MA 765: Topics in Non-linear Algebra

Taught by Dr. Uwe Nagel

Notes by Narendran

University of Kentucky

Fall 2023

1 Gröbner Basis

Denote by $\leq$ the coordinate wise partial order on $\mathbb{N}_0^n$. $(a_1, \dots, a_n) \leq (b_1, \dots, b_n)$ if $a_i \leq b_i$ for $i \in [n]$.
Divisibility is a partial order on monomials.

Theorem 1.1 (Dicksen's lemma)**.** Every infinite subset of $\mathbb{N}_0^n$ contains elements a, b with $a < b$.

Proof. The proof follows by induction. Let $\mathcal{M} \subset \mathbb{N}_0^n$ be an infinite subset. For any $i \in \mathbb{N}_0$ define $\mathcal{M}$,

$$\mathcal{M}_i = \{a = (a_1, \dots, a_n) \in \mathbb{N}_0^{n-1} \, : \, (a, i) \in \mathcal{M}\}$$

If $\mathcal{M}_i$ is finite, then look at $\bigcup_i \in \mathbb{N}_0$, which has finitely many and atleast one minimal element. Thus there is some $j \in \mathbb{N}$ such that $\bigcup_{i=0}^{j} \mathcal{M}_i$ with $a \in \mathcal{M}_i$ for some $i \leq j$.Hence $(a, i) < (b, k)$.

□

Corollary 1.2. For any $\phi \neq \mathcal{M} \subset \mathbb{N}_0^n$ the set of minimal elemnents wrt $<$ is nonempty and finite.

1.3. Monomial order on $\mathbb{N}_0^n$ is a relation $\prec$ such that

1. If $a \neq b$ then $\prec b$ or $b \prec a$.
2. If $A \prec b$ and $b \prec c$ then $a \prec c$.
3. $(0, \dots, 0) \prec a$ for any $a \in \mathbb{N}_0^n$.
4. $a \prec b$ then $a + c \prec b + c$ for any $c \in \mathbb{N}_0^n$.

First two conditions together imply that $\prec$ is a total order.

Remark 1.4.
1. If $a < b$, then $a \prec b$, i.e., any monomial order refines coordinate wise partial order.
2. Any monomial order on $\mathbb{N}_0^n$ gives total order on monomials in $k[X_n]$

Example 1.5. Lexicographic order: Left most non zero entry of $a - b$ is positive the $a >_{lex} b$.

degree lex order if either $|a| > |b|$ or $|a| = |b|$ and right most entry of $a - b$ is negative.

degree reverse lex order, same as above but right most entry of $a - b$ is negative.

Proposition 1.6. For any monomial order $<$ on $\mathbb{N}_0^n$ with $\phi \neq \mathcal{M} \subset \mathbb{N}_0^n$ has a unique minmial element.

Proof. Dicksen's lemma gives that $\mathcal{M}$ has a finite nom empty set of minmal elements wrt coordinate wise order. The minmal elet of thse wrt $<$ is the desired elemnt. □

1.7. Fix a monomial order $<$ on $k[X_n]$

1. The initial monomial $\mathrm{im}_<(F)$ of $f = \sum c_a x^a$ is the largest monomial wrt $<$ appearing in f with non zero coefficients.
2. The leading term $\mathrm{lt}_<(f) := c_a x^a$ with $x^a = \mathrm{im}(f)$

3. The initial ideal of an ideal I is $\text{im}(I) = \langle \text{im}(f) : f \in I \rangle$.

If G is a generating set for an ideal I then $\langle \text{im}(g) : g \in G \rangle \subset \text{im}(I)$ and this inclusion can be strict.

Proposition 1.8. Let $<$ be a monomial order on $k[X_n]$. Every ideal I has a finite subest $\mathcal{G}$ such that $\text{im}(I) = \langle \text{im}(g) : g \in \mathcal{G} \rangle$.
Any such $\mathcal{G}$ is called a Gröbner Basis of I wrt $<$.

Proof. The set of monomials in $\text{im}(I)$ has a finite and nonempty subset of minmal elements wrt divisibility, say $m_1, \dots, m_s$. Thus $\text{im}(I) = \langle m_1, \dots, m_s \rangle$. Every monomial in $\text{im}(I)$ is the initial monomial of some $f \in I$. hence there exists $f_1 \dots, f_s \in I$ with $\text{im}(f_i) = m_i$. Thus $\{f_i\}$ is a Gröbner basis. □

Theorem 1.9. If $\mathcal{G}$ is a Gröbner basis of I, then $I = \langle \mathcal{G} \rangle$

Note that Hilbert's basis theorem is a simple corollary of this.

Proof. We argue by contradiction. By 1.6, choose $f \in I - \langle \mathcal{G} \rangle$ such that $\text{im}(f)$ is minimal. Call $\text{im}(f) = x^b$. $x^b \in \text{im}(I) = \langle \text{im}(g) : g \in \mathcal{G} \rangle$. There exists $g \in \mathcal{G}$ such that $\text{im}(g) | x^b$, say $x^b = x^c \cdot \text{im}(g)$.
$\text{im}(f = x^c \lambda g) < x^b = \text{im}(f)$ where $\lambda = \text{lt}(f)/x^c\,\text{lt}(g) \in k$. But $f - x^c \lambda g \in I - \langle \mathcal{G} \rangle$, which is a contradiction to the minimality. □

Lemma 1.10. Consider $f, g_1, \dots, g_s \in k[X_n]$, with $g_i \neq 0$. Then for any minmal order $<$, there exists $q_1 \dots, q_s, r \in k[X_n]$ such that

1. $f + \sum_{i=1}^{s} q_i g_i + r$
2. $\text{im}(f) \geq \text{im}(q_i g_i) \forall i$ (note that $\text{im}(f) = \text{im}(q_i g_i)$ for some i)
3. $\text{im}(r)$ is not divisible by $\text{im}(g_i)$ for any i.

We say f reduces to r by $\{g_1, \dots, g_s\}$.

1.11 Division Algorithm. Input: $f, g_1 \dots g_s$
Output: $q_1, \dots q_s, r$ satisfying the properties 1-3.

1. Set $r = 0$, $p = gf, q_1 = \dots = q_s = 0$
2. While $p \neq 0$ do :

   If $\text{im}(g_i)$ divides $\text{im}(p)$ for some $i \in [s]$, then set $q_i = q_i + \frac{lt(p)}{lt(g_i)}$ and $p_i = p - \frac{lt(p)}{lt(g_i)} g_i$
   else set $r = r + \text{lt}(p)$, $p = p - \text{lt}(p)$
3. Return $q_1, \dots, q_s, r$

Example 1.12. Consider Lexicographic ordering with $x > y$ and $f = x^2y + xy^2 + y^2$ and

$g_1 = xy - 1$, $g_2 = y^2 - 1$.

p	$xy-1$	y^2-1	r
$x^2y + xy^2 + y^2 - x^2y + x$	x		
$xy^2 + y^2 + x - xy^2 + y$	y		
$y^2 + x + y - x$			x
$y^2 + y - y^2 + 1$	1		
$y + 1 - y$			y
1			1

Corollary 1.13. Buchberger's criteria Let $\mathcal{G}$ be a finite subset of I. Then $\mathcal{G}$ is a Gröbner basis of I iff each $f \in I$ can be reduced to 0 by $\mathcal{G}$.

Proof. If f reduces to r by $\mathcal{G}$, then $\text{im}(g_i)$ does not divide $\text{im}(r)$, for all i. Howevert $f - r \in \langle \mathcal{G} \rangle$ and $r \in I$ and $\mathcal{G}$ is a Gröbner basis of I. So there exists some $g \in \mathcal{G}$ such that $\text{im}(r)$ is divisible by $\text{im}(g)$, which forces $r = 0$.

Conversely, we have $f = \sum q_i g_i$ with $g_i \in \mathcal{G}$ and $\text{im}(q_i g_i) \leq \text{im}(f)$. Hence equality for some i and so $\text{im}(f) \in \langle \text{im}(g) : g \in \mathcal{G} \rangle$. □

Proposition 1.14. Let $<$ be a monomial order. Then

1. Let B be the set of monomials in $k[X_n] - \text{im}(I)$. Then $\bar{B} \subset k[X_n]/I$ is a k vsp basis.
2. If $\mathcal{G}$ is a Gröbner basis of I, then the remainder of f by $\mathcal{G}$ is unique and does not depnd on the choice of $\mathcal{G}$.

Proof.

1. If $p = \sum \lambda_i m_i \in I$ with $m_i \in B$, then $\text{im}(p) \in \text{im}(I)$, but $\text{im}(p) = \text{im}(m_i) \notin I$. To show $\bar{B}$ spans.$m \in k[X_n]$ such that $\bar{m} \notin \text{span}(\bar{B})$.

   Take $\min\{m\} = m$ where $m \notin B$. So we have $m \in \text{im}(I)$. There exists $f \in I$ such that $\text{im}(f) = m$. So any monomial in $f - \text{lt}(f) + I = f - \lambda m + I$ is in span $(\bar{B})$. So $\lambda m + I = p - f + I \in \text{span}(\bar{B})$. This leads to a contradiction

□

Definition 1.15.

1. For terms $\lambda x^a, \mu x^b \quad (\lambda, \mu \in k)$ denote by

$$\gcd\left(\lambda x^a, \mu x^b\right) = \gcd\left(x^a, x^b\right)$$
$$\text{lcm}\left(\lambda x^a, \mu x^b\right) = \text{lcm}\left(x^a, x^b\right)$$

2. For $0 \neq g$, h $\in k\left[x_n\right]$, their s -polynomial (wrt monomial order $<$)

$$S(g,h) := \frac{\text{lt}(h)}{\gcd(\text{lt}(h), \text{lt}(g))} g = \frac{\text{lt}(g)}{\gcd(\text{lt}(h), \text{lt}(g))} h.$$

1.16. Buchberger's Algorithm for computing Gröbner basis Input: $f_1, \ldots, f_s \in k\left[X_n\right]$ in monomial order.
Output: Gröbner basis $\mathcal{G}$ of $I = \langle f_1, \ldots, f_s \rangle$ wrt $<$.

1. Set $\eta = \langle f_1 \cdots, f_s \rangle$
2. Order the elements of $\mathcal{G}$ as $f_1, \ldots, f_t$
3. For $1 \le i < j \le t$ do: Reduce $S(g_i, g_j)$ to r by g. If $r \neq 0$, then set $\mathcal{G} := \mathcal{G} \cup \{r\}$ and go to step 2 .
4. Return $\mathcal{G}$

Remark 1.17. The algorithm computes a Gröbner basis. It terminate vecause in case $r \neq 0.\, \mathrm{im}(r) \notin \langle \mathrm{im}\,(g_1)\,, \cdots, \mathrm{im}\,(g_t) \rangle$.

