Computing Ext algebras with Sage

An F_5 algorithm for path algebra quotients

Simon King
DFG project KI 861/2–1

18$^{\text{th}}$ June, 2013

Outline

Path Algebra quotients

Q: Finite quiver (directed graph; loops and cycles allowed)

- Vertices $v_1, \ldots, v_q$, arrows $\alpha_1, \ldots, \alpha_r$

Path Algebra quotients

Q: Finite quiver (directed graph; loops and cycles allowed)

- Vertices $v_1, \dots, v_q$, arrows $\alpha_1, \dots, \alpha_r$

Path algebra $\mathcal{A} = kQ$ (k a field)

- k-basis: All directed paths (lists of arrows) in Q
- Multiplication $\leftrightarrow$ concatenation and distributivity
  Product is zero if paths don't match!
- *Radical*: $\mathrm{Rad}(\mathcal{A}) = \langle \alpha_1, \dots, \alpha_r \rangle$

Path Algebra quotients

Q: Finite quiver (directed graph; loops and cycles allowed)

- Vertices $v_1, \ldots, v_q$, arrows $\alpha_1, \ldots, \alpha_r$

Path algebra $\mathcal{A} = kQ$ (k a field)

- k-basis: All directed paths (lists of arrows) in Q
- Multiplication $\leftrightarrow$ concatenation and distributivity
  Product is zero if paths don't match!
- *Radical*: $\mathrm{Rad}(\mathcal{A}) = \langle \alpha_1, \ldots, \alpha_r \rangle$

Basic algebras

- An ideal $I \leq \mathcal{A}$ is *admissible*
  $\iff \exists N \in \mathbb{N} : \mathrm{Rad}(\mathcal{A})^N \subset I \subset \mathrm{Rad}(\mathcal{A})^2$

Path Algebra quotients

Q: Finite quiver (directed graph; loops and cycles allowed)

- Vertices $v_1, \dots, v_q$, arrows $\alpha_1, \dots, \alpha_r$

Path algebra $\mathcal{A} = kQ$ (k a field)

- k-basis: All directed paths (lists of arrows) in Q
- Multiplication $\leftrightarrow$ concatenation and distributivity
  Product is zero if paths don't match!
- *Radical*: $\mathrm{Rad}(\mathcal{A}) = \langle \alpha_1, \dots, \alpha_r \rangle$

Basic algebras

- An ideal $I \leq \mathcal{A}$ is *admissible*
  $\iff \exists N \in \mathbb{N} : \mathrm{Rad}(\mathcal{A})^N \subset I \subset \mathrm{Rad}(\mathcal{A})^2$
- $\mathcal{B} = \mathcal{A}/I$ (I admissible. $v_i, \alpha_j \in \mathcal{B}$) is called *basic algebra*.
- Radical $\mathrm{Rad}(\mathcal{B}) = J_{\mathcal{B}} = \langle \alpha_1, \dots, \alpha_r \rangle \leq \mathcal{B}$

Nice properties of basic algebras

Why to consider basic algebras?

G a finite group, $k = \overline{k}$ of characteristic $p \mid |G| \Longrightarrow kG$ is *Morita equivalent* to a basic algebra.

$\rightsquigarrow$Study representation theory, cohomology etc. via basic algebras

Nice properties of basic algebras

Why to consider basic algebras?

G a finite group, $k = \overline{k}$ of characteristic $p \mid |G| \Longrightarrow kG$ is *Morita equivalent* to a basic algebra.
$\rightsquigarrow$Study representation theory, cohomology etc. via basic algebras

Simple and projective modules

- Simple modules: $S_i := v_i\mathcal{B}/v_iJ_{\mathcal{B}}$. Dimension one!

Nice properties of basic algebras

Why to consider basic algebras?

G a finite group, $k = \overline{k}$ of characteristic $p \mid |G| \Longrightarrow kG$ is *Morita equivalent* to a basic algebra.
$\rightsquigarrow$Study representation theory, cohomology etc. via basic algebras

Simple and projective modules

- Simple modules: $S_i := v_i\mathcal{B}/v_iJ_{\mathcal{B}}$. Dimension one!
- Projective covers: $\mathcal{P}_i := v_i\mathcal{B} \twoheadrightarrow S_i \to 0$.

Recall: Projective modules are direct summands of free modules.
The $\mathcal{P}_i$ are the *projective indecomposable* modules (PIMs) of $\mathcal{B}$.

Nice properties of basic algebras

Why to consider basic algebras?

G a finite group, $k = \overline{k}$ of characteristic $p \mid |G| \Longrightarrow kG$ is *Morita equivalent* to a basic algebra.
$\rightsquigarrow$Study representation theory, cohomology etc. via basic algebras

Simple and projective modules

- Simple modules: $S_i := v_i\mathcal{B}/v_iJ_{\mathcal{B}}$. Dimension one!
- Projective covers: $\mathcal{P}_i := v_i\mathcal{B} \twoheadrightarrow S_i \rightarrow 0$.

Recall: Projective modules are direct summands of free modules.
The $\mathcal{P}_i$ are the *projective indecomposable* modules (PIMs) of $\mathcal{B}$.

