Relations between invariant polynomials

Relinde Jurrius

3rd Colloquium on Galois Geometry
May 4, 2012

Motivation

Some objects and their invariant polynomials:

- Linear codes: weight enumerator
- Graphs: chromatic polynomials
- Matrices: characteristic polynomial
- Matroids: Tutte polynomial
- Knots: Alexander polynomial
- ...

Motivation

Questions to ask:

- Does one polynomial determine another?
- Do two polynomials determine each other?
- Does a polynomial determine the same polynomial for the dual structure?

In this talk

Codes and weight enumeration

Möbius and coboundary polynomial

Relations

Application and concluding remarks

Extended weight enumerator

For every linear $[n, k]$ code C with generator matrix G we have:

Extension code $[n, k]$ code $C \otimes \mathrm{GF}(q^m)$ over some extension field $\mathrm{GF}(q^m)$ generated by the words of C.

Generator matrix All the extension codes of C have the same generator matrix G.

Extended weight enumerator

For every linear $[n, k]$ code C with generator matrix G we have:

Extension code $[n, k]$ code $C \otimes \mathrm{GF}(q^m)$ over some extension field $\mathrm{GF}(q^m)$ generated by the words of C.

Generator matrix All the extension codes of C have the same generator matrix G.

Extended weight enumerator

Polynomial counting "for all extension codes" the number of words of a given weight:

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

So for $T = q^m$ we have $W_C(X, Y, q^m) = W_{C \otimes \mathrm{GF}(q^m)}(X, Y)$.

Extended weight enumerator

Theorem

The extended weight enumerator of a code C and its dual $C^{\perp}$ completely determine each other via

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

For $T = q$, we get the well-known MacWilliams relations.

Hyperplane arrangements

Arrangement of hyperplanes n-tuple of hyperplanes in $\mathrm{GF}(q)^k$.

Essential arrangement Intersection of all hyperplanes is $\{\mathbf{0}\}$, hyperplanes are in $\mathrm{PG}(k-1,q)$.

Hyperplane arrangements

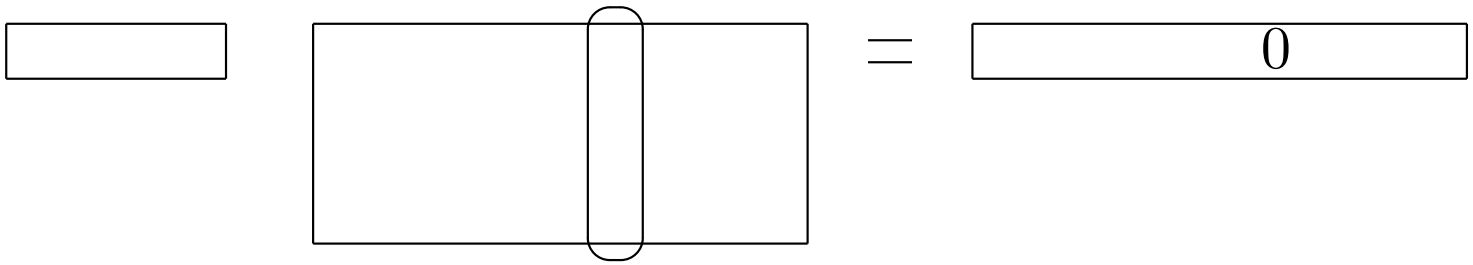
Arrangement of hyperplanes n-tuple of hyperplanes in $\mathrm{GF}(q)^k$.

Essential arrangement Intersection of all hyperplanes is $\{\mathbf{0}\}$, hyperplanes are in $\mathrm{PG}(k-1,q)$.

Columns of a generator matrix G of a linear $[n,k]$ code form a hyperplane arrangement. Notation: $(H_1,\ldots,H_n)$.

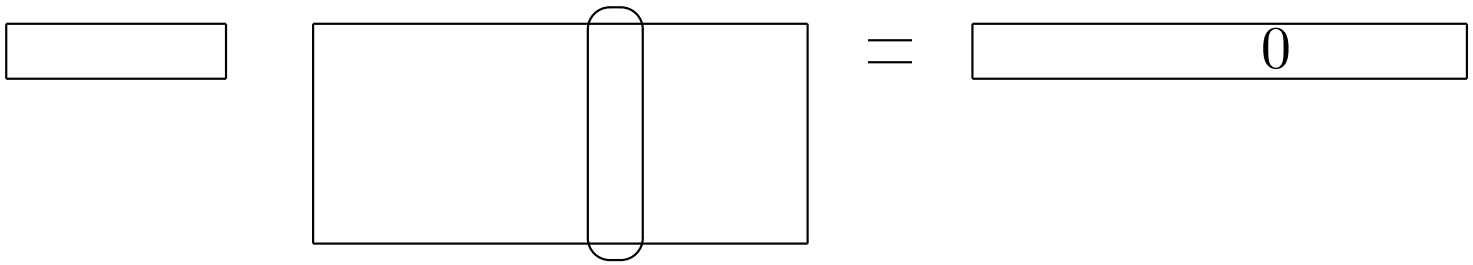
- One-to-one correspondence between equivalence classes.
- Independent of choice of G, so notation: $\mathcal{A}_C$.
- Also valid over an extension field $\mathrm{GF}(q^m)$.

