Projective Planes and Beyond

Thematic Program on Rationality and Hyperbolicity

Undergraduate Workshop

Juan Migliore

June 12-16, 2023

Slides available by emailing migliore.1@nd.edu
or from the conference website.

Lecture 2: A first look at Hilbert functions

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;
- a collection $\mathfrak{L}$ of subsets, called lines;

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;
- a collection $\mathfrak{L}$ of subsets, called lines;

such that the following axioms hold:

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;
- a collection $\mathfrak{L}$ of subsets, called lines;

such that the following axioms hold:

P1. For any two distinct points, there is exactly one line through them.

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;
- a collection $\mathfrak{L}$ of subsets, called lines;

such that the following axioms hold:

P1. For any two distinct points, there is exactly one line through them.

P2. Any two distinct lines meet in exactly one point.

Review of projective planes

A projective plane, denoted $\mathbb{P}^2$, consists of:

- a set $\mathfrak{P}$, whose elements are called points;
- a collection $\mathfrak{L}$ of subsets, called lines;

such that the following axioms hold:

P1. For any two distinct points, there is exactly one line through them.

P2. Any two distinct lines meet in exactly one point.

P3. There exist four points such that no three are collinear.

Consequences for finite projective planes:

1. Any two lines of $\mathbb{P}^2$ have the same number of points. We denote this number by $d+1$, and say that the plane has order d.

Consequences for finite projective planes:

1. Any two lines of $\mathbb{P}^2$ have the same number of points. We denote this number by $d+1$, and say that the plane has order d.

2. Through every point in $\mathbb{P}^2$ there pass $d+1$ lines.

Consequences for finite projective planes:

1. Any two lines of $\mathbb{P}^2$ have the same number of points. We denote this number by $d + 1$, and say that the plane has order d.

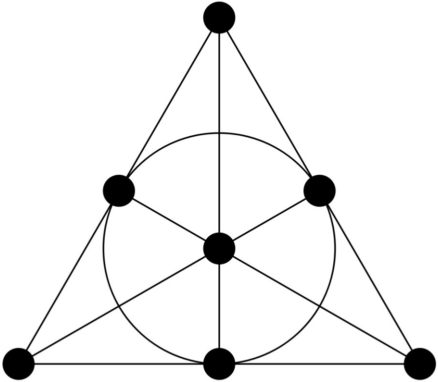
2. Through every point in $\mathbb{P}^2$ there pass $d + 1$ lines.

3. There are $d^2 + d + 1$ points and $d^2 + d + 1$ lines in $\mathbb{P}^2$.

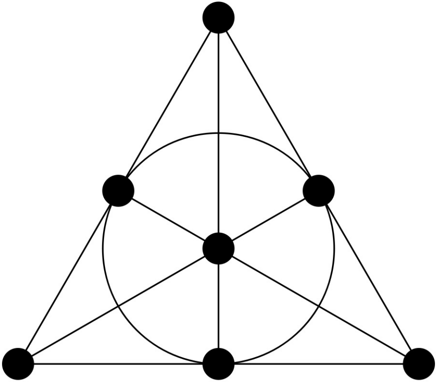
Consequences for finite projective planes:

1. Any two lines of $\mathbb{P}^2$ have the same number of points. We denote this number by $d + 1$, and say that the plane has order d.
2. Through every point in $\mathbb{P}^2$ there pass $d + 1$ lines.
3. There are $d^2 + d + 1$ points and $d^2 + d + 1$ lines in $\mathbb{P}^2$.
4. This reflects the general notion of duality.

Example. The Fano projective plane (picture from Wikipedia):

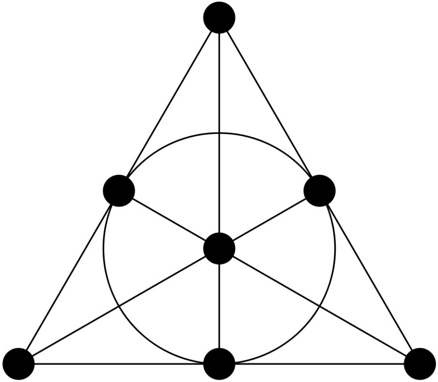


Example. The Fano projective plane (picture from Wikipedia):



This is a plane of order 2. There are exactly $7 = 2^2 + 2 + 1$ points.

Example. The Fano projective plane (picture from Wikipedia):



This is a plane of order 2. There are exactly $7 = 2^2 + 2 + 1$ points. The lines are all subsets of three points, as indicated (there are 7 of them).

Question. Consider given a pair $(\mathfrak{P}, \mathfrak{L})$, where $\mathfrak{P}$ is the set of points and $\mathfrak{L}$ is a collection of subsets called lines.

