Math 765 - Computational Commutative Algebra

Nathan Fieldsteel

Spring 2019

Course Description

This will be a course on computational methods in commutative algebra and algebraic geometry, with a particular focus on the computer algebra system `Macaulay2`. In addition to developing proficiency with `Macaulay2`, we will aim to understand the algorithms which it uses to perform explicit computations with polynomial rings and related objects. A tentative list of topics includes but is not limited to : Gröbner bases and their applications, Buchberger's Algorithm, minimal free resolutions, Betti tables, syzygies, Stanley-Reisner rings, monomial ideals, and the F_4 and F_5 families of algorithms. Depending on time and student interest, we may also discuss other topics at the intersection of mathematics and computation, such as numerical algebraic geometry using `Bertini`, or writing and formally verifying mathematical proofs using `Coq`.

Prerequisites

No familiarity with programming will be assumed. Familiarity with basic commutative algebra (rings, ideals, modules) will be helpful. Students should have access to a computer.

Expectations

Optional homework problems will be assigned. Grade will be based on the completion of a computational project on a topic of the student's choosing.

References

[1] D. A. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.

[2] D. A. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms.* Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[3] D. Eisenbud. *The geometry of syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. A second course in commutative algebra and algebraic geometry.

[4] D. Eisenbud, D. R. Grayson, M. Stillman, and B. Sturmfels, editors. *Computations in algebraic geometry with Macaulay 2*, volume 8 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2002.

[5] H. Schenck. *Computational algebraic geometry*, volume 58 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2003.

Contents

1 January 9 - Monomial Orders and Multivariate Polynomial Division

1.1 Getting Started

As part of the focus of this class will be on the use of computational software, the first thing you should do is install and set up `Macaulay2`, and familiarize yourself with the basics of the system. You can download `Macaulay2` and find installation instuctions at `macaulay2.com`, under the Downloads link in the sidebar. While `Macaulay2` can be run from a terminal, it is significantly easier and more convenient to use `Macaulay2` in an environment which allows you to both run `Macaulay2` commands and also facilitates the editing and saving of text files. The most sensible choice for such an environment is the Emacs text editor. Instructions for getting Emacs and configuring it to run `Macaulay2` are available at the links listed above.

If you already have `Macaulay2` installed, you should verify that you are using the most up-to-date version of the software. `Macaulay2` will tell you which version you have when you start a new session. At the time of this writing (January 2019), version 1.13 has *just today* been released, so if you have an existing installation you'll very likely need to upgrade.

1.2 Multivariate Polynomial Division

These first notes are written following the introductory chapter in [1].

Our first goal is to generalize the polynomial division algorithm to polynomial rings with more than one variable. But first we'll summarize the one-variable case:

Let k be a field and let I be an ideal in the ring $R = k[x]$. Because R is a principal ideal domain, the ideal I is principal, so we can say $I = (g(x))$ for some $g(x) \in R$. Given an arbitrary polynomial $f(x)$ in R, we might want to know whether or not $f(x)$ is in I (equivalently, whether $f(x)$ is 0 in R/I). The division algorithm for $k[x]$ says that there exist unique polynomials $q(x)$ and $r(x)$ in R satisfying

$$f(x) = q(x)g(x) + r(x)$$

with $\deg(r(x)) < \deg(g(x))$, and these polynomials can be found using the Euclidean algorithm. It is immediate that the remainder $r(x)$ is 0 if and only if $f(x)$ is in I.

In order to generalize this statement to the ring $S = k[x_1, \ldots, x_n]$, we'll need a way to order the monomials in S analogous to the degree comparison in the one-variable case.

Definition 1.1. A *monomial ordering* on the set of monomials in S is an order relation $>$ satisfying:

i. $>$ is a total ordering. For any monomials x^α, x^β, either $x^\alpha > x^\beta$ or $x^\beta > x^\alpha$.

ii. $>$ is a well-ordering: Every nonempty set of monomials has a minimum with respect to $>$.

iii. $>$ respects multiplication: for any monomials $x^\alpha, x^\beta, x^\gamma$, if $x^\alpha > x^\beta$ then $x^\alpha x^\gamma > x^\beta x^\gamma$

Some authors also include the requirement that 1 is the smallest monomial with respect to $>$, but this follows from the definition above: If there were a monomial m with with $1 > m$, then we could repeatedly apply (iii) to conclude that $1 > m > m^2 > m^3 > \ldots$, forming a nonempty set of monomials with no minimum, contradicting (ii).

In $R = k[x]$, the *only* monomial order is the degree ordering $\ldots > x^{n+1} > x^n > \ldots > x^2 > x^1 > 1$. But in $S = k[x_1, \ldots, x_n]$ there are many. Here are a few examples:

Example 1.1. The *lexicographic order* of monomials, denoted $>_{\text{lex}}$, is defined by

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{\text{lex}} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

if and only if there exist $i < n$ with $\alpha_j = \beta_j$ for $j < i$ and $\alpha_i > \beta_i$. Said another way, $x^\alpha >_{\text{lex}} x^\beta$ if the leftmost nonzero entry in the difference of exponent vectors $\alpha - \beta$ is positive.

Lexicographic order is sometimes described as "alphabetical" or "dictionary" order, but this is only true if we restrict our attention to monomials with fixed total degree d. In this case, when arranged in decreasing order by $>_{\text{lex}}$, the monomials will be sorted into "alphabetical" order. But between monomials of different total degree, this observation is not true. Note that $x_1^2 > x^1$.

Note also that under lexicographic ordering, if the total degree of x^α is greater than the total degree of x^β, this does not imply that $x^\alpha >_{\text{lex}} x^\beta$. For example, in $k[a, b, c]$ we note that the following is a decreasing sequence of monomials for which the corresponding sequence of total degrees is $2, 6, 5, 11, 1$:

$$x^2 > xy^5 > y^5 > yz^{10} > z$$

If we want to fix this, it is easy to use $>_{\text{lex}}$ to construct an monomial order that respects total degree:

Example 1.2. The *graded lexicographic order*, denoted $>_{\text{grlex}}$, is defined by

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{\text{grlex}} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

if either the total degree of x^α is greater than the total degree of x^β, *or* their total degrees are equal and $x^\alpha >_{\text{lex}} x^\beta$. In other words, we first order by total degree, and break ties with the $>_{\text{lex}}$ order.

Example 1.3. The *graded reverse lexicographic order* is defined by

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} >_{\text{grlex}} x_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

if either the total degree of x^α is greater than the total degree of x^β, of their total degrees are equal and the rightmost nonzero entry in the vector $\alpha - \beta$ is negative.

A heuristic description of this ordering is as follows: First, order the monomials by total degree. Then within a fixed total degree, order the monomials lexicographically, but with the opposite ordering of the variables. Finally, reverse the order in each total degree.

So, while the lexicographic ordering of the degree three monomials in the variables x, y, z is

$$x^3 >_{\text{lex}} x^2y >_{\text{lex}} x^2z >_{\text{lex}} xy^2 >_{\text{lex}} xyz >_{\text{lex}} xz^2 >_{\text{lex}} y^3 >_{\text{lex}} y^2z >_{\text{lex}} yz^2 >_{\text{lex}} z^3$$

If we had instead lexicographically ordered them using the variable order $z > y > x$ we would end up with

$$z^3 > z^2y > z^2x > zy^2 > zyx > zx^2 > y^3 > y^2x > yx^2 > x^3$$

And *reversing* this ordering gives us the $>_{\text{grevlex}}$ ordering on monomials of degree 3 in $x > y > z$:

$$x^3 >_{\text{grevlex}} x^2y >_{\text{grevlex}} xy^2 >_{\text{grevlex}} y^3 >_{\text{grevlex}} x^2z >_{\text{grevlex}} xyz >_{\text{grevlex}} y^2z >_{\text{grevlex}} xz^2 >_{\text{grevlex}} yz^2 >_{\text{grevlex}} z^3$$

All of the preceeding monomial orders can be thought of as sequentially comparing various linear functions of the exponent vectors until an inequality is found. For example, $>_{\text{lex}}$ checks if $\alpha_1 = \beta_1$, then checks if $\alpha_2 = \beta_2$, and so on, until one of these equalities fails to hold. Graded lex first checks if $\sum \alpha_i = \sum \beta_i$, then checks the inequalities for $>_{\text{lex}}$. This framework allows use to make a very general definition of monomial orders which (it turns out) captures *all possible* monomial orders.

Example 1.4. Let $R = k[x_1, \dots, x_n]$ and let M be an $m \times n$ matrix with rows $r_1, \dots, r_m$. We can attempt to define a monomial order on R using M by defining $x^\alpha >_M x^\beta$ if there exists $i \leqslant m$ satisfying $r_j \cdot \alpha = r_j \cdot \beta$ for all $1 \leqslant j < i$ and $r_i \cdot \alpha > r_j \cdot \beta$.

It's easy to come up with matrices M so that $>_M$ fails to be a monomial order. But it turns out that every monomial order can be realized as $>_M$ for some M. For example, lexicographic order is $>_M$ where M is the $n \times n$ identity matrix, and graded lexicographic order is realized by the matrix you get by adding a row of 1s at the top of the $n \times n$ identity matrix.

Monomial orderings are the appropriate generalization of the degree comparison in $k[x]$ to give us a multivariable version of the division algorithm.

Theorem 1.1. Let $R = k[x_1, \dots, x_n]$ and let $>$ be a monomial order on R. Let $f \in R$ and let $(f_1, \dots, f_d)$ be an ordered sequence of elements of R. Then there exists polynomials $a_1, \dots, a_d \in R$ and $r \in R$ so that the equation

$$f = a_1 f_1 + \dots a_d f_d + r$$

holds, and for each i, either $a_i f_i = 0$ or it has leading term smaller than the leading term of f, and r is a sum of terms none of which is divisible by the leading term of any f_i. r is called a remainder of f after division by $f_1, \dots, f_d$.

If the remainder $r = 0$, then f is in the ideal generated by $(f_1, \dots, f_d)$, but the converse doesn't necessarily hold. We note the failure of the desired "if and only if" statement with the following example, taken from [5]:

Example 1.5. In the ring $R = k[x, y]$ consider the elements $(x^2 + y, xy - 1)$ and suppose we want to know if $x^2 - y^2$ is in the ideal they generate. Using polynomial division it is easy to find the expression

$$(x^2 - y^2) = (1)(x^2 + y) + (0)(xy + x) + (-y^2 - y)$$

which satisfies the conditions specified in the multivariate polynomial division algorithm. Despite the remainder being nonzero, we can see that

$$x^2 - y^2 = (-y)(x^2 + y) + (x)(xy + x)$$

so it is clearly in the ideal $(x^2 + y, xy + x)$, despite the nonzero remainder.

2 January 11 – Groebner Bases and Buchberger's Algorithm

2.1 Groebner Bases

Last time we saw that the remainder in multivariate polynomial divison 1.1 doesn't necessarily answer the question of ideal membership: $r = 0 \Rightarrow f \in I$ but this is not an "if and only if". The way to fix this problem is with Groebner Bases, and the way to find Groebner Bases is with Buchberger's Algorithm

First let's note the problem with 1.1. The remainder after multivariate polynomial division is a sum of terms, none of which are divisible by the leading term of any of the f_i. Unfortunately, as we saw in example 1.5, an arbitrary element of the ideal $(f_1, \ldots, f_d)$ may have a leading term which is not divisible by any leading term of the generating set. But if you could replace the generating set for I by a much bigger set, one which has leading terms dividing any leading term of any element of I, then this problem would go away. This motivates the following definition.

Definition 2.1. Let I be an ideal in $R = k[x_1, \ldots, x_n]$ and fix a monomial order $>$ on R. A *Groebner basis* for I with respect to $>$ is a set $\{g_1, \ldots, g_d\} \subseteq I$ with the property that, for any $f \in I$, the leading term of f is divisible by the leading term of g_i for some i.

Such a set, if it exists, will fix the failure of 1.1 to adequately test ideal membership, for the following reason:

Remark 2.1. Let $G = \{g_1, \ldots, G_d\}$ be a Groebner basis for I, and let $f \in R$. We can do polynomial division to write

$f = a_1 g_1 + \ldots, a_d g_d + r.$

If $f \in I$, then $r \in I$ as well. But then either the leading term of r is divisible by the leading term of g_i for some i, a contradiction, or $r = 0$. So when we use a Groebner basis for I instead of an arbitrary generating set, the remainder after division in 1.1 is 0 if and only if the polynomial in question is in I. Note the natural corollary: If G is a Groebner basis for I, then the ideal generated by G is I.

There are other, equivalent formulations of the definition of Groebner basis:

Definition 2.2. Let $>$ be a monomial order on $R = k[x_1, \ldots, x_n]$, let I be an ideal in R and let $G \subseteq I$. The following are equivalent:

i. G is a Groebner basis for I with respect to $>$, following 2.1.

ii. Let $\mathrm{LT}_>(I)$ be the ideal generated by the set $\{\mathrm{LT}_>(f) \mid f \in I\}$. Then the set of leading terms of elements of G generate $\mathrm{LT}_>(I)$.

iii. For any $g_i, g_j \in G$, the element:

$$S(g_i, g_j) = \frac{\mathrm{LCM}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\alpha_i \,\mathrm{LT}_>(g_i)} g_i - \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\alpha_j \,\mathrm{LT}_>(g_j)} g_j$$

has remainder zero after division by G. Here α_i is the leading coefficient of g_i, and similarly for α_j.

While i. ⇒ ii. ⇒ iii. is straightforward, iii. ⇒ i. is a more significant undertaking, the details are spelled out in [2].

2.2 Buchberger's Algorithm

The polynomial $S(g_i, g_j)$ used in this definition is called an *S-polynomial*. The idea here is to take two elements in I and subtract multiples of them from each other to get a new element of R with a leading term (probably) not divisible by the leading terms of either of g_i or g_j. If G is not a Groebner basis for the ideal it generates, then maybe some S-polynomial of elements in G will have a leading term not divisible by any element of G. This observation can be used to outline a procedure for starting with an arbitrary set $\{f_1, \dots, f_d\}$ and find a Groebner basis for the ideal generated by this set

Definition 2.3. *Buchberger's Algorithm* is the process defined in Pseudocode below.

With input a finite set $\{f_1, \dots, f_d\}$ of polynomials, it returns a Groebner basis for the ideal generated by F.

Algorithm 1 Buchberger's Algorithm

procedure BUCHBERGER'S ALGORITHM($f_1, \dots, f_d$) ▷ Gives Grobner basis of $I = (f_1, \dots, f_d)$
    $F \leftarrow \{f_1, \dots, f_d\}$
    $G \leftarrow F$
    repeat
        $G_{\text{temp}} \leftarrow G$
        for each pair $g_i, g_j \in G$ **do**
            $r \leftarrow$ the remainder after dividing $S(g_i, g_j)$ by G
            if $r \neq 0$ **then**
                add r to G_{temp}
    until $G = G_{\text{temp}}$

If this loop actually stops, then the resulting set G will satisfy iii. in 2.2, so it will be a Groebner basis for I. But how do we know this will ever terminate? The idea is to consider the chain of ideals $\{I_k\}$ generated by the leading terms of the elements of G_{temp} after k iterations of the loop. One can show that $I_k \subsetneq I_{k+1}$ if and only if the loop did not terminate after iteration k. So this algorithm will fail to terminate if and only if we have an infinite ascending chain of ideals in R, impossible because R is noetherian.

3 January 14 – An Introduction to `Macaulay2`

3.1 Sample Macaulay2 Session

The purpose of today's class is to demonstrate some basic usage of `Macaulay2`. One thing which I very much wanted to demonstrate was using `Macaulay2` in the `EMACS` text editor. But because I couldn't connect my computer to the projector, I was unable to demonstrate this. Please get `Macaulay2` up and running in `EMACS` if you haven't already: it's a significant upgrade over using the command line only.

When I first launch `Macaulay2` I see something like this:

```
+ M2 --no-readline --print-width 100
Macaulay2, version 1.13
--loading configuration for package "FourTiTwo" from file /Users/nathan/Library/Application Support
--loading configuration for package "Topcom" from file /Users/nathan/Library/Application Support/Ma
with packages: ConwayPolynomials, Elimination, IntegralClosure, InverseSystems,
               LLLBases, PrimaryDecomposition, ReesAlgebra, TangentCone,
               Truncations
i1 :
```

Significantly, `Macaulay2` is telling me that I'm running version 1.13, which is the current version (As of Jan 2019). The prompt `i1 :` is waiting for the first line of input from the user. In emacs, we can type directly into the `Macaulay2` buffer as if it were an ordinary command-line session. We can also press F12 (or whatever key you have configured) while in a file that ends with the `.m2` extension to start a `Macaulay2` session in emacs, or to show the current session. You can use F11 from your `.m2` file to send the line containing the cursor to `Macaulay2`, or to send the current highlighted region to `Macaulay2`.

`Macaulay2` can evaluate basic algebraic expressions:

```
i1 : 2 + 2

o1 = 4

i2 :
```

My first input was `2 + 2`, the first output was `4` (looks good), and `Macaulay2` is now waiting for the second input.

```
i2 : 2/3 + 6/11

     40
o2 = --
     33

o2 : QQ

i3 :
```

When we ask `Macaulay2` to add two fractions, we get two output lines: The first tells use the value of the input expression, which is $\frac{40}{33}$. The second output line, `o2 :  QQ`, is telling us the *type* of the output. In this case, it is a rational number.

Integers and rational numbers are multi-precision by default. We don't need to worry about overflow or rounding errors when we ask for 100! or the 100^{th} partial sum of the harmonic series:

```
i3 : 100!

o3 = 93326215443944152681699238856266700490715968264381621468592963895217599993229915608941463976156
     518286253697920827223758251185210916864000000000000000000000000

i4 : sum(toList(1..100) / (i -> (1/i)))

     14466636279520351160221518043104131447711
o4 = -----------------------------------------
      2788815009188499086581352357412492142272

o4 : QQ
```

However, real and complex numbers are inaccurate. If we take for example the complex number `i` and square it, we'll get -1: But if we raise it to the fourth power, we get a number which is extremely close to 1 but not equal to it:

```
i5 : ii^2
```

```
o5 = -1

o5 : CC (of precision 53)

i6 : ii^4

o6 = 1-2.44929359829471e-16*ii

o6 : CC (of precision 53)
```

This is not typically a big deal, especially since we'll often work in polyomial rings over finite fields we shouldn't expect any issues related to machine precision; but it's something to be aware of. Instead of just evaluating an expression, we can evaluate an expression and save the value to a symbol (any acceptable string):

```
i7 : val = 20!

o7 = 2432902008176640000

i8 : val^2

o8 = 5919012181389927685417441689600000000
```

Now for the rest of this `Macaulay2` session, we can use `val` whenever we need 20!. If the output is so long that you don't want it to be printed to the screen, you can end your input line with a semicolon `;`.

```
i9 : bigval = 500!;

i10 :
```

semicolons also allow you to evaluate multiple expressions in a single line:

```
i10 : a = 2 + 2; b = 6*a; c = a + b;

i13 : a + b + c

o13 = 56
```

We also have access to the previous three outputs using `oo`, `ooo`, and `oooo`. If you want to go further back to a particular output, like our `100!` from earlier, you can access it using `o3`.

```
i14 : length toString o3

o14 = 158
```

`Macaulay2` has plenty of build in rings and fields, for example

```
i15 : ZZ

o15 = ZZ

o15 : Ring
```

```
i16 : ZZ/101

       ZZ
o16 = ---
      101

o16 : QuotientRing

i17 : RR

o17 = RR

o17 : InexactFieldFamily
```

And we can use these rings and fields as the coefficients for our own, user-defined polynomial rings:

```
i18 : R = QQ[x,y,z]

o18 = R

o18 : PolynomialRing
```

Now that we've defined our own polynomial ring, `Macaulay2` can do arithmetic operations in R and will appropriately type the results as being elements of our ring:

```
i19 : (x + y)*(y + z^2)

         2      2           2
o19 = x*z  + y*z  + x*y + y

o19 : R
```

`Macaulay2` has plenty of built-in functions for working with polynomial rings. Some (unsurprising) facts about R can be obtained via:

```
i20 : gens R

o20 = {x, y, z}

o20 : List

i21 : isCommutative R

o21 = true
```

Polynomial rings in `Macaulay2` come with a monomial ordering. The default is `GRevLex` but it is possible to change it, if needed. Here we make a polynomial ring over a finite field, specify that we want to use the `Lex` monomial ordering, and sum to random homogeneous polynomials of degrees 2 and 1. `Macaulay2` will naturally print the output with ordered monomials. Now how `Lex` does not respect degree.

```
i22 : S = ZZ/41[x,y,z,MonomialOrder=>Lex]

o22 = S

o22 : PolynomialRing

i23 : f = random(2,S) + random(1,S)

          2                            2                         2
o23 = 13x  - 10x*y - 15x*z + 10x + 2y  - 20y*z + 4y - 14z  - 3z

o23 : S
```

4 January 16 – Introduction to Affine Algebraic Geometry

4.1 Affine Varieties

For a fixed (usually infinite) field k, we think of the ring $R = k[x_1, \ldots, x_n]$ as being the ring of functions on a particular geometric space, called affine n-space over k:

Definition 4.1. *Affine n-space over k* is the set

$$\mathbb{A}_k^n = \{(a_1, \ldots, a_n \mid a_i \in k)\}$$

of all n-tuples of elements of k. For a polynomial $f \in R = k[x_1, \ldots, x_n]$, we can think of f as a function $f : \mathbb{Q}_k^n \to k$, where to evaluate f at $(a_1, \ldots, a_n)$ we plug in a_i for each x_i and evaluate the resulting expression in k. One reason for insisting that k be a *infinite* field is because we want it to be true that f is the zero function on $\mathbb{A}_k^n$ if and only if f is the zero polynomial in R. This is only true if k is infinite.

