Matroidal Entropy Functions: A Quartet of Theories of Information, Matroid, Design and Coding

Qi Chen [1]

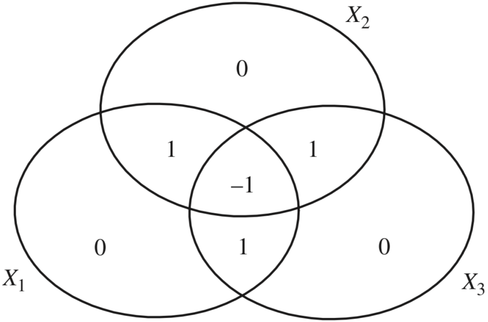
Joint work with Mingquan Cheng [2] and Baoming Bai [1]

1. ISN Lab and School of Telecommunication Engineering, Xidian University
2. Guangxi Normal University

The Chinese University of Hong Kong
April 20, 2023

A toy example

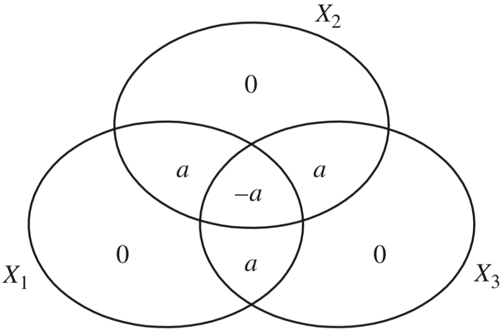
For a discrete random vector (X_1, X_2, X_3), X_1, X_2 and X_3 are pairwise independent, X_i is a function of X_j, X_k.



$X_1 \perp X_2$ and uniformly distributed on $\{0, 1\}$,
$X_3 = X_1 + X_2 \pmod 2$.

A toy example

X_1, X_2 and X_3 are pairwise independent, X_i is a function of X_j, X_k.



where $a = \log v$.
$X_1 \perp X_2$ and uniformly distributed on $\mathbb{Z}_v = \{0, 1, \cdots, v-1\}$
$X_3 = X_1 + X_2 \pmod{v}$. [1]

[1] Z. Zhang and R. W. Yeung, "A non-Shannon type conditional inequality of information quantities," *IEEE Trans. Info. Theory*, vol. 43, no. 11 pp. 1982-1986, Nov. 1997.

Extrames rays of Γ_3 containing matroidal entropy functions induced by matroid $U_{2,3}$

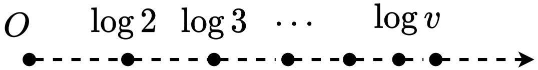


Figure: $R_{U_{2,3}} := \{a \cdot \mathbf{r}_{U_{2,3}} : a \geq 0\}$

Matroidal entropy function

$$\log v \cdot \mathbf{r}_{U_{2,3}}$$

where $v \geq 2$ is an integer and $\mathbf{r}_{U_{2,3}}$ is the rank function of the uniform matroid $U_{2,3}$.

$$\mathbf{r}_{U_{2,3}}(A) = \min\{2, |A|\} \quad \forall A \subseteq N = \{1, 2, 3\}.$$

Entropy functions

Entropy function

Let N be an indexed set. For a random vector $\mathbf{X}_N = (X_i, i \in N)$, the entropy function of $\mathbf{X}$ is a set function $\mathbf{h} : 2^N \to \mathbb{R}$ defined by

$$\mathbf{h}(A) = H(X_A),$$

for any $A \subseteq N$.

Entropy functions

Entropy function

Let N be an indexed set. For a random vector $\mathbf{X}_N = (X_i, i \in N)$, the entropy function of $\mathbf{X}$ is a set function $\mathbf{h} : 2^N \to \mathbb{R}$ defined by

$$\mathbf{h}(A) = H(X_A),$$

for any $A \subseteq N$.

Entropy space

$$\mathcal{H}_N \triangleq \mathbb{R}^{2^N}$$

Entropy functions

Entropy function

Let N be an indexed set. For a random vector $\mathbf{X}_N = (X_i, i \in N)$, the entropy function of $\mathbf{X}$ is a set function $\mathbf{h} : 2^N \to \mathbb{R}$ defined by

$$\mathbf{h}(A) = H(X_A),$$

for any $A \subseteq N$.

Entropy space

$$\mathcal{H}_N \triangleq \mathbb{R}^{2^N}$$

Entropy region:Γ_N^*

$$\Gamma_N^* \triangleq \{\mathbf{h} \in \mathcal{H}_N : \exists\ \mathbf{X}_N,\ \mathbf{h} \text{ is the entropy function of some } \mathbf{X}_N.\}$$

When $N = \{1, 2, \cdots, n\}$, we write it as Γ_n^*.

polymatroidal region

Shannon-type inequalities

For any $A, B \subseteq N$,

$$
\begin{aligned}
H(X_A) &\geq 0, \\
H(X_A) &\leq H(X_B) \quad \text{if } A \subseteq B, \\
H(X_A) + H(X_B) &\geq H(X_{A\cap B}) + H(X_{A\cup B}).
\end{aligned}
$$

Polymatroidal region:Γ_N

$$
\begin{aligned}
\Gamma_N \triangleq \{\mathbf{h} \in \mathcal{H}_N : \; & \mathbf{h}(A) \geq 0, \\
& \mathbf{h}(A) \leq \mathbf{h}(B), \quad \text{if } A \subseteq B, \\
& \mathbf{h}(A) + \mathbf{h}(B) \geq \mathbf{h}(A \cap B) + \mathbf{h}(A \cup B).\}
\end{aligned}
$$

Matroid

Definition

A matroid M is an ordered pair $(N, \mathbf{r})$, where the ground set N is a finite set and the rank function $\mathbf{r}$ is a set function on 2^N, and they satisfy the conditions that: for any $A, B \subseteq N$,

- $0 \leq \mathbf{r}(A) \leq |A|$ and $\mathbf{r}(A) \in \mathbb{Z}$.
- $\mathbf{r}(A) \leq \mathbf{r}(B)$, if $A \subseteq B$,
- $\mathbf{r}(A) + \mathbf{r}(B) \geq \mathbf{r}(A \cup B) + \mathbf{r}(A \cap B)$.

