An F_5 Algorithm for Modules over Path Algebra Quotients and the Computation of Loewy Layers

Simon King [DFG project KI 861/2–1]

June 02, 2015

seit 1558

My motivation for studying path algebras

Group cohomology package for Sage (K, D. Green), #18514 for upgrade

`http://sage.math.washington.edu/home/SimonKing/Cohomology`

- Modular cohomology rings for groups of order 128, HS, McL, Co_3, Janko groups (not J_4), Mathieu groups (not M_{24}), ...
- It starts with computing minimal projective resolutions for $\mathbb{F}_p G$ ($|G| = p^n$), which can be a bottle neck $\rightsquigarrow$ improve it!
- Extend scope: Resolutions for basic algebras $\rightsquigarrow$ Ext algebras.

Computing minimal generating sets for kernels of module homomorphisms

- E. Green, Solberg, Zacharia [2001]: Use non-commutative Gröbner bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases*, used in spkg.
- K [2014]: Non-commutative F_5 algorithm finds *Loewy layers* and avoids redundant computations. Soon in SageMath library.

Basic algebras? Loewy layers?

$\mathcal{P}$ path algebra for quiver Q over field K

- $\mathcal{P}$ is a graded associative algebra, usually with zero divisors.
- We study path algebra *quotients* $\psi\colon \mathcal{P} \twoheadrightarrow \mathcal{A}$, with a focus on Basic algebras: $\mathcal{A}$ finite dimensional, $\ker(\psi) \subset \mathcal{P}_+^2$

Loewy layers of submodule $M \leq \mathcal{A}^r$, $\mathcal{A}$ basic algebra

- $\operatorname{Rad}(\mathcal{A}) = \mathcal{A}_+ = \langle m \in \mathcal{A} | m \text{ arrow}\rangle$ (quadratic relations!)
- $\operatorname{Rad}^0(M) = M$ and $\operatorname{Rad}^d(M) = \operatorname{Rad}^{d-1}(M) \cdot \operatorname{Rad}(\mathcal{A})$
- The d-th *Loewy layer* $\mathcal{L}^d(M)$ is $\operatorname{Rad}^{d-1}(M)/\operatorname{Rad}^d(M)$

Motivation for studying Loewy layers of modules over basic algebras

- Each K–basis of $\mathcal{L}^1(M)$ is a minimal generating set for M $\rightsquigarrow$ replace heady algorithm in the spkg.

Outline

1. Computational setup
   - Path algebra quotients
   - Right modules
   - *Non*-commutative F_5??
2. The F_5 signature
   - Signed elements
   - Signed reduction
3. Signed standard bases
   - Critical pairs and S-polynomials
   - The revised F_5 criterion
4. Reading off Loewy layers via signed standard bases
   - Comparison and questions
5. Status of Implementation in SageMath

$\mathcal{P}$ path algebra of a finite quiver Q over a field K

- Monomials $\mathrm{Mon}(\mathcal{P}) \leftrightarrow$ oriented paths in Q
- Degree of monomial $\leftrightarrow$ path length
- Choose a *monomial ordering* $>$ on $\mathrm{Mon}(\mathcal{P})$.
  For $p \in \mathcal{P}$: $\mathrm{Lm}(p)$, $\mathrm{Lc}(p)$, $\mathrm{Lt}(p) = \mathrm{Lc}(p) \cdot \mathrm{Lm}(p)$.

$\psi\colon \mathcal{P} \twoheadrightarrow \mathcal{A}$ path algebra quotient

- $\mathrm{stdMon}_{\mathcal{A}}(\mathcal{P}) = \{m \in \mathrm{Mon}(\mathcal{P}) | \nexists p \in \ker(\psi)\colon\ \mathrm{Lm}(p) = m\}$
- $\mathrm{Mon}(\mathcal{A}) = \psi\left(\mathrm{stdMon}_{\mathcal{A}}(\mathcal{P})\right)$ is a K-basis of $\mathcal{A}$.
- Lift $\lambda\colon\ \mathrm{Mon}(\mathcal{A}) \to \mathrm{stdMon}_{\mathcal{A}}(\mathcal{P})$ with $\psi(\lambda(m)) = m$.
- $\mathcal{A}$ inherits grading and monomial ordering from $\mathcal{P}$ via λ.
- For $a, b, c \in \mathrm{Mon}(\mathcal{A})$: $a|_c b$ (a divides b with *small cofactor* c)
  $\iff\ \lambda(a) \cdot \lambda(c) = \lambda(b)$. Easy to verify!

