Arrangements, matroids and codes

fourth lecture

Ruud Pellikaan
joint work with
Relinde Jurrius

ACAGM summer school
Leuven Belgium, 22 July 2011

Technische Universiteit Eindhoven
University of Technology

Content fourth lecture

1. Graphs and codes
2. Matroids
3. Circuits and cycles
4. Tutte-Whitney polynomial
5. Exercises

Graphs and codes

Paths and cycles

Definition

Two vertices u to v are connected by a path from u to v if there is a t-tuple of mutually distinct vertices $(v_1, \ldots, v_t)$ with $u = v_1$ and $v = v_t$, and a $(t-1)$-tuple of mutually distinct edges $(e_1, \ldots, e_{t-1})$ such that e_i is incident with v_i and v_{i+1} for all $1 \leq i < t$

If moreover e_t is an edge that is incident with u and v and distinct from e_i for all $i < t$, then $(e_1, \ldots, e_{t-1}, e_t)$ is called a cycle

The length of the smallest cycle is called the girth of the graph and it is denoted by $\gamma(\Gamma)$

Paths and cycles

Definition

Two vertices u to v are connected by a path from u to v
if there is a t-tuple of mutually distinct vertices $(v_1, \ldots, v_t)$
with $u = v_1$ and $v = v_t$, and a $(t-1)$-tuple of mutually distinct edges
$(e_1, \ldots, e_{t-1})$ such that e_i is incident with v_i and v_{i+1}
for all $1 \leq i < t$

If moreover e_t is an edge that is incident with u and v and distinct from e_i
for all $i < t$, then $(e_1, \ldots, e_{t-1}, e_t)$ is called a cycle

The length of the smallest cycle is called the girth of the graph
and it is denoted by $\gamma(\Gamma)$

Paths and cycles

Definition

Two vertices u to v are connected by a path from u to v
if there is a t-tuple of mutually distinct vertices $(v_1, \ldots, v_t)$
with $u = v_1$ and $v = v_t$, and a $(t-1)$-tuple of mutually distinct edges
$(e_1, \ldots, e_{t-1})$ such that e_i is incident with v_i and v_{i+1}
for all $1 \leq i < t$

If moreover e_t is an edge that is incident with u and v and distinct from e_i
for all $i < t$, then $(e_1, \ldots, e_{t-1}, e_t)$ is called a cycle

The length of the smallest cycle is called the girth of the graph
and it is denoted by $\gamma(\Gamma)$

Connected component

Definition

The graph is called connected if
every two vertices are connected by a path

A maximal connected subgraph of Γ is called
a connected component of Γ

The vertex set V of Γ is a disjoint union of subsets V_i
and the set of edges E is a disjoint union of subsets E_i
such that $\Gamma_i = (V_i, E_i)$ is a connected component of Γ

The number of connected components of Γ is denoted by $c(\Gamma)$

Connected component

Definition

The graph is called connected if
every two vertices are connected by a path

A maximal connected subgraph of Γ is called
a connected component of Γ

The vertex set V of Γ is a disjoint union of subsets V_i
and the set of edges E is a disjoint union of subsets E_i
such that $\Gamma_i = (V_i, E_i)$ is a connected component of Γ

The number of connected components of Γ is denoted by $c(\Gamma)$

Isthmus or bridge

Definition

An edge of a graph is called an isthmus
if the number of components of the graph increases
by deleting the edge

It the graph is connected, then deleting an isthmus
gives a graph that is no longer connected
Therefore an isthmus is also called a bridge

An edge is an isthmus if and only if it is not an edge of a cycle.
Therefore an edge that is an isthmus is also called an acyclic edge

Incidence matrix

Definition

Let $\Gamma = (V, E)$ be a finite graph
Suppose that V consists of m elements enumerated by $v_1, \ldots, v_m$
Suppose that E consists of n elements enumerated by $e_1, \ldots, e_n$

The incidence matrix $I(\Gamma)$ is a $m \times n$ matrix with entries a_{ij} defined by

$$a_{ij} = \begin{cases} 1 & \text{if } e_j \text{ is incident with } v_i \text{ and } v_k \text{ for some } i < k, \\ -1 & \text{if } e_j \text{ is incident with } v_i \text{ and } v_k \text{ for some } i > k, \\ 0 & \text{otherwise.} \end{cases}$$

