Algorithmic Isomorphism Classification of Modular Cohomology Rings of Finite Groups

Simon King

Joint work with B. Eick, D. Green, G. Ellis

FSU Jena (Univ. at Cologne since today), DFG project KI 861/2–1

Jahrestagung SPP 1489, Osnabrück, October 01, 2015

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Carlson [2005], proved for $p = 2$, conjectured for $p > 2$

For any $c \in \mathbb{N}$, there are only finitely many graded isomorphism types for the modular cohomology rings of finite p-groups of coclass c.

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Carlson [2005], proved for $p = 2$, conjectured for $p > 2$

For any $c \in \mathbb{N}$, there are only finitely many graded isomorphism types for the modular cohomology rings of finite p-groups of coclass c. How many?

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Carlson [2005], proved for $p = 2$, conjectured for $p > 2$

For any $c \in \mathbb{N}$, there are only finitely many graded isomorphism types for the modular cohomology rings of finite p-groups of coclass c. How many?

Conjecture of Eick and Leedham-Green [2008]

In each "coclass family" of finite p-groups, all but finitely many groups have isomorphic modular cohomology rings.

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Carlson [2005], proved for $p = 2$, conjectured for $p > 2$

For any $c \in \mathbb{N}$, there are only finitely many graded isomorphism types for the modular cohomology rings of finite p-groups of coclass c. How many?

Conjecture of Eick and Leedham-Green [2008]

In each "coclass family" of finite p-groups, all but finitely many groups have isomorphic modular cohomology rings. How many exceptions?

Motivation

G finite group, p prime dividing $|G|$. $H^*(G) := H^*(G; \mathbb{F}_p)$

- Arises in topology, number theory, representation theory, ...
- Is a f.p. graded commutative $\mathbb{F}_p$-algebra determined by G.
- Contravariant functor. $U \leq G \rightsquigarrow$ restriction $\mathrm{res}^G_U : H^*(G) \to H^*(U)$.

Carlson [2005], proved for $p = 2$, conjectured for $p > 2$

For any $c \in \mathbb{N}$, there are only finitely many graded isomorphism types for the modular cohomology rings of finite p-groups of coclass c. How many?

Conjecture of Eick and Leedham-Green [2008]

In each "coclass family" of finite p-groups, all but finitely many groups have isomorphic modular cohomology rings. How many exceptions?

Do computer experiments!

- How to compute $H^*(G)$?
- How to test $H^*(G_1) \cong H^*(G_2)$?

Outline

1. Computational results
   - Minimal ring presentations of cohomology rings
   - Working with the cohomology rings
   - Isomorphism classes of cohomology rings
2. Algorithms in Group Cohomology
   - Computing $H^d(G)$
   - A tower of subgroups for Co_3
   - Completeness criteria
3. Finding graded algebra isomorphisms
   - Finitary algebras
   - Partial isomorphism tests
4. A non-commutative F_5 algorithm

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- http://users.minet.uni-jena.de/cohomology/documentation/
- Results: http://users.minet.uni-jena.de/~king/cohomology

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- http://users.minet.uni-jena.de/cohomology/documentation/
- Results: http://users.minet.uni-jena.de/~king/cohomology

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed $\sim$ 8 months comp. time [1997-2001] for order 64.

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- `http://users.minet.uni-jena.de/cohomology/documentation/`
- Results: `http://users.minet.uni-jena.de/~king/cohomology`

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed ~ 8 months comp. time [1997-2001] for order 64.
We need ~ 30 minutes for order 64, about 2 months for order 128.

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- http://users.minet.uni-jena.de/cohomology/documentation/
- Results: http://users.minet.uni-jena.de/~king/cohomology

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed $\sim$ 8 months comp. time [1997-2001] for order 64.
We need $\sim$ 30 minutes for order 64, about 2 months for order 128.

Interesting non prime power groups

We got the modular cohomology for different primes of (among others)

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- http://users.minet.uni-jena.de/cohomology/documentation/
- Results: http://users.minet.uni-jena.de/~king/cohomology

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed $\sim$ 8 months comp. time [1997-2001] for order 64.
We need $\sim$ 30 minutes for order 64, about 2 months for order 128.

Interesting non prime power groups

We got the modular cohomology for different primes of (among others)

- HS, McL, Janko groups (not J_4), Mathieu groups (not M_{24})

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- `http://users.minet.uni-jena.de/cohomology/documentation/`
- Results: `http://users.minet.uni-jena.de/~king/cohomology`

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed $\sim$ 8 months comp. time [1997-2001] for order 64.
We need $\sim$ 30 minutes for order 64, about 2 months for order 128.