1.18. Extension to submodules of finitely generated $k[X_n]$ module So $F = k[X_n]^r = \bigoplus_{i=1}^{r} k[X_n]e_i$.

Monomials in G are of the form $x^a e_i$ and terms are $\lambda x^a e_i$ with $\lambda \in k$.
A monomial order on F is a total order on the monomials satisfying:
If $x^a \neq 1$, then $m_1 < m_2 \implies m_1 < x^a{,}_1 < x^a m_2$, for monomials m_i in F.

Given a monomial order on the polynomial ring $k[X_n]$ and an order on $\{e_i\}$. We obtain a monomial ordering on F by ordering $\mathbb{N}_0^n \times [r]$ or $[r] \times \mathbb{N}_0^r$ lexicographically.

Dicksen's lemma can be extended to monomials in F. We also define im, lt with respect to $<$ analogously. There is also a division algorithm.

Theorem 1.19. 1. Every submodule M of F has finite Gröbner basis and the basis generates M.

2. If B is the set of monomials in $F - \mathrm{im}(M)$, then $\bar{B} \subset F/M$ form a k basis of F/M.

2 Hilbert Functions

Definition 2.1. Let $I \subset k[X_n]$ be a monomial ideal . The Hilbert function of $A = k[X_n]/I$ (or of I) is

$$\begin{aligned} h_A \ :& \mathbb{N}_0 \to \mathbb{Z} \\ a \mapsto & h_A(j) = \dim_k [A]_j \end{aligned}$$

where $[A]_j$ is k vector space of images of polynomials of degree j, from $k[X_n] \to A$.(So $h_A(j)$=number of monomials in $[k[X_n]]_j - I$).

It's generating function is the Hilbert series

$$H_A(z) = \sum_{j \geq 0} h_A(j) z^j$$

Example 2.2.

1. For $I = 0$, we get $h_{k[X_n]}(j) = \binom{n+j-1}{j}$ and so

$$H_{k[X_n]}(z) = \sum_{j \geq 0} \binom{n+j-1}{n-1} z^j = \frac{1}{(1-z)^n}$$

2. If $I = \langle x^a \rangle$, then let $e = \deg(x^a)$.

3.

$$h_{k[X_n]/I}(j) = \begin{cases} h_{k[X_n]}(j) & j < e \\ h_{k[X_n]}(j) - h_{k[X_n]}(j-e) & j \geq e \end{cases}$$

Hence

$$H_{k[X_n]/I} = \frac{1-z^e}{(1-z)^n}$$

Theorem 2.3. For any proper monomial ideal I of $k[X_n]$, the Hilbert series of $A = k[X_n]/I$ is a rational function of the form

$$H_A(z) = \frac{\kappa_A(z)}{(1-z)^d}$$

with $\kappa_A(z) \in \mathbb{Z}[z], \kappa_A(0) = 1, \kappa_A(1) \neq 0, d \in \mathbb{N}$.(this expression is unique.)

The dimension of A is

$$\dim A \ := d$$

and the multiplicity of A (or degree of I) is

$$\deg(I) = \mathcal{H}_A(1) > 0$$

There is a polynomial called Hilbert polynomial p_A of A such that $h_A(j) = p_A(j)$ if $j >> 0$. If $d = \dim A > 0$, then

$$\begin{aligned} p_A(z) =& \frac{\deg(I)}{(d-1)!} z^{d-1} + \text{lower order terms} \\ =& h_0(A)\binom{z+d-1}{d-1} + h_1(A)\binom{z+d-2}{d-2} + \cdots + h_{d-1}(A)\binom{z}{0} \end{aligned}$$

where $h_0(A) = \deg(I)$ and $h_i(A)$ are integers. Note if $p_A(z) \neq 0$ polynomial, then $\deg p_A = d - 1 = \dim A - 1$.

Example 2.4.

$I = 0$, we get $\dim k[X_n] = n$ and the multiplicity of $k[X_n]$ is $1 = \deg I$.

$I = \langle x^a \rangle$ with $\deg x = e$, then $\dim k[X_n]/I = n - 1$ and $\deg(I) = \deg(x^a)$.

Proof of 2.3. Inclusion exclusion principle: $| \bigcup_{i=1}^{s} X_i | = \sum_{\phi \neq T \subset [S]} (-1)^{|T|+1} | X_t |$ where $X_t = \bigcap_{i \in T} X_i$

Let $I = \langle m_1, \ldots, m_s \rangle = I$, where m_i are monomials. Denote by $X_i(j)$ set of degree j monomials in $\langle m_i \rangle \subset k[X_n]$. hence for $T \subset [s]$, $X_T(j) = \bigcap_{i \in T} X_i(j)$ is the set of deg j monomials that are divisible by $m_T = \mathrm{lcm}(m_i)_{i \in T}$. Define $e_t := \deg m_T$. So

$$|X_T(j)| = \begin{cases} 0 & j < e_t \\ \binom{n-1+j-e_T}{n-1} & j \geq e_T \end{cases}$$

Thus

$$\sum_{j \geq 0} |X_T(j)| z^j = \sum_{j \geq e_T} \binom{n-1+j-e_T}{n-1} z^j = \sum_{k \geq 0} \binom{n-1+k}{n-1} z^{k+e_T} = z^{e_T} \frac{1}{(1-z)^n}$$

Since

$$\begin{aligned} h_A(j) &= \binom{n-1+j}{n-1} - \text{number of deg } j \text{ monomials in } I = \langle m_1 \ldots, m_s \rangle \\ &= \binom{n-1+j}{n-1} - | \bigcup_{i \in [j]} X_i | \end{aligned}$$

We get

$$\begin{aligned} H_A(z) = \sum_{j \geq 0} h_A(j) z^j &= \sum_{j \geq 0} \binom{n-1+j}{n-1} z^j + \sum_{T \in [s]} (-1)^{|T|} \sum_{j \geq 0} |X_T(j)| z^j \\ &= \frac{1}{(1-z)^n} + \sum_{T \in [s]} (-1)^T \frac{z^{e_T}}{(1-z)^n} =: \frac{g(z)}{(1-z)^n} \end{aligned}$$

When $g(z) \in \mathbb{Z}[z]$, with $g(0) = 1$ writing $g(z) = (1-z)^v \kappa_A(z)$ with $\kappa_A(z) \in \mathbb{Z}[z]$, suitable $v \in \mathbb{N}$ and $\kappa_A(1) \neq 0, \kappa_A(0) = 1$. Hence $H_A(z) = \frac{\kappa_A(z)}{(1-z)^d}$ where $d = n - v$. Write

$$\kappa_A(z) = \sum_{k=0}^{w} c_k z^k \text{ with } c_k \in \mathbb{Z}$$

$$\sum_{j \geq 0} h_A(j) z^j = \Big(\sum_{k=0}^{w} c_k z^k\Big)\Big(\sum_{l \geq 0} \binom{d-1+l}{d-1} z^l\Big)$$

comparing coefficients in deg $j >> 0$, we get

$$h_A(j) = \sum_{k+l=j} c_k \binom{d-1+l}{d-1} = \sum_{k=0}^{w} c_k \underbrace{\binom{d-1+j-k}{d-1}}_{\substack{\text{polynomial in } j-k \\ \text{variables of deg } d-1}}$$

$$= \underbrace{\left(\sum_{k=0}^{w} c_k\right)}_{\kappa_A(1)} \binom{j}{d-1} + \text{lower order terms}$$

$$=: \; p_A(j) \text{ (Hilbert polynomial)}$$

If $h_A(j) = 0$ whenever $j >> 0$, then by definition $0 = d = \dim A$ and in this case p_A is the zero polynomial. Hence if $d > 0$, then $h_A(j) > 0$ if $j >> 0$ and so the leading coefficient of $p_A(z)$ must be positive, i.e., $\kappa_A(1) > 0$ ☐

Definition 2.5. A monomial order is called degree compatible if

$$\deg(x^a) > \deg(x^b) \implies x^a > x^b$$

for any two monomials.

2.6. For any ideal $I \subset k[X_n]$ and any $t \in \mathbb{Z}$, set

$$I_{\leq t} = \{f \in I \;:\; \deg f \leq t\}$$

It is a k-subspace of $k[X_n]$. Write $\mathrm{Mon}(k[X_n])$ for the set of monomials in $k[X_n]$.

Lemma 2.7. Let $<$ be a degree compatible monomial order. For any ideal $I \subset k[X_n] = S$, one has

$$\dim_k \frac{k[X_n]_{\leq t}}{I_{\leq} t} = \text{number of monomials in } \frac{k[X_n]_{\leq t}}{\mathrm{im}_<(I)}$$
$$= \mid \mathrm{Mon}(k[X_n])_{\leq t} - \mathrm{im}_<(t) \mid$$

Proof. $B := \mathrm{Mon}(k[X_n])_{\leq t} - \mathrm{im}_<(I)$. We claim

$$\bar{B} \subset \frac{k[X_n]_{\leq t}}{I_{\leq t}} \text{ is a } k\text{- basis}$$

$\overline{\mathrm{Mon}(k[X_n]) - \mathrm{im}(I)}$ is a k-basis of $k[X_n] - \mathrm{im}(I)$, by 1.14. $\bar{B}$ spans remainder of any $F \in k[X_n]$ pon dividing by Gröbner basis of I wrt $<$ satisfies $\deg r \leq \deg f$. ☐

For $I \subset k[X_n]$, the affine Hilbert funtion of $A = k[X_n]/I$ is

$$h_A^a : \mathbb{N}_0 \longrightarrow \mathbb{Z}$$
$$j \mapsto h_A^a(j) = \dim_k \frac{k[X_n]_{\leq j}}{I_{\leq j}}$$

Lemma 2.8. For any degree compatible monoial order $<$ on I, one has

$$h_{\frac{k[X_n]}{\mathrm{im}_<(I)}}(j) = h_A^a(j) - h_A^1(j-1)$$

where $A = k[X_n]/I$.

