# Computational Algebra by Polymath Jr. 

presented by Ruby Lu

mentored by Alexandra Seceleanu
21st January 2023
» Outline

1. Introduction
2. Betti numbers of quadratic ideals
3. Axial constants

## Introduction

* What is a Polynomial Ring?
* What is an Ideal?
* What is a Minimal Free Resolution?
* What are Betti Numbers?


## Introduction

* What is a Polynomial Ring?
* What is an Ideal?
* What is a Minimal Free Resolution?
* What are Betti Numbers?


## » What is a Polynomial?

## Definition (Monomial) <br> A monomial is a product of variables and scalars.

## Example

$3 x^{9} y^{2}$ is a monomial, but $x^{2}+z$ is not.
Definition (Polynomial)
A polynomial is a sum of monomials.

## Example

$x^{2}+y^{2}+2 z^{2}$ and $6 x^{7}-2 x y^{3}$ are both polynomials.
» What is a Polynomial Ring?
In the following slides, let $k$ denote a field (ex. $\mathbb{R}, \mathbb{Q}$, or the integers modulo 2, denoted here as $\mathbb{F}_{2}$ )

## Definition (Polynomial Ring)

A polynomial ring $R=k\left[x_{1}, \ldots, x_{d}\right]$ over $k$ in $d$ variables is the set of all polynomials formed with $d$ variables and coefficients in $k$.

## Example (Polynomial Ring)

$3 x^{2} y+z^{3} \in \mathbb{Q}[x, y, z]$, but $\sqrt{2} x^{2} \notin \mathbb{Q}[x, y, z]$.
We can multiply and add polynomials in $R$ as normal. They obey the standard commutative, associative, and distributive laws.

## Introduction

* What is a Polynomial Ring?
* What is an Ideal?
* What is a Minimal Free Resolution?
* What are Betti Numbers?


## » What is an Ideal?

## Definition (Ideal)

A subset $\emptyset \neq I \subset k\left[x_{1}, \ldots, x_{d}\right]$ is an ideal if it satisfies:

* if $f, g \in I$, then $f+g \in I$
* If $f \in I$ and $h \in k\left[x_{1}, \ldots, x_{d}\right]$, then $h \cdot f \in I$.


## » What is an Ideal?

## Definition (Ideal)

A subset $\emptyset \neq I \subset k\left[x_{1}, \ldots, x_{d}\right]$ is an ideal if it satisfies:

* if $f, g \in I$, then $f+g \in I$
* If $f \in I$ and $h \in k\left[x_{1}, \ldots, x_{d}\right]$, then $h \cdot f \in I$.


## Definition (Ideal from Generators)

Let $f_{1}, \ldots, f_{s}$ be polynomials in $k\left[x_{1}, \ldots, x_{d}\right]$ and set

$$
\left(f_{1}, \ldots, f_{s}\right)=\left\{\sum_{i=1}^{s} h_{i} f_{i}: h_{1}, \ldots, h_{s} \in k\left[x_{1}, \ldots, x_{d}\right]\right\}
$$

Then $\left(f_{1}, \ldots, f_{s}\right)$ is an ideal.
Example (Maximal Ideal)
$\left(x_{1}, \ldots, x_{d}\right)$ is called the homogeneous maximal ideal. It consists of all polynomials with constant term 0 .

## Introduction

* What is a Polynomial Ring?
* What is an Ideal?
* What is a Minimal Free Resolution?
* What are Betti Numbers?


## » Repeatedly Solving (Resolving) Systems of Polynomials

Set $R=k\left[x_{1}, \ldots, x_{d}\right]$. Let $R^{p}=\{$ all $p$-tuples of polynomials in $R\}$.
We wish to solve a linear system of equations over the polynomial ring $R$. The following are equivalent:

Solve the system $B X=0$ over $R$, where $B$ is a matrix

$$
R^{p} \xrightarrow{B} R^{q} \text { with entries in } R
$$

Describe $\operatorname{Null}(B)$

## » Repeatedly Solving (Resolving) Systems of Polynomials

Set $R=k\left[x_{1}, \ldots, x_{d}\right]$. Let $R^{p}=\{$ all $p$-tuples of polynomials in $R\}$.
We wish to solve a linear system of equations over the polynomial ring $R$. The following are equivalent:

Solve the system $B X=0$ over $R$, where $B$ is a matrix

$$
R^{p} \xrightarrow{B} R^{q} \text { with entries in } R
$$

Describe $\operatorname{Null}(B)$
$R^{p}$ is similar to a vector space; null spaces may not have a basis.