Free modules over path algebra quotients

- $F = \bigoplus_{i=1}^{r} \mathfrak{v}_i \mathcal{A}$ free right $\mathcal{A}$-module, and a right $\mathcal{P}$-module via ψ.
- $\mathrm{Mon}(F) = \{\mathfrak{v}_i \cdot a | \, i = 1, ..., r; a \in \mathrm{Mon}(\mathcal{A})\}$.
- For $m = \mathfrak{v}_i \cdot a$, $n = \mathfrak{v}_j \cdot b \in \mathrm{Mon}(F)$: $m|_c n \iff i = j$ and $a|_c b$

Standard (Gröbner) bases of $M = \langle \hat{g}_1, ..., \hat{g}_m \rangle \leq F$

- Fix compatible monomial orderings on $\mathcal{P}$, $\mathcal{A}$, F. Choices!
- $G \subset M \leq F$ is *standard basis* of M $:\iff$ leading monomials of M are divisible by leading monomials of G.
- If it terminates: *Reduction* of $x \in F$ by a standard basis is zero $\iff x \in M$.

Finite standard bases do not always exist.

Buchberger vs. F_5 algorithm

Buchberger algorithm computes standard bases

Increments a generating set by "S-polynomials" of "critical pairs".
Zero reductions of S-polynomials are a waste of time.

Faugère's F_5 *for polynomial rings* beats Buchberger's algorithm!

Signature keeps track how elements of G were computed.
"Trivial syzygies" $f \cdot g = g \cdot f$ detect many redundant critical pairs.

There is no non-commutative $\mathbf{F_5}$! Useless in fin. dim. algebras!

Yes, there is, and it *is* useful!

- In a *quotient* $\psi\colon \mathcal{P} \twoheadrightarrow \mathcal{A}$, $\ker(\psi)$ provides us with trivial syzygies.
- Zero reductions provide *nontrivial* syzygies [Arri–Perry].
- Encode a huge vector space basis by a much smaller standard basis.
- Standard bases are not more than (useful) by-products of F_5 —the *signatures* provide essential information.

The F_5 signature

$\langle \hat{g}_1, \dots, \hat{g}_m \rangle = M \le F$ right $\mathcal{A}$-module, and right $\mathcal{P}$-module via ψ

- Let $S = \bigoplus_{i=1}^{m} \mathfrak{e}_i \mathcal{P}$, with some compatible monomial ordering.
- Epimorphism $ev\colon\ S \twoheadrightarrow M$ of right $\mathcal{P}$-modules with $ev(\mathfrak{e}_i) = \hat{g}_i\ \forall i$.
- $f \in S$ describes $ev(f) \in M$ as an $\mathcal{A}$–linear combination of the $\hat{g}_i$.

Def:

A *signed element* $p \in_s U \subset M$ is a pair $p = (u, \eta)$ with $u \in U$ and $\eta \in \mathrm{Mon}(S)$, such that $\exists f \in S\colon\ ev(f) = u$ and $\mathrm{Lm}(f) = \eta$.
Its *unsigned element* is $\mathrm{u}(p) := u$ and its *signature* $\sigma(p) := \eta$.

We only allow operations that keep track of signatures

- For $p \in_s M$ and $\tau \in \mathrm{Mon}(\mathcal{P})$: $(\mathrm{u}(p) \cdot \psi(\tau),\ \ \sigma(p) \cdot \tau) \in_s M$.
- If $p_1, p_2 \in_s M$, $\sigma(p_1) > \sigma(p_2)$: $(\mathrm{u}(p_1) + \mathrm{u}(p_2),\ \ \sigma(p_1)) \in_s M$.
  Otherwise, the addition won't be performed in the F_5 algorithm.