Graph and cycle code

Definition

Let Γ be a finite graph

The graph code of Γ over $\mathbb{F}_q$ is the $\mathbb{F}_q$-linear code that is generated by the rows of the incidence matrix $I(\Gamma)$

The cycle code C_Γ of Γ is the dual of the graph code of Γ

Proposition

The code C_Γ has parameters $[n, k, d]$ where $n = |E|$, $k = |E| - |V| + c(\Gamma)$ and $d = \gamma(\Gamma)$

Matroids

Definition matroid

Matroids were introduced by Whitney in axiomatizing and generalizing the concepts of independence in linear algebra and cycle in graph theory

Definition

A matroid M is a pair $(E, \mathcal{I})$ consisting of a finite set E and a collection $\mathcal{I}$ of subsets of E such that:

(I.1) $\emptyset \in \mathcal{I}$.

(I.2) If $J \subseteq I$ and $I \in \mathcal{I}$, then $J \in \mathcal{I}$.

(I.3) If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there exists a $j \in (J \setminus I)$ such that $I \cup \{j\} \in \mathcal{I}$.

A subset I of E is called independent if $I \in \mathcal{I}$
otherwise it is called dependent
Condition (I.2) is called the independence augmentation axiom

Definition matroid

Matroids were introduced by Whitney in axiomatizing and generalizing the concepts of independence in linear algebra and cycle in graph theory

Definition

A matroid M is a pair $(E, \mathcal{I})$ consisting of
a finite set E and a collection $\mathcal{I}$ of subsets of E such that:

(I.1) $\emptyset \in \mathcal{I}$.

(I.2) If $J \subseteq I$ and $I \in \mathcal{I}$, then $J \in \mathcal{I}$.

(I.3) If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there exists a $j \in (J \setminus I)$ such that $I \cup \{j\} \in \mathcal{I}$.

A subset I of E is called independent if $I \in \mathcal{I}$
otherwise it is called dependent
Condition (I.2) is called the independence augmentation axiom

Basis and dimension

If J is a subset of E, then J has a maximal independent subset
that is there exists an $I \in \mathcal{I}$ such that $I \subseteq J$ and
I is maximal with respect to this property and the inclusion

If I_1 and I_2 are maximal independent subsets of J
then $|I_1| = |I_2|$ by condition (I.3)

The rank or dimension $r(J)$ of a subset J of E is
the number of elements of a maximal independent subset of J

An independent set of rank $r(M)$ is called a basis of M
The collection of all bases of M is denoted by $\mathcal{B}$

Example: uniform matroid

Let n and k be non-negative integers such that $k \leq n$
Let $[n] = \{1, \ldots, n\}$
Let $\mathcal{I}_{n,k} = \{I \subseteq U_{n,k} : |I| \leq k\}$

Then $([n], \mathcal{I}_{n,k})$ is a matroid and it is denoted by $U_{n,k}$
It is called the uniform matroid of rank k on n elements

A subset B of $[n]$ is a basis of $U_{n,k}$ iff $|B| = k$
The matroid $U_{n,n}$ has no dependent sets and is called free

Simple matroid

Let $(E, \mathcal{I})$ be a matroid
An element x in E is called a loop if $\{x\}$ is a dependent set

Let x and y in E be two distinct elements that are not loops
Then x and y are called parallel if $r(\{x, y\}) = 1$

The matroid is called simple if it has no loops and no parallel elements

$U_{n,2}$ is up to isomorphism the only simple matroid on n elements of rank two

Simple matroid

Let $(E, \mathscr{I})$ be a matroid
An element x in E is called a loop if $\{x\}$ is a dependent set

Let x and y in E be two distinct elements that are not loops
Then x and y are called parallel if $r(\{x, y\}) = 1$

The matroid is called simple if it has no loops and no parallel elements

$U_{n,2}$ is up to isomorphism the only simple matroid on n elements of rank two

Isomorphic matroids

Let $M_1 = (E_1, \mathscr{I}_1)$ and $M_2 = (E_2, \mathscr{I}_2)$ be matroids

A map $\varphi : E_1 \to E_2$ is called a morphism of matroids
if $\varphi(I)$ is dependent in M_2 for all I dependent in M_1

The map is called an isomorphism of matroids
if it is a morphism of matroids and it has an inverse map
$\varphi^{-1} : E_2 \to E_1$ that is a morphism of matroids

The matroids are called isomorphic
if there is an isomorphism of matroids between them

