Polynomial invariants of geometric structures

Ruud Pellikaan
g.r.pellikaan@tue.nl

Castellon
2016 May 4

Characteristic polynomial

- Knots and links and its (multi variable) Alexander polynomial
- Complement of projective curve and its Alexander polynomial
- Arrangement and its (two variable) characteristic polynomial
- Milnor fibre of an isolated singularity and
  its characteristic polynomial of the monodromy

Zeta function

- Number field and its zeta function
- Algebraic variety over a finite field and
  its (two variable) zeta function, characteristic polynomial of Frobenius
- Error-correcting codes and its (two variable) zeta function
- Graph and its zeta function

Weight enumerator

- Code and its weight enumerator
- Code and its extended weight enumerator
- Code and its generalized weight enumerator

Chromatic, Tutte and characteristic polynomial

- Graph and its chromatic polynomial
- Matroid and its characteristic polynomial
- Matroid and its two variable Tutte polynomial
- Matroid its (two variable) zeta function

Content

1. Error-correcting codes
2. Weight enumerator
3. Arrangements and codes
4. Arrangements and weight enumerators
5. Extended weight enumerator
6. Matroids
7. Tutte-Whitney polynomial

References

- T. Britz, Higher support matroids
  Discrete Mathematics 307, 2300-2308, (2007)
- T. Britz, Code enumerators and Tutte polynomials
  IEEE Transactions on Information Theory 56, 4350-4358, (2010)
- Relinde Jurrius
  Codes, arrangements, matroids, and their polynomial links
  PhD thesis, Technical University Eindhoven, August 2012
- Relinde Jurrius and Ruud Pellikaan
  Codes, arrangements and matroids
  in Series on Coding Theory and Cryptology vol. 8
  Algebraic geometry modelling in information theory, pp. 219–325, 2013

(Generalized) weight enumerator

Let C be a code of length n
A_w denotes the number of codewords in C of weight w
$A_w^{(r)}$ denotes the number of subspaces of C of dimension r weight w

The weight enumerator is:

$$W_C(X,Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w.$$

The r-th generalized weight enumerator is:

$$W_C^{(r)}(X,Y) = \sum_{w=0}^{n} A_w^{(r)} X^{n-w} Y^w.$$

Theorem

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

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

Proof
Several proofs are known

Proposition

Let $W_C(X, Y)$ be the weight enumerator of C
Then the probability of undetected error on a
q-ary symmetric channel with cross-over probability p is given by

$$P_{ue}(p) = W_C\left(1 - p, \frac{p}{q-1}\right) - (1-p)^n.$$

Arrangements and codes

Let C and D be linear codes in $\mathbb{F}_q^n$

Then C is called permutation equivalent to D
if there exists a permutation matrix Π such that $\Pi(C) = D$
If moreover $C = D$, then Π is called an permutation automorphism of C

The code C is called generalized or monomial equivalent to D
if there exists a monomial matrix M such that $M(C) = D$
If moreover $C = D$, then M is called a monomial automorphismof C

An arrangement in $\mathbb{F}^k$ is an
n-tuple $(H_1, \ldots, H_n)$ of hyperplanes in $\mathbb{F}^k$

The arrangement is called simple
if all the n hyperplanes are mutually distinct

The arrangement is called central if $\mathbf{0} \in H_j$ for all j
If the arrangement is central one considers the hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F})$

A central arrangement is called essential if $\cap_j H_j = \{\mathbf{0}\}$
Projective systems and essential arrangements are dual notions

Let $G = (g_{ij})$ be a generator matrix of a
nondegenerate code C of dimension k
So G has no zero columns

Let H_j be the linear hyperplane in $\mathbb{F}_q^k$ with equation

$$g_{1j}X_1 + \cdots + g_{kj}X_k = 0.$$

$\mathcal{A}_G$ is the arrangement $(H_1, \ldots, H_n)$ associated with G

There is a one-to-one correspondence between:

1. generalized equivalence classes of nondegenerate $[n, k]$ codes over $\mathbb{F}_q$
2. equivalence classes of essential arrangements of n hyperplanes in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

Proposition

Let C be a nondegenerate code over $\mathbb{F}_q$ with generator matrix G
Let $\mathbf{c}$ be a codeword $\mathbf{c} = \mathbf{x}G$ for the unique $\mathbf{x} \in \mathbb{F}_q^k$

Then $n - \mathrm{wt}(\mathbf{c})$ is equal to the number of hyperplanes of $\mathcal{A}_G$ through $\mathbf{x}$

