# Hilbert Polynomials

1. Monomial Ideals
   - dimension and counting monomials
2. The Dimension of a Variety
   - a Gröbner basis for $I$ reduces to $\mathrm{in}_>(I)$
3. The Complexity of Gröbner Bases
   - a bound on the degrees of polynomials
   - cone decompositions
   - Hilbert functions of cones

MCS 563 Lecture 33
Analytic Symbolic Computation
Jan Verschelde, 11 April 2011

# Hilbert Polynomials

1. Monomial Ideals
   - dimension and counting monomials
2. The Dimension of a Variety
   - a Gröbner basis for $I$ reduces to $\mathrm{in}_>(I)$
3. The Complexity of Gröbner Bases
   - a bound on the degrees of polynomials
   - cone decompositions
   - Hilbert functions of cones

# monomial ideals

The variety of a monomial ideal $I$ is a union of planes:

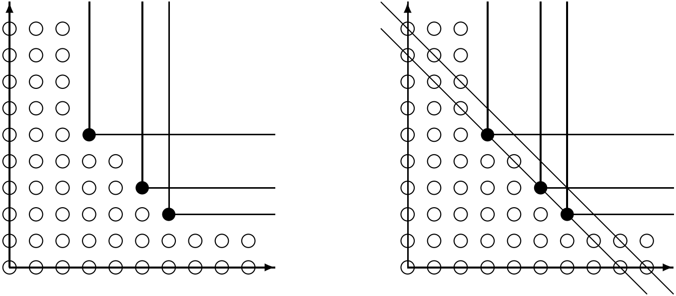
- The dimension of this variety is the highest dimension over all planes in this union.
- For $n$ variables, this dimension is $n - m$, where $m$ is the minimal number of variables in a generator $\mathbf{x}^{\mathbf{a}}$ of $I$.

If $I$ is zero dimensional, then the number of monomials not in $I$ (visualized as the number of dots under the staircase representation of $I$) equals the multiplicity of $\mathbf{0} \in V(I)$.

For positive dimension $I$, we count the monomials not in $I$.

# staircase representation

Consider $I = \langle x_1^3 x_2^5, x_1^5 x_2^3, x_1^6 x_2^2 \rangle$:



Black dots correspond to the generators.
Empty circles belong to the complement of $I$.
Observe that dividing all generators by $x_1^3 x_2^2$ will give an ideal that has **0** as a 7-fold solution.
For degree $d \geq 9$, #monomials in the complement is $5d + 2$
$= (d+1) + d + (d-1) + (d+1) + d + 7 - 6.$

## counting monomials

If $I$ is zero dimensional, then the number of monomials not in $I$ (visualized as the number of dots under the staircase representation of $I$) equals the multiplicity of $\mathbf{0} \in V(I)$.

For positive dimension $I$, we count the monomials not in $I$. For $I = \langle x_1^{a_1} x_2^{a_2} \rangle$, the complement of $I$ consists of $(a_1 + a_2)$ lines of monomials:

$$\{ \, x_1^i x_2^j \mid i = 0, 1, \ldots, a_1 - 1, j = 0, 1, \ldots, a_2 - 1 \, \}.$$

For a monomial ideal $I$ generated by $> 1$ monomial,

- we take as $b_1$ and $b_2$ the respective smallest powers of $x_1$ and $x_2$ of the generators of $I$; and
- count $(b_1 + b_2)$ lines of monomials in addition to the finite number of monomials under the staircase, counting upwards starting at $(b_1, b_2)$.
- Compensate for double counting (inclusion-exclusion).

# the Hilbert polynomial

## Theorem 1

*Consider a monomial ideal $I$ in a polynomial ring of $n$ variables with $\dim V(I) = d$. The number of monomials not in $I$ of degree $\leq s$, for $s$ sufficiently large, is a polynomial of degree $d$ in $s$ with positive coefficient of $s^d$.*

For some intuition, we look at $I = \langle \mathbf{x}^{\mathbf{a}} \rangle$:

Consider $I = \langle x_3^{a_3} \rangle$
and count all monomials not in $I$ of degree $\leq s$.

These monomials lie in $a_3$ planes perpendicular to the third coordinate axis.

