Combinatorial representations

Peter J. Cameron
CAUL, Lisbon, April 2012

Joint work with Max Gadouleau and Søren Riis
see arXiv 1109.1216

Matroids

A matroid is a structure for describing the linear independence and dependence of sets of vectors in a vector space.

Matroids

A matroid is a structure for describing the linear independence and dependence of sets of vectors in a vector space.
Think of the elements of a matroid as being a family $(v_i : i \in E)$ of vectors in a vector space V. (It is a family rather than a set since we don't mind if vectors are repeated.)

Matroids

A matroid is a structure for describing the linear independence and dependence of sets of vectors in a vector space.
Think of the elements of a matroid as being a family $(v_i : i \in E)$ of vectors in a vector space V. (It is a family rather than a set since we don't mind if vectors are repeated.)
A matroid can be described in many different ways: by the independent sets, the bases, the minimal dependent sets, the rank function ...

Examples

Vectors in a vector space form the standard examples of matroids. But the concept is important because there are many other examples:

Examples

Vectors in a vector space form the standard examples of matroids. But the concept is important because there are many other examples:

- Algebraic matroids: E is a family of elements in a field with a prescribed algebraically closed subfield F, and independence means algebraic independence over F (so that rank is transcendence degree).

Examples

Vectors in a vector space form the standard examples of matroids. But the concept is important because there are many other examples:

- Algebraic matroids: E is a family of elements in a field with a prescribed algebraically closed subfield F, and independence means algebraic independence over F (so that rank is transcendence degree).
- Graphic matroids: E is the edge set of a graph, and a set of edges is independent if it contains no circuit (so that the rank of a set A of edges is $n - c(A)$, where n is the number of vertices and $c(A)$ the number of connected components in the graph with edge set A.

Examples

Vectors in a vector space form the standard examples of matroids. But the concept is important because there are many other examples:

- Algebraic matroids: E is a family of elements in a field with a prescribed algebraically closed subfield F, and independence means algebraic independence over F (so that rank is transcendence degree).
- Graphic matroids: E is the edge set of a graph, and a set of edges is independent if it contains no circuit (so that the rank of a set A of edges is $n - c(A)$, where n is the number of vertices and $c(A)$ the number of connected components in the graph with edge set A.
- Transversal matroids: E is the index set of a family of subsets of a set S, and a subset of E is independent if the corresponding subfamily possesses a transversal.

Matroid bases

A matroid is completely specified by its bases, that is, its maximal independent sets.

Matroid bases

A matroid is completely specified by its bases, that is, its maximal independent sets.
Matroids can be axiomatised in this way. The crucial axiom is the exchange axiom:

Matroid bases

A matroid is completely specified by its bases, that is, its maximal independent sets.
Matroids can be axiomatised in this way. The crucial axiom is the exchange axiom:

> *If B and C are bases and $e \in B \setminus C$, then there exists $f \in C \setminus B$ such that $B \setminus \{e\} \cup \{f\}$ is a basis.*

Matroid bases

A matroid is completely specified by its bases, that is, its maximal independent sets.
Matroids can be axiomatised in this way. The crucial axiom is the exchange axiom:

> *If B and C are bases and $e \in B \setminus C$, then there exists $f \in C \setminus B$ such that $B \setminus \{e\} \cup \{f\}$ is a basis.*

It follows that any two bases have the same size, the rank of the matroid.

Matroid bases

A matroid is completely specified by its bases, that is, its maximal independent sets.
Matroids can be axiomatised in this way. The crucial axiom is the exchange axiom:

> *If B and C are bases and $e \in B \setminus C$, then there exists $f \in C \setminus B$ such that $B \setminus \{e\} \cup \{f\}$ is a basis.*

It follows that any two bases have the same size, the rank of the matroid.
I will use bases to describe matroids and similar structures in this talk.