Motivation: weights in linear codes



$1 \times k$ message $\mathbf{m}$ | $k \times n$ generator matrix G | $1 \times n$ codeword $\mathbf{c}$

Motivation: weights in linear codes



$1 \times k$ message $\mathbf{m}$ | $k \times n$ generator matrix G | $1 \times n$ codeword $\mathbf{c}$

Theorem

$$c_j = 0 \iff \mathbf{m} \textit{ lies in hyperplane } H_j$$

So, we need a clever way to count points in (intersections of) hyperplanes of $\mathcal{A}_C$.

Geometric lattices

A *geometric lattice* L is a set with partial ordering $\leq$ and some additional specifying properties.

An arrangement $\mathcal{A}_C$ gives rise to a geometric lattice $L(C)$:

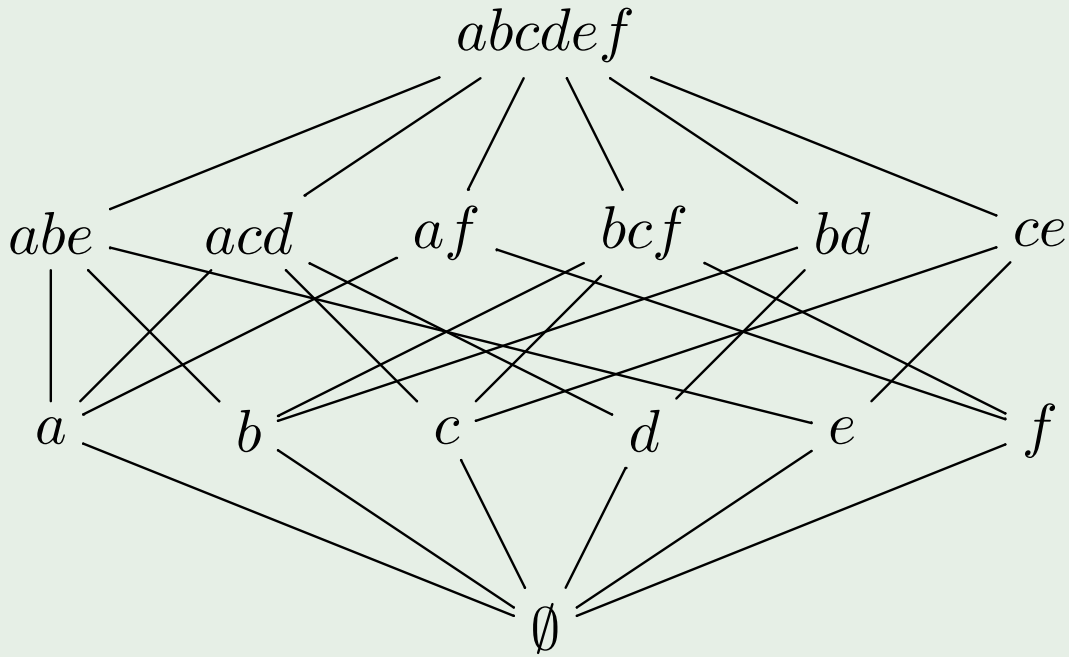
Elements	All intersections of hyperplanes
Ordering	$x \leq y$ if $y \subseteq x$
Minimum	Whole space $\mathrm{GF}(q)^k$
Maximum	Zero vector $\mathbf{0} \in \mathrm{GF}(q)^k$
Rank	Codimension of x in $\mathrm{GF}(q)^k$
Atoms	The hyperplanes of the arrangement

From now on, we will only consider codes where all hyperplanes are different for C and $C^\perp$, i.e., $d, d^\perp \geq 3$.

Geometric lattices

Example

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \end{pmatrix}$$



Möbius polynomial

The *Möbius function* of a geometric lattice is defined for all $x \leq y$ by $\mu(x, x) = 1$ and

$$\sum_{x \leq z \leq y} \mu(x, z) = \sum_{x \leq z \leq y} \mu(z, y) = 0.$$

If $x \not\leq y$, we set $\mu(x, y) = 0$. Note the function is alternating in the rank of the geometric lattice.

Möbius polynomial

The *Möbius function* of a geometric lattice is defined for all $x \leq y$ by $\mu(x, x) = 1$ and

$$\sum_{x \leq z \leq y} \mu(x, z) = \sum_{x \leq z \leq y} \mu(z, y) = 0.$$

If $x \not\leq y$, we set $\mu(x, y) = 0$. Note the function is alternating in the rank of the geometric lattice.

Möbius polynomial

The *Möbius polynomial* of a geometric lattice is defined by

$$\mu_C(S, T) = \sum_{x,y \in L(C)} \mu(x, y) S^{r(x)} T^{r(L)-r(y)}.$$

Coboundary polynomial

Coboundary polynomial

The *coboundary polynomial* of a geometric lattice is defined by

$$\chi_C(S,T) = \sum_{x,y \in L(C)} \mu(x,y) S^{a(x)} T^{r(L)-r(y)},$$

where $a(x)$ is the number of atoms smaller then x.

Coboundary polynomial

Coboundary polynomial

The *coboundary polynomial* of a geometric lattice is defined by

$$\chi_C(S,T) = \sum_{x,y \in L(C)} \mu(x,y) S^{a(x)} T^{r(L)-r(y)},$$

where $a(x)$ is the number of atoms smaller then x.

We often write

$$\mu_C(S,T) = \sum_{i=0}^{k} \mu_i(T) S^i, \qquad \chi_C(S,T) = \sum_{i=0}^{n} \chi_i(T) S^i.$$

Coboundary polynomial

Theorem

The extended weight enumerator and the coboundary polynomial completely determine each other via

$$\chi_C(S,T) = S^n W_C(1, S^{-1}, T),$$

this means $\chi_i(T) = A_{n-i}(T)$.