The value $\mathbf{r}(N)$ is called the rank of M.

Matroid

Definition

A matroid M is an ordered pair $(N, \mathbf{r})$, where the ground set N is a finite set and the rank function $\mathbf{r}$ is a set function on 2^N, and they satisfy the conditions that: for any $A, B \subseteq N$,

- $0 \leq \mathbf{r}(A) \leq |A|$ and $\mathbf{r}(A) \in \mathbb{Z}$.
- $\mathbf{r}(A) \leq \mathbf{r}(B)$, if $A \subseteq B$,
- $\mathbf{r}(A) + \mathbf{r}(B) \geq \mathbf{r}(A \cup B) + \mathbf{r}(A \cap B)$.

The value $\mathbf{r}(N)$ is called the rank of M.

Matroids are special cases of polymatroids

For a polymatroid $\mathbf{h} \in \Gamma_n$, if $\mathbf{h}(A) \in \mathbb{Z}$ and $\mathbf{h}(A) \leq |A|$, then $\mathbf{h}$ is the rank function of a matroid.

Uniform matroid

A uniform matroid $U_{t,n}$ with $0 \le t \le n$ is matroid $(N, \mathbf{r})$ with $|N| = n$ and

$$\mathbf{r}(A) = \min\{t, |A|\} \quad \forall A \subseteq N.$$

When $1 \le t \le n-1$, $U_{t,n}$ is a connected matroid.

Entropy functions on the extreme rays of Γ_N

Theorem

For a matroid $M = (N, \mathbf{r})$, $\mathbf{r}$ is on an extreme ray of Γ_N if and only if it is connected after deleting its loops. [2]

For a matroid $M = (N, \mathbf{r})$,

- $C \subseteq N$ is called a circuit of M if for any $e \in C$, $\mathbf{r}(C) = \mathbf{r}(C - e) = |C| - 1$,
- M is called connected if any two elements in N are in a circuit,
- a single element circuit, or a rank zero element is called a loop of M.

[2] H. Q. Nguyen, "Semimodular functions and combinatorial geometries," *Trans. AMS.*,vol. 238, pp. 355-383, April 1978.

Entropy functions on the extreme rays of Γ_N

Theorem

For a matroid $M = (N, \mathbf{r})$, $\mathbf{r}$ is on an extreme ray of Γ_N if and only if it is connected after deleting its loops. [2]

For a matroid $M = (N, \mathbf{r})$,

- $C \subseteq N$ is called a circuit of M if for any $e \in C$, $\mathbf{r}(C) = \mathbf{r}(C - e) = |C| - 1$,
- M is called connected if any two elements in N are in a circuit,
- a single element circuit, or a rank zero element is called a loop of M.

Entropy functions on 1-dimensional faces of Γ_N

[2] H. Q. Nguyen, "Semimodular functions and combinatorial geometries," *Trans. AMS.*,vol. 238, pp. 355-383, April 1978.

Matroidal entropy functions

Definition

For matroid M and positive integer $v \geq 2$, we call the entropy function in the form

$$\mathbf{h} = \log v \cdot \mathbf{r}_M$$

matroidal entropy function induced by M with degree v.

Extrames rays of Γ_3 containing matroidal entropy functions induced by matroid $U_{2,3}$

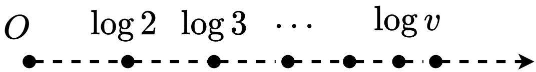


Figure: $R_{U_{2,3}} := \{a \cdot \mathbf{r}_{U_{2,3}} : a \geq 0\}$

Matroidal entropy function

$$\log v \cdot \mathbf{r}_{U_{2,3}}$$

where $v \geq 2$ is an integer and $\mathbf{r}_{U_{2,3}}$ is the rank function of the uniform matroid $U_{2,3}$.

Extrames rays containing $U_{2,3}$ and $U_{2,4}$

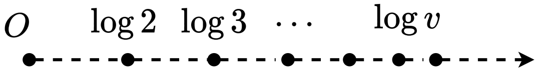


Figure: $R_{U_{2,3}} := \{a \cdot U_{2,3} : a \geq 0\}$

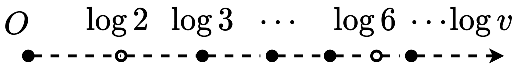
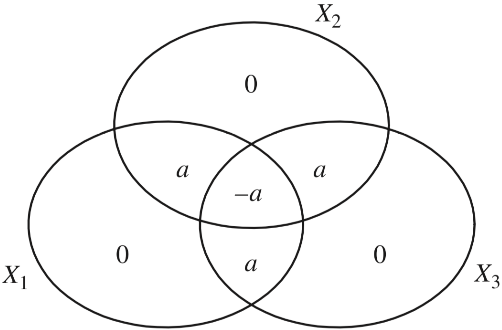


Figure: $R_{U_{2,4}} := \{a \cdot U_{2,4} : a \geq 0\}$

A polymatroid on $R_{U_{2,4}}$ is entropic if and only if $a = \log v$, $v \geq 3, v \neq 6$.

