,

keep the corresponding columns

erase row repetitions but add probabilities

to get the marginal distribution P^I of P

e.g. $I = \{1\}$ P^I

$$\begin{array}{c|c} 0 & p_{000} + p_{011} \\ 1 & p_{101} + p_{110} \end{array}$$

$\xi_1, \dots, \xi_n$ random variables governed by a distribution P

$N = \{1 , 2 , 3\}$ P

$$\begin{array}{ccc|c} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels,

keep the corresponding columns

erase row repetitions but add probabilities

e.g. $I = \{1\}$ P^I

$$\begin{array}{c|c} 0 & p_{000} + p_{011} \\ 1 & p_{101} + p_{110} \end{array}$$

to get the marginal distribution P^I of P

governing the subvector $\xi_I = (\xi_i)_{i \in I}$ of random variables

$\xi_1, \ldots, \xi_n$ random variables governed by a distribution P

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|l} 0 & 0 & 0 & p_{000} \\ 0 & 1 & 1 & p_{011} \\ 1 & 0 & 1 & p_{101} \\ 1 & 1 & 0 & p_{110} \end{array}$$

... an array of joint outcomes
with a column of probabilities
summing to one

for each set I of labels,

keep the corresponding columns

erase row repetitions but add probabilities

e.g. $I = \{1\}\quad P^I$

$$\begin{array}{c|l} 0 & p_{000} + p_{011} \\ 1 & p_{101} + p_{110} \end{array}$$

to get the marginal distribution P^I of P

governing the subvector $\xi_I = (\xi_i)_{i \in I}$ of random variables

look at the entropy $H(\xi_I)$

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|c} 0 & 0 & 0 & 1/4 \\ 0 & 1 & 1 & 1/4 \\ 1 & 0 & 1 & 1/4 \\ 1 & 1 & 0 & 1/4 \end{array}$$

... three binary variables

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

0	0	0	1/4
0	1	1	1/4
1	0	1	1/4
1	1	0	1/4

... three binary variables

$H(\xi_\emptyset)$	$H(\xi_1)$	$H(\xi_2)$	$H(\xi_3)$	$H(\xi_1,\xi_2)$	$H(\xi_1,\xi_3)$	$H(\xi_2,\xi_3)$	$H(\xi_1,\xi_2,\xi_3)$
0	$\ln 2$	$\ln 2$	$\ln 2$	$\ln 4$	$\ln 4$	$\ln 4$	$\ln 4$

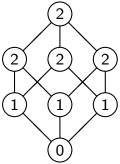
$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|c} 0 & 0 & 0 & 1/4 \\ 0 & 1 & 1 & 1/4 \\ 1 & 0 & 1 & 1/4 \\ 1 & 1 & 0 & 1/4 \end{array}$$

… three binary variables

$H(\xi_\emptyset)$	$H(\xi_1)$	$H(\xi_2)$	$H(\xi_3)$	$H(\xi_1,\xi_2)$	$H(\xi_1,\xi_3)$	$H(\xi_2,\xi_3)$	$H(\xi_1,\xi_2,\xi_3)$
0	$\ln 2$	$\ln 2$	$\ln 2$	$\ln 4$	$\ln 4$	$\ln 4$	$\ln 4$

matroidal rank function



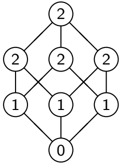
multiplied by $\ln 2$

$N = \{1\ ,\ 2\ ,\ 3\}\quad P$

$$\begin{array}{ccc|c} 0 & 0 & 0 & 1/4 \\ 0 & 1 & 1 & 1/4 \\ 1 & 0 & 1 & 1/4 \\ 1 & 1 & 0 & 1/4 \end{array}$$

... three binary variables

$H(\xi_\emptyset)$	$H(\xi_1)$	$H(\xi_2)$	$H(\xi_3)$	$H(\xi_1,\xi_2)$	$H(\xi_1,\xi_3)$	$H(\xi_2,\xi_3)$	$H(\xi_1,\xi_2,\xi_3)$
0	$\ln 2$	$\ln 2$	$\ln 2$	$\ln 4$	$\ln 4$	$\ln 4$	$\ln 4$

matroidal rank function 

multiplied by $\ln 2$

Theorem

If $\xi_1, \ldots, \xi_n$ are distributed uniformly on the linear code generated by a matrix A over $\mathbb{F}$ then $H(\xi_I) = \mathrm{rank}(A_I) \ln |\mathbb{F}|$, $I \subseteq N$.