Definition 4.2. The *vanishing locus* of a set of polynomials $S \subseteq R$, denoted $V(S)$, is the set of points in affine space where those polynomials simultaneously vanish.

$$V(S) = \left\{p \in \mathbb{A}_k^n \mid f(p) = 0 \text{ for all } f \in S\right\}$$

A subset of affine space which is of the form $V(S)$ for a set $S \subseteq R$ of polynomials is called an *affine variety.*

We note that for a set S of polynomials, $V(S)$ is the same as $V(I)$, where I is the ideal generated by S. As a consequence of this observation, and the fact that R is noetherian, we get that every affine variety X can be written as $X = V(f_1, \ldots, f_m)$, the vanishing locus of a finite set of polynomials.

Example 4.1. If we take the polynomial $y - x^2$ in the ring $\mathbb{R}[x, y]$, then the affine space in question is the usual plane $\mathbb{R}^2$, and the vanishing locus $V(y - x^2)$ is the familiar graph of the function $y = x^2$.

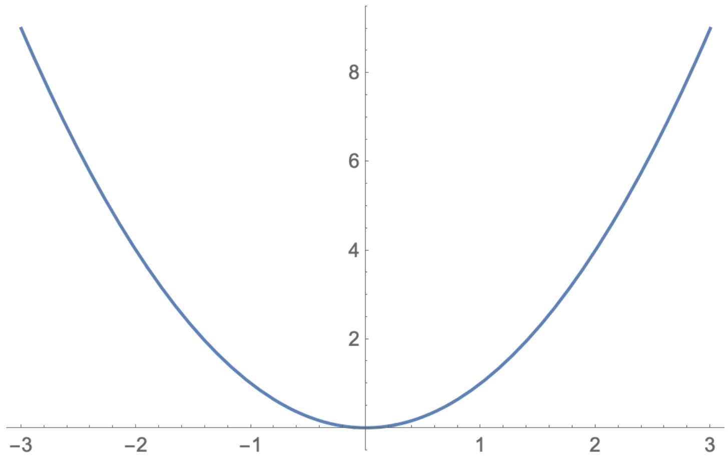
Theorem 4.1. Facts about affine varieties:

a. An arbitrary intersection of affine varieties is an affine variety.

b. A finite union of affine varieties is an affine variety.

c. $V(f_1, \ldots, f_m) = V(f_1) \cap \ldots \cap V(f_m)$.

Note that a. and b., together with the observation that the $\mathbb{A}_k^n$ and the empty set are affine varieties, imply that the affine varieties in $\mathbb{A}_k^n$ form the closed sets of a topology on affine n-space, which is called the *Zariski topology.*



V can be thought of as a function from the set of ideals in R to the set of affine varieties in $\mathbb{A}_k^n$. There's also a function from subsets of affine space to the set of ideals in R:

Definition 4.3. Let $X \subseteq \mathbb{A}_k^n$ be a subset of affine space. We denote by $\boldsymbol{I}$ the set of all functions in R that are identically zero on X:

$$\boldsymbol{I}(X) = \{f \in R \mid f(x) = 0 \text{ for all } x \in X\}$$

One readily checks that this is an ideal in R.

How do V and $\boldsymbol{I}$ interact?

Theorem 4.2.

a. For any ideal $I \subseteq R$, $\boldsymbol{I}(V(I)) = \sqrt{I} = \{f \in R \mid f^m \in I \text{ for some } m > 0\}$.

b. For any set $X \subseteq \mathbb{A}_k^n$, $V(\boldsymbol{I}(X)) = \overline{X}$, the closure of the set X in the Zariski topology mentioned in 4.1.

4.2 Groebner Bases and Elimination Ideals

5 January 18 – First `Macaulay2` Hands-On Session

Today's introduction to `Macaulay2` worksheet is summarized below, with together with my solutions to the problems.

5.1 Problem 1

a. Find the sum of all the multiples of 3 or 5 that are less than 1000. (Project Euler #1)

```
i1 : sum select(toList(1..999), p -> p%3 == 0 or p%5 ==0)

o1 = 233168
```

The expression `1..999` creates a sequence of the integers less than 1000, and `toList` converts it to a list. `select(L, f)` takes a list `L` and a (boolean-valued) function `f` and returns the list of all elements in `L` that satisfy `f(p) == true`. In this case, the function `p -> p%3 == 0 or p%5 ==0` returns true if and only if `p` is 0 (mod 3) or 0 (mod 5). Finally, `sum` adds the values in a list.

Note that while this problem can be done "better" using Gauss's formula for summing arithmetic progressions and inclusion-exclusion, but since `Macaulay2` has no trouble dealing with such short lists and such small sums, there's no reason to fret over efficiency here.

b. Find the sum of all the prime numbers that are less than 2 million. (Project Euler #10)

```
i2 : sum select(toList(2..2000000), isPrime)

o2 = 142913828922
```

Very similar to the approach to question a. It is worth noting that the syntax `sum select(toList(2..2000000), p -> isPrime p)` would also work, but since `isPrime` is a built-in function, `select` will treat it as such, without the need to wrap it in a function closure using the `->` syntax.

c. Find the sum of the digits of 100! (Project Euler #20)

```
i3 : 100! // toString // characters / value // sum

o3 = 648
```

Here we see two useful binary operators: `//` and `/`. The first is an alternative syntax for applying a function to an object. If `X` is a `Macaulay2` object, and `f` is a function that can be applied to it, then then all three of `f(X)`, `f X`, and `X // f` are acceptable ways to apply `f` to `X`. Similarly, if `L` is a list, and `f` is a function that can be applied to the elements of `L`, then `L / f` is the list obtained by applying `f` to the elements of `L`. This can also be achieved using `apply(L,f)`. It is worth noting that these expressions work with the arguments reversed if we also reverse the slashed used. So `X // f` is the same as `f \\ X`, and `L / f` is the same as `f \ L`.

For this problem, we take the integer `100!`, convert it to a string, get the list of characters of that string, get the value of each of those characters, and sum the resulting list.

d. What are the last ten digits of the integer $\sum_{n=1}^{1000} n^n$? (Project Euler #48)

```
i4 : (1..1000) // toList / (n -> powermod(n,n,10^10)) // sum % 10^10

o4 = 9110846700
```

Take the sequence of the first 1000 integers. Convert it to a list. To each element `n` of that list, compute $n^n \pmod{10^{10}}$, which gives the last 10 digits of that number. Sum the entries in the resulting list and reduce mod 10^{10} to get the last ten digits of the sum of those numbers.

It is worth noting that for this particular problem, using `powermod` may have been unnecessary. `powermod(a,b,n)` is a function that computes $a^b \pmod{n}$ without ever computing a^b. For example, if we ask for `powermod(3, 10^9, 126)`, we get the answer of `81` right away. But if we instead asked for `3^(10^9) % 126`, `Macaulay2` will not succeed. For this problem, the numbers may not have been big enough for the distinction to matter.

5.2 Problem 2

a. How many monomials of degree 100 are there in $k[x, y, z]$? If those monomials are listed in decreasing `GRevLex` order, which monomial is in the *middle* of the list?

First we create the polynomial ring in question. While `GRevLex` is the default monomial order in `Macaulay2`, we specify it here for clarity.

```
i5 : R = ZZ/101[x,y,z,MonomialOrder=>GRevLex]

o5 = R

o5 : PolynomialRing
```

Now we ask for a basis for the graded summand of R of degree 100. Note we end this line with a semicolon to prevent Macaulay2 from needlessly printing output.

```
i6 : B = basis(100,R);

              1       5151
o6 : Matrix R  <--- R
```

While the actual output o6 is suppressed, the line giving the type of the output is not, which lets us see that B is a matrix of size 1×5151, which tells us how many monomials of the chosen degree there are. To find the middle monomial of degree 100, we convert B to a list, sort the list, and (remembering that Macaulay2 indexes lists starting from 0, take the entry in position $\frac{5151-1}{2}$. To make sure this division returns an integer, we use // instead of /. We can't use a rational number as an index for an element of a list, even if we know that the rational number we're using is actually an integer; Macaulay2 will complain about the type mismatch.

```
i7 : (sort flatten entries B)_(5150//2)

      19 52 29
o7 = x  y  z

o7 : R
```

b. Find all rational roots of $y = x^7 - 903x^2 - 946x + 1848$.

```
i8 : R = QQ[x]

o8 = R

o8 : PolynomialRing

i9 : factor (x^7 - 903*x^2 - 946*x + 1848)

                               4     3      2
o9 = (x - 4)(x - 1)(x + 2)(x  + 3x  + 15x  + 55x + 231)

o9 : Expression of class Product
```

All we have to do find the rational roots of a (low degree) polynomial of one variable is factor it. (In fact, we only need to repeatedly apply the rational root test). We see that $x = -2, 1, 4$ are teh rational roots of this polynomial. If you want a challenge, try to think about how I might have used Macaulay2 to find a polynomial with specified rational roots but with few terms of high degree.

c. Use Gröbner bases and elimination ideals to find all solutions to the following system (typing it into `Macaulay2` is half the battle. Using `primaryDecomposition` is cheating!).

$$
\begin{aligned}
0 &= 3x^2 - 6x + y^2 + 2\\
0 &= -x^3 - 3x^2y + 5x^2 - 3xy^2 + 6xy - 8x - y^3 + 5y^2 - 2y + 2\\
0 &= 4x^2y - 3x^2 + 4xy^2 - 6xy + 2x - 3y^2 + 2y
\end{aligned}
$$

```
i10 : R = QQ[x,y,z]

o10 = R

o10 : PolynomialRing

i11 : f = 2 - 6*x + 3*x^2 + y^2

        2    2
o11 = 3x  + y  - 6x + 2

o11 : R

i12 : g = 2 - 8*x + 5*x^2 - x^3 - 2*y + 6*x*y - 3*x^2*y + 5*y^2 - 3*x*y^2 - y^3

         3     2         2    3     2             2
o12 = - x  - 3x y - 3x*y  - y  + 5x  + 6x*y + 5y  - 8x - 2y + 2

o12 : R

i13 : h = 2*x - 3*x^2 + 2*y - 6*x*y + 4*x^2*y - 3*y^2 + 4*x*y^2

        2        2     2             2
o13 = 4x y + 4x*y  - 3x  - 6x*y - 3y  + 2x + 2y

o13 : R

i14 : I = ideal(f,g,h);

o14 : Ideal of R
```

With the ideal in hand, we can ask for a Groebner basis. The generators with variables eliminated will be the generators of the appropriate elimination ideal

```
i15 : G = gb I

o15 = GroebnerBasis[status: done; S-pairs encountered up to degree 4]

o15 : GroebnerBasis
```

```
i16 : gens G

o16 = | 2y2-3x+1 2x2-3x+1 |

              1       2
o16 : Matrix R  <--- R
```

The fact that $2x^2 - 3x + 1$ is a generator tells us that the solutions to this system must have x-coordinates satisfying that equation:

```
i17 : factor (flatten entries oo)_1

o17 = (x - 1)(2x - 1)

o17 : Expression of class Product
```

so $x = 1$ or $x = \frac{1}{2}$. When $x = 1$ we see that the generators of the Groebner basis become:

```
i18 : sub(gens G, {x => 1})

o18 = | 2y2-2 0 |

              1       2
o18 : Matrix R  <--- R
```

which means $y = 1$ or $y = -1$. When $x = \frac{1}{2}$ the Groebner basis generators become:

```
i19 : sub(gens G, {x => 1/2})

o19 = | 2y2-1/2 0 |

              1       2
o19 : Matrix R  <--- R
```

which means $y = \frac{1}{2}$ or $y = -\frac{1}{2}$. So the (rational) solutions to this system are $(1, 1), (1, -1), (\frac{1}{2}, \frac{1}{2}), (\frac{1}{2}, -\frac{1}{2})$. For those interested, the graphs of the three generators of I are shown below. The four solutions are the four triple intersections.

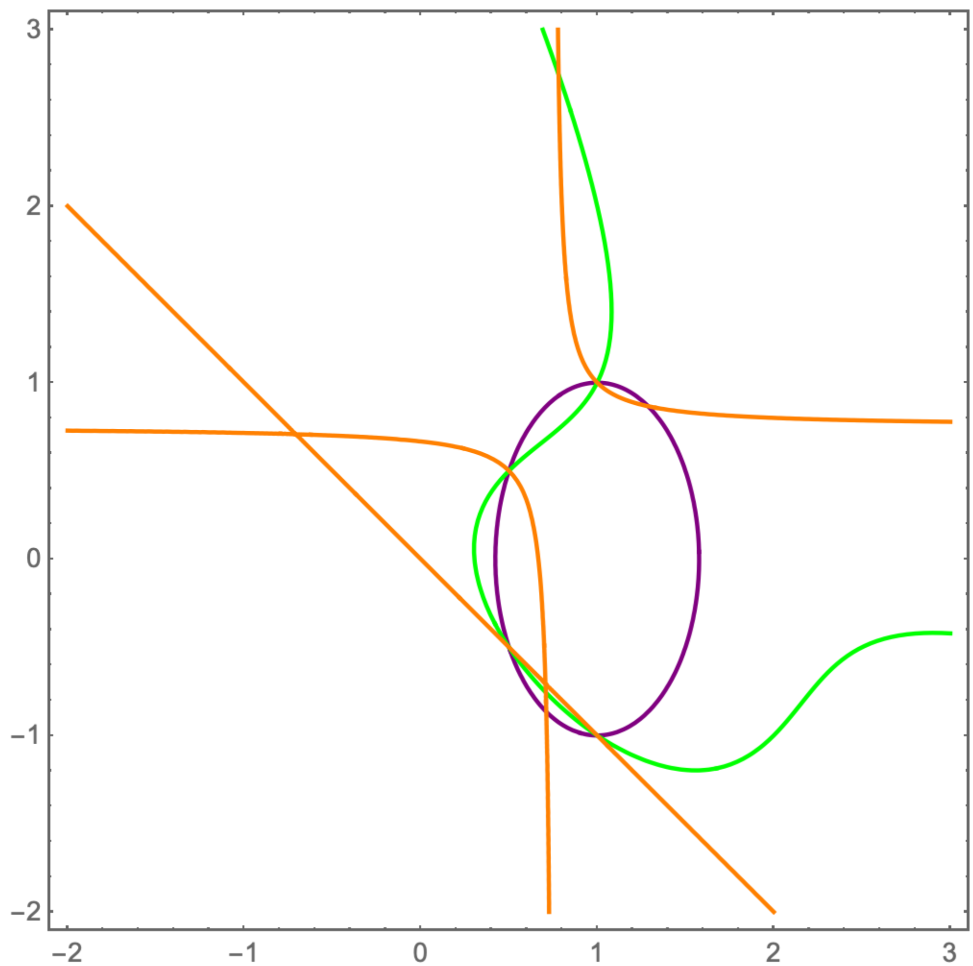
d. Find generators for a radical ideal I such that $V(I) \subseteq k^3$ is the union of the point $(1, 1, 2)$, the line parametrized by $r(t) = (t, 2t, 3t + 1)$, and the cylinder $z^2 + x^2 = 1$.

   Here, after defining the ring we'll work with, we will find the ideals defining the point, line and cylinder separately, intersect those ideals, and take the radical of the result. For the point, we take the ideal generated by three linear equations that vanish at the point. I made the natural choice:

```
i20 : R = QQ[x,y,z]

o20 = R

o20 : PolynomialRing
```




```
i21 : P = ideal(x - 1, y - 1, z - 2)

o21 = ideal (x - 1, y - 1, z - 2)

o21 : Ideal of R
```

For the ideal defining the line, we need the polynomial equations of two planes that vanish on the line.

```
i22 : L = ideal(2*x-y, 3*x - z + 1)

o22 = ideal (2x - y, 3x - z + 1)

o22 : Ideal of R
```

For the cylinder, we already have the equation of its defining ideal

```
i23 : C = ideal(x^2 + z^2 - 1)

              2    2
o23 = ideal(x  + z  - 1)

o23 : Ideal of R
```

Then to answer the question, we just intersect the ideals, take the radical of the result, and we're done (output suppressed because it's long, but we can get the generators of I if we need them.)

```
i24 : I = radical intersect(P,L,C);

o24 : Ideal of R
```

5.3 Problem 3

6 January 23 - R-modules

Definition 6.1. Let R be a commutative ring with 1. An R-*module* is an abelian group M together with a *scalar multiplication* map $R \times M \longrightarrow M$ with the properties that, for any $r, s \in R$ and $m, n \in M$ we have

i. $r(m+n) = rm + rn$

ii. $(r+s)m = rm + sm$

iii. $r(sm) = (rs)m$

iv. $1m = m$

If M is an R module and $\{m_1, \dots, m_d\} \subseteq M$ is a set of elements in M, then the *submodule generated by* $\{m_1, \dots, m_d\}$, denoted $\langle m_1, \dots, m_d\rangle$, is the set

$$\langle m_1, \dots, m_d\rangle = \left\{r_1 m_1 + \dots + r_d m_d \;\middle|\; r_i \in R, \text{ and all but finitely many are nonzero}\right\}$$

M is called *finitely generated* if it contains a finite set $\{m_1, \dots, m_d\}$ so that $\langle m_1, \dots, m_d\rangle = M$

Example 6.1. R is an R-module, and it is finitely-generated because $R = \langle 1\rangle$

Example 6.2. If I is ideal in R, then I can also be thought of as an R-module. If I is a noetherian ring, then every ideal I is finitely-generated as an R-module.

Example 6.3. If I is ideal in R, then the quotient ring R/I is an R-module. It is finitely generated by the class of 1 in the quotient ring.

Example 6.4. Let R^d denote the set of all $d \times 1$ matrices (column vectors) of elements of R. It is an abelian group with componentwise addition, and componentwise scalar multiplication by R makes R^d into an R-module. It is finitely generated by the standard basis vectors

$$e_1 = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{bmatrix}, \; e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \; \cdots, \; e_d = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{bmatrix}$$

and is called a *free R-module of rank d*

If the ring in question is actually a field k, then the k-modules from example 6.4 are just vector spaces, and up to isomorphism any finitely-generated k-modules is just k^n for some n. If R is not a field, then R-modules become a much richer object of study that can be thought of as a significant generalization of vector spaces.

Example 6.5. Let $R = k[x, y, z]$ and let M be the submodule of R^3 generated by

$$m_1 = \begin{bmatrix} y \\ -x \\ 0 \end{bmatrix}, \ m_2 = \begin{bmatrix} -z \\ 0 \\ x \end{bmatrix}, \ \cdots, \ m_3 = \begin{bmatrix} 0 \\ z \\ -y \end{bmatrix}$$

The set $\{m_1, m_2, m_3\}$ is a minimal generating set for M in the sense that no proper subset generates M. In fact, no set of 2 or fewer elements in M will generate M. While it might be tempting to think of this set as a *basis* for M, we notice that it doesn't really behave like a basis should: We can express $0 \in M$ as an R-linear combination of m_1, m_2 and m_3 in non-trivial ways. For example:

$$zm_1 + xm_2 + ym_2 = 0.$$

This gives an example of an important difference between vector spaces and general R-modules. Over a field k, all modules are free. But over a polynomial ring, this is not true. Furthermore, modules over the ring $\mathbb{Z}$ are ordinary abelian groups. While non-free abelian groups do exist (torsion), a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module will still be free. As the above example illustrates, this is not true for more general R-modules.

These facts about k-modules and $\mathbb{Z}$-modules can be restated in terms of *free resolutions*, and then generalized to R-modules.

Theorem 6.1. Let M be a finitely-generated k-module. Then there exists an exact complex of free k-modules $0 \to F_0 \to M \to 0$

This is trivial, of course, since M is already free we can just take $F_0 = M$ with any automorphism between them. But a "better" proof is to let B be any basis of M, let F_0 be the k-module with basis in bijective correspondence with B, and let $F_0 \to M$ be the linear map determined by sending the basis of F_0 to the corresponding elements of S. It is surjective by construction, and injective by linear algebra.