Coboundary polynomial

Theorem

The extended weight enumerator and the coboundary polynomial completely determine each other via

$$\chi_C(S,T) = S^n W_C(1, S^{-1}, T),$$

this means $\chi_i(T) = A_{n-i}(T)$.

Theorem

Let χ_i *be the coefficients of* $\chi_C(S,T)$ *and let* $\chi_i^\perp$ *be the coefficients of* $\chi_{C^\perp}(S,T)$. *Then*

$$T^{v-k} \sum_{i=v}^{n} \chi_i(T) = \sum_{i=n-v}^{n} \chi_i^\perp(T), \qquad v = 0, \ldots, n.$$

This follows from the MacWilliams relations for $A_i(T)$.

Main research topic

What can we say about the relations between the Möbius and coboundary polynomial?

Main research topic

What can we say about the relations between the Möbius and coboundary polynomial?

We have seen:

- $\chi_C(S,T)$ determines $\chi_{C^\perp}(S,T)$ and vice versa.

It can be shown by counter examples that in general:

- $\chi_C(S,T)$ does not determine $\mu_C(S,T)$.
- $\mu_C(S,T)$ does not determine $\chi_C(S,T)$.
- $\mu_C(S,T)$ does not determine $\mu_{C^\perp}(S,T)$.

However, there are some interesting observations to mention.

Observations

Lemma

Let $x \in L(C)$ *with* $r(x) < d^{\perp} - 1$. *Then* $r(x) = a(x)$.

Proof:

Observations

Lemma

Let $x \in L(C)$ with $r(x) < d^{\perp} - 1$. Then $r(x) = a(x)$.

Proof:

- Let G be a generator matrix of C / parity check matrix of $C^{\perp}$.

Observations

Lemma

Let $x \in L(C)$ with $r(x) < d^{\perp} - 1$. Then $r(x) = a(x)$.

Proof:

- Let G be a generator matrix of C / parity check matrix of $C^{\perp}$.
- Fact: every $1, \ldots, d^{\perp} - 1$ columns of G are independent ($G\mathbf{c}^T = \mathbf{0}$ iff $\mathbf{c} \in C^{\perp}$).

Observations

Lemma

Let $x \in L(C)$ with $r(x) < d^\perp - 1$. Then $r(x) = a(x)$.

Proof:

- Let G be a generator matrix of C / parity check matrix of $C^\perp$.
- Fact: every $1, \ldots, d^\perp - 1$ columns of G are independent ($G\mathbf{c}^T = \mathbf{0}$ iff $\mathbf{c} \in C^\perp$).
- Every $x \in L(C)$ with $r(x) < d^\perp - 1$ is the intersection of exactly $r(x)$ hyperplanes of $\mathcal{A}_C$.

Observations

Lemma

Let $x \in L(C)$ with $r(x) < d^\perp - 1$. Then $r(x) = a(x)$.

Proof:

- Let G be a generator matrix of C / parity check matrix of $C^\perp$.
- Fact: every $1, \ldots, d^\perp - 1$ columns of G are independent ($G\mathbf{c}^T = \mathbf{0}$ iff $\mathbf{c} \in C^\perp$).
- Every $x \in L(C)$ with $r(x) < d^\perp - 1$ is the intersection of exactly $r(x)$ hyperplanes of $\mathcal{A}_C$.
- So, $r(x) = a(x)$ if $r(x) < d^\perp - 1$.

Observations

Proposition

The Möbius polynomial $\mu_C(S,T)$ determines $d^\perp$.

Proof:

Observations

Proposition

The Möbius polynomial $\mu_C(S,T)$ determines $d^\perp$.

Proof:

- Coefficient of S^iT^{k-i} in $\mu_C(S,T)$ is $\sum_{\substack{x\in L\\ r(x)=i}} \sum_{\substack{y\in L\\ r(y)=i}} \mu(x,y)$.

Observations

Proposition

The Möbius polynomial $\mu_C(S,T)$ determines $d^\perp$.

Proof:

- Coefficient of S^iT^{k-i} in $\mu_C(S,T)$ is $\sum_{\substack{x\in L\\ r(x)=i}} \sum_{\substack{y\in L\\ r(y)=i}} \mu(x,y)$.
- This is exactly the number of elements in $L(C)$ of rank i.

Observations

Proposition

The Möbius polynomial $\mu_C(S,T)$ determines $d^\perp$.

Proof:

- Coefficient of S^iT^{k-i} in $\mu_C(S,T)$ is $\sum_{\substack{x\in L\\ r(x)=i}} \sum_{\substack{y\in L\\ r(y)=i}} \mu(x,y)$.
- This is exactly the number of elements in $L(C)$ of rank i.
- According to the lemma, the number of elements of rank i is:

$$\begin{aligned} &= \binom{n}{i}, && \text{if } i < d^\perp - 1,\\ &< \binom{n}{i}, && \text{if } i \geq d^\perp - 1. \end{aligned}$$

Observations

Proposition

The Möbius polynomial $\mu_C(S,T)$ determines $d^\perp$.

