Computational Group Cohomology

Bangalore, November 2016

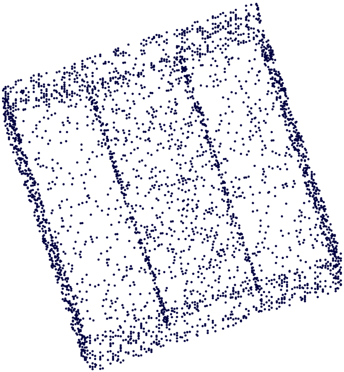
Graham Ellis
NUI Galway, Ireland

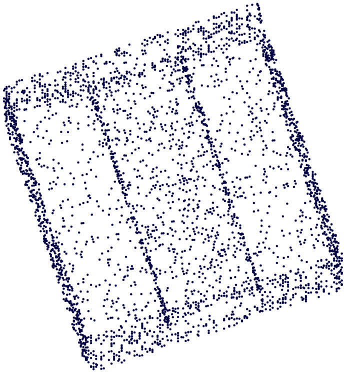
Slides available at **http://hamilton.nuigalway.ie/Bangalore**

Password: **Cork**

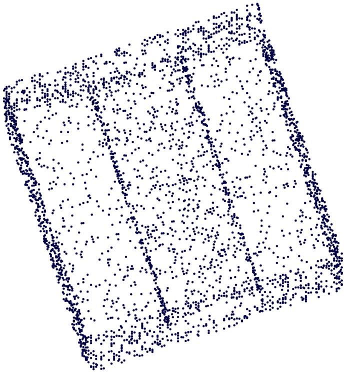
Outline

- Lecture 1: CW spaces and their (co)homology
- Lecture 2: Algorithms for classifying spaces of groups
- Lecture 3: Homotopy 2-types
- **Lecture 4: Steenrod algebra**
- Lecture 5: Curvature and classifying spaces of groups





$$X^0(X,\mathbb{Z}) = \mathbb{Z},\ \ H^1(X,\mathbb{Z}) = \mathbb{Z}\oplus\mathbb{Z},\ \ H^2(X,\mathbb{Z}) = \mathbb{Z},\ \ H^n(X,\mathbb{Z}) = 0, n \geq 3$$



$$X^0(X,\mathbb{Z})=\mathbb{Z},\;\; H^1(X,\mathbb{Z})=\mathbb{Z}\oplus\mathbb{Z},\;\; H^2(X,\mathbb{Z})=\mathbb{Z},\;\; H^n(X,\mathbb{Z})=0, n\geq 3$$

$$X=\mathbb{S}^2\vee\mathbb{S}^1\vee\mathbb{S}^1 \quad \text{or} \quad X=\mathbb{T}\ ?$$

Cup Product

$$\Delta \colon X \to X \times X, x \mapsto (x, x)$$

Cup Product

$$\Delta\colon X \to X \times X, x \mapsto (x, x)$$

$$\Delta_*\colon C_*X \to C_*(X \times X)$$

Cup Product

$$\Delta\colon X \to X \times X, x \mapsto (x, x)$$

$$\Delta_*\colon C_*X \to C_*(X \times X)$$

$$\mathrm{Hom}(C_*X, \mathbb{Z}) \leftarrow \mathrm{Hom}(C_*(X \times X), \mathbb{Z})$$

Cup Product

$$\Delta\colon X \to X \times X, x \mapsto (x, x)$$

$$\Delta_*\colon C_*X \to C_*(X \times X)$$

$$\mathrm{Hom}(C_*X, \mathbb{Z}) \leftarrow \mathrm{Hom}(C_*(X \times X), \mathbb{Z})$$

$$H^{p+q}(X, \mathbb{Z}) \leftarrow H^{p+q}(X \times X, \mathbb{Z})$$

Cup Product

$$\Delta \colon X \to X \times X, x \mapsto (x, x)$$

$$\Delta_* \colon C_* X \to C_*(X \times X)$$

$$\mathrm{Hom}(C_* X, \mathbb{Z}) \leftarrow \mathrm{Hom}(C_*(X \times X), \mathbb{Z})$$