Matroid representations

Now a matroid representation is simply described:

Matroid representations

Now a matroid representation is simply described:
Let E be the ground set and $\mathcal{B}$ the family of bases of a matroid M of rank r. A vector representation of M is an assignment of a vector $v_i \in F^r$ to each $i \in E$, such that, for $i_1, \ldots, i_r \in E$,

$$(v_{i_1}, \ldots, v_{i_r}) \text{ is a basis for } F^r \Leftrightarrow \{i_1, \ldots, i_r\} \in \mathcal{B}.$$

. . . in dual form

Now regard the representing vectors $v_1, \ldots, v_r$ as lying in the dual space of F^r. To emphasise this I will write f_i instead of v_i; thus f_i is a function from F^r to F.

. . . in dual form

Now regard the representing vectors $v_1, \ldots, v_r$ as lying in the dual space of F^r. To emphasise this I will write f_i instead of v_i; thus f_i is a function from F^r to F.
Notation: if $f_{i_1}, \ldots, f_{i_r} : F^r \to F$, then we regard the r-tuple $(f_{i_1}, \ldots, f_{i_r})$ as being a function from F^r to F^r.

. . . in dual form

Now regard the representing vectors $v_1, \ldots, v_r$ as lying in the dual space of F^r. To emphasise this I will write f_i instead of v_i; thus f_i is a function from F^r to F.
Notation: if $f_{i_1}, \ldots, f_{i_r} : F^r \to F$, then we regard the r-tuple $(f_{i_1}, \ldots, f_{i_r})$ as being a function from F^r to F^r.
Now a vector representation of the matroid M is an assignment of a linear map $f_i : F^r \to F$ to each $i \in E$, so that

$$(f_{i_1}, \ldots, f_{i_r}) : F^r \to F^r \text{ is a bijection } \Leftrightarrow \{i_1, \ldots, i_r\} \in \mathcal{B}.$$

. . . generalised

Let $\mathcal{B}$ be any family of r-subsets of a ground set E, and let A be an alphabet of size q. A combinatorial representation of $(E, \mathcal{B})$ over A is an assignment of a function $f_i : A^r \to A$ to each point $i \in E$ so that

$$(f_{i_1}, \ldots, f_{i_r}) : A^r \to A^r \text{ is a bijection } \Leftrightarrow \{i_1, \ldots, i_r\} \in \mathcal{B}.$$

. . . generalised

Let $\mathcal{B}$ be any family of r-subsets of a ground set E, and let A be an alphabet of size q. A combinatorial representation of $(E, \mathcal{B})$ over A is an assignment of a function $f_i : A^r \to A$ to each point $i \in E$ so that

$$(f_{i_1}, \ldots, f_{i_r}) : A^r \to A^r \text{ is a bijection } \Leftrightarrow \{i_1, \ldots, i_r\} \in \mathcal{B}.$$

Thus any vector representation of a matroid, dualised, is a combinatorial representation.

. . . generalised

Let $\mathcal{B}$ be any family of r-subsets of a ground set E, and let A be an alphabet of size q. A combinatorial representation of $(E, \mathcal{B})$ over A is an assignment of a function $f_i : A^r \to A$ to each point $i \in E$ so that

$$(f_{i_1}, \ldots, f_{i_r}) : A^r \to A^r \text{ is a bijection } \Leftrightarrow \{i_1, \ldots, i_r\} \in \mathcal{B}.$$

Thus any vector representation of a matroid, dualised, is a combinatorial representation.
If $X = \{i_1, \ldots, i_r\}$, we denote $(f_{i_1}, \ldots, f_{i_r})$ by f_X.

An example

Let $n = 4$ and $\mathcal{B} = \{\{1,2\},\{3,4\}\}$. A combinatorial representation over a 3-element set $\{a,b,c\}$ is given by taking f_1 and f_2 to be the two coordinate functions (that is, $f_1(x,y) = x$ and $f_2(x,y) = y$), and f_3 and f_4 by the tables

b	a	a
b	c	b
c	c	a

and

b	b	c
a	c	c
a	b	a

.

Note that $(E,\mathcal{B})$ is not a matroid.

