The Theory of Resolvent Degree,
after Hamilton, Sylvester, Hilbert, Segre and Brauer.

Jesse Wolfson
University of California, Irvine

No Boundaries - Groups in Algebra, Geometry and Topology
In honor of Benson Farb
October 27, 2017
Ongoing joint work with Benson Farb
Ongoing joint work with Benson Farb

With Love,
Farbio
Ongoing joint work with Benson Farb
Given $X$, how hard is it to find $Y$?
Given $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>general sextic</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^6 + a_1 x^5 + \cdots + a_6$</td>
</tr>
</tbody>
</table>
Given $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>general sextic</th>
<th>$x^6 + a_1x^5 + \cdots + a_6$</th>
<th>a root</th>
</tr>
</thead>
</table>

Goal: Explain how these three questions can be precisely related.
**Given** $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>general sextic</th>
<th>cubic surface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^6 + a_1x^5 + \cdots + a_6$</td>
<td><img src="image" alt="cubic surface" /></td>
</tr>
<tr>
<td>a root</td>
<td></td>
</tr>
</tbody>
</table>
Given $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>general sextic</th>
<th>cubic surface</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^6 + a_1x^5 + \cdots + a_6$</td>
<td>a root</td>
</tr>
<tr>
<td></td>
<td>a line</td>
</tr>
</tbody>
</table>
Given $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>General Sextic</th>
<th>Cubic Surface</th>
<th>Jacobian</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^6 + a_1x^5 + \cdots + a_6$</td>
<td>a root</td>
<td>a line</td>
</tr>
</tbody>
</table>

Goal: Explain how these three questions can be precisely related.
Given $X$, how hard is it to find $Y$?

<table>
<thead>
<tr>
<th>general sextic</th>
<th>cubic surface</th>
<th>Jacobian</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^6 + a_1x^5 + \cdots + a_6$</td>
<td>a root</td>
<td>a line</td>
</tr>
<tr>
<td></td>
<td>a level structure</td>
<td></td>
</tr>
</tbody>
</table>
Given $X$, how hard is it to find $Y$?

**Goal:** Explain how these three questions can be precisely related.
Overview

Definitions and Remarks

Variations on the theme of the 27 lines
   RD and Classical Enumerative Problems
   RD and Roots of Polynomials
   RD and Congruence Subgroups

Conclusion
Set-up

$k$ - ground field (for this talk, assume $\text{char}(k) = 0$)
Set-up

$k$ - ground field (for this talk, assume $\text{char}(k) = 0$)
$\mathcal{M}$ - variety over $k$
Set-up

$k$ - ground field (for this talk, assume $\text{char}(k) = 0$)
$\mathcal{M}$ - variety over $k$
$\mathcal{M}' \rightarrow \mathcal{M}$ - finite dominant map (i.e. restricts to a cover of a Zariski open)
Set-up

$k$ - ground field (for this talk, assume $\text{char}(k) = 0$)

$\mathcal{M}$ - variety over $k$

$\mathcal{M}' \to \mathcal{M}$ - finite dominant map (i.e. restricts to a cover of a Zariski open)

Example:
Set-up

\( k \) - ground field (for this talk, assume \( \text{char}(k) = 0 \))
\( \mathcal{M} \) - variety over \( k \)
\( \mathcal{M}' \rightarrow \mathcal{M} \) - finite dominant map (i.e. restricts to a cover of a Zariski open)

**Example:**

\( \mathcal{P}_n \) - space of monic degree \( n \) polynomials
Set-up

$k$ - ground field (for this talk, assume $\text{char}(k) = 0$)

$\mathcal{M}$ - variety over $k$

$\mathcal{M}' \to \mathcal{M}$ - finite dominant map (i.e. restricts to a cover of a Zariski open)

**Example:**

$\mathcal{P}_n$ - space of monic degree $n$ polynomials

$\tilde{\mathcal{P}}_n := \{(P, z) \in \mathcal{P}_n \times \bar{k} \mid P(z) = 0\}$

- space of polynomials with a choice of root
Set-up

\( k \) - ground field (for this talk, assume \( \text{char}(k) = 0 \))

\( \mathcal{M} \) - variety over \( k \)

\( \mathcal{M}' \rightarrow \mathcal{M} \) - finite dominant map (i.e. restricts to a cover of a Zariski open)

**Example:**

\( \mathcal{P}_n \) - space of monic degree \( n \) polynomials

\( \widetilde{\mathcal{P}}_n := \{(P, z) \in \mathcal{P}_n \times \bar{k} \mid P(z) = 0\} \)

- space of polynomials with a choice of root

Forgetting the root gives a branched cover

\[ \widetilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n \]

\[ (P, z) \mapsto P \]
Examples of $\mathcal{M}' \to \mathcal{M}$:

- $\tilde{\mathcal{P}}_n \to \mathcal{P}_n$
  (polynomials with or w/o a root)
Set-up

Examples of $\mathcal{M}' \rightarrow \mathcal{M}$:

- $\tilde{P}_n \rightarrow P_n$
  (polynomials with or w/o a root)

- $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$
  (cubic surfaces with or w/o a line)
Set-up

Examples of $\mathcal{M}' \rightarrow \mathcal{M}$:

- $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$
  (polynomials with or w/o a root)

- $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$
  (cubic surfaces with or w/o a line)

- $\mathcal{A}_g[L] \rightarrow \mathcal{A}_g$
  (PPAVs with or w/o a level structure)
Examples of $\mathcal{M}' \rightarrow \mathcal{M}$:

- $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$
  
  (polynomials with or w/o a root)

- $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$
  
  (cubic surfaces with or w/o a line)

- $\mathcal{A}_g[L] \rightarrow \mathcal{A}_g$
  
  (PPAVs with or w/o a level structure)

**Want:** A common invariant that captures the complexity of specifying a point in the cover given a point in the base.
Definition

The essential dimension $\text{ed}_k(\mathcal{M}' \to \mathcal{M})$ is the minimum $d$ for which there exists a Zariski open $U \subset \mathcal{M}$ and a pullback square

\[
\begin{array}{ccc}
\mathcal{M}'|_U & \to & \tilde{Y} \\
\downarrow & & \downarrow \\
U & \to & Y
\end{array}
\]

with $\dim_k(Y) = d$. 
Resolvent Degree

Definition
The resolvent degree \( \text{RD}_k(\mathcal{M}' \to \mathcal{M}) \) is the minimum \( d \) such that there exists a tower of finite dominant maps

\[
E_r \to \cdots \to E_1 \to E_0 = \mathcal{M}
\]

with

\[
\begin{array}{ccc}
E_r & \longrightarrow & \mathcal{M}' \\
\downarrow & & \downarrow \\
\mathcal{M} & \longrightarrow & \mathcal{M}
\end{array}
\]

and with \( \text{ed}_k(E_i \to E_{i-1}) \leq d \) for all \( i \).
Remarks

Resolvent degree quantifies “how hard” it is to specify a point in a cover, given a point in the base.
Resolvent degree quantifies “how hard” it is to specify a point in a cover, given a point in the base.