How do we recognize if $(\mathfrak{P}, \mathfrak{L})$ is a projective plane? Can we find a necessary and sufficient condition other than checking the axioms?

Question. Consider given a pair $(\mathfrak{P}, \mathfrak{L})$, where $\mathfrak{P}$ is the set of points and $\mathfrak{L}$ is a collection of subsets called lines.

How do we recognize if $(\mathfrak{P}, \mathfrak{L})$ is a projective plane? Can we find a necessary and sufficient condition other than checking the axioms?

And "how many" projective planes are there out there?

Question. Consider given a pair $(\mathfrak{P}, \mathfrak{L})$, where $\mathfrak{P}$ is the set of points and $\mathfrak{L}$ is a collection of subsets called lines.

How do we recognize if $(\mathfrak{P}, \mathfrak{L})$ is a projective plane? Can we find a necessary and sufficient condition other than checking the axioms?

And "how many" projective planes are there out there?

Here is one approach from combinatorics: Pure *O*-sequences.

The study of finite projective planes can be approached through algebraic combinatorics.

Pure O-sequences

The study of finite projective planes can be approached through algebraic combinatorics.

One way that this is realized is through the notion of the pure O-sequence corresponding to our projective plane of order d.

Pure O-sequences

The study of finite projective planes can be approached through algebraic combinatorics.

One way that this is realized is through the notion of the pure O-sequence corresponding to our projective plane of order d.

First let's define pure O-sequences in general (independently of projective planes), then say which ones correspond to finite projective planes.

Let $\mathcal{M}_e = \{m_1, \dots, m_r\}$ be a set of distinct monomials of the same degree e (not necessarily squarefree in general) in some polynomial ring $k[x_1, \dots, x_n]$.

Let $\mathcal{M}_e = \{m_1, \ldots, m_r\}$ be a set of distinct monomials of the same degree e (not necessarily squarefree in general) in some polynomial ring $k[x_1, \ldots, x_n]$.

For each $1 \leq i \leq e$, let $\mathcal{M}_i$ be the monomials of degree i that divide at least one of $m_1, \ldots, m_r$.

Let $\mathcal{M}_e = \{m_1, \ldots, m_r\}$ be a set of distinct monomials of the same degree e (not necessarily squarefree in general) in some polynomial ring $k[x_1, \ldots, x_n]$.

For each $1 \leq i \leq e$, let $\mathcal{M}_i$ be the monomials of degree i that divide at least one of $m_1, \ldots, m_r$.

The pure O-sequence associated to $\mathcal{M}_e$ is the sequence

$$(1, |\mathcal{M}_1|, \ldots, |\mathcal{M}_{e-1}|, |\mathcal{M}_e|).$$

Example. Let $R = k[x, y, z]$ and $e = 3$. Let

$$\mathcal{M}_3 = \{x^3, xyz, x^2y, y^3\}.$$

Example. Let $R = k[x, y, z]$ and $e = 3$. Let

$$\mathcal{M}_3 = \{x^3, xyz, x^2y, y^3\}.$$

Then

$$\mathcal{M}_2 = \{x^2, xy, xz, yz, y^2\}$$

Example. Let $R = k[x, y, z]$ and $e = 3$. Let

$$\mathcal{M}_3 = \{x^3, xyz, x^2y, y^3\}.$$

Then

$$\mathcal{M}_2 = \{x^2, xy, xz, yz, y^2\}$$

$$\mathcal{M}_1 = \{x, y, z\}$$

Example. Let $R = k[x, y, z]$ and $e = 3$. Let

$$\mathcal{M}_3 = \{x^3, xyz, x^2y, y^3\}.$$

Then

$$\mathcal{M}_2 = \{x^2, xy, xz, yz, y^2\}$$

$$\mathcal{M}_1 = \{x, y, z\}$$

leading to the pure O-sequence

$$(1, 3, 5, 4).$$

Remark. Algebraic point of view:

For each degree, collect the monomials not in the corresponding list $\mathcal{M}_i$.

Remark. Algebraic point of view:

For each degree, collect the monomials not in the corresponding list $\mathcal{M}_i$.

Fact: Together these generate a monomial ideal, I (i.e. an ideal generated by monomials), whose quotient, R/I, has Hilbert function equal to the pure O-sequence.

Remark. Algebraic point of view:

For each degree, collect the monomials not in the corresponding list $\mathcal{M}_i$.

Fact: Together these generate a monomial ideal, I (i.e. an ideal generated by monomials), whose quotient, R/I, has Hilbert function equal to the pure O-sequence.

(We'll come back to ideals, quotients and Hilbert functions more carefully. This remark is just for completeness now.)