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g\colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g\colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g \colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

$$g(I) \leqslant g(J) \quad \text{for } I \subseteq J \subseteq N$$

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g \colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

$$g(I) \leqslant g(J) \quad \text{for } I \subseteq J \subseteq N$$

$$g(I) + g(J) \geqslant g(I \cup J) + g(I \cap J) \quad \text{for } I, J \subseteq N.$$

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g\colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

$$g(I) \leqslant g(J) \quad \text{for } I \subseteq J \subseteq N$$

$$g(I) + g(J) \geqslant g(I \cup J) + g(I \cap J) \quad \text{for } I, J \subseteq N.$$

(Edmonts 1970), flows in networks, ‘greedy’ definition

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g\colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

$$g(I) \leqslant g(J) \quad \text{for } I \subseteq J \subseteq N$$

$$g(I) + g(J) \geqslant g(I \cup J) + g(I \cap J) \quad \text{for } I, J \subseteq N.$$

(Edmonts 1970), flows in networks, 'greedy' definition

books (Fujishige, Narayanan), review (Lovász 1982)

collecting basic properties of the entropies $H(\xi_I)$, $I \subseteq N$

Definition (Polymatroid)

(N, g) is a polymatroid, with a ground set N and rank function $g\colon I \mapsto [0, +\infty)$, $I \subseteq N$, if

$$g(\emptyset) = 0$$

$$g(I) \leqslant g(J) \quad \text{for } I \subseteq J \subseteq N$$

$$g(I) + g(J) \geqslant g(I \cup J) + g(I \cap J) \quad \text{for } I, J \subseteq N.$$

(Edmonts 1970), flows in networks, ‘greedy’ definition

books (Fujishige, Narayanan), review (Lovász 1982)

connections to entropy: Fujishige 1978, Pippenger 1986

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N,

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N,

is a polyhedral cone (intersection of finitely many halfspaces)

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N,
is a polyhedral cone (intersection of finitely many halfspaces)

H_N has finitely many extreme rays

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N, is a polyhedral cone (intersection of finitely many halfspaces)

H_N has finitely many extreme rays

given $\lambda_{I,J} \geqslant 0$, $\mu_{I,J} \geqslant 0$,

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N, is a polyhedral cone (intersection of finitely many halfspaces)

H_N has finitely many extreme rays

given $\lambda_{I,J} \geqslant 0$, $\mu_{I,J} \geqslant 0$,
for a polymatroidal rank function g

$$\sum_{I \subseteq J \subseteq N} \lambda_{I,J} [g(J) - g(I)] + \sum_{I,J \subseteq N} \mu_{I,J} [g(I) + g(J) - g(I \cup J) - g(I \cap J)] \geqslant 0$$

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N,

is a polyhedral cone (intersection of finitely many halfspaces)

H_N has finitely many extreme rays

given $\lambda_{I,J} \geqslant 0$, $\mu_{I,J} \geqslant 0$,

for a polymatroidal rank function g

$$\sum_{I \subseteq J \subseteq N} \lambda_{I,J}[g(J)-g(I)] + \sum_{I,J \subseteq N} \mu_{I,J}[g(I)+g(J)-g(I\cup J)-g(I\cap J)] \geqslant 0$$

where $g(\emptyset) = 0$

$H_N \subseteq \mathbb{R}^{2^N}$ ... the set of polymatroidal rank functions, given N, is a polyhedral cone (intersection of finitely many halfspaces)

H_N has finitely many extreme rays

given $\lambda_{I,J} \geqslant 0$, $\mu_{I,J} \geqslant 0$,
for a polymatroidal rank function g

$$\sum_{I \subseteq J \subseteq N} \lambda_{I,J} [g(J) - g(I)] + \sum_{I,J \subseteq N} \mu_{I,J} [g(I) + g(J) - g(I \cup J) - g(I \cap J)] \geqslant 0$$

where $g(\emptyset) = 0$

Shannon type inequality

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I \subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I \subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

In an entropic polymatroid (N, g), represented by ξ_N,

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I \subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

In an entropic polymatroid (N, g), represented by ξ_N,

$i \notin I$ and $g(I) = g(i \cup I)$ ... ξ_i a deterministic function of ξ_I

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I \subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

In an entropic polymatroid (N, g), represented by ξ_N,

$i \notin I$ and $g(I) = g(i \cup I)$ ... ξ_i a deterministic function of ξ_I

$I, J \subseteq N$ and $g(I) + g(J) = g(I \cup J) + g(I \cap J)$ ...