Cyclic covers are much simpler than general covers, for example:
Remarks

Resolvent degree quantifies “how hard” it is to specify a point in a cover, given a point in the base.

Cyclic covers are much simpler than general covers, for example:

- Newton’s method (i.e. $z \mapsto z - \frac{P(z)}{P'(z)}$) gives a reliable iterative algorithm for extracting radicals.

\[ \text{Theorem (McMullen, 1988)} \]

There is no generally convergent iterative algorithm for finding the roots of a general polynomial of degree $\geq 4$. $\text{RD} = 1$ reflects this.
Remarks

Resolvent degree quantifies “how hard” it is to specify a point in a cover, given a point in the base.

Cyclic covers are much simpler than general covers, for example:

- Newton’s method (i.e. \( z \mapsto z - \frac{P(z)}{P'(z)} \)) gives a reliable iterative algorithm for extracting radicals.

Theorem (McMullen, 1988)

There is no generally convergent iterative algorithm for finding the roots of a general polynomial of degree \( \geq 4 \).
Remarks

Resolvent degree quantifies “how hard” it is to specify a point in a cover, given a point in the base.

Cyclic covers are much simpler than general covers, for example:

- Newton’s method (i.e. \( z \mapsto z - \frac{P(z)}{P'(z)} \)) gives a reliable iterative algorithm for extracting radicals.

**Theorem (McMullen, 1988)**

*There is no generally convergent iterative algorithm for finding the roots of a general polynomial of degree \( \geq 4 \).*

\( RD = 1 \) reflects this.
Remarks, cont.

Consider $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$ (moduli of polynomials with and w/o a root)
Remarks, cont.

Consider \( \tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n \) (moduli of polynomials with and w/o a root)

Theorem (Babylonians)

\( \text{RD}_k(\tilde{\mathcal{P}}_2 \rightarrow \mathcal{P}_2) = 1. \)
Remarks, cont.

Consider $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$ (moduli of polynomials with and w/o a root)

**Theorem (Babylonians)**

$\text{RD}_k (\tilde{\mathcal{P}}_2 \rightarrow \mathcal{P}_2) = 1$.

**Theorem (Tartaglia, Cardano, Ferrari)**

*For* $n \leq 4$, $\text{RD}_k (\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n) = 1$. 

Consider $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$ (moduli of polynomials with and w/o a root)

**Theorem (Babylonians)**
$RD_k(\tilde{\mathcal{P}}_2 \rightarrow \mathcal{P}_2) = 1$.

**Theorem (Tartaglia, Cardano, Ferrari)**
For $n \leq 4$, $RD_k(\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n) = 1$.

**Theorem (Bring, 1786)**
$RD_k(\tilde{\mathcal{P}}_5 \rightarrow \mathcal{P}_5) = 1$. 
Remarks, cont.

Conjecture (Hilbert)
\[ \text{RD}_k(\tilde{P}_n \rightarrow \mathcal{P}_n) \geq 2 \text{ for } n \geq 6. \]
Conjecture (Hilbert)
\[
\text{RD}_k(\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n) \geq 2 \text{ for } n \geq 6.
\]

Theorem (Doyle–McMullen, 1989)

There exists a tower of iterative algorithms for extracting the roots of a general polynomial of degree at most 5. For \( n > 5 \), no such tower exists.
Conjecture (Hilbert)
$$\text{RD}_k(\tilde{P}_n \rightarrow P_n) \geq 2 \text{ for } n \geq 6.$$ 

Theorem (Doyle–McMullen, 1989)

*There exists a tower of iterative algorithms for extracting the roots of a general polynomial of degree at most 5. For $n > 5$, no such tower exists.*

∴ If you believe Hilbert’s conjecture, Doyle–McMullen is another example of how RD $> 1$ captures intuitive notions of complexity of a problem.
Essential dimension - introduced in 1998 by Buhler and Reichstein.
Essential dimension - introduced in 1998 by Buhler and Reichstein. From the definition, \( ed_k \geq RD_k \).
Essential dimension - introduced in 1998 by Buhler and Reichstein. From the definition, $\text{ed}_k \geq \text{RD}_k$.
In general, the difference can be arbitrarily large:

\[ M := \{ p(z) \in \mathbb{P}^2_n \mid p(z) = (z^2 - a_1) \cdots (z^2 - a_n) \} \]

\[ M' := \tilde{\mathbb{P}}^2_n \mid M \].

Then for $n > 1$

\[ \text{ed}_k (M' \rightarrow \rightarrow M) = n > \gg \text{RD}_k (M' \rightarrow \rightarrow M) = 1 \]

$\therefore$ ed$_k$ very sensitive to arithmetic of the fields $k$ and $k'$. RD$_k$ captures traditional notions of complexity of a problem.
Essential dimension - introduced in 1998 by Buhler and Reichstein. From the definition, \( \text{ed}_k \geq \text{RD}_k \).

In general, the difference can be arbitrarily large:

\[
\mathcal{M} := \{ p(z) \in \mathcal{P}_{2n} \mid p(z) = (z^2 - a_1) \cdots (z^2 - a_n) \}
\]

\[
\mathcal{M}' := \tilde{\mathcal{P}}_{2n}|_{\mathcal{M}}.
\]

Then for \( n > 1 \)

\[
\text{ed}_k(\mathcal{M}' \to \mathcal{M}) = n \gg \text{RD}_k(\mathcal{M}' \to \mathcal{M}) = 1
\]
Essential dimension - introduced in 1998 by Buhler and Reichstein. From the definition, $\text{ed}_k \geq \text{RD}_k$. In general, the difference can be arbitrarily large:

$$
\mathcal{M} := \{ p(z) \in \mathcal{P}_{2n} \mid p(z) = (z^2 - a_1) \cdots (z^2 - a_n) \}
$$

$$
\mathcal{M}' := \tilde{\mathcal{P}}_{2n} |_{\mathcal{M}}.
$$

Then for $n > 1$

$$
\text{ed}_k(\mathcal{M}' \rightarrow \mathcal{M}) = n >> \text{RD}_k(\mathcal{M}' \rightarrow \mathcal{M}) = 1
$$

$\therefore \text{ed}_k$ very sensitive to arithmetic of the fields $k$ and $k(\mathcal{M})$. $\text{RD}_k$ captures traditional notions of complexity of a problem.
Remarks, cont.