The toy example for $U_{2,3}$

X_1, X_2 and X_3 are pairwise independent, X_i is a function of X_j, X_k.



where $a = \log v$.

$X_1 \perp X_2$ and uniformly distributed on $\mathbb{Z}_v = \{0, 1, \cdots, v-1\}$

$X_3 = X_1 + X_2 \pmod{v}$.

Latin square: additive group

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

The multiplication table of the additive group $\langle \mathbb{Z}_v, + \rangle$

Latin square: quasigroup

0	1	2	3	4
1	0	3	4	2
2	4	0	1	3
3	2	4	0	1
4	3	2	2	0

If X_1 is uniformly distributed on rows and X_2 is uniform distributed on columns, then X_3 is uniformly distributed on the symbols

A bit more generalization

How to construct X_1, X_2, X_3, X_4 such that

- $X_i \perp X_j$ for each $1 \leq i < j \leq 4$
- X_k is a function of X_i and X_j for any $1 \leq i < j \leq 4$ and $k \in \{1, 2, 3, 4\} \setminus \{i, j\}$

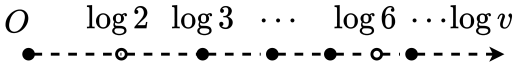


Figure: $R_{U_{2,4}} := \{a \cdot U_{2,4} : a \geq 0\}$

Mutually orthogonal latin squares

$$A := \begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix}, \qquad B := \begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix}$$

X_1, X_2, X_3 and X_4 are uniformly distributed on the rows, columns, symbols of the first square and symbols of the second square, respectively.

Mutually orthogonal latin squares

$$A := \begin{bmatrix} A & K & Q & J \\ Q & J & A & K \\ J & Q & K & A \\ K & A & J & Q \end{bmatrix}, \qquad B := \begin{bmatrix} \spadesuit & \heartsuit & \diamondsuit & \clubsuit \\ \clubsuit & \diamondsuit & \heartsuit & \spadesuit \\ \heartsuit & \spadesuit & \clubsuit & \diamondsuit \\ \diamondsuit & \clubsuit & \spadesuit & \heartsuit \end{bmatrix}$$

X_1, X_2, X_3 and X_4 are uniformly distributed on the rows, columns, symbols of the first square and symbols of the second square, respectively.

For this case, $v \neq 2, 6$

- $v \neq 2$: trivial
- $v \neq 6$: Euler's 36 officer problem

Characterizing matroidal entropy functions via variable strength orthogonal array(VOA)

Theorem

A random vector $\mathbf{X} = (X_i : i \in N)$ *characterizes matroidal entropy function* $\log v \cdot \mathbf{r}_M$ *for a connected matroid with rank* $\mathbf{r}(N) \geq 2$ *if and only if random variable* $Y = \mathbf{X}$ *is uniformly distributed on the rows of a* $\mathrm{VOA}(M, v)$. [3]

[3] Q. Chen, M. Cheng and B. Bai, "Matroidal entropy functions: a quartet of theories of information, matroid, design and coding," *Entropy*, vol. 23:3, 1-11, 2021.

Characterizing matroidal entropy functions via variable strength orthogonal array(VOA)

Theorem

A random vector $\mathbf{X} = (X_i : i \in N)$ *characterizes matroidal entropy function* $\log v \cdot \mathbf{r}_M$ *for a connected matroid with rank* $\mathbf{r}(N) \geq 2$ *if and only if random variable* $Y = \mathbf{X}$ *is uniformly distributed on the rows of a* $\mathrm{VOA}(M, v)$*.* [3]

Corollary

For a connected matroid $M = (N, \mathbf{r}_M)$ *with rank* $\mathbf{r}(N) \geq 2$*, if the polymatroid*

$$a \cdot \mathbf{r}_M$$

with $a > 0$ *is entropic, then* $a = \log v$ *for some integer* $v \geq 2$*.*

---

[3] Q. Chen, M. Cheng and B. Bai, "Matroidal entropy functions: a quartet of theories of information, matroid, design and coding," *Entropy*, vol. 23:3, 1-11, 2021.

Probabilistically characteristic set of a matroid

For a matroid M, we call the set χ_M of all $v \geq 2$ such that $\mathbf{h} = \log v \cdot M$ is entropic the probabilistically (p-)characteristic set of M.

Probabilistically characteristic set of a matroid

For a matroid M, we call the set χ_M of all $v \geq 2$ such that $\mathbf{h} = \log v \cdot M$ is entropic the probabilistically (p-)characteristic set of M.

$$\chi_{U_{2,3}} = \{v \in \mathbb{Z} : v \geq 2\}, \quad \chi_{U_{2,4}} = \{v \in \mathbb{Z} : v \geq 3, v \neq 6\}$$

Orthogonal array

Example

0	1	2
1	2	0
2	0	1

0	1	2
2	0	1
1	2	0

0	0	0	0
0	1	1	1
0	2	2	2
1	0	1	2
1	1	2	0
1	2	0	1
2	0	2	1
2	1	0	2
2	2	1	0

is an $\mathrm{OA}(2, 4, 3)$ corresponding to the MOLS.