Interesting non prime power groups

We got the modular cohomology for different primes of (among others)

- HS, McL, Janko groups (not J_4), Mathieu groups (not M_{24})
- [K, Green, Ellis 2011]: $H^*(Co_3; \mathbb{F}_2)$ is Cohen-Macaulay.

Some cohomology rings that we can compute

Optional package for SageMath (K, Green)

- `http://users.minet.uni-jena.de/cohomology/documentation/`
- Results: `http://users.minet.uni-jena.de/~king/cohomology`

All groups of orders 64 and 128; all but 6 groups of order 243

Carlson needed $\sim$ 8 months comp. time [1997-2001] for order 64.
We need $\sim$ 30 minutes for order 64, about 2 months for order 128.

Interesting non prime power groups

We got the modular cohomology for different primes of (among others)

- HS, McL, Janko groups (not J_4), Mathieu groups (not M_{24})
- [K, Green, Ellis 2011]: $H^*(Co_3; \mathbb{F}_2)$ is Cohen-Macaulay.
- $Sz(8)$: minimal presentation of $H^*(Sz(8); \mathbb{F}_2)$ has 102 generators of maximal degree 29 and 4790 relations of maximal degree 58.

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$
- Massey products

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$
- Massey products
- Via induced homomorphisms:
  - nilradical
  - essential ideals.
    $\mathrm{Syl}_2\left(U_3(4)\right)$, $\mathrm{Syl}_2\left(U_3(4)\right) \times C_2$ are the only known examples for which the essential ideal does not square to zero.

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$
- Massey products
- Via induced homomorphisms:
  - nilradical
  - essential ideals.
    $\mathrm{Syl}_2(U_3(4))$, $\mathrm{Syl}_2(U_3(4)) \times C_2$ are the only known examples for which the essential ideal does not square to zero.

Hambleton [2013]: Is $H^2(G; \mathbb{F}_2)$ detected by metabelian groups?

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$
- Massey products
- Via induced homomorphisms:
  - nilradical
  - essential ideals.
    $\mathrm{Syl}_2(U_3(4))$, $\mathrm{Syl}_2(U_3(4)) \times C_2$ are the only known examples for which the essential ideal does not square to zero.

Hambleton [2013]: Is $H^2(G; \mathbb{F}_2)$ detected by metabelian groups?

- Computational data suggest: $H^*(G; \mathbb{F}_p)$ (any degree, any prime p) is detected by metabelian groups.

Further available data

The SageMath package can also compute...

- Poincaré series, depth, a-invariants, ... of $H^*(G)$
- Massey products
- Via induced homomorphisms:
  - nilradical
  - essential ideals.
    $\mathrm{Syl}_2\left(U_3(4)\right)$, $\mathrm{Syl}_2\left(U_3(4)\right) \times C_2$ are the only known examples for which the essential ideal does not square to zero.

Hambleton [2013]: Is $H^2(G; \mathbb{F}_2)$ detected by metabelian groups?

- Computational data suggest: $H^*(G; \mathbb{F}_p)$ (any degree, any prime p) is detected by metabelian groups.
- Green [2015]: There is a non-metabelian group G of order 3^{16} that is p-centric (hence, has essential classes).

Isomorphism classes, sorted by group order

Eick, K [2015], paper accepted, software not published yet

We provide a complete classification of $H^*(G)$ up to isomorphisms of graded $\mathbb{F}_p$-algebras, for p-groups G, $|G| \leq 81$.

$\|G\|$	#groups	#rings	cum. #groups	cum. #rings
2	1	1	1	1
4	2	2	3	3
8	5	5	8	7
16	14	14	22	18
32	51	48	73	55
64	267	239	340	260
3	1	1	1	1
9	2	2	3	2
27	5	5	8	5
81	15	13	23	14

Work in progress: $|G| \leq 128$.

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

But not general enough,

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

But not general enough, difficult to implement and *to interprete*.

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

But not general enough, difficult to implement and *to interprete*.

Via *approximation* $\tau_n H^*(G)$ of $H^*(G)$ à la [Carlson 2001]

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

But not general enough, difficult to implement and *to interprete*.