$$H^{p+q}(X, \mathbb{Z}) \leftarrow H^{p+q}(X \times X, \mathbb{Z}) \leftarrow H^p(X, \mathbb{Z}) \times H^q(X, \mathbb{Z})$$

$$x \cup y \leftarrow (x, y)$$

The cohomology ring

$$H^*(X, \mathbb{Z}) = \bigoplus_{n>0} H^n(X, \mathbb{Z})$$

is a **graded commutative** ring:

$$x \cup y = (-1)^{pq} y \cup x$$

for $x \in H^p(X, \mathbb{Z})$, $y \in H^q(X, \mathbb{Z})$.

We'll consider the special case: $X = EG/G$

For $BG = EG/G$ the first n degrees of

$$H^*(BG, \mathbb{Z})$$

are calculated from $n + 1$ terms of a free $\mathbb{Z}G$-resolution with contracting homotopy.

We'll consider the special case: $X = EG/G$

For $BG = EG/G$ the first n degrees of

$$H^*(BG, \mathbb{Z})$$

are calculated from $n+1$ terms of a free $\mathbb{Z}G$-resolution with contracting homotopy.

For a fundamental group $G = \pi_1 X$ of **any** space X there is a ring homomorphism

$$H^*(BG, \mathbb{Z}) \longrightarrow H^*(X, \mathbb{Z})$$

We'll consider the special case: $X = EG/G$ and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$

For $BG = EG/G$ the first n degrees of

$$H^*(BG, \mathbb{F})$$

is calculated from $n+1$ terms of a free $\mathbb{F}G$-resolution with contracting homotopy.

For a fundamental group $G = \pi_1 X$ of **any** space X there is a ring homomorphism

$$H^*(BG, \mathbb{F}) \longrightarrow H^*(X, \mathbb{F})$$

Diagonal map $\Delta\colon C_*(BG) \to C_*(BG \times BG)$

Diagonal map $\Delta\colon C_*(BG) \to C_*(BG \times BG)$

The homomorphism $\phi\colon G \to G \times G, g \mapsto g \times g$ induces a ϕ-equivariant chain map of free resolutions

$$
\begin{array}{ccc}
\downarrow & & \downarrow \\
C_3(EG) & \longrightarrow & C_3(EG \times EG) \\
\downarrow & & \downarrow \\
C_2(EG) & \longrightarrow & C_2(EG \times EG) \\
\downarrow & & \downarrow \\
C_1(EG) & \longrightarrow & C_1(EG \times EG) \\
\downarrow & & \downarrow \\
C_0(EG) & \longrightarrow & C_0(EG \times EG)
\end{array}
$$

Diagonal map $\Delta\colon C_*(BG) \to C_*(BG \times BG)$

The homomorphism $\phi\colon G \to G \times G, g \mapsto g \times g$ induces a ϕ-equivariant chain map of free resolutions

$$
\begin{array}{ccc}
\downarrow & & \downarrow \\
C_3(EG) & \longrightarrow & C_3(EG \times EG) \\
\downarrow & & \downarrow \\
C_2(EG) & \longrightarrow & C_2(EG \times EG) \\
\downarrow & & \downarrow \\
C_1(EG) & \longrightarrow & C_1(EG \times EG) \\
\downarrow & & \downarrow \\
C_0(EG) & \longrightarrow & C_0(EG \times EG)
\end{array}
$$

and $\Delta\colon C_*(EG) \otimes_{\mathbb{Z}G} \mathbb{Z} \to C_*(EG \times EG) \otimes_{\mathbb{Z}G} \mathbb{Z}$

Cartan-Eilenberg double coset formula

For finite G and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$

$$H^*(Syl_p(G), \mathbb{F})$$

is the sub**algebra** of

$$H^*(G, \mathbb{F})$$

consisting of the 'stable elements'.