Example (cont).

$$\mathcal{M}_3 = \{x^3, xyz, x^2y, y^3\}$$

$$\mathcal{M}_2 = \{x^2, xy, xz, yz, y^2\}$$

$$\mathcal{M}_1 = \{x, y, z\}$$

Example (cont).

$$\begin{aligned} \mathcal{M}_3 &= \{x^3, xyz, x^2y, y^3\} \\ \mathcal{M}_2 &= \{x^2, xy, xz, yz, y^2\} \\ \mathcal{M}_1 &= \{x, y, z\} \end{aligned}$$

Then

$$I = \langle z^2, x^2z, xy^2, xz^2, y^2z, yz^2, z^3\rangle = \langle z^2, x^2z, xy^2, y^2z\rangle.$$

Again, we'll come back to this.

Example (cont).

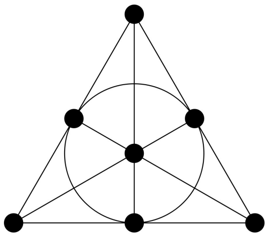
$$\begin{aligned} \mathcal{M}_3 &= \{x^3, xyz, x^2y, y^3\} \\ \mathcal{M}_2 &= \{x^2, xy, xz, yz, y^2\} \\ \mathcal{M}_1 &= \{x, y, z\} \end{aligned}$$

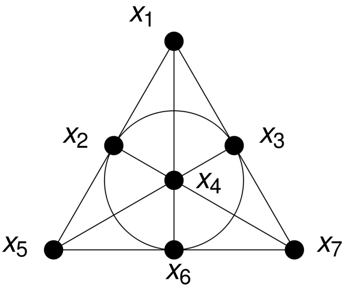
Then

$$I = \langle z^2, x^2z, xy^2, xz^2, y^2z, yz^2, z^3 \rangle = \langle z^2, x^2z, xy^2, y^2z \rangle.$$

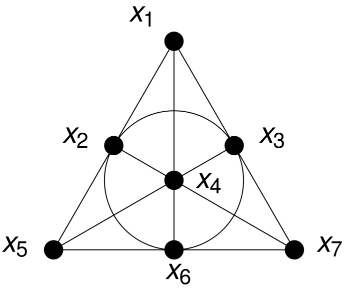
Again, we'll come back to this.

Let's see how we can associate a pure O-sequence to a finite projective plane, using the Fano plane as an example.



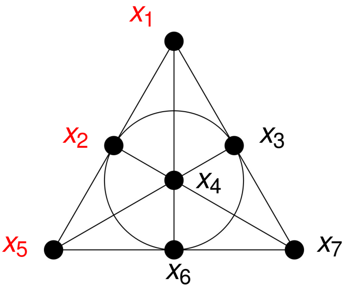


1. Label each point with a different variable. Recall that the plane has $q = 2^2 + 2 + 1 = 7$ points and 7 lines, and order $d = 2$.



1. Label each point with a different variable. Recall that the plane has $q = 2^2 + 2 + 1 = 7$ points and 7 lines, and order $d = 2$.

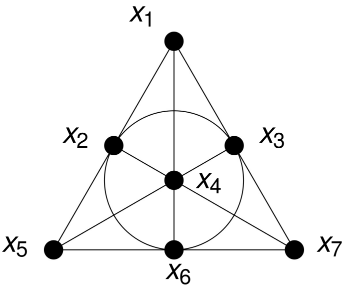
2. Collect and count the (squarefree) monomials of degree $d + 1 = 3$ corresponding to points on a line:



1. Label each point with a different variable. Recall that the plane has $q = 2^2 + 2 + 1 = 7$ points and 7 lines, and order $d = 2$.

2. Collect and count the (squarefree) monomials of degree $d + 1 = 3$ corresponding to points on a line:

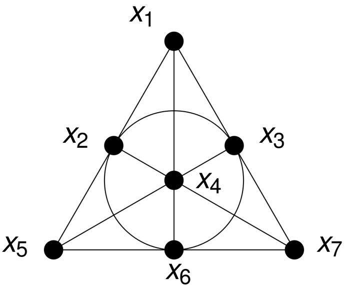
$x_1 x_2 x_5$



1. Label each point with a different variable. Recall that the plane has $q = 2^2 + 2 + 1 = 7$ points and 7 lines, and order $d = 2$.

2. Collect and count the (squarefree) monomials of degree $d + 1 = 3$ corresponding to points on a line:

$$x_1x_2x_5,\ x_1x_4x_6,\ x_1x_3x_7,\ x_2x_4x_7,\ x_2x_3x_6,\ x_3x_4x_5,\ x_5x_6x_7$$



1. Label each point with a different variable. Recall that the plane has $q = 2^2 + 2 + 1 = 7$ points and 7 lines, and order $d = 2$.