Theorem 6.2. Let M be a finitely-generated $\mathbb{Z}$-module. Then there exists an exact complex of free $\mathbb{Z}$-modules $0 \to F_1 \to F_0 \to M$ which is exact

Let $G = \{a_1, a_2, \ldots, a_g\}$ be a finite generating set for M, and let $\varphi_0 : \mathbb{Z}^g \to M$ be the $\mathbb{Z}$-module homomorphism determined by sending the standard basis for $\mathbb{Z}^g$ to the elements of G. This is surjective by construction, but it might have a kernel. However, $\ker(\phi_0)$ is a submodule of a free $\mathbb{Z}$-module, so it is also free (structure theorem for modules over a PID). So, letting $F_1 - \ker(\phi_0)$ and letting $\phi_1 : F_1 \to F_0$ be the inclusion homomorphism, we have constructed an exact complex of $\mathbb{Z}$-modules:

$$0 \to F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$$

It is worth noting that in both of the above examples, if we know the whole complex except for M, we can still recover M. In the abelian group setting, M is the cokernel of ϕ_1. In the vector space case, M is just F_0, which you can think of as the cokernel of the inclusion map $0 \to F_0$.

We want to generalize this to modules over the ring $R = k[x_1, \ldots, x_n]$, but first we'll add a bit of structure.

Definition 6.2. The ring R is *graded* by degree. It can be written as a direct sum of finitely-generated abelian groups

$$R = \bigoplus_{d \geqslant 0} R_d$$

where R_d is the free abelian (sub)group of R generated by all degree d monomials. The multiplication in R respects this grading, in the sense that the multiplication map $R \times R \to R$ descends to a map on graded pieces $R_s \times R_t \to R_{s+t}$. An R-modules M is called a *graded* R-module if M has a direct sum decomposition

$$M = \bigoplus_{d \geqslant 0} M_d$$

So that the R action $R \times M \to M$ descends to an action on graded pieces $R_s \times M_t \to M_{s+t}$. A *graded* homomorphism φ of graded R-modules M and N is one satisfying $\varphi(M_d) \subseteq N_d$ for all d.

This definition may seem artificial, but note that 6.1 and 6.4 are in fact graded modules. If I is an ideal generated by *homogeneous* polynomials, then 6.2 and 6.3 are also graded R-modules.

Theorem 6.3. *Hilbert Syzygy Theorem.* Let $R = k[x_1, \dots, x_n]$ and let M be a graded R-module. Then there exists an exact sequence of graded R-modules:

$$0 \to F_r \xrightarrow{\phi_r} F_{r-1} \xrightarrow{\phi_{r-1}} F_{r-2} \xrightarrow{\phi_{r-2}} \dots \xrightarrow{\phi_2} F_1 \xrightarrow{\phi_1} F_0 \xrightarrow{\phi_0} M \to 0$$

where:

- The F_i are all free of finite rank.

- The ϕ_i are all graded homomorphisms.

- $r \leqslant n$

7 January 25 - More on Graded Modules, Minimal Free Resolutions, Betti Numbers

Before we continue, it's worth noting that when we consider R-modules without thinking about the grading, there is only one (up to isomorphism) free R-module of rank 1, namely R. However, if we consider graded R-modules and graded isomorphisms, this is no longer true. If F is a free graded R-module of rank 1 with generated e, then as a set, F is the set $\{r \cdot e \mid r \in R$. If F' is another free R-module of rank 1 with generator e', then any isomorphism between them has to carry e to a unit multiple of e'. But (since units have degree 0) such a map can only be graded if e and e' have the same degree. So we end up with *different* graded free modules of rank 1, corresponding to the possible degrees of the generator. Such modules are useful when we're constructing free resolutions: Say I is an ideal generated by homogeneous polynomials f and g in R of degrees 2 and 3. Then if we want a free module that maps onto the kernel of the projection map $R \to R/I$, it will need to have one generator of degree 2 and one generator of degree 3 in order for the map to be graded.

Definition 7.1. With $R = k[x_1, \dots, x_n]$ with its standard grading, we use $R(-n)$ to denote the free R-module of rank 1 generated in degree n. More generally, if M is any graded R-module, we use $M(-n)$ to denote the "shifted" R module with graded pieces given by $M(-n)_d := M_{d-n}$.

In the example outlined above, a free resolution of R/I would begin:

$$R(-2) \oplus R(-3) \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

We are interested not just in the resolution guaranteed by the Hilbert Syzygy Theorem (which is both a resolution of finite length and is made up of finitely-generated free modules) but in fact we want the *minimal* such resolution. What does that mean? We hope it describes the result of the intuitive process. If M is a finitely generated R-module, then it has a (not unique) minimal generating set. If we take a surjective map from a free module with bases corresponding to those generators, that map's kernel has a (not unique) minimal generating set we can use to repeat this process.

But there's no guarantee that this intuitive process actually stops with a finite resolution. There's no guarantee that the choices you make in picking one generating set don't affect the size of the generating sets of the kernels later in the process, and there isn't even a guarantee that you couldn't pick a non-minimal generating set for M at the first step, leading to a later step where you get an even smaller generating set than you would have found if you'd started with a minimal generating set for M.

Luckily, none of these "problems" actually ever arise, but it's worth fretting about them momentarily in order to motivate a more precise definition of minimal

Definition 7.2. Let $\mathfrak{m}$ be the graded irrelevant ideal of R (the ideal generated by $(x_1, \dots, x_n)$), and consider a complex of R-modules $F_\bullet$:

$$\cdots \longrightarrow F_d \xrightarrow{\phi_d} F_{d-1} \longrightarrow \cdots$$

$F_\bullet$ is called *minimal* if the image of ϕ_d is contained in $\mathfrak{m}F_{d-1}$ for all d.

Theorem 7.1. $F_\bullet$ is minimal if and only if for all d, ϕ_d takes a basis for F_d to a minimal generating set of its image.

Proof: Consider the right exact sequence

$$F_d \xrightarrow{\phi_d} F_{d-1} \to \operatorname{im}(\phi_{d-1}) \to 0,$$

as well as the (still right exact) sequence obtained by applying the functor $- \otimes_R R/\mathfrak{m}$:

$$F_d \otimes_R R/\mathfrak{m} \xrightarrow{\phi_d \otimes_R R/\mathfrak{m}} F_{d-1} \otimes_R R/\mathfrak{m} \to \operatorname{im}(\phi_{d-1}) \otimes_R R/\mathfrak{m} \to 0,$$

which is best re-written as

$$F_d/\mathfrak{m}F_d \xrightarrow{\phi_d \otimes_R R/\mathfrak{m}} F_{d-1}/\mathfrak{m}F_{d-1} \to (\operatorname{im}(\phi_{d-1}))/\mathfrak{m}(\operatorname{im}(\phi_{d-1})) \to 0,$$

The complex is minimal if and only if $\phi_d \otimes_R R/\mathfrak{m}$ is the zero map (for all d) if and only if the surjective map in the above sequence is actually an isomorphism (for all d). But $(\operatorname{im}(\phi_{d-1}))/\mathfrak{m}(\operatorname{im}(\phi_{d-1}))$ is a vector space with dimension equal to the size of a minimal generating set for $\operatorname{im}(\phi_{d-1})$. So if the isomorphism above sends a basis for $F_{d-1}/\mathfrak{m}F_{d-1}$ to a basis $\bar{m}_1, \dots, \bar{m}_l$, which generate $(\operatorname{im}(\phi_{d-1}))/\mathfrak{m}(\operatorname{im}(\phi_{d-1}))$, which means (by Nakayama' s lemma) that $m_1, \dots, m_l$ generate $\operatorname{im}(\phi_{d-1})$ minimally

Note: the condition that the image of ϕ_d is contained in $\mathfrak{m}F_{d-1}$ is the same as saying that ϕ_d can also be expressed as a matrix of homogeneous elements in $\mathfrak{m}$.

They exist, any two of them are isomorphic by a chain complex isomorphism that is the identity on M, and any free resolution of M contains a copy of the minimal free resolution as a direct summand.

Example 7.1. Koszul complexes: Let $R = k[x, y, z]$. The ideal $I = (x)$ has minimal free resolution

$$0 \to R(-1) \xrightarrow{\begin{bmatrix} x \end{bmatrix}} R \to R/I \to 0$$

The ideal $J = (x, y)$ has minimal free resolution

$$0 \to R(-2) \xrightarrow{\begin{bmatrix} y \\ -x \end{bmatrix}} R^2(-1) \xrightarrow{\begin{bmatrix} x & y \end{bmatrix}} R \to R/J \to 0$$

And the ideal $K = (x, y, z)$ has minimal free resolution

$$0 \to R(-3) \xrightarrow{\begin{bmatrix} x \\ y \\ z \end{bmatrix}} R^3(-2) \xrightarrow{\begin{bmatrix} 0 & z & -y \\ -z & 0 & x \\ y & -x & 0 \end{bmatrix}} R^3(-1) \xrightarrow{\begin{bmatrix} x & y & z \end{bmatrix}} R \to R/K \to 0$$

These are examples of the koszul complex on a set $g_1, \dots, g_r \in R$. they give minimal free resolutions but only sometimes.

We haven't yet proven that minimal free resolutions exist, are unique up to chain complex isomorphism, and can be found as a direct summand of any free resolution. Postponing that for the moment, we introduce the *Betti numbers* of a finitely-generated graded R-module M, a numerical invariant of M which is determined by the minimal free resolution:

Definition 7.3. Let M be a finitely generated R-module, and let $F_\bullet$ be a minimal free resolution of M. The number(s) of degree j generators needed for F_i are called the graded betti numbers of M and are denoted $\beta_{i,j}$.

8 January 28 - Betti Diagrams, The Koszul Complex for $R/\mathfrak{m}$, Proof of Hilbert Syzygy Theorem

Last time we define the graded betti numbers of a (finitely-generated graded) R-module M: $\beta_{i,j}$ is the number of degree j generators in the i^{th} free module in a minimal free resolution of M. Now we prove the equivalence of a more homological definition:

Theorem 8.1. Let M be a finitely generated graded R-module and suppose $F_\bullet$ is a minimal free resolution of M. Then, in a minimal (homogeneous) generating set for F_i, there are exactly $\mathrm{Tor}_i^R(M, R/\mathfrak{m})_j$ generators of degree j. In other words,

$$\beta_{i,j} = \dim_k \left(\mathrm{Tor}_i^R(M, R/\mathfrak{m})\right)_j$$

Proof. $\mathrm{Tor}_i^R(M, R/\mathfrak{m})_j$ can be found by taking j^{th} graded piece of the i^{th} homology of the complex $F_\bullet \otimes_R R/\mathfrak{m}$. Since the complex $F_\bullet$ is minimal, after tensoring with $R/\mathfrak{m}$, all maps become zero maps. So the $\mathrm{i}^t h$ homology is just $F_i \otimes_R R/\mathfrak{m}$, and the dimension of the degree j component of this vector space is the number of generators of degree j that F_i has (again using Nakayama's lemma).

When we know the graded betti numbers of an R-module, we use *betti diagrams* to encode them: Note that while the columns correspond to homological degree, the rows do not correspond to generator degree; instead, there's a shift depending on homological degree: In column i, row j we put $\beta_{i,j+i}$. The reasons for this choice will be made clear later. Note that while any chain complex of graded free modules has a betti table, when we refer to the betti table of M, we mean the betti table of its minimal free resolution, which have the homological interpretation noted above.

	0	1	2
0	$\beta_{0,0}$	$\beta_{1,1}$	$\beta_{2,2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
j	$\beta_{0,j}$	$\beta_{1,j+1}$	$\beta_{2,j+2}$
$j+1$	$\beta_{0,j+1}$	$\beta_{1,j+2}$	$\beta_{2,j+3}$

Theorem 8.2. Fix M, R as above and fix a homological degree i. If there is a d so that $\beta_{i,j} = 0$ for $j < d$, then $\beta_{i+1,j+1} = 0$ for all $j < d$. In other words, if there's a zero in the Betti table of M that also has a column of zeros above it, then it has a rectangle of zeros above and to the right of it, going on forever.

Proof. By assumption, F_i has no generators (hence no elements at all) of degree less than d. Consider a generator of F_{i+1}. It has to map to something nonzero in $\mathfrak{m}F_i$ (if it maps to zero, the map to F_{i+1} has a unit in its matrix representation, contradicting minimality). Since all nonzero elements of $\mathfrak{m}F_i$ have degree $d+1$ or higher, the generator of F_{i+1} must also have degree $d+1$ or higher. So $\beta_{i+1,j+1} = 0$ is $j < d$

Example 8.1. Let $R = k[x, y, z]$ and let $I = (xy, yz)$. The minimal free resolution of I is

$$R/I \leftarrow R^1 \xleftarrow{\begin{bmatrix} xy & yz \end{bmatrix}} R^2(-2) \xleftarrow{\begin{bmatrix} z \\ -x \end{bmatrix}} R^1(-3) \leftarrow 0$$

This is the minimal free resolution, which shows that $\beta_{0,0} = 1$ (true for any quotient of R by a homogeneous ideal), $\beta_{1,2} = 2$, encoding the number of and degrees of a minimal generating set for I, and $\beta_{2,3} = 1 = 1$, encoding the only relation among the generators of I, namely that $z(xy) - x(yz) = 0$. The betti diagram of R/I is therefore

	0	1	2
0	1	-	-
1	-	2	1
2	-	-	-

Later we will see more Betti diagrams, learn about their geometric content, and see how to use `Macaulay2` to find them. But for now we'll introduce the Koszul complex and use it to prove a result about Betti numbers that implies the Hilbert Syzygy Theorem from earlier:

Definition 8.1. Consider $R = k[x_1, \dots, x_n]$ with $\mathfrak{m} = (x_1, \dots, x_n)$. Let F be the graded free module $R^n(-1)$ with bases $e_1, \dots, e_n$, and let $E = \bigwedge^\bullet F$, the exterior algebra on F. Then E itself is graded (since the degree of each e_i is 1, the degree of a wedge product $e_{i_1 \wedge \dots \wedge e_{i_d}}$ is just d), and the graded pieces of E form a chain complex which is a free resolution of $R/\mathfrak{m}$. Note that

$$E_0 = R$$
$$E_1 = F = \bigoplus_i R_{e_i}$$
$$E_2 = \bigoplus_{i<j} Re_i \wedge e_j$$
$$E_3 = \bigoplus_{i<j<k} Re_i \wedge e_j \wedge e_k$$
$$\vdots$$
$$E_n = Re_1 \wedge \dots \wedge e_n$$
$$E_{n+1} = 0$$
$$E_{n+2} = 0$$
$$\vdots$$

The R-module map $\partial : E_d \longrightarrow E_{d-1}$ defined on basis elements by

$$\partial(e_{i_1} \wedge \dots \wedge e_{i_d}) = \sum_{j=1}^{d} x_j e_{i_1} \wedge \dots \wedge \widehat{e_{i_j}} \wedge \dots e_{i_d}$$

Makes

$$\cdots E_{i+1} \to E_i \to E_{i-1} \to \cdots$$

into a chain complex of free R-modules. One can check that this is indeed a complex, and that it is exact except at E_0, where the homology is $R/\mathfrak{m}$. This gives us a free resolution of $k = R/\mathfrak{m}$

Theorem 8.3. Let M be a finitely generated R-module. The Betti numbers of M satisfy $\beta_{i,j} = 0$ if $i > n$. In other words, the minimal free resolution of M doesn't have nonzero terms in homological degrees greater than the number of variables in R.

Proof: Using the formula $\beta_{i,j} = \dim_k \left(\mathrm{Tor}_i^R(M, R/\mathfrak{m})\right)_j$, we note that we can compute Tor using a free resolution for M or a free resolution for $R/\mathfrak{m}$. If we use the Koszul complex for $R/\mathfrak{m}$, we start with a free resolution for $k = R/\mathfrak{m}$:

$$E_0 \xleftarrow{\partial} E_1 \xleftarrow{\partial} E_2 \leftarrow \cdots \leftarrow E_n \leftarrow 0$$

Applying the functor $M \otimes_R -$ we have

$$M \otimes_R E_0 \xleftarrow{M\otimes_R \partial} M \otimes_R E_1 \xleftarrow{M\otimes_R \partial} M \otimes_R E_2 \leftarrow \cdots \leftarrow M \otimes_R E_n \leftarrow 0$$

A not necessarily exact chain complex whose homology at the term $M \otimes E_i$ will compute the Tor we're interested in. This proves the statement above, but note that we can actually say a little more:

Instead of taking Tor and looking at the j^{th} graded piece, we can instead look at the degree j strand of this complex and look at the homology of that complex of vector spaces in homological degree i. Because we know the degrees of the E_i modules, the degree j strand of this complex will look like:

$$M_j \otimes_R E_0 \leftarrow M_{j-1} \otimes_R E_1 \leftarrow M_{j-2} \otimes_R E_2 \leftarrow \cdots \leftarrow M_{j-n} \otimes_R E_n \rightarrow 0.$$

The betti number $\beta_{i,j}$ is the dimension of the homology of this complex *of vector spaces* in homological degree i. The most this number could possibly be is the product of the ranks of the tensored vector spaces:

$$\beta_{i,j} \leqslant \dim_k(M_{j-i}) \cdot \binom{n}{i}$$

The function $d \mapsto$ the dimension of the degree d summand of M is called the *Hilbert Function* of M, and we'll talk about it next time.

9 January 30 - Projective Geometry, Hilbert Functions

Snow Day!

10 February 1 - Worksheet 2

a. Let ℓ_1, ℓ_2, ℓ_3 be three general homogeneous linear polynomials in $R = k[x_0, x_1, x_2]$, and let I be the ideal $(\ell_1\ell_2, \ell_1\ell_3, \ell_2\ell_3)$. Describe the projective variety $V(I) \subseteq \mathbb{P}^2_k$.

b. Let $\ell_1, \ell_2, \ell_3, \ell_4$ be four general homogeneous linear polynomials in $R = k[x_0, x_1, x_2]$, and let J be the ideal $(\ell_1, \ell_2\ell_3\ell_4)$. Describe the projective variety $V(J) \subseteq \mathbb{P}^2_k$.

c. Try to find the betti numbers of R/I and R/J, first by constructing minimal free resolutions by hand, then by checking your answers using `Macaulay2`.

d. Find the Hilbert Functions and Hilbert Polynomials of R/I and R/J. Explain the geometric significance of the difference in the Hilbert Functions.

a. Let $R = k[x_0, \ldots, x_n]$, and let M be a graded R-module. We've proven the Hilbert syzygy theorem, which says that M has a free resolution of length at most $n+1$. Now we'll prove a bound in the other direction. Prove that if $0 \leqslant m \leqslant n$ and M contains a submodule that is isomorphic to $R/(x_0, \ldots, x_m)$, then M does *not* have a free resolution of length less than $m + 1$.

b. Let $R = k[x_0, x_1, x_2, x_3]$ and let $I = (x_0, x_1) \cap (x_2, x_3)$. ($V(I)$ is two lines in $\mathbb{P}^3_k$ that don't intersect.) Prove that $I = (x_0x_2, x_0x_3, x_1x_2, x_1x_3)$, and compute the minimal free resolution of R/I. Why does your answer not contradict what was proven in 2a?

In `Macaulay2`, using the ideal I from question 2b, run the command `F = koszul gens I`. Now `F` is a chain complex in `Macaulay2`. You can look at the modules in the complex with `F_i`, you can look at the differentials in the complex with `F.dd_i`, and you can even see the betti table of the complex with the command `betti F`.

a. What can you say about this chain complex as it relates to I?

b. In class I claimed (without proof) that the minimal free resolution of any graded R-module M can be found as a subcomplex of any graded free resolution of M. Using degree considerations, prove that the minimal free resolution of R/I is *not* a subcomplex of `F`, and explain why this doesn't contradict my claim.

11 February 4

11.1 The Hilbert Function, Series, and Polynomial

With $R = k[x_1, \ldots, x_n]$ with the usual grading and M a finitely-generated graded R-module, we've seen that the minimal free resolution of M determines the graded Betti numbers of M. Today we'll see some coarser invariants of M that are determined by the graded Betti numbers (or by the minimal free resolution). Our eventual goal is an algorithmic computation of the minimal free resolution of M, which will give us computational access to all these other algebraic invariants.

Definition 11.1. Let M be a finitely-generated graded $R = k[x_1, \ldots, x_n]$-module. The *Hilbert Function* of M, denoted by H_M (or sometimes HF_M), is the function defined on any non-negative integer d by:

$$H_M(d) = \dim_k(M_d).$$

When I is an ideal in R, it is a common abuse of notation to say *the Hilbert function of I* to refer to the Hilbert function of R/I. Though, in light of example 11.1 below and the standard $0 \to I \to R \to R/I \to 0$ exact sequence of graded R-modules, the Hilbert functions of I as an R-module and of R/I are very closely related.

The hilbert function has geometric significance. For a very simple example, which we saw on the previous worksheet, let I be the ideal of a set X of points in $\mathbb{P}^2$. There is a 3-dimensional vector space of linear functions in $k[x_0, x_1, x_2]$. What is the dimension of the space of linear functions that vanish on X? It's the degree 1 component of R/I. If X consists of just 1 point, then $H_I(1) = 2$. If X consists of 2 points, then $H_I(1) = 1$. But when X is three points, the hilbert function $H_I(1)$ can be either 1 or 0. This is because if the three points are not collinear, there are no linear functions that vanish on all three. But if the three points are collinear, then there's a 1-dimensional vector space of linear functions that vanish on them: any scalar multiple of the equation of the line passing through all three points.