Poincaré series

For a finite group G and $\mathbb{F} = \mathbb{Z}/p\mathbb{Z}$ define

$$P(t) = \sum_{n \geq 0} a_n t^n$$

with

$$a_n = \dim(H^n(G, \mathbb{F})) \ .$$

Example (E, Green, King)

For the third Conway group Co_3 the cohomology ring

$$H^*(Co_3, \mathbb{F}_2)$$

has Poincaré series

$$P(t) = \frac{f(t)}{(1-t^8)(1-t^{12})(1-t^{14})(1-t^{15})}$$

where $f(t)$ is the monic polynomial of degree 45 with coefficients 1, 1, 1, 1, 2, 3, 3, 4, 4, 6, 7, 8, 9, 10, 10, 11, 13, 12, 14, 15, 13, 13, 15, 14, 12, 13, 11, 10, 10, 9, 8, 7, 6, 4, 4, 3, 3, 2, 1, 1, 1, 1.

Example (E, Green, King)

$$H^*(Co_3, \mathbb{F}_2) \cong \frac{\mathbb{F}_2[x_1, \cdots, x_{16}]}{(r_1 = 0, \cdots, r_{71} = 0)}$$

where $3 \leq \deg(x_i) \leq 13$ and $deg(r_i) \leq 33$.

Example (E, Green, King)

$$H^*(Co_3, \mathbb{F}_2) \cong \frac{\mathbb{F}_2[x_1, \cdots, x_{16}]}{(r_1 = 0, \cdots, r_{71} = 0)}$$

where $3 \leq \deg(x_i) \leq 13$ and $deg(r_i) \leq 33$.

This answers a question of Dave Benson: is this cohomology ring Cohen-Macaulay?

Example (E, Green, King)

$$H^*(Co_3, \mathbb{F}_2) \cong \frac{\mathbb{F}_2[x_1, \cdots, x_{16}]}{(r_1 = 0, \cdots, r_{71} = 0)}$$

where $3 \leq \deg(x_i) \leq 13$ and $deg(r_i) \leq 33$.

This answers a question of Dave Benson: is this cohomology ring Cohen-Macaulay?

Yes: it has Krull dimension 4 and depth 4.

Simpler Example

$$H^*(D_{256}, \mathbb{F}) = \frac{\mathbb{F}[x, y, z]}{(xy = y^2)}$$

where $\deg(x) = \deg(y) = 1, \deg(z) = 2$

Simpler Example

$$H^*(D_{256}, \mathbb{F}) = \frac{\mathbb{F}[x, y, z]}{(xy = y^2)}$$

where $\deg(x) = \deg(y) = 1, \deg(z) = 2$

```
gap> Mod2CohomologyRingPresentation(DihedralGroup(512));
Graded algebra GF(2)[ x_1, x_2, x_3 ] / [ x_1*x_2+x_2^2
 ] with indeterminate degrees [ 1, 1, 2 ]
```

Mod-2 cohomology rings of small 2-groups

Mod-2 cohomology rings of small 2-groups

1. $G \leq 32$: cohomology rings and many (but not all) Steenrod operations computed by Rusin (1989).

Mod-2 cohomology rings of small 2-groups

1. $G \leq 32$: cohomology rings and many (but not all) Steenrod operations computed by Rusin (1989).

2. $G = 64$: cohomology rings computed by Jon Carlson (2003).

Mod-2 cohomology rings of small 2-groups

1. $G \leq 32$: cohomology rings and many (but not all) Steenrod operations computed by Rusin (1989).
2. $G = 64$: cohomology rings computed by Jon Carlson (2003).
3. $G = 32$: more (but not all) Steenrod operations computed by Thanh (2011).

Mod-2 cohomology rings of small 2-groups

1. $G \leq 32$: cohomology rings and many (but not all) Steenrod operations computed by Rusin (1989).

2. $G = 64$: cohomology rings computed by Jon Carlson (2003).

3. $G = 32$: more (but not all) Steenrod operations computed by Thanh (2011).

4. $G = 128$: cohomology rings computed by Green and King (2011).

The computation has two parts

The computation has two parts

1. It was shown by Len Evens and others that $H^*(G, \mathbb{F}_2)$ is a finitely presented algebra. So we can compute a presentation from sufficiently many terms of a free $\mathbb{F}G$-resolution of $\mathbb{F}$.