The polymatroid (N,g) is entropic if a random vector $\xi_N=(\xi_i)_{i\in N}$ exists such that $g(I)=H(\xi_I)$ for all $I\subseteq N$.

$I\mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I\subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

In an entropic polymatroid (N,g), represented by ξ_N,

$i\notin I$ and $g(I)=g(i\cup I)$ ... ξ_i a deterministic function of ξ_I

$I,J\subseteq N$ and $g(I)+g(J)=g(I\cup J)+g(I\cap J)$ ... $\xi_{I\setminus J}$ and $\xi_{J\setminus I}$ are conditionally independent given $\xi_{I\cap J}$

The polymatroid (N, g) is entropic if a random vector $\xi_N = (\xi_i)_{i \in N}$ exists such that $g(I) = H(\xi_I)$ for all $I \subseteq N$.

$I \mapsto H(\xi_I)$ ... entropy function

$\big(H(\xi_I)\big)_{I \subseteq N}$ ... entropic point, in $\mathbb{R}^{2^N}$

In an entropic polymatroid (N, g), represented by ξ_N,

$i \notin I$ and $g(I) = g(i \cup I)$ ... ξ_i a deterministic function of ξ_I

$I, J \subseteq N$ and $g(I) + g(J) = g(I \cup J) + g(I \cap J)$ ...

$\xi_{I \setminus J}$ and $\xi_{J \setminus I}$ are conditionally independent given $\xi_{I \cap J}$

in particular, if $I \cap J = \emptyset$ this is independence of ξ_I and ξ_J

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

$$\text{for } L \subseteq N \text{ let } g_1(L) = g(L \cap K) \text{ and } g_2(L) = g(L \cap (N \setminus K))$$

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

for $L \subseteq N$ let $g_1(L) = g(L \cap K)$ and $g_2(L) = g(L \cap (N \setminus K))$

then $g = g_1 + g_2$ and g is not on an extreme ray of H_N

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

for $L \subseteq N$ let $g_1(L) = g(L \cap K)$ and $g_2(L) = g(L \cap (N \setminus K))$

then $g = g_1 + g_2$ and g is not on an extreme ray of H_N

(provided $g_1 \neq 0$ and $g_2 \neq 0$ which implies each one is not a multiple of the other)

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

for $L \subseteq N$ let $g_1(L) = g(L \cap K)$ and $g_2(L) = g(L \cap (N \setminus K))$

then $g = g_1 + g_2$ and g is not on an extreme ray of H_N

(provided $g_1 \neq 0$ and $g_2 \neq 0$ which implies each one is not a multiple of the other)

Theorem (H.Q. Nguen 1978)

For a matroid (N, r), the rank function r is on an extreme ray of H_N iff it has a connected set $I \subseteq N$ such that $r(N \setminus I) = 0$.

a set $I \subseteq N$ in a polymatroid (N, g) is connected iff

$$g(I) = g(J) + g(I \setminus J) \text{ and } J \subseteq I \text{ imply } J = \emptyset \text{ or } J = I$$

if N not connected, decompose to $g(N) = g(K) + g(N \setminus K)$,

$$g(I \cup J) = g(I) + g(J) \text{ for all } I \subseteq K \text{ and } J \subseteq N \setminus K$$

for $L \subseteq N$ let $g_1(L) = g(L \cap K)$ and $g_2(L) = g(L \cap (N \setminus K))$

then $g = g_1 + g_2$ and g is not on an extreme ray of H_N

(provided $g_1 \neq 0$ and $g_2 \neq 0$ which implies each one is not a multiple of the other)

Theorem (H.Q. Nguen 1978)

For a matroid (N, r), the rank function r is on an extreme ray of H_N iff it has a connected set $I \subseteq N$ such that $r(N \setminus I) = 0$.