2. Collect and count the (squarefree) monomials of degree $d + 1 = 3$ corresponding to points on a line:

$$x_1x_2x_5,\ x_1x_4x_6,\ x_1x_3x_7,\ x_2x_4x_7,\ x_2x_3x_6,\ x_3x_4x_5,\ x_5x_6x_7$$

3. These monomials will be our set $\mathcal{M}_3$ generating our pure *O*-sequence. Note $|\mathcal{M}_3| = 7$ (there are 7 lines).

3. These monomials will be our set $\mathcal{M}_3$ generating our pure O-sequence. Note $|\mathcal{M}_3| = 7$ (there are 7 lines).

4. Since two points lie on exactly one line, we get

$$|\mathcal{M}_2| = 7 \cdot \binom{3}{2} = 7 \cdot 3 = 21$$

3. These monomials will be our set $\mathcal{M}_3$ generating our pure O-sequence. Note $|\mathcal{M}_3| = 7$ (there are 7 lines).

4. Since two points lie on exactly one line, we get

$$|\mathcal{M}_2| = 7 \cdot \binom{3}{2} = 7 \cdot 3 = 21 = \binom{7}{2}.$$

3. These monomials will be our set $\mathcal{M}_3$ generating our pure O-sequence. Note $|\mathcal{M}_3| = 7$ (there are 7 lines).

4. Since two points lie on exactly one line, we get

$$|\mathcal{M}_2| = 7 \cdot \binom{3}{2} = 7 \cdot 3 = 21 = \binom{7}{2}.$$

5. Since there are 7 points (hence 7 variables), we get

$$|\mathcal{M}_1| = 7.$$

3. These monomials will be our set $\mathcal{M}_3$ generating our pure O-sequence. Note $|\mathcal{M}_3| = 7$ (there are 7 lines).

4. Since two points lie on exactly one line, we get

$$|\mathcal{M}_2| = 7 \cdot \binom{3}{2} = 7 \cdot 3 = 21 = \binom{7}{2}.$$

5. Since there are 7 points (hence 7 variables), we get

$$|\mathcal{M}_1| = 7.$$

This leads to the pure O-sequence

$$(1, 7, 21, 7).$$

This is the pure O-sequence associated to the Fano plane.

Theorem. *A projective plane of order d exists if and only if*

$$\left(1, q, q\binom{d+1}{2}, q\binom{d+1}{3}, \ldots, q\binom{d+1}{d}, q\right).$$

is a pure O-sequence, where $q = d^2 + d + 1$, $d \geq 2$.

Theorem. *A projective plane of order d exists if and only if*

$$\left(1, q, q\binom{d+1}{2}, q\binom{d+1}{3}, \ldots, q\binom{d+1}{d}, q\right).$$

is a pure O-sequence, where $q = d^2 + d + 1$, $d \geq 2$.

Note again: the monomials generating such a sequence must be squarefree.

Theorem. *A projective plane of order d exists if and only if*

$$\left(1, q, q\binom{d+1}{2}, q\binom{d+1}{3}, \ldots, q\binom{d+1}{d}, q\right).$$

is a pure O-sequence, where $q = d^2 + d + 1$, $d \geq 2$.

Note again: the monomials generating such a sequence must be squarefree.

Easy exercise:

$$q\binom{d+1}{2} = \binom{q}{2}.$$

Theorem. *A projective plane of order d exists if and only if*

$$\left(1, q, q\binom{d+1}{2}, q\binom{d+1}{3}, \dots, q\binom{d+1}{d}, q\right).$$

is a pure O-sequence, where $q = d^2 + d + 1$, $d \geq 2$.

Note again: the monomials generating such a sequence must be squarefree.

Easy exercise:

$$q\binom{d+1}{2} = \binom{q}{2}.$$

The above theorem is not a trivial argument, although some of our facts are immediate (q points, q lines, ...).

This provides an algebraic approach to finite projective planes.

See for instance

D. Cook II, J.M., U. Nagel and F. Zanello, *An algebraic approach to finite projective planes*, Journal of Algebraic Combinatorics **43** (2016), 495–519.

This provides an algebraic approach to finite projective planes.

See for instance

D. Cook II, J.M., U. Nagel and F. Zanello, *An algebraic approach to finite projective planes*, Journal of Algebraic Combinatorics **43** (2016), 495–519.

We described algebraic properties of algebras associated to finite projective planes, obtained as above.

Some of these properties are related to the characteristic of the field defining the polynomial ring in which we place our monomials.

Our next goal is to realize our pure O-sequences as Hilbert functions, and then move on studying Hilbert functions more generally.

Our next goal is to realize our pure O-sequences as Hilbert functions, and then move on studying Hilbert functions more generally.