Three major sources of $\mathcal{M}' \rightarrow \mathcal{M}$:
Remarks, cont.

Three major sources of $\mathcal{M}' \rightarrow \mathcal{M}$:
- Roots of polynomials, e.g. $\tilde{P}_n \rightarrow P_n$
Remarks, cont.

Three major sources of $\mathcal{M}' \longrightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{P}_n \longrightarrow P_n$
- Classical enumerative problems, e.g.
Remarks, cont.

Three major sources of \( \mathcal{M}' \rightarrow \mathcal{M} \):

- Roots of polynomials, e.g. \( \tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n \)
- Classical enumerative problems, e.g.
  - \( \mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3} \) (cubic surfaces with or w/o a line)
Remarks, cont.

Three major sources of $\mathcal{M}' \rightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$
- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \rightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)
Remarks, cont.

Three major sources of $\mathcal{M}' \rightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$
- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \rightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)
  - $\vdots$

Congruence subgroups, i.e. $X(\Gamma) = \Gamma \setminus G/K$ arithmetic, locally symmetric space.

$\Gamma' \subset \Gamma$ finite index subgroup $X(\Gamma') \rightarrow X(\Gamma)$. Resolvent degree gives a common, natural invariant of each.
Three major sources of $\mathcal{M}' \rightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n$
- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \rightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)
  - Congruence subgroups, i.e.
Remarks, cont.

Three major sources of $\mathcal{M}' \longrightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{\mathcal{P}}_n \longrightarrow \mathcal{P}_n$

- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \longrightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \longrightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)

- Congruence subgroups, i.e.
  $$X(\Gamma) = \Gamma \backslash G/K$$
  arithmetic, locally symmetric space.
Remarks, cont.

Three major sources of $M' \rightarrow M$:

- Roots of polynomials, e.g. $\tilde{P}_n \rightarrow P_n$
- Classical enumerative problems, e.g.
  - $M_{3,3}(1) \rightarrow M_{3,3}$ (cubic surfaces with or w/o a line)
  - $M_{4,2}(1) \rightarrow M_{4,2}$ (quartic curves with or w/o a bitangent)

- Congruence subgroups, i.e.
  \[ X(\Gamma) = \Gamma \setminus G/K \text{ arithmetic, locally symmetric space.} \]
  \[ \Gamma' \subset \Gamma \text{ finite index subgroup} \]
Remarks, cont.

Three major sources of $\mathcal{M}' \longrightarrow \mathcal{M}$:
- Roots of polynomials, e.g. $\widetilde{\mathcal{P}}_n \longrightarrow \mathcal{P}_n$
- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \longrightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \longrightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)
  
- Congruence subgroups, i.e.
  $X(\Gamma) = \Gamma \setminus G/K$ arithmetic, locally symmetric space.
  $\Gamma' \subset \Gamma$ finite index subgroup
  - $X(\Gamma') \longrightarrow X(\Gamma)$. 
Remarks, cont.

Three major sources of $\mathcal{M}' \longrightarrow \mathcal{M}$:

- Roots of polynomials, e.g. $\tilde{\mathcal{P}}_n \longrightarrow \mathcal{P}_n$
- Classical enumerative problems, e.g.
  - $\mathcal{M}_{3,3}(1) \longrightarrow \mathcal{M}_{3,3}$ (cubic surfaces with or w/o a line)
  - $\mathcal{M}_{4,2}(1) \longrightarrow \mathcal{M}_{4,2}$ (quartic curves with or w/o a bitangent)
  
- Congruence subgroups, i.e.
  \[ X(\Gamma) = \Gamma \backslash G/K \text{ arithmetic, locally symmetric space.} \]
  \[ \Gamma' \subset \Gamma \text{ finite index subgroup} \]
  - $X(\Gamma') \longrightarrow X(\Gamma)$.

Resolvent degree gives a common, natural invariant of each.
Many (most) examples come with towers of covers, e.g.
Many (most) examples come with towers of covers, e.g.

- $\mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$
Remarks, cont.

Many (most) examples come with towers of covers, e.g.

- \( \mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3} \)
- \( \cdots \rightarrow \mathcal{M}_g[\ell^n] \rightarrow \mathcal{M}_g[\ell^{n-1}] \rightarrow \cdots \rightarrow \mathcal{M}_g \)

Much of algebraic geometry pre-1930 concerned with:
Given one datum, specify others.
I.e. specify the relationships between intermediate covers.
Resolvent degree gives a natural framework for understanding and organizing classical work.
Many (most) examples come with towers of covers, e.g.

- $\mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$
- $\cdots \rightarrow \mathcal{M}_g[\ell^n] \rightarrow \mathcal{M}_g[\ell^{n-1}] \rightarrow \cdots \rightarrow \mathcal{M}_g$

Much of algebraic geometry pre-1930 concerned with:
Many (most) examples come with towers of covers, e.g.

- $\mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}(1) \rightarrow \mathcal{M}_{3,3}$

- $\cdots \rightarrow \mathcal{M}_g[\ell^n] \rightarrow \mathcal{M}_g[\ell^{n-1}] \rightarrow \cdots \rightarrow \mathcal{M}_g$

Much of algebraic geometry pre-1930 concerned with:

Given one datum, specify others.

I.e. specify the relationships between intermediate covers.
Many (most) examples come with towers of covers, e.g.

- \( \mathcal{M}_{3,3}(27) \to \mathcal{M}_{3,3}(1) \to \mathcal{M}_{3,3} \)
- \( \cdots \to \mathcal{M}_g[\ell^n] \to \mathcal{M}_g[\ell^{n-1}] \to \cdots \to \mathcal{M}_g \)

Much of algebraic geometry pre-1930 concerned with:

Given one datum, specify others.

I.e. specify the relationships between intermediate covers. Resolvent degree gives a natural framework for understanding and organizing classical work.
Remarks, cont.

Resolvent degree first defined (as far as we can find) in Brauer, 1975.
Remarks, cont.

Resolvent degree first defined (as far as we can find) in Brauer, 1975.
However, explicit study of $\text{RD}_k(\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n)$ is classical:
Remarks, cont.

Resolvent degree first defined (as far as we can find) in Brauer, 1975. However, explicit study of $\text{RD}_k(\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n)$ is classical:

- Tschirnhausen, 1683
Remarks, cont.

Resolvent degree first defined (as far as we can find) in Brauer, 1975.
However, explicit study of $\text{RD}_k(\overline{P}_n \rightarrow P_n)$ is classical:

- Tschirnhausen, 1683
- Bring, 1786
Remarks, cont.

