Combinatorial Representations

Maximilien Gadouleau
Joint work with Peter J. Cameron and Søren Riis

Queen Mary, University of London

26 October, 2011

Outline

Outline

Combinatorial representations

- $E = \{1, \ldots, n\}$ (elements), $\mathcal{B} \subseteq \binom{E}{r}$ (bases) a family of r-subsets of E (r: rank)
- A a finite set with $|A| \geq 2$ (alphabet)
- Combinatorial representation of $(E, \mathcal{B})$ over A: collection of n functions $f_i : A^r \to A$ s.t. for all $b = \{i_1, \ldots, i_r\} \in \binom{E}{r}$

$$\begin{aligned} f_b &: A^r \to A^r \\ f_b(x_1, \ldots, x_r) &= (f_{i_1}(x_1, \ldots, x_r), \ldots, f_{i_r}(x_1, \ldots, x_r)) \end{aligned}$$

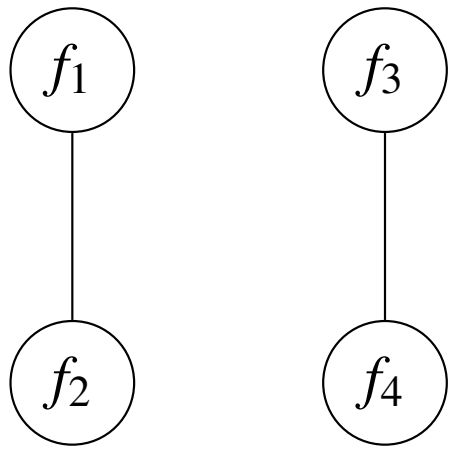
is a bijection iff $b \in \mathcal{B}$

Motivating example: secure data dissemination

- Alice has two messages $x_1, x_2 \in A$ she wants to transmit to two receivers
- She can encode her messages using functions

$$f_1(x_1, x_2), \quad f_2(x_1, x_2), \quad f_3(x_1, x_2), \quad f_4(x_1, x_2)$$

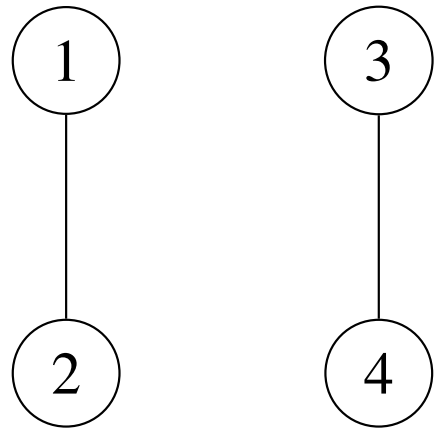
- An eavesdropper Eve intercepts one message sent to each receiver



- Each receiver should decode, whereas Eve must not

Example, continued

- $E = \{1,2,3,4\}, \mathcal{B} = \{\{1,2\},\{3,4\}\}$



- Without loss, $A = \mathbb{Z}_{|A|}$,

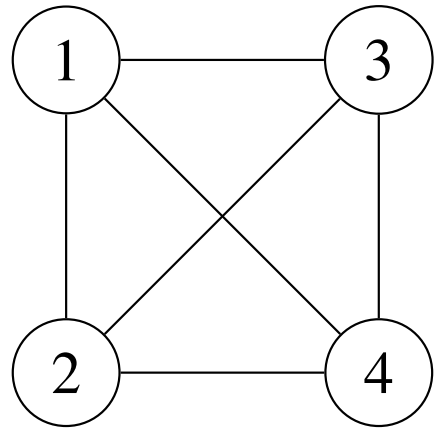
$$f_1(x_1,x_2) = x_1, \quad f_2(x_1,x_2) = x_2$$

- This is possible iff $|A| \geq 3$, e.g.

$$f_3(x_1,x_2) = x_1 + \delta_{x_1,x_2}, \qquad f_4(x_1,x_2) = x_2 + \delta_{x_1,x_2}$$

Example: orthogonal Latin squares

- A representation of K_n over A is a family of $n-2$ mutually orthogonal Latin squares of order $|A|$