We need a little bit of background. Some of this material is taken from *Commutative Algebra* by Atiyah and Macdonald.

Let $R = k[x_0, x_1, \ldots, x_n]$ be the set of polynomials in the variables $x_0, x_1, \ldots, x_n$ with coefficients in a field k.

Let $R = k[x_0, x_1, \ldots, x_n]$ be the set of polynomials in the variables $x_0, x_1, \ldots, x_n$ with coefficients in a field k.

First of all, R has the structure of a commutative ring with unity.

Let $R = k[x_0, x_1, \ldots, x_n]$ be the set of polynomials in the variables $x_0, x_1, \ldots, x_n$ with coefficients in a field k.

First of all, R has the structure of a commutative ring with unity. Specifically,

- it has two binary operations (you can add polynomials and you can multiply polynomials);
- $(R, +)$ is an abelian group;
- multiplication is associative;
- the distributive properties hold;
- multiplication is commutative;
- the polynomial 1 is the multiplicative identity element.

An ideal $I \subset R$ is a subset of R for which

- $(I, +) \subset (R, +)$ is an additive subgroup;
- if $f \in I$ and $h \in R$ then $hf \in I$.

An ideal $I \subset R$ is a subset of R for which

- $(I, +) \subset (R, +)$ is an additive subgroup;
- if $f \in I$ and $h \in R$ then $hf \in I$.

In particular, $(I, +) \subset (R, +)$ is a normal subgroup (since $(R, +)$ is commutative).

An ideal $I \subset R$ is a subset of R for which

- $(I, +) \subset (R, +)$ is an additive subgroup;
- if $f \in I$ and $h \in R$ then $hf \in I$.

In particular, $(I, +) \subset (R, +)$ is a normal subgroup (since $(R, +)$ is commutative).

Then the quotient group R/I not only has the structure of a group, but in fact it also inherits a ring structure from R.

The elements of R/I are the cosets $f + I$ of I in R.

An ideal $I \subset R$ is a subset of R for which

- $(I, +) \subset (R, +)$ is an additive subgroup;
- if $f \in I$ and $h \in R$ then $hf \in I$.

In particular, $(I, +) \subset (R, +)$ is a normal subgroup (since $(R, +)$ is commutative).

Then the quotient group R/I not only has the structure of a group, but in fact it also inherits a ring structure from R.

The elements of R/I are the cosets $f + I$ of I in R.

Multiplication is defined by $(f + I) \cdot (g + I) = fg + I$.

Facts:

- The mapping $\phi : R \to R/I$ given by $\phi(f) = f + I$ is a surjective ring homomorphism.

Facts:

- The mapping $\phi : R \to R/I$ given by $\phi(f) = f + I$ is a surjective ring homomorphism.

- There is a one-to-one order-preserving correspondence between the ideals J of R which contain I and the ideals $\overline{J}$ of R/I, given by $J = \phi^{-1}(\overline{J})$.

Now let's look at the polynomial ring $R = k[x_0, x_1, \dots, x_n]$.

Note that any polynomial can be decomposed in a unique way as the sum of terms of the same degree. E.g.

$$f = x^4y + 2xyz + 3y + 4z^2 + 5y^5 + 6x + 7x^2y + 8y^2z^2 + 9x^4$$

$$= (x^4y + 5y^5) + (8y^2z^2 + 9x^4) + (2xyz + 7x^2y) + 4z^2 + (6x + 3y)$$

The parts in parentheses are the homogeneous components of f.

Now let's look at the polynomial ring $R = k[x_0, x_1, \dots, x_n]$.

Note that any polynomial can be decomposed in a unique way as the sum of terms of the same degree. E.g.

$$f = x^4y + 2xyz + 3y + 4z^2 + 5y^5 + 6x + 7x^2y + 8y^2z^2 + 9x^4$$

$$= (x^4y + 5y^5) + (8y^2z^2 + 9x^4) + (2xyz + 7x^2y) + 4z^2 + (6x + 3y)$$

The parts in parentheses are the homogeneous components of f.

In general, a polynomial is homogeneous if the monomials in each term (ignoring the coefficients) all have the same degree.

Now let's look at the polynomial ring $R = k[x_0, x_1, \ldots, x_n]$.

Note that any polynomial can be decomposed in a unique way as the sum of terms of the same degree. E.g.

$$f = x^4y + 2xyz + 3y + 4z^2 + 5y^5 + 6x + 7x^2y + 8y^2z^2 + 9x^4$$

$$= (x^4y + 5y^5) + (8y^2z^2 + 9x^4) + (2xyz + 7x^2y) + 4z^2 + (6x + 3y)$$

The parts in parentheses are the homogeneous components of f.

In general, a polynomial is homogeneous if the monomials in each term (ignoring the coefficients) all have the same degree.