Resolvent degree first defined (as far as we can find) in Brauer, 1975.
However, explicit study of $\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n)$ is classical:

- Tschirnhausen, 1683
- Bring, 1786
- Hamilton, 1836
Resolvent degree first defined (as far as we can find) in Brauer, 1975.
However, explicit study of $\text{RD}_k(\tilde{P}_n \rightarrow P_n)$ is classical:
- Tschirnhausen, 1683
- Bring, 1786
- Hamilton, 1836
- Sylvester, 1886
:: (more below)
Remarks, cont.

For $\text{RD}_k$, there exist techniques for obtaining upper bounds.

Conjecture (Hilbert)
1. $\text{RD}_{\tilde{C}}(\sim P_6 \rightarrow \sim P_6) = 2$.
2. (Hilbert's 13th Problem) $\text{RD}_{\tilde{C}}(\sim P_7 \rightarrow \sim P_7) = 3$.

Question: Is $\text{RD}_{C}(\sim) \equiv 1$?
Hilbert thought no. Benson and I are working on this!

Keywords: "braid Galois group." Hopefully, more soon!
Remarks, cont.

For $\text{RD}_k$, there exist techniques for obtaining upper bounds. However:

There are no known nontrivial lower bounds on $\text{RD}_k$. 
Remarks, cont.

For \( \text{RD}_k \), there exist techniques for obtaining upper bounds. However:

There are no known nontrivial lower bounds on \( \text{RD}_k \).

Conjecture (Hilbert)

1. \( \text{RD}_C(\tilde{P}_6 \rightarrow P_6) = 2 \).
2. (Hilbert’s 13th Problem) \( \text{RD}_C(\tilde{P}_7 \rightarrow P_7) = 3 \).
For \( \text{RD}_k \), there exist techniques for obtaining upper bounds. However:

**There are no known nontrivial lower bounds on \( \text{RD}_k \).**

**Conjecture (Hilbert)**

1. \( \text{RD}_C(\tilde{\mathcal{P}_6} \to \mathcal{P}_6) = 2 \).
2. *(Hilbert’s 13th Problem)* \( \text{RD}_C(\tilde{\mathcal{P}_7} \to \mathcal{P}_7) = 3 \).

**Question**

Is \( \text{RD}_C(\cdot) \equiv 1 \)?

Benson and I are working on this! Keywords: “braid Galois group.” Hopefully, more soon!
For \( \text{RD}_k \), there exist techniques for obtaining upper bounds. However:

**There are no known nontrivial lower bounds on** \( \text{RD}_k \).

**Conjecture (Hilbert)**

1. \( \text{RD}_\mathbb{C}(\tilde{P}_6 \rightarrow P_6) = 2 \).
2. \( (\text{Hilbert’s 13th Problem}) \ \text{RD}_\mathbb{C}(\tilde{P}_7 \rightarrow P_7) = 3 \).

**Question**

Is \( \text{RD}_\mathbb{C}(\sim) \equiv 1 \)?

Hilbert thought no.
For \( \text{RD}_k \), there exist techniques for obtaining upper bounds. However:

**There are no known nontrivial lower bounds on \( \text{RD}_k \).**

**Conjecture (Hilbert)**

1. \( \text{RD}_C(\tilde{\mathcal{P}}_6 \rightarrow \mathcal{P}_6) = 2 \).
2. (Hilbert’s 13th Problem) \( \text{RD}_C(\tilde{\mathcal{P}}_7 \rightarrow \mathcal{P}_7) = 3 \).

**Question**

Is \( \text{RD}_C(\mathcal{-}) \equiv 1 \)?

Hilbert thought no. Benson and I are working on this!
Remarks, cont.

For RD$_k$, there exist techniques for obtaining upper bounds. However:

**There are no known nontrivial lower bounds on RD$_k$.**

Conjecture (Hilbert)

1. RD$_C(\tilde{\mathcal{P}}_6 \rightarrow \mathcal{P}_6) = 2$.
2. *(Hilbert’s 13th Problem)* RD$_C(\tilde{\mathcal{P}}_7 \rightarrow \mathcal{P}_7) = 3$.

Question

*Is RD$_C(-) \equiv 1$?*

Hilbert thought no. Benson and I are working on this!

Keywords: “braid Galois group.”
Remarks, cont.

For $\text{RD}_k$, there exist techniques for obtaining upper bounds. However:

There are no known nontrivial lower bounds on $\text{RD}_k$.

Conjecture (Hilbert)

1. $\text{RD}_\mathbb{C}(\tilde{P}_6 \rightarrow P_6) = 2$.
2. (Hilbert’s 13th Problem) $\text{RD}_\mathbb{C}(\tilde{P}_7 \rightarrow P_7) = 3$.

Question

Is $\text{RD}_\mathbb{C}(\_\) \equiv 1$?

Hilbert thought no. Benson and I are working on this!

Keywords: “braid Galois group.” Hopefully, more soon!
A plane quartic with its 28 bitangents
RD and Classical Enumerative Problems

A cubic surface with its 27 lines
RD and Classical Enumerative Problems

Theorem (Cayley–Salmon, 1856)

*There exist 27 lines on every smooth cubic surface.*
Theorem (Cayley–Salmon, 1856)

There exist 27 lines on every smooth cubic surface.

Question

Given a cubic, how hard is it to find one line? All 27?
Theorem (Cayley–Salmon, 1856)

*There exist 27 lines on every smooth cubic surface.*

**Question**

*Given a cubic, how hard is it to find one line? All 27?*

Let $\mathcal{M}_{3,3}(n)$ denote the moduli of cubic surfaces with a choice of $n$ (ordered) lines.
RD and Classical Enumerative Problems

Theorem (Cayley–Salmon, 1856)

*There exist 27 lines on every smooth cubic surface.*

Question

*Given a cubic, how hard is it to find one line? All 27?*

Let $\mathcal{M}_{3,3}(n)$ denote the moduli of cubic surfaces with a choice of $n$ (ordered) lines.

Theorem (Jordan, 1870; Harris, 1979)

RD$_k(\mathcal{M}_{3,3}(27) \longrightarrow \mathcal{M}_{3,3}^{\text{disj}}(3)) = 1$. 

**RD and Classical Enumerative Problems**

**Theorem (Cayley–Salmon, 1856)**

*There exist 27 lines on every smooth cubic surface.*

**Question**

*Given a cubic, how hard is it to find one line? All 27?*

Let $\mathcal{M}_{3,3}(n)$ denote the moduli of cubic surfaces with a choice of $n$ (ordered) lines.

**Theorem (Jordan, 1870; Harris, 1979)**

$$\text{RD}_k(\mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}^{\text{disj}}(3)) = 1.$$ 

**Observation (Farb–W.)**

$$\text{RD}_k(\mathcal{M}_{3,3}(27) \rightarrow \mathcal{M}_{3,3}(1)) = \text{RD}_k(\tilde{\mathcal{P}}_5 \rightarrow \mathcal{P}_5) = 1.$$
Lines on cubics, cont.