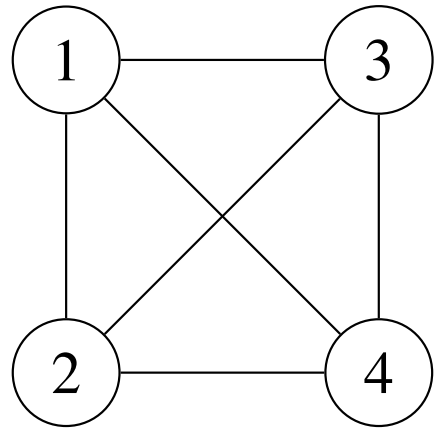


$$f_1 : \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix} \quad f_2 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad f_3 : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix} \quad f_4 : \begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}$$

- Proof: $f_1(x_1,x_2) = x_1$: row, $f_2(x_1,x_2) = x_2$ column
  (f_1,f_3) and (f_2,f_3) bijections iff f_3 defines a Latin square
  (f_3,f_4) bijection iff orthogonal

Example: orthogonal Latin squares

- A representation of K_n over A is a family of $n-2$ mutually orthogonal Latin squares of order $|A|$



$$f_1 : \begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix} \quad f_2 : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad (f_3, f_4) : \begin{pmatrix} 12 & 23 & 31 \\ 33 & 11 & 22 \\ 21 & 32 & 13 \end{pmatrix}$$

- Proof: $f_1(x_1, x_2) = x_1$: row, $f_2(x_1, x_2) = x_2$ column
  (f_1, f_3) and (f_2, f_3) bijections iff f_3 defines a Latin square
  (f_3, f_4) bijection iff orthogonal

Existence of MOLS

- Existence of two MOLS: conjectured wrongly by Euler, solved by Parker, Bose and Shrikhande in 1960
- Existence of $n-1$ MOLS of order n iff n is a prime power
- For any k, the set of alphabet sizes for which k MOLS exist contains all sufficiently large integers
- Representation of $\binom{E}{r}$: $(n, n-r, r+1)$ MDS code. Existence still an open problem

Matroids

- Combinatorial properties of vector spaces
- Let $E = \{1, \ldots, n\}$ and $\mathcal{B} \subseteq \binom{E}{r}$ a family of r-subsets of E
- Definition: $(E, \mathcal{B})$ is a matroid if it satisfies the exchange axiom: for all $b_1, b_2 \in \mathcal{B}$ and all $i_1 \in b_1 \backslash b_2$, there exists $i_2 \in b_2 \backslash b_1$ s.t.

$$b_1 \backslash \{i_1\} \cup \{i_2\} \in \mathcal{B}$$

- Trivial ex: $(E, \binom{E}{r})$ has all r-subsets
- Other ex:
  - E vector space, $\mathcal{B}$ its bases
  - E edges of a connected graph, $\mathcal{B}$ spanning trees

Linear matroids

- $(E, \mathcal{B})$ is a linear matroid if there exist n vectors $v_i \in F^r$ s.t.

$$b \in \mathcal{B} \Leftrightarrow \{v_i : i \in b\} \text{ basis of } F^r$$

- Then, we can associate a function to each element:

$$f_i(x) = v_i \cdot x \qquad \forall\, x = (x_1, \ldots, x_r) \in F^r$$

- For all $b = \{i_1, \ldots, i_r\}$ the function

$$\begin{aligned} f_b &: F^r \to F^r \\ f_b(x) &= (f_{i_1}(x), \ldots, f_{i_r}(x)) = x(v_{i_1}^T, \ldots, v_{i_r}^T) \end{aligned}$$

  is a bijection iff $b \in \mathcal{B}$

Any family is representable

- Matrix function: A is a vector space, $x_1, \ldots, x_r$ are vectors and $f_i(x) = \sum_j x_j F_{i,j}$
- Theorem: $(E, \mathcal{B})$ is representable by matrix functions over some A
- Proof: (if $\mathcal{B} = \binom{E}{r}$, it is a linear matroid)
  - Express

$$\mathcal{B} = \bigcap_{c \in \binom{E}{r} \setminus \mathcal{B}} \binom{E}{r} \setminus \{c\}$$