A normalisation

Suppose that $b = \{i_1, \ldots, i_r\} \in \mathcal{B}$. Define functions g_i, for $i \in E$, by

$$g_i(x_1, \ldots, x_r) = f_i(y_1, \ldots, y_r),$$

where $(y_1, \ldots, y_r)$ is the inverse image of $(x_1, \ldots, x_r)$ under the bijection f_b. These functions also define a combinatorial representation, with the property that g_{i_j} is the jth coordinate function. So, where necessary, we may suppose that the first r elements of E form a basis and the first r functions are the coordinate functions. This transformation can be viewed as a change of variables.

Linear representations

Before going to the general case, we observe the following:

Linear representations

Before going to the general case, we observe the following:

Theorem

A set family has a combinatorial representation by linear functions over a field F if and only if it consists of the bases of a matroid (representable over F).

Linear representations

Before going to the general case, we observe the following:

Theorem

A set family has a combinatorial representation by linear functions over a field F if and only if it consists of the bases of a matroid (representable over F).

Proof.

We verify the exchange axiom. Let $B_1, B_2 \in \mathcal{B}$; we may assume that the elements of B_1 are the coordinate functions. Now consider the $r-1$ functions f_i for $i \in B_2$, $i \neq k$, for some fixed $k \in B_2$. These define a surjective function from F^r to F^{r-1}. Take any non-zero vector in the kernel, and suppose that its lth coordinate is non-zero. Then it is readily checked that the functions with indices in $B_2 \setminus \{k\} \cup \{l\}$ give a bijection from F^r to F^r; so this set is a basis. □

Which families are representable?

After the last result, the answer is a bit surprising:

Which families are representable?

After the last result, the answer is a bit surprising:

Theorem

Every uniform set family has a combinatorial representation over some alphabet.

Which families are representable?

After the last result, the answer is a bit surprising:

Theorem
Every uniform set family has a combinatorial representation over some alphabet.

This depends on the following result:

Which families are representable?

After the last result, the answer is a bit surprising:

Theorem
Every uniform set family has a combinatorial representation over some alphabet.

This depends on the following result:

Theorem
Let $(E, \mathcal{B}_1)$ and $(E, \mathcal{B}_2)$ be families of r-sets, which have representations over alphabets of cardinalities q_1 and q_2 respectively. Then $(E, \mathcal{B}_1 \cap \mathcal{B}_2)$ has a representation over an alphabet of size $q_1 q_2$.

Now, to prove the theorem, we observe that

$$\mathcal{B} = \bigcap_{C \notin \mathcal{B}} \left(\binom{E}{r} \setminus \{C\} \right)$$

so it is enough to represent the family consisting of all but one of the r-sets; and it is not too hard to show that this family is indeed a representable matroid.

Now, to prove the theorem, we observe that

$$\mathcal{B} = \bigcap_{C \notin \mathcal{B}} \left(\binom{E}{r} \setminus \{C\} \right)$$

so it is enough to represent the family consisting of all but one of the r-sets; and it is not too hard to show that this family is indeed a representable matroid.
Note that our proof shows that in fact every set family has a representation by "matrix functions". More on this later.

Now, to prove the theorem, we observe that

$$\mathcal{B} = \bigcap_{C \notin \mathcal{B}} \left(\binom{E}{r} \setminus \{C\} \right)$$

so it is enough to represent the family consisting of all but one of the r-sets; and it is not too hard to show that this family is indeed a representable matroid.
Note that our proof shows that in fact every set family has a representation by "matrix functions". More on this later.

Question

Given a set family, what are the cardinalities of alphabets over which it has a combinatorial representation?

Graphs

In the case $r = 2$, our family is just the edge set of a graph.

Graphs

In the case $r = 2$, our family is just the edge set of a graph.

Theorem

A graph is representable over all sufficiently large alphabets.

Graphs

In the case $r = 2$, our family is just the edge set of a graph.

Theorem

A graph is representable over all sufficiently large alphabets.

As a warm-up, let us consider the complete graph. It is readily checked from the definitions that a representation of K_n over an alphabet of size q is the same thing as a set of $n - 2$ mutually orthogonal Latin squares of order q; these are known to exist for all sufficiently large q.