Example 11.1. The Hilbert function of the graded ring $R = k[x_0, \ldots, x_n]$ is given by

$$H_R(i) = \binom{n+i}{i}.$$

This is because R_i is spanned as a k-vector space by the set of degree i monomials in the $n+1$ variables of R. The number of such monomials is found using a "stars and bars" counting argument: A degree d monomial can be represented as a string of length $n+i$ made up of i stars and n bars. The continguous blocks of stars encode the powers on the different powers of the variables; the bars separate the blocks of stars to encode which power goes on which variable. The following string of length $10 + 7 = 17$

$$* * *| * *|| * *| * ||| * *$$

corresponds to the degree 10 monomial $x_0^3x_1^2x_3^2x_4x_7^2$. All strings encoding a degree i monomial in the variables $x_0, \ldots, x_n$ will be of length $n+i$, and the number of such strings is equal to the number of ways to choose which i of the $n+i$ characters will be stars.

Similarly, for the degree-shifted R-module $R(-d)$, the Hilbert function is

$$H_{R(-d)}(i) = \dim_k(R(-d)_i) = \dim_k R_{i-d} = H_R(i-d) = \binom{i-d+n}{i-d} = \binom{i-d+n}{n}.$$

It turns out that for large values of i, the Hilbert function $H_M(i)$ is equal to a polynomial $p(x) \in \mathbb{Q}[x]$ evaluated at i.

Theorem 11.1. Let M be a graded R-module. Then we can compute the Hilbert function of M in terms of a finite-length free resolution of M.

Proof. Suppose M has a free resolution of the form

$$0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_m \leftarrow 0,$$

and suppose further that each F_i is the finitely generated free R-module:

$$F_i = \bigoplus_j F(-a_{i,j})$$

for some integers $a_{i,j}$. Then if we look at the degree ℓ subcomplex of vector spaces and consider degrees, we see that

$$H_M(\ell) = \sum_{i=0}^{m}(-1)^{\ell} H_{F_i}(\ell) = \sum_{i=0}^{m}(-1)^i \sum_j H_{R(-a_{i,j})}(d) = \sum_{i=0}^{m}(-1)^i \sum_j \binom{\ell - a_{i,j} + n}{n}$$

Note that we didn't need the complex to be minimal, we just needed a finite-length free resolution comprised of finitely-generated R-modules.

Theorem 11.2. There is a polynomial $P_M(x) \in \mathbb{Q}[x]$ satisfying that for any $\ell \geqslant \max\{a_{i,j} - n\}$, we have $H_M(\ell) = P_M(\ell)$.

Proof. Note that

$$\binom{\ell - a_{i,j} + n}{n} = \frac{(\ell - a_{i,j} + n)(\ell - a_{i,j} + n - 1)(\ell - a_{i,j} + n - 2)\cdots(\ell - a_{i,j} + 1)}{n!}$$

is a polynomial with rational coefficients in the variable ℓ provided $\ell - a_{i,j} + n \geq 0$. So for values of ℓ satisfying $\ell \geqslant a_{i,j} - n$ for all $a_{i,j}$, the value of $H_M(\ell)$ is equal to the value of the polynomial given by the equation in the proof of 11.1.

Definition 11.2. The polynomial in 11.2 does not depend on the free resolution used in 11.1, because if two polynomials in $\mathbb{Q}[x]$ agree at infinitely many x-values, then they're the same polynomial. It is called the *Hilbert polynomial* of M

Theorem 11.3. The Betti numbers of M determine the Hilbert function.

Proof. If $\{\beta_{i,j}\}$ are the graded Betti numbers of M, a module over $R = k[x_0, \ldots, x_n]$, then let

$$B_j = \sum_{i \geqslant 0}(-1)^i \beta_{i,j}.$$

Using the minimal free resolution of M and continuing the expression in 11.1, we see that the Hilbert function of M is given by the formula

$$H_M(\ell) = \sum_{i=0}^{m}(-1)^i \sum_j \binom{\ell - a_{i,j} + n}{n} = \sum_j B_j \binom{\ell + n - j}{n}$$

This formula comes from "rearranging the expression" in 11.1, I don't see how. Something like: the first expression is taking the alternating sum over each F_i of a sum that has terms coming from each graded component of F_i. The second expression is a sum in each degree of the alternating sum of the dimension in that degree of each F_i. Unclear. Also, using this formula with j plugged in for ℓ, you get a recursive formula for B_j in terms of previous B_k via

$$B_j = H_M(j) - \sum_{k<j} B_k \binom{n + j - k}{n}$$

Definition 11.3. For M a finitely-generated graded $R = k[x_0, \ldots, x_n]$-module, the *Hilbert series* of M is the power series in the variable t given by

$$HS_M(t) = \sum_{d=0}^{\infty} H_M(d)t^d$$

The Hilbert series is a rational function, since it is a power series with coefficients eventually given by a polynomial.

All of these are computationally accessible if we have a minimal free resolution of M. Next time we'll talk about algorithms to find the minimal free resolution.

12 February 6 - Algorithms for minimal free resolutions

Our current goal is to describe explicit algorithms for computing minimal free resolutions for finitely-generated graded $k[x_1, \ldots, x_n]$-modules. Our primary resource for this discussion is the paper "Strategies for Computing Minimal Free Resolutions" by La Scala - Stillman [make second bib.]. There's a little bit of setup needed first, where we extend our notions of monomial orderings to apply to more general rings and modules. (Some of this will not be necessary, strictly speaking, but by doing it we'll end up with a class of algorithms that can compute free resolutions for modules over a more general class of rings.) Then we'll see some algorithmic computations of free resolutions over R (and over more general rings). Finally, we'll see some ways to improve efficiency and performance.

12.1 More general terms orders:

For all of what follows, let $R = k[x_1, \ldots, x_n]$ and fix a monomial ordering $>$ on R. When $S = R/J$ is a quotient of R by an ideal J, then let N be the k-vector space spanned by the set of *standard monomials* in R, which is the set of monomials that are not in the initial ideal of J. Any element f in the quotient ring S can be written in a unique way as the coset of J represented by an element of $g \in N$, and we define *leading term, coefficient and monomial* of f to be the corresponding leading thing of the unique representative g.

For any subset G of the quotient ring S, we will use $\mathrm{in}(G)$ for the k-vector space of initial monomials of elements of S. Note that $\mathrm{in}(S) = N$, and as vector spaces we have a decomposition $R = N \oplus \mathrm{in}(J)$

If F is a free S-module with a chosen basis $\mathcal{E}$, we use $\widehat{F}$ to denote the free R-module with basis $\widehat{\mathcal{E}}$ in natural correspondence with the basis of F.

Definition 12.1. A *monomial* in F is an element $n \cdot e \in F$, where $n \in N$ is a standard monomial, and $e \in \widehat{\mathcal{E}}$ is a basis element for $\widehat{F}$. (Note that "a monomial of F" is in fact an element of the free R-module $\widehat{F}$. This is similar to the way elements of S can be expressed in a canonical way using elements of R)

A *term order* on F is a total order on the monomials of F satisfying that for any monomials $m_1 = n_1 \cdot e_1$ and $m_2 = n_2 \cdot e_2$ in F, basis vector $e \in \widehat{\mathcal{E}}$ and for any ordinary monomials $s, t \in R$

a. $m_1 > m_2 \Rightarrow tm_1 > tm_2$

b. $s > t \Rightarrow s \cdot e > t \cdot e$

Once we've fixed a term order on F, and element $f \in F$ can be written uniquely as the image of an element $\widehat{f} \in \widehat{F}$ of the form

$$\widehat{f} = c_1 \cdot m_1 + \ldots + c_k \cdot m_k$$

where the coefficients c_i are in k and the m_i are monomials. the lets us define the leading coefficient, leading term, and leading monomial (leading power product) of $f \in F$ as you'd expect: The leading coefficient of f is c_1. The leading monomial of f is m_1 (which, recall, is a standard monomial in $n \in N$ times a basis vector in $\widehat{e} \in \widehat{E}$), and the "leading power product" is n

What good is this generalization of monomial orderings to free modules over quotients of R? There are two reasons: One is that it gives you a generalization of Gröbner basis: For a submodule K of F, a subset $G = \{g_1, \ldots, g_s\} \subseteq K$ is a Gröbner basis for K if the initial monomials of the elements of G generate $\text{in}(K)$. This allows us to algorithmically check the "submodule membership" question, similar to the ideal membership question from befow.

Additionally, given an tuple $(f_1, \ldots, f_m) \in F$, Gröbner bases will allow us to compute generators for the module of Syzygies for this tuple, which (as we'll see) is relevant to the task of computing free resolutions.

Definition 12.2. Let $(f_1, \ldots, f_m) \in F$ be a tuple of elements in a free S-module. Then the *(first) module of syzygies* of this tuple is the set of all column vectors $(a_1, \ldots, a_m)^\top \in S^m$ satisfying $a_1 f_1 + \ldots + a_m f_m = 0 \in F$. It is denoted $\text{Syz}(f_1, \ldots, f_m)$.

Finding generating sets, (especially minimal generating sets) for the module of syzygies is significant because of its relation to building a free resolution: If $\cdots \leftarrow F_{i-1} \xleftarrow{\varphi_i} F_i$ is the beginning of a free resolution, then the standard basis for F_i is mapped by φ_i to an ordered tuple of generators of the image of φ_i. Loosely speaking, the generators of the module of syzygies for this tuple will be columns in the matrix defining φ_{i+1}. (Proofs and whatnot postponed until later)

13 February 8

13.1 Schreyer Resolutions and Schreyer Frames

Last time we talked about how, given a monomial ordering on R, we get to define leading (term / coefficient / monomial) for elements of R, R/J, $\widehat{F}$ and F. However, it's not necessarily the case that S will get a "monomial ordering" (as defined last time when $F = S^1$) just by using the ordering from R on standard representatives. By way of example (from Chris), consider the `GrLex` ordering on $R = k[x, y]$ and the ideal $J = (xy - 1)$. The standard monomial basis for R/J are just the powers of x and the powers of y, $\{1, x, y, x^2, y^2, \ldots\}$, since the initial ideal of J is (xy). However, in S we can consider the elements $\overline{x} > \overline{y}$. Multiplying both of these elements by x, we end up with $\overline{xy} > \overline{y^2}$, but after rewriting using standard monomials we have $\overline{1} > \overline{y^2}$. This means `GRLex` does not descend to a monomial ordering on the R/J.

However, it is worth noting that before we quotient, free modules over R *do* inherit a monomial order from the order on R: Namely, choose an ordering $e_1 > e_2 > \ldots > e_n$ and compare monomial summands in this order.

With the same $S = R/J$ as before, consider a complex of free S-modules:

$$F_\bullet = F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} F_2 \leftarrow \cdots F_{i-1} \xleftarrow{\varphi_i} F_i \leftarrow \cdots$$

Where each F_i has a canonical basis $\mathcal{E}_i$

Definition 13.1. A sequence $\{\tau_0, \tau_1, \ldots\}$ of term orders (on $F_0, F_1, \ldots$ respectively) on the modules of $F_\bullet$ is called a *term ordering* on $F_\bullet$ if for any $e_1, e_2 \in \mathcal{E}_i$ and any $s, t \in R$ (or in S??) we have

$$s \cdot \mathrm{lm}(\varphi_i(e_1) > t \cdot \mathrm{lm}(\varphi_i(e_2) \Rightarrow s \cdot e_1 > t \cdot e_2.$$

Given a term ordering on F_{bullet}, we defined the initial terms of $F_\bullet$, denoted $\mathrm{in}(F_\bullet)$, to be the complex with the same modules as $F_\bullet$ but with different maps:

$$\mathrm{in}(F_\bullet) = F_0 \xleftarrow{\xi_1} F_1 \xleftarrow{\xi_2} F_2 \leftarrow \cdots F_{i-1} \xleftarrow{\xi_i} F_i \leftarrow \cdots$$

where ξ_i is the map defined by sending any basis element $e \in \mathcal{E}_i$ to the initial monomial of $\varphi_i(e)$. I think this is the same as taking the matrix representations of the maps in $F_\bullet$ and, thinking of the columns as the generators of the image of φ_i, replace those columns with their initial monomials.

Definition 13.2. For M and S-module, a complex of free S-modules

$$F_\bullet = F_0 \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} F_2 \leftarrow \cdots F_{i-1} \xleftarrow{\varphi_i} F_i \leftarrow \cdots$$

together with a term ordering $\{\tau_0, \tau_1, \ldots\}$ is called a *Schreyer resolution* for M if:

i. $F_\bullet$ is exact.

ii. $\mathrm{coker}(\varphi_1) = M$.

iii. The image of $\varphi_i(\mathcal{E}_i)$ is a Gröbner basis for the image of φ_i.

Definition 13.3. For an S-module M, a sequence

$$\Xi_\bullet = F_0 \xleftarrow{\xi_1} F_1 \xleftarrow{\xi_2} F_2 \leftarrow \cdots F_{i-1} \xleftarrow{\xi_i} F_i \leftarrow \cdots$$

together with a term ordering $\{\tau_0, \tau_1, \ldots\}$ is called a *Schreyer frame* for M if:

i. Each column of each matrix ξ_i is a monomial.

ii. $M = F_0/K$ for some submodule K, and $\xi_1(\mathcal{E}_1)$ is a minimal set of generators for $\mathrm{in}(K)$.

iii. $\xi_i(\mathcal{E}_i)$ is a minimal set of generators for the kernel of ξ_{i-1} for all $i \geqslant 2$

If $F_\bullet$ is a Schreyer resolution for M, then $\mathrm{in}(F_\bullet)$ is a Schreyer frame for M. But you can also construct a Schreyer resolution for M starting from a Schreyer frame. So how do we find a Schreyer frame for M?

a bit of notation first: For a given Schreyer frame, we let $\mathcal{B}_i$ be the image of $\mathcal{E}_i$ under ξ_i. For a basis element $e \in \mathcal{E}_{i-1}$, we let $\mathcal{E}_i(e)$ be the (possibly empty) set $\{\varepsilon \in \mathcal{E}_i \mid \xi_i(\varepsilon) = t \cdot e\}$ where t is a monomial (power product) in S.

LEMMA 3.5 AND ITS PROOF (tells you an algo to compute a schreyer frame based on one map, presumably the presentation map for M?)

14 February 11 - Example of Computing a Schreyer Frame

Our goal for today is to understand the definitions and claimed results from last week with an explicit example.

Example 14.1. Let $R = k[x, y, z]$ with the `GrLex` monomial ordering. Then the free module R^3 with standard basis $\{e_1, e_2, e_3\}$ can be given the *term over position up* term order, defined by

$$m_i \cdot e_i > m_j \cdot e_j \Leftrightarrow m_i > m_j \text{ or } m_i = m_j \text{ and } i > j.$$

Under this term ordering, the initial term of $(x^2+y^2)\cdot e_1+(x^2+xy)\cdot e_2+z^2\cdot e_3$ would be $x^2\cdot e_2$. Now, consider the map φ to R^3 from R^5 shown below, where R^4 has standard basis $\{\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4,\epsilon_5\}$.

$$R^3 \xleftarrow{\varphi = \begin{bmatrix} x^2+yz & x^2+y^2 & x^2y & xy & x \\ y^2 & x^2+xy & x^2z & xz & z \\ x^2+z^2 & z^2 & y^2z & y^2 & y \end{bmatrix}} R^5$$

We note that, if we want a term order on this *complex*, we can't just put the term over position up ordering on R^5. This is because the compatibility condition

$$m_i\cdot(\mathrm{in}(\varphi(\epsilon_i))) > m_j\cdot(\mathrm{in}(\varphi(\epsilon_j))) \Longrightarrow m_i\cdot\epsilon_i > m_j\cdot\epsilon_j$$

is not satisfied. For example, consider $x\cdot\epsilon_2$ and $x\cdot\epsilon_1$. Applying φ and taking initial terms we see that

$$x\cdot\mathrm{in}(\varphi(\epsilon_1)) = x^3\cdot e_3$$
$$x\cdot\mathrm{in}(\varphi(\epsilon_2)) = x^3\cdot e_2$$

and so $x\cdot\mathrm{in}(\varphi(\epsilon_1)) > x\cdot\mathrm{in}(\varphi(\epsilon_2))$, which necessitates the comparison in $x\cdot\epsilon_1 > x\cdot\epsilon_2$, which contradicts term over position up order on R^5. But we can always come up with a compatible term ordering. Consider the initial terms of φ (We're not going in circles here: to take the initial terms of a complex, you only need a term ordering on the codomain of every map)

$$R^3 \xleftarrow{\mathrm{in}(\varphi) = \begin{bmatrix} 0 & 0 & x^2y & xy & x \\ 0 & x^2 & 0 & 0 & 0 \\ x^2 & 0 & 0 & 0 & 0 \end{bmatrix}} R^5$$

First, place a total order on each of the subsets of $\{\epsilon_1,\epsilon_2,\epsilon_3,\epsilon_4,\epsilon_5\}$ that get sent to multiples of a particular element of $\{e_1,e_2,e_3\}$ by $\mathrm{in}(\varphi)$. In this case, we can order $\{\epsilon_5>\epsilon_4>\epsilon_3\}$, and there are no choices to be made for $\{\epsilon_2\}$ or $\{\epsilon_1\}$. Now, define an term ordering on R^5 by

$$m_i\cdot\epsilon_i > m_j\cdot\epsilon_j \Longleftrightarrow m_i\mathrm{in}(\varphi(\epsilon_i)) > m_j\mathrm{in}(\varphi(\epsilon_j)) \text{ or } m_i\mathrm{in}(\varphi(\epsilon_i)) = m_j\mathrm{in}(\varphi(\epsilon_j)) \text{ and } \epsilon_i>\epsilon_j \text{ in the chosen total order.}$$

Now that we have an term order for the two-term complex defined by φ, the kernel of $\mathrm{in}(\varphi)$ is some submodule of R_4. We want a minimal generating set for the initial submodule of this kernel, using the lemma from the end of Friday's class.

Consider $f\in\ker(\mathrm{in}(\varphi))$. The only possible ϵ_1 coefficient is 0. Similar for ϵ_2. However, all three of ϵ_3,ϵ_4 and ϵ_5 are sent to monomial multiples of e_1, so the kernel can have nonzero coefficients on these basis elements. Suppose $f=p_3\epsilon_3+p_4\epsilon_4+p_5\epsilon_5$, and its image under $\mathrm{in}(\varphi)$ is $(x^2yp_3+xyp_4+xp_5)e_1=0$. It can't be the case that $p_3\neq 0$ while $p_4=p_5=0$. If p_3 is nonzero then so is at least one of p_4 and p_5, and since f is in the kernel of $\mathrm{in}(\varphi)$, this means any monomial $m\cdot e_1$ in $\mathrm{in}(\varphi)(p_3\epsilon_3)$ is cancelled by a term from $\mathrm{in}(\varphi)(p_4\epsilon_4)$ or $\mathrm{in}(\varphi)(p_5\epsilon_5)$. By our definition of the term order on R^5, this means the initial term of f can't be a multiple of ϵ_3 (This is why the inner union in the lemma starts at $j=2$.

If $p_5=0$, then any monomial in p_4 has to have the property that, after you multiply by xy, it is in the ideal generated by x^2y. In otherwords, any monomial in p_4 (and hence the coefficient on the initial term of f) is in the ideal $(x^2y:xy)=(x)$, and any minimal generator of this ideal shows up as the initial term of some $f\in\ker(\mathrm{in}(\varphi))$. So $x\cdot\epsilon_4$ is a generator of the initial module of the kernel of the initial terms of φ

If $p_5\neq 0$, then any monomial in p_5 has to have the property that, when you multiply it by x, it's in the ideal (x^2y,xy). In other words, the initial monomial of f is a multiple of ϵ_5 by an element of $(x^2y,xy):(x)=(xy:x)=(y)$. So $y\cdot\epsilon_5$ is a generator of the initial module of the kernel of the initial terms of φ. And that's all.