A homogeneous polynomial is sometimes called a form.

The polynomial ring R is an example of a graded ring.

The polynomial ring R is an example of a graded ring.

Specifically, a graded ring consists of

- a ring, A;
- a family $(A_n)_{n \geq 0}$ of subgroups of the additive group of A;

The polynomial ring R is an example of a graded ring.

Specifically, a graded ring consists of

- a ring, A;
- a family $(A_n)_{n \geq 0}$ of subgroups of the additive group of A;
- such that $A = \bigoplus_{t=0}^{\infty} A_t$
- and $A_s A_t \subseteq A_{s+t}$ for all $s, t \geq 0$.

The polynomial ring R is an example of a graded ring.

Specifically, a graded ring consists of

- a ring, A;
- a family $(A_n)_{n\geq 0}$ of subgroups of the additive group of A;
- such that $A = \bigoplus_{t=0}^{\infty} A_t$
- and $A_s A_t \subseteq A_{s+t}$ for all $s, t \geq 0$.

In the case of the polynomial ring R, we have

$$R_t = \{\text{homogeneous polynomials of degree } t\}$$

Notice that R_t is a little more than an additive subgroup of R:

it has the structure of a k-vector space!!!

Notice that R_t is a little more than an additive subgroup of R:

it has the structure of a k-vector space!!!

In particular, if $R = k[x_0, x_1, \ldots, x_n]$ then

$$\dim_k R_t = \binom{n+t}{n}$$

with basis given by the monomials of degree t (exercise).

Notice that R_t is a little more than an additive subgroup of R:

it has the structure of a k-vector space!!!

In particular, if $R = k[x_0, x_1, \ldots, x_n]$ then

$$\dim_k R_t = \binom{n+t}{n}$$

with basis given by the monomials of degree t (exercise).

Example. $R = k[x, y, z]$, so $n = 2$. Then the vector space of homogeneous polynomials of degree $t = 3$ has basis

$$x^3, x^2y, x^2z, xy^2, xyz, xz^2, y^3, y^2z, yz^2, z^3$$

and

$$\dim_k R_3 = \binom{2+3}{2} = 10.$$

Now we want to look at graded quotient algebras of R and their Hilbert functions.

We need homogeneous ideals in order to make it work.

Now we want to look at graded quotient algebras of R and their Hilbert functions.

We need homogeneous ideals in order to make it work.

Definition/Proposition. (See for instance Cox-Little-O'Shea; this is also in the exercises for today's lecture.)

An ideal $I \subset R = k[x_0, x_1, \ldots, x_n]$ is homogeneous if either of the following equivalent conditions holds.

Now we want to look at graded quotient algebras of R and their Hilbert functions.

We need homogeneous ideals in order to make it work.

Definition/Proposition. (See for instance Cox-Little-O'Shea; this is also in the exercises for today's lecture.)

An ideal $I \subset R = k[x_0, x_1, \ldots, x_n]$ is homogeneous if either of the following equivalent conditions holds.

- *If $f \in I$ then the homogeneous components of f are also in I;*

Now we want to look at graded quotient algebras of R and their Hilbert functions.

We need homogeneous ideals in order to make it work.

Definition/Proposition. (See for instance Cox-Little-O'Shea; this is also in the exercises for today's lecture.)

An ideal $I \subset R = k[x_0, x_1, \ldots, x_n]$ is homogeneous if either of the following equivalent conditions holds.

- *If $f \in I$ then the homogeneous components of f are also in I;*
- *the ideal I has a generating set consisting of homogeneous polynomials.*

Theorem. *Assume $I \subset R = k[x_0, x_1, \dots, x_n]$ is a homogeneous ideal.*

Theorem. *Assume* $I \subset R = k[x_0, x_1, \ldots, x_n]$ *is a homogeneous ideal. Then:*

1. *We also have a decomposition* $I = \bigoplus_{t \geq 0} I_t$*, where* I_t *is a (finite dimensional) k-vector subspace of* R_t*;*

Theorem. *Assume $I \subset R = k[x_0, x_1, \ldots, x_n]$ is a homogeneous ideal. Then:*

1. *We also have a decomposition $I = \bigoplus_{t \geq 0} I_t$, where I_t is a (finite dimensional) k-vector subspace of R_t;*
2. *In this situation the quotient ring R/I is a standard graded k-algebra:*

$$R/I = \bigoplus_{t \geq 0} [R/I]_t.$$

Theorem. *Assume $I \subset R = k[x_0, x_1, \ldots, x_n]$ is a homogeneous ideal. Then:*

1. *We also have a decomposition $I = \bigoplus_{t \geq 0} I_t$, where I_t is a (finite dimensional) k-vector subspace of R_t;*
2. *In this situation the quotient ring R/I is a standard graded k-algebra:*
$$R/I = \bigoplus_{t \geq 0} [R/I]_t.$$
3. *We have* $\dim [R/I]_t = \dim R_t - \dim I_t$.