Pairwise balanced designs

A pairwise balanced design, or PBD, consists of a set X and a collection $\mathcal{L}$ of subsets of X (each of size greater than 1) such that every two points of X are contained in a unique "line" in $\mathcal{L}$. If the line sizes all belong to the set K of positive integers, we call it a PBD(K).

Pairwise balanced designs

A pairwise balanced design, or PBD, consists of a set X and a collection $\mathcal{L}$ of subsets of X (each of size greater than 1) such that every two points of X are contained in a unique "line" in $\mathcal{L}$. If the line sizes all belong to the set K of positive integers, we call it a PBD(K).

A set K of positive integers is PBD-closed if, whenever there exists a PBD(K) on a set of size v, then $v \in K$.

Pairwise balanced designs

A pairwise balanced design, or PBD, consists of a set X and a collection $\mathcal{L}$ of subsets of X (each of size greater than 1) such that every two points of X are contained in a unique "line" in $\mathcal{L}$. If the line sizes all belong to the set K of positive integers, we call it a PBD(K).

A set K of positive integers is PBD-closed if, whenever there exists a PBD(K) on a set of size v, then $v \in K$.

Given K, we define

$$\begin{aligned} \alpha(K) &= \gcd\{k-1 : k \in K\}, \\ \beta(K) &= \gcd\{k(k-1) : k \in K\}. \end{aligned}$$

Wilson's Theorem

Wilson's Theorem is well known to design theorists, maybe less so to other mathematicians.

Wilson's Theorem

Wilson's Theorem is well known to design theorists, maybe less so to other mathematicians.

Theorem

If K is PBD-closed, then K contains all but finitely many integers v sucn that $\alpha(K) \mid v-1$ and $\beta(K) \mid v(v-1)$.

Wilson's Theorem

Wilson's Theorem is well known to design theorists, maybe less so to other mathematicians.

Theorem

If K is PBD-closed, then K contains all but finitely many integers v sucn that $\alpha(K) \mid v-1$ and $\beta(K) \mid v(v-1)$.

This is the essential tool in the proof of our theorem.

Sketch proof

A combinatorial representation of a graph is idempotent if $f(x, x) = x$ for all functions f in the representation and all alphabet symbols x.

Sketch proof

A combinatorial representation of a graph is idempotent if $f(x,x) = x$ for all functions f in the representation and all alphabet symbols x.
We claim that the set K of alphabet sizes for which the given graph Γ has an idempotent representation is PBD-closed.

Sketch proof

A combinatorial representation of a graph is idempotent if $f(x,x) = x$ for all functions f in the representation and all alphabet symbols x.
We claim that the set K of alphabet sizes for which the given graph Γ has an idempotent representation is PBD-closed.
Let $(X, \mathcal{L})$ be a PBD, and suppose that Γ has a representation (f^L) with alphabet L, for every line $L \in \mathcal{L}$. Define a representation (f) of Γ over X by the rule that $f_i(x,x) = x$, while if $x \neq y$ then

$$f_i(x,y) = f_i^L(x,y),$$

where L is the unique line containing x and y. It is readily checked that this is a combinatorial representation.

Now it is straightforward to see that the set K of alphabet sizes over which Γ has a combinatorial representation satisfies $\alpha(K) = 1$ and $\beta(K) = 2$. (Using the proof of the first theorem, we see that K contains a sufficiently high power of any prime.)

Now it is straightforward to see that the set K of alphabet sizes over which Γ has a combinatorial representation satisfies $\alpha(K) = 1$ and $\beta(K) = 2$. (Using the proof of the first theorem, we see that K contains a sufficiently high power of any prime.) By Wilson's Theorem, K contains all sufficiently large integers, and we are done.

Now it is straightforward to see that the set K of alphabet sizes over which Γ has a combinatorial representation satisfies $\alpha(K) = 1$ and $\beta(K) = 2$. (Using the proof of the first theorem, we see that K contains a sufficiently high power of any prime.) By Wilson's Theorem, K contains all sufficiently large integers, and we are done.