Representable matroids

Let G be a $k \times n$ matrix with entries in a field $\mathbb{F}$

Let E be the set $[n]$ indexing the columns of G
Let $\mathcal{I}_G$ be the collection of all subsets I of E
such that the columns of G_I are independent
Then $M_G = (E, \mathcal{I}_G)$ is a matroid

A matroid that is isomorphic with an M_G is called representable

The Fano plane is representable iff $\mathbb{F}$ has characteristic two

A representable matroid satisfies Pappos

Representable matroids

Let G be a $k \times n$ matrix with entries in a field $\mathbb{F}$

Let E be the set $[n]$ indexing the columns of G
Let $\mathcal{I}_G$ be the collection of all subsets I of E
such that the columns of G_I are independent
Then $M_G = (E, \mathcal{I}_G)$ is a matroid

A matroid that is isomorphic with an M_G is called representable

The Fano plane is representable iff $\mathbb{F}$ has characteristic two

A representable matroid satisfies Pappos

Number of representable matroids

Let g_n be the number of isomorphism classes of simple matroids on n points

n	1	2	3	4	5	6	7	8
g_n	1	1	2	4	9	26	101	950

Asymptotically $g_n \approx 2^{2^n}$ for $n \to \infty$ since:

$$\log_2 \log_2 g_n \leq n - \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

$$\log_2 \log_2 g_n \geq n - \frac{3}{2} \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

Number of $k \times n$ matrices with entries in $\mathbb{F}_q$, $k \leq n$ is at most $(n+1)q^{n^2}$
Vast majority of all matroids on n elements is not representable

Number of representable matroids

Let g_n be the number of isomorphism classes of simple matroids on n points

n	1	2	3	4	5	6	7	8
g_n	1	1	2	4	9	26	101	950

Asymptotically $g_n \approx 2^{2^n}$ for $n \to \infty$ since:

$$\log_2 \log_2 g_n \leq n - \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

$$\log_2 \log_2 g_n \geq n - \frac{3}{2} \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

Number of $k \times n$ matrices with entries in $\mathbb{F}_q$, $k \leq n$ is at most $(n+1)q^{n^2}$

Vast majority of all matroids on n elements is not representable

Number of representable matroids

Let g_n be the number of isomorphism classes of simple matroids on n points

n	1	2	3	4	5	6	7	8
g_n	1	1	2	4	9	26	101	950

Asymptotically $g_n \approx 2^{2^n}$ for $n \to \infty$ since:

$$\log_2 \log_2 g_n \leq n - \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

$$\log_2 \log_2 g_n \geq n - \tfrac{3}{2} \log_2 n + \mathcal{O}(\log_2 \log_2 n)$$

Number of $k \times n$ matrices with entries in $\mathbb{F}_q$, $k \leq n$ is at most $(n+1)q^{n^2}$

Vast majority of all matroids on n elements is not representable

Matroids and codes

Suppose that $\mathbb{F}$ is a finite field and
G_1 and G_2 are generator matrices of a code C
Then $(E, \ell_{G_1}) = (E, \ell_{G_2})$

So the matroid $M_C = (E, \ell_C)$ of a code C is well defined by
(E, ℓ_G) for some generator matrix G of C

Simple versus projective

If C is degenerate, then there is a position i
such that $c_i = 0$ for every codeword $\mathbf{c} \in C$ and
all such positions correspond one-to-one with loops of M_C

If C is nondegenerate, then M_C has no loops and
the positions i and j with $i \neq j$ are parallel in M_C
iff the i-th column of G is a scalar multiple of the j-th column

The code C is projective iff the matroid M_C is simple

A $[n, k]$ code C is MDS iff
the matroid M_C is the uniform matroid $U_{n,k}$

Simple versus projective

If C is degenerate, then there is a position i
such that $c_i = 0$ for every codeword $\mathbf{c} \in C$ and
all such positions correspond one-to-one with loops of M_C

If C is nondegenerate, then M_C has no loops and
the positions i and j with $i \neq j$ are parallel in M_C
iff the i-th column of G is a scalar multiple of the j-th column

The code C is projective iff the matroid M_C is simple

A $[n, k]$ code C is MDS iff
the matroid M_C is the uniform matroid $U_{n,k}$

Dual matroid

Let $M = (E, \mathcal{I})$ be a matroid
Let $\mathcal{B}$ be the collection of all bases of M

