Frodo Meets Neo: Studying rings using matrices

Amelia Taylor

Colorado College

Young Mathematicians Conference, August 2007

Outline

Some Ring Examples

A ring is a set with two binary operations that play nice and one makes the set an Abelian group.

Example

1. $\mathbb{Z}$
2. $\mathbb{Q}$
3. $\mathbb{R}[x, y, z] = \{\textit{polynomials in the indeterminates } x, y, z \textit{ with coefficients in } \mathbb{R}\}.$
4. $M_n(R) = \{n \times n \textit{ matrices with entries in the ring } R\}.$

We'll assume all our rings are *commutative* and have *unity*.

Ideals

An ideal I of a ring R is a subring of R with the additional property that for all $a \in I$ and $r \in R$, $ar \in I$.

Example

1. *In $\mathbb{Z}$ all multiples of 3 form an ideal, denoted $\langle 3 \rangle$.*
2. *In $\mathbb{R}[x, y, z]$ all polynomials with each term divisible by at least one of x or y form an ideal, denoted $\langle x, y \rangle$.*
3. *In $M_2(R)$ all multiples of $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ form an ideal.*

Quotient Rings

$\frac{R}{I}$ is the set of equivalence classes under the relation $a \equiv b$ iff $a - b \in I$. We usually denote the equivalence classes by $a + I$.

Example

1. $\frac{\mathbb{Z}}{\langle 3 \rangle}$ *and* $2 + \langle 3 \rangle = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$
2. $\frac{\mathbb{R}[x,y,z]}{\langle x,y \rangle}$ *and* $z + \langle x, y \rangle = \{z, z+x, z+y, z+x-5y, z+x^2y^3z^8+4z^6y^7, \ldots\}$.

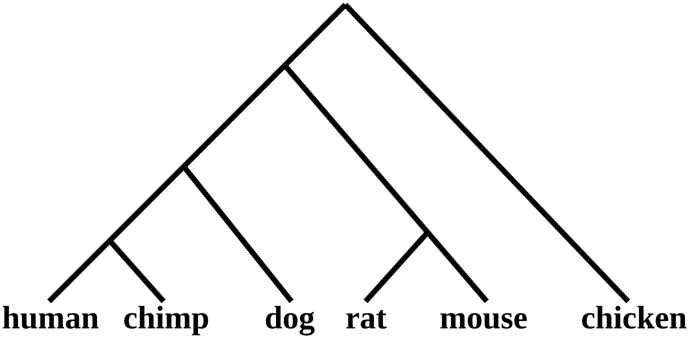
Some areas where rings might be useful

- Phylogenetics
- SET® Game
- Gene Networks
- Statistics
- Game Theory

There are many others, but the first 3 represent recent developments that I have worked on and the other two I've studied some.

Phylogenetics: Intro to Evolutionary Bio

Goal: Given sequence (morphological, molecular (DNA), geographical) data infer a "tree" that describes the evolutionary descent.



How do we build such trees from only knowing the leaves? This is the study of phylogenetics.

Phylogenetics: Polynomials

E. neopterum	AAAGCCCTCGAATGAGCC
E. nigripinne	AAAGCCCTCGGATGAGCC
E. pseudovulatum	AAAGCCCTCGAATGAGCC
E. crossopterum	AAAGCCCTCGGATGAGCC
E. squamiceps	AAGGACCTCGGATGAGCC

Phylogenetics: Polynomials

E. neopterum	AAAGCCCTCGAATGAGCC
E. nigripinne	AAAGCCCTCGGATGAGCC
E. pseudovulatum	AAAGCCCTCGAATGAGCC
E. crossopterum	AAAGCCCTCGGATGAGCC
E. squamiceps	AAGGACCTCGGATGAGCC

$\hat{p}_{AAAAA} = 4/18$ $\hat{p}_{CCCCC} = 5/18$ $\hat{p}_{GGGGG} = 4/18$
$\hat{p}_{TTTTT} = 2/18$ $\hat{p}_{AAAAG} = 1/18$ $\hat{p}_{CCCCA} = 1/18$
$\hat{p}_{AGAGG} = 1/18$

We call these *frequency data*.

Goal: Polynomials based on a tree and a model that evaluate to 0 on frequency data for the correct tree and do not for the wrong tree.

Phylogenetics: Polynomials

Goal: Polynomials based on a tree and a model that evaluate to 0 on frequency data for the correct tree and do not for the wrong tree.