Question

Does an analogous result hold for families of r-sets with $r > 2$?

Matrix representations

We saw that, if two families of sets have representations, then their intersection has a representation given by a "direct product" construction over the Cartesian product of the alphabets.

Matrix representations

We saw that, if two families of sets have representations, then their intersection has a representation given by a "direct product" construction over the Cartesian product of the alphabets.
In particular, if two families have linear representations over F, then their intersection has a "representation by two-rowed matrices", each point associated with a function from $(F^r)^2$ to F^2.

A question

Question

Which set families have representations by two-rowed matrices?

A question

Question

Which set families have representations by two-rowed matrices?

This condition is strictly stronger than that of being the intersection of two representable matroids. An example is given by

$$E = \{1, \ldots, 6\}, \mathcal{B} = \{\{1,2\}, \{3,4\}, \{5,6\}\}.$$

A question

Question

Which set families have representations by two-rowed matrices?

This condition is strictly stronger than that of being the intersection of two representable matroids. An example is given by

$$E = \{1, \ldots, 6\}, \mathcal{B} = \{\{1,2\}, \{3,4\}, \{5,6\}\}.$$

There are families which do not have representations by two-rowed matrices. An example is given by

$$E = \{1, \ldots, 7\}, \mathcal{B} = \{\{1,2\}, \{3,4\}, \{5,6\}, \{5,7\}, \{6,7\}\}.$$

The proof of non-representability uses the Ingleton inequality.

Rank functions

A rank function for a set family $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ satisfying

- $0 \leq \mathrm{rk}(X) \leq |X|$ for all $X \subseteq E$.

Rank functions

A rank function for a set family $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ satisfying

- $0 \leq \mathrm{rk}(X) \leq |X|$ for all $X \subseteq E$.
- $X \subseteq Y$ implies $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$.

Rank functions

A rank function for a set family $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ satisfying

- $0 \leq \mathrm{rk}(X) \leq |X|$ for all $X \subseteq E$.
- $X \subseteq Y$ implies $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$.
- rk is submodular, that is, for any subsets X, Y of E,

$$\mathrm{rk}(X \cap Y) + \mathrm{rk}(X \cup Y) \leq \mathrm{rk}(X) + \mathrm{rk}(Y).$$

Rank functions

A rank function for a set family $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ satisfying

- $0 \leq \mathrm{rk}(X) \leq |X|$ for all $X \subseteq E$.
- $X \subseteq Y$ implies $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$.
- rk is submodular, that is, for any subsets X, Y of E,

$$\mathrm{rk}(X \cap Y) + \mathrm{rk}(X \cup Y) \leq \mathrm{rk}(X) + \mathrm{rk}(Y).$$

- If $|X| = r$, then $\mathrm{rk}(X) = r$ if and only if $X \in \mathcal{B}$.

Rank functions

A rank function for a set family $(E, \mathcal{B})$ is a function $\mathrm{rk} : 2^E \to [0, r]$ satisfying

- $0 \leq \mathrm{rk}(X) \leq |X|$ for all $X \subseteq E$.
- $X \subseteq Y$ implies $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$.
- rk is submodular, that is, for any subsets X, Y of E,

$$\mathrm{rk}(X \cap Y) + \mathrm{rk}(X \cup Y) \leq \mathrm{rk}(X) + \mathrm{rk}(Y).$$

- If $|X| = r$, then $\mathrm{rk}(X) = r$ if and only if $X \in \mathcal{B}$.

The first three conditions are equivalent to the definition of a polymatroid.

Rank functions from representations

Theorem

Let $f = (f_i)$ be a representation of $(E, \mathcal{B})$ over an alphabet X of size q. Then the function r_f, defined by $r_f(S) = H(f_S)$, is a rank function for $(E, \mathcal{B})$.