Observation (Farb–W.)

\[ \text{RD}_k(\mathcal{M}_{3,3}(27) \to \mathcal{M}_{3,3}(1)) = \text{RD}_k(\tilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1. \]

This follows from a beautiful classical trick:
Observation (Farb–W.)

$$\text{RD}_k(\mathcal{M}_{3,3}(27) \to \mathcal{M}_{3,3}(1)) = \text{RD}_k(\tilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1.$$ 

This follows from a beautiful classical trick:
Given $L \subset S$, each plane $V$ in the pencil containing $L$ has

$$V \cap S = L \cup C$$

for some conic $C$. 

Lines on cubics, cont.

Observation (Farb–W.)

\[ \text{RD}_k(M_{3,3}(27) \rightarrow M_{3,3}(1)) = \text{RD}_k(\tilde{P}_5 \rightarrow P_5) = 1. \]

This follows from a beautiful classical trick:

Given \( L \subset S \), each plane \( V \) in the pencil containing \( L \) has

\[ V \cap S = L \cup C \]

for some conic \( C \). Moreover, \( C \) degenerates to a pair of lines \( L_1 \cup L_2 \) at the roots of the discriminant of the pencil of conics, and this discriminant has degree 5.
Lines on cubics, cont.

Observation (Farb–W.)
\[ \text{RD}_k(\mathcal{M}_{3,3}(27) \to \mathcal{M}_{3,3}(1)) = \text{RD}_k(\tilde{\mathcal{P}_5} \to \mathcal{P}_5) = 1. \]

This follows from a beautiful classical trick:
Given \( L \subset S \), each plane \( V \) in the pencil containing \( L \) has
\[ V \cap S = L \cup C \]
for some conic \( C \). Moreover, \( C \) degenerates to a pair of lines \( L_1 \cup L_2 \) at the roots of the discriminant of the pencil of conics, and **this discriminant has degree 5**. Solving this quintic, we get 5 pairs of disjoint lines on \( S \). By a theorem of Harris, we get the remaining 17 lines by adjoining radicals.
Lines on cubics, cont.

Observation (Farb–W.)

\[ \text{RD}_k(\mathcal{M}_{3,3}(27) \to \mathcal{M}_{3,3}(1)) = \text{RD}_k(\tilde{\mathcal{P}}_5 \to \mathcal{P}_5) = 1. \]

This follows from a beautiful classical trick:
Given \( L \subset S \), each plane \( V \) in the pencil containing \( L \) has

\[ V \cap S = L \cup C \]

for some conic \( C \). Moreover, \( C \) degenerates to a pair of lines \( L_1 \cup L_2 \) at the roots of the discriminant of the pencil of conics, and this discriminant has degree 5. Solving this quintic, we get 5 pairs of disjoint lines on \( S \). By a theorem of Harris, we get the remaining 17 lines by adjoining radicals.

Question

What is \( \text{RD}_k(\mathcal{M}_{3,3}(1) \to \mathcal{M}_{3,3}) \)?
RD and Roots of Polynomials

“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:
- Hilbert 1927
- Segre 1947, 1955,
- Brauer 1975.

That’s it!
“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.”

(Sylvester, Hammond 1887)
“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
- Segre 1947, 1955,
- Brauer 1975.
RD and Roots of Polynomials

“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
- Segre 1947, 1955,
RD and Roots of Polynomials

“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
- Segre 1947, 1955,
- Brauer 1975.
RD and Roots of Polynomials

“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
- Segre 1947, 1955,
- Brauer 1975.

That’s it!
“The theory has been a ‘plant of slow growth’. The Lund Thesis [Bring] of December, 1786 (a matter of a couple of pages), Hamilton’s report of 1836, with the tract of Mr. Jerrard referred to therein, and the memoire [Sylvester] of ‘Crelle’ of December, 1886, constitute, as far as we are aware, the complete bibliography of the subject up to the present date.” (Sylvester, Hammond 1887)

To bring this up to 2017, add:

- Hilbert 1927
- Segre 1947, 1955,
- Brauer 1975. (0 citations!)

That’s it!
What’s Known

Theorem (Hamilton, 1836)

There exists a monotone increasing function $H : \mathbb{N} \to \mathbb{N}$ such that for $n > H(r)$, $RD_k(\tilde{P}_n \to P_n) \leq n - r$. 

Hamilton computed the initial values of $H$: 

$r \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9 \quad 10 \quad 11 \quad 12 \quad 13 \quad 14 \quad 15 \quad 16 \quad 17 \quad 18 \quad 19 \quad 20 \quad 21 \quad 22 \quad 23 \quad 24 \quad 25 \quad 26 \quad 27 \quad 28 \quad 29 \quad 30 \quad 31 \quad 32 \quad 33 \quad 34 \quad 35 \quad 36 \quad 37 \quad 38 \quad 39 \quad 40 \quad 41 \quad 42 \quad 43 \quad 44 \quad 45 \quad 46 \quad 47 \quad 48 \quad 49 \quad 50 \quad 51 \quad 52 \quad 53 \quad 54 \quad 55 \quad 56 \quad 57 \quad 58 \quad 59 \quad 60 \quad 61 \quad 62 \quad 63 \quad 64 \quad 65 \quad 66 \quad 67 \quad 68 \quad 69 \quad 70 \quad 71 \quad 72 \quad 73 \quad 74 \quad 75 \quad 76 \quad 77 \quad 78 \quad 79 \quad 80 \quad 81 \quad 82 \quad 83 \quad 84 \quad 85 \quad 86 \quad 87 \quad 88 \quad 89 \quad 90 \quad 91 \quad 92 \quad 93 \quad 94 \quad 95 \quad 96 \quad 97 \quad 98 \quad 99 \quad 100$

$H(r) \quad 5 \quad 11 \quad 47 \quad 923 \quad 409,619 \quad 83,763,206,255$

Sylvester–Hammond, 1887 - generating function for $H(r)$
What’s Known

Theorem (Hamilton, 1836)

There exists a monotone increasing function $H: \mathbb{N} \to \mathbb{N}$ such that for $n > H(r)$, $RD_k(\tilde{P}_n \to P_n) \leq n - r$.

Hamilton computed the initial values of $H$:

<table>
<thead>
<tr>
<th>$r$</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H(r)$</td>
<td>5</td>
<td>11</td>
<td>47</td>
<td>923</td>
<td>409,619</td>
<td>83,763,206,255</td>
</tr>
</tbody>
</table>
What’s Known

Theorem (Hamilton, 1836)

There exists a monotone increasing function $H : \mathbb{N} \to \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r$.