Nguyen: a necessary and sufficient condition for an integer polymatroid to be on an extreme ray of H_N

N ... a set of participants

N ... a set of participants

$0 \in N$ ... dealer of a secret

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

a polymatroid (N, g) admits a (perfect) secret sharing with the access structure $\mathcal{A}$ if

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

a polymatroid (N, g) admits a (perfect) secret sharing with the access structure $\mathcal{A}$ if

$g(0 \cup I) = g(I)$ for $I \in \mathcal{A}$

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

a polymatroid (N, g) admits a (perfect) secret sharing

with the access structure $\mathcal{A}$ if

$g(0 \cup I) = g(I)$ for $I \in \mathcal{A}$

$g(0 \cup J) = g(0) + g(J)$ for J containing no $I \in \mathcal{A}$

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

a polymatroid (N, g) admits a (perfect) secret sharing with the access structure $\mathcal{A}$ if

$g(0 \cup I) = g(I)$ for $I \in \mathcal{A}$

$g(0 \cup J) = g(0) + g(J)$ for J containing no $I \in \mathcal{A}$

this implies $g(0) \leqslant g(i)$, $i \in N$

N ... a set of participants

$0 \in N$ ... dealer of a secret

$\emptyset \neq \mathcal{A} \subseteq 2^{N \setminus 0}$ ... an access structure

if different $I, J \in \mathcal{A}$ are not in inclusion and $\bigcup \mathcal{A} = N \setminus 0$.

($I \in \mathcal{A}$ ... a minimal authorized group of participants)

a polymatroid (N, g) admits a (perfect) secret sharing with the access structure $\mathcal{A}$ if

$g(0 \cup I) = g(I)$ for $I \in \mathcal{A}$

$g(0 \cup J) = g(0) + g(J)$ for J containing no $I \in \mathcal{A}$

this implies $g(0) \leqslant g(i)$, $i \in N$

the sharing is ideal if $g(0) = g(i)$, $i \in N$

Theorem (Blakley Kabatianski 1997)

For a set N of participants and access structure $\mathcal{A}$, a polymatroid (N, g) admits perfect secret sharing with $\mathcal{A}$ and $g(i) = 1$, $i \in N$, iff (N, g) is a matroid.

Theorem (Blakley Kabatianski 1997)

For a set N of participants and access structure $\mathcal{A}$, a polymatroid (N, g) admits perfect secret sharing with $\mathcal{A}$ and $g(i) = 1$, $i \in N$, iff (N, g) is a matroid.

Brickell and Davenport 1991

Theorem (Blakley Kabatianski 1997)

For a set N of participants and access structure $\mathcal{A}$, a polymatroid (N,g) admits perfect secret sharing with $\mathcal{A}$ and $g(i)=1$, $i\in N$, iff (N,g) is a matroid.

Brickell and Davenport 1991

an analogous theorem identifying matroids in the network coding?