In Sage? Trac ticket #12630

Jim Stark: Python code for acyclic quivers/algebras/modules.
SD 49: Refactor code, add categories/coercion. Later: Cythonize

Ext groups

M, N right-$\mathcal{B}$ modules. $\mathrm{Rad}(M) = M \cdot J_{\mathcal{B}}$ for basic algebras!

Projective resolution of M

$\cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$, such that

- $P_0, P_1, \ldots$ projective $\mathcal{B}$ modules
- $\ker(\epsilon) = \mathrm{im}(d_1)$ and $\ker(d_i) = \mathrm{im}(d_{i+1})$ for $i = 1, 2, \ldots$

Ext groups

M, N right-$\mathcal{B}$ modules. $\mathrm{Rad}(M) = M \cdot J_{\mathcal{B}}$ for basic algebras!

Projective resolution of M

$\cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$, such that

- $P_0, P_1, \ldots$ projective $\mathcal{B}$ modules
- $\ker(\epsilon) = \mathrm{im}(d_1)$ and $\ker(d_i) = \mathrm{im}(d_{i+1})$ for $i = 1, 2, \ldots$

Resolution is minimal $\iff$ $\mathrm{im}(d_i) \subseteq \mathrm{Rad}(P_{i-1})$ for $i = 1, 2, \ldots$

Ext groups

M, N right-$\mathcal{B}$ modules. $\mathrm{Rad}(M) = M \cdot J_{\mathcal{B}}$ for basic algebras!

Projective resolution of M

$\cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$, such that

- $P_0, P_1, \ldots$ projective $\mathcal{B}$ modules
- $\ker(\epsilon) = \mathrm{im}(d_1)$ and $\ker(d_i) = \mathrm{im}(d_{i+1})$ for $i = 1, 2, \ldots$

Resolution is minimal $\iff$ $\mathrm{im}(d_i) \subseteq \mathrm{Rad}(P_{i-1})$ for $i = 1, 2, \ldots$

Ext group $\mathrm{Ext}^n_{\mathcal{B}}(M, N)$

$$:= \left\{ P_n \xrightarrow{f} N \mid f|_{\mathrm{im}(d_{n+1})} = 0 \right\} / \{ f = g \circ d_n \mid \exists g : P_{n-1} \to N \}$$

Ext groups

M, N right-$\mathcal{B}$ modules. $\mathrm{Rad}(M) = M \cdot J_{\mathcal{B}}$ for basic algebras!

Projective resolution of M

$\cdots \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \cdots \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} M \to 0$, such that

- $P_0, P_1, \ldots$ projective $\mathcal{B}$ modules
- $\ker(\epsilon) = \mathrm{im}(d_1)$ and $\ker(d_i) = \mathrm{im}(d_{i+1})$ for $i = 1, 2, \ldots$

Resolution is minimal $\iff$ $\mathrm{im}(d_i) \subseteq \mathrm{Rad}(P_{i-1})$ for $i = 1, 2, \ldots$

Ext group $\mathrm{Ext}^n_{\mathcal{B}}(M, N)$

$$:= \left\{ P_n \xrightarrow{f} N \mid f|_{\mathrm{im}(d_{n+1})} = 0 \right\} / \{f = g \circ d_n \mid \exists g : P_{n-1} \to N\}$$

If resolution minimal and N simple:

$\mathrm{Ext}^n_{\mathcal{B}}(M, N) = \mathrm{Hom}_{\mathcal{B}}(P_n, N)$,
since the image of the radical in a simple module is zero.

Ext algebras: The Yoneda product

Let $Q_* \xrightarrow{\eta} N \to 0$ be a minimal projective resolution, N simple.

Lifting $f \in \mathrm{Ext}^n_{\mathcal{B}}(M, N)$ to a chain map

$$
\begin{tikzcd}
\cdots \arrow[r, "d_{n+2}"] \arrow[d, dotted] & P_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, dashed, "f_1"'] & P_n \arrow[d, dashed, "f_0"'] \arrow[dr, "f"] & & \\
\cdots \arrow[r, "\delta_2"] & Q_1 \arrow[r, "\delta_1"] & Q_0 \arrow[r, two heads, "\eta"] & N \arrow[r] & 0
\end{tikzcd}
$$

Ext algebras: The Yoneda product

Let $Q_* \xrightarrow{\eta} N \to 0$ be a minimal projective resolution, N simple.

Lifting $f \in \mathrm{Ext}^n_{\mathcal{B}}(M, N)$ to a chain map

$$\begin{tikzcd}
\cdots \arrow[r, "d_{n+2}"] \arrow[d, dotted] & P_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, dashed, "f_1"'] & P_n \arrow[d, dashed, "f_0"'] \arrow[dr, "f"] & & \\
\cdots \arrow[r, "\delta_2"] & Q_1 \arrow[r, "\delta_1"] & Q_0 \arrow[r, two heads, "\eta"] & N \arrow[r] & 0
\end{tikzcd}$$

Multiplying f with $g \in \mathrm{Ext}^r_{\mathcal{B}}(N, L)$, L simple module

$g \cdot f$ is given by $P_{n+r} \xrightarrow{f_r} Q_r \xrightarrow{g} L \in \mathrm{Ext}^{n+r}_{\mathcal{B}}(M, L)$