Every plane holds $s(s+1)/2$ monomials $\leq s$,
so the polynomial is $a_3 s(s+1)/2$. For $I = \langle x_1^{a_1} x_2^{a_2} x_2^{a_3} \rangle$,
we have $(a_1 + a_2 + a_3)$ planes of monomials not in $I$.

## continue counting

For $I$ generated by more than one monomial,
imagine a 3-dimensional staircase representation.

As in 2 variables, we define powers $b_i$ as the smallest powers of $x_i$ in the generators of the monomial ideal.

We count the monomials in the complement of $\langle x_1^{b_1} x_2^{b_2} x_3^{b_3} \rangle$.

For sufficiently large degrees,
we add the finite number of monomials under the staircase,
starting the count at $(b_1, b_2, b_3)$.

# Gregory-Newton interpolation

## Proposition

*For a monomial ideal $I$ in a polynomial ring of $n$ variables of dimension $d$, denote by $h(s)$ the number of monomial ideals in $I$ of degree $\leq s$, for $s$ sufficiently large, then*

$$h(s) = \sum_{i=0}^{d} a_{d-i} \left( \begin{array}{c} s \\ d-i \end{array} \right), \quad a_i \in \mathbb{Z}, a_d > 0.$$

*Sketch of Proof.* That $\deg(h(s)) = d$ follows from Theorem 1. Furthermore $h(s)$ returns natural numbers when evaluated at natural values for $s$.
Counting the number of monomials for $d+1$ consecutive values of $s$ leads to a special interpolation problem.
The coefficients of the Gregory-Newton interpolating polynomial are binomial coefficients. ☐

# Hilbert Polynomials

# initial ideals

Given a term order $>$, a Gröbner basis $G$ for an ideal $I$ in $\mathbb{K}[\mathbf{x}]$ gives a basis for the initial ideal $\mathrm{in}_>(I)$ as

$$\{ \, \mathrm{LT}_>(g) \mid g \in G \, \}.$$

With $G$ we have sufficiently many leading monomials for the division (or normal form) algorithm to give a unique outcome.

If the Hilbert polynomial for $\mathrm{in}_>(I)$ is the same as the Hilbert polynomial for $I$, then a Gröbner basis gives an algorithm to compute $\dim(V(I))$.

# some notations

To reduce the dimension computation to counting monomials, we restrict our consideration to polynomials of bounded degree.

We denote

$$\begin{aligned}
\mathbb{K}[\mathbf{x}]_{\leq s} &= \{\, f \in \mathbb{K}[\mathbf{x}] \mid \deg(f) \leq s \,\}, \\
I_{\leq s} &= \{\, f \in I \mid \deg(f) \leq s \,\}, \quad \text{and} \\
\mathrm{in}_>(I)_{\leq s} &= \{\, f \in \mathrm{in}_>(I) \mid \deg(f) \leq s \,\}.
\end{aligned}$$

# Hilbert polynomials

Hilbert polynomials for $I$ and $\mathrm{I}_>(I)$ are the same:

$$\begin{aligned} h_I(s) &= \dim \mathbb{K}[\mathbf{x}]_{\leq s}/I_{\leq s} && (1) \\ &= \dim \mathbb{K}[\mathbf{x}]_{\leq s}/\mathrm{in}_>(I)_{\leq s} && (2) \\ &= h_{\mathrm{in}_>(I)} && (3) \end{aligned}$$

The equation between (1) and (2) means that the quotient rings have the same number of basis elements.

To justify this equation consider a Gröbner basis $G_>$ for $I$.

An argument by contradition assumes a different number of basis elements for the quotient rings, which then conflicts with the property of $G_>$ a Gröbner basis for $I$.