Proof. By definition, we have

$$h_{\frac{k[X_n]}{\mathrm{im}(I)}}(j) = \mid \mathrm{Mon}(k[X_n])_j - \mathrm{im}(I) \mid$$

2.7 $\Longrightarrow$ $h_A^a(j) = \mid \mathrm{Mon}(k[X_n])_{\leq j} - \mathrm{im}(I) \mid$ □

Remark 2.9. If $A \neq 0$, $h_A^a(0) = 1$. Then by 2.8 we have $h_A^a(j) = \sum_{k=0}^{j} h_{k[X_n]/\mathrm{im}(I)}(k)$. It follows that generating function of h_A^a and $h_{\frac{k[X_n]}{\mathrm{im}_<(I)}}$ have analogous properties

2.10. We define dimensin of A,

$$\dim \frac{k[X_n]}{I} := \dim_k \frac{k[X_n]}{\mathrm{im}(I)}$$

and the degree

$$\deg(I) = \deg(\mathrm{im}(I))$$

where $<$ is a degree compatible monomial order.

2.11. Let $G = (G, +)$ be an abelian group. A G-graded ring R is a family of subgroups $([R]_{a \in G}) \leq (R, +)$ such that

1. $R = \oplus_{a \in G}[R]_a$ (as $\mathbb{Z}$-modules)
2. $[R]_a \cdot [R]_b \subset [R]_{a+b}$

The elements of $[R]_a$ are called homogeneous of degree a.

Example 2.12. Fine or $\mathbb{Z}$-grading of $k[X_n]$, where $G = \mathbb{Z}^n$

$$[S]_a = \begin{cases} 0 & \text{if some } a_i < 0 \\ \{\lambda x^a \ : \ \lambda \in k\} & \end{cases}$$

Definition 2.13. $R = G-$graded ring

1. G-graded R-module is an R-module M with a decomposition $([M]_a)_{a \in G}$ such that $M = \oplus_{a \in G}[M]_a$ and $[R]_a \cdot [M]_b \subset [M]_{a+b}$.
2. A G-graded or simply graded submoudle of such a graded M is a graded submodule $N \subset M$ such that
$$[N]_a \subset [M]_a$$

Lemma 2.14. For an arbitrary submodule N of a G graded R-module M the following are equivalent

1. N is a graded submodule
2. N has a generating set consisting of homogeneous elemnents
3. If $m = \sum_{a \in G} m_a$ with $m_a \in [M]_a$, then $m \in N$ iff each $m_a \in N$.
4. M/N is a G-graded R-module with grading $[M/N]_a := \frac{[M]_a + N}{N}$.

Proof. □

Example 2.15. 1. M and N are G-graded, then so is $M \oplus N$ with grading $[M \oplus N]_a := [M]_a \oplus [N]_a$ (as R modules). So if R is G graded, then so is R^n.

2. $I \subset k[X_n]$ is a $\mathbb{Z}^n$ graded submodule if I is a monomial ideal.

3. A $\mathbb{Z}$-graded or homogeneous ideal of $k[X_n]$, is an ideal that has generating set consisting of homogeneous polyonomials. In that case $k[X_n]/I$ is a graded module.

2.16. A homomorphism of G-graded modules or a G-graded homomorphism is a R-module homomorphism $\phi : M \to N$ that is degree preserving, $\phi([M]_a) \subset [N]_a$.

For any $a \in G$ and a G-graded module M, the module $M(a)$ has the same module structure as M, but grading given by

$$[M(a)]_b := [M]_{a+b}$$

$M(a)$ is a degree a shift of M. (Note here that the convention is opposite of that in algebraic topology.)

Example 2.17. 1. Consider $k[X_n]$ with standard grading.

$$\begin{aligned} \phi : k[X_n] &\to k[X_n] \\ f &\mapsto x_1^2 f \end{aligned}$$

is not a graded homomorphism. However define

$$\begin{aligned} \psi : k[X_n](-2) &\to k[X_n] \\ f &\mapsto x_1^2 f \end{aligned}$$

then $f \in k[X_n](-2)$ has degree $\deg f + 2$. So $f \in [k[X_n](-2)]_{\deg f+2}$.

2. For any $a \neq$ in G, $R(a)$ is not a graded ring, (because identity is not in 0 dimension), but it is a graded R-module.

Lemma 2.18. If $\phi : M \to N$ is a homomorphism of graded modules, then $\ker \phi, \mathrm{im}\phi, \mathrm{coker}\phi$ are graded modules.

Proof. $[\ker \phi]_a = \ker \phi \bigcap [M]_a$, and $[\mathrm{im}\phi]_a = \mathrm{im}\phi \bigcap [N]_a$.

□

Example 2.19. 1. If M is a $\mathbb{Z}$ graded module with generators $m_1, \ldots, m_t$ where $d_i = \deg m_i$, then

$$\begin{aligned} \phi : \bigoplus_{i=1}^{t} R(-d_i) &\longrightarrow M \\ \begin{bmatrix} r_1 \\ \vdots \\ r_t \end{bmatrix} &\mapsto \sum_{i=1}^{t} r_i m_i \end{aligned}$$

is a homomorphism of graded R-modules and is surjective.

2. Consider $I = \langle x^3, xy, y^4 \rangle \subset k[x,y] + S$ with standard grading.

$$\phi : S(-3) \oplus S(-2) \oplus S(-4) \to I$$
$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \end{bmatrix} \mapsto f_1 x^3 + f_x y + f_3 y^4$$

$$\ker\phi : \left\langle \begin{bmatrix} y \\ -x^2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ y^3 \\ -x \end{bmatrix} \right\rangle \xleftarrow[\text{graded hom}]{\simeq} S(-4) \oplus S(-5)$$

There exists an exact sequence,

$$0 \to \begin{matrix} S(-4) \\ \oplus \\ S(-5) \end{matrix} \xrightarrow[\begin{bmatrix} y & 0 \\ -x^2 & y^3 \\ 0 & -x \end{bmatrix}]{} \begin{matrix} S(-3) \\ \oplus \\ S(-2) \\ \oplus \\ S(-4) \end{matrix} \xrightarrow[\begin{bmatrix} x^3 & xy & y^4 \end{bmatrix}]{\phi} S \to S/I \to 0$$

Definition 2.20. For any $\mathbb{Z}$ graded module M over $k[X_n]$ its Hilbert function is

$$h_m : \mathbb{Z} \to \mathbb{Z}$$
$$j \mapsto h_m(j) := \dim_k [M]_j$$

assuming $[M]_j$ is finitely generated for all j.

Remark 2.21. For any monomial ideal $I \subset k[X_n]$,2.1 and 2.20 agree.

$$\dim_k [k[X_n]/I]_j = \mid [\mathrm{Mon}(k[X_n])]_j - I \mid$$

Proposition 2.22. For every graded submodule M of a finitely generated free $k[X_n]$ module F and any monomial order $<$ of F,

$$h_{F/M}(j) = \frac{h_F(j)}{\mathrm{im}(M)} \; \forall j \in Z$$

Corollary 2.23. For any finitely generated $k[X_n]$ submodule $m \neq 0$, Hilbert series is of the form

$$H_M(z) := \sum_{j \in Z} h_M(j) z^j$$
$$= \frac{\kappa_M(z) z^t}{(1-z)^d}$$

where $\kappa_M(z) \in \mathbb{Z}[z]$, $\kappa_M(0) \neq 0, \kappa_M(1) > 0, t \in \mathbb{Z}$.

There is a HIlbert polynomial $p_M(z) \in \mathbb{Q}(z)$ such that

$$h_M(j) = p_M(j) \; j >> 0$$

(krull) dimension of M is defined as

$$\dim M = d$$

and the degree is

$$\deg(M) = \kappa_M(1)$$

Proof. Let M be generated by $m_1, \dots, m_t$ of degree $d_1, \dots, d_t$ respectively. Define

$$\begin{aligned} \phi \,:\, \oplus_{i=1}^{t} S(-d_i) &\twoheadrightarrow M \\ f &\mapsto x_1^2 f \end{aligned}$$

is not a graded homomorphism. However define

$$\begin{aligned} \psi \,:\, k[X_n](-2) &\to k[X_n] \\ \begin{bmatrix} f_1 \\ vdots \\ f_t \end{bmatrix} &\mapsto \sum f_i m_i \end{aligned}$$

Set $N = \ker \phi$ and we have a short exct sequence $0 \to N \to F \to M \to 0$ and by rank nullity theorem we have $h_M(j) = h_F(j) - h_N(j)$. S and F have desired Hilbert series which are rational functions. So it is enough to show the same for N, which is same as $h_{F/\operatorname{im}(N)}$.

$\operatorname{im}(N)$ is generated by monomials. So

$$\frac{F}{\operatorname{im}(N)} \cong \bigoplus_{i=1}^{t} \underbrace{\left(\frac{S}{J_i}\right)}_{\substack{\text{has the}\\ \text{desired}\\ \text{properties}}} (-d_i)$$

for monomial ideals J_i. □

Example 2.24. 1. $S = k[X_n], F - \bigoplus_{i=1}^{t} S(-d_i)$. Then

$$H_{S(-d_i)}(z) = \frac{z_i^d}{(1-z)^n}$$

2. Consider $I = \langle x^3, xy, y^4 \rangle \subset k[x,y] + S$ with standard grading. $A = S/I$. We have the exact sequence,

$$0 \to \begin{matrix} S(-4) \\ \oplus \\ S(-5) \end{matrix} \to \begin{matrix} S(-3) \\ \oplus \\ S(-2) \\ \oplus \\ S(-4) \end{matrix} \xrightarrow[\begin{bmatrix} x^3 & xy & y^4 \end{bmatrix}]{\phi} S \to A = S/I \to 0$$

$$\begin{aligned} H_A(z) =& H_S(z) - H_{S(-3)\oplus S(-2)\oplus S(-4)}(z) + H_{S(-4)\oplus S(-5)}(z) \\ =& H_S(z) - H_{S(-3)}(z) - H_{S(-2)}(z) + H_{S(-4)}(z) + H_{S(-5)}(z) - H_{S(-4)}(z) \\ =& \frac{1 - z^3 - z^2 + z^5}{(1-z)^2} \\ =& 1 + 3z + 2z^2 + z^3 \end{aligned}$$

So $\dim A = 0$ and $\deg M = 6$ (polyonomial evaluated at 1).

Lemma 2.25. Let $d \in N$. Every $a \in \mathbb{N}$ admits a unique presentation of the form

$$a = \binom{k_d}{d} + \binom{k_{d-1}}{d-1} + \cdots + \binom{k_s}{s}$$

with integers $k_d > k_{d-1} \cdots > k_s$. It is called the d-Macaulay presentation of a.