Via *approximation* $\tau_n H^*(G)$ of $H^*(G)$ à la [Carlson 2001]

- Compute $H^d(G)$ for $d \leq n$, products out to degree n, and relations.
- $\tau_n H^*(G)$ is presented by generators and relations of $H^*(G)$ of degree at most n.

Computational approaches

Topology

Construct *Classifying spaces*. — Tailor made.

Spectral Sequences

- Lyndon–Hochschild–Serre: extrasp. 2–groups (Quillen (1971])
- Eilenberg–Moore: groups of order 32 (Rusin [1989])

But not general enough, difficult to implement and *to interprete*.

Via *approximation* $\tau_n H^*(G)$ of $H^*(G)$ à la [Carlson 2001]

- Compute $H^d(G)$ for $d \leq n$, products out to degree n, and relations.
- $\tau_n H^*(G)$ is presented by generators and relations of $H^*(G)$ of degree at most n.
- If n is large enough: $H^*(G) \cong \tau_n H^*(G)$.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases* computing a minimal generating set of the kernel in a single step. Used in SageMath.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases* computing a minimal generating set of the kernel in a single step. Used in SageMath.
- K [2014]: Non-commutative F_5 algorithm finds *Loewy layers* in one step and avoids redundant computations. Soon in SageMath.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases* computing a minimal generating set of the kernel in a single step. Used in SageMath.
- K [2014]: Non-commutative F_5 algorithm finds *Loewy layers* in one step and avoids redundant computations. Soon in SageMath.

For G not a prime power group: Stable elements [Cartan–Eilenberg 1956]

- If $Syl_p(G) \ni S \leq U \leq G$, then $\mathrm{res}^G_U : H^*(G) \hookrightarrow H^*(U)$.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases* computing a minimal generating set of the kernel in a single step. Used in SageMath.
- K [2014]: Non-commutative F_5 algorithm finds *Loewy layers* in one step and avoids redundant computations. Soon in SageMath.

For G not a prime power group: Stable elements [Cartan–Eilenberg 1956]

- If $Syl_p(G) \ni S \leq U \leq G$, then $\mathrm{res}^G_U : H^*(G) \hookrightarrow H^*(U)$.
- The sub-algebra is determined by stability conditions, corresponding to double cosets $U \setminus G / U$.

Computing $H^d(G)$

For G a prime power group: Via minimal projective resolutions.

- E. Green, Solberg, Zacharia [2001]: Use non-commutative standard bases to compute kernels, and then minimise the generating set.
- Carlson [1997-2001]: Use linear algebra.
- D. Green [2001]: *Heady standard bases* computing a minimal generating set of the kernel in a single step. Used in SageMath.
- K [2014]: Non-commutative F_5 algorithm finds *Loewy layers* in one step and avoids redundant computations. Soon in SageMath.

For G not a prime power group: Stable elements [Cartan–Eilenberg 1956]

- If $Syl_p(G) \ni S \leq U \leq G$, then $\mathrm{res}^G_U : H^*(G) \hookrightarrow H^*(U)$.
- The sub-algebra is determined by stability conditions, corresponding to double cosets $U \setminus G / U$.
- Holt [1985] suggests to use a tower $S = U_0 \leq U_1 \leq ... \leq U_k = G$

A tower of subgroups for Co_3

Why should one use a subgroup tower?

A tower of subgroups for Co_3

Why should one use a subgroup tower?

- For $G = Co_3$: $|S| = 1024$ and $|S \setminus G/S| = 484\,680$.

A tower of subgroups for Co_3

Why should one use a subgroup tower?

- For $G = Co_3$: $|S| = 1024$ and $|S \setminus G/S| = 484\,680$.
- $S = U_0 \leq U_1 = N_G(\underbrace{Z_2(S)}_{\cong C_4 \times C_2}) \leq U_2 = N_G(C_4) \leq U_3 = N_G(\underbrace{Z(S)}_{\cong C_2}) \leq U_4 = G$

A tower of subgroups for Co_3

Why should one use a subgroup tower?

- For $G = Co_3$: $|S| = 1024$ and $|S \setminus G/S| = 484\,680$.
- $S = U_0 \leq U_1 = N_G(\underbrace{Z_2(S)}_{\cong C_4 \times C_2}) \leq U_2 = N_G(C_4) \leq U_3 = N_G(\underbrace{Z(S)}_{\cong C_2}) \leq U_4 = G$
-

i	1	2	3	4
$\|U_{i-1} \setminus U_i/U_{i-1}\|$	2	3	3	7

Discarding trivial double cosets, only 11 stability conditions remain.