Proof

Now $c_j = \sum_i g_{ij} x_i$
So $c_j = 0$ if and only if $\mathbf{x} \in H_j$
Hence

$$n - \mathrm{wt}(\mathbf{c}) = |\{ j \mid c_j = 0 \}| = |\{ j \mid \mathbf{x} \in H_j \}|$$

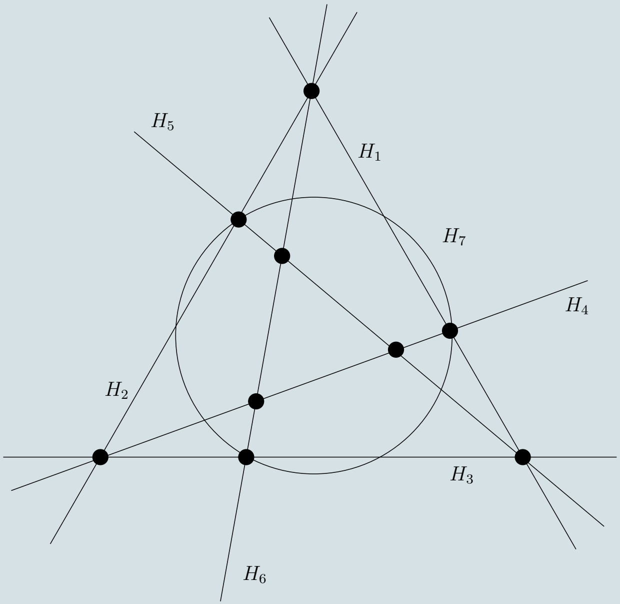
Arrangements and weight enumerator

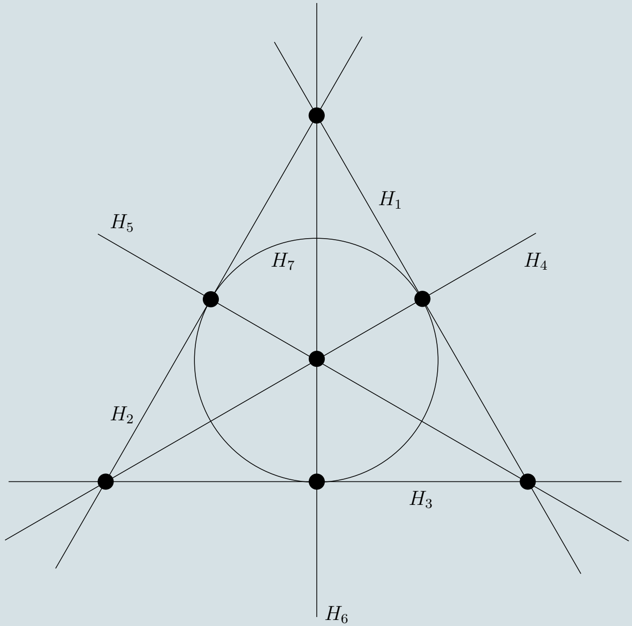
A_w the number of codewords of weight w equals
the number of points that are on exactly $n-w$ of the hyperplanes of $\mathcal{A}_G$

In particular A_n is equal to the number of points that is in
the complement of the union of these hyperplanes in $\mathbb{F}_q^k$

This number can be computed by the principle of inclusion/exclusion:

$$\begin{aligned} A_n &= q^k - |H_1 \cup \cdots \cup H_n| \\ &= q^k + \sum_{w=1}^{n} (-1)^w \sum_{i_1 < \cdots < i_w} |H_{i_1} \cap \cdots \cap H_{i_w}|. \end{aligned}$$





$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Let C be the code over $\mathbb{F}_q$ with generator matrix G
For $q = 2$, this is the simplex code $\mathcal{S}_2(2)$
The columns of G represent also the coefficients of the lines of $\mathcal{A}_G$

Assume q is even
$A_0 = 1$
$A_4 = 7(q-1)$ there are 7 points on exactly 3 lines
$A_6 = 7(q-1)[(q+1)-3] = 7(q-1)(q-2)$ there are 7 lines
and $(q+1)-3$ points of such a line is exactly on one of these
$A_7 = q^3 - A_0 - A_4 - A_6 = (q-1)(q-2)(q-4)$
So

$$W_C(X,Y) = X^7 + 7(q-1)X^3Y^4 + 7(q-1)(q-2)XY^6 + (q-1)(q-2)(q-4)Y^7$$

Assume q is odd, then similarly

$$W_C(X,Y) =$$

$$X^7+6(q-1)X^3Y^4+3(q-1)X^2Y^5+(q-1)(7q-17)XY^6+(q-1)(q-3)^2Y^7$$

The following method is based on Katsman-Tsfasman
Later we will encounter another method:
matroids and the Tutte polynomial by Greene