## » Repeatedly Solving (Resolving) Systems of

## Polynomials

$\operatorname{Null}(B)$ may be generated by another matrix $C$, in which case our goal is to describe $\operatorname{Null}(C)$. We get a sequence

$$
R^{\prime} \xrightarrow{C} R^{p} \xrightarrow{B} R^{q}
$$

such that $\operatorname{Col}(C)=\operatorname{Null}(B)$.
But then $\operatorname{Null}(C)$ may be generated by another matrix $D$, so we continue to obtain a sequence

$$
R^{k} \xrightarrow{D} R^{\prime} \xrightarrow{C} R^{p} \xrightarrow{B} R^{q}
$$

so that $\operatorname{Col}(D)=\operatorname{Null}(C)$.
This process continues, resulting in a longer sequence that we call a free resolution.

## » What is a Minimal Free Resolution?

Definition (Free Resolution)
Set $R=k\left[x_{1}, \ldots, x_{d}\right]$. A free resolution is a sequence

$$
R^{\beta_{0}} \stackrel{d_{1}}{\leftrightarrows} R^{\beta_{1}} \stackrel{d_{2}}{\longleftarrow} R^{\beta_{2}} \stackrel{d_{3}}{\longleftarrow} \cdots \stackrel{d_{p}}{\leftarrow} R^{\beta_{p}} \ldots
$$

where each $d_{i}$ is a matrix with (homogenous) entries in $R$,

* (Exactness) Null $\left(d_{i}\right)=\operatorname{Col}\left(d_{i+1}\right)$ for each $i \geq 1$,
* $\beta_{i}=$ the number of columns of $d_{i}$, and
* $\beta_{i-1}=$ the number of rows of $d_{i}$.

Definition (Minimal Free Resolution)
A free resolution is minimal if each of the entries of the matrices $d_{i}$ is in the homogeneous maximal ideal $m$ of $R$.

## » What is a Minimal Free Resolution

## Example Minimal Free Resolution

The minimal free resolution

$$
R^{1} \stackrel{d_{1}=\left[\begin{array}{lll}
x^{3} & x y & y^{5}
\end{array}\right]}{\longleftarrow} R^{3} \longleftarrow d_{2}=\left[\begin{array}{cc}
y & 0 \\
-x^{2} & -y^{4} \\
0 & x
\end{array}\right] R^{2} \stackrel{d_{3}=0}{\leftrightarrows} 0 .
$$

has

$$
\beta_{0}=1, \beta_{1}=3, \beta_{2}=2 .
$$

Since $d_{1}$ has one row, we can obtain an ideal from its entries by setting $I=\left(x^{3}, x y, y^{5}\right) \subseteq R=\mathbb{Q}[x, y]$.
We say that this is the resolution of $R / I$.

## Introduction

* What is a Polynomial Ring?
* What is an Ideal?
* What is a Minimal Free Resolution?
* What are Betti Numbers?


## » What are Betti Numbers?

Definition (Betti Number)
The $i$-th Betti number of a minimal free resolution is $\beta_{i}$.

## Definition (Betti Sequences)

The Betti sequence is $\left(\beta_{i}\right)_{i \geq 0}$, also written $\left(\beta_{0}, \ldots, \beta_{p}\right)$ if $\beta_{i}=0$ for $i>p$.