Ext algebra $\mathrm{Ext}^*(\mathcal{B}) = \bigoplus_{i,j=1}^{q} \bigoplus_{n=0}^{\infty} \mathrm{Ext}^n_{\mathcal{B}}(S_i, S_j)$

Associative and graded, but very much non-commutative

Finitely presented graded associative algebras in Sage

- $\mathrm{Ext}^*(\mathcal{B})$ is a *graded* associative algebra
  $\rightsquigarrow$ can represent it as quotient of a free associative algebra modulo *weighted homogeneous* relations

Finitely presented graded associative algebras in Sage

- $\mathrm{Ext}^*(\mathcal{B})$ is a *graded* associative algebra
  $\rightsquigarrow$ can represent it as quotient of a free associative algebra modulo *weighted homogeneous* relations
- Idea of LETTERPLACE (Levandovskyy–LaScala):
  Represent degree-$\leq d$ part of a free algebra in a large *commutative* ring, whose size grows with d.

Finitely presented graded associative algebras in Sage

- $\mathrm{Ext}^*(\mathcal{B})$ is a *graded* associative algebra
  $\rightsquigarrow$ can represent it as quotient of a free associative algebra modulo *weighted homogeneous* relations
- Idea of LETTERPLACE (Levandovskyy–LaScala):
  Represent degree-$\leq d$ part of a free algebra in a large *commutative* ring, whose size grows with d.
- Singular's LETTERPLACE can only deal with *homogeneous* elements and a fixed degree bound.
- Sage's LETTERPLACE wrapper (in Sage–5.5) has *adaptive* degree bound and can use positive integral degree weights

Finitely presented graded associative algebras in Sage

- $\mathrm{Ext}^*(\mathcal{B})$ is a *graded* associative algebra
  $\rightsquigarrow$ can represent it as quotient of a free associative algebra modulo *weighted homogeneous* relations
- Idea of LETTERPLACE (Levandovskyy–LaScala):
  Represent degree-$\leq d$ part of a free algebra in a large *commutative* ring, whose size grows with d.
- Singular's LETTERPLACE can only deal with *homogeneous* elements and a fixed degree bound.
- Sage's LETTERPLACE wrapper (in Sage–5.5) has *adaptive* degree bound and can use positive integral degree weights
- Bad: Polynomial rings were kept alive in memory. Needed:
  - Weak cache for `UniqueRepresentation` and coercion maps
    $\rightsquigarrow$ Trac tickets #715, #11521, #12215, #12313, #14159, ...

Finitely presented graded associative algebras in Sage

- $\mathrm{Ext}^*(\mathcal{B})$ is a *graded* associative algebra
  $\rightsquigarrow$ can represent it as quotient of a free associative algebra modulo *weighted homogeneous* relations
- Idea of LETTERPLACE (Levandovskyy–LaScala):
  Represent degree-$\leq d$ part of a free algebra in a large *commutative* ring, whose size grows with d.
- Singular's LETTERPLACE can only deal with *homogeneous* elements and a fixed degree bound.
- Sage's LETTERPLACE wrapper (in Sage–5.5) has *adaptive* degree bound and can use positive integral degree weights
- Bad: Polynomial rings were kept alive in memory. Needed:
  - Weak cache for `UniqueRepresentation` and coercion maps
    $\rightsquigarrow$ Trac tickets #715, #11521, #12215, #12313, #14159, ...
  - fix of a memory corruption in Singular
  - fix of a bug in Cython related with weak references

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.
- Represent P_n, P_{n-1} as sub-modules of $\mathcal{A}^s, \mathcal{A}^t$, modulo G_0.
- For $\mathfrak{x}_1, \ldots, \mathfrak{x}_s$ generators for P_n, let $p_i \in \mathcal{A}^t$ represent $d_n(\mathfrak{x}_i)$.

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.
- Represent P_n, P_{n-1} as sub-modules of $\mathcal{A}^s, \mathcal{A}^t$, modulo G_0.
- For $\mathfrak{x}_1, \ldots, \mathfrak{x}_s$ generators for P_n, let $p_i \in \mathcal{A}^t$ represent $d_n(\mathfrak{x}_i)$.
- Let $M \subset \mathcal{A}^t \oplus \mathcal{A}^s$ be generated by $\{p_i - \mathfrak{x}_i | \ i = 1, \ldots, s\}$
- G standard basis of M for elimination order $\rightsquigarrow$ Elements of G vanishing in the first block yield generators of $\ker(d_n)$.

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.
- Represent P_n, P_{n-1} as sub-modules of $\mathcal{A}^s, \mathcal{A}^t$, modulo G_0.
- For $\mathfrak{x}_1, \ldots, \mathfrak{x}_s$ generators for P_n, let $p_i \in \mathcal{A}^t$ represent $d_n(\mathfrak{x}_i)$.
- Let $M \subset \mathcal{A}^t \oplus \mathcal{A}^s$ be generated by $\{p_i - \mathfrak{x}_i | \; i = 1, \ldots, s\}$
- G standard basis of M for elimination order $\rightsquigarrow$ Elements of G vanishing in the first block yield generators of $\ker(d_n)$.

How to get a *minimal* generating set of $\ker(d_n)$?