Orthogonal array

Definition

A $\lambda v^t \times n$ array T with entries from $\mathbb{Z}_v$ is called an orthogonal array of strength t, factor n, level v and index λ if any $\lambda v^t \times t$ subarray of T contains each t-tuple in $\mathbb{Z}_v^t$ exactly λ times as a row. We call T an $\mathrm{OA}(\lambda \times v^t; t, n, v)$.

Orthogonal array

Definition

A $\lambda v^t \times n$ array T with entries from $\mathbb{Z}_v$ is called an orthogonal array of strength t, factor n, level v and index λ if any $\lambda v^t \times t$ subarray of T contains each t-tuple in $\mathbb{Z}_v^t$ exactly λ times as a row. We call T an $\mathrm{OA}(\lambda \times v^t; t, n, v)$.

When $\lambda = 1$, we say such orthogonal array has *index unity* and call it an $\mathrm{OA}(t, n, v)$ for short.

Variable strength orthogonal array(VOA)

Definition

Given a matroid $M = (N, \mathbf{r})$ with $\mathbf{r}(N) \geq 2$,

- a $v^{\mathbf{r}(N)} \times n$ array T
- with columns indexed by N,
- entries from $\mathbb{Z}_v$,

is called a variable strength orthogonal array(VOA) induced by M with level v if for any $A \subseteq N$, $v^{\mathbf{r}(N)} \times |A|$ subarray of T consisting of columns indexed by A satisfy the following condition:

- each row of this subarray occurs $v^{\mathbf{r}(N)-\mathbf{r}(A)}$ times.

We also call such T a $\mathrm{VOA}(M, v)$.

Variable strength orthogonal array(VOA)

Definition

Given a matroid $M = (N, \mathbf{r})$ with $\mathbf{r}(N) \geq 2$,

- a $v^{\mathbf{r}(N)} \times n$ array T
- with columns indexed by N,
- entries from $\mathbb{Z}_v$,

is called a variable strength orthogonal array(VOA) induced by M with level v if for any $A \subseteq N$, $v^{\mathbf{r}(N)} \times |A|$ subarray of T consisting of columns indexed by A satisfy the following condition:

- each row of this subarray occurs $v^{\mathbf{r}(N)-\mathbf{r}(A)}$ times.

We also call such T a $\mathrm{VOA}(M, v)$.

For $U_{t,n}$, $\mathrm{VOA}(U_{t,n}, v) = \mathrm{OA}(t, n, v)$

Variable strength orthogonal array

Example

Let $M_1 = (N, \mathbf{r}_1)$ be a matroid with $N = \{1,2,3,4,5\}$ and rank function

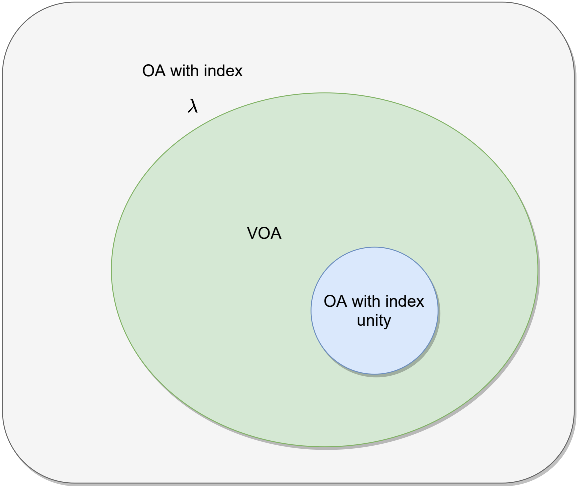
$$\mathbf{r}_1(A) = \begin{cases} |A| & |A| \leq 2 \\ 2 & A \in \{\{1,2,3\},\{3,4,5\}\} \\ 3 & \text{o.w.} \end{cases}$$

Then

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{matrix}$$

is a $\mathrm{VOA}(M_1, 2)$.

Relations between *OA* and *VOA*



Relations to coding theory

For a matroid M over a field $\mathrm{GF}(q)$, that is, M is the vector matroid of a matrix $\hat{M}$ over $\mathrm{GF}(q)$, the set of rows of a $\mathrm{VOA}(M, q)$ is the code book of the (n, k, q) linear code generated by $\hat{M}$, where $k = \mathbf{r}_M(N)$.

Relations to coding theory

For a matroid M over a field $\mathrm{GF}(q)$, that is, M is the vector matroid of a matrix $\hat{M}$ over $\mathrm{GF}(q)$, the set of rows of a $\mathrm{VOA}(M,q)$ is the code book of the (n,k,q) linear code generated by $\hat{M}$, where $k = \mathbf{r}_M(N)$.

Example

Let $M_1 = (N, \mathbf{r}_1)$ be a matroid with $N = \{1,2,3,4,5\}$ and rank function

$$\mathbf{r}_1(A) = \begin{cases} |A| & |A| \leq 2 \\ 2 & A \in \{\{1,2,3\},\{3,4,5\}\} \\ 3 & \text{o.w.} \end{cases}$$

is the vector matroid of the matrix

$$\hat{M}_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Relations to coding theory

Example

For matrix

$$\hat{M}_1 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

the mapping $\mathbf{x} \mapsto \mathbf{x}M$ maps the tuples in $\mathbb{Z}_2^3$ to the set of rows of $\mathrm{VOA}(M_1, 2)$ below.

$$\begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \end{matrix}$$

It is a $(5, 3, 2)$ linear code.