Example

For a 5 fish (taxa) tree, if we assume any of the 4 nucleotides are equally possible, we might expect the number of GGGGG patterns to match the number of AAAAA patterns, so a polynomial representing this is $X_{AAAAA} - X_{GGGGG}$.

Phylogenetics: Polynomials

Goal: Polynomials based on a tree and a model that evaluate to 0 on frequency data for the correct tree and do not for the wrong tree.

Example

For a 5 fish (taxa) tree, if we assume any of the 4 nucleotides are equally possible, we might expect the number of GGGGG patterns to match the number of AAAAA patterns, so a polynomial representing this is $X_{AAAAA} - X_{GGGGG}$.

Good polynomial as it is based on the model. It is not useful because

1. it is based on a very simple model.
2. it is not based on the tree.

Phylogenetics: Polynomials

Goal: Polynomials based on a tree and a model that evaluate to 0 on frequency data for the correct tree and do not for the wrong tree.

Some of what is known:

- The full set of polynomials for certain models.
- Biologically significant polynomials for several general models.

It is not known how to effectively use these polynomials with actual data.

SET® Game

Consists of a deck of cards.

Exactly one card for each combination.

Color	Number	Shape	Shade
red	1	oval	open
green	2	diamond	solid
purple	3	squiggle	striped

A *SET* is a collection of 3 cards such that for every parameter the cards are all the same or all different.

SET® Game

Key Question: What is the maximal number of cards that do not contain a SET®?

SET® Game

Key Question: What is the maximal number of cards that do not contain a SET®?

The answer is 20 for the game, 45 for 5 parameters and open for ≥ 6 parameters.

SET® Game

Key Question: What is the maximal number of cards that do not contain a SET®?

The answer is 20 for the game, 45 for 5 parameters and open for ≥ 6 parameters.

Let $R = k[x_1, \ldots, x_{81}]$ with each variable corresponding to a card in the SET® deck.

Set I to be the ideal generated by $x_i x_j x_k$ where x_i, x_j and x_k correspond to 3 cards that form a SET®.

Then $\dim(R/I)$ is the maximal number of cards not containing a SET.

Introduction

A vectorspace is a set V with a binary operation (vector addition) that makes it an abelian group along with a field F and an operation (scalar multiplication) that allows F to act on V in a nice way.

Example

1. $\mathbb{R}^n$ *with component addition over the field* $\mathbb{R}$. *This vector space has a particularly nice basis,* $e_1, \ldots, e_n$ *where* e_i *has a 1 in the ith spot and* 0*'s elsewhere.*
2. $\mathbb{R}[x]$ *with polynomial addition over* $\mathbb{R}$. *A basis in this case is* $1, x, x^2, x^3, \ldots$.

Mapping Vector Spaces

Let V be a vector space over $\mathbb{R}$ with basis $v_1, \ldots, v_n$.

Define $\phi : \mathbb{R}^n \to V$ by $\phi(e_i) = v_i$.

For vectorspaces

- It is enough to define a function by what it does to the basis.
- ϕ is naturally onto, but since V is a vector space it also an *isomorphism*.
- Define $\ker \phi = \{\mathbf{v} \in \mathbb{R}^n \mid \phi(\mathbf{v}) = \mathbf{0}\}$.

Mapping Pictures

Let $\phi : \mathbb{R}^n \to V$ by $\phi(e_i) = v_i$. Then

- ϕ is both surjective and injective (so $\ker(\phi) = \{\mathbf{0}\}$).
- Use the picture

$$0 \longrightarrow \mathbb{R}^n \xrightarrow{\phi} V \longrightarrow 0$$

to illustrate that the image of one map is the kernel of the next map.

We'll use such pictures many more times.

Modules

A module is a vectorspace, but the scalars come from a *ring* rather than a field.

Example

Let R be a ring.

1. R^n *is a module over* R *with basis* $e_1, \ldots, e_n$.
2. $R[x]$ *is a module over* R *with basis* $1, x, x^2, \ldots$.
3. *If* I *is an ideal of* R *then* I *is a module over* R*. It has no "basis", but for all the rings we consider it has a finite generating set.*

Intro to Free Modules

Definition

A *free module* is an R-module that has a basis.

- Basis here means the same thing it does for vector spaces.
- The module R^n a free module with basis $e_1, \ldots, e_n$.
- Just as all vectorspaces over $\mathbb{R}$ are isomorphic to $\mathbb{R}^n$, all free modules over R are isomorphic to R^n.
- We want to use R^n to help us understand non-free modules; particularly ideals and quotient rings.