- E. Green, Solberg, Zacharia: Minimization as a second step

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.
- Represent P_n, P_{n-1} as sub-modules of $\mathcal{A}^s, \mathcal{A}^t$, modulo G_0.
- For $\mathfrak{x}_1, \dots, \mathfrak{x}_s$ generators for P_n, let $p_i \in \mathcal{A}^t$ represent $d_n(\mathfrak{x}_i)$.
- Let $M \subset \mathcal{A}^t \oplus \mathcal{A}^s$ be generated by $\{p_i - \mathfrak{x}_i | \ i = 1, \dots, s\}$
- G standard basis of M for elimination order $\rightsquigarrow$ Elements of G vanishing in the first block yield generators of $\ker(d_n)$.

How to get a *minimal* generating set of $\ker(d_n)$?

- E. Green, Solberg, Zacharia: Minimization as a second step
- Carlson: Linear algebra is faster!

How to compute minimal projective resolutions

Recall: Computing Syzygies with standard bases

- Let G_0 be a standard basis for I, hence, $\mathcal{B} = \mathcal{A}/\langle G_0 \rangle$.
- Represent P_n, P_{n-1} as sub-modules of $\mathcal{A}^s, \mathcal{A}^t$, modulo G_0.
- For $\mathfrak{x}_1, \ldots, \mathfrak{x}_s$ generators for P_n, let $p_i \in \mathcal{A}^t$ represent $d_n(\mathfrak{x}_i)$.
- Let $M \subset \mathcal{A}^t \oplus \mathcal{A}^s$ be generated by $\{p_i - \mathfrak{x}_i \mid\ i = 1, \ldots, s\}$
- G standard basis of M for elimination order $\rightsquigarrow$ Elements of G vanishing in the first block yield generators of $\ker(d_n)$.

How to get a *minimal* generating set of $\ker(d_n)$?

- E. Green, Solberg, Zacharia: Minimization as a second step
- Carlson: Linear algebra is faster!
- D. Green: "Heady Buchberger algorithm"
  This is currently fastest, see p_group_cohomology.

Basic setup for Faugère F_5

Algebra:

- $\mathrm{Mon}(\mathcal{A}) \leftrightarrow$ paths, with *admissible* monomial ordering.
- $\psi : \mathcal{A} \twoheadrightarrow \mathcal{B} = \mathcal{A}/I$,
  $\mathrm{Mon}(\mathcal{B}) = \{\psi(\tilde{\mathfrak{m}}) : \tilde{\mathfrak{m}}$ standard monomial, i.e., $\mathfrak{m} \notin \mathrm{lead}(I)\}$
- $\lambda : \mathrm{Mon}(\mathcal{B}) \to \mathrm{Mon}(\mathcal{A})$ — lift,
  $\lambda(\mathfrak{m}) = \tilde{\mathfrak{m}}$ unique standard monomial with $\psi(\lambda(\tilde{\mathfrak{m}})) = \mathfrak{m}$

Basic setup for Faugère F_5

Algebra:

- $\mathrm{Mon}(\mathcal{A}) \leftrightarrow$ paths, with *admissible* monomial ordering.
- $\psi : \mathcal{A} \twoheadrightarrow \mathcal{B} = \mathcal{A}/I$,
  $\mathrm{Mon}(\mathcal{B}) = \{\psi(\tilde{\mathfrak{m}}) : \tilde{\mathfrak{m}}$ standard monomial, i.e., $\mathfrak{m} \notin \mathrm{lead}(I)\}$
- $\lambda : \mathrm{Mon}(\mathcal{B}) \to \mathrm{Mon}(\mathcal{A})$ — lift,
  $\lambda(\mathfrak{m}) = \tilde{\mathfrak{m}}$ unique standard monomial with $\psi(\lambda(\tilde{\mathfrak{m}})) = \mathfrak{m}$
- For $\mathfrak{m}, \mathfrak{c}, \mathfrak{n} \in \mathrm{Mon}(\mathcal{B})$: $\mathfrak{m}|_{\mathfrak{c}}\mathfrak{n} \iff \lambda(\mathfrak{n}) = \lambda(\mathfrak{m}) \cdot \lambda(\mathfrak{c})$
  In this case, $\mathfrak{c}$ is called a *small cofactor* of $\mathfrak{m}$.

Basic setup for Faugère F_5

Algebra:

- $\mathrm{Mon}(\mathcal{A}) \leftrightarrow$ paths, with *admissible* monomial ordering.
- $\psi : \mathcal{A} \twoheadrightarrow \mathcal{B} = \mathcal{A}/I$,
  $\mathrm{Mon}(\mathcal{B}) = \{\psi(\tilde{\mathfrak{m}}) : \tilde{\mathfrak{m}}$ standard monomial, i.e., $\mathfrak{m} \notin \mathrm{lead}(I)\}$
- $\lambda : \mathrm{Mon}(\mathcal{B}) \to \mathrm{Mon}(\mathcal{A})$ — lift,
  $\lambda(\mathfrak{m}) = \tilde{\mathfrak{m}}$ unique standard monomial with $\psi(\lambda(\tilde{\mathfrak{m}})) = \mathfrak{m}$
- For $\mathfrak{m}, \mathfrak{c}, \mathfrak{n} \in \mathrm{Mon}(\mathcal{B})$: $\mathfrak{m}|_{\mathfrak{c}}\mathfrak{n} \iff \lambda(\mathfrak{n}) = \lambda(\mathfrak{m}) \cdot \lambda(\mathfrak{c})$
  In this case, $\mathfrak{c}$ is called a *small cofactor* of $\mathfrak{m}$.