Example 2.26. For $d = 3$ and $a = 12$, we have

$$12 = \binom{5}{3} + \binom{2}{2} + \binom{1}{1}$$

Definition 2.27. If $a > 0$ with d-Macaulay presentation

$$a = \binom{k_d}{d} + \binom{k_{d-1}}{d-1} + \cdots + \binom{k_s}{s}$$

set

$$a^{\langle d \rangle} = \binom{k_{d+1}}{d+1} + \binom{k_d}{d} + \cdots + \binom{k_{s+1}}{s+1}$$

Example 2.28. $12^{\langle 3 \rangle} = 17$

Theorem 2.29 (Macaulay). Let $h : \mathbb{N}_0 \to \mathbb{Z}$, the following are equivalent,

1. There is some $n \in \mathbb{N}_0$ and some homogeneous ideal $I \subset k[X_n]$ such that Hilbert function of $A = k[X_n]/I$ is h.
2. There is a monomial ideal (Lexicographic ideal) $I \subset k[X_n]$ with $n = h(1)$ such that Hilbert function of A is h.
3. $h(0) = 1$ and

   $$h(j+1) \leq h(j)^{\langle j \rangle} \text{ if } j > 0$$

   Moreover for every graded k-algebra A, one has

   $$h_A(j+1) = h_A(j)^{\langle j \rangle} \text{ if } j >> 0$$

Example 2.30.

j	0	1	2	3	4	5	6
$\tilde{h}$	1	4	10	12	18	18	$\cdots$
h	1	4	10	12	17	17	$\cdots$

$\tilde{h}$ is not a possible Hilbert function because $12^{\langle 3 \rangle} = 17$. While h is a possible Hilbert function.

3 Ideals and Schemes

3.1 Affine case

Definition 3.1. A ring R is reduced if $r^n = 0$ for some $n \in \mathbb{N}$ implies $r = 0$.

Lemma 3.2. Considere a reduced ring R and an ideal I of R. Then R/I is reduced iff $I = \sqrt{I}$.

Hilbert's Nullstellensatz gives bijection if $k = \bar{k}$. Let $S = k[x_1, \dots, x_n]$.

$$\left\{ \begin{matrix} \text{Subvarieties of} \\ \mathbb{A}^n_k \end{matrix} \right\} \underset{Z}{\overset{I}{\leftrightarrows}} \left\{ \begin{matrix} \text{Radical Ideals of} \\ S \end{matrix} \right\} \leftrightarrows \left\{ \begin{matrix} \text{Reduced factor} \\ \text{rings of } S \end{matrix} \right\}$$

$$J \mapsto S/J$$

$$\ker(S \to A) \leftarrow A$$

Definition 3.3. The geometric object X associated to an ideal $J \subset S$ is called an affine (sub) scheme of $\mathbb{A}^n_k$. $I_X := J$ is called the defining ideal of X and S/J is called co-ordinate ring. $X = \text{spec}(S/J)$ to denote the scheme X. The reduced subscheme of X is $X_{red} = \text{spec}(S/\sqrt{J})$. It is also called the *support* of X.

Remark 3.4.

1. Definition 3.3 is a special case of an affine scheme. $\text{Spec}(S/J)$ is the set of prime ideals of S/J endowed with Zariski topology where closed sets are of the form $V(p)$ where p is a prime in S containing J.
2. If $k = \bar{k}$, then the points of $X = \text{Spec}(k[X_n]/\sqrt{J}) \subset \mathbb{A}^n_k$ are the points of $X_{red} = Z(J) = Z(\sqrt{J})$. (The scheme X captures more information, for example multiplicities of the common zeroes)

Example 3.5. For any $j \in \mathbb{N}$ the scheme $Y_j \subset \mathbb{A}^n$ defined by $(x_1, \dots, x_n)^j$ is supported at the point $(0, \dots, 0)$ i.e. $(Y_j)_{red} = \{(0, \dots, 0)\}$. Sometimes Y_j is called a *fat point*.

Definition 3.6. The dimension of $Y = \text{Spec}(k[X_n]/J)$ is $\dim Y = \dim k[X_n]/J$ (as defined using Hilbert series 2.3)

Example 3.7. $\dim \text{Spec} \frac{k[X_n]}{(x_1,\dots,x_n)^j} = 0 \quad \forall j$

Definition 3.8. Let $X, Y \subset \mathbb{A}^n$ be subschemes of $\mathbb{A}^n$. Then X is called a subscheme of Y, if $I_Y \subset I_X$. In symbols $X \subset Y$.

The intersection $X \cap Y$ is the scheme defined by $I_X + I_Y$ and the union $X \cup Y$ is defined by $I_X \cap I_Y$.

Example 3.9. Continuing with the notation used in 3.5, we have $Y_1 \subsetneq Y_2 \subsetneq \cdots$, but $Y_2 \not\subseteq \text{Spec}(\underbrace{\frac{k[X_n]}{(x_2, \dots, x_n)}}_{\text{line}})$ ("fat point sticks out of line")

Theorem 3.10 (Primary decomposition theorem).

Example 3.11. An affine scheme $Y \subset \mathbb{A}^n$ is irreducible if for any subschemes $Y_1, Y_2 \subset Y$ with $Y_1 \cup Y_2 = Y$ either $Y = Y_1$ or $Y = Y_2$ or $Y_{red} = (Y_1)_{red} = (Y_2)_{red}$

Lemma 3.12.
1. Y is irreducible iff I_Y is primary.
2. Y is irreducible and reduced iff I_Y is a primary ideal.

3.13.
1. The fat points Y_j in 3.5 are irreducible but not reduced if $j \geq 2$
2. A line Y is defined by $I_Y = \langle l_1, \ldots, l_{n-1} \rangle$, where l_i are linear independent polynomials in $k[X_n]$. Any line is reduced and irreducible.

Corollary 3.14. Every affine scheme is a finite union of irreducible schemes

3.2 Projective Schemes

3.15 Notation. $m = \langle x_0, \ldots, x_n \rangle \subset k[x_0, \ldots, x_n] \subset S$.

$J \subsetneq S$ is a homogeneous ideal or equivalently $J \subset m$

If $k = \bar{k}$ we have bijections

$$\left\{ \begin{array}{c} V \subset \mathbb{P}^n \\ \text{projective} \\ \text{variety} \end{array} \right\} \underset{Z}{\overset{I}{\leftrightarrows}} \left\{ \begin{array}{c} \text{homogeneous} \\ \text{Radical Ideals} \\ J \subset m \end{array} \right\} \leftrightarrows \left\{ \begin{array}{c} \text{Reduced graded} \\ \text{quotient} \\ \text{rings of } S \end{array} \right\}$$

Definition 3.16. Let $\mathfrak{p}$ be a prime ideal. A $\mathfrak{p}$-primary ideal $\mathfrak{q}$ is a primary ideal $\mathfrak{q}$ with $\sqrt{\mathfrak{q}} = p$

Lemma 3.17. A homogeneous ideal $J \subset m$ is $m-$ primary iff $\sqrt{J} = m$.

Definition 3.18. The saturation of a homogeneous ideal J is the ideal

$$J^{\text{sat}} := \bigcup_{n \geq 1} (J : m^k) \supset J$$

J is saturated if $J = J^{\text{sat}}$.

Lemma 3.19. Let $J \subset m$ be homogeneous. TFAE

1. J is saturated
2. m is not an associated prime ideal of S/J.
3. There is some homogeneous $f \in S$ of positive degree such that $\bar{f} \in S/J$ is a non-zero divisor equivalent to $(J : f) = J$.

Remark 3.20.
1. If $J = q_1 \cap q_2 \cap \cdots \cap q_s$ is a minimal primary decomposition of J with homogeneous q_i and say q_s is $m-$primary , then

$$J^{\text{sat}} = q_1 \cap \cdots \cap q_{s-1}$$

2. If $\sqrt{J} \subsetneq m$ then J^{sat} is the largest homogeneous ideal $I \subset S$ such that $[J]_k = [I]_k$ for any $k >> 0$. ($[J] - k$ is the space of polynomials of degree k.)

Example 3.21. Consider $J = \langle x^3, x^2y \rangle = \langle x^2 \rangle \cap \underbrace{\langle x^3, y \rangle}_{\langle x,y \rangle}$. $J^{\text{sat}} = \langle x^2 \rangle$. In $k[x, y, z]$, $J^{\text{sat}} = J$

Definition 3.22. For every homogeneous ideal J with $\sqrt{J} \subsetneq m$, we consider S/J^{sat} as a geometric object X called a projective (sub)scheme of $\mathbb{P}^n$. The homogeneous ideal of X is $I_X = J^{\text{sat}}$ and S/J^{sat} is called the homogeneous coordinate ring of X. Sometimes we write $X = \text{Proj}(S/J) = \text{Proj}(S/J^{\text{sat}})$ for the projective scheme defined by J.

Remark 3.23.
1. One has the following bijections

$$\{\emptyset\} \bigcup \left\{ \begin{matrix} \text{Projective} \\ \text{subschemes} \\ \text{of } \mathbb{P}^n \end{matrix} \right\} \overset{1:1}{\leftrightarrow} \{m\} \bigcup \left\{ \begin{matrix} \text{homogeneous} \\ \text{saturated ideals} \\ J \\ \text{with } \sqrt{J} \subsetneq m \end{matrix} \right\} \overset{1:1}{\leftrightarrow} \left\{ \begin{matrix} k \\ \cong S/m \end{matrix} \right\} \bigcup \left\{ \begin{matrix} \text{graded quotient} \\ \text{ring} \\ \text{of } S \text{ with a} \\ \text{non-zero} \\ \text{divisor of} \\ \text{positive degree} \end{matrix} \right\}$$

2. For projective subschemes $X, Y \subset \mathbb{P}^n$ the concepts of reducible, irreducible, $X \subset Y, X \cap Y, X \cup Y$ are analogous to affine case.

$$I_{X\cap Y} = (I_X + I_Y)^{\text{sat}}$$
$$I_{X\cup Y} = (I_X \cap I_Y)$$

Example 3.24. $X, Y \subset \mathbb{P}^3$ be schemes with homogeneous ideals

$$I_X = \langle x_0, x_1 \rangle \cap \langle x_2, x_3 \rangle \leftsquigarrow \text{pair of skew lines}$$

$$I_Y = \langle x_1 + x_2 \rangle \leftsquigarrow \text{hyperplane}$$

$X \cap Y$ should consist of two points.

$$I_X + I_Y = \langle x_0, x_1, x_2 \rangle \cap \langle x_1, x_2, x_3 \rangle \cap \underbrace{\langle x_0, x_3, x_1 + x_2, x_1 x_2 \rangle}_{\langle x_0,\dots,x_3\rangle-\text{primary}}$$

$I_{X\cap Y} = (I_X + I_Y)^{\text{sat}} = \langle x_0, x_1, x_2 \rangle \cap \langle x_1, x_2, x_3 \rangle$ and $X \cap Y = X \cap Y_{\text{red}} = \{(0 : 0 : 0 : 1), (1 : 0 : 0 : 0)\}$.
$\dim X = 1, \dim Y = 2$
$\deg X = 2, \deg Y = 1$

Definition 3.25. For a projective subscheme $X \subset \mathbb{P}^n$, we define it's dimension as

$$\dim(X) = \dim(S/I_X) - 1$$

and degree as

$$\deg X = \deg I_X = \deg(S/I_X)$$

4 Bezout's theorem

Definition 4.1. Consider any R- module M. An element $r \in R$ is called M-regular if $rm = 0$ for any $m \in M \implies m = 0_M$ Otherwise r is called a zero-divisor of M.