Rank functions from representations

Theorem

Let $f = (f_i)$ be a representation of $(E, \mathcal{B})$ over an alphabet X of size q. Then the function r_f, defined by $r_f(S) = H(f_S)$, is a rank function for $(E, \mathcal{B})$.

Here H is the q-ary entropy function given by

$$H(f_S) = -\sum \frac{|f_S^{-1}(a)|}{q^r} \log_q \left(\frac{|f_S^{-1}(a)|}{q^r} \right).$$

Rank functions from representations

Theorem

Let $f = (f_i)$ be a representation of $(E, \mathcal{B})$ over an alphabet X of size q. Then the function r_f, defined by $r_f(S) = H(f_S)$, is a rank function for $(E, \mathcal{B})$.

Here H is the q-ary entropy function given by

$$H(f_S) = -\sum \frac{|f_S^{-1}(a)|}{q^r} \log_q \left(\frac{|f_S^{-1}(a)|}{q^r} \right).$$

The converse is false; there are rank functions which do not arise from any combinatorial representation.

Bounds for rank functions

If we set $r_m(X) = \max_{B \in \mathcal{B}} |B \cap X|$ and $r_M(X) = \min\{r, |X|\}$, (so that r_M is the rank function for the uniform matroid of rank r), then it is easy to see that $r_m(X) \leq \mathrm{rk}(X) \leq r_M(X)$.

Bounds for rank functions

If we set $r_m(X) = \max_{B \in \mathcal{B}} |B \cap X|$ and $r_M(X) = \min\{r, |X|\}$, (so that r_M is the rank function for the uniform matroid of rank r), then it is easy to see that $r_m(X) \leq \mathrm{rk}(X) \leq r_M(X)$.
Hence $(E, \mathcal{B})$ is a matroid if and only if it has an integer-valued rank function.

Bounds for rank functions

If we set $r_m(X) = \max_{B \in \mathcal{B}} |B \cap X|$ and $r_M(X) = \min\{r, |X|\}$, (so that r_M is the rank function for the uniform matroid of rank r), then it is easy to see that $r_m(X) \leq \mathrm{rk}(X) \leq r_M(X)$.
Hence $(E, \mathcal{B})$ is a matroid if and only if it has an integer-valued rank function.
On the other hand, we have:

Theorem

Any family $(E, \mathcal{B})$ has a rank function which takes integer or half-integer values (or indeed, values in the rationals with denominator dividing p, for any $p > 1$).

Bounds for rank functions

If we set $r_m(X) = \max_{B \in \mathcal{B}} |B \cap X|$ and $r_M(X) = \min\{r, |X|\}$, (so that r_M is the rank function for the uniform matroid of rank r), then it is easy to see that $r_m(X) \leq \mathrm{rk}(X) \leq r_M(X)$.
Hence $(E, \mathcal{B})$ is a matroid if and only if it has an integer-valued rank function.
On the other hand, we have:

Theorem

Any family $(E, \mathcal{B})$ has a rank function which takes integer or half-integer values (or indeed, values in the rationals with denominator dividing p, for any $p > 1$).

An example of such a function is given by

$$\mathrm{rk}(X) = \begin{cases} |X| & \text{if } |X| \leq r-1 \text{ or } X \in \mathcal{B}, \\ r - 1/p & \text{if } |X| = r,\ X \notin \mathcal{B}, \\ r & \text{if } |X| \geq r+1. \end{cases}$$

Bounds for rank functions

If we set $r_m(X) = \max_{B \in \mathcal{B}} |B \cap X|$ and $r_M(X) = \min\{r, |X|\}$, (so that r_M is the rank function for the uniform matroid of rank r), then it is easy to see that $r_m(X) \leq \mathrm{rk}(X) \leq r_M(X)$.
Hence $(E, \mathcal{B})$ is a matroid if and only if it has an integer-valued rank function.
On the other hand, we have:

Theorem

Any family $(E, \mathcal{B})$ has a rank function which takes integer or half-integer values (or indeed, values in the rationals with denominator dividing p, for any $p > 1$).