Modules:

- $F = \mathcal{B}^{\oplus r} \supset M = \langle \hat{g}_1, \ldots, \hat{g}_m \rangle_{\mathcal{B}}$, right–$\mathcal{A}$–module via ψ
- $E = \mathcal{A}^{\oplus m}$, free generators $\mathfrak{e}_1, \ldots, \mathfrak{e}_m$,
  $\mathrm{Mon}(E) = \{\mathfrak{e}_i \cdot \mathfrak{m} : \mathfrak{m} \in \mathrm{Mon}(\mathcal{A}), i = 1, \ldots, m\}$, mon. ordering
- $\mathrm{ev} : E \twoheadrightarrow M$ — epi of right–$\mathcal{A}$–modules, $\mathrm{ev}(\mathfrak{e}_i \cdot \mathfrak{m}) = \hat{g}_i \cdot \psi(\mathfrak{m})$

Signed standard bases

- $x = (\mathrm{u}(x), \sigma(x)) \in M \times \mathrm{Mon}(E)$ is a *signed element* of M
  $x \in_s M :\Longleftrightarrow \; \exists \tilde{x} \in E : \mathrm{ev}(\tilde{x}) = \mathrm{u}(x)$ and $\mathrm{lm}(\tilde{x}) = \sigma(x)$.
  Similarly $G \subset_s M$

Signed standard bases

- $x = (\mathrm{u}(x), \sigma(x)) \in M \times \mathrm{Mon}(E)$ is a *signed element* of M
  $x \in_s M :\Longleftrightarrow \exists \tilde{x} \in E : \mathrm{ev}(\tilde{x}) = \mathrm{u}(x)$ and $\mathrm{lm}(\tilde{x}) = \sigma(x)$.
  Similarly $G \subset_s M$
- $g \in_s M$ *reductor* of $x \in_s M$
  $:\Longleftrightarrow \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(x)),\ \sigma(g) \cdot \lambda(\mathfrak{c}) < \sigma(x)$
- $x \in_s M$ *irreducible* $:\Longleftrightarrow$ it has no reductor in M

Signed standard bases

- $x = (\mathrm{u}(x), \sigma(x)) \in M \times \mathrm{Mon}(E)$ is a *signed element* of M
  $x \in_s M :\Longleftrightarrow \exists \tilde{x} \in E : \mathrm{ev}(\tilde{x}) = \mathrm{u}(x)$ and $\mathrm{lm}(\tilde{x}) = \sigma(x)$.
  Similarly $G \subset_s M$
- $g \in_s M$ *reductor* of $x \in_s M$
  $:\Longleftrightarrow \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(x)),\ \sigma(g) \cdot \lambda(\mathfrak{c}) < \sigma(x)$
- $x \in_s M$ *irreducible* $:\Longleftrightarrow$ it has no reductor in M
- *Elementary reduction*

$$x \searrow \left(\mathrm{u}(x) - \frac{\mathrm{lc}(\mathrm{u}(x))}{\mathrm{lc}(\mathrm{u}(g))}\mathrm{u}(g) \cdot \mathfrak{c}, \sigma(x)\right) \in_s M$$

Signed standard bases

- $x = (\mathrm{u}(x), \sigma(x)) \in M \times \mathrm{Mon}(E)$ is a *signed element* of M
  $x \in_s M :\iff \exists \tilde{x} \in E : \mathrm{ev}(\tilde{x}) = \mathrm{u}(x)$ and $\mathrm{lm}(\tilde{x}) = \sigma(x)$.
  Similarly $G \subset_s M$
- $g \in_s M$ *reductor* of $x \in_s M$
  $:\iff \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(x)),\ \sigma(g) \cdot \lambda(\mathfrak{c}) < \sigma(x)$
- $x \in_s M$ *irreducible* $:\iff$ it has no reductor in M
- *Elementary reduction*
  $$x \searrow \left(\mathrm{u}(x) - \frac{\mathrm{lc}(\mathrm{u}(x))}{\mathrm{lc}(\mathrm{u}(g))} \mathrm{u}(g) \cdot \mathfrak{c}, \sigma(x)\right) \in_s M$$
- $\mathrm{NF}(x; G) \in_s M$: Iterate elementary reductions wrt. G.
  $\sigma(\mathrm{NF}(x; G)) = \sigma(x)$, and $\mathrm{NF}(x; G)$ has no reductor in G.