Mapping Modules

Let M be a module over R with generating set $m_1, \ldots, m_n$.

Define $\phi : R^n \to M$ by $\phi(e_i) = m_i$.

Again, $\ker \phi = \{\mathbf{v} \in R^n \mid \phi(\mathbf{v}) = \mathbf{0}\}$.

Mapping Modules

Let M be a module over R with generating set $m_1, \ldots, m_n$.

Define $\phi : R^n \to M$ by $\phi(e_i) = m_i$.

Again, $\ker \phi = \{\mathbf{v} \in R^n \mid \phi(\mathbf{v}) = \mathbf{0}\}$.

For Modules

- It is enough to define a function by what it does to the generating set.
- ϕ is naturally onto.
- ϕ is not necessarily an isomorphism, so it is possible that $\ker(\phi) \neq \{\mathbf{0}\}$. (It is an isomorphism iff M is free and $m_1, \ldots, m_n$ is a basis.)

Mapping Modules Example

Example

Let $R = \mathbb{R}[x, y, z]$ *and* $I = \langle x^2, xy, y^2 \rangle$. *Then*

- I *is an* R *module with generating set* $\{x^2, xy, y^2\}$.
- ϕ *maps* R^3 *onto* I *by*
  - $\phi(e_1) = \phi\left(\begin{bmatrix}1\\0\\0\end{bmatrix}\right) = x^2$, $\phi(e_2) = \phi\left(\begin{bmatrix}0\\1\\0\end{bmatrix}\right) = xy$, *and*
    $\phi(e_3) = \phi\left(\begin{bmatrix}0\\0\\1\end{bmatrix}\right) = y^2$.
  - $\phi\left(\begin{bmatrix}3y^2\\2x\\4x - z\end{bmatrix}\right) = 3y^2(x^2) + 2x(xy) + (4x - z)(y^2)$.
- *The kernel contains elements like* $ye_1 - xe_2$ *and* $ye_2 - xe_3$.

Using Maps

Let M be an R-module with generating set $\{g_1, \ldots, g_n\}$.

[Example: $I = \langle x^2, xy, y^2 \rangle \in \mathbf{R}[x, y, z]$]

Then $\phi : R^n \to M$ with $\phi(e_i) = g_i$ gives a surjective map of the free module R^n onto M.

Using Maps

Let M be an R-module with generating set $\{g_1, \ldots, g_n\}$.

[Example: $I = \langle x^2, xy, y^2 \rangle \in \mathbf{R}[x, y, z]$]

The picture $R^n \to M \to 0$ tells us about the generators of M:

- there are n and
- a matrix representation of ϕ, $\begin{bmatrix} g_1 & g_2 & \ldots & g_n \end{bmatrix}$ shows a generating set.

$$\begin{bmatrix} g_1 & g_2 & \ldots & g_n \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = g_2$$

Using Maps

Let M be an R-module with generating set $\{g_1, \ldots, g_n\}$.
[Example: $I = \langle x^2, xy, y^2 \rangle \in \mathbf{R}[x, y, z]$]

The picture $R^n \to M \to 0$ tells us about the generators of M:

What about the kernel of ϕ? It may or may not be free.

What about the kernel of ϕ?

$$R^n \to M \to 0$$

If ker(ϕ) *is* free:

- We have two free modules that tell us all about the generators and the relations for the module.
- Using theorems about free modules we know lots (algebraically) about M, in particular if the kernel has m basis elements, we get the picture

$$0 \longrightarrow R^m \xrightarrow{\iota} R^n \xrightarrow{\phi} M \longrightarrow 0$$

This is a *free resolution* of M.

What about the kernel of ϕ?

If $\ker(\phi)$ *is not* free, let n_1 be the number of generators of $\ker(\phi)$. Then there is a map $\phi_1 : R^{n_1} \to \ker(\phi)$.

$$\begin{tikzcd}
R^{n_1} \arrow[dr, "\phi_1"] & & R^n \arrow[r, "\phi"] & M \arrow[r] & 0 \\
& \ker(\phi) \arrow[ur, "\iota"] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

Composing ϕ_1 and ι gives a map $R^{n_1} \to R^n$ whose image is the kernel of ϕ. Label this map ϕ_1. Now the picture of M is ...

What about the kernel of ϕ?

Composing ϕ_1 and ι gives a map $R^{n_1} \to R^n$ whose image is the kernel of ϕ. Label this map ϕ_1. Now the picture of M is ...

$$R^{n_1} \xrightarrow{\phi_1} R^n \xrightarrow{\phi} M \longrightarrow 0$$

with $\mathrm{im}(\phi_1) = \ker(\phi)$

What about $\ker(\phi_1)$?