Proof:

- Coefficient of $S^i T^{k-i}$ in $\mu_C(S,T)$ is $\sum_{\substack{x\in L \\ r(x)=i}} \sum_{\substack{y\in L \\ r(y)=i}} \mu(x,y)$.
- This is exactly the number of elements in $L(C)$ of rank i.
- According to the lemma, the number of elements of rank i is:

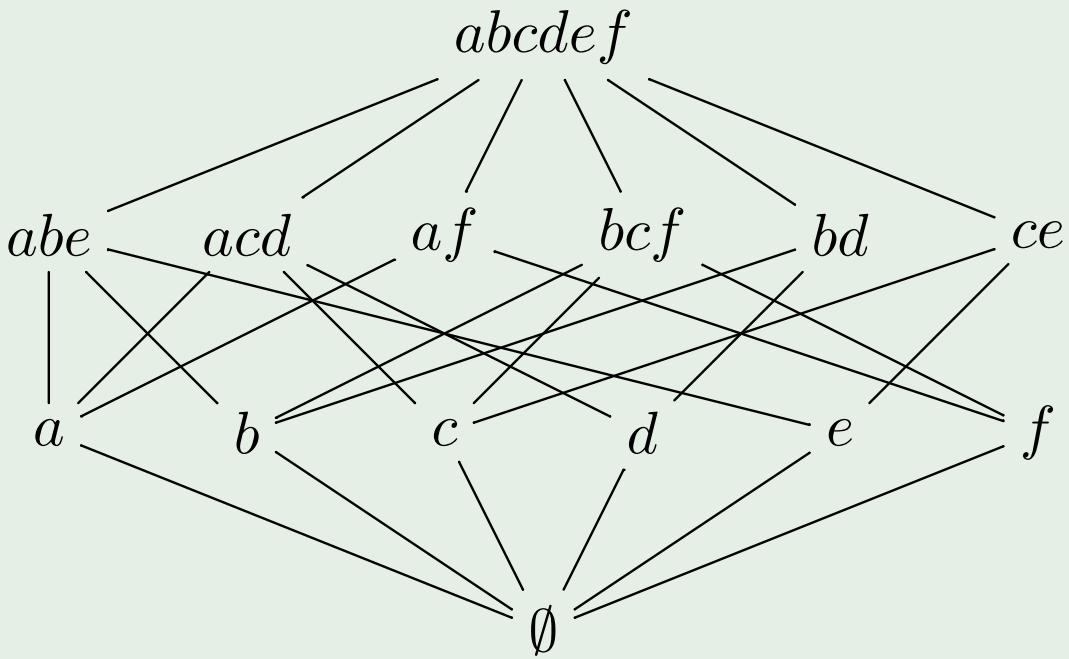
$$\begin{aligned} &= \binom{n}{i}, && \text{if } i < d^\perp - 1, \\ &< \binom{n}{i}, && \text{if } i \geq d^\perp - 1. \end{aligned}$$

- By counting elements of rank i in $L(C)$ we can determine $d^\perp$.

Observations

Example

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f \end{pmatrix}$$



We see: $a(x) = r(x)$ for $r(x) < 2$, so $d^{\perp} = 3$.

Main theorem

Question:

Given $\mu_C(S,T)$ and $\mu_{C^\perp}(S,T)$, can we determine $\chi_C(S,T)$?

Main theorem

Question:

Given $\mu_C(S,T)$ and $\mu_{C^\perp}(S,T)$, can we determine $\chi_C(S,T)$?

Answer:

Theorem

The Möbius polynomials $\mu_C(S,T)$ and $\mu_{C^\perp}(S,T)$ determine the coboundary polynomial $\chi_C(S,T)$ if $2(d+d^\perp) \geq n+3$.

Proof of main theorem

Proposition

$$\chi_i(T) = \begin{cases} \mu_i(T), & \text{for } i < d^\perp - 1, \\ 0, & \text{for } n - d < i < n, \\ 1, & \text{for } i = n. \end{cases}$$

Proof:

- $a(x) = r(x)$ for $r(x) < d^\perp - 1$ (Lemma).
- $\chi_i(T) = A_{n-i}(T)$ and there are no words of weight $0 < i < d$.
- $A_0(T) = 1 = \chi_n(T)$.

This leaves $n - d - d^\perp + 2$ of the $\chi_i(T)$ unknown.

Proof of main theorem

Idea: use MacWilliams relations on

$$\chi_{d^\perp-1}(T), \chi_{d^\perp}(T), \ldots, \chi_{n-d}(T), \chi^\perp_{d-1}(T), \chi^\perp_d(T), \ldots, \chi^\perp_{n-d^\perp}(T).$$