Note. $f \in R$ is M-regular if $0 :_M f = 0 :_M \langle f \rangle = 0$

Example 4.2. The zero divisors of $\mathbb{Z}-$ mod $Z/6Z$ are precisely the integers $\langle 2 \rangle \cup \langle 3 \rangle$

Proposition 4.3. If M is finitely generated graded S-module and $f \in S$ is M regular of positive degree, then

1. $\dim M/fM = \dim M - 1$
2. $\deg M/fM = \deg f \deg M$

Proof. Since f is M regular, there exists a short exact sequence ($d = \deg f$)

$$0 \to M(-d) \overset{f}{\hookrightarrow} M \to \frac{M}{fM} \to 0$$
$$m \mapsto fm$$

So $h_{M/fM}(j) = h_M(j) - h_M(j-d)$ □

Lemma 4.4 (Mayer-Vietoris sequence)**.** If N_1, N_2 ar graded submodules of a graded submodule M, then there is a SEQ of graded modules

$$0 \to \frac{M}{N_1 \cap N_2} \to \frac{M}{N_1} \oplus \frac{M}{N_2} \to \frac{M}{N_1 + N_2} \to 0$$
$$m \mapsto (m, m)$$
$$(m_1, m_2) \mapsto m_1 - m_2$$

Corollary 4.5. If $I, J \subset S$ are homogeneous ideals, then $h_{\frac{S}{I+J}(k)} = h_{\frac{S}{I}}(k) + h_{\frac{S}{I \cap J}}(k)$ for all $k \in \mathbb{Z}$.

Corollary 4.6.

1. $\dim(\frac{S}{I \cap J}) = \max\{\dim S/I, \dim S/J\}$
2. If WLOG $\dim S/I \geq \dim S/J$, then

$$\deg(\frac{S}{I \cap J}) = \begin{cases} deg S/I & \dim S/I > \dim S/J \\ \deg S/I + \deg S/J & \dim S/I = \dim S/J > \dim S/I + J \\ \deg S/I + \deg S/J & \dim S/I = \dim S/I + J \\ - \deg S/I + J & \end{cases}$$

5 Free Resolutions

5.1 Notation. $S = k[x_0, \dots, x_n]$ where $\deg x_i = 1, m = \langle x_0, \dots x_n \rangle = \oplus_{j>0}[S]_j$

$A = S/I, m = m_A = \bigoplus_{j>0} [S/I]_j$

M finitely generated $\mathbb{Z}$ graded A-module. $\phi : M \to N$ hom of graded modules (degree preserving).

Lemma 5.2 (Nakayama's lemma).

1. If $\frac{M}{mM} = 0$, then $M = 0$
2. If the images of homogeneous $m_1, ..., m_t \in M$ generate $\frac{M}{mM}$ as an A module, then they generated M as an A module.

Proof.

1. See Eisenbud Cor 4.8
2. Set $N = \frac{M}{\langle m_1, ... m_t \rangle}$, then $\frac{N}{mN} \cong \frac{M}{mM + \langle m_1, ..., m_t \rangle} = 0$. This gives $N = 0, \implies M = \langle m_1, \dots, m_t \rangle$.

□

Corollary 5.3. For homogeneous elements $m_1, \dots, m_t \in M$ TFAE:

1. $M = \langle m_1, \dots, m_t \rangle$
2. The images $\overline{m_1}, \dots, \overline{m_t}$ in M/mM genearted M/mM as a module over $A/m \simeq k$.

Definition 5.4. A minimal generating set G consists of homogeneous lements such that G $\{g\}$ is not a generating set $\forall g \in G \dots$

Corollary 5.5. If $\{m_1, \dots, m_t\}, \{n_1, \dots, n_s\}$ are minimal generating sets of M, then $s = t$ and $\deg m_i = \deg n_i$ for $i \in [t]$ upto reindexing.

Definition 5.6. Let $\phi : F \to M$ be any surjective hom of fg graded A modules, where F is free.

1. The fg A module $\ker \phi$ is called a (first) syzygy module of M (over A). It's elements are called (first) syzygies (correspond to relations among generators of M).
2. The map ϕ is said to be minimal if the induced hom

$$\begin{aligned} \overline{\phi} : \frac{F}{mF} &\xrightarrow{\approx} \frac{M}{mM} \\ \overline{f} &\mapsto \overline{\phi(f)} \end{aligned}$$

   is an isomorphism of k-vector spaces where $k \simeq A/m$.

Remark 5.7. Let $\{e_1, \dots, e_s\}$ be a basis of F. Then ϕ is minimal iff $\{\phi(e_1), \dots, \phi(e_s)\}$ is a min gen set of M.

Example 5.8. $S = k[x]$.

$$0 \to S(-1) \xrightarrow{x} S \xrightarrow{\phi} k \to 0 \quad \phi \text{ is minimal}$$

$$0 \to \begin{array}{c} S(-1) \\ \oplus \\ S \end{array} \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}} S^2 \xrightarrow{\psi} k \to 0 \quad \psi \text{ is not minimal}$$

In fact $\ker\psi \cong \ker\phi \oplus S$.

Lemma 5.9. The first syzygy module of M is unique upto isomorphism and free direct sums.

Proof. Consider surjective map $\phi : F \to M$ where $F = \oplus_{i=1}^{t} Ae_i$.

1. Suppose ϕ is not minimal. WLOG $\{\phi(e_1), \ldots, \phi(e_r)\}$ is a min gen set of M $(r \leq t)$. Write $F - G \oplus P$ where $G = \oplus_{i=1}^{r} Ae_i$ and $P = \oplus_{i=r+1}^{t} Ae_i$. Then the restriciont $\psi = \phi|_G : G \to M$ is minimal.

$$\begin{array}{ccccccccc} & & & & 0 & & & & \\ & & & & \downarrow & & & & \\ 0 & \longrightarrow & \ker\psi & \longrightarrow & G & \xrightarrow{\psi} & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \Vert & & \\ 0 & \longrightarrow & \ker\phi & \longrightarrow & F & \xrightarrow{\phi} & M & \longrightarrow & 0 \\ & & & & \downarrow & & & & \\ & & & & P & & & & \\ & & & & \downarrow & & & & \\ & & & & 0 & & & & \end{array}$$

The commutative diagram induces (snake lemma) a short exact sequence

$$0 \to \ker\psi \to \ker\phi \to P \to 0$$

P free $\implies \ker\phi = P \oplus \ker\psi \rightsquigarrow$ syzygy from minimal map.

2. Assume ϕ is minimal and $\psi : G \to M$ is another minimal homomorphism. To show $\ker\phi \cong \ker\psi$. By 5.5 there is an isomorphism $\epsilon : G \to F$ such that

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker\psi & \longrightarrow & G & \longrightarrow & M & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \epsilon} & & \Vert & & \\ 0 & \longrightarrow & \ker\phi & \longrightarrow & F & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

this commutative diagram gives us $\ker\phi \cong \ker\psi$.

□

Definition 5.10 (Minimal Free resolution).

1. A hom $\phi : F \to G$ of free A - modules is called minimal if $\mathrm{im}(\phi) \leq m_A G$.

2. A (graded) free resolution of M (over A) is an exact sequence of fg graded A modules

$$F_\bullet \quad \cdots \to F_t \xrightarrow{\phi_t} F_{t-1} \to \cdots \to F_1 \xrightarrow{\phi_1} F_0 \to M \to 0$$

where each F_i is free and ϕ_i is graded.
It is called minimal free resolution if each ϕ_i with $i \geq 1$ is minimal.

Remark 5.11. 1. $\phi : F \xrightarrow{[B]} G$ is minimal iff any coordinate matrix of ϕ does not have any units of A as entries.

2. The first sequence in 5.8 is a MFR, but second sequence is a free resolution but not minimal.

Theorem 5.12. 1. Any fg graded A module has a MFR (graded) $F_\bullet$.

2. If G is any free resolution of M, then there is a complex $P_\bullet$ of free A modules and an isomorphism of complexes $G_\bullet \cong F_\bullet \oplus P_\bullet$. In particular any two MFR of M are isomorphic.

Proof. 1. Existence and uniqueness follows from iterating 5.7 and 5.9.

$$\begin{array}{ccccccccc}
\cdots \to & F_2 & \xrightarrow{\phi_2} & F_1 & \xrightarrow{\phi_1} & F_0 & \xrightarrow{\phi} & M & \longrightarrow 0 \\
& & \searrow & \uparrow & \searrow & \uparrow & & & \\
& & & \ker\phi_1 & & \ker\phi & & & \\
& & & \uparrow & & \uparrow & & & \\
& & & 0 & & 0 & & &
\end{array}$$

2. Suppose G is not minimal, we will show that we can "cancel" at least a (shifted) copy of A in two consecutive free modules. Indeed by assumption there is some $i \geq 1$, such that ϕ_k is not minimal. Fix a coordinate matrix $B = (b_{ij})$ of ϕ_k. It contains a unit, say $b_{i_0 j_0} \in k^\star$.

   Performing elementary row and column operations (changing base of G_k, G_{k-1}) we get another coordinate matrix.

$$\tilde{B} = \begin{bmatrix} & 0 & \\ & \vdots & \\ 0 \cdots & b_{i_0 j_0} & 0 \cdots \\ & \vdots & \\ & 0 & \end{bmatrix}$$

   Denote by B', the matrix obtained from $\tilde{B}$ by deleting row i_0 and column j_0.
   Then ϕ_k decomposes as

$$\phi_k = \begin{matrix} \phi'_k \\ \oplus \\ \psi \end{matrix} : \begin{matrix} G'_k \\ \oplus \\ A(-d) \end{matrix} \to \begin{matrix} G'_{k-1} \\ \oplus \\ A(-d) \end{matrix}$$

   and

$$\phi'_k : G'_k \xrightarrow{B'} G'_{k-1}$$

   is given by multiplication by B' and

$$\psi : A(-d) \xrightarrow[\approx]{b_{i_0 j_0}} A(-d)$$

   Since $\ker\phi_k = \ker\phi'_k$ and $\operatorname{im}\phi_k = \operatorname{im}\phi'_k \oplus A(-d)$ the sequence obtained from G_0 by cancelling the complex

$$0 \to A(-d) \xrightarrow{b_{i_0 j_0}} A(-d) \to 0$$

is also a free resolution of M.