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

assume a sample $0, 2, 0, 0, 2, 2$ is observed

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

assume a sample $0, 2, 0, 0, 2, 2$ is observed

MLE suggests to guess that p be $1/2 = \operatorname{argmax}_p p^6(1-p)^6$

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

assume a sample $0, 2, 0, 0, 2, 2$ is observed

MLE suggests to guess that p be $1/2 = \mathrm{argmax}_p\, p^6(1-p)^6$

this is the same as taking the empirical distribution

$$P = (1/2, 0, 1/2)$$

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

assume a sample $0, 2, 0, 0, 2, 2$ is observed

MLE suggests to guess that p be $1/2 = \operatorname{argmax}_p p^6(1-p)^6$

this is the same as taking the empirical distribution

$$P = (1/2, 0, 1/2)$$

and minimizing the relative entropy $D(P, Q_p)$ over p

a variable with the outcomes $0, 1, 2$ governed by

$$Q_p = (p^2, 2p(1-p), (1-p)^2) \qquad \text{with } p \text{ unknown}$$

assume a sample $0, 2, 0, 0, 2, 2$ is observed

MLE suggests to guess that p be $1/2 = \mathrm{argmax}_p\, p^6(1-p)^6$

this is the same as taking the empirical distribution

$$P = (1/2, 0, 1/2)$$

and minimizing the relative entropy $D(P, Q_p)$ over p

the minimum is called the distance of P from model

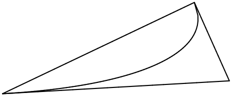
N. Ay 2002

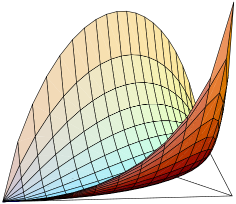
N. Ay 2002

suggested to maximize this distance from exponential families

N. Ay 2002

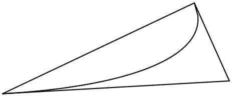
suggested to maximize this distance from exponential families

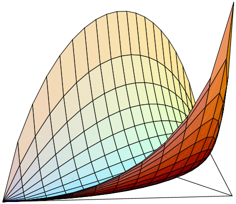




N. Ay 2002

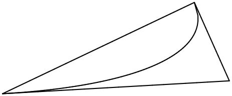
suggested to maximize this distance from exponential families

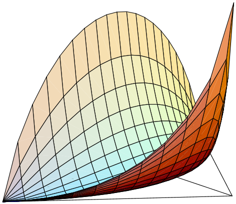




N. Ay 2002

suggested to maximize this distance from exponential families

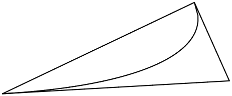


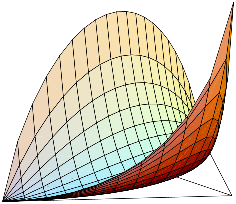


when the model consists of the factorizable distributions over

N. Ay 2002

suggested to maximize this distance from exponential families

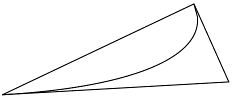


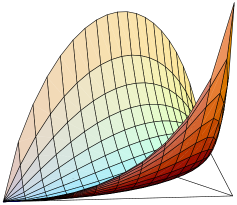


when the model consists of the factorizable distributions over a hypergraph (hierarchical log-linear models, in particular

N. Ay 2002

suggested to maximize this distance from exponential families

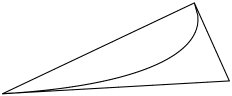


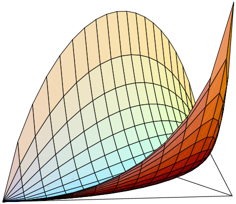


when the model consists of the factorizable distributions over a hypergraph (hierarchical log-linear models, in particular graphical Markov ones) then sometimes maximizers correspond to

N. Ay 2002

suggested to maximize this distance from exponential families





when the model consists of the factorizable distributions over a hypergraph (hierarchical log-linear models, in particular graphical Markov ones) then sometimes maximizers correspond to the ideal sss's (FM 2009)

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

Given the matroid, for which $t > 0$ is $(N, r \cdot t)$ entropic?

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

Given the matroid, for which $t > 0$ is $(N, r \cdot t)$ entropic?

Theorem (FM 1994)

Given a matroid (N, r) and $t \geqslant 0$, a random vector $(\xi_i)_{i \in N}$ represents $(N, r \cdot t)$ iff $t = \ln d$ for some integer $d \geqslant 1$ and ξ_I takes $d^{r(I)}$ values with the same probability, $I \subseteq N$.

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

Given the matroid, for which $t > 0$ is $(N, r \cdot t)$ entropic?

Theorem (FM 1994)

Given a matroid (N, r) and $t \geqslant 0$, a random vector $(\xi_i)_{i \in N}$ represents $(N, r \cdot t)$ iff $t = \ln d$ for some integer $d \geqslant 1$ and ξ_I takes $d^{r(I)}$ values with the same probability, $I \subseteq N$.

if this happens, the matroid is called p-representable of degree d

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

Given the matroid, for which $t > 0$ is $(N, r \cdot t)$ entropic?