Re-stating the result from the end of lecture 13 in this context (without a quotienting ideal):

Theorem 14.1. Let $R = k[x_1, \ldots, x_n]$ be a polynomial ring with monomial order $>$, and consider a two-term complex of free R-modules

$$F_0 \xleftarrow{\xi_1} F_1$$

with monomial columns, and with a chosen term order on F_0. Let $\{e_1, \ldots, e_n\}$ be the canonical basis for F_0 and let $\epsilon_1, \ldots, \epsilon_m$ be the canonical basis for F_1. For each e_i, let $X_i = \{\epsilon_{i_1}, \ldots, \epsilon_{i_{r_i}}\}$ be the (possibly empty) set of basis elements of F_1 which are mapped by xi_1 to monomial multiple of e_i.

a. Choosing a total order $B_i = \{\epsilon_{i_1} < \cdots < \epsilon_{i_{r_i}}\}$ determines a total order on the complex $F_\bullet$

b. The minimal generating set of $\mathrm{in}(\ker(\xi_1))$ is the following:

$$\bigcup_{e_i} \bigcup_{\substack{\epsilon_{i_j} \in B_i \\ j \geqslant 2}} \left\{ m \cdot \epsilon_{i_j} \;\middle|\; m \text{ is a minimal generator of } (I_{i,j-1} : c_{i_j}) \right\}$$

Here c_{i_j} is the monomial coefficient on $\xi(\epsilon_{i_j})$, and $I_{i,j}$ is the monomial ideal $I_{i,j} = (c_{i_1}, c_{i_2}, \ldots, c_{i_j})$

Now, suppose M is a finitely-generated R-module, so that M is a quotient of a finitely-generated free R-module F_0 by an R-submodule N. We can compute a Schreyer frame for M by the following procedure:

1. Consider a map $F_0 \xleftarrow{\varphi_1} F_1$ presenting M.
2. Put a term order on F_0 (term over position up is fine) and let $\xi_1 = \mathrm{in}(\varphi_1)$.
3. Apply 14.1 to the complex $F_0 \xleftarrow{\xi_1} F_1$. This gives us a term order on F_1 and a minimal generating set for $\mathrm{in}(\ker(\xi_1))$.
4. Use this minimal generating set to construct $F_1 \xleftarrow{\xi_2} F_2$, a monomial map that surjects onto $\mathrm{in}(\ker(\varphi))$.
5. Repeat as many times as needed.

This gives us a Schreyer frame for M. Next time, we'll talk about how to fill in a Schreyer frame to get a Schreyer resolution for M, and eventually how to use the Schreyer resolution to get a minimal free resolution.

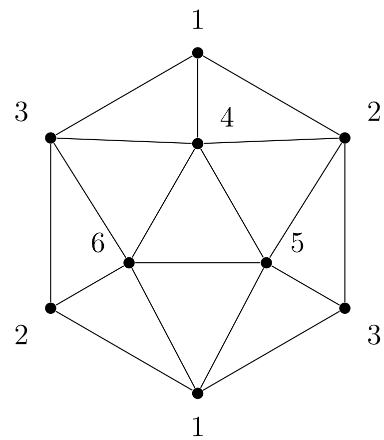
15 February 13 - Example of Computing a Schreyer Resolution

Now that we know how to compute a Schreyer frame for a given R-module M, we want to see how to fill it in to get a Schreyer resolution for M. Once again we'll accomplish this via an example.

Example 15.1. Let Δ be the simplicial complex attained by triangulating $\mathbb{RP}^2$ as shown below: Note the identifications made on the boundary. Δ has 6 vertices, 15 edges and 10 triangles. Let $R = k[x_1, x_2, x_3, x_4, x_5, x_6]$ with variable corresponding to the vertices of Δ. We will consider the *Stanlei-Reiser ideal* $I_\Delta \subseteq R$ of Δ, which is the ideal generated by the squarefree monomials corresponding to subsets of $\{1, 2, 3, 4, 5, 6\}$ that are *not* faces of Δ.

With the simplicial complex above, we have

$$I_\Delta = (x_3x_5x_6, x_2x_5x_6, x_2x_4x_6, x_1x_4x_6, x_1x_3x_6, x_3x_4x_5, x_1x_4x_5, x_1x_2x_5, x_2x_3x_4, x_1x_2x_3)$$



There's a map of free modules with cokernel R/I_Δ

$$R \xleftarrow{\xi_1=\begin{bmatrix} x_3x_5x_6 & x_2x_5x_6 & x_2x_4x_6 & x_1x_4x_6 & x_1x_3x_6 & x_3x_4x_5 & x_1x_4x_5 & x_1x_2x_5 & x_2x_3x_4 & x_1x_2x_3 \end{bmatrix}} R^{10}$$

Where R^{10} has standard basis vectors $\{\epsilon_1, \dots, \epsilon_{10}\}$ sent to the generators of I_Δ. Note that this is already a monomial map; nothing changes when we take initial terms. Furthermore, all basis elements of R^{10} are sent to monomial multiples of the same (only) basis element of R. So we impose a term order on R by choosing a total order, such as $\{\epsilon_1 < \dots < \epsilon_{10}\}$.We can use the result from last class to find minimal generators for the initial module of the kernel of this map. It will be minimally generated by $m \cdot \epsilon_2$ where m is a minimal generator of $(x_3x_5x_6) : (x_2x_5x_6) = (x_3)$. And $m \cdot \epsilon_3$ where m is a minimal generator of $(x_3x_5x_6, x_2x_5x_6) : (x_2x_4x_6) = (x_5)$. We can keep going like this but I'd prefer to use Macaulay2.

```
i1 : R = ZZ/101[x_1..x_6]

o1 = R

o1 : PolynomialRing

i2 : I = ideal(x_3*x_5*x_6,x_2*x_5*x_6,x_2*x_4*x_6,x_1*x_4*x_6,x_1*x_3*x_6,
          x_3*x_4*x_5,x_1*x_4*x_5,x_1*x_2*x_5,x_2*x_3*x_4,x_1*x_2*x_3)

o2 = ideal (x x x , x x x , x x x , x x x , x x x , x x x , x x x , x x x , x x x , x x x )
             3 5 6   2 5 6   2 4 6   1 4 6   1 3 6   3 4 5   1 4 5   1 2 5   2 3 4   1 2 3

o2 : Ideal of R

i3 : toList(1..9) / (i -> (i+1,(ideal (flatten entries gens I)_(toList(0..(i-1))):ideal(I_(i)))))

o3 = {(2, ideal x ), (3, ideal x ), (4, ideal (x , x x )), (5, ideal (x , x )), (6, ideal x ), (7,
                 3              5               2   3 5                5   4               6
     ----------------------------------------------------------------------------------------------
     ideal (x , x )), (8, ideal (x , x )), (9, ideal (x , x )), (10, ideal (x , x , x ))}
             6   3                6   4                6   5                 6   5   4

o3 : List
```

This tells us that in(ker(φ)) is minimally generated by the 16 elements

$$\{x_3\epsilon_2, x_5\epsilon_3, x_2\epsilon_4, x_3x_5\epsilon_4, x_5\epsilon_5, x_4\epsilon_5, x_6\epsilon_6, x_6\epsilon_7, x_3\epsilon_7, x_6\epsilon_8, x_4\epsilon_8, x_6\epsilon_9, x_5\epsilon_9, x_6\epsilon_{10}, x_5\epsilon_{10}, x_4\epsilon_{10}\}$$

which we can represent with the matrix

$$R^{10} \xleftarrow{\xi_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_2 & x_3x_5 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & x_5 & x_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_6 & x_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_6 & x_4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_6 & x_5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_6 & x_5 & x_4 \end{bmatrix}} R^{16}$$

Where R^{16} has standard basis $\{\beta_1, \ldots, \beta_{16}\}$. As discussed previously, we can define a term order on R^{16} which is compatible with the complex we're building simply by assigning (arbitrary) total orderings as follows:

$$\{\beta_1\}, \{\beta_2\}, \{\beta_3 < \beta_4\}, \{\beta_5 < \beta_6\}, \{\beta_7\}, \{\beta_8 < \beta_9\}, \{\beta_{10} < \beta_{11}\}, \{\beta_{12} < \beta_{13}\}, \{\beta_{14} < \beta_{15} < \beta_{16}\}.$$

Once these orders are chosen, we can find the initial module of the kernel of this map by again using the method described on Monday. This one is small enough to not need `Macaulay2`. Our generators will be

any minimal generator of $(x_2 : x_3x_5) = (x_2)$ times β_4

any minimal generator of $(x_5 : x_4) = (x_5)$ times β_6

any minimal generator of $(x_6 : x_3) = (x_6)$ times β_9

any minimal generator of $(x_6 : x_4) = (x_6)$ times β_{11}

any minimal generator of $(x_6 : x_5) = (x_6)$ times β_{13}

any minimal generator of $(x_6 : x_5) = (x_6)$ times β_{15}

any minimal generator of $(x_6, x_5 : x_4) = (x_6, x_5)$ times β_{16}

So our minimal generators are $\{x_2\beta_4, x_5\beta_6, x_6\beta_9, x_6\beta_{11}, x_6\beta_{13}, x_6\beta_{15}, x_6\beta_{16}, x_5\beta_{16}\}$. So the next map in our complex should be

$$R^{16} \xleftarrow{\xi_3=\begin{bmatrix} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ x_2&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&x_5&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&x_6&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&x_6&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&x_6&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&x_6&0&0\\ 0&0&0&0&0&0&x_6&x_5 \end{bmatrix}} R^8$$

And if R^8 has basis $\{\gamma_1, \dots, \gamma_8\}$, the initial submodule of the kernel of this map will be minimally generated by one element, $x_6\gamma_8$. The map

$$R^8 \xleftarrow{\xi_4=\begin{bmatrix} 0\\0\\0\\0\\0\\0\\0\\x_6 \end{bmatrix}} R^1,$$

where R^1 has basis δ_1, is injective. This finishes the computation of the Schreyer frame for I_Δ:

$$R^1 \xleftarrow{\xi_1} R^{10} \xleftarrow{\xi_2} R^{16} \xleftarrow{\xi_3} R^8 \xleftarrow{\xi_4} R^1$$

With this very explicit example in hand, our goal is to complete this frame to a Schreyer resolution. First note that this Schreyer frame is *graded*, with $\epsilon_1, \dots, \epsilon_{10}$ all having degree 3, β_i having degree 4 for all i except $i = 4$, since β_4, has degree 5. γ_i has degree 5 for all i except $i = 1$, since γ_1 has degree 6 Finally, δ_1 has degree 6.

We'll introduce a little bit of notation before proceeding. Let B_i be the monomial basis of the image of ξ_i (i.e. the columns of ξ_i), and let $\mathcal{B}$ be the union of all B_i. An element $m \in \mathcal{B}$ is said to have *level* i if $m \in B_i$.

Impose a total order on $\mathcal{B}$ as follows: $m < n$ if $\deg(m) < \deg(n)$ or $\deg(m) = \deg(n)$ and $\text{level}(m) > \text{level}(n)$, or $\deg(m) = \deg(n)$ and $\text{level}(m) = \text{level}(n) = i$ and $m < n$ in the monomial ordering F_{i-1}.

First, compute an irredundant Groebner basis $\overline{C}_1$ for I_Δ. Since this is a monomial ideal which is minimally generated by the 10 cubic monomials above, the generating set we already have for I_Δ is an irredundant Groebner basis. Let G_i be a "partial Groebner basis" for the eventual Schreyer resolution, and H_i "partial minimal generating sets" for the syzygies (LaScala + Stillman says $H_i \subseteq G_i$ but that doesn't seem right?)

Let m be the smallest element in $\mathcal{B}$, which in our example is $x_3x_5x_6e_1 \in R^1$. Since this element has level 1, we know there's some $g \in \overline{G}_1$ with initial term equal to m. In this case, of course, $g = x_3x_5x_6 \in I_\Delta$. So we add g to G_1, since we're building a Groebner basis for the image of φ_1 in our eventual resolution, and we add g to H_1 since it's a "syzygy" (a column of the eventual φ_1 in the resolution we're computing). Now we're done considering m, so we remove it from $\mathcal{B}$ and consider the second-smallest element of $\mathcal{B}$. This will be $x_2x_5x_6e_1$. The process is the same, we add $x_2x_5x_6$ to both G_1 and to H_1. This continues for the first ten smallest elements of $\mathcal{B}$, which are precisely the monomial basis for the image of ξ_1, which all have level 1. (If we weren't starting with a monomial ideal, this step would be a bit more interesting: it would start with the columns of ξ_1 and give us a matrix $1\times n$ matrix H_1 with entires the actual generators of the ideal.)

What's the eleventh smallest element of $\mathcal{B}$? It's going to be one of the (degree 3) monomial generators of the image of ξ_2, which is a submodule of R^{10} with term over position up ordering. The smallest element of B_2 is $x_6\epsilon_6$. We should be thinking of this as the initial term of a syzygy. To find the full syzygy, consider the following:

$x_6\epsilon_6$ is sent to $x_3x_4x_5x_6e_1 \in R^1$. We have C_1 already done (or at least partially done, in general). The lead (only) monomial of this term is divisible by $x_3x_5x_6$, which is the monomial coefficient on the image of ϵ_1. When we use this fact to cancel the lead term of $x_3x_4x_5x_6e_1$ while tracking the syzygy, we get

$$0 = x_3x_4x_5x_6e_1 - x_4\xi_1(\epsilon_1)$$

This one step finishes the reduction of $x_1x_2x_3x_6e_1$ by G_1, and it tells us the syzygy $x_6\epsilon_6 - x_4\epsilon_1$. This "fills in" the seventh column in the matrix ξ_2 with an actual syzygy.

Doing one more example, the next smallest element of $\mathcal{B}$ is $x_6\epsilon_7$. It is sent by ξ_1 to $x_1x_4x_5x_6e_1$. The monomial coefficients is divisible by $x_1x_4x_6 = \xi_1(\epsilon_4)$. Cancelling this term gives us zero, and a new complete syzygy $x_6\epsilon_7 - x_5\epsilon_4$, filling in another column in ξ_2.

Collecting what we have so far and continuing along, we get

$$\begin{aligned}
x_6\epsilon_6 &\rightsquigarrow x_6\epsilon_6 - x_4\epsilon_1\\
x_6\epsilon_7 &\rightsquigarrow x_6\epsilon_7 - x_5\epsilon_4\\
x_6\epsilon_8 &\rightsquigarrow x_6\epsilon_8 - x_1\epsilon_2\\
x_6\epsilon_9 &\rightsquigarrow x_6\epsilon_9 - x_3\epsilon_3\\
x_6\epsilon_{10} &\rightsquigarrow x_6\epsilon_{10} - x_2\epsilon_5\\
x_5\epsilon_3 &\rightsquigarrow x_5\epsilon_3 - x_4\epsilon_2\\
x_5\epsilon_5 &\rightsquigarrow x_5\epsilon_5 - x_1\epsilon_1\\
x_5\epsilon_9 &\rightsquigarrow x_5\epsilon_9 - x_2\epsilon_6\\
x_5\epsilon_{10} &\rightsquigarrow x_5\epsilon_{10} - x_3\epsilon_8\\
x_4\epsilon_5 &\rightsquigarrow x_4\epsilon_5 - x_3\epsilon_4\\
x_4\epsilon_8 &\rightsquigarrow x_4\epsilon_8 - x_2\epsilon_7\\
x_4\epsilon_{10} &\rightsquigarrow x_4\epsilon_{10} - x_2\epsilon_7\\
x_3\epsilon_2 &\rightsquigarrow x_3\epsilon_2 - x_2\epsilon_1\\
x_3\epsilon_7 &\rightsquigarrow x_3\epsilon_7 - x_1\epsilon_6\\
x_2\epsilon_4 &\rightsquigarrow x_2\epsilon_4 - x_1\epsilon_3
\end{aligned}$$

(La Scala + Stillman seemed to indicate that one of these degree 4 columns would give rise to an element that doesn't reduce to 0 using G_1. That didn't happen for me. I numbered my triangulation differently but I don't see why that would make a difference. In fact, since at this point G_1 is a groebner basis for I_Δ, shouldn't any $\xi_2(b)$ for b a column of level 2 be in I_Δ? And therefore will reduce to 0 using the Groebner bases G_1? Very confused.)

Some issues:

i. When you're doing the reduction for an element $b \in B_i$, you might not have a complete Groebner basis G_{i-1} yet. So it's possible your reduction of $\xi_i(b)$ will not reach 0. What do we do in this case? Why do these

ii. While this algorithm is certainly going to terminate ($\mathcal{B}$ is finite), why should we expect it to yield a free resolution, let alone a Schreyer resolution? Similarly, why are the finished G_i irredundant Groebner bases?

iii.

16 February 15 - An Algorithm for Computing a Schreyer Resolution

Let $R = k[x_1, \ldots, x_n]$ with a monomial order $>$, and let M be a finitely-generated R-module which is a quotient of a free R-module F_0, say $M = F_0/N$. Let $\overline{G}_1$ be an irredundant Groebner basis for N, and let $\Xi_\bullet$ be a Schreyer frame for M. The following algorithm will compute a Schreyer resolution $F_\bullet$ for M which has $\text{in}(F_\bullet) = \Xi_\bullet$. G_i (initialized to $\varnothing$) will eventually be a Groebner basis for the i^{th} syzygy module of M (is this right?), and H_i (also initialized to $\varnothing$) will be minimal generators for the syzygies. The details can be found in [4].

---

procedure SCHREYER RESOLUTION
    Input: $M = F_0/N$, $\overline{G}_1$, $\Xi_\bullet$.
    $G_i, H_i := \varnothing$
    while $\mathcal{B} \neq \varnothing$ **do**
        $b := \min \mathcal{B}$
        $\mathcal{B} := \mathcal{B} \setminus \{b\}$
        $i :=$ level b
        if $i = 1$ **then**
            Choose $g \in \overline{G}_1$ with $\text{in}(g) = b$
            add g to G_1
            add g to H_1
        else if $i > 1$ **then**
            Reduce the image of b using C_{i-1}
            Add the syzygy (successful or not) to C_i
            if it doesn't reduce to 0 **then**
                Add the remainder to C_{i-1}
                Remove the initial term of the remainder from $\mathcal{B}$.
            else if it does reduce to 0 **then**
                Add the reduction to H_i.
        Output: G_i, H_i for all i.

Example 16.1. Another example, smaller but not monomial this time. Let $R = k[x, y, z]$ and let $I = (x^3 + yz^2, x^2y + y^2z)$. Computing a Groebner basis for I yields

$$\overline{G}_1 = (g_1, g_2, g_3, g_4) = (x^2y + y^2z, x^3 + yz^2, xy^2z - y^2z^2, y^3z^2 + y^2z^3)$$

Note things like the expressions you get from S poly reductions (or just S polys in terms of gens):

$$xg_1 - yg_2 = g_3$$

$$yzg_1 + (-x - z)g_3 = g_4$$

$$(yz + z^2g_3 + (-x + z)g_4)$$

turn them into syzygies on these 4 gens of I. How to get syz on the original 2 gens of I?

Say we want to run this algorithm to get a Schreyer resolution for I. We start with our Schreyer frame :

$$\Xi_\bullet : R \xleftarrow{\begin{bmatrix} x^2y & x^3 & xy^2z & y^3z^2 \end{bmatrix}} R^4 \xleftarrow{\begin{bmatrix} 0 & 0 & 0 \\ x & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & x \end{bmatrix}} R^3$$

The ordered set $\mathcal{B}$ is $\{x^2ye_1 < x^3e_1 < x\epsilon_2 < xyz^2e_1 < x\epsilon_3 < y^3z^2e_1 < x\epsilon_4\}$

Make it work. In class Example.

Theorem 16.1. The chain complex $F_\bullet$ computed by this algorithm is a Schreyer resolution, and $\text{in}(F_\bullet) = \Xi_\bullet$.

Proof: Since the algorithm just adds smaller terms to the columns of the matrices in $\Xi_\bullet$, when we take initial terms we'll just get $\Xi_\bullet$ back.

Exactness?

We know that C_1 is an irredundant Groebner basis for N, which is the image of φ_1 and hence the kernel of φ_0, because of the behavior of the algorithm on elements of level 1. Assume that C_i is an irredundant Groebner basis for the image of φ_i. We need to prove that $\text{in}(\ker(\varphi_{i+1}))$ is generated by C_{i+1}

17 February 18

Buchberger's criterion gives you a generating set for all syzygies:

Recall the division algorithm for modules: Let $R = k[x_1, \ldots, x_n]$ and let F be a finitely-generated free R-module with a chosen term order $>$. For a set $G = \{g_1, \ldots, g_t\}$ and an element $f \in F$ we can always find an expression

$$f = \sum_{i=1}^{t} f_i g_i + r$$

Where $f_1, \ldots, f_t \in R$, $r \in F$, and

$$\text{in}(f) \geqslant \text{in}(f_i g_i)$$

for all i, and r is a sum of monomials in F, none of which are in the submodule generated by the initial terms of the g_i. r is called a remainder of f after division by G.

For R, F and G as above, where F has basis $\{e_1, \ldots, e_m\}$, consider the free R-module mape

$$F \longleftarrow R^t$$

defined by sending the standard basis element ϵ_i to g_i. If g_i and g_j have initial terms that are multiples of the same e_ℓ, then we define

$$\sigma_{ij} = \frac{\text{in}(g_j)}{\text{gcd}(\text{in}(g_i), \text{in}(g_j))}\epsilon_i - \frac{\text{in}(g_i)}{\text{gcd}(\text{in}(g_i), \text{in}(g_j))}\epsilon_j$$

For convenience, we'll rename these coefficients

$$\sigma_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j$$

The division algorithm tells us that

$$\sigma_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j = \sum_{k=1}^{t} f_k^{(ij)} g_k + h_{ij}.$$

In the case when the initial terms of g_i and g_j are multiples of different basis elements of F, we say that $h_{ij} = 0$.