An example of such a function is given by

$$\mathrm{rk}(X) = \begin{cases} |X| & \text{if } |X| \leq r-1 \text{ or } X \in \mathcal{B}, \\ r - 1/p & \text{if } |X| = r,\ X \notin \mathcal{B}, \\ r & \text{if } |X| \geq r+1. \end{cases}$$

We see that the function r_M is the supremum of all rank functions for $(E, \mathcal{B})$, and can be approached arbitrarily closely.

In the other direction, we have:

Theorem

Let $(E, \mathcal{B})$ be a set family of rank r. Then there is a set X with $|X| = r$ and $r_m(X) = (r + I)/2$, where

$$I = \min_{B \in \mathcal{B}} \max_{C \in \mathcal{B}, C \neq B} |B \cap C|.$$

Moreover, for any rank function rk*, we have*

$$\mathrm{rk}(X) - r_m(X) \geq (r - I)/4.$$

In the other direction, we have:

Theorem

Let $(E, \mathcal{B})$ be a set family of rank r. Then there is a set X with $|X| = r$ and $r_m(X) = (r + I)/2$, where

$$I = \min_{B \in \mathcal{B}} \max_{C \in \mathcal{B}, C \neq B} |B \cap C|.$$

Moreover, for any rank function rk*, we have*

$$\mathrm{rk}(X) - r_m(X) \geq (r - I)/4.$$

So a basis disjoint from all other bases leads to large differences between any rank function and the lower bound r_m.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ for all $X \subseteq E$.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ for all $X \subseteq E$.
- $\mathrm{rk}(\mathrm{cl}(X)) = \mathrm{rk}(X)$ for all $X \subseteq E$.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ for all $X \subseteq E$.
- $\mathrm{rk}(\mathrm{cl}(X)) = \mathrm{rk}(X)$ for all $X \subseteq E$.
- $\mathrm{cl}(X) = E$ if and only if $\mathrm{rk}(X) = r$.

Closure

A rank function defines a closure operator cl, by

$$\mathrm{cl}(X) = \{e \in E : \mathrm{rk}(X \cup \{e\}) = \mathrm{rk}(X)\}.$$

It has the properties

- $X \subseteq \mathrm{cl}(X)$ for all $X \subseteq E$.
- If $X \subseteq Y$, then $\mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
- $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$ for all $X \subseteq E$.
- $\mathrm{rk}(\mathrm{cl}(X)) = \mathrm{rk}(X)$ for all $X \subseteq E$.
- $\mathrm{cl}(X) = E$ if and only if $\mathrm{rk}(X) = r$.

Not every closure operator (satisfying the first three conditions) comes from a rank function.

Closure in a representation

If the rank function arises from a combinatorial representation $f = (f_e : e \in E)$, then we have

$$\mathrm{cl}(X) = \{e \in E : f_X \text{ refines } f_e\}.$$

(We say that f_1 refines f_2 if $f_1(x) = f_1(y)$ implies $f_2(x) = f_2(y)$.)

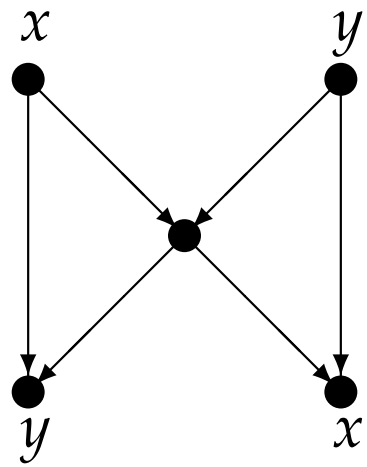
Network coding

This work was done as part of a project on Network Coding. I cannot explain here all the connections, but I will try to give a brief overview of the subject.