Theorem (FM 1994)

Given a matroid (N, r) and $t \geqslant 0$, a random vector $(\xi_i)_{i \in N}$ represents $(N, r \cdot t)$ iff $t = \ln d$ for some integer $d \geqslant 1$ and ξ_I takes $d^{r(I)}$ values with the same probability, $I \subseteq N$.

if this happens, the matroid is called p-representable of degree d

… an equivalent combinatorial definition through partitions

If a matroid (N, r) is linear over a field $\mathbb{F}$
then the polymatroid $(N, r \ln |\mathbb{F}|)$ is entropic.

From now on, a matroid (N, r) is connected and $r(N) \geqslant 2$.

Given the matroid, for which $t > 0$ is $(N, r \cdot t)$ entropic?

Theorem (FM 1994)

Given a matroid (N, r) and $t \geqslant 0$, a random vector $(\xi_i)_{i \in N}$ represents $(N, r \cdot t)$ iff $t = \ln d$ for some integer $d \geqslant 1$ and ξ_I takes $d^{r(I)}$ values with the same probability, $I \subseteq N$.

if this happens, the matroid is called p-representable of degree d

… an equivalent combinatorial definition through partitions

… secret sharing matroids, almost affine codes

$d = 3$

$d = 3$

11	23	32
33	12	21
22	31	13

two orthogonal Latin squares

$d = 3$

11	23	32
33	12	21
22	31	13

two orthogonal Latin squares

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$

$d = 3$

11	23	32
33	12	21
22	31	13

two orthogonal Latin squares

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$

with the uniform distribution

$d = 3$

11	23	32
33	12	21
22	31	13

two orthogonal Latin squares

array of nine four-tuples $\{(i, j, k, l)\colon\ i, j \in \{1, 2, 3\}\}$ with the uniform distribution

the four variables represent the uniform matroid $U_{2,4}$

$d = 3$

11	23	32	
33	12	21	two orthogonal Latin squares
22	31	13	

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$
with the uniform distribution

the four variables represent the uniform matroid $U_{2,4}$

each representation of $U_{2,4}$ is of this sort

$d = 3$

11	23	32	
33	12	21	two orthogonal Latin squares
22	31	13	

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$ with the uniform distribution

the four variables represent the uniform matroid $U_{2,4}$

each representation of $U_{2,4}$ is of this sort

p-representation of $U_{2,4}$ of the degree $d = 10$ exists

$d = 3$

11	23	32
33	12	21
22	31	13

two orthogonal Latin squares

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$
with the uniform distribution

the four variables represent the uniform matroid $U_{2,4}$

each representation of $U_{2,4}$ is of this sort

p-representation of $U_{2,4}$ of the degree $d = 10$ exists

(ideal sss for 2 out 3 participants with the secret of size 10)

$d = 3$

11	23	32	
33	12	21	two orthogonal Latin squares
22	31	13	

array of nine four-tuples $\{(i, j, k, l) \colon i, j \in \{1, 2, 3\}\}$
with the uniform distribution

the four variables represent the uniform matroid $U_{2,4}$

each representation of $U_{2,4}$ is of this sort

p-representation of $U_{2,4}$ of the degree $d = 10$ exists
(ideal sss for 2 out 3 participants with the secret of size 10)

A matroid (N, r) is p-representable of the degree $2/3$ iff it is linear over $\mathrm{GF}(2)/\mathrm{GF}(3)$. (Beimel, FM, independently)

$d = |G|$ where $(G, \cdot)$ is a finite group

$d = |G|$ where $(G, \cdot)$ is a finite group

array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$

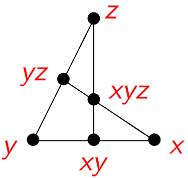
$d = |G|$ where $(G, \cdot)$ is a finite group

array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$

with d^3 rows and the uniform distribution

$d = |G|$ where $(G, \cdot)$ is a finite group

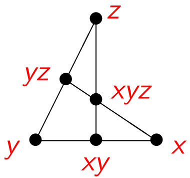
array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$



with d^3 rows and the uniform distribution

$d = |G|$ where $(G, \cdot)$ is a finite group

array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$

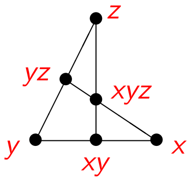


with d^3 rows and the uniform distribution

the six random variables p-represent the matroid

$d = |G|$ where $(G, \cdot)$ is a finite group

array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$



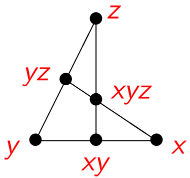
with d^3 rows and the uniform distribution

the six random variables p-represent the matroid

each representation of this matroid is of this type (FM 1999)