Definition
For a subset J of $[n] := \{1, 2, \dots, n\}$ define

$$\begin{aligned} C(J) &= \{\mathbf{c} \in C | c_j = 0 \text{ for all } j \in J\} \\ l(J) &= \dim C(J) \\ B_J &= q^{l(J)} - 1 \\ B_t &= \sum_{|J|=t} B_J \end{aligned}$$

The encoding map $\mathbf{x} \mapsto \mathbf{x}G = \mathbf{c}$
from vectors $\mathbf{x} \in \mathbb{F}_q^k$ to codewords
gives the following isomorphism of vector spaces

$$\bigcap_{j \in J} H_j \cong C(J)$$

Furthermore B_J is equal to the number of nonzero codewords $\mathbf{c}$
that are zero at all H_j in J

$$B_J = |C(J) \setminus \{0\}| = \left| \bigcap_{j \in J} H_j \setminus \{0\} \right|$$

Lemma

Let C be a linear code with generator matrix G

Let $J \subseteq [n]$ and $|J| = t$

G_J is the $k \times t$ submatrix of G existing of the columns of G indexed by J

Let $r(J)$ be the rank of G_J

Then $l(J) = k - r(J)$

Lemma

Let C be an $\mathbb{F}_q$-linear code of dimension k

Let d and $d^\perp$ be the minimum distance of C and $C^\perp$, respectively

Let $J \subseteq [n]$ and $|J| = t$

Then

$$l(J) = \begin{cases} k-t & \text{for all } t < d^\perp \\ 0 & \text{for all } t > n-d \end{cases}$$

and

$$B_t = \begin{cases} \binom{n}{t}(q^{k-t}-1) & \text{for all } t < d^\perp \\ 0 & \text{for all } t > n-d \end{cases}$$

Proposition

B_t relates to the weight distribution as follows:

$$B_t = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w$$

Proof

Count in two ways the number of elements of the set

$$\{\ (J, \mathbf{c}) \mid J \subseteq [n], |J| = t, \mathbf{c} \in C(J), \mathbf{c} \neq 0\ \}$$

Theorem
The generalized weight enumerator is given by the following formula:

$$W_C(X,Y) = X^n + \sum_{t=0}^{n} B_t (X-Y)^t Y^{n-t}$$

Proof
Use the previous proposition
the fact that $B_t = 0$ for $t > n-d$
change the order of summation and
use the binomial expansion:

$$X^{n-w} = ((X-Y)+Y)^{n-w}$$

Proposition

The following formula holds:

$$A_w = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t.$$

Proposition

The weight distribution of an MDS code of length n, dimension k and minimum distance $d = n - k + 1$

$$A_w = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} \left(q^{w-d+1-j} - 1\right)$$

for $w \geq d = n - k + 1$

Extended weight enumerator

Let G be the generator matrix of a linear $[n, k]$ code C over $\mathbb{F}_q$

$\mathbb{F}_q$ is a subfield of $\mathbb{F}_{q^m}$

Consider the code $C \otimes \mathbb{F}_{q^m}$ over $\mathbb{F}_{q^m}$
by taking all $\mathbb{F}_{q^m}$-linear combinations of the codewords in C
This is called the extension code of C over $\mathbb{F}_{q^m}$

G is also a generator matrix for the extension code $C \otimes \mathbb{F}_{q^m}$
Hence $C \otimes \mathbb{F}_{q^m}$ has dimension k over $\mathbb{F}_{q^m}$

Remember:

Definition

For a subset J of $[n] := \{1, 2, \ldots, n\}$ define

$$\begin{aligned} C(J) &= \{\, \mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J \,\} \\ l(J) &= \dim C(J) \end{aligned}$$

Lemma

Let C be a linear code with generator matrix G
Let $J \subseteq [n]$ and $|J| = t$
G_J is the $k \times t$ submatrix of G existing of the columns of G indexed by J
Let $r(J)$ be the rank of G_J
Then $l(J) = k - r(J)$

$l(J) = k - r(J)$ by the previous lemma
$r(J)$ is independent of the extension field $\mathbb{F}_{q^m}$