A tower of subgroups for Co_3

Why should one use a subgroup tower?

- For $G = Co_3$: $|S| = 1024$ and $|S \setminus G/S| = 484\,680$.
- $S = U_0 \leq U_1 = N_G(\underbrace{Z_2(S)}_{\cong C_4 \times C_2}) \leq U_2 = N_G(C_4) \leq U_3 = N_G(\underbrace{Z(S)}_{\cong C_2}) \leq U_4 = G$
-

i	1	2	3	4
$\lvert U_{i-1} \setminus U_i/U_{i-1}\rvert$	2	3	3	7

Discarding trivial double cosets, only 11 stability conditions remain.

Theorem [K, Green, Ellis 2011]

- $H^*(Co_3; \mathbb{F}_2)$ is Cohen–Macaulay, presentable in degree 33 with generators up to degree 15.

A tower of subgroups for Co_3

Why should one use a subgroup tower?

- For $G = Co_3$: $|S| = 1024$ and $|S \setminus G/S| = 484\,680$.
- $S = U_0 \leq U_1 = N_G(\underbrace{Z_2(S)}_{\cong C_4 \times C_2}) \leq U_2 = N_G(C_4) \leq U_3 = N_G(\underbrace{Z(S)}_{\cong C_2}) \leq U_4 = G$
-

i	1	2	3	4
$\lvert U_{i-1} \setminus U_i/U_{i-1}\rvert$	2	3	3	7

Discarding trivial double cosets, only 11 stability conditions remain.

Theorem [K, Green, Ellis 2011]

- $H^*(Co_3; \mathbb{F}_2)$ is Cohen–Macaulay, presentable in degree 33 with generators up to degree 15.
- $\mathrm{nilrad}\,(H^*(Co_3; \mathbb{F}_2)) = 0$.
- $H^*(Co_3; \mathbb{F}_2)$ is detected on max. elementary abelian 2–subgroups.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be “large enough” wrt. parameter degrees.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

Green, K [2011] (modified Benson test)

- $|G| = p^n$: Dickson invariants $\rightsquigarrow$ f.r. HSOP $X = \{x_1, \ldots, x_r\}$, maxdeg $\sim p^{\mathrm{rk}_p(G) - \mathrm{rk}(Z(G))}$.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

Green, K [2011] (modified Benson test)

- $|G| = p^n$: Dickson invariants $\rightsquigarrow$ f.r. HSOP $X = \{x_1, \ldots, x_r\}$, maxdeg $\sim p^{\mathrm{rk}_p(G) - \mathrm{rk}(Z(G))}$. Expl: Degrees 8, 4, 6, 7; detects in degree 22.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

Green, K [2011] (modified Benson test)

- $|G| = p^n$: Dickson invariants $\rightsquigarrow$ f.r. HSOP $X = \{x_1, \ldots, x_r\}$, maxdeg $\sim p^{\mathrm{rk}_p(G) - \mathrm{rk}(Z(G))}$. Expl: Degrees 8, 4, 6, 7; detects in degree 22.
- General G: Techniques to get smaller HSOP from given HSOP.

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

Green, K [2011] (modified Benson test)

- $|G| = p^n$: Dickson invariants $\rightsquigarrow$ f.r. HSOP $X = \{x_1, \ldots, x_r\}$, maxdeg $\sim p^{\mathrm{rk}_p(G) - \mathrm{rk}(Z(G))}$. Expl: Degrees 8, 4, 6, 7; detects in degree 22.
- General G: Techniques to get smaller HSOP from given HSOP.
- Find d, m: $\exists$ finite field extension $k/\mathbb{F}_p$: $H^*(G; k)$ has f.r. HSOP $\tilde{X} = \{x_1, \ldots, x_{r-m}, \tilde{x}_1, \ldots, \tilde{x}_m\}$ and $|\tilde{x}_i| = d$

The completeness criteria we are using

- In $\tau_n H^*(G)$, find parameters for $H^*(G)$ on which to perform tests.
- n needs to be "large enough" wrt. parameter degrees.

Benson [2004]

Dickson invariants $\rightsquigarrow$ filter regular HSOP, maxdeg $\sim p^{\mathrm{rk}_p(G)}$.
Expl $\mathrm{Syl}_2(Co_3)$: Degrees 8, 12, 14, 15; detect completeness in degree 46.