Definition (Ordering Betti Sequences)
For two Betti sequences $\left(\beta_{i}\right)_{i \geq 0}$ and $\left(\beta_{i}^{\prime}\right)_{i \geq 0}$, we say that $\left(\beta_{i}\right)_{i \geq 0} \geq\left(\beta_{i}^{\prime}\right)_{i \geq 0}$ if $\beta_{i} \geq \beta_{i}^{\prime}$ for all $i \geq 0$.

Example Betti Sequence Order
We have $(1,3,3,1) \geq(1,3,2)$ since $1 \geq 1,3 \geq 3,3 \geq 2$, and $1 \geq 0$.

## » What are Betti Numbers?

## Example Betti Table

The Betti numbers of the free resolution

$$
R^{1} \stackrel{d_{1}}{\leftrightarrows} R^{3} \stackrel{d_{2}}{\leftrightarrows} R^{2} \stackrel{d_{3}}{\leftrightarrows} 0 .
$$

are arranged together into a Betti table

|  | 0 | 1 | 2 |
| :---: | :---: | :---: | :---: |
| total: | 1 | 3 | 2 |
| $0:$ | 1 | . | . |
| 1: | . | 1 | . |
| 2: | . | 1 | 1 |
| 3: | . |  |  |
| 4: | . | 1 | 1 |

The row labeled "total" gives Betti numbers $\beta_{0}=1, \beta_{1}=3, \beta_{2}=2$ with Betti sequence ( $1,3,2$ ).

## Definition (Regularity)

## The Castelnuovo-Mumford regularity $\operatorname{reg}(R / I)$ is the maximum index of a nonzero row in the Betti table of the minimal free resolution of $R / I$.

Informally, $\operatorname{reg}(R / I)$ is a measurement of the highest degrees of the entries of the matrices appearing in the resolution.

Example Regularity

|  | 0 | 1 | 2 |
| :---: | :---: | :---: | :---: |
| total $:$ | 1 | 3 | 2 |
| 0: | 1 | . | . |
| 1: | . | 1 | . |
| 2: | . | 1 | 1 |
| 3: | . | . | . |
| 4: | . | 1 | 1 |

The regularity is $\operatorname{reg}(R / I)=4$.

Betti numbers of quadratic ideals

* Computationally Generating Betti Tables
* Theoretical Approach

Betti numbers of quadratic ideals

* Computationally Generating Betti Tables
* Theoretical Approach
» Computations (Two variables)

1. All possible Betti tables for ideals of $\mathbb{F}_{2}[x, y]$ generated by homogeneous quadratics were computed.

## Computations (Two variables)

1. All possible Betti tables for ideals of $\mathbb{F}_{2}[x, y]$ generated by homogeneous quadratics were computed.
2. There are only 7 such quadratics and thus, only 127 nonempty generating sets.

## » Computations (Two variables)

1. All possible Betti tables for ideals of $\mathbb{F}_{2}[x, y]$ generated by homogeneous quadratics were computed.
2. There are only 7 such quadratics and thus, only 127 nonempty generating sets.
3. These were generated using M2 and it was found that there are only 15 distinct ideals and 4 distinct Betti tables as below.

» Computations (Three variables)
4. Trying the naïve calculations as earlier doesn't work since there are 63 quadratics giving us $2^{63}-1>9 \cdot 10^{18}$ possible generating sets.
» Computations (Three variables)
5. Trying the naïve calculations as earlier doesn't work since there are 63 quadratics giving us $2^{63}-1>9 \cdot 10^{18}$ possible generating sets.
6. However, there is a natural bijection between the set of ideals that we are interested in and the (nonzero) subspaces of $\operatorname{Span} \mathbb{F}_{2}\left\{x^{2}, y^{2}, z^{2}, x y, y z, x z\right\}$.
» Computations (Three variables)
7. Trying the naïve calculations as earlier doesn't work since there are 63 quadratics giving us $2^{63}-1>9 \cdot 10^{18}$ possible generating sets.
8. However, there is a natural bijection between the set of ideals that we are interested in and the (nonzero) subspaces of $\operatorname{Span} \mathbb{F}_{2}\left\{x^{2}, y^{2}, z^{2}, x y, y z, x z\right\}$.
9. This brings down the number to simply 2824 ideals.
10. Trying the naïve calculations as earlier doesn't work since there are 63 quadratics giving us $2^{63}-1>9 \cdot 10^{18}$ possible generating sets.
11. However, there is a natural bijection between the set of ideals that we are interested in and the (nonzero) subspaces of $\operatorname{Span} \mathbb{F}_{2}\left\{x^{2}, y^{2}, z^{2}, x y, y z, x z\right\}$.
12. This brings down the number to simply 2824 ideals.
13. This was computable in M2 and we get a total of 15 distinct Betti tables, as depicted in the next slides.