There's a Buchberger criterion for modules, which says that G is a Groebner basis for the submodule of F that it generates if and only if $h_{ij} = 0$ for all $1 \leqslant i, j \leqslant t$

Lemma 17.1. Let M be a monomial submodule of F, generated by $m_1, \dots, m_t$, and consider the map

$$F \xleftarrow{\varphi} R^t$$

determined by $\epsilon_i \mapsto m_i$. Then the kernel of this map is generated by

$$\rho_{ij} = \frac{m_j}{\gcd(m_i, m_j)}\epsilon_i - \frac{m_i}{\gcd(m_i, m_j)}\epsilon_j$$

for $i < j$

Proof omitted, for now.

Theorem 17.1. Let R, F be as above and let $G = \{g_1, \dots, g_t\}$ be a Groebner basis for $M \subseteq F$. With the same map

$$F \xleftarrow{\varphi} R^t$$

as above, for any g_i, g_j whose initial terms are multiples of the same e_ℓ, let

$$\tau_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j - \sum_{k=1}^{t} f_k^{(ij)}\epsilon_k$$

Place the same "term over position up" monomial order on R^t that we've talked about before: $m_i\epsilon_i > m_j\epsilon_j$ if $\mathrm{in}(m_i g_i) > \mathrm{in}(m_j g_j)$, or if they're equal and $i < j$.

Then the initial term of τ_{ij} is $m_{ji}\epsilon_i$ and the set $\{\tau_{ij} \mid i < j\}$ is a Groebner basis for the syzygy module $\ker(\varphi)$

Proof. For any τ_{ij}, we know that the initial term can only be $m_{ji}\epsilon_i$ or $m_{ij}\epsilon_j$, by the definition of the term order on R^t. But since $i < j$ we get that $m_{ji}\epsilon_i$ is the larger term in τ_{ij}.

To prove that the τ_{ij} form a Groebner basis, let τ be an arbitrary syzygy in R^t. We need to show that the initial term of τ is a multiple of the initial term of some τ_{ij}. Suppose that

$$\tau = \sum_k f_k\epsilon_k,$$

and for any k, let $m_k\epsilon_k$ be the initial term of $f_k\epsilon_k$. Since these terms can't cancel with each other (different ϵ), the initial term of τ must be $n_i\epsilon_i$ for some i. Consider the sum

$$\sigma = \sum n_\ell\epsilon_\ell,$$

where ℓ ranges over those indices so that $n_\ell \mathrm{in}(g_\ell)$ is a scalar multiple of $n_k \mathrm{in}(g_k)$. All these ℓ must be bigger than k.

So this σ is a syzygy on the set $\mathrm{in}(g_\ell)$ for $\ell \geqslant i$. But by the above lemma, this set is generated by the ρ_{ij} described above, which will be $m_{ji}\epsilon_i - m_{ij}\epsilon_j$, where $k \leq i < j$. The generators with ϵ_k appearing are ρ_{kj} with $k < j$. So n_k must be in the ideal generated by m_{kj} for $j > k$.

□

Minimizing a free res.

18 February 20 - Worksheet Day

First, recap and finish the theorem from last time. In what follows, $R = k[x_1, \dots, x_n]$ with a monomial order $>$ and F is a free R-*module* with basis $\{e_1, \dots, e_m\}$ with its own term order, also called $>$.

Lemma 18.1. Let $M \subseteq F$ is a monomial submodule of F, generated by

$$M = \langle m_1 e_{\ell_1}, m_2 e_{\ell_2}, \dots, m_t e_{\ell_t} \rangle,$$

where each m_i is a monomial in R. Let R^t be the free R-module with basis $\{\epsilon_1, \dots, \epsilon_t\}$, and let $\varphi : R^t \longrightarrow F$ be defined by $\epsilon_i \mapsto m_i e_{j_i}$.

For each $i < j$ so that $\ell_i = \ell_j$, let

$$\sigma_{ij} = \frac{m_j}{\gcd(m_i, m_j)} \epsilon_i - \frac{m_i}{\gcd(m_i, m_j)} \epsilon_j$$

Then the kernel of φ is generated by these σ_{ij}

Theorem 18.1. Let M be a submodule of F and let $G = \{g_1, \dots, g_t\} \subseteq F$ be a Groebner basis for M. Let $\varphi : R^t \to F$ be defined by $\epsilon_i \mapsto g_i$. The map φ lets us define a term order on R^t, given by

$$n\epsilon_p > m\epsilon_q \Leftrightarrow ng_p > ng_q, \text{ or } ng_p = ng_q \text{ and } p < q.$$

For any $i < j$ where $\text{in}(g_i)$ and $\text{in}(g_j)$ are monomial multiples of the same basis element of F, let

$$\tau_{ij} = m_{ji}\epsilon_i - m_{ij}\epsilon_j - \sum_{k=1}^{t} f_k^{(ij)} \epsilon_k$$

be the syzygy that comes from the reduction of the pair (g_i, g_j) using G. These τ_{ij} form a Groebner basis for the kernel of φ, using the term order on R^t defined above.

Proof. We sketch the a successful proof to make up for the failed proof from last lecture:

i. The initial term of τ_{ij} is $m_{ji}\epsilon_i$.

ii. For any $\tau \in \ker(\varphi)$, we can show $\text{in}(\tau) = n_i \epsilon_i$ for some i.

iii. Let $\sigma = \sum n_p \epsilon_p$ be the sum over all p so that $\text{in} n_p g_p$ and $\text{in} n_i g_i$ are multiples of the same basis element of F. Note that all such p satisfy $p \geqslant i$

iv. σ is a syzygy on $\text{in}(g_1), \dots, \text{in}(g_t)$, which by the lemma above is generated by the σ_{ij}. This means that n_i is in the ideal generated by m_{pi} for $p > i$.

v. We conclude that the initial term of τ is in the submodule generated by the initial terms of the τ_{ij}, hence the τ_{ij} form a Groebner basis for $\ker(\varphi.)$

□

19 February 22 - More on Hilbert Functions, Points in Projective Space

19.1 Geometric Information from the Hilbert Function

For $X \subseteq \mathbb{P}^n_k$, we want to know what the dimension of the i^{th} graded component of $I(X)$ says about X. Start with an example. Let $X \subseteq \mathbb{P}^2_k$ be a set of three points,

$$X = \{(a_0, a_1, a_2), (b_0, b_1, b_2), (c_0, c_1, c_2)\}$$

and suppose we want to know the dimension of the degree 2 component of the ideal I_X of polynomials that vanish on X. Such polynomials are of the form

$$f = r_0x_0^2 + r_1x_0x_1 + r_2x_1^2 + r_3x_0x_2 + r_4x_1x_2 + r_5x_2^2$$

If we want to know whether f vanishes on the point (a_0, a_1, a_2), all we do is check whether the dot product below is zero:

$$\begin{bmatrix} a_0^2 & a_0a_1 & a_1^2 & a_0a_2 & a_1a_2 & a_2^2 \end{bmatrix} \cdot \begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \end{bmatrix} = 0$$

Similarly, to check whether f vanishes on all of X, we check whether the matrix product below is zero:

$$\begin{bmatrix} a_0^2 & a_0a_1 & a_1^2 & a_0a_2 & a_1a_2 & a_2^2 \\ b_0^2 & b_0b_1 & b_1^2 & b_0b_2 & b_1b_2 & b_2^2 \\ c_0^2 & c_0c_1 & c_1^2 & c_0c_2 & c_1c_2 & c_2^2 \end{bmatrix} \cdot \begin{bmatrix} r_0 \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \end{bmatrix} = 0$$

So, the set of points X determines a linear map $R_2 \longrightarrow k^3$, and the kernel of this map is precisely the polynomials of degree 2 that vanish on X. And this is true in any degree d and for any number of points n. So (using auspicious notation for the cokernel of this map) we can write a four-term exact sequence of (finite-dimensional) vector spaces

$$0 \longrightarrow (I_X)_d \longrightarrow R_d \xrightarrow{\Phi_d} k^n \longrightarrow H^1(I_X(d)) \longrightarrow 0$$

An example of the values of HF and $\dim H^1(I_X(d))$ for small d, when X is a set of five points, four of which lie on a line

$$\begin{array}{lllllll} d & = 0 & 1 & 2 & 3 & 4 & 5 \\ \mathrm{H}_{R/I}(d) & = 1 & 3 & 4 & 5 & 5 & 5 \\ \dim_k H^1(I_X(d)) & = 4 & 2 & 1 & 0 & 0 & 0 \end{array}$$

Goal is to relate the Hilbert function of I_X, the vanishing of $H^1(I_X(d))$, and the Betti numbers of I_X.

20 February 25 - Points in Projective Space, Regularity, Resolutions, Examples

20.1 Imposed Conditions

Recall, for a set X of n points in $\mathbb{P}^r_k$, for any degree d we get (after a choice of affine patch) a four-term sequence

$$0 \longrightarrow (I_X)_d \longrightarrow R_d \xrightarrow{\Phi}_d k^n \longrightarrow H^1(I_X(d)) \longrightarrow 0,$$

Where Φ_d is the evaluation map from degree d monomials to function $X \to k$. This sequence tells us that $H_{R/I_X}(d) + \dim(H^1(I_X(d))) = n$, and note that $H_{R/I_X}(d) = 0$ for $d \gg 0$. The rank of Φ_d is the difference in dimension betweenthe vector space of polynomials of degree d, namely R_d and the vector space of degree d polynomials vanishing on X, which is $(I_X)_d$. This leads to a natural definition

Definition 20.1. We say that the set of points X *imposes m conditions* on polynomials of degree d if Φ_d has rank m. We say that X *imposes independent conditions* on polynomials of degree d, if Φ_d has rank $n = |X|$.

Rephrasing the fact that $H_{R/I_X}(d) = 0$ for $d \gg 0$ using this definition, we say that for $d \gg 0$, the set X imposes n conditions on polynomials of degree d.

Lemma 20.1. $X \subseteq \mathbb{P}^r$ imposes m conditions on polynomials of degree d if and only if X contains a subset Y of m points so that for any point y in Y there exists a degree d polynomial vanishing on all of Y except y.

Proof. Since the column space of Φ_d is m dimensional, we can do column operations to Φ_d until it has an $m \times m$ identity matrix in the top left corner. Think about how this changes the basis for R_d, and what the first m basis elements do to the first m points. For the other direction, note that the set of m separating polynomials get sent to a linearly independent set of vectors under Φ_d □

Lemma 20.2. If X imposes $m < n$ conditions on polynomials of degree d, then it imposes at least $m + 1$ conditions on polynomials of degree $d + 1$.

Proof. Let Y be a set of m points with separating polynomials $\{f_1, \ldots, f_m\}$. Choose $x \in X \setminus Y$ to form $Y \cup \{x\}$, and consider $\{\ell \cdot f_1, \ldots, \ell \cdot f_m\}$, where ℓ is the equation of a line through x that misses Y. That's almost a set of separating polynomials, but we need a polynomial of degree $d + 1$ that vanishes on Y but not at x. Well, we can show that I_Y is generated in degree $d + 1$: for each $y \in Y$, choose r linear polynomials $\{\ell_j\}$ that vanish at y. Then the sets of polynomials $\{f_i \ell_j\}$, for all i, will generate I_Y. So I_Y is generated in degree $d + 1$. How does this help? Hal's book says I_Y is actually generated in degree d. But this doesn't seem true: if we take X a set of 3 points in $\mathbb{P}^2$, we note that X imposes 2 conditions on polyomials of degree 1 If we take a subset $Y \subseteq X$ of two points, we see that I_Y is not generated in degree 1. So what's going on here?

□

How does this tie in with Hilbert Functions and the four-term sequence from before?

Corollary 20.1. For any degree d for which $H^1(I_X(d))$ is not zero, we have

$$\dim H^1(I_X(d)) > \dim H^1(I_X(d + 1)).$$

And, for $d > |X| - 1$, we have $H^1(I_X(d) = 0$

Proof. The first inequality follows from the lemma. For the equality, note that $H^1(I_X(0)) = |X| - 1$, since the rank of Φ_0 can only be 1. The apply the inequality repeatedly. □

Definition 20.2. For a finitely generated graded $R = k[x_0, \ldots, x_n]$-module with minimal free resolution

$$F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_n \leftarrow F_{n+1} \leftarrow 0$$

where

$$F_i = \bigoplus_j R(-a_{i,j})$$

the *regularity* of M is $\sup(a_{i,j} - i)$

Example 20.1. For $R = k[x_0, x_1, x_2]$, consider general polynomials $f \in R_5$ and $\ell \in R_1$, and consider $I = (f, \ell)$. Then $X = V(I)$ is the intersection of a quintic and a line, which by Bezout's Theorem will be a set of 5 points. The Betti table of such an ideal will be

	0	1	2
total:	1	2	1
0:	1	1	.
1:	.	.	.
2:	.	.	.
3:	.	.	.
4:	.	1	1

reflecting a resolution of the form

$$R \leftarrow R(-1) \oplus R(-5) \leftarrow R(-6)$$

So I_X has regularity 4. If we compute the Hilbert function, we'll get

$$\begin{array}{ll} d & = 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \\ \mathrm{H}_{R/I_X}(d) & = 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 5 \end{array}$$

Example 20.2. Let $\ell_1, \ldots, \ell_{10}$ be 10 general polynomials in R_1. Let I be the ideal $(\ell_1, \ell_2) \cap \ldots \cap (\ell_9, \ell_{10})$, so that $V(I)$ is a set of 10 points in general position. The Betti table of such an ideal will be

	0	1	2
total:	1	3	2
0:	1	.	.
1:	.	1	.
2:	.	2	2

reflecting a resolution of the form

$$R \longleftarrow R(-2) \oplus R(-3) \oplus R(-3) \longleftarrow R(-4) \oplus R(-4).$$

so that R/I has regularity 2. The Hilbert function of R/I is

$$\begin{array}{ll} d & = 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \\ \mathrm{H}_{R/I_X}(d) & = 1 \quad 3 \quad 5 \quad 5 \quad 5 \quad 5 \end{array}$$

In the preceeding examples, the regularity of R/I was equal to the index of the last row in the Betti table, and was equal to the first degree d after which the hilbert Function started to agree with the Hilbert Polynomial. This is not a coincidence, but is something we'll work towards proving. But some setup is required first.

21 February 27 - Some background towards (stating and) proving the theorem

We want to prove that the regularity of a set X of points in projective space controls when the Hilbert function of X starts agreeing with the Hilbert polynomial. We need some background in order to make this precise, and to prove it.

Definition 21.1. An R-module P is called *projective* if, for any surjective map of R-modules $M \to N$, any map $P \to N$ lifts to a map $P \to M$ making the triangle below commute.

$$\begin{tikzcd} & P \arrow[dl, dashed] \arrow[d] & \\ M \arrow[r] & N \arrow[r] & 0 \end{tikzcd}$$

It is a useful exercise to show that the following conditions are all equivalent:

i. P is projective.

ii. P is a direct summand of a free module.

iii. The functor $\mathrm{Hom}_R(P, -)$ is exact.

iv. Any short exact sequence $0 \to A \to B \to P \to 0$ is split exact.

Note that if M is a free R-module, then it's projective, but the converse is not true for a general ring R. However, when R is a polynomial ring over a field, if P is a finitely generated projective R-module, then P is free. This is the Quillen-Suslin Theorem, which we are definitely not going to prove in this class.

Definition 21.2. The *projective dimension* of an R-module M is the smallest integer d so that there exists an exact sequence

$$0 \leftarrow M \leftarrow P_0 \leftarrow \cdots \leftarrow P_d \leftarrow 0$$

By the previous remark, over a polynomial ring the projective dimension of a graded module can be found by looking at its minimal free resolution. If R is a graded or local ring with maximal ideal $\mathfrak{m}$, after recalling that $- \otimes_R R/\mathfrak{m}$ applied to the minimal free resolution just replaces free modules with vector spaces and replaces the R-linear maps with 0 maps, we can say that

$$\mathrm{pdim}(M) = \sup(\{i \mid \mathrm{Tor}_i^R(M, R/\mathfrak{m}) \neq 0\}$$

Here's the theorem about regularity:
Cohen-Macaulay

Theorem 21.1. Let M be a finitely-generated graded $R = k[x_0, \ldots, x_n]$-module, with Hilbert function H_M and Hilbert polynomial P_M.

i. For $d > \mathrm{reg}(M)$ we have $H_M(d) = P_M(d)$.

ii. In fact, if $\mathrm{pdim}(M) = \delta$, then for $d \geqslant \mathrm{reg}(M) + \delta - n$ we have $H_M(d) = P_M(d)$.

iii. If X is a set of points in $\mathbb{P}^n$ and $M = R/I_X$, then $H_M(d) = P_M(d)$ if and only if $d \geqslant \mathrm{reg}(M)$. More generally, if M is Cohen-Macaulay, then the statement of ii becomes an if and only if.

Proof. Start with the minimal free resolution of M:

$$0 \longleftarrow M \longleftarrow \bigoplus_j R(-a_{0,j}) \longleftarrow \bigoplus_j R(-a_{1,j}) \longleftarrow \cdots \longleftarrow \bigoplus_j R(-a_{\delta,j}) \longleftarrow 0$$

Recalling 11, the Hilbert function of M (and consequently, the Hilbert polynomial of M) can be computed as the alternating sum of the Hilbert functions (polynomials) of the free modules in the minimal free resolution:

$$H_M(d) = \sum_{i,j} (-1)^i \binom{d - a_{i,j} + n}{n}$$

$$P_M(d) = \sum_{i,j} (-1)^i \frac{(d - a_{i,j} + n)(d - a_{i,j} + n - 1) \cdots (d - a_{i,j} + 1)}{n!}$$

For the binomial coefficient

$$\binom{d - a_{i,j} + n}{n}$$

to be equal to the polynomial expression

$$\frac{(d - a_{i,j} + n)(d - a_{i,j} + n - 1) \cdots (d - a_{i,j} + 1)}{n!}$$

we need that $d \geqslant a_{i,j} - n$. So, assuming $d \geqslant \operatorname{reg} M + \delta - n$, we get that for any $a_{i,j}$

$$d \geqslant \operatorname{reg} M + \delta - n \geqslant a_{i,j} - i + \delta - n \geqslant a_{i,j} - n.$$

So if d satisfies this bound, then $H_M(d) = P_M(d)$, proving (ii). Note that since $\delta - n$ is nonnegative by the Hilbert syzygy theorem 8.3, this proof implies (i) as well.

We have to postpone the proof of iii until we do more setup □

Slight generalization of the koszul complex: for a ring R, consider a sequence of elements $f_1, \ldots, f_m$. The Koszul complex on this sequence is the map defined by considering the map of free R-module

$$R \longrightarrow R^m$$

defined by $e_i \mapsto f_i$. Then let E be the exterior algebra on R^d, and consider the differential $\partial : E^d \mapsto E_{d-1}$ defined by

$$\partial(e_{i_1} \wedge \ldots \wedge e_{i_d}) = \sum_{j=1}^{d} f_j e_{i_1} \wedge \ldots \wedge \widehat{e_{i_j}} \wedge \ldots e_{i_d}$$

We'll use $K_\bullet = K_\bullet(f_1, \ldots, f_t)$ for this complex.

This complex is, in a sense, the most naive attempts at finding syzygies among the f_i, syzygies on the syzygies, and so forth. Like $f_j e_i - f_i e_j$. Then higher up, things like the image of $e_i \wedge e_j \wedge e_k$, which is

$$f_i e_j \wedge e_k - f_j e_i \wedge e_k + f_k e_i \wedge e_j$$

corresponding to the second syzygy:

$$f_i(f_k e_j - f_j e_k) - f_j(f_k e_i - f_i e_k) + f_k(f_j e_i - f_i e_j)$$

Definition 21.3. For a graded R-module M, a sequence $f_1, \ldots, f_t$ of elements of $\mathfrak{m}$ is called an M-regular sequence if any of the following equivalent conditions hold:

i. f_i is a nonzero divisor on $\dfrac{M}{(f_1, \ldots, f_{i-1})M}$ for all i, and $\dfrac{M}{(f_1, \ldots, f_t)M}$ is not zero.

ii. $H_i(K_\bullet(f_1, \ldots, f_t)) = 0$ for $i \geqslant 1$.

iii. $H_i(K_\bullet(f_1, \ldots, f_t)) = 0$ for $i = 1$.

The *depth* of M is the maximum length of an M-regular sequence.

22 March 1 - Worksheet Day - Writing your own `Macaulay2` functions.

Writing and loading your own `Macaulay2` functions: Open a new text file in the editor of your choice, enter the lines below, and save it as `MyFile.m2` (the name is not important, but the `.m2` extension is).

```
idealOfPoints = (m) -> (
    k := ring m;
    r := numRows m;
    n := numColumns m;

    R := k[x_0..x_r];
    idealList := apply(n, i -> ideal(toList(x_0..x_(r-1)) - (x_r)*(flatten entries m_i)));

    return intersect idealList;
    )
```

Once your files is saved, start a `Macaulay2` session and run the commands:

```
load "/path/to/MyFile.m2"
k = ZZ/101;
m = random(k^3, k^5);
I = idealOfPoints m;
```

replacing the path as appropriate.