Define $B^\perp = (E \setminus B)$ for $B \in \mathcal{B}$
and $\mathcal{B}^\perp = \{B^\perp : B \in \mathcal{B}\}$

Define $\mathcal{I}^\perp = \{I \subseteq E : I \subseteq B \text{ for some } B \in \mathcal{B}^\perp\}$
Then $(E, \mathcal{I}^\perp)$ is called the dual matroid of M and is denoted by $M^\perp$
The dual matroid is indeed a matroid

Dual matroids and codes

Let C be a code over a finite field
Then $(M_C)^{\perp}$ is isomorphic with $M_{C^{\perp}}$ as matroids

Let e be a loop of the matroid M
Then e is not a member of any basis of M
Hence e is in every basis of $M^{\perp}$

An element of M is called an isthmus if
it is an element of every basis of M
Hence e is an isthmus of M iff e is a loop of $M^{\perp}$

Dual matroids and codes

Let C be a code over a finite field
Then $(M_C)^\perp$ is isomorphic with $M_{C^\perp}$ as matroids

Let e be a loop of the matroid M
Then e is not a member of any basis of M
Hence e is in every basis of $M^\perp$

An element of M is called an isthmus if
it is an element of every basis of M
Hence e is an isthmus of M iff e is a loop of $M^\perp$

Proposition

Let $(E, \mathcal{I})$ be a matroid with rank function r
Then the dual matroid has rank function $r^{\perp}$ given by

$$r^{\perp}(J) = |J| - r(E) + r(E \setminus J)$$

Proof

The proof is based on the observation that

$$r(J) = \max_{B \in \mathcal{B}} |B \cap J|$$

and

$$B \setminus J = B \cap (E \setminus J)$$

Proof dual rank

$$r(J) = \max_{B \in \mathcal{B}} |B \cap J| \text{ and } B \setminus J = B \cap (E \setminus J)$$

$$\begin{aligned}
r^{\perp}(J) &= \max_{B \in \mathcal{B}^{\perp}} |B \cap J| \\
&= \max_{B \in \mathcal{B}} |(E \setminus B) \cap J| \\
&= \max_{B \in \mathcal{B}} |J \setminus B| \\
&= |J| - \min_{B \in \mathcal{B}} |J \cap B| \\
&= |J| - (|B| - \max_{B \in \mathcal{B}} |B \setminus J|) \\
&= |J| - r(E) + \max_{B \in \mathcal{B}} |B \cap (E \setminus J)| \\
&= |J| - r(E) + r(E \setminus J)
\end{aligned}$$

Circuits

Circuit

Definition

Let $M = (E, \mathcal{I})$ be a matroid
A subset C of E is called a circuit
if it is dependent and all its proper subsets are independent

A circuit of the dual matroid of M is called a cocircuit of M

Let C be a code with matroid M_C
Then $\mathbf{c}$ is a minimal codeword iff $\mathrm{supp}(\mathbf{c})$ is a cocircuit of M_C

Circuit

Definition

Let $M = (E, \mathcal{I})$ be a matroid
A subset C of E is called a circuit
if it is dependent and all its proper subsets are independent

A circuit of the dual matroid of M is called a cocircuit of M

Let C be a code with matroid M_C
Then $\mathbf{c}$ is a minimal codeword iff $\mathrm{supp}(\mathbf{c})$ is a cocircuit of M_C

Properties of circuits

Proposition

Let $\mathcal{C}$ be the collection of circuits of a matroid
Then

(C.0) $\emptyset \notin \mathcal{C}$

(C.1) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$

(C.2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \neq C_2$ and $x \in C_1 \cap C_2$
then there exists a $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$

Condition (C.2) is called the circuit elimination axiom

Properties of circuits

Proposition

Let $\mathcal{C}$ be the collection of circuits of a matroid

Then

(C.0) $\emptyset \notin \mathcal{C}$

(C.1) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$

(C.2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \neq C_2$ and $x \in C_1 \cap C_2$
then there exists a $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{x\}$

Condition (C.2) is called the circuit elimination axiom

Converse

Proposition

Let $\mathcal{C}$ be a collection of subsets of a finite set E that satisfies the conditions (C.1), (C.2) and (C.3)

Let $\mathcal{I}$ be the collection of all subsets of E that contain no member of $\mathcal{C}$

Then $(E, \mathcal{I})$ is a matroid with $\mathcal{C}$ as its collection of circuits