  - Each $\binom{E}{r} \setminus \{c\}$ is a linear matroid
  - If (f_i) represents $(E, \mathcal{B})$ over A and (g_i) represents $(E, \mathcal{B}')$ over A', then (h_i) represents $(E, \mathcal{B} \cap \mathcal{B}')$ over $A \times A'$:

$$h_i((a_1, a'_1), \ldots, (a_r, a'_r)) = (f_i(a_1, \ldots, a_r), g_i(a'_1, \ldots, a'_r))$$

  - The cartesian product of linear functions is a matrix function

Outline

Idea

- We fix r and A
- An infinite number of $(E, \mathcal{B})$ of rank r is representable over A
- But they are all based on a finite number of simple families
- Instead of considering a function $f : A^r \to A^k$, we look at the partition of A^r it induces:

$$\bar{f} = \{f^{-1}(a) : a \in A^k\}$$

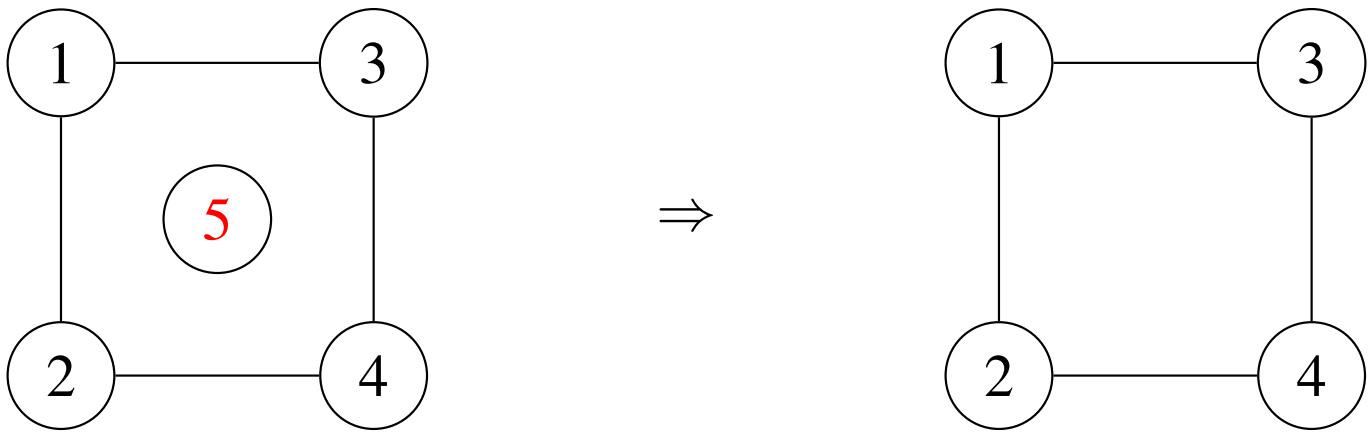
$$f_b : A^r \to A^r \text{ bijection } \Leftrightarrow f_b(A^r) = A^r \Leftrightarrow \bar{f}_b \text{ has } |A|^r \text{ parts}$$

Loops

- $l \in E$ is a loop if no basis contains l.
- A function $f : A^r \to A$ is balanced if

$$\bar{f} \text{ has } |A| \text{ equal parts}$$

  i.e. $|f^{-1}(a)| = |A|^{r-1}$ for all $a \in A$
- If $l \in E$ is not a loop, then f_l is balanced. Otherwise, let f_l be imbalanced.

