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
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, $C_{03}$, 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.
Basic algebras? Loewy layers?

**Path algebra for quiver** $Q$ over field $K$

- $\mathcal{P}$ is a graded associative algebra, usually with zero divisors.
- We study path algebra quotients $\psi: \mathcal{P} \rightarrow \mathcal{A}$, with a focus on basic algebras: $\mathcal{A}$ finite dimensional, $\ker(\psi) \subseteq \mathcal{P}^2$

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

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

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

\[ \psi : \mathcal{P} \rightarrow \mathcal{A} \] path algebra quotient

- \( \text{stdMon}_\mathcal{A}(\mathcal{P}) = \{ m \in \text{Mon}(\mathcal{P}) | \not\exists p \in \ker(\psi) : \text{Lm}(p) = m \} \)
- \( \text{Mon}(\mathcal{A}) = \psi(\text{stdMon}_\mathcal{A}(\mathcal{P})) \) is a \( K \)-basis of \( \mathcal{A} \).
- Lift \( \lambda : \text{Mon}(\mathcal{A}) \rightarrow \text{stdMon}_\mathcal{A}(\mathcal{P}) \) with \( \psi(\lambda(m)) = m \).
- \( \mathcal{A} \) inherits grading and monomial ordering from \( \mathcal{P} \) via \( \lambda \).
- For \( a, b, c \in \text{Mon}(\mathcal{A}) \): \( a \mid_c b \) (\( a \) divides \( b \) with \textit{small cofactor} \( c \))
  \[ \iff \lambda(a) \cdot \lambda(c) = \lambda(b) \]. \textit{Easy to verify!}
Free modules over path algebra quotients

- \( F = \bigoplus_{i=1}^r v_i A \) free right \( A \)-module, and a right \( \mathcal{P} \)-module via \( \psi \).
- \( \text{Mon}(F) = \{ v_i \cdot a \mid i = 1, \ldots, r; a \in \text{Mon}(A) \} \).
- For \( m = v_i \cdot a, n = v_j \cdot b \in \text{Mon}(F) \): \( m|_c n \iff i = j \) and \( a|_c b \)

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

- Fix compatible monomial orderings on \( \mathcal{P}, A, F \). Choices!
- \( G \subset M \leq F \) is standard basis of \( M \): 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 $F_5$! Useless in fin. dim. algebras!

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

- In a *quotient* $\psi: \mathcal{P} \to A$, $\ker(\psi)$ 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

Let $S = \bigoplus_{i=1}^{m} e_i \mathcal{P}$, with some compatible monomial ordering.

Epimorphism $ev: S \rightarrow M$ of right $\mathcal{P}$-modules with $ev(e_i) = \hat{g}_i \ \forall i$.

$f \in S$ describes $ev(f) \in M$ as an $A$–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 $\eta \in \text{Mon}(S)$, such that $\exists f \in S: ev(f) = u$ and $\text{Lm}(f) = \eta$.

Its unsigned element is $u(p) := u$ and its signature $\sigma(p) := \eta$.

We only allow operations that keep track of signatures

For $p \in_s M$ and $\tau \in \text{Mon}(\mathcal{P})$: $(u(p) \cdot \psi(\tau), \ \sigma(p) \cdot \tau) \in_s M$.

If $p_1, p_2 \in_s M$, $\sigma(p_1) > \sigma(p_2)$: $(u(p_1) + u(p_2), \ \sigma(p_1)) \in_s M$.

Otherwise, the addition won’t be performed in the $F_5$ algorithm.
Signed reduction

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

- $p$ is $\eta$-reducible modulo $G \iff p \neq 0$, and
  1. $\exists g \in G : \text{Lm}(u(g))|_c \text{Lm}(p)$
  2. $\sigma(g) \cdot \lambda(c) < \eta$

- Otherwise, $p$ is $\eta$-irreducible modulo $G$.

- Replace $p$ by $p - \frac{\text{Lc}(p)}{\text{Lc}(u(g))}g \cdot c$ and iterate
  $\leadsto \text{NF}_\eta(p; G)$, which is $\eta$-irreducible modulo $G$. Termination?

- $p$ is weakly $\eta$-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 $u(p)$ is $\sigma(p)$-irreducible modulo any signed $G \subset_s M$.
  I.e., $\sigma(p)$ is optimal, there is no cheaper computation of $u(p)$.

- $\text{NF}(p; G) := (\text{NF}_{\sigma(p)}(u(p); G), \sigma(p)) \in_s M$. Signature is preserved!
Signed standard bases

Def: \( G \subset_{s} M \setminus \{0\} \) is a signed standard basis of \( M \)
\[ \iff \text{Every irreducible } p \in_{s} M \setminus \{0\} \text{ is weakly } \sigma(p)-\text{reducible modulo } G. \]

Lemma
Let \( G \) be a signed standard basis of \( M \).
- \( p \in_{s} M \setminus \{0\} \) not irreducible \( \implies \) \( \text{NF}(p; G) = (0, \sigma(p)). \)
  
  Proof idea: \( p \) has irreducible reductor \( \in_{s} M \).
- \( u(G) = \{ u(g) \mid g \in G \} \) is a standard basis of \( M \).