Almost affine code

Definition

For a set of v symbols, say $\mathbb{Z}_v$, $\mathcal{C} \subseteq \mathbb{Z}_v^N$ is called an almost affine code if

$$\mathbf{r}(A) := \log_v |\mathcal{C}_A| \quad (1)$$

is an integer for all $A \subseteq N$. [4]

[4] J. Simonis and A. Ashikhmin, "Almost affine codes," *Desings, Codes Cryptogr.*, vol. 14, pp. 179–797, 1998.

Almost affine code

Definition

For a set of v symbols, say $\mathbb{Z}_v$, $\mathcal{C} \subseteq \mathbb{Z}_v^N$ is called an almost affine code if

$$\mathbf{r}(A) := \log_v |\mathcal{C}_A| \qquad (1)$$

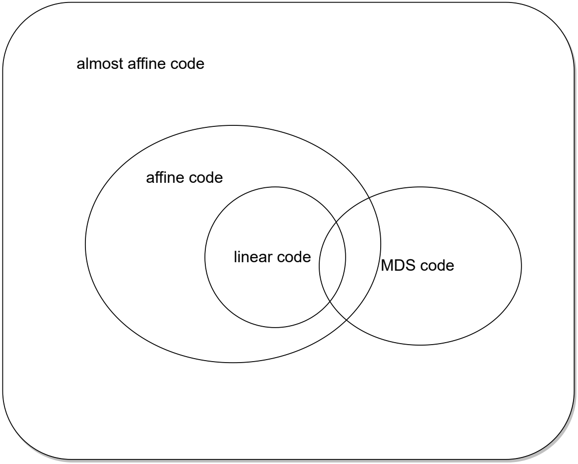
is an integer for all $A \subseteq N$. [4]

Almost affine code induced by matroid

- For any almost affine code $\mathcal{C}$, $(N, \mathbf{r})$ forms a matroid M, where the rank function $\mathbf{r}$ is defined in (1). We call such almost affine code an (M, v) (almost affine) code.
- For an (M, v) code, if M is a uniform matroid $U_{t,n}$, it coincides with a (n, t, v) maximum distance separable (MDS) code.

[4] J. Simonis and A. Ashikhmin, "Almost affine codes," *Desings, Codes Cryptogr.*, vol. 14, pp. 179–797, 1998.

Almost affine code



(7, 4) Hamming code is a characterization of the dual matroid of Fano matroid

Parity check matrix of (7, 4) Hamming code.

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

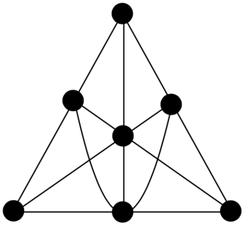
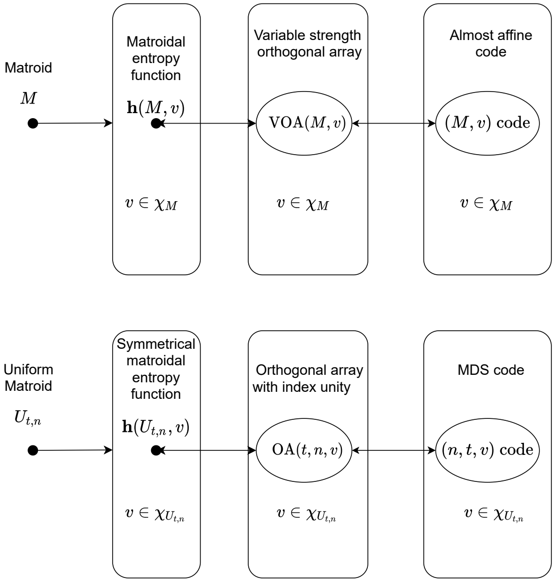


Figure: Fano matroid

Correspondences among four fields



Some applications

- E. F. Brickell.; D. M. Davenport, "On the classification of ideal secret sharing schemes," *J. Cryptol.* vol. 4, 123-134, 1991.
- R. Dougherty, C. Freiling and K Zeger,"Networks, matroids, and non-Shannon information inequalities," *IEEE Trans. Inf. Theory* vol. 53, pp. 1949-1969, 2007. (network coding)
- S. El Rouayheb, A. Sprintson and C. Georghiades, "On the index coding problem and its relation to network coding and matroid theory", *IEEE Trans. Inf. Theory* vol. 56, no.7 pp. 3187-3195, 2010.
- T. Westerbäck, R. Freij-Hollanti, T. Ernvall and C. Hollanti, "On the combinatorics of locally repairable codes via matroid theory", *IEEE Trans. Inf. Theory* vol. 62, no.10 pp. 5296-5315, 2016.

An application to network coding

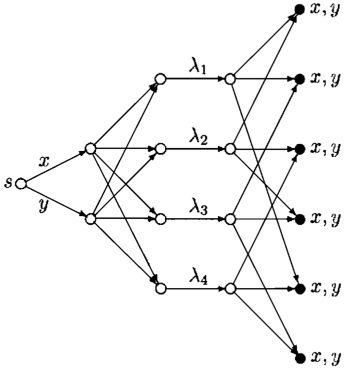


Figure: $\lambda_1 = x, \lambda_2 = y, \lambda_3 = L_1(x, y), \lambda_4 = L_2(x, y)$, where L_1, L_2 are MOLSs. Thus, $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ forms $\mathrm{VOA}(U_{2,4}, v)$.