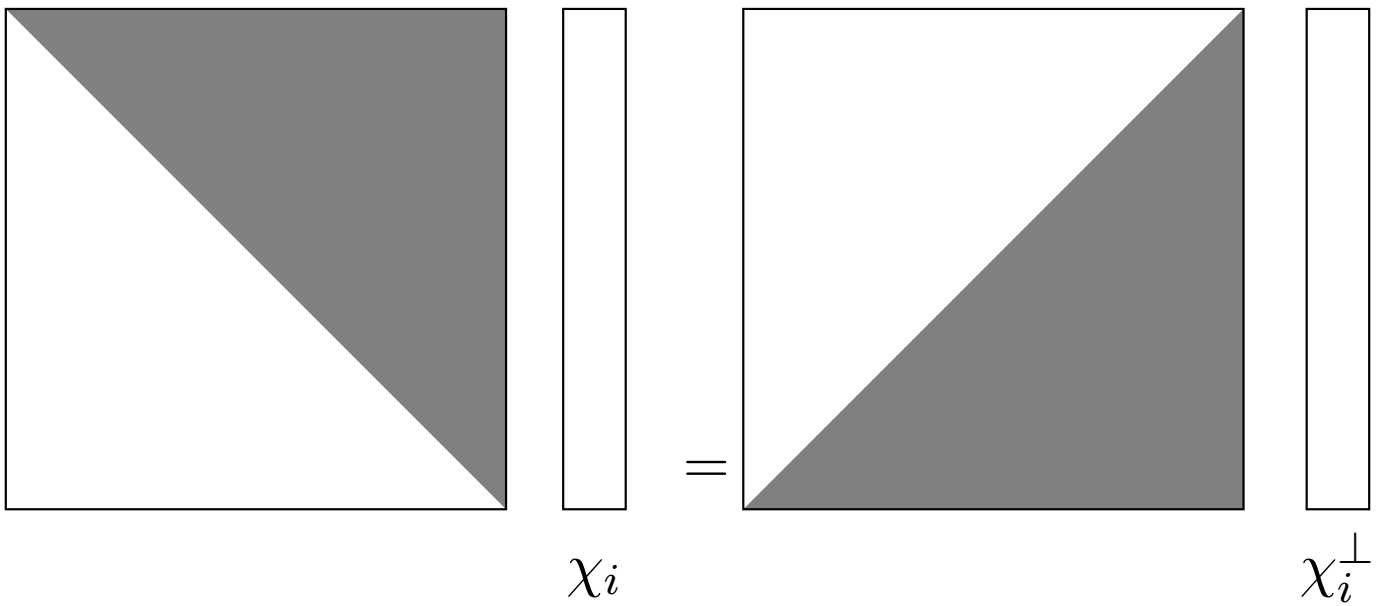
This only works is we have more equations then unknowns, so if

$$\begin{aligned} n+1 &\geq 2(n-d-d^\perp+2) \\ n+1 &\geq 2n+4-2(d+d^\perp) \\ 2(d+d^\perp) &\geq n+3. \end{aligned}$$

Left to show: the MacWilliams relations we need are independent.

Proof of main theorem

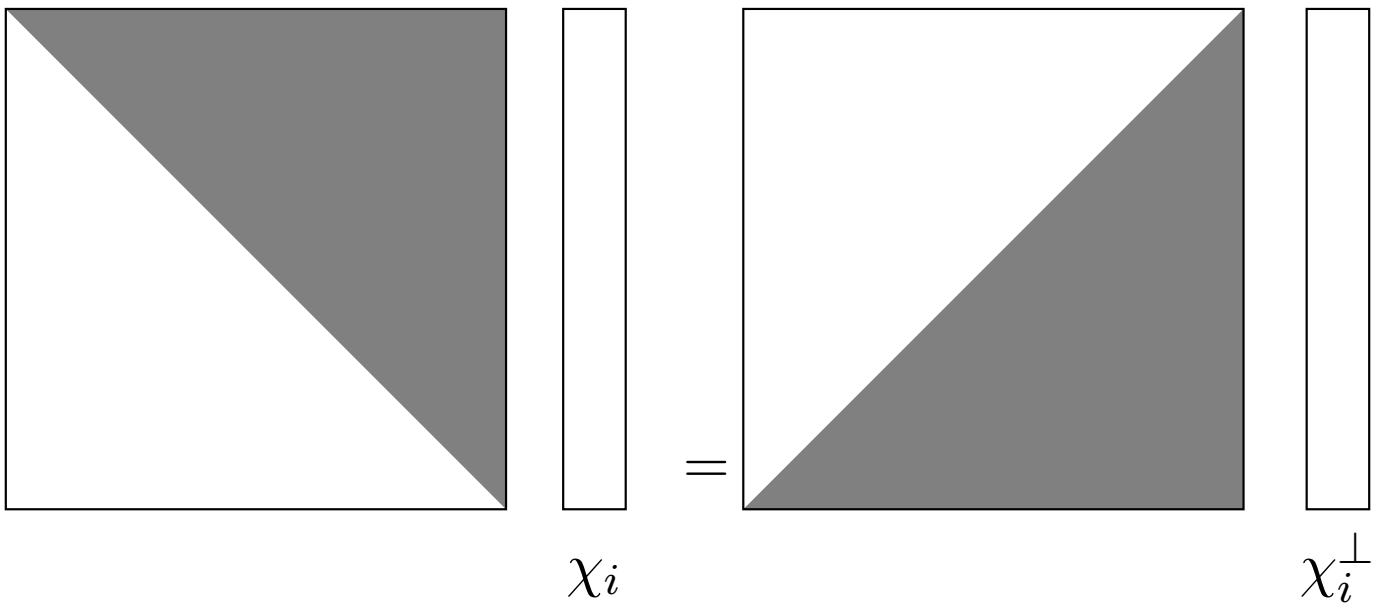
$$T^{v-k}\sum_{i=v}^{n}\chi_i(T)=\sum_{i=n-v}^{n}\chi_i^{\perp}(T),\qquad v=0,\dots,n.$$



The grey areas are nonzero entries. Both matrices have full rank.