1. Explain what the function `idealOfPoints` does. What is the precise meaning of the input `m`, and what is the output?

2. **Random sets are all the same:** Add to your `Macaulay2` file the following function:

```
HFPrinter = (n) -> (

    )
```

   i. Fill in the function so that `HFPrinter(n)` prints the first 30 values of the Hilbert Function of a generic set of n points in $\mathbb{P}^2$. (You can use `idealOfPoints` in your function definition!)

   ii. Do some experiments to convince yourself that *random* matrices will usually give you sets of points with the same Hilbert function.

   iii. Through experimentation, can you guess a formula for the Hilbert function of a generic set of n points in $\mathbb{P}^r$?

3. **Non-generic sets of points:** Let $R = k[x_0, x_1, x_2]$ and let $I = (f, g)$ be the ideal generated by homogeneous polynomials $f, g \in R_3$. What is the degree of I, and what is its Hilbert Function? Compare this to a generic set of the same number of points in $\mathbb{P}^2$, and give geometric interpretations for the differences.

4. **Possible Hilbert functions:** Let I be the ideal of a set X of 6 points in $\mathbb{P}^2$.

   i. Give an upper bound for the regularity of I. Can you find a set X so that this bound is met? What about a lower bound?

   ii. find two different sets of 6 points X and X' with the same Hilbert function, but where X has no subsets of 3 collinear points, but X' does. As a hint, try looking at cases where $H_{R/I_X}(2) = 5$.

   iii. Give an upper bound on the number of different possible Hilbert functions of the set X. How many different Hilbert functions can you realize with an explicit ideal?

23 March 4 - Regularity, Depth, and Local Cohomology

Last time, we said that the *Depth* of an R-module M is the largest integer d so that there exists an M-regular sequence $(f_1, \ldots, f_d)$.

Definition 23.1. For an R-module M, the *dimension* of M is the Krull dimension of $R/\text{ann}(M)$. In other words, it is the longest r such that there exisst a chain of proper containments of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_r$$

in $R/\text{ann}(M)$

Definition 23.2. An R-module M is called *Cohen-Macaulay* if $\text{depth}(M) = \dim(M)$

23.1 Local Cohomology

Definition 23.3. Let R be a Noetherian ring and let $I \subseteq R$ be an ideal. For any R-module M, the 0^{th} *local cohomology module* $H_I^0(M)$ is defined to be

$$H_I^0(M) = \{m \in M \mid I^n m = 0 \text{ for some } n \geqslant 1\}$$

.

The assignment $M \mapsto H_I^0(M)$ is a left exact (covariant) functor, which means it has a family of right derived functors, which we denote by $R^i H_I^0(-) = H_I^i(M)$, and we call this functor's value on M the i^{th} *local cohomology module of M*

Recall that one definition right derived functors tells use that to "compute" $H_I^i(M)$, we take an *injective* resolution of M:

$$0 \to M \to Q^0 \to Q^1 \to Q^2 \to \cdots,$$

apply the functor to the resolution

$$H_I^0(Q^0) \to H_I^0(Q^1) \to H_I^0(Q^2) \to \cdots$$

and define $H_I^i(M)$ to be the cohomology of this complex at $H_I^0(Q^i)$. This is not a particularly practical definition. We've been working in a situation where projective (in fact free) resolutions are easy to find and describe, even compute with. The same is rarely true for injective resolutions.

Lemma 23.1. Local cohomology as a limit of Ext modules.

Consider the diagram:

$$\cdots R/I^{n+1} \to R/I^n \to \cdots \to R/I^2 \to R/I.$$

Applying $\text{Ext}_R^i(-, M)$, we get

$$\text{Ext}_R^i(R/I, M) \to \text{Ext}_R^i(R/I^2, M) \to \cdots \to \text{Ext}_R^i(R/I^n, M) \to \text{Ext}_R^i(R/I^{n+1}, M) \to \cdots$$

There is a natural isomorphism between the i^{th} local cohomology module of M and the direct limit of this diagram:

$$H_I^i(M) \simeq \varinjlim_n \text{Ext}_R^i(R/I^n, M)$$

The proof comes from "abstract nonsense". This new expression for local cohomology tells us that any $m \in H_I^i(M)$ is annihilated by some power of I. This is because local cohomology is a direct limit of Ext modules, each of which is annihilated by a power of I. Another definition of local cohomology comes from the Cech complex:

Lemma 23.2. If $I = (a_1, \ldots, a_t)$, consider the complex

$$0 \to M \to \bigoplus_{1 \leqslant j \leqslant t} M_{a_j} \to \bigoplus_{1 \leqslant j_1 < j_2 \leqslant t} M_{a_{j_1} a_{j_2}} \to \cdots \to \bigoplus_{1 \leqslant j_1 < \ldots j_s \leqslant t} M_{a_{j_1} \cdots a_{j_s}} \to \cdots \to M_{a_1 a_2 \cdots a_t} \to 0$$

where we are using M_a for the localization $M \otimes_R R[\frac{1}{a}]$, and the differential

$$\bigoplus_{1 \leqslant j_1 < \ldots j_s \leqslant t} M_{a_{j_1} \cdots a_{j_s}} \to \bigoplus_{1 \leqslant j_1 < \ldots j_{s+1} \leqslant t} M_{a_{j_1} \cdots a_{j_{s+1}}}$$

is defined by sending an element $m \in M_{a_{j_1} \cdots a_{j_s}}$ to the alternating sum of the images of m in the further localizations by a_k, for $k \neq j_1, \ldots, j_s$, where the sign is $(-1)^p$, where k gets inserted into the p^{th} spot ordered tuple $(j_1, \ldots, j_{p-1}, k, j_p, j_s)$. This complex, denoted $\check{C}(a_1, \ldots, a_t; M)$, is called the Cech complex. The cohomology of this complex in position i (i = number of localizing elements) is $H^i_I(M)$.

24 March 6

This is just a cursory introduction to local cohomology, but it lets us state a theorem that will be useful in proving what's left of the statement of the theorem 21.1, which we recall here

iii. If X is a set of points in $\mathbb{P}^n$, then $H_M(d) = P_M(d)$ if and only if $d \geqslant \text{reg}(R/I_X)$. More generally, if M is Cohen-Macaulay, then $H_M(d) = P_M(d)$ if and only if $d \geqslant \text{reg}(M) + \delta - n$.

Example 24.1. Let $R = k[x_0, \ldots, x_n]$ and let $\mathfrak{m}$ be the ideal generated by the variables. Then for $i < n+1$ we have

$$H^i_{\mathfrak{m}}(R) = 0$$

$$H^{n+1}_{\mathfrak{m}}(R) = \text{Hom}_R(R(-n-1), k)$$

Proof. Consider the Cech complex, which is $\mathbb{Z}^{n+1}$ graded, and choose a degree $\alpha \in \mathbb{Z}^n$ and look at the degree α component of the complex. Let $J \subseteq \{0, \ldots, r\}$ be the indices where α is negative. x^α is in a summand $R[\frac{1}{x_{i_1} \cdots x_{i_s}}]$ if and only if $J \subseteq \{i_1, \ldots, i_s\}$ (x^α might have x_is in a "denominator" so you need to be able to divide by those variables). So we have that in degree α, $R[\frac{1}{x_{i_1} \cdots, x_{i_t}}]$ is either 0 or k, depending on whether J is a subset of $\{i_1, \ldots, i_t\}$.

So our chain complex in degree α is indexed by subsets of $\{0, \ldots, r\}$ that contain J. That's the same as indexing by subsets of $\{0, \ldots, r\} \setminus J$. In fact, the complex in degree α is the complex computing the simplicial homology of the complete simplex on this set.

Anyways, if this makes sense, then the complex in degree α has zero homology (unless the simplex is empty, α entirely negative, but that can only contribute to $H^{n+1}_{\mathfrak{m}(R)}$). So the degree α component of $H^{n+1}_{\mathfrak{m}}(R)$ is k if and only if α is entirely negative. This agrees with the multigrading on the dual of the canonical module. $\square$

The theorem that will be useful (but will take some work to prove) is the following relationship between regularity and local cohomology.

Theorem 24.1. For M a finitely-generated graded $R = k[x_0, \ldots, x_n]$-module and d an integer, the following are equivalent:

i. $d \geqslant \text{reg}(M)$.

ii. $d \geqslant \max\{e \mid H^i_{\mathfrak{m}}(M)_e \neq 0\} + i$ for all i.

iii. $d \geqslant \max\{e \mid H^0_{\mathfrak{m}}(M)_e \neq 0\}$ and $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$ for all $i > 0$

Proof.

(i ⇒ ii) . Proceed by induction on the projective dimension of M. $\mathrm{pdim}(M) = 0$, then $M = \oplus R(-a_i)$ is free, and its regularity is $\max\{a_i\}$

□

25 March 8

Theorem 25.1. For M a finitely-generated graded $R = k[x_0, \dots, x_n]$-module and d an integer, the following are equivalent:

i. $d \geqslant \mathrm{reg}(M)$.

ii. $d \geqslant \max\{e \mid H^i_{\mathfrak{m}}(M)_e \neq 0\} + i$ for all i.

iii. $d \geqslant \max\{e \mid H^0_{\mathfrak{m}}(M)_e \neq 0\}$ and $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$ for all $i > 0$

Proof.

(i) ⇒ (ii) . Proceed by induction on the projective dimension of M.

If $\mathrm{pdim}(M) = 0$, then $M = \bigoplus_j R(-a_j)$ is free, and its regularity is $\max\{a_j\}$. By Local Duality, we have that $H^i_{\mathfrak{m}}(M) = 0$ for $i < n+1$, and

$$H^{n+1}_{\mathfrak{m}}(M) = \bigoplus_d \mathrm{Hom}_k\left(\mathrm{Hom}_R(M, R(-n-1))_{-d}, k\right).$$

Important note: this Hom_R is the *internal* Hom in the category of graded R modules with graded maps, the right adjoint to the tensor product. The degree e component consists of the R-module maps that increase degree by e, so $\mathrm{Hom}_R(M, N)_e)$ is all the degree 0 maps from M to $N(-e)$, or from $M(e)$ to N. A good way to think about it is, the identity map $\mathrm{id} : M \to M$ should be degree 0, so $x \cdot \mathrm{id}$ should be degree 1)

So we have

$$\begin{aligned}
H^{n+1}_{\mathfrak{m}}(M)_e &= \mathrm{Hom}_R(M, R(-n-1))_e \\
&= \mathrm{Hom}_R(M, R(-n-1-e)) \\
&= \mathrm{Hom}_R(\bigoplus_j R(-a_j), R(-n-1-e)) \\
&= \bigoplus_j \mathrm{Hom}_R(R(-a_j), R(-n-1-e)) \\
&= \bigoplus_j \mathrm{Hom}_R(R, R(a_j-n-1-e))
\end{aligned}$$

For any degree e, this module is nonzero if and only if $\max\{a_j\} - n - 1 - e > 0$, which means $d \geqslant \max\{a_j\} > n + 1 + e$ for all e, so in particular it's true for the maximum such e. So $d \geqslant$

$n+1+\max\{e \mid H^{n+1}_{\mathfrak{m}}(M)\}$. And since this is the only non-vanishing local cohomology module of M, (ii) is satisfied.

Now, assume M has projective dimension $\delta > 0$, with minimal free resolution

$$0 \leftarrow M \xleftarrow{\varphi_0} F_0 \xleftarrow{\varphi_1} F_1 \leftarrow \cdots \leftarrow F_\delta \leftarrow 0$$

Re-using notation, let $F_0 = \bigoplus\limits_j R(-a_j)$. Consider $\operatorname{im}(\varphi_1)$, which has minimal free resolution

$$0 \leftarrow \operatorname{im}(\varphi_1) \xleftarrow{\varphi_1} F_1 \xleftarrow{\varphi_2} F_2 \leftarrow \cdots \leftarrow F_\delta \leftarrow 0$$

This tells us two things: That $\operatorname{reg}(\operatorname{im}(\varphi_1)) = \operatorname{reg}(M) + 1$, and that $\operatorname{im}(\varphi_1)$ has projective dimension $\delta - 1$, so we can apply our induction hypothesis to it. So if $d \geqslant \operatorname{reg}(M)$, we know $d+1 \geqslant \operatorname{reg}(\operatorname{im}(\varphi_1))$, and so for any $i \geqslant 0$

$$d + 1 \geqslant i + \max\{e \mid H^i_{\mathfrak{m}}(\operatorname{im}(\varphi_1))_e \neq 0\}$$

Consider the short exact sequence

$$0 \to \operatorname{im}(\varphi_1) \to F_0 \to M \to 0$$

This gives rise to a long exact sequence in local cohomology:

$$\begin{tikzcd}
0 \arrow[r] & H^0_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \arrow[r] & H^0_{\mathfrak{m}}(F_0) \arrow[r] & H^0_{\mathfrak{m}}(M) \arrow[dll, rounded corners] & \\
 & H^1_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \arrow[r] & H^1_{\mathfrak{m}}(F_0) \arrow[r] & H^1_{\mathfrak{m}}(M) \arrow[dll, rounded corners] & \\
 & H^2_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \arrow[r] & H^2_{\mathfrak{m}}(F_0) \arrow[r] & H^2_{\mathfrak{m}}(M) \arrow[dll, rounded corners] & \\
 & \cdots & & \arrow[dll, rounded corners] & \\
 & H^n_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \arrow[r] & H^n_{\mathfrak{m}}(F_0) \arrow[r] & H^n_{\mathfrak{m}}(M) \arrow[dll, rounded corners] & \\
 & H^{n+1}_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \arrow[r] & H^{n+1}_{\mathfrak{m}}(F_0) \arrow[r] & H^{n+1}_{\mathfrak{m}}(M) \arrow[r] & 0
\end{tikzcd}$$

But since F_0 is free, all of its local cohomology modules vanish, except $H^{n+1}_{\mathfrak{m}}(F_0)$, and we know what this top local cohomology module is (again using local duality). Filling in this long exact sequence with zeros, we conclude that for $i = 0, 1, 2, \ldots, n-1$, we have an isomorphism

$$H^i_{\mathfrak{m}}(M) \simeq H^{i+1}_{\mathfrak{m}}(\operatorname{im}(\varphi_1))$$

And at the end of the long exact sequence we get a four-term short exact sequence

$$0 \to H^n_{\mathfrak{m}}(M) \to H^{n+1}_{\mathfrak{m}}(\operatorname{im}(\varphi_1)) \to \bigoplus_j \operatorname{Hom}_R(R(-a_j), R(-n-1)) \to H^{n+1}_{\mathfrak{m}}(M) \to 0.$$

We know by induction that for any $i \geqslant 0$ we have

$$d + 1 \geqslant i + \max\{e \mid H^i(\mathrm{im}(\varphi_1)) \neq 0\}.$$

Using the isomorphisms, we can say that for $i = 1, 2, 3, \ldots, n$ we have

$$d + 1 \geqslant i + \max\{e \mid H^{i-1}_{\mathfrak{m}}(M) \neq 0\}.$$

So subtract 1 from both sides and re-index to say that for $i = 0, 1, 2, \ldots, n-1$ we have what we need:

$$d \geqslant i + \max\{e \mid H^i_{\mathfrak{m}}(M) \neq 0\}$$

Now we need to prove it for $i = n$ and $i = n + 1$. Think about the four-term exact sequence

$$0 \to H^n_{\mathfrak{m}}(M) \to H^{n+1}_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \to \bigoplus_j \mathrm{Hom}_R(R, R(a_j - n - 1)) \to H^{n+1}_{\mathfrak{m}}(M) \to 0.$$

If

(ii) $\Rightarrow$ (iii)

$\square$

26 March 18

26.1 Completing the Proof from Last Time:

We finish the missing implication from the theorem from last class. Some claims in the proof require nontrivial justifications, but these justifications will be suppressed in the interest of expediency.

(iii) $\Rightarrow$ (i) Assume that $d \geqslant \max\{e \mid H^0_{\mathfrak{m}}(M)_e \neq 0\}$ and $H^i_{\mathfrak{m}}(M)_{d-i+1} = 0$ for $i > 0$. We can assume the field k is infinite. We need to show $d \geqslant \mathrm{reg}(M)$.

We'll proceed by induction on the projective dimension of M. If $\mathrm{pdim}(M) = 0$, then $M = \oplus R(-a_{0,j})$ and we have to show that $d \geqslant a_{0,j}$ for all j, i.e. that the generators of M all have degree at most d. We prove this by induction on the dimension of M: If $\dim(M) = 0$, then $\ell(M) < \infty$, so M is annihilated by a power of $\mathfrak{m}$. This means $M = H^0_{\mathfrak{m}}(M)$ and the fact the M has no generators of degree larger than d follows from the hypothesis.

Now assume $\dim(M) > 0$. Look at the short exact sequence

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to \overline{M} \to 0.$$

If we can show that $H^0_{\mathfrak{m}}(M)$ and $\overline{M}$ have no generators of degree greater than d, then we know it's true of M as well. By assumption, $H^0_{\mathfrak{m}}(M)_e = 0$ for $e > d$, so that's straightforward. For $\overline{M}$, choose $x \in R_1$ an almost-regular element on $\overline{M}$, i.e. the kernel of $M \xrightarrow{\cdot x} M$ is finite length (the existence of such an element is why we needed k to be infinite, and even then it still needs further justification). Then $\overline{M}/x\overline{M}$ is d-regular (since $\overline{M}$ is?) and it has dimension strictly smaller than $\dim(M)$. So $\overline{M}/x\overline{M}$ has no generators of degree greater than d. We can draw the same conclusion about $\overline{M}/\mathfrak{m}\overline{M}$, and by Nakayama's lemma, $\overline{M}$ has no generators of degrees greater than d. From the short exact sequence above, this shows M has no generators with degree greater than d. So $d \geqslant a_{0,j}$ for all j.

Now, if M has positive projective dimension, the same argument above shows that $d \geqslant a_{0,j}$ for all j, but there are more $a_{i,j}$ to check. consider the minimal free resolution of M :

$$M \leftarrow F_0 = \bigoplus_j R(-a_{0,j}) \xleftarrow{\phi_1} F_1 = \bigoplus_j R(-a_{1,j}) \leftarrow \cdots \leftarrow F_\delta = \bigoplus_j R(-a_{\delta,j}).$$

Once again, consider $\mathrm{im}(\varphi_1)$ and the short exact sequence

$$0 \to \mathrm{im}(\varphi_1) \to F_0 \to M \to 0,$$

which gives rise to the long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H^0_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \arrow[r] & H^0_{\mathfrak{m}}(F_0) \arrow[r] & H^0_{\mathfrak{m}}(M) \arrow[dll] & \\
& H^1_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \arrow[r] & H^1_{\mathfrak{m}}(F_0) \arrow[r] & H^1_{\mathfrak{m}}(M) \arrow[dll] & \\
& H^2_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \arrow[r] & H^2_{\mathfrak{m}}(F_0) \arrow[r] & H^2_{\mathfrak{m}}(M) \arrow[dl] & \\
& & \cdots \arrow[dl] & & \\
& H^n_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \arrow[r] & H^n_{\mathfrak{m}}(F_0) \arrow[r] & H^n_{\mathfrak{m}}(M) \arrow[dll] & \\
& H^{n+1}_{\mathfrak{m}}(\mathrm{im}(\varphi_1)) \arrow[r] & H^{n+1}_{\mathfrak{m}}(F_0) \arrow[r] & H^{n+1}_{\mathfrak{m}}(M) \arrow[r] & 0
\end{tikzcd}$$

This long exact sequence, together with our assumption that M is d-regular, tells use that $\mathrm{im}(\varphi_1)$ is $d+1$-regular. And as before, we can say $\mathrm{reg}(\mathrm{im}(\varphi_1)) \leqslant \mathrm{reg}(M) + 1.$. By induction on projective dimension, we get that $d+1 \geqslant \mathrm{reg}(\mathrm{im}(\varphi))$. But think about what this means in terms of the minimal free resolution of M: It means that $d+1 \geqslant (a_{i,j} - (i+1))$ for all $i > 0$ and all j. Combined with the $i = 0$ case from earlier, we get that $d \geqslant \mathrm{reg}(M)$.

26.2 Applications of the theorem:

Let's use this to prove part (iii.) of 21.1

Proof. Let X be a set of points in $\mathbb{P}^n$, let $M = R/I_X$ and let $d = \mathrm{reg}(M)$. A geometric argument (the existence of a line that does not contain any of the points in X) shows that $\mathrm{depth}(M) \geqslant 1$. The dimension of M is 1, so the depth is 1 too. We have a four-term exact sequence

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to H^0(\widetilde{M}) \to H^1_{\mathfrak{m}}(M) \to 0.$$

The first term is zero because the depth of R/I_X is positive (?) The global sections $H^0(\widetilde{M})$ are just the functions on X in each degree, so

$$H^0(\widetilde{M}) = \bigoplus_d H^0(\mathcal{O}_X(d)),$$

and since X is affine, the global sections $H^0(\mathcal{O}_X(d))$ is just k^X for each d. Since $d = \mathrm{reg}(M)$, the previous theorem says that d is also equal to $1 + \max\{e \mid H^1_{\mathfrak{m}}(M)_e \neq 0\}$, which means d is the smallest integer so that $H^1_{\mathfrak{m}}(M)_d = 0$. But this is zero if and only if the middle map is an isomorphism, i.e. if and only if $\dim(R/I_X)_d = n$. But the degree where the coordinate ring of X because n-dimensional is exact the degree where the Hilbert function and Hilbert polynomial begin to coincide.