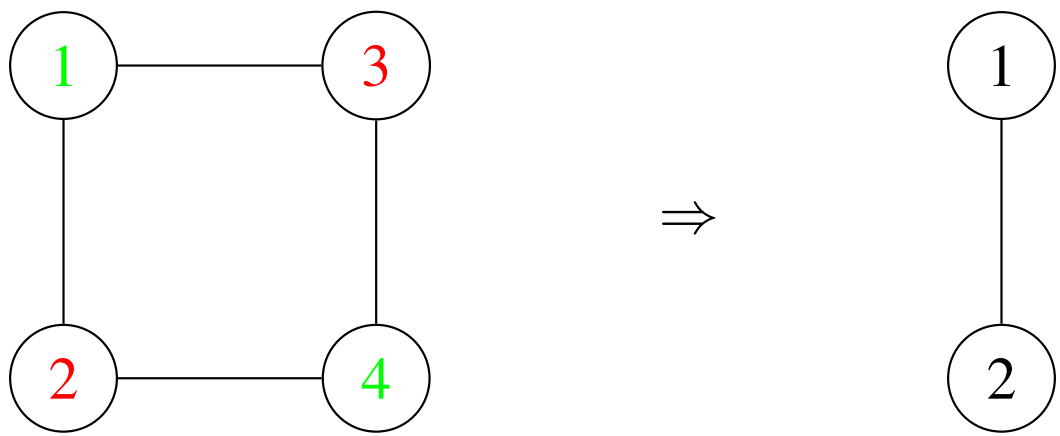


Parallel elements

- $i, j \in E$ are parallel if each can be replaced by the other in a basis and no basis contains both.
- Two functions $f, g : A^r \to A$ are parallel if they induce the same partition:

$$\bar{f} = \bar{g}$$

  i.e. $f = \pi \circ g$ for some $\pi \in S_A$.
- If i and j are not parallel, then neither are f_i and f_j. Otherwise, let f_i and f_j be parallel.



Characterisation

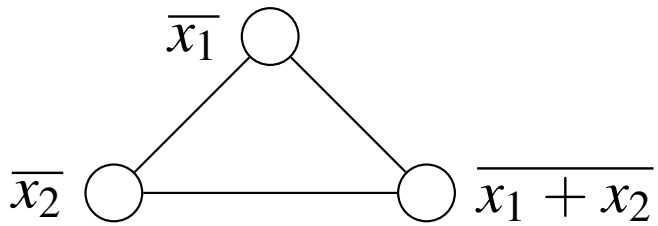
- $P(A,r) = \{\bar{f}_1, \ldots, \bar{f}_k\}$: set of partitions of A^r into $|A|$ equal parts.
- Let $\mathcal{M}(A,r) = (P(A,r), \mathcal{B})$, where

$$\begin{aligned} \mathcal{B} &= \{\{\bar{f}_{i_1}, \ldots, \bar{f}_{i_r}\} : \bar{f}_{\{i_1,\ldots,i_r\}} \text{has } |A|^r \text{ parts}\} \\ &= \{\{\bar{f}_{i_1}, \ldots, \bar{f}_{i_r}\} : f_{\{i_1,\ldots,i_r\}} \text{bijection}\} \end{aligned}$$

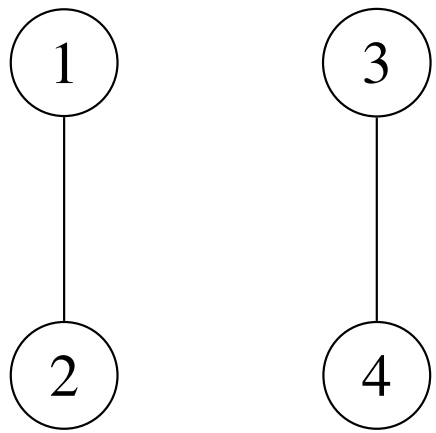
- Theorem: $(E, \mathcal{B})$ of rank r is representable over A iff after simplification it is isomorphic to an induced subgraph of $\mathcal{M}(A,r)$
- $\mathcal{M}(A,r)$ is large, but very regular. Each regularity constant gives a criterion for representability over alphabets up to $|A|$