Proof of main theorem

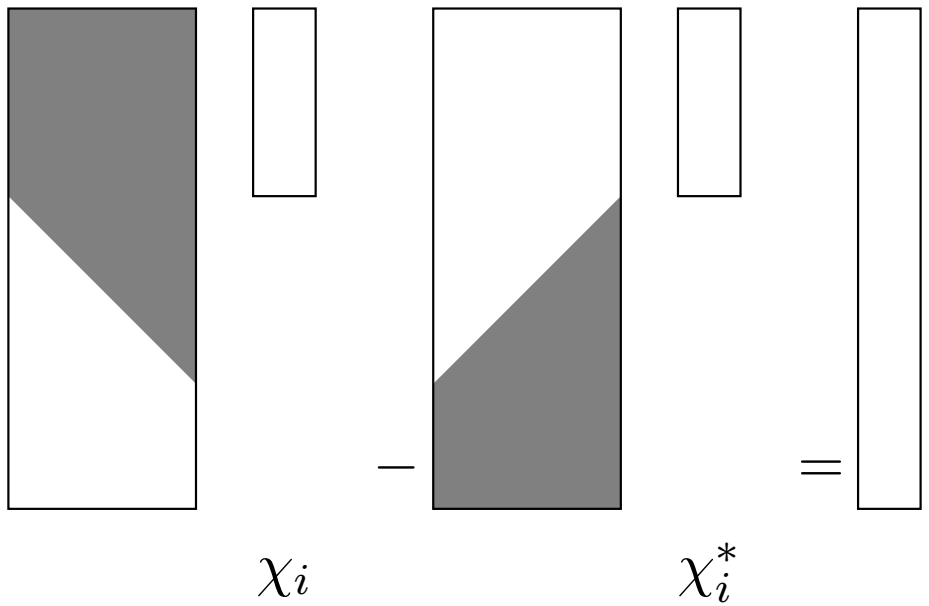
$$T^{v-k}\sum_{i=v}^{n}\chi_i(T)=\sum_{i=n-v}^{n}\chi_i^{\perp}(T),\qquad v=0,\ldots,n.$$



The grey areas are nonzero entries. Both matrices have full rank.

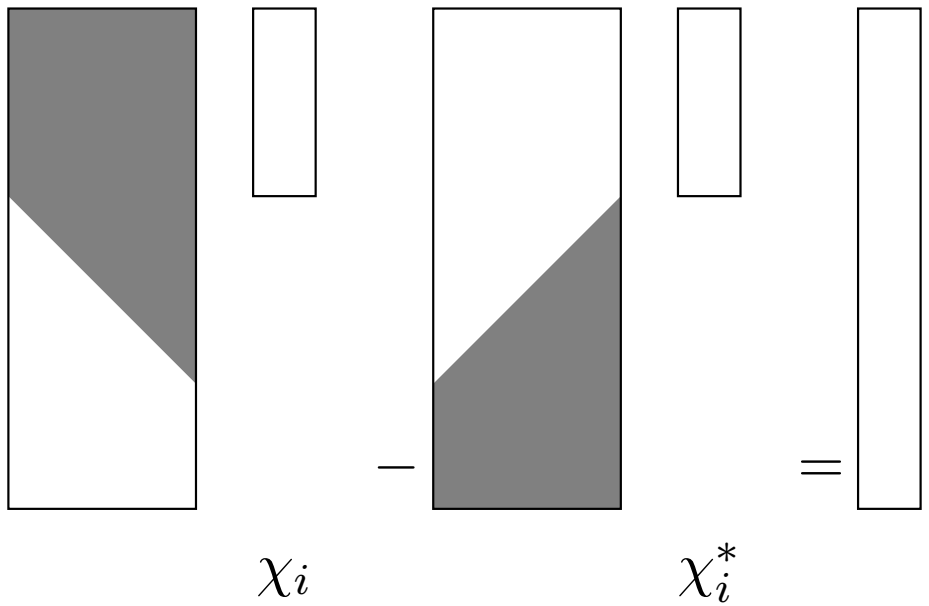
Next: "cut off" the columns corresponding to known values of $\chi_i(T)$ and $\chi_i^{\perp}$.

Proof of main theorem



We have cut off at least half of the columns, because $2(n - d - d^{\perp} + 2) \leq n + 1$. Both matrices still have full rank.

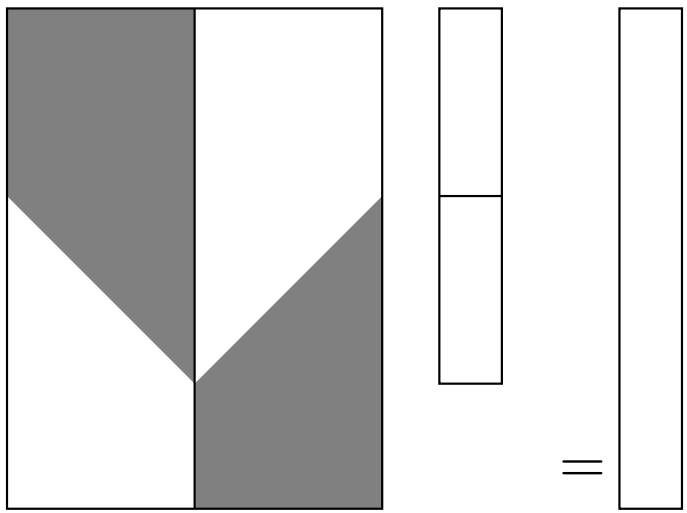
Proof of main theorem



We have cut off at least half of the columns, because $2(n - d - d^{\perp} + 2) \leq n + 1$. Both matrices still have full rank.