Hamilton computed the initial values of $H$:

<table>
<thead>
<tr>
<th>$r$</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>H(r)</td>
<td>5</td>
<td>11</td>
<td>47</td>
<td>923</td>
<td>409,619</td>
<td>83,763,206,255</td>
</tr>
</tbody>
</table>

Sylvester–Hammond, 1887 - generating function for $H(r)$
What’s Known, cont.

By mid-20th century, Hamilton’s Theorem appears to have been forgotten:
By mid-20th century, Hamilton’s Theorem appears to have been forgotten:

**Conjecture (Segre, Annals 1947)**

*There exists a monotone increasing function $H: \mathbb{N} \rightarrow \mathbb{N}$ such that for $n > H(r)$, $RD_k(\tilde{P}_n \rightarrow P_n) \leq n - r.$*
Theorem (Hamilton, 1836)

There exists a monotone increasing function $H : \mathbb{N} \rightarrow \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r.$

By mid-20th century, Hamilton’s Theorem appears to have been forgotten:

Conjecture (Segre, Annals 1947)

There exists a monotone increasing function $H : \mathbb{N} \rightarrow \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r.$

Segre and Brauer reproved the theorem soon after, but without an explicit formula.

Theorem (Brauer, 1975)

Let $B(r) := \frac{(r-1)!}{2}$.

For $n > B(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r.$
What’s Known, cont.

Theorem (Hamilton, 1836)

There exists a monotone increasing function $H : \mathbb{N} \to \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \to P_n) \leq n - r$.

By mid-20th century, Hamilton’s Theorem appears to have been forgotten:

Conjecture (Segre, Annals 1947)

There exists a monotone increasing function $H : \mathbb{N} \to \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \to P_n) \leq n - r$.

Segre and Brauer reproved the theorem soon after, but without an explicit formula.
What’s Known, cont.

Theorem (Hamilton, 1836)

There exists a monotone increasing function $H : \mathbb{N} \rightarrow \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r$.

By mid-20th century, Hamilton’s Theorem appears to have been forgotten:

Conjecture (Segre, Annals 1947)

There exists a monotone increasing function $H : \mathbb{N} \rightarrow \mathbb{N}$ such that for $n > H(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r$.

Segre and Brauer reproved the theorem soon after, but without an explicit formula.

Theorem (Brauer, 1975)

Let $B(r) := (r - 1)!$ For $n > B(r)$, $\text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq n - r$. 
Improving on Hamilton, Brauer

Let $M_{3, N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.

Let $M_{r, 3, N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.

Let $L_{3, (r, N)} := RD_{k}(\tilde{\mathbb{P}}^n \to \mathbb{P}^n) \to M_{3, N}.$

**Theorem (Farb–W.)**

There exist polynomial functions $f, g : N \times N \to N$ such that for all $n \geq (d + k)! d!$,

$$RD_{k}(\tilde{\mathbb{P}}^n \to \mathbb{P}^n) \leq \max\{n - (d + k + 1), L_{3, (f(d, k), g(d, k))}\}.$$

**Corollary**

There exist monotone increasing functions $FW, \phi : N \to N$ s.t.

- For $n > FW(r)$,
  $$RD_{k}(\tilde{\mathbb{P}}^n \to \mathbb{P}^n) \leq n - r,$$
- For all $d \geq 0, r \geq \phi(d)$, then $B(r)/FW(r) \geq d!.$
Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3, N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$. 

Theorem (Farb–W.)

There exist polynomial functions $f, g : N \times N \to N$ such that for all $n \geq \binom{d+k+1}{d}$,

$$\text{RD}_k(\tilde{P}_n \to P_n) \leq \max\{n - (d+k+1), L_3(f(d, k), g(d, k))\}.$$ 

Corollary

There exist monotone increasing functions $FW, \phi : N \to N$ s.t.

- For $n > FW(r)$,

$$\text{RD}_k(\tilde{P}_n \to P_n) \leq n - r,$$

- For all $d \geq 0, r \geq \phi(d)$, then $B(r)/FW(r) \geq d!.$
Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}'_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}_{3,N}^r$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
- Let $L_3(r, N) := \text{RD}_k(\mathcal{M}_{3,N}^r \to \mathcal{M}_{3,N})$.

Theorem (Farb–W.)

There exist polynomial functions $f, g: N \times N \to N$ such that for all $n \geq (d + k)! d!$,

$$\text{RD}_k(\tilde{\mathbb{P}}^n \to \mathbb{P}^n) \leq \max \{ n - (d + k + 1), L_3(f(d, k), g(d, k)) \}.$$

Corollary

There exist monotone increasing functions $F_W, \phi: N \to N$ s.t.

- For $n > F_W(r)$, $\text{RD}_k(\tilde{\mathbb{P}}^n \to \mathbb{P}^n) \leq n - r$,
- For all $d \geq 0, r \geq \phi(d)$, then $B(r)/F_W(r) \geq d!$. 

Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}_{3,N}^r$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
- Let $L_3(r, N) := \text{RD}_k(\mathcal{M}_{3,N}^r \to \mathcal{M}_{3,N})$.

Theorem (Farb–W.)

There exist polynomial functions $f, g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \geq \frac{(d+k)!}{d!}$,

$$\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq \max\{n - (d + k + 1), L_3(f(d, k), g(d, k))\}.$$
Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}_{3,N}^r$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
- Let $L_3(r, N) := \text{RD}_k(\mathcal{M}_{3,N}^r \rightarrow \mathcal{M}_{3,N})$.

**Theorem (Farb–W.)**

There exist polynomial functions $f, g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ such that for all $n \geq \frac{(d+k)!}{d!}$,

$$\text{RD}_k(\tilde{\mathcal{P}}_n \rightarrow \mathcal{P}_n) \leq \max\{n - (d + k + 1), L_3(f(d, k), g(d, k))\}.$$  

**Corollary**

There exist monotone increasing functions $FW, \varphi : \mathbb{N} \rightarrow \mathbb{N}$ s.t.
Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}_{3,N}^r$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
- Let $L_3(r, N) := \text{RD}_k(\mathcal{M}_{3,N}^r \to \mathcal{M}_{3,N})$.

**Theorem (Farb–W.)**

*There exist polynomial functions $f, g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \geq \frac{(d+k)!}{d!}$,*

$$\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq \max\{n - (d + k + 1), L_3(f(d, k), g(d, k))\}.$$  

**Corollary**

*There exist monotone increasing functions $FW, \varphi : \mathbb{N} \to \mathbb{N}$ s.t.*

- For $n > FW(r)$, $\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n - r$,  


Improving on Hamilton, Brauer

- Let $\mathcal{M}_{3,N}$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$.
- Let $\mathcal{M}_{3,N}^r$ denote the moduli of cubic hypersurfaces in $\mathbb{P}^N$ with a choice of $r$-plane lying on them.
- Let $L_3(r, N) := \text{RD}_k(\mathcal{M}_{3,N}^r \to \mathcal{M}_{3,N})$.