What about $\ker(\phi_1)$?

$$R^{n_1} \xrightarrow{\phi_1} R^n \xrightarrow{\phi} M \longrightarrow 0$$

and $\mathrm{im}(\phi_1) = \ker(\phi)$

Iterate the process:

If $\ker(\phi_1)$ is free of dimension n_2 we are done and get the *free resolution*.

$$0 \longrightarrow R^{n_2} \xrightarrow{\iota} R^{n_1} \xrightarrow{\phi_1} R^n \xrightarrow{\phi} M \longrightarrow 0$$

What about $\ker(\phi_1)$?

$$R^{n_1} \xrightarrow{\phi_1} R^n \xrightarrow{\phi} M \longrightarrow 0$$

and $\mathrm{im}(\phi_1) = \ker(\phi)$

If $\ker(\phi_1)$ is not free it has n_2 generators. Set $\phi_2 : R^{n_2} \to \ker(\phi_1)$ the big picture is

$$\begin{tikzcd}
R^{n_2} \arrow[dr, "\phi_2"] & & R^{n_1} \arrow[dr, "\phi_1"] & & R^n \arrow[r, "\phi"] & M \arrow[r] & 0 \\
& \ker(\phi_1) \arrow[ur, "\iota"] \arrow[dr] & & \ker(\phi) \arrow[ur, "\iota"] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

What about $\ker(\phi_1)$?

the big picture is

$$\begin{tikzcd}
R^{n_2} \arrow[dr, "\phi_2"] & & R^{n_1} \arrow[dr, "\phi_1"] & & R^n \arrow[r, "\phi"] & M \arrow[r] & 0 \\
& \ker(\phi_1) \arrow[ur, "\iota"] \arrow[dr] & & \ker(\phi) \arrow[ur, "\iota"] \arrow[dr] & & & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

Composing ϕ_2 and ι we get the new picture

$$R^{n_2} \xrightarrow{\phi_2} R^{n_1} \xrightarrow{\phi_1} R^n \xrightarrow{\phi} M \longrightarrow 0$$

Iterating, we look at $\ker(\phi_2)$.

Theorem (Hilbert Syzygy Theorem, ˜1888)

For modules over polynomial rings over a field, this process must stop after a finite number of steps, i.e. the kernel will be a free module after a finite number of iterations.

(Hilbert 1863-1943)

Example

Consider $I = \langle x^2, xy, y^2 \rangle \in k[x,y,z] = R$, where k is a field.

- 3 generators: x^2, xy, y^2.
- 3 relations: $s_1 = ye_1 - xe_2$, $s_2 = ye_2 - xe_3$, and $s_3 = y^2e_1 - x^2e_3$ (given as elements of R^3).
- $s_3 = ys_1 - xs_2$, so s_1 and s_2 generate the module of relations.
- There are no relations on s_1 and s_2 the free resolution is

$$0 \longrightarrow R^2 \xrightarrow{\begin{bmatrix} y & 0 \\ -x & y \\ 0 & -x \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} x^2 & xy & y^2 \end{bmatrix}} I \longrightarrow 0$$

Example

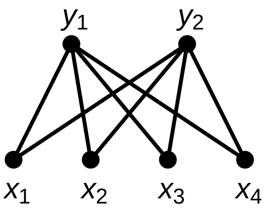
$$I = \langle x^2, xy, y^2 \rangle \in k[x,y,z] = R$$

$$0 \longrightarrow R^2 \xrightarrow{\begin{bmatrix} y & 0 \\ -x & y \\ 0 & -x \end{bmatrix}} R^3 \xrightarrow{\begin{bmatrix} x^2 & xy & y^2 \end{bmatrix}} I \longrightarrow 0$$

- Macaulay2, Singular, CoCoA, Sage, Magma, others.
- Complexity can be very bad.
- Some theorems describing the structure.
  - 1966Taylor resolution. Generally not minimal.
  - Mid 90's Bayer, Sturmfels give cellular resolutions.
  - Late 90's others begin work on combinatorial expressions of the Betti numbers and some minimal free resolutions.
  - Last 2 years there has been lots of activity.