Signed standard bases

- $x = (\mathrm{u}(x), \sigma(x)) \in M \times \mathrm{Mon}(E)$ is a *signed element* of M
  $x \in_s M :\Longleftrightarrow \exists \tilde{x} \in E : \mathrm{ev}(\tilde{x}) = \mathrm{u}(x)$ and $\mathrm{lm}(\tilde{x}) = \sigma(x)$.
  Similarly $G \subset_s M$
- $g \in_s M$ *reductor* of $x \in_s M$
  $:\Longleftrightarrow \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(x)),\ \sigma(g) \cdot \lambda(\mathfrak{c}) < \sigma(x)$
- $x \in_s M$ *irreducible* $:\Longleftrightarrow$ it has no reductor in M
- *Elementary reduction*
  $$x \searrow \left(\mathrm{u}(x) - \frac{\mathrm{lc}(\mathrm{u}(x))}{\mathrm{lc}(\mathrm{u}(g))}\mathrm{u}(g) \cdot \mathfrak{c}, \sigma(x)\right) \in_s M$$
- $\mathrm{NF}(x; G) \in_s M$: Iterate elementary reductions wrt. G.
  $\sigma\left(\mathrm{NF}(x; G)\right) = \sigma(x)$, and $\mathrm{NF}(x; G)$ has no reductor in G.

Def: *Signed standard basis* $G \subset_s M$ of M

$:\Longleftrightarrow$ for all irreducible $x \in_s M \setminus \{0\}$ there is $g \in G$ with
$\mathrm{lm}(g)|_{\mathfrak{c}} \mathrm{lm}(x),\ \sigma(g) \cdot \lambda(\mathfrak{c}) \leq \sigma(x)$ (actually: "$=$")

Computing signed standard bases

Let $g \in G \subset_s M$, $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$, $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$

Critical pairs with cofactor $\mathfrak{c}$: Getting new leading monomials

Computing signed standard bases

Let $g \in G \subset_s M$, $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$, $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$

Critical pairs with cofactor $\mathfrak{c}$: Getting new leading monomials

Type T: ("toppling" in D. Green's work)

- $\mathfrak{c}$ is *not* small cofactor of $\mathrm{lm}(\mathrm{u}(g))$, but all proper divisors are.
- *L-normal pair* $\iff$ g irreducible wrt. G, and $\sigma(g) \cdot \lambda(\mathfrak{c}) \notin L$
- *S-polynomial* $\mathcal{S} := (\mathrm{u}(g) \cdot \mathfrak{c},\ \sigma(g) \cdot \lambda(\mathfrak{c})) \in_s M$

Computing signed standard bases

Let $g \in G \subset_s M$, $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$, $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$

Critical pairs with cofactor $\mathfrak{c}$: Getting new leading monomials

Type T: ("toppling" in D. Green's work)

- $\mathfrak{c}$ is *not* small cofactor of $\mathrm{lm}(\mathrm{u}(g))$, but all proper divisors are.
- *L-normal pair* $\iff$ g irreducible wrt. G, and $\sigma(g) \cdot \lambda(\mathfrak{c}) \notin L$
- *S-polynomial* $\mathcal{S} := (\mathrm{u}(g) \cdot \mathfrak{c},\ \sigma(g) \cdot \lambda(\mathfrak{c})) \in_s M$

Type S: ("S-polynomial" in the unsigned world)

- $\exists g' \in G : \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}}\, \mathrm{lm}(\mathrm{u}(g'))$ and $\sigma(g') < \sigma(g) \cdot \lambda(\mathfrak{c})$
- *L-normal pair* $\iff$ g, g' irred. wrt. G, and $\sigma(g) \cdot \lambda(\mathfrak{c}) \notin L$
- *S-polynomial* $\mathcal{S} := \left(\mathrm{u}(g) \cdot \mathfrak{c} - \frac{\mathrm{lc}(g')}{\mathrm{lc}(g)} g',\ \sigma(g) \cdot \lambda(\mathfrak{c})\right) \in_s M$

Computing signed standard bases

Let $g \in G \subset_s M$, $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$, $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$

Critical pairs with cofactor $\mathfrak{c}$: Getting new leading monomials

Type T: ("toppling" in D. Green's work)

- $\mathfrak{c}$ is *not* small cofactor of $\mathrm{lm}(\mathrm{u}(g))$, but all proper divisors are.
- *L-normal pair* $\iff$ g irreducible wrt. G, and $\sigma(g) \cdot \lambda(\mathfrak{c}) \notin L$
- *S-polynomial* $\mathcal{S} := (\mathrm{u}(g) \cdot \mathfrak{c},\ \sigma(g) \cdot \lambda(\mathfrak{c})) \in_s M$

Type S: ("S-polynomial" in the unsigned world)

- $\exists g' \in G : \mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}}\, \mathrm{lm}(\mathrm{u}(g'))$ and $\sigma(g') < \sigma(g) \cdot \lambda(\mathfrak{c})$
- *L-normal pair* $\iff$ g, g' irred. wrt. G, and $\sigma(g) \cdot \lambda(\mathfrak{c}) \notin L$
- *S-polynomial* $\mathcal{S} := \left(\mathrm{u}(g) \cdot \mathfrak{c} - \frac{\mathrm{lc}(g')}{\mathrm{lc}(g)} g',\ \sigma(g) \cdot \lambda(\mathfrak{c})\right) \in_s M$

Not L-normal $\Rightarrow$ there is a "smaller" construction for $\mathrm{u}(\mathcal{S})$!