Examples

- Ex: $\mathcal{M}(2,2) = K_3$

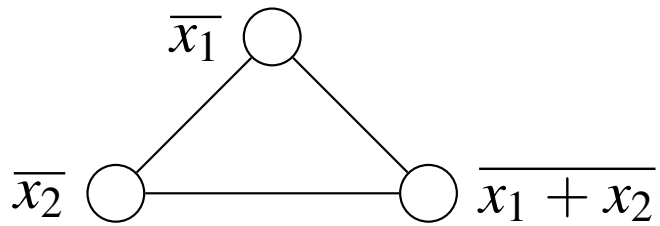


- First ex: Not representable if $|A| = 2$

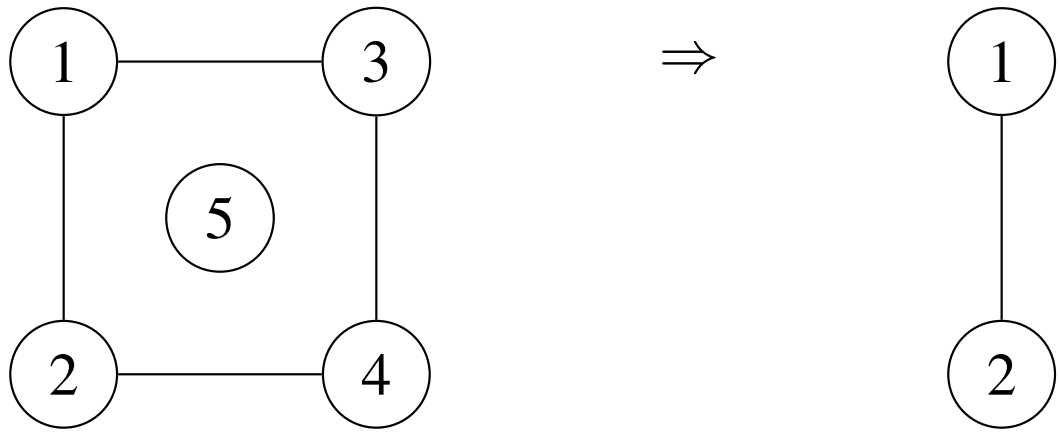


Examples

- Ex: $\mathcal{M}(2,2) = K_3$



- Second ex: Representable over any alphabet



Outline

Combinatorial Representations

Characterisation

Rank Functions

Information received by Eve

- We required "not a bijection" for non-bases. Very loose requirement
- How much info the functions give away about the input $x = (x_1, \ldots, x_r)$: for any $S \subseteq E$, we have

$$\begin{aligned} H(x) - H(x \,|\, f_S) &= I(f_S; x) \\ &= H(f_S) - H(f_S \,|\, x) \\ &= H(f_S) \end{aligned}$$

- $H(f_S)$: entropy of f_S

$$H(f_S) \leq \log_{|A|} |f_S(A^r)| \leq |S|$$

Definition

- A rank function for $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ s.t.
  - if $S \subseteq E$, then
    $$0 \leq \mathrm{rk}(S) \leq |S|,$$
  - rk is increasing, i.e. if $S \subseteq T \subseteq E$, then
    $$\mathrm{rk}(S) \leq \mathrm{rk}(T),$$
  - rk is submodular, i.e. if $S, T \subseteq E$, then
    $$\mathrm{rk}(S) + \mathrm{rk}(T) \geq \mathrm{rk}(S \cup T) + \mathrm{rk}(S \cap T),$$
  - if $|S| = r$, then $\mathrm{rk}(S) = r$ iff $S \in \mathcal{B}$
- $(E, \mathcal{B})$ matroid iff has a rank function with integer values

Representation and rank

- If (f_i) is a representation of $(E, \mathcal{B})$ over A, then the entropy for a randomly distributed input x

$$\begin{aligned} H(f_S) &= -\sum_{a \in f_S(A^r)} \frac{|f_S^{-1}(a)|}{|A|^r} \log_{|A|} \left\{ \frac{|f_S^{-1}(a)|}{|A|^r} \right\} \\ &= r - |A|^{-r} \sum_{a \in f_S(A^r)} |f_S^{-1}(a)| \log_{|A|} |f_S^{-1}(a)| \end{aligned}$$