Network coding

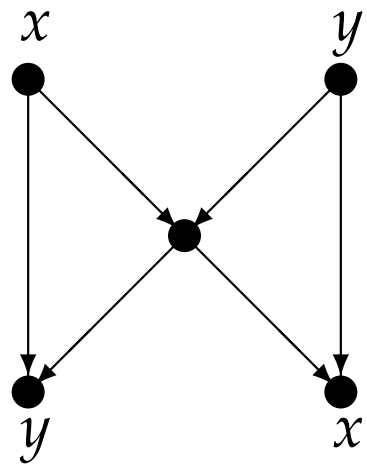
This work was done as part of a project on Network Coding. I cannot explain here all the connections, but I will try to give a brief overview of the subject.
I begin with the butterfly network, the paradigm of the subject.

The butterfly network



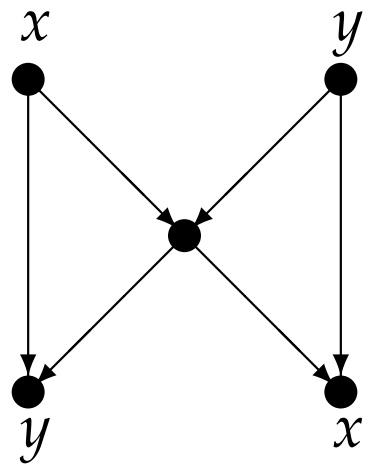
The nodes at the top have to send the corresponding messages to the nodes at the bottom.

The butterfly network



The nodes at the top have to send the corresponding messages to the nodes at the bottom.
In a network carrying ordinary commodities such as water, it would take two time steps because of the bottleneck in the middle.

The butterfly network



The nodes at the top have to send the corresponding messages to the nodes at the bottom.
In a network carrying ordinary commodities such as water, it would take two time steps because of the bottleneck in the middle.
But with information, the transfer can be done in one time step, if the nodes have the computational capability to do "exclusive or" (addition mod 2) on their inputs.

Guessing number

Given a digraph, in which each vertex holds a symbol from the alphabet A of size q. A vertex is not aware of its own symbol, but knows the symbols of all its out-neighbours.

Guessing number

Given a digraph, in which each vertex holds a symbol from the alphabet A of size q. A vertex is not aware of its own symbol, but knows the symbols of all its out-neighbours.
We want to maximise the probability that every node guesses its own symbol correctly.

Guessing number

Given a digraph, in which each vertex holds a symbol from the alphabet A of size q. A vertex is not aware of its own symbol, but knows the symbols of all its out-neighbours.
We want to maximise the probability that every node guesses its own symbol correctly.
Suppose for example that we have the complete directed graph on n nodes. Guessing at random gives a probability $1/q^n$ that everyone is correct. But if the alphabet is an abelian group, and if the nodes each make the assumption that the sum of all the symbols is zero, the probability of guessing correctly is $1/q$.

Guessing number

Given a digraph, in which each vertex holds a symbol from the alphabet A of size q. A vertex is not aware of its own symbol, but knows the symbols of all its out-neighbours.
We want to maximise the probability that every node guesses its own symbol correctly.
Suppose for example that we have the complete directed graph on n nodes. Guessing at random gives a probability $1/q^n$ that everyone is correct. But if the alphabet is an abelian group, and if the nodes each make the assumption that the sum of all the symbols is zero, the probability of guessing correctly is $1/q$.
We say that the guessing number of the complete directed graph is $n-1$ (the logarithm to base q of the improvement in odds that can be achieved by the best strategy).

A connection

Søren Riis showed that there is a relation between the capacity of an information network and the guessing number of a digraph.

A connection

Søren Riis showed that there is a relation between the capacity of an information network and the guessing number of a digraph.
Suppose that the network has n input nodes required to send characters from an alphabet of size q to n output nodes in specified order. Form a digraph by identifying each input node with the corresponding output node. The guessing number of the resulting digraph is equal to the capacity of the original network.

An example

If we do Riis's construction to the butterfly network, we obtain the complete directed graph on three nodes.

An example

If we do Riis's construction to the butterfly network, we obtain the complete directed graph on three nodes.
This digraph has guessing number 2.

An example

If we do Riis's construction to the butterfly network, we obtain the complete directed graph on three nodes.
This digraph has guessing number 2.
So two pairs of nodes of the original network can communicate simultaneously.