Signed reduction

η-reduction modulo G of $p \in F$, for $\eta \in \mathrm{Mon}(S)$, $G \subset_s M \setminus \{0\}$

- p is η-reducible modulo $G \iff p \neq 0$, and
  1. $\exists g \in G: \ \mathrm{Lm}(\mathrm{u}(g))|_c \, \mathrm{Lm}(p)$
  2. $\sigma(g) \cdot \lambda(c) < \eta$
- Otherwise, p is η-irreducible modulo G.
- Replace p by $p - \frac{\mathrm{Lc}(p)}{\mathrm{Lc}(\mathrm{u}(g))} g \cdot c$ and iterate $\rightsquigarrow \mathrm{NF}_\eta(p; G)$, which is η-irreducible modulo G. Termination?
- p is *weakly* η-reducible modulo $G \iff \ldots \ \sigma(g) \cdot \lambda(c) \leq \eta$.

For $p \in_s M$, implicitly choose $\eta = \sigma(p)$

- p is *irreducible* iff $\mathrm{u}(p)$ is $\sigma(p)$-irreducible modulo any signed $G \subset_s M$. *I.e.*, $\sigma(p)$ is optimal, there is no cheaper computation of $\mathrm{u}(p)$.
- $\mathrm{NF}(p; G) := \left(\mathrm{NF}_{\sigma(p)}(\mathrm{u}(p); G), \ \sigma(p)\right) \in_s M$. Signature is preserved!

Signed standard bases

Def: $G \subset_s M \setminus \{0\}$ is a *signed standard basis* of M

$\iff$ Every irreducible $p \in_s M \setminus \{0\}$ is weakly $\sigma(p)$-reducible modulo G.

Lemma

Let G be a signed standard basis of M.

- $p \in_s M \setminus \{0\}$ not irreducible $\implies \mathrm{NF}(p; G) = (0, \sigma(p))$.
  Proof idea: p has *irreducible* reductor $\in_s M$.
- $\mathrm{u}(G) = \{\mathrm{u}(g) | \, g \in G\}$ is a standard basis of M.

Def: $G \subset_s M \setminus \{0\}$ is *interreduced*

$\iff$ Every $g \in G$ is not weakly $\sigma(g)$-reducible modulo $G \setminus \{g\}$.

Critical pairs and S-polynomials

(g, c) *critical pair of type T* of G

$g \in G$ with $\mathrm{Lm}(\mathrm{u}(g)) = \mathfrak{v}_i \cdot a$, $c \in \mathrm{Mon}(\mathcal{A})$ such that c is not a small cofactor of a, and if $c' | c$ with $\deg(c') < \deg(c)$ then c' is a small cofactor of a. Chain criterion!
$S(g, c) := (\mathrm{u}(g) \cdot c,\ \ \sigma(g) \cdot \lambda(c)) \in_s M$

(g, g') *critical pair of type R* of G

$g \neq g' \in G$ with $\mathrm{Lm}(\mathrm{u}(g))|_c \mathrm{Lm}(\mathrm{u}(g'))$, but $\sigma(g) \cdot \lambda(c) > \sigma(g')$.
$S(g, g') := \left(\mathrm{u}(g') - \frac{\mathrm{Lc}(g')}{\mathrm{Lc}(g)} \mathrm{u}(g) \cdot c,\ \ \sigma(g) \cdot \lambda(c)\right) \in_s M$

Buchberger style computation of signed standard bases

- Start with $G = \{(\hat{g}_1, \mathfrak{e}_1), \ldots, (\hat{g}_m, \mathfrak{e}_m)\}$.
- Repeatedly add S-polynomials of critical pairs and interreduce.
- Be upset if a zero reduction occurs.

The revised F_5 criterion (A. Arri and J. Perry)

Let $L \subset \mathrm{Lm}(\ker(ev))$.

Def: A critical pair (g, c) resp. (g, g') is *normal* wrt. L

$\iff$ g (and g') is irreducible modulo G, and $\sigma(g) \cdot \lambda(c) \notin L$.

Def: G has the F_5 property relative to L

$\iff$ For all normal critical pairs $p = (g, c)$ resp. $p = (g, g')$ rel. L, $\exists h \in G$ and a small cofactor d of $\mathrm{Lm}(\mathrm{u}(h))$ s.t.

1. $\sigma(S(p)) = \sigma(g) \cdot \lambda(c) = \sigma(h) \cdot \lambda(d)$
2. $\mathrm{u}(h) \cdot d$ is $\sigma(g) \cdot \lambda(c)$-irreducible modulo G.

Learning from zero-reductions

If $\mathrm{u}(\mathrm{NF}(p; G)) = 0$ then $\sigma(p) \in \mathrm{Lm}(\ker(ev))$.
Add its two-sided multiples to $L \rightsquigarrow$ weaken the F_5 property.