$\square$

Definition 5.13. Let $\cdots \to F_1 \to F_0 \to M \to 0$ be a MFR of M. By the previous theorem, there are unique integers $\beta_{ij} \in \mathbb{N}_0$ such that $F_i \cong \oplus_j A(-j)^{\beta_{ij}}$

The numbers $\beta_{ij}^A(M)$ are called the graded Betti numbers of M (over A).

Example 5.14. Consider $I = \langle x^2, xy, y^3 \rangle \subset S = k[x,y]$. Then S/I has a MFR

$$0 \to \begin{matrix} S(-3) \\ \oplus \\ S(-4) \end{matrix} \xrightarrow{\begin{pmatrix} y & 0 \\ -x & y^2 \\ 0 & -x \end{pmatrix}} \begin{matrix} S(-2)^2 \\ \oplus \\ S(-3) \end{matrix} \xrightarrow{\begin{pmatrix} x^2 & xy & y^3 \end{pmatrix}} S \to S/I \to 0$$

Definition 5.15. 1. $F = \oplus_1^r Ae_i$. Define the j^{th} exterior power to be the free A-module $\wedge^j F$ whose basis elements are of the form

$$e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_j} \quad \text{with } 1 \leq e_i < i_2 < \cdots < i_j \leq r$$

Thus $\operatorname{rank}(\wedge^j F) = \binom{r}{j}$.

2. $g. = g_1, \ldots, g_r \in A$ be sequence of homogeneous elements. Set $F = \oplus_1^r Ae_i$ with $\deg e_i = \deg g_i$. Then the Koszul complex to $g.$ is the complex

$$K.(g.) : 0 \to \wedge^r F \to \wedge^{r-1} F \to \cdots \to \wedge^j F \xrightarrow{\phi_j} \wedge^{j-1} F \to \cdots \to \wedge F \to \wedge^0 F = A \to \frac{A}{\langle g_1, \ldots, g_r \rangle} = F \to 0$$

with

$$\begin{aligned} \phi_j : \wedge^j F &\to \wedge^{j-1} F \\ e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_j} &\mapsto \sum_{k=1}^{j} (-1)^{k+1} g_{i_k} e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge \hat{e}_{i_k} \wedge \cdots \wedge e_{i_j} \end{aligned}$$

It is a graded complex: $\phi_{j-1}\phi_j = 0$ and $\deg(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_j}) = \sum_1^j \deg e_{i_k}$

Example 5.16. The complex to x^2, y over $S = k[x,y]$ is

$$0 \to \begin{matrix} S(-3) \\ < e_1 \wedge e_2 > \end{matrix} \xrightarrow{\begin{bmatrix} -y \\ x^2 \end{bmatrix}} \begin{matrix} S(-2) \\ \oplus \\ S(-1) \end{matrix} \xrightarrow{[x^2 y]} \frac{S}{(x^2, y)} \to 0$$

It is exact.

"repeating elements break exactness"

$$0 \to S(-3) \xrightarrow{\begin{bmatrix} -1 \\ 1 \end{bmatrix}} \begin{matrix} S(-2) \\ \oplus \\ S(-2) \end{matrix} \xrightarrow{[x^2 x^2]} S \to 0$$

cancel

$$0 \to S(-2) \xrightarrow{x^2} S \to \frac{S}{x^2} \to 0$$

which is the Koszul comlex of x^2.

Proposition 5.17. The Koszhul complex to $g. = g_1, \dots, g_r \in A$ is exact iff $g_1, \dots, g_r$ is a regular sequence.

Proof. Refer Eisenbud. □

Theorem 5.18 (Hilbert's Syzygy theorem)**.** Every finitely generated graded $S = k[x_0, \dots, x_n]$-module M has a finte minmal finite resolution:

$$0 \to F_t \to F_{t-1} \to \cdots \to F_0 \to M \to 0$$

with $t \leq n + 1 \dim S$.

Proof. There is a homological argument using Koszul complex on $x_0, \dots, x_n$ and another constructive proof using Gröbner basis. □

Example 5.19. $A = \frac{k(x)}{x^2}$

$$\cdots \to A(-2) \xrightarrow{x} A(-1) \xrightarrow{x} \frac{A}{x} = k \to 0$$

is a MFR of k over A. It is infinite.

Remark 5.20. Describing which sets of graded Betti numbers occur among (classes of) fg graded S-modules is an active area of research.

Theorem 5.21. The greaded Betti number of fg graded S module determine its Hilbert series

$$H_m(z) = \frac{\sum_{i,j}(-1)^i \beta_{i,j}(z)^j}{(1-z)^{n+1}} \leftarrow \text{rational}$$

Proof. Let $0 \to F_t \to \cdots \to F_1 \to F_0 \to M \to 0$ be a MFR of M. Then

$$H_M(z) = \sum_{i=0}^{t} (1)^j H_{F_i}(z)$$

$$H_{S(-j)}(z) = \frac{z^j}{(1-z)^{n+1}}$$

Since $F_i \cong \oplus_j S(-j)^{\beta_{i,j}}$, the claim follows. □

Definition 5.22. The depth of a graded A-module M is the maximal length of a M-regular seqeunce consisting of homogeneous elements of A of positive degree, denoted by $\text{depth}_A(M)$.

Remark 5.23. 1. For any homogeneous ideal $S, I \subset m_s$

$$\text{depth}(S/I) \geq 1 \iff I \text{ is saturated}$$

2. For any graded M, $\text{depth}(M) \leq \dim(M)$. ($\dim = 0 \implies \text{depth} = 0$.)

Definition 5.24. A finitely generated A-module is it Cohen-Macaulay if $\text{depth}(M) = \dim(M)$.

Example 5.25.
1. S is CM as an S-module.
2. Any 0-dimensinoal module is CM.
3. For $I = \langle x^3, x^2y \rangle = \langle x^2 \rangle \cap \langle x^3, y \rangle \subset k[x, y]$ $\dim S/I = 1$ and $\text{depth}_s S/I = 0$. ($I^{sat} = \langle x^2 \rangle$). So $/I$ is not CM.
4. If $X \subset \mathbb{P}^n$, $\dim X = 0$. S/I_X is CM S-module.
5. $\dim S/I_x = 1 \geq \text{depth}\, S/I_x \geq 1$(since I_x is saturated.)

Proposition 5.26. A K algebra $A = S/I$ is CM (as an A-module) iff there is graded polynomial subalgebra N with $\dim N = \dim A$ and A is a fg generated graded free N-module. (Nother Normalization)(Free module over polynomial subalgebra)

Proof. Refer Eisenbud. □

Theorem 5.27 (Auslander-Buchsbaum)**.** Suppose a finitely generated graded A-module M has a MFR

$$0 \to F_t \to F_{t-1} \to \cdots \to F_0 \to M \to 0$$

It's length t is called the it projective dimension of M. So $\text{projdim}(M) := t$

If $A = S$, then

$$\text{projdim}(M) = \underbrace{n+1}_{\dim(S)} - \text{depth}(M) \geq n + 1 - \dim(M)$$

Proposition 5.28. For any fg graded A-module M

$$\text{projdim} M \geq n + 1 - \dim M$$

with equality iff M is CM.

Proof. $\text{projdim} M = n + 1 - \text{depth}\, M$
$\dim M \geq \text{depth}\, M$ □

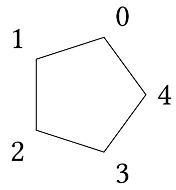
Definition 5.29. $A = S/I$ is said to be Gorenstein algebra if it is CM and if the last free module in a MFR of A has rank one, i.e.,

$$0 \to S(-d) \to F_{t-1} \to \cdots \to F_1 \to S \to A \to 0$$

with $t = n + 1 - \text{depth}\, A$.

Example 5.30.
1. The Koszul complex shows that any complete intersection is Gorenstein.

2. If Δ is a triangualtion of sphere then it's Stanley-Reisner ring is Gorenstein.



For example the above figure has Stanley-reisner ring $A = S/I$ where $I = \langle x_0x_2, x_0x_3, x_1x_3, x_1x_4, x_2x_4\rangle$. The MFR of A has the for

$$0 \to S(-5) \to S(-3)^5 \to S(-2)^5 \to S \to A \to 0$$

$$\begin{bmatrix} x_3 & x_4 & 0 & 0 & 0 \\ -x_2 & \vdots & -z_1 & 0 & \vdots \\ & & -x_0 & x_4 & x_2 \\ & -x_0 & \vdots & -x_3 & -x_1 \end{bmatrix}$$

5.31. Notation $\text{char}(K) = 0$ and $S = k[x_0, \dots, x_n]$, $R = k[y_0, \dots, y_n]$

Definition 5.32.

$$\begin{aligned} \beta : S \times R &\to R \\ (f, G) &\mapsto \partial_f \cdot G(\text{ differentiation}) \end{aligned}$$

induced by $\partial_{x^a} G = \frac{\partial^{a_0}}{\partial y_0^{a_0}} \cdots \frac{\partial^{a_n}}{\partial y_n^{a_n}}$ and extend k-linearly

Lemma 5.33. 1. β is a perfect pairing, i.e. it is k bilinear and $\beta(f, G) = 0 \forall G \in R \implies f = 0$ and $\beta(f, G) = 0, \forall f \in S \implies G = 0$.

2. For an $i, j \in \mathbb{Z}$ β induces maps

$$[S]_j \times [R]_j \to [R]_{i-j}$$

In particular for any $j \in \mathbb{Z}$,

$$[S]_j \times [R]_j \to k$$

is also a perfect pairing.

Proof. Bilinearity is clear. Now for any monomials $x^a \in S, y^b \in R$ of deg j then $\partial_{x^a} Y^b \neq 0$ iff $a = b$. □

The map β turns R into an S module: $f \cdot g := \partial_f G$.

Definition 5.34. 1. For any homogeneous ideal $I \subset S$ define Macaulay's inverse system $I^\perp$ as

$$I^\perp := \left\{G \in R | \partial_f G = 0 \forall f \in I\right\}$$

a graded S-submodule of R.

2. For any graded S-submodule M of R define it's annihilator as

$$\text{Ann}(M) := \left\{f \in S | \partial_f G = 0 \text{ for any } G \in M\right\}$$

Note: $[S]_j[R]_i \subset [R]_{i-j}$ (not exactly what we mean by graded module. Can think of it as $[S]_{-j}$ but thats messy. So we bare with this little inconvenience.)