Determine χ_M of a matroid via VOA operations of the corresponding matroid operation

- Q. Chen, M. Cheng, and B. Bai,"Matroidal entropy functions: constructions, characterizations and representations," in IEEE Int.Symp. Info. Theory, Espoo, Finland June 2022.
- Q. Chen, M. Cheng, and B. Bai,"Matroidal entropy functions: constructions, characterizations and representations," in preparing for submitting to *IEEE, Trans. Inf. Theory*

Matroid operations

Unitary matroid operations

- deletion
- contraction
- minor

Binary matroid operations

- series connection
- parallel connection
- 2-sum

Matroid operations: deletion

Definition (Deletion)

Given a matroid $M = (N, \mathbf{r})$ and $S \subseteq N$, the matroid $M \setminus S = (N', \mathbf{r}')$ with $N' = N \setminus S$ and

$$\mathbf{r}'(A) = \mathbf{r}(A), \quad \forall A \subseteq N'$$

is called a matroid of M deleted by S or the restriction of M on N'.

VOA operations: deletion

For $S \subseteq N$, let $\mathbf{T} \setminus S$ denote the array whose rows are exactly those of $\mathbf{T}(N')$ with each occurring once, where $N' = N \setminus S$.

$\mathbf{T} : \mathrm{VOA}(U_{3,4}, 2)$

0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$\mathbf{T} \setminus \{3,4\} : \mathrm{VOA}(U_{2,2}, 2)$

0	0
0	1
1	0
1	1

Note that
$U_{2,2} \simeq U_{3,4} \setminus \{3,4\}$.

VOA operations:deletions

Proposition

For a $\mathrm{VOA}(M, v)$ $\mathbf{T}$ *and* $S \subseteq N$, $\mathbf{T} \setminus S$ *is a* $\mathrm{VOA}(M \setminus S, v)$.

Matroid operations: contractions

Definition (Contraction)

Given a matroid $M = (N, \mathbf{r})$ and $S \subseteq N$, the matroid $M/S = (N', \mathbf{r}')$ with $N' = N \setminus S$ and

$$\mathbf{r}'(A) = \mathbf{r}(A \cup S) - \mathbf{r}(S), \quad \forall A \subseteq N'$$

is called the contraction of S from M.

VOA operations: contraction

For a $\mathrm{VOA}(M, v)$ $\mathbf{T}$ and $S \subseteq N$, let $\mathbf{a}$ be a row of $\mathbf{T}(S)$. We denote by $\mathbf{T}_{|S:\mathbf{a}}$ the array whose rows are $\mathbf{c}(N \setminus S)$ with $\mathbf{c}$ the rows of $\mathbf{T}$ and $\mathbf{c}(S) = \mathbf{a}$.

$\mathbf{T} : \mathrm{VOA}(U_{3,4}, 2)$

0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

$\mathbf{T}_{|\{4\}:0} : \mathrm{VOA}(U_{2,3}, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

Note that $U_{2,3} \simeq U_{3,4}/\{4\}$.

VOA operations: contractions

Proposition

For a $\mathrm{VOA}(M, v)$ $\mathbf{T}$ *and* $S \subseteq N$, $\mathbf{T}_{|S:\mathbf{a}}$ *is a* $\mathrm{VOA}(M/S, v)$ *where* $\mathbf{a}$ *is any row of* $\mathbf{T}(S)$.

Matroid operations: minors

Definition (Minor)

For a sequence of disjoint $S_1, S_2, \ldots, S_k \subseteq N$, M being deleted or contracted by S_i, the result can be written in the form of $M \setminus S / T$, where S is the union of the deleted S_i and T is the union of the contracted S_j. Such $M \setminus S / T$ is called a minor of M.

Matroid operations: minors

Definition (Minor)

For a sequence of disjoint $S_1, S_2, \ldots, S_k \subseteq N$, M being deleted or contracted by S_i, the result can be written in the form of $M \setminus S / T$, where S is the union of the deleted S_i and T is the union of the contracted S_j. Such $M \setminus S / T$ is called a minor of M.

Theorem

Let M be a matroid and M' be its minor. Then $\chi_M \subseteq \chi_{M'}$.

Proof sketch.

If $\mathrm{VOA}(M, v)$ is constructible, so is $\mathrm{VOA}(M', v)$. □

Matroid operations

Unitary matroid operations

- deletion
- contraction
- minor

Binary matroid operations

- series connection
- parallel connection
- 2-sum

Matroid operations: series and parallel connections

Definition (Series and parallel connections)

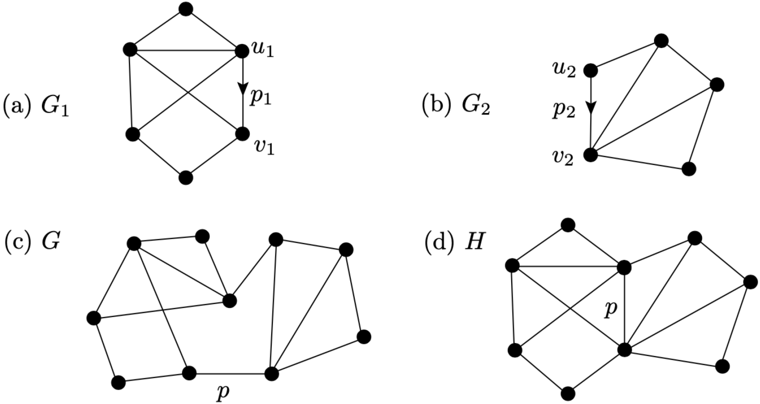
For two matroids $M_1 = (N_1, \mathbf{r}_1)$ and $M_2 = (N_2, \mathbf{r}_2)$ with $p_i \in N_i$, p_i neither loops nor coloops, $i = 1, 2$, and any $p \notin N_1 \cup N_2$ the series connection $S((M_1; p_1), (M_2; p_2))$ of M_1 and M_2 with respect to base points p_1 and p_2 is a matroid with ground set $N \triangleq (N_1 \setminus p_1) \cup (N_2 \setminus p_2) \cup p$ and family of circuits