Green, K [2011] (modified Benson test)

- $|G| = p^n$: Dickson invariants $\rightsquigarrow$ f.r. HSOP $X = \{x_1, \ldots, x_r\}$, maxdeg $\sim p^{\mathrm{rk}_p(G) - \mathrm{rk}(Z(G))}$. Expl: Degrees 8, 4, 6, 7; detects in degree 22.
- General G: Techniques to get smaller HSOP from given HSOP.
- Find d, m: $\exists$ finite field extension $k/\mathbb{F}_p$: $H^*(G;k)$ has f.r. HSOP $\tilde{X} = \{x_1, \ldots, x_{r-m}, \tilde{x}_1, \ldots, \tilde{x}_m\}$ and $|\tilde{x}_i| = d$

Use X for test, $\tilde{X}$ for bound. Expl: Degrees $8, 4, 2, 2$; detects in degree 14.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X\rangle\rangle$. E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X\rangle\rangle$-module needs to be computed.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

1. Bound for the generator degrees of $H^*(G)$ in terms of the generating degree of $H^*(U)$ as a $\tau_n H^*(G)$-module.

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

1. Bound for the generator degrees of $H^*(G)$ in terms of the generating degree of $H^*(U)$ as a $\tau_n H^*(G)$-module.
   Very useful: Stability conditions only in *lower* degrees. Expl: $Sz(8)$

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

1. Bound for the generator degrees of $H^*(G)$ in terms of the generating degree of $H^*(U)$ as a $\tau_n H^*(G)$-module.
   Very useful: Stability conditions only in *lower* degrees. Expl: $Sz(8)$
2. Completeness criterion in terms of
   - parameter degrees for $H^*(G; k)$, $k/\mathbb{F}_p$,

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X\rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X\rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

1. Bound for the generator degrees of $H^*(G)$ in terms of the generating degree of $H^*(U)$ as a $\tau_n H^*(G)$-module.
   Very useful: Stability conditions only in *lower* degrees. Expl: $Sz(8)$
2. Completeness criterion in terms of
   - parameter degrees for $H^*(G;k)$, $k/\mathbb{F}_p$,
   - $\operatorname{depth}(H^*(U))$,

Symonds [2010]

- Let $X \subset \tau_n H^*(G)$ be so that $H^*(G)$ is finite over $\langle\langle X \rangle\rangle$.
  E.g., X a subset of a generating set $\rightsquigarrow$ rather small degrees.
- Easy to use: Only the generating degree of $\tau_n H^*(G)$ as a $\langle\langle X \rangle\rangle$-module needs to be computed.
- Usually at least as good as the modified Benson test.

K [2013], if $|G|$ is not prime power, $S \leq U \leq G$

1. Bound for the generator degrees of $H^*(G)$ in terms of the generating degree of $H^*(U)$ as a $\tau_n H^*(G)$-module.
   Very useful: Stability conditions only in *lower* degrees. Expl: $Sz(8)$
2. Completeness criterion in terms of
   - parameter degrees for $H^*(G; k)$, $k/\mathbb{F}_p$,
   - $\operatorname{depth}(H^*(U))$,
   - Poincaré series of $\tau_n H^*(G)$.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: “finitary algebras”

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: "finitary algebras"

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: "finitary algebras"

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.
- Also, we can compute in *nilpotent quotients* $R_i^{(>0)} / \left(R_i^{(>0)}\right)^k$.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: “finitary algebras”

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.
- Also, we can compute in *nilpotent quotients* $R_i^{(>0)} / \left(R_i^{(>0)}\right)^k$.
- For cohomology rings, we can even use Gröbner bases.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: "finitary algebras"

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.
- Also, we can compute in *nilpotent quotients* $R_i^{(>0)} / \left(R_i^{(>0)}\right)^k$.
- For cohomology rings, we can even use Gröbner bases.

Assume nilradical, Poincaré series equal. Very naive isomorphism test:

- Let $\{g_1, \ldots, g_n\}$ be a homogeneous generating set for R_1.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: "finitary algebras"

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.
- Also, we can compute in *nilpotent quotients* $R_i^{(>0)} / \left(R_i^{(>0)}\right)^k$.
- For cohomology rings, we can even use Gröbner bases.