Theorem: [F_5 *and* rewritten criterion in Faugère's terminology]

Let $G \subset_s M \setminus \{0\}$ be finite interreduced, and for all $i = 1, \dots, m$, either $\mathfrak{e}_i \in \mathrm{Lm}(\ker(ev))$ ($\hat{g}_i$ is redundant generator), or $\exists g \in G$ with $\sigma(g) = \mathfrak{e}_i$.
G signed standard basis of $M \iff$ it has the F_5 property.

F_5 algorithm

- Start with $G = \{(\hat{g}_1, \mathfrak{e}_1) \dots, (\hat{g}_m, \mathfrak{e}_m)\} \subset_s M$, and $L = \bigcup_{i=1}^m \mathfrak{e}_i \cdot \mathrm{Lm}(\ker(\psi)) \subset \mathrm{Lm}(\ker(ev))$.
  These are the trivial syzygies.
- For normal critical pairs rel. L violating F_5 (sorted):
  Compute the normal form of the S-polynomial
  - If non-zero: Add it to G, and interreduce G.
  - If zero: Add its signature to L.

Return G: It is an interreduced signed standard basis of M.

Rem: Each signature η of S-polynomials occurs at most once

Further crit. pairs for η will not be normal or will not violate F_5!

Signed standard bases and Loewy layers

Let $\mathcal{A}$ be a basic algebra and $>$ negative degree ordering on $\mathcal{P}, \mathcal{A}, F, S$

- $\mathcal{A}$ finite-dimensional $\Rightarrow F_5$ algorithm terminates, for all $>$, since only finitely many signatures are not in L.
- Let $\tau_d \in \mathrm{Mon}(S)$ maximal with $\deg(\tau) = d \in \mathbb{N}$.
  $\mathrm{Rad}^d(M) = \{f \in M\colon\ \exists \widetilde{f} \in S\colon\ \mathrm{Lm}(\widetilde{f}) \leq \tau_d \text{ and } ev(\widetilde{f}) = f\}$
  Uses that $\mathcal{A}$ is a basic algebra!
- Let G be an interreduced signed standard basis of M
  The elements $\mathrm{u}(g) \cdot c$ with
  1. $g \in G$, c small cofactor of $\mathrm{Lm}(\mathrm{u}(g))$
  2. $\sigma(g) \cdot \lambda(c) \leq \tau_d$
  3. $\mathrm{u}(g) \cdot c$ is $\sigma(g) \cdot \lambda(c)$-irreducible modulo G

  form a K-vector space basis $B_{\tau_d}(M, G)$ of $\mathrm{Rad}^d(M)$.
  Uses that $\mathcal{P}$ is a path algebra!
- $B_{\tau_{d-1}}(M, G) \setminus B_{\tau_d}(M, G)$ yields a basis of $\mathcal{L}^d(M)$.

Comparison and open questions

Comparison with David Green's "heady standard bases"

- "Heady" only keeps track whether $\deg(\sigma(p)) > 0$.
- "Heady" only computes $\mathcal{L}^1(M)$ (the "head" of M) and is state of the art for computing minimal generating sets.
- Critical pairs of type T are enough for the heady algorithm.
  But: Many zero reductions occur! $\rightsquigarrow$ F_5 should be better.

Questions

- Termination for noetherian algebras of infinite dimension? (open)
- Negative degree orderings in infinite dimension? (*weak* NF)
- When does F_5 run without any zero reduction? (open)
- Other problems whose solution can be encoded in the signature, for suitable monomial ordering?
- Competitive implementation?

Status of Implementation in SageMath

Quiver paths: #16453, merged last week → `sage.quivers.paths`

- Implement the semigroup formed by the paths of a quiver, in Cython
- Encode a path as a *long integer*
- Concatenation etc. based on fast shift operations in GMP/mpir.

Path algebras: #17435, *needs review*

- Path algebra elements as pointed lists; four term orderings available
- Uses copy-by-identity for monomials and a kill list for terms
- Basic arithmetic faster than with LETTERPLACE.

F_5 implementation, only on my laptop yet

- Uses geobucket data structure for the general case...
- ... and matrices as an alternative in the finite dimensional case.
- Faster than heady algo in examples, but needs debugging.