□

27 March 20

It remains to prove that if M is Cohen-Macaulay, then $1 + \operatorname{reg}(M) - \operatorname{pdim}(M)$ is the smallest integer so that the Hilbert function and polynomial agree.

Wrapping up 21.1, let M be a finitely generated $R = k[x_0, \ldots, x_n]$-module with $\operatorname{pdim}(M) = \delta$. We need to show that $H_M(d) = P_M(d)$ if and only if $d \geqslant \operatorname{reg}(M) + \delta - n$. For this we need one lemma:

Lemma 27.1. For M a finitely-generated graded R-module, we have

$$P_M(d) = H_M(d) - \sum_{i \geqslant 0} (-1)^i \dim_k H^i_{\mathfrak{m}}(M)_d.$$

Proof. For a sheaf $\mathscr{F}$ on projective space, the euler characteristic of $\mathscr{F}$ is defined to be

$$\chi(\mathscr{F}) = \sum_{i \geqslant 0} (-1)^i \dim_k H^i(\mathbb{P}^n, \mathscr{F}).$$

We claim that the Hilbert polynomial of M is related to the Euler characteristic of $\widetilde{M}$ in the following way:

$$P_M(d) = \chi(\widetilde{M}(d)).$$

Why is this true? By Serre vanishing, for $d \gg 0$, all higher cohomology of $\widetilde{M}(d)$ is zero, and $H^0(\mathbb{P}^n, \widetilde{M}(d))$ is just M_d. So the equality holds for infinitley many values of d. To get the equality for all values of d, we just have to show that the right-hand side is a polynomial. We do this by induction on the dimension of M:

If M is 0-dimensional, then $\widetilde{M}$ has 0-dimensional support, and the euler characteristic of $\widetilde{M}$ is just the dimension of the space of global sections. For any sheaf, when you tensor with a vector bundle, euler characteristic gets multiplied by the rank of the vector bundle. Since $\widetilde{M}(d)$ is just $\widetilde{M} \otimes \mathcal{O}(d)$, the euler characteristic doesn't change.

Now suppose M has positive dimension. For a general linear polynomial $\ell \in R_1$ we get an exact sequence

$$0 \to \widetilde{M}(-1) \xrightarrow{\ell} \widetilde{M} \to \widetilde{M/xM} \to 0$$

which gives a long exact sequence in sheaf cohomology

$$\begin{tikzcd}
0 \arrow[r] & H^0(\mathbb{P}^n, \widetilde{M}(-1)) \arrow[r] & H^0(\mathbb{P}^n, \widetilde{M}) \arrow[r] & H^0(\mathbb{P}^n, \widetilde{M/xM}) \arrow[dll] & \\
& H^1(\mathbb{P}^n, \widetilde{M}(-1)) \arrow[r] & H^1(\mathbb{P}^n, \widetilde{M}) \arrow[r] & H^1(\mathbb{P}^n, \widetilde{M/xM}) \arrow[dll] & \\
& H^2(\mathbb{P}^n, \widetilde{M}(-1)) \arrow[r] & H^2(\mathbb{P}^n, \widetilde{M}) \arrow[r] & H^2(\mathbb{P}^n, \widetilde{M/xM}) \arrow[dl] & \\
& & \cdots \arrow[dl] & & \\
& H^n(\mathbb{P}^n, \widetilde{M}(-1)) \arrow[r] & H^n(\mathbb{P}^n, \widetilde{M}) \arrow[r] & H^n(\mathbb{P}^n, \widetilde{M/xM}) \arrow[r] & 0
\end{tikzcd}$$

The alternating sum of the dimensions of all the terms in this long exact sequence will be 0, which tells you that $\chi(\widetilde{M}) - \chi(\widetilde{M}(-1)) = \chi(\widetilde{M/xM})$. The right-hand side is a polynomial, because $\dim(M/xM)$ is lower than $\dim(M)$. You can repeat this argument for any twist to get

$$\chi(\widetilde{M}(d)) - \chi(\widetilde{M}(d-1)) = \chi(\widetilde{M/xM(d)})$$

This means that $\chi(\widetilde{M}(d))$ is a polynomial in d (why does it mean this? calculus trick?)

By the result from last time, we have a four-term exact sequence

$$0 \to H^0_{\mathfrak{m}}(M) \to M \to \bigoplus_d H^0(\mathbb{P}^n, \widetilde{M}(d)) \to H^1_{\mathfrak{m}}(M) \to 0$$

(possibly not needed here?) as well as isomorphisms for $i > 0$:

$$\bigoplus_d H^i(\mathbb{P}^n, \widetilde{M}(d)) \simeq H^{i+1}_{\mathfrak{m}}(M)$$

Note: M determines *two* sheaves: a sheaf $\mathscr{F}_M$ on punctured affine space $X = \mathbb{A}^{n+1} \setminus \{0\}$, and a sheaf $\widetilde{M}$ on $\mathbb{P}^n$. the relationship between the cohomology of these sheaves is

$$H^i(X, \mathscr{F}_M) = \bigoplus_d H^i(\mathbb{P}^n, \widetilde{M}(d))$$

The vertical Cech complex from the lemma that gives the four-term and the isomorphisms computes the cohomology of $\mathscr{F}_M$. But in degree d it computes the cohomology of $\widetilde{M}(d)$.

The isomorphisms from the lemma let us say that for $i \geqslant 1$,

$$\dim_k H^i(\widetilde{M}(d)) = \dim_k H^{i+1}_{\mathfrak{m}}(M)_d,$$

while the four-term sequence (in degree d) tells us that

$$\dim_k H^0_{\mathfrak{m}}(M)_d - \dim_k M_d + \dim_k H^0(\widetilde{M}(d)) - \dim_k H^1_{\mathfrak{m}}(M)_d = 0$$

Putting this all together, we have

$$\begin{aligned} P_M(d) = \chi(\widetilde{M}(d)) &= \sum_{i \geqslant 0} (-1)^i \dim_k H^i(\mathbb{P}^n, \widetilde{M}(d)) \\ &= \dim_k H^0(\widetilde{M}(d)) + \sum_{i \geqslant 1} (-1)^i \dim_k H^i(\widetilde{M}(d)) \\ &= \left(\dim(M_d) - \dim H^0_{\mathfrak{m}}(M)_d + \dim H^1_{\mathfrak{m}}(M)_d\right) + \left(\sum_{i \geqslant 1} (-1)^i \dim H^{i+1}_{\mathfrak{m}}(M)_d\right) \end{aligned}$$

which after replacing $\dim M_d$ with $H_M(d)$ and re-indexing and simplifying the rest of the expression, proves what we were trying to show. □

Using this, we get a quick proof of the last bit of 21.1.

Proof. We already know that when $d \geqslant \operatorname{reg}(M) + \delta - n$, the Hilbert function and Hilbert polynomial agree. We need to show that this bound is sharp. The Auslander-Buchsbaum formula tells us that

$$\operatorname{depth}(M) + \operatorname{pdim}(M) = \operatorname{depth}(R) = n + 1,$$

so $\delta = n + 1 - \operatorname{depth}(M)$, which lets us rewrite

$$\operatorname{reg}(M) + \delta - n = \operatorname{reg}(M) - \operatorname{depth}(M) + 1.$$

Local cohomology $H^i_{\mathfrak{m}}(M)$ can only be nonzero when $\operatorname{depth}(M) \leqslant i \leqslant \dim(M)$, and is guaranteed to be nonzero when $i = \operatorname{depth}(M)$ Since M is Cohen-Macaulay, $\operatorname{depth}(M) = \dim(M)$, so there's only one non-vanishing local cohomology is $H^{\operatorname{depth}(M)}_{\mathfrak{m}}(M)$. So by the preceeding lemma we have

$$P_M(d) = H_M(d) - \sum_{i \geqslant 0} (-1)^i \dim H^i_{\mathfrak{m}}(M)_d$$

$$= H_M(d) \pm \dim H^{\mathrm{depth}(M)}_{\mathfrak{m}}(M)_d$$

And by the big theorem from before, we know

$$\mathrm{reg}(M) = \max\{e \mid H^{\mathrm{depth}(M)}_{\mathfrak{m}}(M)_e\} + \mathrm{depth}(M),$$

so $\mathrm{reg}(M) - \mathrm{depth}(M) + 1$ is the smallest degree after which the local cohomology module giving the correction term becomes permanently zero.

□

28 March 22: Loading Packages, Depth in Macaulay2

In addition to the main Macaulay2 system, users can write and load their own *packages* to accomplish specific tasks. Some of these packages are bundled with Macaulay2, so are automatically available to you. But you can also find and use packages that aren't shipped with the main system, or you can write and load your own packages.

28.1 Problem 1

Recall that when $R = k[x_0, \ldots, x_n]$, the *depth* of an R-module M is the length of a maximal M-regular sequence, i.e. a sequence $r_1, \ldots, r_d$ of homogeneous elements in R for which the Koszul complex $K_\bullet(r_1, \ldots, r_d) \otimes_R M$ is exact.

i. Let $I = (x, y) \cap (z, w) \subseteq k[x, y, z, w]$. Through experimentation, try to guess the depth of the R module $M = R/I$. Functions you may find useful are:

   1. `koszul`, returns the koszul complex of a $1 \times n$ matrix of ring elements.
   2. `**`, a binary operator for tensor product. Can be used to take the tensor product of two modules, or of chain complexes, or both.
   3. `HH`, computes the homology of a chain complex. Use `HH_i` if you want a particular homology module
   4. `prune`, to simplify the presentation of a module, especially a homology module. For example, if `m = matrix{{x,y,z,w}}`, compare the output of `HH koszul m` to the output of `prune HH koszul m`.

ii. Load the `Depth` package and look at the documentation, using the commands

```
i1 : loadPackage "Depth"

i2 : help "Depth"
```

Using the functionality provided by this package, compute the depth of M, and whether or not M is Cohen-Macaulay.

iii. Find the source code for the Depth package. It will be a file called `Depth.m2`, probably in `../Macaulay2-1.13/sha` but if not, you can use the command `path` to ask `Macaulay2` where it is finding packages. If for some reason you can't find it locally, the source code can be found on the `Macaulay2` Github page.

Read the source code for the function `Depth(Module)`, and explain how it is calculating depth.

28.2 Problem 2

There are many `Macaulay2` packages that may bring its functionality close to your mathematical interest, such as `AbstractToricVarieties, Divisor, Graphs, LatticPolytopes, Matroids, Points, StronglyStableIdeals, ToricTopology, Tropical.` Look at these or other packages that look interesting to you, and put some thought into your project for this course.

If you are interested in writing your own `Macaulay2` package (by no means required!), you might want to take a look at `PackageTemplate` and `SimpleDoc` in the packages directory for some guidance on how to get started.

29 Week of March 25 - 29: Simplicial Complexes Worksheet

A *simplicial complex* on the vertex set $V = \{1, 2, \ldots, n\}$ is a collection of subsets $\Delta \subseteq \mathcal{P}(V)$, with the property that if $\sigma \in \Delta$ and $\tau \subseteq \sigma$, then $\tau \in \Delta$. The elements of Δ are called the *faces* of the simplicial complex, and the *dimension* of a face σ is $|\sigma| - 1$.

A simplicial complex Δ determines an ideal in the ring $R = k[x_1, \ldots, x_n]$, called the *Stanley-Reisner ideal* of Δ. It is defined to be the ideal I_Δ generated by the squarefree monomials corresponding to the subsets of V that are not faces of Δ. The *Stanley-Reisner ring* of Δ is the quotient R/I_Δ.

29.1 Problem 1

Warm up: Fixing $V = \{1, 2, \ldots, n\}$, describe the Stanley-Reisner ideal of each simplicial complex below:

i. $\Delta = \varnothing$ (The *void complex*)

ii. $\Delta = \{\varnothing\}$ (The *irrelevant complex*)

iii. $\Delta = \{\{1\}, \{2\}, \ldots, \{n\}\}$.

iv. $\Delta = \mathcal{P}(V)$ (The $(n-1)$-*simplex*)

v. $\Delta =$ the d-skeleton of the $(n-1)$-simplex: The set of all faces of dimension $\leqslant d$.

29.2 Problem 2

Let Δ be a simplicial complex with Stanley Reisner ideal I_Δ. We can write this ideal using a generating set, but we can also write it as an intersection of prime monomial ideals:

$$I_\Delta = \bigcap_{??} \mathfrak{p}_?$$

Where the prime ideals have a nice combinatorial description in terms of Δ. By playing with examples in `Macaulay2`, make a conjecture as to what this expression should be. Once you're empirically convinced yourself that you know the answer, prove it. (Hints: Use the command `primaryDecomposition.` Note that "prime monomial ideal" is a very restrictive condition.)

29.3 Problem 3

A simplicial complex Δ determines a chain complex of k-vector spaces $\widetilde{C}_\bullet(\Delta)$, where $\widetilde{C}_i(\Delta)$ is the k-vector space with basis the i-dimensional faces of Δ. The differential

$$\partial : \widetilde{C}_i \longrightarrow \widetilde{C}_{i-1}$$

is defined by

$$\partial(\sigma) := \sum_{v\in\sigma} (-1)^{i_v} \sigma \setminus \{v\}$$

where i_v is the position of v among the vertices of σ. $\widetilde{C}_\bullet(\Delta)$ is called the *reduced chain complex of* Δ, and the homology of this chain complex is the *reduced homology of* Δ with k coefficients, denoted $\widetilde{H}_i(\Delta, k)$. For the non-reduced chain complex and non-reduced homology, we make all the same definitions but we replace $\widetilde{C}_{-1}(\Delta)$ with 0. These complexes are accessible through the `SimplicialComplexes` package in `Macaulay2`

For simplicial complexes Δ_1 and Δ_2, give combinatorial interpretations of the complexes below. It will help you to do small examples on paper, and mid-sized examples in `Macaulay2`.

i. $\widetilde{C}_\bullet(\Delta_1) \otimes \widetilde{C}_\bullet(\Delta_2)$.

ii. $C_\bullet(\Delta_1) \otimes C_\bullet(\Delta_2)$.

There is a relationship between the graded Betti numbers of I_Δ and the reduced homology $\widetilde{H}_i(\Delta, k)$. *Hochster's formula* says that

$$\beta_{i,j}(I_\Delta) = \sum_{\substack{W\subseteq V \\ |W|=j}} \widetilde{H}_{j-i-2}(\Delta \cap \mathcal{P}(W), k).$$

The simplicial complex $\Delta \cap \mathcal{P}(W)$ is called the *restriction of* Δ *to* W. Write a `Macaulay2` function that computes the betti number of I_Δ using Hochster's formula. Do you think your approach is slower or faster than the built-in algebraic methods? Test it using the `timing` keyword.

29.4 Problem 4

Hochster's formula ought to provide an explanation for the existence of ideals whose betti numbers depend on the characteristic of the field k, and suggest ways to construct them.

i. Find (or remember from class) the triangulation of $\mathbb{RP}^2$. In light of Hochster's formula, predict which values of $\mathrm{char}(k)$ will give different Betti tables for I_Δ, and verify this using `Macaulay2`.

ii. Building off the above, find an ideal $I \subseteq k[x_1, \ldots, x_n]$ for which the Betti tables displaying $\dim_k \mathrm{Tor}_i^r(R/I, k)$ can take *three* different values, depending on the characteristic of k. Bonus points if your ring and ideal are reasonable enough that `Macaulay2` can actually do these computations.

30 Week of April 1: Alexander Duality

30.1 Problem 1

There is a duality for squarefree monomial ideals called *Alexander duality*, defined as follows: A squarefree monomial ideal I admits a primary decomposition

$$I = P_1 \cap P_2 \cap \ldots \cap P_d$$

where each P_i is generated by a subset of the variables of R. If we define m_i to be the product of the variable generators of P_i, then the Alexander dual of I, denoted I^*, is the ideal

$$I^* = \langle m_1, \ldots, m_d \rangle.$$

If Δ is a simplicial complex on the vertex set $\{1, 2, \ldots, n\}$, then the Alexander dual of Δ, denoted Δ^*, is the simplicial complex on $\{1, 2, \ldots, n\}$ whose maximal faces are the complements of the minimal subsets of $\{1, 2, \ldots, n\}$ that are not faces of Δ

i. Convince yourself that Alexander duality "commutes" with taking Stanley-Reisner ideals, i.e. that for a simplicial complex Δ we have $I_{\Delta^*} = (I_\Delta)^*$.

ii. Prove that Alexander duality is in fact a *duality*: That $(I^*)^* = I$ (equivalently, that $(\Delta^*)^* = \Delta$).

iii. What are the Alexander duals of:

   a. The void complex.
   b. The irrelevant complex.
   c. The d-skeleton of the n-simplex
   d. The minimal triangulation of $\mathbb{RP}^2$ from class.

iv. Give examples of

   a. A simplicial complex that is self-dual: $\Delta = \Delta^*$.
   b. A simplicial complex that is isomorphic to its dual, but where $\Delta \neq \Delta^*$.
   c. A simplicial complex Δ that is *pure* (all maximal faces of Δ are of the same dimension) for which Δ^* is not pure.

30.2 Problem 2

A *labeled simplicial complex* is a simplicial complex Δ together with a vertex labeling $\{1, 2, \ldots, n\} \to \mathbb{N}^m$, where we think of vectors in $\mathbb{N}^m$ as corresponding to monomials in $k[x_1, \ldots, x_m]$. Given a labeling on Δ, we label any higher-dimensional face σ of Δ with m_σ, the least-common multiple of the monomial vertex labels of that face. A labeled simplicial complex determines a chain complex of free $k[x_1, \ldots, x_m]$-modules:

$$\bigoplus_{\substack{\sigma\in\Delta \\ \dim(\sigma)=-1}} Re_\sigma \xleftarrow{\partial} \bigoplus_{\substack{\sigma\in\Delta \\ \dim(\sigma)=0}} Re_\sigma \xleftarrow{\partial} \bigoplus_{\substack{\sigma\in\Delta \\ \dim(\sigma)=1}} Re_\sigma \xleftarrow{\partial} \cdots \xleftarrow{\partial} \bigoplus_{\substack{\sigma\in\Delta \\ \dim(\sigma)=i}} Re_\sigma \xleftarrow{\partial} \cdots$$

Where the differential is defined for a face $\sigma = \{i_1, \ldots, i_d\}$ as

$$\partial(e_\sigma) = \sum_{j=1}^{d} (-1)^{j+1} \frac{m_\sigma}{m_{\sigma\setminus\{i_j\}}} \cdot e_{\sigma\setminus\{i_j\}}$$

i. When Δ is the complete $(n-1)$-simplex on $\{1, 2, \ldots, n\}$ and the vertex labeling is $\{i\} \mapsto x_i$, what is the free resolution determined by this labeling? Is it exact, and what is it resolving?

ii. Write a `Macaulay2` function which takes a simplicial complex Δ and a vertex labeling $\{1, 2, \ldots, n\} \to \mathbb{N}^m$ and returns the resolutions specified above.

iii. Let Δ be the octahedron, where antipodal vertices are labeled with corresponding variables x_0, x_1, y_0, y_1 and z_0, z_1 for expediency. It has six vertices, twelve edges, and eight 2-dimensional faces. What is the alexander dual of Δ?

   A *polyhedral cell complex* is a set $\mathcal{P}$ of convex polytopes in $\mathbb{R}^n$ that is closed under taking intersections, and closed under taking faces. A *labeled polyhedral cell complex* is defined analagously to labeled simplicial complex, only now we have to be more careful with signs. If we choose orientations on all faces of $\mathcal{P}$, then the differential $\partial(e_\sigma$ is the sum of $\pm\frac{m_\sigma}{m_\tau}e_\tau$, where τ ranges over the codimension 1 faces of $sigma$ and the sign is positive if and only if the orientation on τ is induced by the orientation on σ.

iv. Compare your answer in part iii. to the *polar* dual of Δ, which has a vertex for each face of Δ, an edge for each pair of adjacent faces in Δ, and a face for each vertex of Δ. In this case, the polar dual to the octahedron is a (hollow) cube, which is not a simplicial complex but can be thought of as a polyhedral cell complex. If you label the vertices of the cube by the monomial labels of the corresponding faces of Δ, what is the resulting cellular resolution?

30.3 Problem 3

(Challenging) Let Δ be a simplicial complex with Stanley-Reisner ideal I_Δ. We say that Δ is *Cohen-Macaulay* if R/I_Δ is a Cohen-Macaulay ring.

i. Use `Macaulay2` to find examples of Cohen-Macaulay simplicial complexes.

ii. For each Cohen-Macaulay Δ that you found, look at the Betti table of I_{Δ^*}. Make a conjecture about the relationship between Cohen-Macaulayness of Δ and the structure of the minimal free resolution of I_{Δ^*}.