$$\begin{aligned} \mathcal{C}_S =& \mathcal{C}(M_1 \setminus p_1) \cup \mathcal{C}(M_2 \setminus p_2) \\ & \cup \{(C_1 - p_1) \cup (C_2 - p_2) \cup p : C_i \in \mathcal{C}(M_i), i = 1, 2\} \end{aligned} \quad (2)$$

and the parallel connection $P((M_1; p_1), (M_2; p_2))$ of M_1 and M_2 with respect to base points p_1 and p_2 is a matroid with ground set N and family of circuits

$$\begin{aligned} \mathcal{C}_P =& \mathcal{C}(M_1 \setminus p_1) \cup \mathcal{C}(M_2 \setminus p_2) \cup \{(C_1 - p_1) \cup p : C_1 \in \mathcal{C}(M_1)\} \\ & \cup \{(C_2 - p_2) \cup p : C_2 \in \mathcal{C}(M_2)\} \end{aligned} \quad (3)$$

Matroid operations: series and parallel connections



VOA operations: series connections

Let

- $\mathbf{T}_1$ be a $\mathrm{VOA}(M_1, v)$ with $M_1 = (N_1, \mathbf{r}_1)$,
- $\mathbf{T}_2$ be a $\mathrm{VOA}(M_2, v)$ with $M_1 = (N_2, \mathbf{r}_2)$,
- v an integer and
- $\mathbf{U}$ be any $\mathrm{VOA}(U_{2,3}, v)$.

We construct a $v^{rs} \times (|N_1| + |N_2| - 1)$ array $\mathbf{T}$ with columns indexed by $N = (N_1 \setminus p_1) \cup (N_2 \setminus p_2) \cup p$ according to the following rule, where $r_S = \mathbf{r}_1(N_1) + \mathbf{r}_2(N_2)$.

- For any row $\mathbf{a}_1$ of $\mathbf{T}_1$ and $\mathbf{a}_2$ of $\mathbf{T}_2$, we construct a row $\mathbf{b}$ of $\mathbf{T}$ such that
- $\mathbf{b}(N_1 \setminus p_1) = \mathbf{a}_1(N_1 \setminus p_1)$, $\mathbf{b}(N_2 \setminus p_2) = \mathbf{a}_2(N_2 \setminus p_2)$ and $(\mathbf{a}_1(p_1), \mathbf{a}_2(p_2), \mathbf{b}(p))$ is a row of $\mathbf{U}$.

We denote such constructed $\mathbf{T}$ by $S((\mathbf{T}_1; p_1), (\mathbf{T}_2; p_2))$ or $S(\mathbf{T}_1, \mathbf{T}_2)$ if there is no ambiguity. It can be checked that $\mathbf{T}$ is a VOA.

VOA operations: series connections

$\mathbf{T}_1 : \mathrm{VOA}(U_{2,3}, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

$\mathbf{T}_2 : \mathrm{VOA}(U_{2,3}, 2)$

0	0	1
0	1	0
1	0	0
1	1	1

$S(\mathbf{T}_1, \mathbf{T}_2)$

0	0	0	0	1
0	0	0	1	0
0	1	1	0	1
0	1	1	1	0
⋮	⋮	⋮	⋮	⋮
1	1	1	1	1

is a $\mathrm{VOA}(U_{4,5}, 2)$, where $U_{4,5} \simeq S(U_{2,3}, U_{2,3})$.

$\mathbf{U} : \mathrm{VOA}(U_{2,3}, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

VOA operations: series connections

Proposition

For a $\mathrm{VOA}(M_1, v)$ $\mathbf{T}_1$ *and a* $\mathrm{VOA}(M_2, v)$ $\mathbf{T}_2$*, the array* $S((\mathbf{T}_1; p_1), (\mathbf{T}_2; p_2))$ *is a* $\mathrm{VOA}(S((M_1; p_1), (M_2, p_2)), v)$*.*

VOA operations: parallel connections

Let

- $\mathbf{T}_1$ be a $\mathrm{VOA}(M_1, v)$ with $M_1 = (N_1, \mathbf{r}_1)$,
- $\mathbf{T}_2$ be a $\mathrm{VOA}(M_2, v)$ with $M_1 = (N_1, \mathbf{r}_2)$ and
- v an integer.

We construct a $v^{r_P} \times (|N_1| + |N_2| - 1)$ array $\mathbf{T}$ with columns indexed by $N = (N_1 \setminus p_1) \cup (N_2 \setminus p_2) \cup p$ according to the following rule, where $r_P = r_1 + r_2 - 1$.

- For any row $\mathbf{a}_1$ of $\mathbf{T}_1$ and $\mathbf{a}_2$ of $\mathbf{T}_2$ with $\mathbf{a}_1(p_1) = \mathbf{a}_2(p_2)$, we construct row $\mathbf{b}$ of $\mathbf{T}$ such that
- $\mathbf{b}(N_i \setminus p_i) = \mathbf{a}_i$, $i = 1, 2$, and $\mathbf{b}(p) = \mathbf{a}_1(p_1)$.

We denote such constructed $\mathbf{T}$ by $P((\mathbf{T}_1; p_1), (\mathbf{T}_2; p_2))$ or $P(\mathbf{T}_1, \mathbf{T}_2)$ if there is no ambiguity. It can be checked that $\mathbf{T}$ is a VOA.