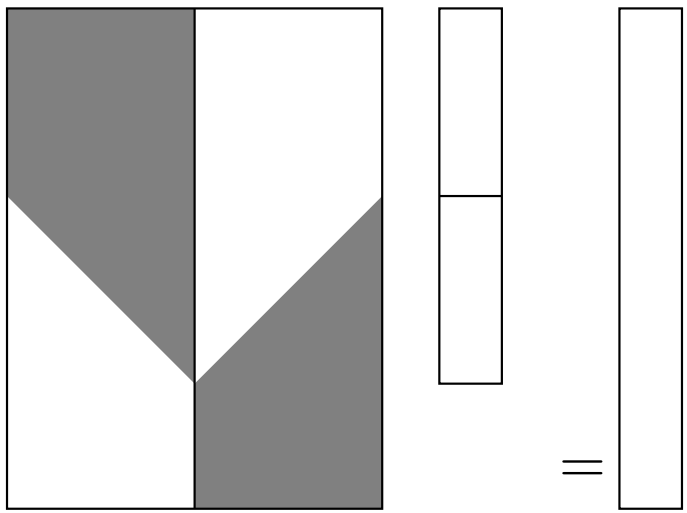
Next: we "glue" the matrices together to make one system.

Proof of main theorem



We need to show that this matrix has full rank.

Proof of main theorem



We need to show that this matrix has full rank.

Next: look at the bottom d rows, and ignore the first half of the columns – they are zero.

Proof of main theorem

The bottom-right sub matrix is part of Pascal's triangle:

$$\begin{pmatrix} 1 & 4 & 10 & 20 & 35 \\ 3 & 6 & 10 & 15 & 21 \\ 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Such a matrix always has full rank.

Proof of main theorem

The bottom-right sub matrix is part of Pascal's triangle:

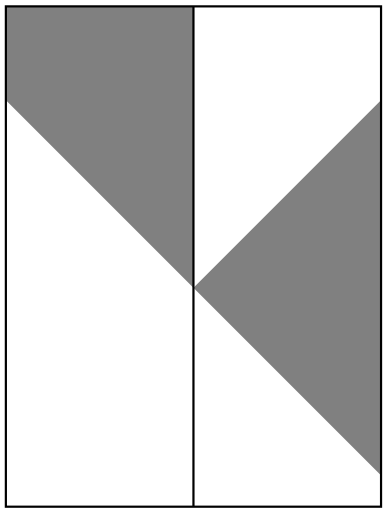
$$\begin{pmatrix} 1 & 4 & 10 & 20 & 35 \\ 3 & 6 & 10 & 15 & 21 \\ 3 & 4 & 5 & 6 & 7 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 & 0 & 1 & 4 \\ 0 & 0 & 1 & 3 & 6 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Such a matrix always has full rank.

Next: there are two possibilities.

Proof of main theorem

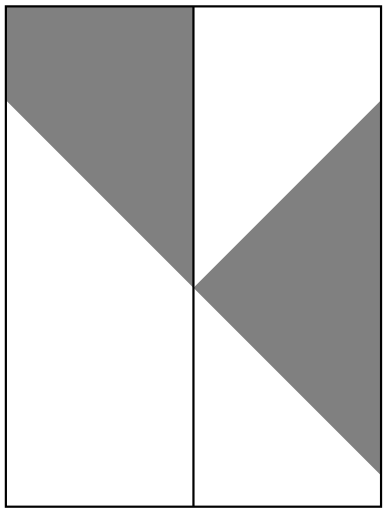
Lucky case:



If necessary we can switch d and $d^{\perp}$ by rotating over $180°$.

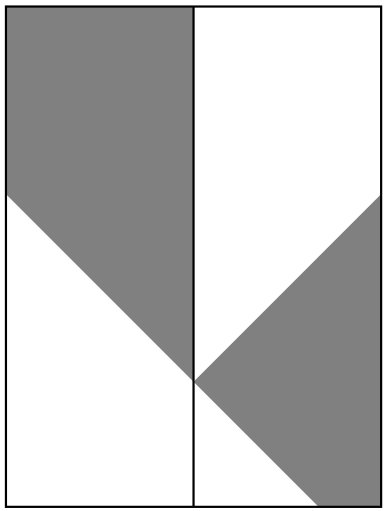
Proof of main theorem

Lucky case:



If necessary we can switch d and $d^{\perp}$ by rotating over $180°$.

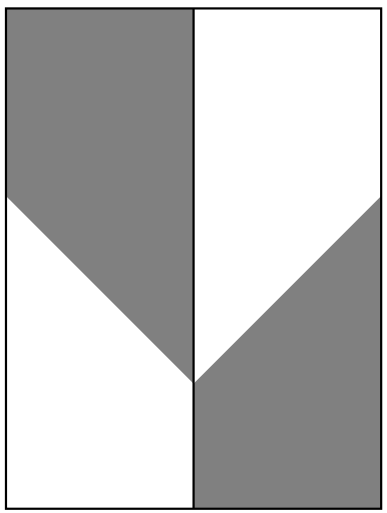
Unlucky case:



$d, d^{\perp} < n - d - d^{\perp} + 2$ in this case. We need to solve separately.