# using Macaulay 2

```
i1 : R = QQ[x,y];

i2 : I = ideal(x^3*y^5,x^5*y^3,x^6*y^2);

i3 : h = hilbertPolynomial I

o3 = 5*P
        0

o3 : ProjectiveHilbertPolynomial

i4 : H = hilbertPolynomial(I, Projective=>false)

o4 = 5

o4 : QQ[i]
```

# Hilbert Polynomials

# complexity of Gröbner basis

Thomas Dubé proved the following theorem:

## Theorem 2

*Let* $I = \langle f_1, f_2, \ldots, f_N \rangle$ *be an ideal in* $\mathbb{K}[\mathbf{x}]$ *and let*

$$d = \max_{i=1}^{N} \deg(f_i).$$

*For any term order* $>$*, the degree of polynomials required in a Gröbner basis for* $I$ *with respect to* $>$ *is bounded by*

$$2\left(\frac{d^2}{2} + d\right)^{2^{n-2}}.$$

As the Hilbert function counts the number of monomials in the complement of the ideal, it provides a measure for the monomials in a Gröbner basis of the ideal.

# Hilbert Polynomials

# cones

Let $\mathbf{u}$ be a subset of $X = \{x_1, x_2, \ldots, x_n\}$ and $f \in \mathbb{K}[\mathbf{x}]$ a homogeneous polynomial. The set

$$C(f, \mathbf{u}) = \{\ fg \mid g \in \mathbb{K}[\mathbf{u}]\ \}$$

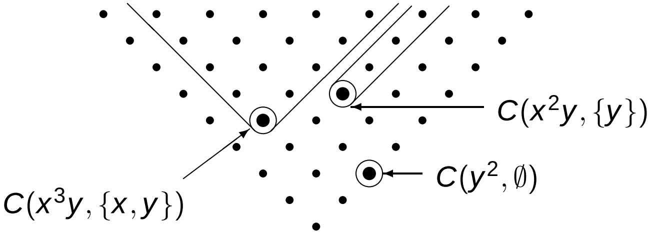
is a *cone* spanned by $f$ in $\mathbf{u}$.
The name for $C(f, \mathbf{u})$ is justified by a graphical representation for two variables.

For example $C(x^2y^3, \emptyset)$ is just one dot at $(2, 3)$.

The cone $C(x^2y^3, \{x\})$ are all multiples for $x^2y^3$, depicted as a ray extending in the left $x$-direction.

The cone $C(x^2y^3, \{x, y\})$ is a proper cone extending both to the left and right direction.

# graphical representation



Three cones:

- $C(y^2,\emptyset)$ is one dot,
- $C(x^2y^3,\{y\})$ is a ray, and
- the cone $C(x^3y,\{x,y\})$ has dimension 2.

# cone decompositions

Let $\{f_1, f_2, \ldots, f_r\}$ be a set of homogeneous polynomials with $\{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_r\}$ a set of subsets of $X$.

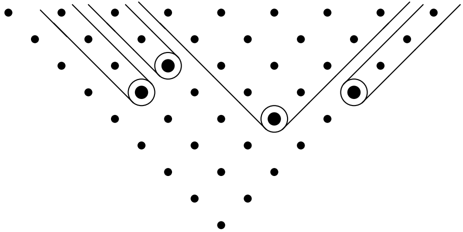
Then $P = \{(f_1, \mathbf{u}_1), (f_2, \mathbf{u}_2), \ldots, (f_r, \mathbf{u}_r)\}$ is a cone decomposition of $R$, a subring of $\mathbb{K}[\mathbf{x}]$ if

$$R = C(f_1, \mathbf{u}_1) \oplus C(f_2, \mathbf{u}_2) \oplus \cdots \oplus C(f_r, \mathbf{u}_r),$$

i.e.: the cones $C(f_i, \mathbf{u}_i)$ form a direct decomposition of $R$.

# an example

Consider $I = \langle x^4y, xy^3, y^5 \rangle$ and its cone decomposition:



The cone decomposition for $I = \langle x^4y, xy^3, y^5 \rangle$ is $\{C(x^4y, \{x\}), C(x^4y^2, \{x\}), C(xy^3, \{x, y\}), C(y^5, \{y\})\}$.

# splitting $\mathbb{K}[\mathbf{x}]$ relative to $I$

The Lemma below provides an algorithm to split $\mathbb{K}[\mathbf{x}]$ relative to an ideal $I$.

## Lemma

*Let $I$ be a monomial ideal, $f \in \mathbb{K}[\mathbf{x}]$, and $B$ is a basis for $I : f$. Then*

1. $C(f, \mathbf{u}) \subseteq I \Leftrightarrow 1 \in B$.
2. $C(f, \mathbf{u}) \cap I = \emptyset \Leftrightarrow B \cap \{ \mathbf{u}^{\mathbf{a}} \mid \mathbf{a} \in \mathbb{N}^{|\mathbf{u}|} \} = \emptyset$.