Assume nilradical, Poincaré series equal. Very naive isomorphism test:

- Let $\{g_1, \ldots, g_n\}$ be a homogeneous generating set for R_1.
- For any $\{x_1, \ldots, x_n\}$ with $x_i \in R_2^{(|g_i|)}$ $(i = 1, \ldots, n)$, we can test if $\psi(g_i) = x_i$ extends to a graded isomorphism $\psi : R_1 \to R_2$.

Finding graded algebra isomorphisms [Eick, K 2015]

Setting: "finitary algebras"

- Hypothesis: k finite field, R_1, R_2 graded associative unital k-algebras, finitely generated in positive degrees.
- Thus, $R_i^{(d)}$ is a *finite set* for all d.
- Also, we can compute in *nilpotent quotients* $R_i^{(>0)} / \left(R_i^{(>0)}\right)^k$.
- For cohomology rings, we can even use Gröbner bases.

Assume nilradical, Poincaré series equal. Very naive isomorphism test:

- Let $\{g_1, ..., g_n\}$ be a homogeneous generating set for R_1.
- For any $\{x_1, ..., x_n\}$ with $x_i \in R_2^{(|g_i|)}$ ($i = 1, ..., n$), we can test if $\psi(g_i) = x_i$ extends to a graded isomorphism $\psi : R_1 \to R_2$.
- Only *finitely many choices* for $\{x_1, ..., x_n\}$. Hence we can test in finite time whether or not $R_1 \cong R_2$.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, ..., g_n)/\mathcal{Q}$.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\}$) extends to an isomorphism, then...

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \dots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \dots, n\}$) extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I \rangle \subset R_1$, $X_I := \langle x_i | i \in I \rangle \subset R_2$.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If $(g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\})$ extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I \rangle \subset R_1$, $X_I := \langle x_i | i \in I \rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I \rangle \subset \mathcal{F}(g_1, \ldots, g_n)$ yields zero.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\}$) extends to an isomorphism, then…

1. equal Poincaré series of $G_I := \langle g_i | i \in I \rangle \subset R_1$, $X_I := \langle x_i | i \in I \rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I \rangle \subset \mathcal{F}(g_1, \ldots, g_n)$ yields zero.
3. $\mathrm{Ann}(G_I)$ and $\mathrm{Ann}(X_I)$ have the same Poincaré series.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \dots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \dots, n\}$) extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I\rangle \subset R_1$, $X_I := \langle x_i | i \in I\rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I\rangle \subset \mathcal{F}(g_1, \dots, g_n)$ yields zero.
3. $\mathrm{Ann}(G_I)$ and $\mathrm{Ann}(X_I)$ have the same Poincaré series.

Expl: G_1 extraspecial of order 3^{2+1} and exponent 3, $G_2 = \mathrm{Syl}_3(U_3(8))$

For some $g_i \in H^2(G_1)$, (3) shows $H^*(G_1) \ncong H^*(G_2)$ (80 tests).

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If $(g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\})$ extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I\rangle \subset R_1$, $X_I := \langle x_i | i \in I\rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I\rangle \subset \mathcal{F}(g_1, \ldots, g_n)$ yields zero.
3. $\mathrm{Ann}(G_I)$ and $\mathrm{Ann}(X_I)$ have the same Poincaré series.

Expl: G_1 extraspecial of order 3^{2+1} and exponent 3, $G_2 = \mathrm{Syl}_3(U_3(8))$

For some $g_i \in H^2(G_1)$, (3) shows $H^*(G_1) \not\cong H^*(G_2)$ (80 tests).
The naive approach studies $8^2 \cdot 80^4 \cdot 728^2 \cdot 19682 > 10^{19}$ choices.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\}$) extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I \rangle \subset R_1$, $X_I := \langle x_i | i \in I \rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I \rangle \subset \mathcal{F}(g_1, \ldots, g_n)$ yields zero.
3. $\mathrm{Ann}(G_I)$ and $\mathrm{Ann}(X_I)$ have the same Poincaré series.

Expl: G_1 extraspecial of order 3^{2+1} and exponent 3, $G_2 = \mathrm{Syl}_3(U_3(8))$

For some $g_i \in H^2(G_1)$, (3) shows $H^*(G_1) \not\cong H^*(G_2)$ (80 tests).
The naive approach studies $8^2 \cdot 80^4 \cdot 728^2 \cdot 19682 > 10^{19}$ choices.

Expl: $G_1 = \mathrm{SmallGroup}(32, 27)$, $G_2 = \mathrm{SmallGroup}(64, 128)$

Naive approach: $7^3 \cdot 127^3 > 7 \cdot 10^8$ choices of generator images.