## » Betti tables (three variables)



## One may refine the above collection and only look at Betti tables corresponding to a fixed codimension.

One may refine the above collection and only look at Betti tables corresponding to a fixed codimension. Here is how the posets of the total Betti sequences look, restricting to each codimension.

One may refine the above collection and only look at Betti tables corresponding to a fixed codimension. Here is how the posets of the total Betti sequences look, restricting to each codimension.


Figure: Hasse diagrams for Betti sequences in 3 variables

Betti numbers of quadratic ideals * Computationally Generating Betti Tables * Theoretical Approach

## » Koszul Complex

## Definition

Let $R$ be a ring. We say that $a$ is a zero divisor in $R$ if $a b=0$ for some nonzero $b \in R$. Otherwise $a$ is $a$ non-zero divisor in $R$.

## Proposition

Let $R=K\left[x_{1}, \ldots, x_{d}\right]$, and $f_{1}, \ldots, f_{n} \in\left(x_{1}, \ldots, x_{d}\right)$ such that $f_{1}$ is a non-zero divisor in $R$, and $f_{i}$ is a non-zero divisor in $R /\left(f_{1}, \ldots, f_{i-1}\right)$ for all $i \in\{2, \ldots, n\}$. Then the following gives a minimal free resolution of $R /\left(f_{1}, \ldots, f_{n}\right)$ :

$$
0 \rightarrow R \xrightarrow{a_{n}} R^{\binom{n}{n-1}} \xrightarrow{a_{n-1}} R^{\binom{n}{n-2}} \rightarrow \cdots \rightarrow R^{\binom{n}{1}} \xrightarrow{a_{1}} R .
$$

## » Mapping Cones

Let $f_{1}, f_{2}, f_{3} \in \mathbb{F}_{2}[x, y, z]$. Then, we have the following exact sequence

$$
0 \rightarrow R /\left(\left(f_{1}, f_{2}\right):\left(f_{3}\right)\right) \rightarrow R /\left(f_{1}, f_{2}\right) \rightarrow R /\left(f_{1}, f_{2}, f_{3}\right) \rightarrow 0
$$

The theory of mapping cones tells us that generally speaking, given minimal free resolutions of the first two terms in the exact sequence, we can determine the minimal free resolution of the last term. The Betti tables "add."

## » Ideals with 1 Generator

This is the simplest case. Indeed, given a nonzero $f \in\left(x_{1}, \ldots, x_{t}\right)$, we simply have

$$
0 \rightarrow R \xrightarrow{d=(f)} R
$$

as a minimal free resolution of $R /(f)$.
Thus, the betti table of $R /(f)$ is

|  | 0 | 1 |
| :---: | :---: | :---: |
| total: | 1 | 1 |
| $0:$ | 1 |  |
| 1: | . | 1 |

» Ideals with 2 Generators
Quadratic ideals $\left(f_{1}, f_{2}\right)$ in $\mathbb{F}_{2}[x, y, z]$ fall into two categories:

1. If $f_{2}$ is a nonzerodivisor in $R /\left(f_{1}\right)$, then by the Koszul complex, the Betti table corresponding to $R / I$ is

|  | 0 | 1 | 2 |
| :---: | :---: | :---: | :---: |
| total: | 1 | 2 | 1 |
| $0:$ | 1 | . | . |
| 1: | . | 2 | . |
| 2: | . | . | 1 |