Definition. If $A = \bigoplus_t A_t$ is a standard graded k-algebra then

$$h_A(t) = \dim_k A_t$$

is the Hilbert function of A.

Definition. If $A = \bigoplus_t A_t$ is a standard graded k-algebra then

$$h_A(t) = \dim_k A_t$$

is the Hilbert function of A.

Example. If $n = 3$, so $R = k[x_0, x_1, x_2, x_3]$, then $h_R(t)$ is the sequence

$$\binom{0+3}{3}, \binom{1+3}{3}, \binom{2+3}{3}, \binom{3+3}{3}, \binom{4+3}{3}, \binom{5+3}{3}, \dots, \binom{t+3}{3}, \dots$$

$$= 1,\ 4,\ 10,\ 20,\ 35,\ 56,\ \dots.$$

We'll have examples of graded quotients of R in a minute.

Monomial ideals, and pure $\mathcal{O}$-sequences revisited

A monomial is obviously homogeneous (since “all terms” of the monomial have the same degree).

So a monomial ideal is always a homogeneous ideal!

Monomial ideals, and pure O-sequences revisited

A monomial is obviously homogeneous (since "all terms" of the monomial have the same degree).

So a monomial ideal is always a homogeneous ideal!

Hence if $I = \bigoplus_{t \geq 0} I_t$ is a monomial ideal then R/I has the structure of a graded k-algebra.

Monomial ideals, and pure O-sequences revisited

A monomial is obviously homogeneous (since “all terms” of the monomial have the same degree).

So a monomial ideal is always a homogeneous ideal!

Hence if $I = \bigoplus_{t \geq 0} I_t$ is a monomial ideal then R/I has the structure of a graded k-algebra.

Let $m_1, \ldots, m_r$ be a basis for I_t. Then the monomials of degree t not in this list can be taken as a basis for $[R/I]_t$, and it computes the Hilbert function $h_{R/I}(t)$.

Monomial ideals, and pure O-sequences revisited

A monomial is obviously homogeneous (since "all terms" of the monomial have the same degree).

So a monomial ideal is always a homogeneous ideal!

Hence if $I = \bigoplus_{t \geq 0} I_t$ is a monomial ideal then R/I has the structure of a graded k-algebra.

Let $m_1, \dots, m_r$ be a basis for I_t. Then the monomials of degree t not in this list can be taken as a basis for $[R/I]_t$, and it computes the Hilbert function $h_{R/I}(t)$.

As promised, this means a pure O-sequence is the Hilbert function of a suitable monomial ideal.

Example. Let $R = k[x, y, z]$ and $e = 3$. Let

$$\begin{aligned}
\mathcal{M}_3 &= \{x^3, xyz, x^2y, y^3\} \\
\mathcal{M}_2 &= \{x^2, xy, xz, yz, y^2\} \\
\mathcal{M}_1 &= \{x, y, z\}
\end{aligned}$$

Example. Let $R = k[x,y,z]$ and $e = 3$. Let

$$\begin{aligned} \mathcal{M}_3 &= \{x^3, xyz, x^2y, y^3\} \\ \mathcal{M}_2 &= \{x^2, xy, xz, yz, y^2\} \\ \mathcal{M}_1 &= \{x, y, z\} \end{aligned}$$

Then

$$I = \langle z^2, x^2z, xy^2, xz^2, y^2z, yz^2, z^3\rangle = \langle z^2, x^2z, xy^2, y^2z\rangle.$$

$\{h_{R/I}(t) \mid t \geq 0\}$ is the pure O-sequence $(1,3,5,4)$.

Macaulay's theorem

Question. What are all the possible Hilbert functions of standard graded k-algebras $k[x_0, \ldots, x_n]/I$?

Macaulay's theorem

Question. What are all the possible Hilbert functions of standard graded k-algebras $k[x_0, \ldots, x_n]/I$?

Note we are really talking about all standard graded k-algebras, not just monomial k-algebras.

Macaulay's theorem

Question. What are all the possible Hilbert functions of standard graded k-algebras $k[x_0, \dots, x_n]/I$?

Note we are really talking about all standard graded k-algebras, not just monomial k-algebras.

The amazing fact is that this question actually has a clean answer! (See Bruns-Herzog "Cohen-Macaulay Rings" for proofs.)

We need a little notation.

Definition. A sequence $(1, h_1, h_2, \dots)$ (possibly infinite) is an $\mathcal{O}$-sequence if it is the Hilbert function of some standard graded algebra R/I.