Def: \( G \subset_{s} M \setminus \{0\} \) is interreduced
\[ \iff \text{Every } g \in G \text{ is not weakly } \sigma(g)-\text{reducible modulo } G \setminus \{g\}. \]
Signed standard bases

Critical pairs and S-polynomials

\[(g, c) \text{ critical pair of type } T \text{ of } G\]

\[g \in G \text{ with } \text{Lm}(u(g)) = v_i \cdot a, \ c \in \text{Mon}(\mathcal{A}) \text{ such that } c \text{ is not a small cofactor of } a, \text{ and if } c'|c \text{ with } \deg(c') < \deg(c) \text{ then } c' \text{ is a small cofactor of } a. \text{ Chain criterion!} \]

\[S(g, c) := (u(g) \cdot c, \ \sigma(g) \cdot \lambda(c)) \in_s M\]

\[(g, g') \text{ critical pair of type } R \text{ of } G\]

\[g \neq g' \in G \text{ with } \text{Lm}(u(g))|_c \text{Lm}(u(g')), \text{ but } \sigma(g) \cdot \lambda(c) > \sigma(g'). \]

\[S(g, g') := \left( u(g') - \frac{\text{Lc}(g')}{\text{Lc}(g)} u(g) \cdot c, \ \sigma(g) \cdot \lambda(c) \right) \in_s M\]

Buchberger style computation of signed standard bases

- Start with \( G = \{(\hat{g}_1, \epsilon_1), \ldots, (\hat{g}_m, \epsilon_m)\} \).
- 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 $L \subset \text{Lm}(\text{ker}(ev))$.

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

$$g \text{ (and } g') \text{ is irreducible modulo } G, \text{ and } \sigma(g) \cdot \lambda(c) \not\in L.$$  

**Def:** $G$ has the $F_5$ property relative to $L$ if

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

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

**Learning from zero-reductions**

If $u(\text{NF}(p; G)) = 0$ then $\sigma(p) \in \text{Lm}(\text{ker}(ev))$. Add its two-sided multiples to $L \rightsquigarrow \text{weaken the } F_5 \text{ property.}$
Theorem: \([F_5 \text{ and rewritten criterion in Faugère’s terminology}]\)

Let \( G \subset_s M \setminus \{0\} \) be finite interreduced, and for all \( i = 1, \ldots, m \), either \( e_i \in \text{Lm}(\ker(ev)) \) (\( \hat{g}_i \) is redundant generator), or \( \exists g \in G \) with \( \sigma(g) = e_i \).

\( G \) signed standard basis of \( M \) \( \iff \) it has the \( F_5 \) property.

**\( F_5 \) algorithm**

- Start with \( G = \{ (\hat{g}_1, e_1), \ldots, (\hat{g}_m, e_m) \} \subset_s M \), and 
  \( L = \bigcup_{i=1}^m e_i \cdot \text{Lm}(\ker(\psi)) \subset \text{Lm}(\ker(ev)) \).
  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 \( \eta \) of S-polynomials occurs at most once

Further crit. pairs for \( \eta \) will not be normal or will not violate \( F_5 \)!
Signed standard bases and Loewy layers

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

- $\mathcal{A}$ finite-dimensional $\Rightarrow F_5$ algorithm terminates, for all $\succ$, since only finitely many signatures are not in $L$.

- Let $\tau_d \in \text{Mon}(S)$ maximal with $\deg(\tau) = d \in \mathbb{N}$.
  \[
  \text{Rad}^d(M) = \{ f \in M : \exists \tilde{f} \in S : Lm(\tilde{f}) \leq \tau_d \text{ and } ev(\tilde{f}) = f \}
  \]
  Uses that $\mathcal{A}$ is a basic algebra!

- Let $G$ be an interreduced signed standard basis of $M$
  The elements $u(g) \cdot c$ with
    1. $g \in G$, $c$ small cofactor of $Lm(u(g))$
    2. $\sigma(g) \cdot \lambda(c) \leq \tau_d$
    3. $u(g) \cdot c$ is $\sigma(g) \cdot \lambda(c)$-irreducible modulo $G$
  form a $K$-vector space basis $B_{\tau_d}(M, G)$ of $\text{Rad}^d(M)$.
  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 with David Green’s “heady standard bases”

- “Heady” only keeps track whether $\deg(\sigma(p)) > 0$.
- “Heady” only computes $L^1(M)$ (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! $\sim \sim F_5$ 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?**
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.