2. If $f_{2}$ is a zerodivisor in $R /\left(f_{1}\right)$, the Betti table corresponding to $R / I$ is

|  | 0 | 1 | 2 |
| :---: | :---: | :---: | :---: |
| total: | 1 | 2 | 1 |
| $0:$ | 1 |  |  |
| 1: | . | 2 | 1 |

## » Ideals with 3 Generators

To resolve all quadratic ideals $\left(f_{1}, f_{2}, f_{3}\right)$ in $\mathbb{F}_{2}[x, y, z]$, we divide the ideals into four cases:

|  | $f_{2}$ <br> zero divisor <br> in $R /\left(f_{1}\right)$ | $f_{3}$ <br> zero divisor <br> in $R /\left(f_{1}, f_{2}\right)$ | Number | Example |
| :--- | :--- | :--- | :--- | :--- |
| Case 1 |  |  | 512 | $\left(x^{2}, y^{2}, z^{2}\right)$ |
| Case 2 | $\checkmark$ |  | 297 | $\left(x^{2}, x y, z^{2}\right)$ |
| Case 3 | $\checkmark$ | $\checkmark$ | 874 | $\left(x^{2}, y^{2}, x y\right)$ |
| Case 4 |  | $\checkmark$ | 161 | $\left(x^{2}, x y, y^{2}\right)$ |

In all, there are 1844 ideals with three generators in $\mathbb{F}_{2}[x, y, z]$. Except for a special case in case 4 , we managed to use Koszul Complex and Mapping Cone to obtain the Betti Tables for all the ideals in the four cases.

## Axial constants

* Background
* Growth of Axial Constants


## Axial constants

* Background
* Growth of Axial Constants


## » Monomial Orders

Let $R=K\left[x_{1}, \ldots, x_{d}\right]$. For each $\alpha=\left(a_{1}, \ldots, a_{d}\right) \in \mathbb{Z} \geq 0$ set
$x^{\alpha}=x_{1}^{a_{1}} \ldots x_{d}^{a_{d}}$.

## Definition (Graded Reverse Lexicographic (Grevlex) Order)

For each $x^{\alpha}, x^{\beta} \in R, x^{\alpha}>x^{\beta}$ provided that
$\operatorname{deg}\left(x^{\alpha}\right)>\operatorname{deg}\left(x^{\beta}\right)$ or if $\operatorname{deg}\left(x^{\alpha}\right)=\operatorname{deg}\left(x^{\beta}\right)$ and the last nonzero entry of $\alpha-\beta$ is negative.

## Example

Let $R=\mathbb{Q}[x, y, z]$.

* $x^{4} y z>x^{2} y$ because $6>3$
* $x^{2} y>x y z$ because $(2,1,0)-(1,1,1)=(1,0,-1)$


## » Initial Ideals

## Definition (Initial Term)

Given $f \in R \backslash\{0\}$, the initial term of $f$, denoted in $(f)$, is the largest monomial appearing as a term in $f$.

Example
Let $R=\mathbb{Q}[x, y, z]$. Then $\operatorname{in}\left(x^{4} y z+x^{2} y+x y z\right)=x^{4} y z$
Definition (Initial Ideal)
Let $I$ be an ideal. Then the initial ideal of $I$, is defined to be

$$
\operatorname{in}(I):=(\{\operatorname{in}(f) \mid f \in I\})
$$

## » Initial Ideals

Initial ideals depend on the choice of coordinate system.

## Example

Let $I=\left(x^{2}, y^{2}\right) \subseteq \mathbb{Q}[x, y]$. A change of coordinates
$x \mapsto x+y$ and $y \mapsto x-y$, results in

$$
I^{\prime}=\left((x+y)^{2},(x-y)^{2}\right) .
$$

Taking initial ideals,

$$
\operatorname{in}(I)=\left(x^{2}, y^{2}\right) \text { and } \operatorname{in}\left(I^{\prime}\right)=\left(x^{2}, x y, y^{3}\right) .
$$

This motivates the introduction of generic initial ideals.