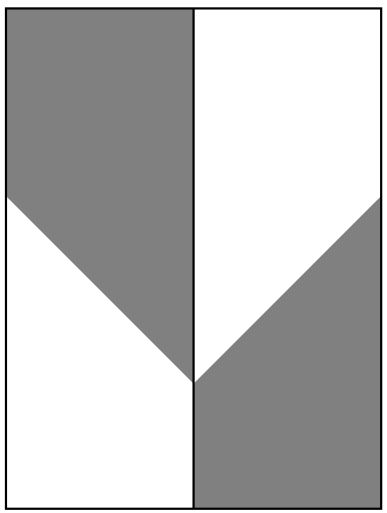
Proof of main theorem

Last step: show that powers of T and T^{-1} make it impossible to find linear combination of columns that is $\mathbf{0}$.



Proof of main theorem

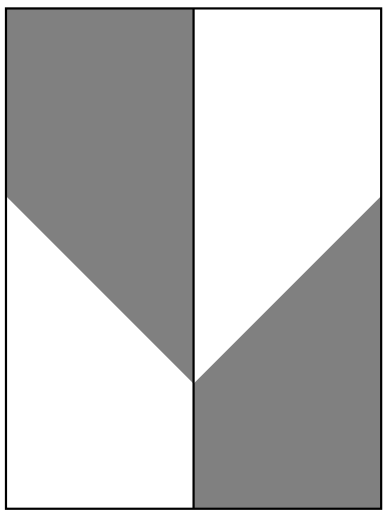
Last step: show that powers of T and T^{-1} make it impossible to find linear combination of columns that is $\mathbf{0}$.



Left side of matrix: every row is multiplied by some power of T, so linear combination of these columns has different powers of T in every entry.

Proof of main theorem

Last step: show that powers of T and T^{-1} make it impossible to find linear combination of columns that is $\mathbf{0}$.

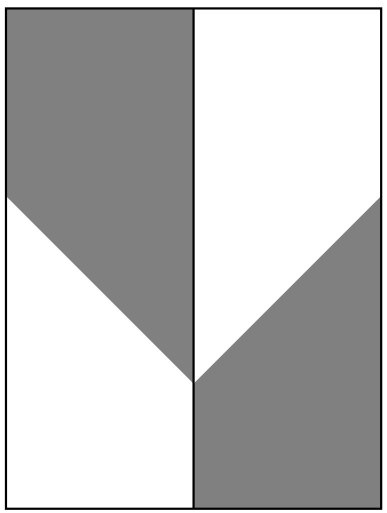


Left side of matrix: every row is multiplied by some power of T, so linear combination of these columns has different powers of T in every entry.

Right side of matrix: all entries are integers, so linear combination of these columns has same powers of T in every entry.

Proof of main theorem

Last step: show that powers of T and T^{-1} make it impossible to find linear combination of columns that is $\mathbf{0}$.



Left side of matrix: every row is multiplied by some power of T, so linear combination of these columns has different powers of T in every entry.

Right side of matrix: all entries are integers, so linear combination of these columns has same powers of T in every entry.

There are not enough free variables to compensate for this.

Proof of main theorem

We have proven the main theorem:

Theorem

The Möbius polynomials $\mu_C(S,T)$ and $\mu_{C^\perp}(S,T)$ determine the coboundary polynomial $\chi_C(S,T)$ if $2(d+d^\perp) \geq n+3$.

We have a constructive way to prove this:

- $$\chi_i(T) = \begin{cases} \mu_i(T), & \text{for } i < d^\perp - 1, \\ 0, & \text{for } n-d < i < n, \\ 1, & \text{for } i = n. \end{cases}$$
- Use this for both $\chi_i(T)$ and $\chi_i^\perp(T)$.
- Use MacWilliams relations to find the other $\chi_i(T)$ and $\chi_i^\perp(T)$.

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)
- q-ary Hamming code (dual: simplex code)

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)
- q-ary Hamming code (dual: simplex code)
- q-ary first order Reed-Muller code

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)
- q-ary Hamming code (dual: simplex code)
- q-ary first order Reed-Muller code
- ...

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)
- q-ary Hamming code (dual: simplex code)
- q-ary first order Reed-Muller code
- ...

Application

Some codes with $2(d + d^{\perp}) \geq n + 3$ are:

- MDS codes
- Almost-MDS codes ($d = n - k$) with $k \leq n/2$
- Near-MDS codes ($d = n - k, d^{\perp} = k$)
- q-ary Hamming code (dual: simplex code)
- q-ary first order Reed-Muller code
- ...

In general, a code has to be "close to MDS" to satisfy $2(d + d^{\perp}) \geq n + 3$.

Concluding remarks

- Alternative proof of main theorem: use zeta function of code.

Concluding remarks

- Alternative proof of main theorem: use zeta function of code.
- Is this bound sharp? Smallest possible counter-example: $n = 10$, $d = d^{\perp} = 3$. (Any volunteers to program this?)

Concluding remarks

- Alternative proof of main theorem: use zeta function of code.
- Is this bound sharp? Smallest possible counter-example: $n = 10$, $d = d^{\perp} = 3$. (Any volunteers to program this?)
- What about $\mu_i(T)$ for $i \geq d^{\perp} - 1$? We did not use them.

Concluding remarks

- Alternative proof of main theorem: use zeta function of code.
- Is this bound sharp? Smallest possible counter-example: $n = 10$, $d = d^{\perp} = 3$. (Any volunteers to program this?)
- What about $\mu_i(T)$ for $i \geq d^{\perp} - 1$? We did not use them.
- Look at affine space generated by coefficients of the polynomials. It's dimension tells "how many different polynomials there are". This is done for $\chi_C(S, T)$. How about $\mu_C(S, T)$ and $\mu_{C^{\perp}}(S, T)$?

Thank you for your attention.