Proposition
Let $\Gamma = (V, E)$ be a finite graph

Let $\mathcal{C}$ the collection of all subsets $\{e_1, \ldots, e_t\}$
such that $(e_1, \ldots, e_t)$ is a cycle in Γ

Then $\mathcal{C}$ is the collection of circuits of a matroid M_Γ on E
It is called the cycle matroid of Γ

Remark
Loops in Γ correspond one-to-one to loops in M_Γ
Two edges that are no loops, are parallel in Γ iff they are parallel in M_Γ
So Γ is simple iff M_Γ is simple
e is an isthmus in the graph Γ iff e is an isthmus in the matroid M_Γ

Proposition

Let $\Gamma = (V, E)$ be a finite graph

Let $\mathcal{C}$ the collection of all subsets $\{e_1, \ldots, e_t\}$
such that $(e_1, \ldots, e_t)$ is a cycle in Γ

Then $\mathcal{C}$ is the collection of circuits of a matroid M_Γ on E
It is called the cycle matroid of Γ

Remark

Loops in Γ correspond one-to-one to loops in M_Γ
Two edges that are no loops, are parallel in Γ iff they are parallel in M_Γ
So Γ is simple iff M_Γ is simple
e is an isthmus in the graph Γ iff e is an isthmus in the matroid M_Γ

Graphic matroids

A matroid M is called graphic
if M is isomorphic with M_Γ for some graph Γ

and it is called cographic if $M^\perp$ is graphic

If Γ is a planar graph
then the matroid M_Γ is graphic by definition
but it is also cographic

Graphic matroids

A matroid M is called graphic
if M is isomorphic with M_Γ for some graph Γ

and it is called cographic if $M^\perp$ is graphic

If Γ is a planar graph
then the matroid M_Γ is graphic by definition
but it is also cographic

Let Γ be a finite graph with incidence matrix $I(\Gamma)$
Its rows generate the code C_Γ over a field $\mathbb{F}_q$

Consider the binary field
Look at all the columns indexed by the edges of a cycle of Γ
Since every vertex in a cycle is incident with exactly two edges
the sum of these columns is zero and therefore they are dependent
Removing a column gives an independent set of vectors

Hence the circuits in the matroid M_{C_Γ} coincide with the cycles in Γ
Therefore M_Γ is isomorphic with M_{C_Γ}

One can generalize this argument for any field
Hence graphic matroids are representable over any field

(Counter) examples

The matroids of the binary Hamming $[7, 4, 3]$ code
is not graphic and not cographic

Clearly the matroids of the complete graph K_5
and the bipartite graph $K_{3,3}$ are graphic by definition
but both are not cographic

Tutte found a classification for graphic matroids

Tutte-Whitney polynomial

Tutte and Whitney rank polynomial

Definition

Let $M = (E, \mathcal{I})$ be a matroid

The Whitney rank generating function $R_M(X, Y)$ is defined by

$$R_M(X, Y) = \sum_{J \subseteq E} X^{r(E)-r(J)} Y^{|J|-r(J)}$$

and the Tutte-Whitney or Tutte polynomial by

$$t_M(X, Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)}$$

Hence

$$t_M(X, Y) = R_M(X-1, Y-1)$$

Tutte and Whitney rank polynomial

Definition

Let $M = (E, \mathcal{I})$ be a matroid

The **Whitney rank generating function** $R_M(X, Y)$ is defined by

$$R_M(X, Y) = \sum_{J \subseteq E} X^{r(E)-r(J)} Y^{|J|-r(J)}$$

and the **Tutte-Whitney** or **Tutte polynomial** by

$$t_M(X, Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)}$$

Hence

$$t_M(X, Y) = R_M(X-1, Y-1)$$

Nonnegative coefficients

Whitney defined the coefficients m_{ij}
of the polynomial $R_M(X, Y)$ such that

$$R_M(X, Y) = \sum_{i=0}^{r(M)} \sum_{j=0}^{|M|} m_{ij} X^i Y^j$$

He did not define the polynomial $R_M(X, Y)$ as such

It is clear that these coefficients are nonnegative
since they count the number of elements of certain sets

The coefficients of the Tutte polynomial are also nonnegative
This follows from the counting of certain
internal and external bases of a matroid