Therefore

$$\dim_{\mathbb{F}_q} C(J) = \dim_{\mathbb{F}_{q^m}} (C \otimes \mathbb{F}_{q^m})(J)$$

This motivates the usage of T as a variable for q^m in the next definition

Remember:
Let C be a linear code over $\mathbb{F}_q$

$$\begin{aligned} B_J &= q^{l(J)} - 1 \\ B_t &= \sum_{|J|=t} B_J \end{aligned}$$

Extend: Definition

$$\begin{aligned} B_J(T) &= T^{l(J)} - 1 \\ B_t(T) &= \sum_{|J|=t} B_J(T) \end{aligned}$$

Note that $B_J(q^m)$ is the number of nonzero codewords in $(C \otimes \mathbb{F}_{q^m})(J)$

Remember:

$$W_C(X,Y) = X^n + \sum_{t=0}^{n} B_t (X-Y)^t Y^{n-t}$$

Define the extended weight enumerator by

$$W_C(X,Y,T) = X^n + \sum_{t=0}^{n} B_t(T) (X-Y)^t Y^{n-t}$$

Is well-defined for any linear subspace C of $\mathbb{F}^n$ over any field $\mathbb{F}$

Theorem
The following holds:

$$W_C(X,Y,T) = \sum_{w=0}^{n} A_w(T) X^{n-w} Y^w$$

$$A_0(T) = 1, \text{ and } A_w(T) = \sum_{t=n-w}^{n} (-1)^{n+w+t} \binom{t}{n-w} B_t(T)$$

for $0 < w \leq n$ and

$$B_t(T) = \sum_{w=d}^{n-t} \binom{n-w}{t} A_w(T)$$

Proof is similar to the proof relating the A_w's and B_t's

Proposition

The weight distribution of an MDS code of length n and dimension k is given by

$$A_w(T) = \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} \left(T^{w-d+1-j} - 1\right)$$

for $w \geq d = n - k + 1$

Proof

Similar to the proof for A_w

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

$$W_C(X, Y, q^m) = W_{C \otimes \mathbb{F}_{q^m}}(X, Y)$$

The number of codewords in $C \otimes \mathbb{F}_{q^m}$ of weight w
is equal to $A_w(q^m)$

Proof
Substituting $T = q^m$ in $B_t(T)$ gives
$B_t(q^m)$ which is equal to the B_t of $C \otimes \mathbb{F}_{q^m}$

Theorem

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

Then

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

Proof

Substituting $T = q^m$ gives the MacWilliams identity for $C \otimes \mathbb{F}_{q^m}$

$$W_{C^\perp}(X, Y, q^m) = q^{-mk} W_C(X + (q^m - 1)Y, X - Y, q^m)$$

which holds for all m

Now $A_w(T)$ is a polynomial in T with coefficient in $\mathbb{Z}$

Giving infinitely many identities for the weight distributions of $C \otimes \mathbb{F}_{q^m}$ and $C^\perp \otimes \mathbb{F}_{q^m} = (C \otimes \mathbb{F}_{q^m})^\perp$

The following formula will be useful later in identifying the extended weight enumerator with the Tutte polynomial

Proposition

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

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

Proof

Use the description of $W_C(X,Y,T)$ in terms of the $B_t(T)$ and the definition of $B_t(T)$ in terms of the $l(J)$

Matroids

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

If J is a subset of E, then J has a maximal independent subset
if 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 $\mathcal{B}$

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

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 over the field $\mathbb{F}$

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

So the matroid $M_C = (E, \mathcal{I}_C)$ of a code C is well defined by
$(E, \mathcal{I}_G)$ for some generator matrix G of C

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

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

Tutte-Whitney 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 dichromatic Tutte polynomial by

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

Hence

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

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

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

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

Theorem

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

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

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

Second identity proved by Greene (1976) in case $T = \mathbb{F}_q$

Similar result holds the generalized weight enumerators $W_C^{(r)}(X, Y)$ by Britz (2007,2010)

Theorem

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

Let $M^\perp$ be the dual matroid

Then

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

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

The following polynomials determine each other:

$W_C(X, Y, T)$ extended weight enumerator of C

$\{W_C^{(r)}(X, Y) | r = 1, \ldots, k\}$ generalized weight enumerators of C

$t_C(X, Y)$ dichromatic Tutte polynomial of matroid M_C

$\chi_C(S, T)$ coboundary or two variable char.pol. of geometric lattice L_C

$\zeta_C(S, T)$ two variable zeta function of C by Duursma

But

$W_C(X, Y)$ is weaker than $W_C(X, Y, T)$