The F_5 criterion—including Faugère's "rewritten criterion"

- Let $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$, let $G \subset_s M \setminus \{0\}$ be *interreduced*

The F_5 criterion—including Faugère's "rewritten criterion"

- Let $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$, let $G \subset_s M \setminus \{0\}$ be *interreduced*
- Assume $\forall i$ with $\mathfrak{e}_i \notin \mathrm{lead}(\ker(\mathrm{ev}))$ $\exists g \in G$ with $\sigma(g) = \mathfrak{e}_i$

The F_5 criterion—including Faugère's "rewritten criterion"

- Let $L \subset \text{lead}(\ker(\text{ev}))$, let $G \subset_s M \setminus \{0\}$ be *interreduced*
- Assume $\forall i$ with $\mathfrak{e}_i \notin \text{lead}(\ker(\text{ev}))$ $\exists g \in G$ with $\sigma(g) = \mathfrak{e}_i$

The F_5 *criterion* holds for an S-polynomial $\mathcal{S}$

$:\Longleftrightarrow$ $\exists g \in G$ and a small cofactor $\mathfrak{c} \in \text{Mon}(\mathcal{B})$ of $\text{Im}(\text{u}(g))$ with

- $\sigma(g) \cdot \lambda(\mathfrak{c}) = \sigma(\mathcal{S})$, and
- $(\text{u}(g) \cdot \mathfrak{c}, \sigma(\mathcal{S})) \in_s M$ has no reductor in G.

The F_5 criterion—including Faugère's "rewritten criterion"

- Let $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$, let $G \subset_s M \setminus \{0\}$ be *interreduced*
- Assume $\forall i$ with $\mathfrak{e}_i \notin \mathrm{lead}(\ker(\mathrm{ev}))$ $\exists g \in G$ with $\sigma(g) = \mathfrak{e}_i$

The F$_5$ *criterion* holds for an S-polynomial $\mathcal{S}$

$:\Longleftrightarrow$ $\exists g \in G$ and a small cofactor $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$ of $\mathrm{lm}(\mathrm{u}(g))$ with

- $\sigma(g) \cdot \lambda(\mathfrak{c}) = \sigma(\mathcal{S})$, and
- $(\mathrm{u}(g) \cdot \mathfrak{c}, \sigma(\mathcal{S})) \in_s M$ has no reductor in G.

Remark

If not $\mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(\mathcal{S}))$, then $\mathrm{lm}(\mathrm{u}(\mathcal{S}))$ can be obtained by a different construction that is *smaller* than $\sigma(\mathcal{S})$.

The F_5 criterion—including Faugère's "rewritten criterion"

- Let $L \subset \mathrm{lead}(\ker(\mathrm{ev}))$, let $G \subset_s M \setminus \{0\}$ be *interreduced*
- Assume $\forall i$ with $\mathfrak{e}_i \notin \mathrm{lead}(\ker(\mathrm{ev}))$ $\exists g \in G$ with $\sigma(g) = \mathfrak{e}_i$

The F_5 *criterion* holds for an S-polynomial $\mathcal{S}$

$:\Longleftrightarrow$ $\exists g \in G$ and a small cofactor $\mathfrak{c} \in \mathrm{Mon}(\mathcal{B})$ of $\mathrm{lm}(\mathrm{u}(g))$ with

- $\sigma(g) \cdot \lambda(\mathfrak{c}) = \sigma(\mathcal{S})$, and
- $(\mathrm{u}(g) \cdot \mathfrak{c}, \sigma(\mathcal{S})) \in_s M$ has no reductor in G.

Remark

If not $\mathrm{lm}(\mathrm{u}(g))|_{\mathfrak{c}} \mathrm{lm}(\mathrm{u}(\mathcal{S}))$, then $\mathrm{lm}(\mathrm{u}(\mathcal{S}))$ can be obtained by a different construction that is *smaller* than $\sigma(\mathcal{S})$.

Theorem

G is a signed standard basis of M $\Longleftrightarrow$
F_5 criterion holds for S-polynomials of all L-normal critical pairs.

F_5 algorithm variant by Arri–Perry: Learn from mistakes

- $L_0 := \{\mathfrak{e}_i \cdot \mathfrak{m} \colon i = 1, \ldots, m,\ \mathfrak{m} \in \mathrm{lead}(I)\} \subset \mathrm{lead}(\mathrm{ker}(\mathrm{ev}))$
  trivial Syzygies
- For $x \in_s M$, $G \subset_s M$: $\mathrm{u}(\mathrm{NF}(x; G)) = 0$
  $\Longrightarrow \exists y \in_s M \colon \mathrm{u}(y) = \mathrm{u}(x)$ and $\sigma(y) < \sigma(x)$
  $\Longrightarrow \sigma(x) \in \mathrm{lead}(\mathrm{ker}(\mathrm{ev}))$

F_5 algorithm variant by Arri–Perry: Learn from mistakes

- $L_0 := \{\mathfrak{e}_i \cdot \mathfrak{m} \colon i = 1, \ldots, m,\ \mathfrak{m} \in \text{lead}(I)\} \subset \text{lead}(\ker(\text{ev}))$
  trivial Syzygies
- For $x \in_s M$, $G \subset_s M$: $\text{u}(\mathrm{NF}(x; G)) = 0$
  $\Longrightarrow \exists y \in_s M \colon \text{u}(y) = \text{u}(x)$ and $\sigma(y) < \sigma(x)$
  $\Longrightarrow \sigma(x) \in \text{lead}(\ker(\text{ev}))$