$d = |G|$ where $(G, \cdot)$ is a finite group

array $\{(x, y, z, xy, yz, xyz) \colon x, y, z \in G\}$



with d^3 rows and the uniform distribution

the six random variables p-represent the matroid

each representation of this matroid is of this type (FM 1999)

… an equivalent definition of the group via entropy

H_N ... the polymatroidal rank functions with the ground set N

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\mathrm{ent}} \subseteq H_N$ ... the entropy functions within

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\mathrm{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\mathrm{ent}})$ ... the closure of H_N^{ent}

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\mathrm{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\mathrm{ent}})$ ... the closure of H_N^{ent}

consists of almost entropic points (aent)

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\text{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\text{ent}})$ ... the closure of H_N^{ent}

consists of almost entropic points (aent)

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\text{ent}})$ *is a convex cone*

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\text{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\text{ent}})$ ... the closure of H_N^{ent}

consists of almost entropic points (aent)

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\text{ent}})$ *is a convex cone*

hence, $h \in cl(H_N^{\text{ent}})$ iff each $h \cdot t \in cl(H_N^{\text{ent}})$, $t \geqslant 0$

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\text{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\text{ent}})$ ... the closure of H_N^{ent}

consists of almost entropic points (aent)

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\text{ent}})$ is a convex cone

hence, $h \in cl(H_N^{\text{ent}})$ iff each $h \cdot t \in cl(H_N^{\text{ent}})$, $t \geqslant 0$

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\text{ent}})$ is a properly contained in H_N if $|N| \geqslant 4$

H_N ... the polymatroidal rank functions with the ground set N

$H_N^{\mathrm{ent}} \subseteq H_N$ ... the entropy functions within

$cl(H_N^{\mathrm{ent}})$ ... the closure of H_N^{ent}

consists of almost entropic points (aent)

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\mathrm{ent}})$ is a convex cone

hence, $h \in cl(H_N^{\mathrm{ent}})$ iff each $h \cdot t \in cl(H_N^{\mathrm{ent}})$, $t \geqslant 0$

Theorem (Zhang & Yeung 1997)

$cl(H_N^{\mathrm{ent}})$ is a properly contained in H_N if $|N| \geqslant 4$

non-Shannon type inequalities

a matroid (N, r) is aent if $r \in cl(H_N^{\mathrm{ent}})$

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for ‘subsets’

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions
iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

a matroid (N, r) is aent if $r \in cl(H_N^{\mathrm{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions
iff it holds in the aent matroids for ‘subsets’

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent
by Zhang & Yeung inequality

a matroid (N, r) is aent if $r \in cl(H_N^{\mathrm{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

by Zhang & Yeung inequality

the most simple and fundamental non-Shannon type $\leqslant$

a matroid (N, r) is aent if $r \in cl(H_N^{\mathrm{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

by Zhang & Yeung inequality

the most simple and fundamental non-Shannon type $\leqslant$

aent matroid can violate Ingleton inequality (FM 2007)

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

by Zhang & Yeung inequality

the most simple and fundamental non-Shannon type $\leqslant$

aent matroid can violate Ingleton inequality (FM 2007)

the class of aent matroids has ∞-many excluded minors

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

by Zhang & Yeung inequality

the most simple and fundamental non-Shannon type $\leqslant$

aent matroid can violate Ingleton inequality (FM 2007)

the class of aent matroids has ∞-many excluded minors

(FM, unpublished)

a matroid (N, r) is aent if $r \in cl(H_N^{\text{ent}})$

an inequality holds for the entropy functions

iff it holds in the aent matroids for 'subsets'

p-representable implies aent

an aent matroid exists without any p-representation (FM 2007)

Vamos matroid is not aent

by Zhang & Yeung inequality

the most simple and fundamental non-Shannon type $\leqslant$

aent matroid can violate Ingleton inequality (FM 2007)

the class of aent matroids has ∞-many excluded minors

(FM, unpublished)

? can a p-representable matroid violate Ingleton inequality ?