Definition. A sequence $(1, h_1, h_2, \dots)$ (possibly infinite) is an *O-sequence* if it is the Hilbert function of some standard graded algebra R/I.

Question (rephrased): What are all the possible O-sequences for standard graded k-algebras?

Definition. A sequence $(1, h_1, h_2, \dots)$ (possibly infinite) is an *O-sequence* if it is the Hilbert function of some standard graded algebra R/I.

Question (rephrased): What are all the possible O-sequences for standard graded k-algebras?

Definition Let m and i be positive integers. The *i-binomial expansion of m* is the expression

$$m = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + ... + \binom{m_j}{j},$$

where $m_i > m_{i-1} > ... > m_j \geq j \geq 1$.

Such an expansion always exists and is unique.

Example. $m = 20$, $i = 4$. Then

$$20 \quad =$$

Example. $m = 20$, $i = 4$. Then

$$20 = \binom{}{4}$$

Example. $m = 20$, $i = 4$. Then

$$20 = \binom{6}{4} +$$

$$15$$

Example. $m = 20$, $i = 4$. Then

$$20 = \underset{15}{\binom{6}{4}} + \binom{\ }{3}$$

Example. $m = 20$, $i = 4$. Then

$$
\begin{array}{ccccccc}
20 & = & \binom{6}{4} & + & \binom{4}{3} & + \\
 & & 15 & + & 4 &
\end{array}
$$

Example. $m = 20$, $i = 4$. Then

$$20 = \binom{6}{4} + \binom{4}{3} + \binom{\ }{2}$$

$$15 + 4$$

Example. $m = 20$, $i = 4$. Then

$$20 = \binom{6}{4} + \binom{4}{3} + \binom{2}{2}$$

$$15 + 4 + 1$$

Example. $m = 20$, $i = 4$. Then

$$20 = \binom{6}{4} + \binom{4}{3} + \binom{2}{2}$$
$$15 + 4 + 1$$

So $m_4 = 6,\ m_3 = 4,\ m_2 = 2$.

Given the *i*-binomial expansion

$$m = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + ... + \binom{m_j}{j}$$

of m we define

$$m^{\langle i \rangle} = \binom{m_i + 1}{i+1} + \binom{m_{i-1} + 1}{i} + ... + \binom{m_j + 1}{j+1},$$

Given the i-binomial expansion

$$m = \binom{m_i}{i} + \binom{m_{i-1}}{i-1} + \dots + \binom{m_j}{j}$$

of m we define

$$m^{\langle i \rangle} = \binom{m_i + 1}{i+1} + \binom{m_{i-1} + 1}{i} + \dots + \binom{m_j + 1}{j+1},$$

Example. If $m = 20$ and $i = 4$ we saw that

$$20 = \binom{6}{4} + \binom{4}{3} + \binom{2}{2}. \quad \text{Hence}$$

$$20^{\langle 4 \rangle} = \binom{7}{5} + \binom{5}{4} + \binom{3}{3} = 21 + 5 + 1 = 27.$$

Macaulay's Theorem. *A sequence*

$$(1, h_1, h_2, \dots)$$

(possibly infinite) is an O-sequence if and only if $h_{j+1} \leq h_j^{\langle j \rangle}$ *for all* $j \geq 1$.

Macaulay's Theorem. *A sequence*

$$(1, h_1, h_2, \dots)$$

(possibly infinite) is an O-sequence if and only if $h_{j+1} \leq h_j^{\langle j \rangle}$ *for all* $j \geq 1$*.*

(Note that this does not involve the number of variables, n.)

Example. The sequence

$$(1, 4, 10, 17, 26, 28)$$

is an O-sequence, but the sequence

$$(1, 4, 10, 17, 27, 28)$$

is not.

Example. The sequence

$$(1, 4, 10, 17, 26, 28)$$

is an O-sequence, but the sequence

$$(1, 4, 10, 17, 27, 28)$$

is not. The issue is the 3-binomial expansion of 17 is

$$17 = \binom{5}{3} + \binom{4}{2} + \binom{1}{1}$$

so

$$17^{\langle 3 \rangle} = \binom{6}{4} + \binom{5}{3} + \binom{2}{2} = 15 + 10 + 1 = 26.$$

Remark. Macaulay's theorem is very simple, but finding a standard k-algebra for a given O-sequence can be very challenging, depending on what you are looking for.

It can involve a lot of geometry. We'll see some of this in the next lecture.

Remark. Macaulay's theorem is very simple, but finding a standard k-algebra for a given O-sequence can be very challenging, depending on what you are looking for.

It can involve a lot of geometry. We'll see some of this in the next lecture.

One approach is via a certain kind of monomial ideal called a lex-segment ideal. Details omitted.