The computation has two parts

1. It was shown by Len Evens and others that $H^*(G, \mathbb{F}_2)$ is a finitely presented algebra. So we can compute a presentation from sufficiently many terms of a free $\mathbb{F}G$-resolution of $\mathbb{F}$.

2. But we don't have realistic bounds on the number of terms of the resolution that we need.

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*\colon \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0\colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,
- determine a subset $\{v_1, \cdots v_k\} \subset \ker d_n$ whose $\mathbb{F}G$-span equals $\ker d_n$,

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_* : \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,
- determine a subset $\{v_1, \cdots v_k\} \subset \ker d_n$ whose $\mathbb{F}G$-span equals $\ker d_n$,
- set $R_{n+1} = (\mathbb{F}G)^k$,

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,
- determine a subset $\{v_1, \cdots v_k\} \subset \ker d_n$ whose $\mathbb{F}G$-span equals $\ker d_n$,
- set $R_{n+1} = (\mathbb{F}G)^k$,
- define $d_{n+1} \colon (\mathbb{F}G)^k \to R_n$ by sending the ith free generator to v_i.

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*\colon \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0\colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,
- determine a subset $\{v_1, \cdots v_k\} \subset \ker d_n$ whose $\mathbb{F}G$-span equals $\ker d_n$,
- set $R_{n+1} = (\mathbb{F}G)^k$,
- define $d_{n+1}\colon (\mathbb{F}G)^k \to R_n$ by sending the ith free generator to v_i.
- construct $\mathbb{F}$-linear contracting homomorphisms $h\colon R_n \to R_{n+1}$ using linear algebra.

Computing a free $\mathbb{F}G$-resolution for a finite p-group G

$$R_*: \quad \cdots \to R_n \to R_{n-1} \to \cdots \to R_0$$

- set $R_0 = \mathbb{F}G$,
- define $d_0 \colon \mathbb{F}G \to \mathbb{F}, \Sigma\lambda_g g \mapsto \Sigma\lambda_g$,

Then recursively

- determine $\ker d_n$ using gaussian elimination,
- **determine a subset** $\{v_1, \cdots v_k\} \subset \ker d_n$ **whose** $\mathbb{F}G$**-span equals** $\ker d_n$**,**
- set $R_{n+1} = (\mathbb{F}G)^k$,
- define $d_{n+1} \colon (\mathbb{F}G)^k \to R_n$ by sending the ith free generator to v_i.
- construct $\mathbb{F}$-linear contracting homomorphisms $h \colon R_n \to R_{n+1}$ using linear algebra.

Computing generators for an $\mathbb{F}G$-module $M \subseteq \mathbb{F}G$

The **Radical** of M is the submodule

$$\mathrm{Rad}(M) = \{v - g \cdot v \colon v \in M, g \in G\}.$$

Computing generators for an $\mathbb{F}G$-module $M \subseteq \mathbb{F}G$

The **Radical** of M is the submodule

$$\mathrm{Rad}(M) = \{v - g \cdot v \colon v \in M, g \in G\}.$$

$\mathrm{Rad}(M)$ is the $\mathbb{F}$-span of vectors $v - g \cdot v$ where v runs over a basis of M and g runs over a generating set of G.

Computing generators for an $\mathbb{F}G$-module $M \subseteq \mathbb{F}G$

The **Radical** of M is the submodule

$$\mathrm{Rad}(M) = \{v - g \cdot v \colon v \in M, g \in G\}.$$

$\mathrm{Rad}(M)$ is the $\mathbb{F}$-span of vectors $v - g \cdot v$ where v runs over a basis of M and g runs over a generating set of G.

Any basis for the vector space $M/\mathrm{Rad}(M)$ corresponds to a minimal generating set of the module M.

Size of computation determined by:

- order of G.

Size of computation determined by:

- order of G.