Nonnegative coefficients

Whitney defined the coefficients m_{ij}
of the polynomial $R_M(X, Y)$ such that

$$R_M(X, Y) = \sum_{i=0}^{r(M)} \sum_{j=0}^{|M|} m_{ij} X^i Y^j$$

He did not define the polynomial $R_M(X, Y)$ as such

It is clear that these coefficients are nonnegative
since they count the number of elements of certain sets

The coefficients of the Tutte polynomial are also nonnegative
This follows from the counting of certain
internal and external bases of a matroid

Proposition

Let C be a $[n, k]$ code over $\mathbb{F}_q$

Then the Tutte polynomial t_C of the matroid M_C of the code C is

$$t_C(X, Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)}$$

Proof

$$t_M(X, Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)}$$

Now $r(E) = k$, $t = |j|$ and $l(J) = k - r(J)$

Tutte polynomial of a code

Proposition

Let C be a $[n, k]$ code over $\mathbb{F}_q$
Then the Tutte polynomial t_C of the matroid M_C of the code C is

$$t_C(X, Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)}$$

Proof

$$t_M(X, Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)} (Y-1)^{|J|-r(J)}$$

Now $r(E) = k$, $t = |j|$ and $l(J) = k - r(J)$

Tutte polynomial and ext. wt. enumerator

Theorem

Let C be a $[n, k]$ code over $\mathbb{F}_q$
Then the Tutte polynomial t_C of the matroid M_C of the code C
and the extended weight enumerator $W_C(X, Y, T)$
determine each other

$$t_C(X, Y) = Y^n (Y-1)^{-k} W_C(1, Y^{-1}, (X-1)(Y-1))$$

and

$$W_C(X, Y, T) = (X-Y)^k Y^{n-k}\ t_C\left(\frac{X + (T-1)Y}{X-Y}, \frac{X}{Y}\right)$$

Proof

$$t_C(X,Y) = \sum_{t=0}^{n} \sum_{|J|=t} (X-1)^{l(J)} (Y-1)^{l(J)-(k-t)}$$

and

$$W_C(X,Y,T) = \sum_{t=0}^{n} \sum_{|J|=t} T^{l(J)} (X-Y)^t Y^{n-t}$$

Substitute $T = (X-1)(Y-1)$

TU/e Technische Universiteit Eindhoven University of Technology

Tutte polynomial of dual matroid

Theorem

Let $t_M(X, Y)$ be the Tutte polynomial of a matroid M

Let $M^\perp$ be the dual matroid

Then

$$t_{M^\perp}(X, Y) = t_M(Y, X)$$

Proof

We proved

$$r^\perp(J) = |J| - r(E) + r(E \setminus J)$$

In particular

$$r^\perp(E) + r(E) = |E|$$

Substitute this relation into

the definition of the Tutte polynomial for the dual code

Tutte polynomial of dual matroid

Theorem

Let $t_M(X, Y)$ be the Tutte polynomial of a matroid M
Let $M^\perp$ be the dual matroid
Then

$$t_{M^\perp}(X, Y) = t_M(Y, X)$$

Proof

We proved

$$r^\perp(J) = |J| - r(E) + r(E \setminus J)$$

In particular

$$r^\perp(E) + r(E) = |E|$$

Substitute this relation into
the definition of the Tutte polynomial for the dual code

Technische Universiteit Eindhoven University of Technology

$$t_M(X,Y) = \sum_{J \subseteq E} (X-1)^{r(E)-r(J)}(Y-1)^{|J|-r(J)}$$

$r^{\perp}(J) = |J| - r(E) + r(E \setminus J)$ and $r^{\perp}(E) + r(E) = |E|$

Hence

$$\begin{aligned}
t_{M^{\perp}}(X,Y) &= \sum_{J \subseteq E} (X-1)^{r^{\perp}(E)-r^{\perp}(J)}(Y-1)^{|J|-r^{\perp}(J)} \\
&= \sum_{J \subseteq E} (X-1)^{r^{\perp}(E)-|J|-r(E \setminus J)+r(E)}(Y-1)^{r(E)-r(E \setminus J)} \\
&= \sum_{J \subseteq E} (X-1)^{|E \setminus J|-r(E \setminus J)}(Y-1)^{r(E)-r(E \setminus J)} \\
&= \sum_{J \subseteq E} (Y-1)^{r(E)-r(E \setminus J)}(X-1)^{|E \setminus J|-r(E \setminus J)} \\
&= t_M(Y,X)
\end{aligned}$$