Detecting non-extendible partial assignments

Let $R_1 \cong \mathcal{F}(g_1, \ldots, g_n)/\mathcal{Q}$.

If ($g_i \mapsto x_i$ for all $i \in I \subset \{1, \ldots, n\}$) extends to an isomorphism, then...

1. equal Poincaré series of $G_I := \langle g_i | i \in I \rangle \subset R_1$, $X_I := \langle x_i | i \in I \rangle \subset R_2$.
2. substituting x_i for g_i in $\mathcal{Q} \cap \langle g_i | i \in I \rangle \subset \mathcal{F}(g_1, \ldots, g_n)$ yields zero.
3. $\mathrm{Ann}(G_I)$ and $\mathrm{Ann}(X_I)$ have the same Poincaré series.

Expl: G_1 extraspecial of order 3^{2+1} and exponent 3, $G_2 = \mathrm{Syl}_3(U_3(8))$

For some $g_i \in H^2(G_1)$, (3) shows $H^*(G_1) \ncong H^*(G_2)$ (80 tests).
The naive approach studies $8^2 \cdot 80^4 \cdot 728^2 \cdot 19682 > 10^{19}$ choices.

Expl: $G_1 = \mathrm{SmallGroup}(32, 27)$, $G_2 = \mathrm{SmallGroup}(64, 128)$

Naive approach: $7^3 \cdot 127^3 > 7 \cdot 10^8$ choices of generator images.
After applying the partial tests on increasing subsets of generators, only 176 choices remain. In fact, $H^*(G_1) \ncong H^*(G_2)$.

Minimal generating sets for modules over basic algebras

- $\mathcal{P}$ path algebra over field K
- $\psi : \mathcal{P} \twoheadrightarrow \mathcal{A}$; in applications: $\mathcal{A}$ basic algebra.
- $\langle g_1, ..., g_k \rangle = M \subset \mathcal{A}^r$ right $\mathcal{A}$ module.

Minimal generating sets for modules over basic algebras

- $\mathcal{P}$ path algebra over field K
- $\psi : \mathcal{P} \twoheadrightarrow \mathcal{A}$; in applications: $\mathcal{A}$ basic algebra.
- $\langle g_1, \dots, g_k \rangle = M \subset \mathcal{A}^r$ right $\mathcal{A}$ module.
- Monomial ordering on $\mathcal{P} \rightsquigarrow$ "leading monomial" in $\mathcal{P}$, $\mathcal{A}$, M.

Minimal generating sets for modules over basic algebras

- $\mathcal{P}$ path algebra over field K
- $\psi : \mathcal{P} \twoheadrightarrow \mathcal{A}$; in applications: $\mathcal{A}$ basic algebra.
- $\langle g_1, ..., g_k \rangle = M \subset \mathcal{A}^r$ right $\mathcal{A}$ module.
- Monomial ordering on $\mathcal{P} \rightsquigarrow$ "leading monomial" in $\mathcal{P}$, $\mathcal{A}$, M.
- $\mathrm{NF}(f; G) \in \mathcal{A}^r$ for $f \in \mathcal{A}^r$, $G \subset M$ (termination?).

Minimal generating sets for modules over basic algebras

- $\mathcal{P}$ path algebra over field K
- $\psi : \mathcal{P} \twoheadrightarrow \mathcal{A}$; in applications: $\mathcal{A}$ basic algebra.
- $\langle g_1, \ldots, g_k \rangle = M \subset \mathcal{A}^r$ right $\mathcal{A}$ module.
- Monomial ordering on $\mathcal{P} \rightsquigarrow$ “leading monomial” in $\mathcal{P}$, $\mathcal{A}$, M.
- $\mathrm{NF}(f; G) \in \mathcal{A}^r$ for $f \in \mathcal{A}^r$, $G \subset M$ (termination?).

Standard bases and Buchberger algorithm

- $G \subset M$ standard basis $\iff$ all $p \in M$ are reducible mod G.
- Standard bases are generally not minimal generating sets.

Minimal generating sets for modules over basic algebras

- $\mathcal{P}$ path algebra over field K
- $\psi : \mathcal{P} \twoheadrightarrow \mathcal{A}$; in applications: $\mathcal{A}$ basic algebra.
- $\langle g_1, \ldots, g_k \rangle = M \subset \mathcal{A}^r$ right $\mathcal{A}$ module.
- Monomial ordering on $\mathcal{P} \rightsquigarrow$ "leading monomial" in $\mathcal{P}$, $\mathcal{A}$, M.
- $\mathrm{NF}(f; G) \in \mathcal{A}^r$ for $f \in \mathcal{A}^r$, $G \subset M$ (termination?).