- $\text{growth}(G) = \min\{s \in \mathbb{N}\colon \lim_{n\to\infty} \frac{\dim_{\mathbb{F}} H_n(G,\mathbb{F}\}}{n^s} = 0\}$.

Size of computation determined by:

- order of G.

- $\text{growth}(G) = \min\{s \in \mathbb{N} \colon \lim_{n\to\infty} \frac{\dim_{\mathbb{F}} H_n(G,\mathbb{F}\}}{n^s} = 0\}$.

Theorem [Quillen]
$\text{growth}(G) =$ rank of largest elementary abelian subgroup of G.

Size of computation determined by:

- order of G.

- $\text{growth}(G) = \min\{s \in \mathbb{N}\colon \lim_{n\to\infty} \frac{\dim_{\mathbb{F}} H_n(G,\mathbb{F}\}}{n^s} = 0\}$.

Theorem [Quillen]
$\text{growth}(G) =$ rank of largest elementary abelian subgroup of G.

- degrees of ring generators and relations

Complete set of generators and relators for the ring $H^*(G, \mathbb{F})$

are found using Len Evens' proof that $H^*(G, \mathbb{F})$ is finitely presented if G is finite.

Complete set of generators and relators for the ring $H^*(G, \mathbb{F})$

are found using Len Evens' proof that $H^*(G, \mathbb{F})$ is finitely presented if G is finite.

Example $G =$ quaternion group of order 8

Complete set of generators and relators for the ring $H^*(G, \mathbb{F})$

are found using Len Evens' proof that $H^*(G, \mathbb{F})$ is finitely presented if G is finite.

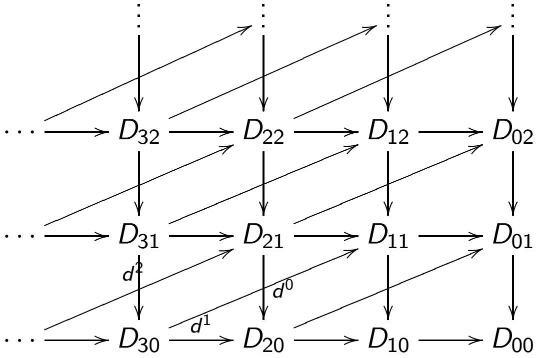
Example $G =$ quaternion group of order 8

$$N \rightarrowtail Q_8 \twoheadrightarrow Q$$

$$N = Z(G) = C_2, \quad Q = C_2 \times C_2$$

Wall's resolution

$$R_n^G = \bigoplus_{p+q=n} D_{pq}, \quad D_{pq} = R_p^N \otimes_{\mathbb{Z}} R_q^G$$



Lyndon-Hochschild-Serre spectral sequence

$$E^0_{pq} = D_{pq} \otimes_{\mathbb{F}G} \mathbb{F}, \quad E^0 = \bigoplus E^0_{pq}$$

$$d^0 \colon E^0 \longrightarrow E^0$$

$$\begin{array}{ccccc}
 & \vdots & \vdots & \vdots & \vdots \\
 & \downarrow & \downarrow & \downarrow & \downarrow \\
\cdots & E^0_{32} & E^0_{22} & E^0_{12} & E^0_{02} \\
 & \downarrow & \downarrow & \downarrow & \downarrow \\
\cdots & E^0_{31} & E^0_{21} & E^0_{11} & E^0_{01} \\
 & \downarrow & \downarrow{\scriptstyle d^0} & \downarrow & \downarrow \\
\cdots & E^0_{30} & E^0_{20} & E^0_{10} & E^0_{00}
\end{array}$$