$M \subset R$ a graded S-submodule (in the above sense). Define $\text{Ann}(M)$ in the same way.

Example 5.35. 1. $G = y_0^2 y_1^3$, $\mathrm{Ann}(G) = \langle x_0^3, x_1^4 \rangle$

2. $I = \langle x_0^2, x_1^3 \rangle$. Thn $I^\perp$ has a k-basis $y_0 y_1^2, y_0 y_1, y_1^2, y_1, y_1, 1$.

   Note:$\dim A/I = \dim S/\sqrt{I} = \dim k = 0$. To think about $\dim 0$ in terms of Hilbert dimension is $\dim S/I = 0 \iff [S/I]_j = 0$ when $j >> 0$ iff $\dim_k(S/I) < \infty$. $H_{S/I}(z) = \sum_{j \geq 0} \dim_{[}; S/I]_j = \rho/(1-z)^d$.

3. $J = \langle x_0, x_1 \rangle \subset k[x_0, x_1, x_2]$. $J^\perp$ has a k-basis $\left\{ y_2^j : j \in \mathbb{N}_0 \right\}$. It is not a fg S module $\dim S/I = 1$.

Theorem 5.36. There are bijections

$$\{\text{homogeneous ideals of S}\} \leftrightarrow \{\text{ Graded } S \text{ submodules of } R\}$$
$$I \mapsto I^\perp$$
$$\mathrm{Ann}(M) \leftarrow M$$

$I^\perp$ is a fg graded S -module $\iff \dim S/I = 0$.

Proof. The definition implies $I \subset \mathrm{Ann}(I^\perp)$ and $M \subset \mathrm{Ann}(M)^\perp$. The equality follows by comparing dimensions. □

Proposition 5.37. For any homogeneous ideal $I \subset S$ one has

$$\dim_k [I^\perp]_j = \dim_k [S/I]_j$$

for any $j \in \mathbb{Z}$.

Proof. Note that $[I^\perp]_j = \left\{ G \in [R]_j : \partial_f G = 0, \forall f \in [I]_j \right\}$. Because if $f \in [I]_{j-1}$, then $\partial_f G = 0$ iff $\partial_l \partial_f G = \underbrace{\partial_{lf} G}_{\in [I]_j} = 0$ for any $l \in [S]_1$.So it is enough to test G against polynomials of deg j in I.

Since $[S]_j \times [R]_j \to k$ is also a perfect pairing, it follows that $\dim_k [I]_j = \dim[S]_j - \dim[I]_j = \dim_k [S/I]_j$. □

5.38. Properties of ythe bijection in 5.36

1. For any two graded S-submodules M, N of R one has $Ann(M+N) = Ann(M) \cap Ann(N)$
2. For any homogeneous ideals $I, J \subset S$, $(I \cap J)^\perp = I^\perp + J^\perp$.

Definition 5.39. An ideal $I \subset S$ is reducible if $I = a \cap b$ with $I \subsetneq a, I \subsetneq b$.

Remark 5.40. 1. $I = \langle x^2, y^2 \rangle$ is irreducible ($I = Ann(xy)$).

2. Every irreducible ideal is primary but not true conversely.

$$\left\langle x^2, xy, y^2 \right\rangle = \left\langle x^2, y \right\rangle \cap \left\langle x, y^2 \right\rangle$$

   is not irreducible but primary.

Corollary 5.41. If $I \subset S$ homogeneous with $\dim S/I = 0$ the I is irreducible iff $I^\perp$ is principal. $I = Ann(G)$ for some $G \in R$.

Proof. Use the properties of the bijection and $I = Ann(I^{\perp})$ □

Theorem 5.42. Let $I \subset S$ be a homogeneous ideal such that $\sim S/I = 0$. TFAE

1. S/I is gorenstein.
2. I is irreducible.
3. $I = Ann(G)$ for some $G \in R$.
4. $I^{\perp}$ is principal.

Proof. Since β is perfect pairing it follows that

$$\hom_k(S/I, k) \cong I^{\perp}(\text{up to adjustment of grading})$$

It foolows for the MFR of S/I

$$0 \to F_{n+1} \to \cdots F_1 \to S \to S/I \to 0$$

F_{n+1} has rank 1 iff $I^{\perp}$ is principal. □

rank F_{n+1} is number of min generators of $I^{\perp}$.

Proposition 5.43. If S/I is gorenstein of $\dim 0$ then it's Hilbert function is symmetric (or palindromic) in teh sense, $\exists e \in \mathbb{N}$ such that

$$\dim_k[S/I]_j = \dim_k[S/I]_{e-j}$$

for any j.

Proof. By the previous theorem $I = Ann(G)$ for soem $G \in R$. Let $e = \deg G$.

Cpmsoder the map induced by β

$$\begin{aligned} [S]_j &\overset{[}{\underset{\phi}{\to}} R]_{e-j} \\ f &\mapsto \partial_f \circ G \end{aligned}$$

We get

$$\begin{aligned} \dim_k[I^{\perp}]_{e-j} &= \dim_k \left\{ \partial_f G | f \in [S]_j \right\} \\ &= \dim_k[S]_j - \dim_k[\underbrace{\ker \phi}_{I}]_j \\ &= \dim_k[S/I]_j \end{aligned}$$

By 5.37 $\dim_k[I^{\perp}]_{e-j} = \dim_k[S/I]_{e-j}$

□

Example 5.44. $I = \langle x^2, y^2, z^2 \rangle \subset S = k[x, y, z]$. S/I is gorenstein.

j	0	1	2	3	4
$\dim_k[S/I]_j$	1	3	3	1	0
				xyz	

Lemma 5.45. If $X \subset \mathbb{P}^n$ is a finite set of pints and $h_X(j) = k$, then there is a subset $Y \subset X$ of k points with $h_Y(j) = k = h_X(j)$

Corollary 5.46. Let $X \subset \mathbb{P}^n_k$ be a fintie set of pioonts where k is infinite.

1. There is some $e \in \mathbb{N}_0$ such that

$$h_X(0) < \cdots < h_X(e-1) < h_X(e) = h_X(j) = |X|$$

   for an $j \geq e$.

2. If X is gorenstein, then $H_X(e-1) = |X| - 1$.

Proof. Since $\operatorname{depth}(S/I_X) > 0$ (Ideal of scheme saturated $\implies$ depth> 0). So $A = S/I_X$ contains a nonzero divisor of positive degree. As K is infinite there exists a nonzerodivisor of degree 1, say l

$$\begin{aligned} 0 \to A(-1) \xrightarrow{l} A \to A/lA \to 0 \\ a \mapsto al \end{aligned}$$

is exact and so

$$h_{A/lA}(j) = h_A(j) - h_A(j-1)$$

and

$$\dim A/lA = \dim A - 1 = 0$$

finite set of points geom dim =0 so Krull dim =1

$H_{A/lA}(z)$ is a polynomial. Denote it by e it's degree. Now first statement follows. By 5.43 we know

$$1 = h_{A/lA}(0) = h_{l/lA}(e)$$

which implies the second statement. □

Example 5.47. If A/lA has Hilbert function

deg	0	1	2	3	4	5
dim	1	3	5	3	1	0

then A has Hilbert function $1, 4, 9, 12, 13, 13$

Theorem 5.48 (Davis, Geramita, Orrechia, 1985)**.** For a fintie set of points $X \subset ¶^n$, TFAE

1. X is Gorenstein
2. There is some $c \in |X| - h_X(e-j) = h_X(j)$ for $0 \leq j \leq e/2$ and for any subset $Y \subset X$ with $|Y| = |X| - 1$ one has $h_Y(e-1) = |X| - 1$

6 Waring Rank

$S = k[x_0, \ldots, x_n]$ char$(K) = 0$. For any $d \in \mathbb{N}$, the k vector space of $[S]_d$ has a k basis of $\binom{n+d}{d}$ of powers of linear forms l_i^d , $l_i \in [S]_2$, $i \in [\binom{n+d}{d}]$

Hence for any $f \in [S]_d$ can be written as

$$f = \sum_{i=1}^{\binom{n+d}{d}} \lambda_i l_i^d \quad l_i \in k$$

If K is algebraically closed using $\lambda_i = \mu_i^d$ one gets

$$f = \sum_{i=1}^{\binom{n+d}{d}} (\mu_i l_i)^d$$

Definition 6.1. Given $f \in [S]_d$ any expression of the form

$$f = \sum_{i=1}^{r} l_i^d$$

where $l_i \in [S]_1$ is called a Waring decomposition of f.

The least r such that f has a Waring decomposition with r summands is called the waring rank denoted wr$(f) :=$ wr$_k(f)$

Example 6.2. $xy = \frac{1}{4}[(x+y)^2 - (x-y)^2]$ so wr$_{\mathbb{R}}(xy) = 2$.

Determining the waring rank of a general polynomial is the problem of interest.

Proposition 6.3. If K is algebraically closed then for any $q \in [S]_2$ one has

$$\wr(q) = \text{rank}(Q)$$

where $Q \in K^{(n+1)\times(n+1)}$ is symmetric with $q = [x_0 \cdots x_n]Q \begin{bmatrix} x_0 \\ \vdots \\ x_n \end{bmatrix}$

Proof. Since Q is symmetric $\exists T$ invertible $\in K^{(n+1)\times(n+1)}$ such that

$$T^t Q T = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{bmatrix}$$

Hence $x^t(T^tQT)x = \sum a_i x_i^2$. $q = [l_0 \cdots l_n]Q \begin{bmatrix} l_0 \\ \vdots \\ l_n \end{bmatrix} = q(l_0, \ldots, l_n)$

Changing basis $l_i = y_i$, x_i is a linear form $\tilde{l}_i$ in $y_0, \ldots, y_n$ we get $q(y_0, \ldots, y_n) = \sum a_0 \tilde{l}_i^2$ □

Theorem 6.4. For any sufficiently general $f \in [s]_d$ with $d \geqslant 3$, one has

$$\operatorname{war}(f) = \left\lceil \frac{\binom{n+d}{n}}{n+1} \right\rceil$$

except if $d = 3$ and $n = 4$ or $d = 4$ and $2 \leq n \leq 4$

Remark 6.5. This is a consequence of a result about Hilbert function Set $I := \cap_{j=1}^{r} I_{p_j}^2$ when $P_1, .., P_r \in \mathbb{P}^n$ are general points. Then $h_A(j) = \min\left\{ (n+1)r, \quad \binom{n+j}{r} \right\}$ for any j except $j = 3, n = 4$ and $n = 9$. or $j = 4, 2 \leq n \leq 4$ and $r = \binom{n+2}{4} - 1$

Recall for $R = k\left[y_0, \dots, x_n\right]$ we have perfect pairing

$$\begin{aligned} S \times R &\longrightarrow R \\ (f, G) &\mapsto \partial_f \circ G \\ I \subset S &\mapsto I^{\perp} \subset R \\ \operatorname{Ann}(M) &\leftarrow M \end{aligned}$$

Every linear form $l = a_0 y_0 + \dots . + a_n y_n \in R$ corresponds to a point and $P = (a_0 : \dots : a_n) \in \mathbb{P}^n$.