Standard bases and Buchberger algorithm

- $G \subset M$ standard basis $\iff$ all $p \in M$ are reducible mod G.
- Standard bases are generally not minimal generating sets.
- Obtain standard basis from arbitrary generating set by repeated addition of S-polynomials, and interreduction.
- S-polynomials reducing to zero are a waste of time.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

Signed standard bases: [K 2014] inspired by Faugère's F_5 [2002]

Evaluation $\mathrm{ev} : \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P} \twoheadrightarrow M$, $\mathrm{ev}(\mathfrak{e}_i) = g_i$

- If $\tilde{f} \in \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P}$ with $\mathrm{ev}(\tilde{f}) = f \in M$: $\mathrm{Lt}(\tilde{f})$ is *an* F_5 *signature* of f.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

Signed standard bases: [K 2014] inspired by Faugère's F_5 [2002]

Evaluation $\mathrm{ev} : \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P} \twoheadrightarrow M$, $\mathrm{ev}(\mathfrak{e}_i) = g_i$

- If $\tilde{f} \in \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P}$ with $\mathrm{ev}(\tilde{f}) = f \in M$: $\mathrm{Lt}(\tilde{f})$ is *an* F_5 *signature* of f.
- Let $\mathrm{NF}_\sigma(f; G)$ be obtained from *signature preserving reductions*.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

Signed standard bases: [K 2014] inspired by Faugère's F_5 [2002]

Evaluation $\mathrm{ev} : \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P} \twoheadrightarrow M$, $\mathrm{ev}(\mathfrak{e}_i) = g_i$

- If $\tilde{f} \in \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P}$ with $\mathrm{ev}(\tilde{f}) = f \in M$: $\mathrm{Lt}(\tilde{f})$ is *an* F_5 *signature* of f.
- Let $\mathrm{NF}_\sigma(f; G)$ be obtained from *signature preserving reductions*.
- Disregard all S-polynomials with a signature in $\mathrm{lead}(\ker(\mathrm{ev}))$.

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to $\mathrm{Rad}(M)$.
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

Signed standard bases: [K 2014] inspired by Faugère's F_5 [2002]

Evaluation $\mathrm{ev} : \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P} \twoheadrightarrow M$, $\mathrm{ev}(\mathfrak{e}_i) = g_i$

- If $\tilde{f} \in \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P}$ with $\mathrm{ev}(\tilde{f}) = f \in M$: $\mathrm{Lt}(\tilde{f})$ is *an* F_5 *signature* of f.
- Let $\mathrm{NF}_\sigma(f; G)$ be obtained from *signature preserving reductions*.
- Disregard all S-polynomials with a signature in lead(ker(ev)).
  - *Quotient relations of* $\mathcal{A}$ yield info on lead(ker(ev)).
  - Any remaining zero reduction yields more info! [Arri, Perry 2011]

"Heady" standard bases [Green 2001]

- By construction, S-polynomials belong to Rad(M).
- $\mathrm{NF}_h(f; G)$: Only consider radicality preserving reductions.
- **Thm:** If a negative degree ordering is used, the non-radical elements of a heady standard basis form a minimal generating set of M.

Signed standard bases: [K 2014] inspired by Faugère's F_5 [2002]

Evaluation $\mathrm{ev} : \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P} \twoheadrightarrow M$, $\mathrm{ev}(\mathfrak{e}_i) = g_i$

- If $\tilde{f} \in \bigoplus_{i=1}^{k} \mathfrak{e}_i \mathcal{P}$ with $\mathrm{ev}(\tilde{f}) = f \in M$: $\mathrm{Lt}(\tilde{f})$ is *an* F_5 *signature* of f.
- Let $\mathrm{NF}_\sigma(f; G)$ be obtained from *signature preserving reductions*.
- Disregard all S-polynomials with a signature in lead(ker(ev)).
  - *Quotient relations of* $\mathcal{A}$ yield info on lead(ker(ev)).
  - Any remaining zero reduction yields more info! [Arri, Perry 2011]
- **Thm:** If a negative degree ordering is used, a *signed standard basis* allow to read off bases for $\mathrm{Rad}^i(M)$.