Lyndon-Hochschild-Serre spectral sequence

$$E^1 = H(E^0)$$

Lyndon-Hochschild-Serre spectral sequence

$$E^1 = H(E^0)$$

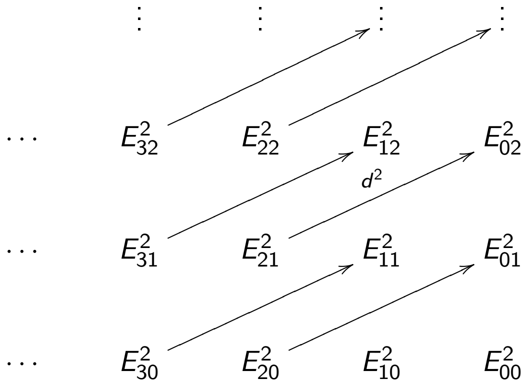
$$d^1\colon E^1 \longrightarrow E^1$$

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \vdots \\
\cdots & & E^1_{32} & \longrightarrow & E^1_{22} & \longrightarrow & E^1_{12} & \longrightarrow & E^1_{02} \\
\cdots & & E^1_{31} & \longrightarrow & E^1_{21} & \xrightarrow{d^1} & E^1_{11} & \longrightarrow & E^1_{01} \\
\cdots & & E^1_{30} & \longrightarrow & E^1_{20} & \longrightarrow & E^1_{10} & \longrightarrow & E^1_{00}
\end{array}$$

Lyndon-Hochschild-Serre spectral sequence

$$E^2 = H(E^1)$$

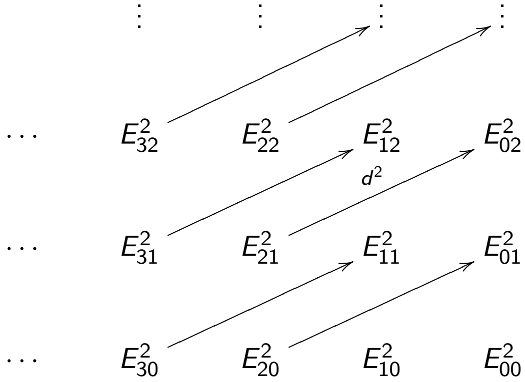
$$d^2 \colon E^2 \longrightarrow E^2$$



Lyndon-Hochschild-Serre spectral sequence

$$E^2 = H(E^1) \;\cong H^*(Q,\mathbb{F}) \otimes H^*(N,\mathbb{F})$$

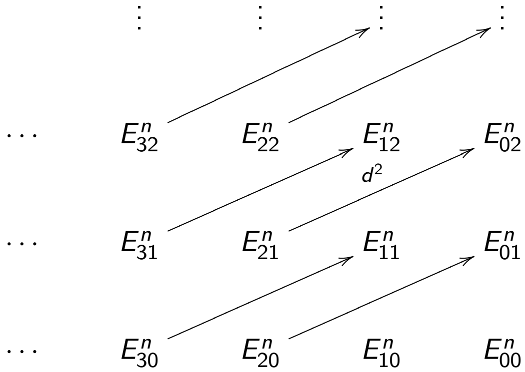
$$d^2\colon E^2 \longrightarrow E^2 \quad \textbf{a derivation}$$



Lyndon-Hochschild-Serre spectral sequence

$$E^n = H(E^{n-1})$$

$$d^n \colon E^n \longrightarrow E^n$$ **a derivation**

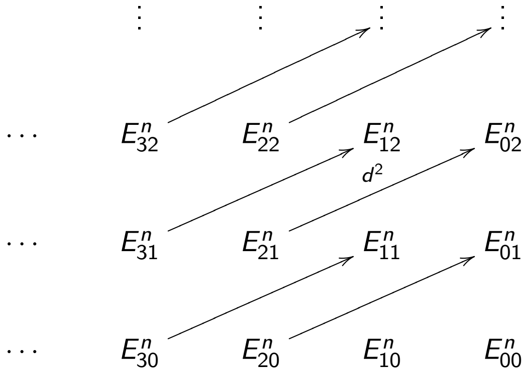


Lyndon-Hochschild-Serre spectral sequence

$$E^n = H(E^{n-1})$$

$$d^n \colon E^n \longrightarrow E^n \quad \textbf{a derivation}$$

Gröbner bases yield $H^{n+1}(E^n)$.