*Proof.*

1. $1 \in B \Leftrightarrow 1 \in I : f \Leftrightarrow f \in I \Leftrightarrow C(f, X) \subseteq I$.

# proof continued

② $\Rightarrow$ Assume $C(f, \mathbf{u}) \cap I = \emptyset$, then for any monomial $\mathbf{u}^\mathbf{a}$:

$$\begin{aligned} f\mathbf{u}^\mathbf{a} \in C(f, \mathbf{u}) \quad & \Rightarrow \quad f\mathbf{u}^\mathbf{a} \not\in I \\ & \Rightarrow \quad \mathbf{u}^\mathbf{a} \not\in I : f \\ & \Rightarrow \quad \mathbf{u}^\mathbf{a} \not\in B. \end{aligned}$$

$\Leftarrow$ Assume $B \cap \{ \mathbf{u}^\mathbf{a} \mid \mathbf{a} \in \mathbb{N}^{|\mathbf{u}|} \} = \emptyset$.

Then for any $\mathbf{u}^\mathbf{a}$, we have $\mathbf{u}^\mathbf{a} \not\in I : f$, otherwise $B$ would have to contain a divisor of $\mathbf{u}^\mathbf{a}$ of the form $\mathbf{u}^\mathbf{b}$.

So $\mathbf{u}^\mathbf{a} \not\in I : f \Rightarrow f\mathbf{u}^\mathbf{a} \not\in I$.

By the definition of $C(f, \mathbf{u})$, every polynomial in $C(f, \mathbf{u})$ is of the form $f\mathbf{u}^\mathbf{a}$ and hence not in $I$. $\square$

# Hilbert Polynomials

1. Monomial Ideals
    - dimension and counting monomials
2. The Dimension of a Variety
    - a Gröbner basis for $I$ reduces to $\mathrm{in}_>(I)$
3. The Complexity of Gröbner Bases
    - a bound on the degrees of polynomials
    - cone decompositions
    - Hilbert functions of cones

# Hilbert functions

The Hilbert function of $C(f, \mathbf{u})$ depends only on $\deg(f)$ and the size $|\mathbf{u}|$ of $\mathbf{u}$:

$$h_{C(f,\emptyset)}(s) = \begin{cases} 0 & \text{if} \quad s \neq \deg(f) \\ 1 & \text{if} \quad s = \deg(f) \end{cases}$$

and for $|\mathbf{u}| > 0$:

$$h_{C(f,\mathbf{u})}(s) = \begin{cases} 0 & \text{if} \quad s < \deg(f) \\ \begin{pmatrix} s - \deg(f) + |\mathbf{u}| - 1 \\ |\mathbf{u}| - 1 \end{pmatrix} & \text{if} \quad s \geq \deg(f). \end{cases}$$

For any cone decomposition $P$ of $R$, the Hilbert function of $R$ is

$$h_R(s) = \sum_{(f,\mathbf{u}) \in P} h_{C(f,\mathbf{u})}(s).$$

# deriving an upper bound

Thomas Dubé derived the following expression for the Hilbert polynomial of an ideal $I$:

$$\begin{aligned} h_I(s) &= \binom{s-d+n-1}{n-1} + \binom{s-d+n}{n} - 1 \\ &+ \sum_{i=1}^{n} \binom{s-a_i+i-1}{i}, \end{aligned}$$

where the coefficients $a_i$ are the coefficients of the Hilbert polynomial of the cone decomposition.
Applying the backward difference operator
and other techniques leads to bounds on the coefficients of the Hilbert polynomial.

# Summary + Exercises

We defined Hilbert polynomials and outlined a decomposition method to bound the complexity of a Gröbner basis.

Exercises:

1. Use a computer algebra package to derive the Gregory-Newton interpolation formulas to interpolate $(i, h_i) \in \mathbb{Z}^2$, for $i = d, d+1, \ldots, d+n$. Show that the interpolating polynomial is a linear combination of binomial coefficients.
2. Explore the command `hilbertSeries` in Macaulay 2.