## » Generic Initial Ideals

## Definition (Generic Initial Ideals)

The generic initial ideal of a homogeneous ideal $I$, denoted $\operatorname{gin}(I)$, is the ideal obtained by first applying a sufficiently general linear change of coordinates on $R$, then taking the initial ideal.

Example
Let $I=\left(x^{2}, y^{2}\right) \subseteq \mathbb{Q}[x, y]$. Taking a sufficiently general change of coordinates $x \mapsto x+y$ and $y \mapsto x-y$ we have

$$
\operatorname{gin}(I)=\operatorname{in}\left((x+y)^{2},(x-y)^{2}\right)=\left(x^{2}, x y, y^{3}\right) .
$$

» Powers of Ideals
We study how the operation of taking the generic initial ideal interacts with the operation of multiplication.

## Definition ( $n$-th Power of an Ideal)

For $n \in \mathbb{N}$ the $n$-th power of an ideal $I$ is the ideal generated by the $n$-fold products of elements of $I$, i.e.,

$$
I^{n}=\left(f_{1} f_{2} \ldots f_{n} \mid f_{i} \in I\right) .
$$

## Example

Suppose $I=\left(x^{2}, y^{2}\right)$. It follows that $I^{2}=\left(x^{4}, x^{2} y^{2}, y^{4}\right)$, $I^{3}=\left(x^{6}, x^{4} y^{2}, x^{2} y^{4}, y^{6}\right)$, etc.

## » What is an Axial Number?

## Definition

Let $I$ be a monomial ideal and $1 \leq i \leq d$. Then we define the $i$-th axial number of $I$, denoted $n_{i}(I)$, to be equal to the smallest power of $x_{i}$ contained in $I$.

Example
Let $I=\left(x^{2}, x y, y^{3}\right)$. Then $n_{1}(I)=2$ and $n_{2}(I)=3$.


## » Axial Numbers of Powers of Ideals

## Proposition

Let I be a monomial ideal and $1 \leq i \leq d$. Then $n_{i}\left(I^{n}\right)$ is linear.

## Example

Let $I=\left(x^{2}, y^{2}\right)$. Then $n_{i}\left(I^{n}\right)=2 n$.




## » What is an Axial Constant?

## Definition (Axial Constants)

For a homogeneous ideal $I$, let $a_{i}(I)=n_{i}(\operatorname{gin}(I))$.

## Definition

Let $I$ be a homogenous ideal. Let $a_{i}(n)=a_{i}\left(I^{n}\right)$.

## Example

Let $I=\left(x^{2}, y^{2}\right) \subseteq \mathbb{Q}[x, y]$. So $\operatorname{gin}(I)=\left(x^{2}, x y, y^{3}\right)$, and we can show that $a_{i}(n)=2 n+i-1$.




## » Significance

Proposition
If $r$ is the largest integer for which $a_{r}(I)$ is defined, then $a_{r}(I)=\operatorname{reg}(I)$.

## Fact

$\operatorname{reg}\left(I^{n}\right)$ is linear for $n \gg 0$.
Corollary
$a_{r}(n)$ is linear for $n \gg 0$.

## Axial constants

* Background
* Growth of Axial Constants


## » Linearity of Axial Constants

## Let $I$ be a homogeneous ideal.

## Theorem

For some $\bar{I}$ depending on $I, a_{i}(n)=\operatorname{reg}\left(\bar{I}^{n}\right)$.
Corollary (Linearity of Axial Constants)
$a_{i}(n)$ is linear for $n \gg 0$.
Example (First Axial Constant)
$a_{1}(n)=n a_{1}(I)$
Example (Last Axial Constant)
If $I=\left(x_{1}^{a_{1}}, \ldots, x_{d}^{a_{d}}\right)$ and $a=\max \left\{a_{i}\right\}$ then

$$
a_{d}(n)=a(n-1)+\left(a_{1}+\ldots+a_{d}\right)-(d-1) .
$$

Thanks to our Polymath mentor Professor Alexandra Seceleanu and NCUWM for providing such a valuable opportunity to share our work!