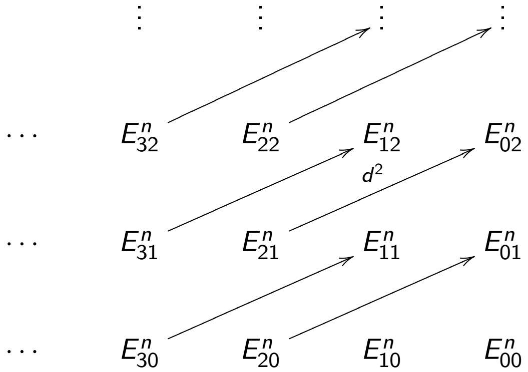


Lyndon-Hochschild-Serre spectral sequence

$$E^n = H(E^{n-1})$$

$$d^n \colon E^n \longrightarrow E^n$$ **a derivation**

Gröbner bases yield $H^{n+1}(E^n)$. At some point $E^n \cong E^{n+1}$; minimal generators/relations for E^n and $H^*(G, \mathbb{F})$ have same degrees



For the quaternion group G

$$E^4 \cong E^\infty$$

has presentation with generators and relators of degree ≤ 4.

For the quaternion group G

$$E^4 \cong E^\infty$$

has presentation with generators and relators of degree ≤ 4.

A presentation for $H^*(G, \mathbb{F})$ can be read from five terms of a free $\mathbb{F}G$-resolution of $\mathbb{F}$.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i\colon H^n(X,\mathbb{F}) \to H^{n+i}(X,\mathbb{F}) \qquad (i \geq 0)$$

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.
4. $Sq^i(x) = 0$ if x is a homogeneous element of degree $< i$.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i : H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.
4. $Sq^i(x) = 0$ if x is a homogeneous element of degree $< i$.
5. $Sq^i(x + y) = Sq^i(x) + Sq^i(y)$.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.
4. $Sq^i(x) = 0$ if x is a homogeneous element of degree $< i$.
5. $Sq^i(x + y) = Sq^i(x) + Sq^i(y)$.
6. $Sq^i(x \cup y) = \sum_{j=0}^{i} Sq^j(x) \cup Sq^{i-j}(y)$.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.
4. $Sq^i(x) = 0$ if x is a homogeneous element of degree $< i$.
5. $Sq^i(x + y) = Sq^i(x) + Sq^i(y)$.
6. $Sq^i(x \cup y) = \sum_{j=0}^{i} Sq^j(x) \cup Sq^{i-j}(y)$.
7. $Sq^i(f^*(x)) = f^*(Sq^i(x))$ for the cohomology homomorphism f^* induced by any map $f \colon X \to X'$.

Steenrod operations ($\mathbb{F} = \mathbb{Z}/2\mathbb{Z}$)

$$Sq^i \colon H^n(X, \mathbb{F}) \to H^{n+i}(X, \mathbb{F}) \qquad (i \geq 0)$$

1. Sq^0 is the identity homomorphism.
2. $Sq^1 = \beta$ is equal to the Bockstein homomorphism.
3. $Sq^i(x) = x \cup x$ if x is a homogeneous element of degree i.
4. $Sq^i(x) = 0$ if x is a homogeneous element of degree $< i$.
5. $Sq^i(x + y) = Sq^i(x) + Sq^i(y)$.
6. $Sq^i(x \cup y) = \sum_{j=0}^{i} Sq^j(x) \cup Sq^{i-j}(y)$.
7. $Sq^i(f^*(x)) = f^*(Sq^i(x))$ for the cohomology homomorphism f^* induced by any map $f \colon X \to X'$.
8. $$Sq^a Sq^b = \sum_{c=0}^{[a/2]} \binom{b-c-1}{a-2c} Sq^{a+b-c} Sq^c$$

Example: $X = BG$ with $G = D_{32}$

```
gap> CohomologicalData(DihedralGroup(64),9);

Group order: 64
Group number: 52
Group description: D64

Cohomology generators
Degree 1: a, b
Degree 2: c

Cohomology relations
1: a*b+b^2

Poincare series
(1)/(x^2-2*x+1)

Steenrod squares
Sq^1(c)=c*a
```

Ingredients of the construction

$C_2 = \langle z | z^2 = 1 \rangle$

Ingredients of the construction

$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G \times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G$