VOA operations: parallel connections

Example

$\mathbf{T}_1 : \mathrm{VOA}(U_{2,3}, 2)$

0	0	0
0	1	1
1	0	1
1	1	0

$\mathbf{T}_2 : \mathrm{VOA}(U_{2,3}, 2)$

0	0	1
0	1	0
1	0	0
1	1	1

$P(\mathbf{T}_1, \mathbf{T}_2)$

0	0	0	0	1
0	0	0	1	0
0	1	1	0	0
0	1	1	1	1
1	0	1	0	0
1	0	1	1	1
1	1	0	0	1
1	1	0	1	0

is a $\mathrm{VOA}(M_1, 2)$, where $M_1 = P(U_{2,3}, U_{2,3})$.

VOA operations: parallel connections

Proposition

For a $\mathrm{VOA}(M_1, v)$ $\mathbf{T}_1$ *and a* $\mathrm{VOA}(M_2, v)$ $\mathbf{T}_2$*, the array* $P((\mathbf{T}_1; p_1), (\mathbf{T}_2; p_2))$ *is a* $\mathrm{VOA}(P((M_1; p_1), (M_2, p_2)), v)$*.*

Matroid operations: 2-sum

Definition

For matroids $M_1 = (N_1, \mathbf{r}_1)$ and $M_2 = (N_2, \mathbf{r}_2)$, the 2-sum of them $M_1 \oplus_2 M_2$ is defined by $S(M_1, M_2)/p$ or equivalently $P(M_1, M_2) \setminus p$.

VOA operations: 2-sum

Let

- $\mathbf{T}_1$ be a $\mathrm{VOA}(M_1, v)$ with $M_1 = (N_1, \mathbf{r}_1)$,
- $\mathbf{T}_2$ be a $\mathrm{VOA}(M_2, v)$ with $M_1 = (N_1, \mathbf{r}_2)$,
- v an integer.

We construct $\mathbf{T}_1 \oplus_2 \mathbf{T}_2$ by

- $S(\mathbf{T}_1, \mathbf{T}_2)|_{p:a}$ for some $a \in \mathbb{Z}_v$, or equivalently
- $P(\mathbf{T}_1, \mathbf{T}_2) \setminus p$.

Proposition

For a $\mathrm{VOA}(M_1, v)$ $\mathbf{T}_1$ *and a* $\mathrm{VOA}(M_2, v)$ $\mathbf{T}_2$*,* $\mathbf{T}_1 \oplus_2 \mathbf{T}_2$ *is a* $\mathrm{VOA}(M_1 \oplus_2 M_2, v)$*.*

Characteristic set of binary VOA operations

Theorem

For any matroids M_1 and M_2, $\chi_{M_1 \oplus_2 M_2} = \chi_{M_1} \cap \chi_{M_2}$.

Smaller building blocks

Corollary

The p-characteristic set of a connected matroid is the intersection of the p-characteristic set of its 3-connected components.

Regular matroids

Definition

A matroid M is regular if it is represented by a totally unimodular matrix, i.e., a matrix over $\mathbb{R}$ for which every square submatrix has determinant in $\{-1, 1, 0\}$.

Theorem

For a matroid M, $\chi_M = \{v \in \mathbb{Z} : v \geq 2\}$ if and only if M is regular.

Proof Sketch.

- For the if part construct a totally unimodular matrix, i.e., a matrix over a ring $\mathbb{Z}_v$;
- for the only if part, excluded minor of regular matroid $U_{2,4}$, F_7 and F_7^*.

□

Regular matroids

Definition

A matroid M is regular if it is represented by a totally unimodular matrix, i.e., a matrix over $\mathbb{R}$ for which every square submatrix has determinant in $\{-1, 1, 0\}$.

Theorem

For a matroid M, $\chi_M = \{v \in \mathbb{Z} : v \geq 2\}$ if and only if M is regular.

Proof Sketch.

- For the if part construct a totally unimodular matrix, i.e., a matrix over a ring $\mathbb{Z}_v$;
- for the only if part, excluded minor of regular matroid $U_{2,4}$, F_7 and F_7^*.

□

Remark

It is a generalization of the matroid representation problem over a field.

Whirl matroids

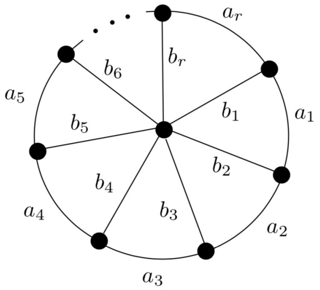


Figure: The wheel graph $\mathcal{W}_r$

Definition

The whirl matroid $\mathcal{W}^r$ is a matroid by relaxing the circuit-hyperplane A, i.e., the rim of the wheel matroid $M(\mathcal{W}_r)$.

Note that $\mathcal{W}^2 = U_{2,4}$.

Whirl matroids

Proposition

For matroid $\mathcal{W}^r$, $r \geq 2$, $\chi_{\mathcal{W}^r} = \chi_{U_{2,4}} = \{v \in \mathbb{Z} : v \geq 3, v \neq 6\}$.

Matroids with the same p-characteristic set as $U_{2,4}$

Theorem

For any matroid M, let M_i be its connected components, and $M_{i,j}$ be the 3-connected components of M_i. Then $\chi_M = \chi_{U_{2,4}}$ if each of these $M_{i,j}$ is either a regular matroid or a $\mathcal{W}^r$ with $r \geq 2$, and at least one of them is a $\mathcal{W}^r$.

Thank you!