Proof Tutte polynomial of dual matroid

$$t_M(X,Y) = \sum_{J\subseteq E} (X-1)^{r(E)-r(J)}(Y-1)^{|J|-r(J)}$$

$r^{\perp}(J) = |J| - r(E) + r(E \setminus J)$ and $r^{\perp}(E) + r(E) = |E|$

Hence

$$\begin{aligned} t_{M^{\perp}}(X,Y) &= \sum_{J\subseteq E} (X-1)^{r^{\perp}(E)-r^{\perp}(J)}(Y-1)^{|J|-r^{\perp}(J)} \\ &= \sum_{J\subseteq E} (X-1)^{r^{\perp}(E)-|J|-r(E\setminus J)+r(E)}(Y-1)^{r(E)-r(E\setminus J)} \\ &= \sum_{J\subseteq E} (X-1)^{|E\setminus J|-r(E\setminus J)}(Y-1)^{r(E)-r(E\setminus J)} \\ &= \sum_{J\subseteq E} (Y-1)^{r(E)-r(E\setminus J)}(X-1)^{|E\setminus J|-r(E\setminus J)} \\ &= t_M(Y,X) \end{aligned}$$

Theorem

Let C be a $[n, k]$ code over $\mathbb{F}_q$

Then

$$W_{C^\perp}(X, Y, T) = T^{-k} W_C(X + (T-1)Y, X - Y, T)$$

Proof Use

- $t_{M^\perp}(X, Y) = t_M(Y, X)$
- $M_{C^\perp} = (M_C)^\perp$
- $t_C(X, Y)$ and $W_C(X, Y, T)$ determine each other

MacWilliams identity of ext. wt. enum.

Theorem
Let C be a $[n, k]$ code over $\mathbb{F}_q$
Then

$$W_{C^\perp}(X, Y, T) = T^{-k} W_C(X + (T-1)Y, X - Y, T)$$

Proof Use

- $t_{M^\perp}(X, Y) = t_M(Y, X)$
- $M_{C^\perp} = (M_C)^\perp$
- $t_C(X, Y)$ and $W_C(X, Y, T)$ determine each other

Deletion-contraction of matroids

Let $M = (E, \mathcal{I})$ be a matroid of rank k
Let e be an element of E

Then the deletion $M \setminus e$
is the matroid on the set $E \setminus \{e\}$
with independent sets of the form $I \setminus \{e\}$
where I is independent in M

The contraction M/e is the matroid on the set $E \setminus \{e\}$
with independent sets of the form $I \setminus \{e\}$
where I is independent in M and e in I

Deletion-contraction of matroids

Let $M = (E, \mathcal{I})$ be a matroid of rank k
Let e be an element of E

Then the deletion $M \setminus e$
is the matroid on the set $E \setminus \{e\}$
with independent sets of the form $I \setminus \{e\}$
where I is independent in M

The contraction M/e is the matroid on the set $E \setminus \{e\}$
with independent sets of the form $I \setminus \{e\}$
where I is independent in M and e in I

Del-contr of matroids versus graphs

Let M be a graphic matroid
So $M = M_\Gamma$ for some finite graph Γ

Let e be an edge of Γ
Then

$$M_\Gamma \setminus e = M_{\Gamma \setminus e}$$

and

$$M_\Gamma / e = M_{\Gamma / e}$$

Del-contr of matroids versus codes

Let C be a code with reduced generator matrix G at position e
So $a = (1, 0, \ldots, 0)^T$ is the column of G at position e

Then

$$M_G \setminus e = M_{G \setminus a}$$

and

$$M_G / e = M_{G / a}$$

Del-contr formula for matroids

Proposition

Let $M = (E, \mathcal{I})$ be a matroid
Let e in E that is not a loop and not an isthmus

Then the following deletion-contraction formula holds:

$$t_M(X, Y) = t_{M\setminus e}(X, Y) + t_{M/e}(X, Y).$$

Exercises

Exercises fourth lecture

1. Determine the parameters of the graph code and the cycle code of the graph K_m
2. Show that the code C_{K_4} over $\mathbb{F}_2$ is equivalent to the punctured binary $[7, 3, 4]$ simplex code
3. Show that all matroids on at most 3 elements are graphic
4. Give an example of a matroid that is not graphic and give a proof of this fact
5. Give a classification of the equivalence classes of all matroids on at most 5 points
6. Compute the Tutte polynomials of all matroids on at most 5 points by means of the deletion-contraction formula