  is a rank function for $(E, \mathcal{B})$
- Proof: Shannon's inequality

$$I(U; V|W) \geq 0$$

Bounds on rank

- Denote

$$m(S) = \max_{b \in \mathcal{B}} |b \cap S|,$$

  when $(E, \mathcal{B})$ is a matroid, it's its rank function
- The rank function of $(E, \binom{E}{r})$ is given by

$$M(S) = \min\{r, |S|\}$$

- For any family $(E, \mathcal{B})$ and any rank function rk,

$$m(S) \leq \mathrm{rk}(S) \leq M(S)$$

- The upper bound $M(S)$ can be approached by

$$\mathrm{rk}(S) = M(S) - \epsilon\{|S| = r, S \notin \mathcal{B}\}$$

  for any $0 < \epsilon \leq 1/2$

Lower bounds on rank

- We want to refine the lower bound $m(S) = \max_{b \in \mathcal{B}} |b \cap S|$
- Tight for matroids, which are generally dense due to the exchange axiom
  $\Rightarrow$ Idea: look at "holes" in the family
- Proposition: If there exists $b \in \mathcal{B}$ s.t. for any other $c \in \mathcal{B}$,

$$|b \cap c| \leq I,$$

then there exists $S \subseteq E$ s.t. $|S| = r$ and

$$\mathrm{rk}(S) - m(S) \geq \frac{r - I}{4}$$

for any rank function for $(E, \mathcal{B})$

Bounds on rank: extreme case

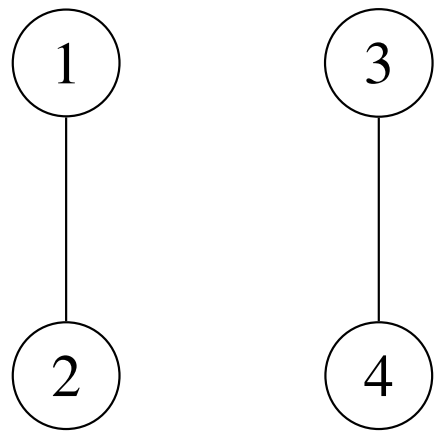
- Transversal: a set of elements which intersects all bases
- Theorem: Let t be the min. size of a transversal for $(E, \mathcal{B})$, then there exists $S \subseteq E$ s.t.

$$m(S) = 1, \qquad \mathrm{rk}(S) \geq r\left(1 - \left(1 - \frac{1}{r}\right)^t\right)$$

- Ex: if $\mathcal{B} = \{12, 34\}$, then $t = 2$ and

$$\mathrm{rk}(13) + \mathrm{rk}(14) \geq \mathrm{rk}(1) + \mathrm{rk}(134) = 3$$

So $\mathrm{rk}(13)$ or $\mathrm{rk}(14) \geq 1.5$



Closure

- Any rank function defines a closure operator $\mathrm{cl}(S)$ for any $S \subseteq E$

$$\mathrm{cl}(S) = \{i \in E : \mathrm{rk}(S \cup \{i\}) = \mathrm{rk}(S)\}$$

- Nicely behaved: closure operator,

$$\mathrm{rk}(\mathrm{cl}(S)) = \mathrm{cl}(S), \qquad \mathrm{cl}(S) = E \Leftrightarrow \mathrm{rk}(S) = r$$

- In particular, for the representation (f_i)

$$\begin{aligned} \mathrm{cl}_{(f_i)}(S) &= \{i \in E : H(f_{S\cup\{i\}}) = H(f_S)\} \\ &= \{i \in E : \bar{f}_{S\cup\{i\}} = \bar{f}_S\} \\ &= \{i \in E : \bar{f}_S \text{ refines } \bar{f}_i\} \end{aligned}$$

- Axiomatic definition of a closure generated by a rank function?

Conclusion

- Relations with matroid theory, information theory and combinatorics
- Extensions

- Foundations: more concepts from matroids, representations by matrices with a given number of rows, infinite alphabets
- Theorems: All graphs are representable over all but finitely many alphabets, structure theorems
- Applications: computations, network coding, optimisation

- PJC, MG and SR, "Combinatorial Representations" available on arXiv