Lemma 6.6. For any $f \in [S]_j \quad l = s_0 y0 + \dots \cdot a_n y_n$ and $d \in \mathbb{N}$ one has

$$\partial_f \cdot l^d = \frac{d!}{(d-j)!} f\left(a_0, \dots, a_n\right) l^{d-j}$$

Proof. It suffices to check this for $f = x^b = x_0^b \cdots x_n^{bn} \in [S]_j$ if $d \geqslant |b|$ where $l^{d-j} := 0$ if $d < j$. ☐

Lemma 6.7 (Apolarity Lemma). Let $X \in \mathbb{P}^n$ be a set of s distinct points corresponding to linear forms $l_1, \dots, l_s$. Cot $f \in [R]_d$ Then there are $c_1 \dots c_s \in K$ st.

$$f = \sum_{i=1}^{\infty} c_i l_i^d \text{ iff } I_x \subset \operatorname{Ann}(f)$$

Proof. $\Longrightarrow$ To simplify notation, for $P = (a_0 : \dots : a_n)$ write $f(p)$ instead of $f\left(a_0, \dots, a_n\right)$. By definition $g \in \operatorname{Ann}(f)$ iff $0 = \partial_g \cdots f = 0$

$g \in I_X$ satisfies $g(P_i) = 0$ for $i \in [s]$ This shows $I_X \subset \operatorname{Ann}(f)$.

$\Longleftarrow \qquad I_x \subseteq \operatorname{Ann}(f) \Leftrightarrow I_X^{\perp} \supset \operatorname{Ann}(f)^{\perp} = \Leftrightarrow I_X^{\perp} \ni f$

For any point $p = (a_0 \cdots a_n) \in \mathbb{P}^n$, one has

$$I_p^{\perp} = \left\{ c l_p^j : c \in k \quad j \in \mathbb{N}_0 \right\} \text{ with } l_p = c_0 x_0 + \cdots a_n x_n$$

(It is ETS for $p = (1 : 0 \cdots : 0)$. Then $I_p = \langle x_1, \dots, x_n \rangle$ Thus $f \in I_p^{\perp} \iff \frac{\partial f}{\partial x_i} = 0 \iff f = c x_0^j$ for $c \in k \quad j \in \mathbb{N}_0$.)

$I_x = I_{p_1} \cap \dots \cap I_{ps} I_x^{\perp} = I_{p_1}^{\perp} + \dots + I_{P_s}^{\perp}$ So $\left[I_x^{\perp}\right]_d = \left\langle l_1^d \right\rangle + \dots + \left\langle l_s^d \right\rangle$ Hence $f = \sum_{i=1}^{s} c_i l_i^d$ with $c_i \in k$ ☐

Theorem 6.8 (Catkin, Catalisamo, Geramita,2012)**.** If k is algebraically closed, $1 \leq a_0 \leq a_1 \leq \ldots \leq a_n$, then

$$\mathrm{wr}(\underbrace{y_0^{a_0} y_1^{a_1 \ldots y_n} a_n}_{G}) = \frac{1}{(a_0+1)} \prod_{i=0}^{n} (a_i + 1)$$

Proof. If $n = 0$, then $\mathrm{wr}(a_0^{x_0}) = 1$

Let $n \geq 1$. Since $\mathrm{Ann}(G) = \left\langle x_0^{a_0+1}, x_1^{a_1+1}, \ldots, x_n^{a_{n+1}} \right\rangle$ and $a_1 \leq a_1 \leq \ldots a_m$, we get

$$\mathrm{Ann}(G) \supset J = \left\langle x_0^{a_1+1} - x_2^{a+1}, \ldots \quad x_0^{a_{n+1}} - x_n^{a+1} \right\rangle \tag{1}$$

J is generated by a regular sequence, so $\dim S/J = 1$ and $\deg J = (a_1+1)\ldots(a_n+1) = r$. Let $\eta_i \in k$ be a primitive a_i+1 root of unity and consider $X := \left\{(1 : \eta_1^{k_1} : \cdots : \eta_n^{k_n}) \mid 0 \leq k_i \leq a_i \forall i\right\}$. Then $|X| = (a_1+1)\ldots(a_m+1) = r$ and $X \subset Z(J)$. Hence $X = Z(J)$, $I_X = J \implies \mathrm{wr}(G) \leq r$ by Apolarity lemma.

Conversely by apolarity there is a saturated ideal $I \subset \mathrm{Ann}(G)$ defining a set $\Gamma \subset \mathbb{P}^n$ of s points. So $I = \cap_{p\in\Gamma}(I_p : x_0) = \cap_{p\in\Gamma'} I_p$ where $\Gamma' \subset \Gamma$ is the subset of points not lying in the hyperplane defined by $X_0 = Z(x_0)$.

Set $s' = |\Gamma'| \leq |\Gamma| = s$. So it suffices to show $s' \geq r$. Since $a_0 \geq 1$, we have $x_0 \notin \mathrm{Ann}(G)$(1 calculated explicitly) and thus $x_0 \notin I$ So $s' \geq q$, i.e., $\tilde{I} \neq S$, so $\tilde{I} : x_0 = \tilde{I}$. Hence for every $j >> 0$, we get

$$s' = h_{\frac{S}{\tilde{I}}}(j) = \sum_{k=0}^{j} h_{\frac{S}{\tilde{I}+x_0 S}}(k)$$

Degree of regular system of parameters=product of degrees

Moreover I $\subseteq \mathrm{Ann}(G)$ implies

$$\begin{aligned} \tilde{I} = I : x_0 &\subseteq \mathrm{Ann}(G) : x_0 \\ &= \left\langle x_0^{a_0}; x_1^{a_1+1}, \cdots, x_n^{a_{n+1}} \right\rangle \end{aligned}$$

so

$$\tilde{I} + x_0 S = \left\langle x_0, x_1^{a_1+1}, \ldots, x_n^{a_n+1} \right\rangle = \tilde{J} \rightsquigarrow \text{regular system of parameters}$$

Note, $\dim S/\tilde{J} = 0$ and $\deg \tilde{J} = (a_1+1)\ldots(a_n+1) = r$

It follows that

$$\begin{aligned} s' &= \sum_{r=0}^{j} h_{\frac{S}{\tilde{I}+x_0 S}}(k) \geqslant \sum_{k=0}^{j} h_{s/\tilde{J}}(k) \\ &= \deg \tilde{J} = r \end{aligned}$$

$$\Rightarrow \mathrm{wr}(a) \geqslant s' \geqslant r$$

□

7 Complexity of Matrix multiplication

Question. How many multiplications in K does one need to compute $A \cdot B$ for $A, B \in K^{n \times n}$

Example 7.1 (Stransen, 1989)**.** $n = 1$. Let $C = (c_{ij})$. Set

$I = (a_{11} + a_{22})(b_{11} + b_{22})$
$II = (a_{21} + a_{22})b_{11}$
$III = a_{11}(b_{21} + b_{22})$
$IV = a_{22}(-b_{11} + b_{21})$
$V = (a_{11} + a_{22})(b_{22})$
$VI = (-a_{12} + a_{22})(b_{12} + b_{12})$
$VII = (a_{12} - a_{22})(b_{21} + b_{22})$

$c_{11} = I + IV - V + VII$
$c_{21} = II + IV$
$c_{12} = II + V$
$c_{22} = I - II + III + VI$

Remark 7.2. This is optimal. (Uimogradov, 1971)

Definition 7.3. The exponenet of matrix multiplication

$$\omega = \inf\{\tau \in \mathbb{R} : \text{computing the product of two } n \times n \text{ matrices takes } O(n^\tau) \text{ multiplications}\}$$

Theorem 7.4 (Strassen, 1969)**.** $\omega \leq \log_2 7 \approx 2.81$

Current record: $\omega < 2.374$ (Gall, 2014)

7.5. Conjecture $\omega = 2$.

If U, V, W are k-vector spaces with bases $\{u_i\}, \left\{v_j\right\}, \{w_k\}$, then the tensor product $u \otimes v \otimes w$ is a k vector space with basis $\left\{u_i \otimes v_j \otimes w_k\right\}\ldots$

The rank of a tensor $T \in U \otimes V \otimes W$ is

$$\mathrm{rk}(T) := \min\left\{r : T = \sum_{I=1}^{r}(u_i \otimes v_j \otimes w_k)_I\right\}$$

for any $u_i, v_j, w_k \in U, V, W$ respectively.

$\hom(U \otimes V, W) \cong U \otimes V \otimes W$ fo[r] fin dim space[s]

Under this isomorphism the map

$$U \otimes V \to W$$
$$A \otimes B \mapsto A \cdot B$$

$M_n = \sum_{i,j,k=1}^{r} E_{ij} \otimes E_{jk} \otimes E_{ki}$ where $E_{ij} \in K^{n \times n}$ has a 1 in position (i, j) and all other entries 0.

Theorem 7.6 (Strassen, 1983)**.** $\omega = \inf\{\tau \in \mathbb{R} : \mathrm{rank}(M_n) = O(n^\tau)\}$

The symmetrization of M_n gives a symmetric tensor corresponding to the polynomial

$$f_n = \mathrm{trace}(X_{n \times n}^3)$$

where $X = (\underbrace{x_{i,j}}_{\text{variable}})_{i,j} \in [n]$

$$\begin{aligned} &\dim v = n \\ &v_1 \otimes v_2 \rightsquigarrow v_1 \otimes v_2 + v_1 \oplus v_3 + \cdots + v_{n-1} \oplus v_n \\ &\qquad\qquad \updownarrow \\ &\qquad\qquad 1_{x_1 x_2} \\ &\qquad\quad = \sum_{i,j,k=1}^{n} x_{ij} x_{jk} x_{ki} \text{ homo. of deg 3} \end{aligned}$$

Theorem 7.7 (Chiantini, Ikenmeyer, Landsberg, Ottarini, 2018)**.** $\omega = \inf\{\tau \in \mathbb{R} : \mathrm{wr}(f_n) = O(n^\tau)\}$