F_5 algorithm

START: Set $G \leftarrow \{\hat{g}_1, \ldots, \hat{g}_r\}$, $L \leftarrow L_0$

WHILE $\exists$ L-normal critical pair with S-polynomial $\mathcal{S}$ violating F_5:

  $x \leftarrow \mathrm{NF}(\mathcal{S}; G)$

  IF $\text{u}(x) = 0$: $L \leftarrow L \cup (\sigma(x) \cdot \text{Mon}(\mathcal{P}))$

    ELSE: $G \leftarrow \text{interred}(G \cup \{x\})$ (interred may add to L)

RETURN G

Application: Read off Loewy layers

- The d-th *Loewy layer* is $\mathcal{L}_d(M) := \operatorname{Rad}^{d-1}(M) / \operatorname{Rad}^d(M)$
- Recall $\operatorname{Rad}^d(M) = M \cdot J_{\mathcal{B}}^d$ for basic algebras $\mathcal{B}$

Application: Read off Loewy layers

- The d-th *Loewy layer* is $\mathcal{L}_d(M) := \operatorname{Rad}^{d-1}(M)/\operatorname{Rad}^d(M)$
- Recall $\operatorname{Rad}^d(M) = M \cdot J_{\mathcal{B}}^d$ for basic algebras $\mathcal{B}$

The k-bases of $\mathcal{L}_0(M)$ are the minimal generating sets of M!

Application: Read off Loewy layers

- The d-th *Loewy layer* is $\mathcal{L}_d(M) := \operatorname{Rad}^{d-1}(M)/\operatorname{Rad}^d(M)$
- Recall $\operatorname{Rad}^d(M) = M \cdot J_{\mathcal{B}}^d$ for basic algebras $\mathcal{B}$

The k-bases of $\mathcal{L}_0(M)$ are the minimal generating sets of M!

- Hypothesis: G is an interreduced signed standard basis of M wrt. a negative degree monomial ordering.
- Denote $[f]$ for the equ. class of $f \in \operatorname{Rad}^{d-1}(M)$ in $\mathcal{L}_d(M)$.

Application: Read off Loewy layers

- The d-th *Loewy layer* is $\mathcal{L}_d(M) := \operatorname{Rad}^{d-1}(M)/\operatorname{Rad}^d(M)$
- Recall $\operatorname{Rad}^d(M) = M \cdot J_{\mathcal{B}}^d$ for basic algebras $\mathcal{B}$

The k-bases of $\mathcal{L}_0(M)$ are the minimal generating sets of M!

- Hypothesis: G is an interreduced signed standard basis of M wrt. a negative degree monomial ordering.
- Denote $[f]$ for the equ. class of $f \in \operatorname{Rad}^{d-1}(M)$ in $\mathcal{L}_d(M)$.

Theorem

The set of all $[\mathrm{u}(g) \cdot \mathfrak{c}]$ with $g \in G$ and small cofactors $\mathfrak{c} \in \operatorname{Mon} \mathcal{B}$ of $\operatorname{Im}(\mathrm{u}(g))$ such that

- $\deg(\sigma(g) \cdot \lambda(\mathfrak{c})) = d - 1$ and
- $(\mathrm{u}(g) \cdot \mathfrak{c}, \sigma(g) \cdot \lambda(\mathfrak{c})) \in_s M$ has no reductor in G.

forms a k-vector space basis of $\mathcal{L}_d(M)$.

Results of a toy implementation in Sage

Why to compute Ext algebras?

- $H^*(G;k) = \mathrm{Ext}^*(S_0, S_0)$, S_0 trivial representation.

Results of a toy implementation in Sage

Why to compute Ext algebras?

- $H^*(G; k) = \mathrm{Ext}^*(S_0, S_0)$, S_0 trivial representation.
- Presentation degree for Ext versus cohomology:
  - M11 mod 2: Degree 5 versus degree 10
  - L3(2) mod 2: Degree 3 versus degree 6
  - J1 mod 7: Degree 7 versus degree 22
  - J1 mod 11: Degree 11 versus degree 38
  - J1 mod 19: Degree 15 versus degree 22

Results of a toy implementation in Sage

Why to compute Ext algebras?

- $H^*(G;k) = \mathrm{Ext}^*(S_0, S_0)$, S_0 trivial representation.
- Presentation degree for Ext versus cohomology:
  - M11 mod 2: Degree 5 versus degree 10
  - L3(2) mod 2: Degree 3 versus degree 6
  - J1 mod 7: Degree 7 versus degree 22
  - J1 mod 11: Degree 11 versus degree 38
  - J1 mod 19: Degree 15 versus degree 22

Efficiency: F_5 versus Heady

- A_9 mod 3, 2^{nd} and 3^{rd} term of min. proj. resolution
  - Heady needs > 1800 and < 2600 zero reductions.
  - F_5 can do with < 1300 and < 1500 zero reductions.
- F_5 computes resolutions out to degree 13 for A_5 mod 3 and 2nd block of M_{12} mod 5 without any zero reduction.