Ingredients of the construction

$$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G\times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G \qquad R_*^{C_2\times G} = R_*^{C_2} \otimes_{\mathbb{Z}} R_*^G$$

Ingredients of the construction

$$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G\times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G \qquad R_*^{C_2\times G} = R_*^{C_2} \otimes_{\mathbb{Z}} R_*^G$$

$C_2 \times G$ acts on $R_*^{G\times G}$ by

$$(z, g) \cdot (g' e_i^p \otimes g'' e_j^q) = (-1)^{pq} g g'' e_j^q \otimes g g' e_i^p$$

Ingredients of the construction

$$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G\times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G \qquad R_*^{C_2\times G} = R_*^{C_2} \otimes_{\mathbb{Z}} R_*^G$$

$C_2 \times G$ acts on $R_*^{G\times G}$ by

$$(z,g)\cdot(g' e_i^p \otimes g'' e_j^q) = (-1)^{pq} gg'' e_j^q \otimes gg' e_i^p$$

$$\phi_*\colon R_*^{C_2\times G} \to R_*^{G\times G}, f^0 \otimes e_j^0 \mapsto e_j^0 \otimes e_j^0$$

Ingredients of the construction

$$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G\times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G \qquad R_*^{C_2\times G} = R_*^{C_2} \otimes_{\mathbb{Z}} R_*^G$$

$C_2 \times G$ acts on $R_*^{G\times G}$ by

$$(z,g)\cdot(g' e_i^p \otimes g'' e_j^q) = (-1)^{pq} g g'' e_j^q \otimes g g' e_i^p$$

$$\phi_* \colon R_*^{C_2\times G} \to R_*^{G\times G}, f^0 \otimes e_j^0 \mapsto e_j^0 \otimes e_j^0$$

$$R_p^G \longrightarrow Hom_{\mathbb{Z}G}(R_p^G, \mathbb{Z}), u \mapsto \overline{u}$$

Ingredients of the construction

$$C_2 = \langle z | z^2 = 1 \rangle \qquad R_*^{G\times G} = R_*^G \otimes_{\mathbb{Z}} R_*^G \qquad R_*^{C_2\times G} = R_*^{C_2} \otimes_{\mathbb{Z}} R_*^G$$

$C_2 \times G$ acts on $R_*^{G\times G}$ by

$$(z,g)\cdot(g' e_i^p \otimes g'' e_j^q) = (-1)^{pq} gg'' e_j^q \otimes gg' e_i^p$$

$$\phi_*\colon R_*^{C_2\times G} \to R_*^{G\times G}, f^0 \otimes e_j^0 \mapsto e_j^0 \otimes e_j^0$$

$$R_p^G \longrightarrow Hom_{\mathbb{Z}G}(R_p^G, \mathbb{Z}), u \mapsto \overline{u}$$

$$Hom_{\mathbb{Z}G}(R_p^G,\mathbb{Z}) \otimes Hom_{\mathbb{Z}G}(R_q^G,\mathbb{Z}) \longrightarrow Hom_{\mathbb{Z}G}(R_{p+q}^G,\mathbb{Z}), \overline{u}\otimes\overline{v} \mapsto \overline{u}\cup_i\overline{v}$$

$$\overline{u} \cup_i \overline{v}\,(c) = \overline{u\otimes v}\,\phi_{p+q}(f^i \otimes c)$$

Theorem

The operation

$$Hom_{\mathbb{Z}G}(R_n^G) \to Hom_{\mathbb{Z}G}(R_{2n-1}^G), \overline{u} \mapsto \overline{u} \cup_i \overline{u}$$

induces a homomorphism

$$Sq_i \colon H^n(G, \mathbb{Z}_2) \to H^{2n-i}(G, \mathbb{Z}_2).$$

The homomorphism

$$Sq^i = Sq_{n-i} \colon H^n(G, \mathbb{Z}_2) \to H^{n+i}(G, \mathbb{Z}_2)$$

is independent of the choices in ϕ_* and satisfies the required properties.