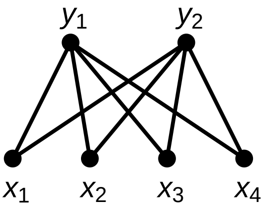
Theorem (Visscher, Coyle)

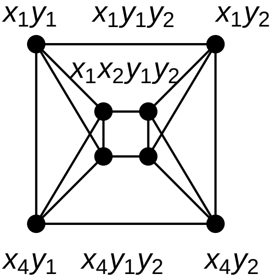
If I is the ideal of the hypergraph generated by the maximal cliques of a complete multi-partite graph, then the cellular resolution is a minimal free resolution.



Theorem (Visscher, Coyle)

If I is the ideal of the hypergraph generated by the maximal cliques of a complete multi-partite graph, then the cellular resolution is a minimal free resolution.

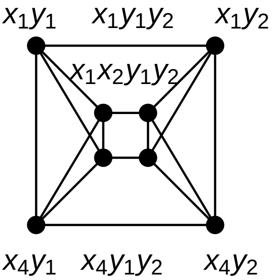




$$0 \longrightarrow R \longrightarrow R^6 \longrightarrow R^{14} \longrightarrow R^{16} \longrightarrow R^8 \longrightarrow I \longrightarrow 0$$

Theorem (Visscher, Coyle)

If I is the ideal of the hypergraph generated by the maximal cliques of a complete multi-partite graph, then the cellular resolution is a minimal free resolution.



$$
\begin{array}{c c}
 & x_1x_2x_3x_4y_1y_2 \\
\begin{array}{c} x_1x_2x_3x_4y_1 \\ x_1x_2x_3x_4y_2 \\ x_1x_2x_3y_1y_2 \\ x_1x_2x_4y_1y_2 \\ x_1x_3x_4y_1y_2 \\ x_2x_3x_4y_1y_2 \end{array} & \begin{bmatrix} y_2 \\ -y_1 \\ -x_4 \\ x_3 \\ -x_2 \\ x_1 \end{bmatrix}
\end{array}
$$

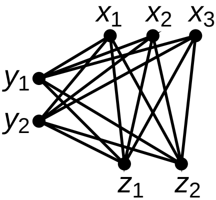
Theorem (Visscher, Coyle)

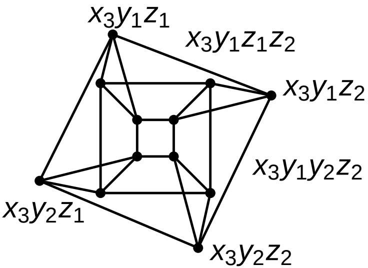
If I is the ideal of the hypergraph generated by the maximal cliques of a complete multi-partite graph, then the cellular resolution is a minimal free resolution.

$$0 \longrightarrow R \xrightarrow{\begin{bmatrix} y_2 \\ -y_1 \\ -x_4 \\ x_3 \\ -x_2 \\ x_1 \end{bmatrix}} R^6 \longrightarrow R^{14} \longrightarrow R^{16} \longrightarrow R^8 \xrightarrow{\begin{bmatrix} x_1y_1x_2y_1 \ldots \end{bmatrix}} I \longrightarrow 0$$

Theorem (Visscher, Coyle)

If I is the ideal of the hypergraph generated by the maximal cliques of a complete multi-partite graph, then the cellular resolution is a minimal free resolution.





$$E = \{\{x_1, y_1, z_1\}, \{x_1, y_1, z_2\}, \{x_1, y_2, z_1\}, \{x_1, y_2, z_2\},$$
$$\{x_2, y_1, z_1\}, \{x_2, y_1, z_2\}, \{x_2, y_2, z_1\}, \{x_2, y_2, z_2\},$$
$$\{x_3, y_1, z_1\}, \{x_3, y_1, z_2\}, \{x_3, y_2, z_1\}, \{x_3, y_2, z_2\}\}$$

Corollary (Visscher)

The resolution is linear, so the kth graded Betti number for the ideal of a complete bi-partite graph is

$$\sum_{j=1}^{k+1} \binom{n}{j} \binom{m}{k-j+2}.$$

Corollary (Coyle)

The resolution in the multi-partite case is also linear and we get a combinatorial formula for the kth graded Betti number.

Future

- Are there similar results for other complete graphs?
- Are there similar results for other partite graphs?
- Are there similar results for the full minimal free resolution for the ideals discussed in Huy Tái Há and Adam Van Tuyl's paper "Resolutions of square free monomial ideals via facet ideals: a survey" found in the mathematics arXiv and related papers?

In general finding combinatorial structures for minimal free resolutions of monomial ideals is a useful and open question.