**Theorem (Farb–W.)**

*There exist polynomial functions $f, g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \geq \frac{(d+k)!}{d!}$,*

$$\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq \max\{n - (d + k + 1), L_3(f(d, k), g(d, k))\}.$$  

**Corollary**

*There exist monotone increasing functions $FW, \varphi : \mathbb{N} \to \mathbb{N}$ s.t.*

- For $n > FW(r)$, $\text{RD}_k(\tilde{\mathcal{P}}_n \to \mathcal{P}_n) \leq n - r$,
- For all $d \geq 0$, $r \geq \varphi(d)$, then $B(r)/FW(r) \geq d!$.  

Improving on Hamilton, Brauer, cont.

Idea comes from:

Theorem (Hilbert, 1927)

$$\text{RD}_k(\tilde P \to P) \leq \max \{4, \text{RD}_k(M_3, 3) \to M_3, 3(1) \to M_3, 3)\}.$$
Improving on Hamilton, Brauer, cont.

Idea comes from:

**Theorem (Hilbert, 1927)**

\[ \text{RD}_k(\tilde{P}_9 \to P_9) \leq \max\{4, \text{RD}_k(M_{3,3}(1) \to M_{3,3})\} . \]

i.e. Hilbert used a line on a cubic surface to simplify the solution of the general degree 9 polynomial!

His proof suggests two things:

1. A method for finding special points on Fano varieties of complete intersections.
Improving on Hamilton, Brauer, cont.

Idea comes from:

**Theorem (Hilbert, 1927)**

\[ \text{RD}_k(\tilde{P}_9 \to P_9) \leq \max\{4, \text{RD}_k(M_{3,3}(1) \to M_{3,3})\}. \]

i.e. Hilbert used a line on a cubic surface to simplify the solution of the general degree 9 polynomial!
Improving on Hamilton, Brauer, cont.

Idea comes from:

**Theorem (Hilbert, 1927)**

\[ \text{RD}_k(\tilde{P}_9 \rightarrow P_9) \leq \max\{4, \text{RD}_k(M_{3,3}(1) \rightarrow M_{3,3})\}. \]

i.e. Hilbert used a line on a cubic surface to simplify the solution of the general degree 9 polynomial!

His proof suggests two things:
Improving on Hamilton, Brauer, cont.

Idea comes from:

**Theorem (Hilbert, 1927)**

\[ RD_k(\tilde{P}_9 \to \mathcal{P}_9) \leq \max\{4, RD_k(\mathcal{M}_{3,3}(1) \to \mathcal{M}_{3,3})\} \].

i.e. Hilbert used a line on a cubic surface to simplify the solution of the general degree 9 polynomial!

His proof suggests two things:

1. A method for finding special points on Fano varieties of complete intersections.
Improving on Hamilton, Brauer, cont.

Idea comes from:

**Theorem (Hilbert, 1927)**

$$\text{RD}_k(\tilde{P}_9 \rightarrow P_9) \leq \max\{4, \text{RD}_k(M_{3,3}(1) \rightarrow M_{3,3})\}.$$ 

i.e. Hilbert used a line on a cubic surface to simplify the solution of the general degree 9 polynomial!

His proof suggests two things:

1. A method for finding special points on Fano varieties of complete intersections.

Improving on Hamilton, Brauer, cont.

Idea for 2 actually goes back to the beginnings of the subject:

Theorem (Bring, 1786)

\[ RD_k(\tilde{P}_n \rightarrow \tilde{P}_n) \leq \max\{ n - 4, RD_k(M_1M_2 \rightarrow M_2M_2) \} = n - 4, \]

for \( n \geq 5 \).

Question By combining Hamilton’s method with that of Bring–Hilbert, can we go further?
Improving on Hamilton, Brauer, cont.

Idea for 2 actually goes back to the beginnings of the subject:

Theorem (Bring, 1786)

\[
\text{RD}_k(\tilde{P}_n \to P_n) \leq \max\{n - 4, \text{RD}_k(M^{1}_{2,2} \to M_{2,2})\} \quad (= n - 4), \quad \text{for } n \geq 5.
\]
Idea for 2 actually goes back to the beginnings of the subject:

**Theorem (Bring, 1786)**

\[ \text{RD}_k(\tilde{P}_n \rightarrow P_n) \leq \max\{n - 4, \text{RD}_k(M_{2,2}^1 \rightarrow M_{2,2})\} = n - 4, \]

for \( n \geq 5 \).

**Question**

*By combining Hamilton’s method with that of Bring–Hilbert, can we go further?*
RD and Congruence Subgroups

**Theme in Kähler geometry:** study/obstruct compressions to a smaller dimensional variety.
RD and Congruence Subgroups

**Theme in Kähler geometry:** study/obstruct compressions to a smaller dimensional variety.

- Gromov–Schoen
RD and Congruence Subgroups

**Theme in Kähler geometry:** study/obstruct compressions to a smaller dimensional variety.

- Gromov–Schoen
- Beauville–Siu
RD and Congruence Subgroups

**Theme in Kähler geometry:** study/obstruct compressions to a smaller dimensional variety.

- Gromov–Schoen
- Beauville–Siu

:
Theme in Kähler geometry: study/obstruct compressions to a smaller dimensional variety.

- Gromov–Schoen
- Beauville–Siu

Resolvent degree suggests a natural refinement:

**Question**

*Given a cover $\tilde{X} \longrightarrow X$, can we (virtually) compress the cover to a cover of a lower dimensional variety?*
RD and Congruence Subgroups

**Theme in Kähler geometry:** study/obstruct compressions to a smaller dimensional variety.
- Gromov–Schoen
- Beauville–Siu

Resolvent degree suggests a natural refinement:

**Question**

*Given a cover \( \tilde{X} \longrightarrow X \), can we (virtually) compress the cover to a cover of a lower dimensional variety?*

More precisely:

**Question**

*Given arithmetic locally symmetric space \( X = \Gamma \backslash G/K \), and \( \Gamma' \subset \Gamma \) finite index, what is \( \text{RD}_k(X(\Gamma') \longrightarrow X(\Gamma)) \)?
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Let $\Gamma_4 = \text{PU}(4, 1)(\mathcal{E})$. 
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Let $\Gamma_4 = \text{PU}(4,1)(\mathcal{E})$.
$\Gamma_4 \twoheadrightarrow W(E_6)$. Denote kernel by $\Gamma'_4$. 
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Let $\Gamma_4 = \text{PU}(4,1)(\mathcal{E})$.
$\Gamma_4 \rightarrow W(E_6)$. Denote kernel by $\Gamma'_4$.
$\Gamma_4 \odot \mathbb{CH}^4$. Get a congruence cover

$$X(\Gamma'_4) \longrightarrow X(\Gamma_4)$$
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers. Let $\Gamma_4 = \text{PU}(4, 1)(\mathcal{E})$. $\Gamma_4 \rightarrow W(E_6)$. Denote kernel by $\Gamma_4'$. $\Gamma_4 \trianglelefteq \mathbb{CH}^4$. Get a congruence cover

$$X(\Gamma_4') \twoheadrightarrow X(\Gamma_4)$$

By work of Clemens–Griffiths and Allcock–Carlson–Toledo:
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Let $\Gamma_4 = \text{PU}(4, 1)(\mathcal{E})$.
$\Gamma_4 \to W(E_6)$. Denote kernel by $\Gamma'_4$.
$\Gamma_4 \bowtie \mathbb{CH}^4$. Get a congruence cover

$$X(\Gamma'_4) \rightarrow X(\Gamma_4)$$

By work of Clemens–Griffiths and Allcock–Carlson–Toledo:
- $X(\Gamma_4)$ is a moduli space of certain intermediate Jacobians,
Example

Let $\mathcal{E} = \mathbb{Z}[\omega]$ denote the Eisenstein integers.
Let $\Gamma_4 = \text{PU}(4, 1)(\mathcal{E})$.
$\Gamma_4 \twoheadrightarrow W(E_6)$. Denote kernel by $\Gamma'_4$.
$\Gamma_4 \bowtie \mathbb{CH}^4$. Get a congruence cover

$$X(\Gamma'_4) \twoheadrightarrow X(\Gamma_4)$$

By work of Clemens–Griffiths and Allcock–Carlson–Toledo:
- $X(\Gamma_4)$ is a moduli space of certain intermediate Jacobians,
- $X(\Gamma'_4)$ is the moduli space of these intermediate Jacobians equipped with a $W(E_6)$-level structure.
Sample Theorem

Theorem (Farb–W.)

Hilbert's Sextic Conjecture \( \Rightarrow \) 

\( RD_C(\Gamma_4) \rightarrow X(\Gamma_4) \geq 2 \).

Proof.

Two steps:

1. A variant of Hilbert's trick for the degree 9 shows that 

\( RD_k(\tilde{P}_6 \rightarrow P_6) \leq RD_k(M_3, 3(1) \rightarrow M_3, 3(1)) \).

2. Allcock–Carlson–Toledo's uniformization theorem implies that 

\( RD_C(M_3, 3(1) \rightarrow M_3, 3(1)) = RD_C(\Gamma_4) \rightarrow X(\Gamma_4) \).
Sample Theorem

Theorem (Farb–W.)

Hilbert’s Sextic Conjecture \Rightarrow \text{RD}_\mathbb{C}(X(\Gamma_4') \rightarrow X(\Gamma_4)) \geq 2.
Sample Theorem

Theorem (Farb–W.)

*Hilbert’s Sextic Conjecture* ⇒ $\text{RD}_\mathbb{C}(X(\Gamma_4') \rightarrow X(\Gamma_4)) \geq 2$.

Proof.

Two steps:
Sample Theorem

Theorem (Farb–W.)

\[ \text{Hilbert's Sextic Conjecture} \Rightarrow \text{RD}_\mathbb{C}(X(\Gamma'_4) \to X(\Gamma_4)) \geq 2. \]

Proof.

Two steps:

1. A variant of Hilbert's trick for the degree 9 shows that

\[ \text{RD}_k(\tilde{\mathcal{P}}_6 \to \mathcal{P}_6) \leq \text{RD}_k(\mathcal{M}_{3,3}(1) \to \mathcal{M}_{3,3}). \]
Sample Theorem

Theorem (Farb–W.)

Hilbert’s Sextic Conjecture $\Rightarrow$ $\text{RD}_\mathbb{C}(X(\Gamma_4') \to X(\Gamma_4)) \geq 2$.

Proof.

Two steps:

1. A variant of Hilbert’s trick for the degree 9 shows that

$$\text{RD}_k(\tilde{P}_6 \to P_6) \leq \text{RD}_k(M_{3,3}(1) \to M_{3,3}).$$

2. Allcock–Carlson–Toledo’s uniformization theorem implies that

$$\text{RD}_\mathbb{C}(M_{3,3}(1) \to M_{3,3}) = \text{RD}_\mathbb{C}(X(\Gamma_4') \to X(\Gamma_4)).$$
Sample Theorem

Theorem (Farb–W.)

*Hilbert’s Sextic Conjecture* ⇒ $\text{RD}_C(X(\Gamma'_4) \to X(\Gamma_4)) \geq 2$.

Proof.

Two steps:

1. A variant of Hilbert’s trick for the degree 9 shows that

   $\text{RD}_k(\tilde{P}_6 \to P_6) \leq \text{RD}_k(M_{3,3}(1) \to M_{3,3})$.

2. Allcock–Carlson–Toledo’s uniformization theorem implies that

   $\text{RD}_C(M_{3,3}(1) \to M_{3,3}) = \text{RD}_C(X(\Gamma'_4) \to X(\Gamma_4))$. 

\[\square\]
Two things I like about this theorem:
Two things I like about this theorem:
  - It relates three seemingly very different problems.
Two things I like about this theorem:
- It relates three seemingly very different problems.
- It uses a uniformization theorem to obtain nontrivial relations between algebraic problems.
Two things I like about this theorem:

- It relates three seemingly very different problems.
- It uses a uniformization theorem to obtain nontrivial relations between algebraic problems.

No Boundaries!
“The study of [resolvent degree], far from being exhausted, has, in leaving our hands, little more than reached its first stage, and it is believed will furnish a plentiful aftermath to those who may feel hereafter inclined to pursue to the end the thorny path we have here contented ourselves with indicating, which lies so remote from the beaten track of research, and offers an example and suggestion of infinite series (as far as we are aware) wholly unlike any which have previously engaged the attention of mathematicians.”

(Sylvester, Hammond 1887)
“The study of [resolvent degree], far from being exhausted, has, in leaving our hands, little more than reached its first stage, and it is believed will furnish a plentiful aftermath to those who may feel hereafter inclined to pursue to the end the thorny path we have here contented ourselves with indicating, which lies so remote from the beaten track of research, and offers an example and suggestion of infinite series (as far as we are aware) wholly unlike any which have previously engaged the attention of mathematicians.”

(Sylvester, Hammond 1887)

Sylvester and Hammond’s words apply just as much today!
Happy Birthday, Benson!