Let $A$ be the mod 2 Steenrod algebra. The elements $Sq^{2^i}$, $i \geq 0$, form a minimal set of generators for $A$.

**Theorem (Wall)**

*A minimal set of relations for $A$ consists of two families:*

\[(Sq^{2^i})^2 = \ldots \text{ for } i \geq 0,\]

\[[Sq^{2^i}, Sq^{2^{i+j}}] = \ldots \text{ for } j \geq 2.\]

Want to find a “standard” form for elements of $A$: try sums of products $Sq^{2^{i_1}} Sq^{2^{i_2}} \ldots Sq^{2^{i_n}}$ with $i_1 < i_2 < \cdots < i_n$.

A problem with this:

- no way to rewrite $Sq^{2^{i+1}} Sq^{2^i}$: see the $j \geq 2$ restriction in Wall’s theorem.

This is the only problem, though, and you can fix it.
Define elements $s_?^i$ as follows:

- $s_{2i} = \text{Sq}^{2i}$,
- $s_{2i,2i+1} = [\text{Sq}^{2i}, \text{Sq}^{2i+1}]$,
- $s_{2i,...,2i+j} = [s_{2i,...,2i+j-1}, \text{Sq}^{2i+j}]$.

**Example**

- $s_{12} = [\text{Sq}^{1}, \text{Sq}^{2}] = \text{Sq}^{3} + \text{Sq}^{2} \text{Sq}^{1} = \text{Sq}(0, 1)$
- $s_{24} = [\text{Sq}^{2}, \text{Sq}^{4}] = \text{Sq}^{4} \text{Sq}^{2} + \text{Sq}^{5} \text{Sq}^{1} + \text{Sq}^{6} = \text{Sq}(0, 2)$
- $s_{48} = [\text{Sq}^{4}, \text{Sq}^{8}] = \text{Sq}^{8} \text{Sq}^{4} + \text{Sq}^{10} \text{Sq}^{2} + \text{Sq}^{11} \text{Sq}^{1} + \text{Sq}^{12} = \text{Sq}(0, 4) + \text{Sq}(3, 3)$
- $s_{124} = [s_{12}, \text{Sq}^{4}] = \text{Sq}^{4} \text{Sq}^{2} \text{Sq}^{1} + \text{Sq}^{5} \text{Sq}^{2} + \text{Sq}^{6} \text{Sq}^{1} + \text{Sq}^{7} = \text{Sq}(0, 0, 1)$

Call these elements *iterated commutators*. 
Now we can achieve our standard form, using computations like this:

$$\text{Sq}^{2i+1} \text{Sq}^{2i} = \text{Sq}^{2i} \text{Sq}^{2i+1} + [\text{Sq}^{2i}, \text{Sq}^{2i+1}].$$

That is, we can use iterated commutators to rewrite elements of $A$ in a standard form, for example like this:

$$\text{Sq}^2 \text{Sq}^1 \text{Sq}^8 = s_2 s_1 s_8 = s_1 s_2 s_8 + s_{12} s_8.$$
Theorem

Choose a linear ordering on the set \( \{ s_{2i},...,2i+j : i \geq 0, j \geq 0 \} \) of iterated commutators. Then the set of products

\[ s_{2i_1},...,2i_1+j_1 \cdots s_{2i_n},...,2i_n+j_n, \]

where \( s_{2i_1},...,2i_1+j_1 < \cdots < s_{2i_n},...,2i_n+j_n \), forms a basis for A.

These bases are called **commutator bases**.
Example

For example, the sets of commutators whose products lie in dimension 7 are \( \{s_1, s_2, s_4\} \), \( \{s_1, s_{24}\} \), \( \{s_{12}, s_4\} \), and \( \{s_{124}\} \). To form a commutator basis in this dimension, we choose an ordering on the set \( \{s_1, s_2, s_4, s_{12}, s_{24}, s_{124}\} \), and then multiply distinct elements in increasing order. Here are two different commutator bases:

\[
(s_1 s_2 s_4, s_1 s_{24}, s_{12} s_4, s_{124}),
\]
\[
(s_1 s_4 s_2, s_1 s_{24}, s_4 s_{12}, s_{124}).
\]

All together, there are 24 different commutator bases in this dimension, one for each of the possible permutations of the factors from the above sets of factors. Some iterated commutators commute with each other, so e.g., in dimension 6 the factors \( \{s_1, s_2, s_{12}\} \) combine to give only two different products, \( s_1 s_2 s_{12} \) and \( s_2 s_1 s_{12} \).
The commutator bases restrict to give bases for the sub-Hopf algebras $A(n)$.

Example

To obtain a basis for $A(2)$, first order the iterated commutators in $A(2)$, e.g.:

$$\{s_1, s_2, s_4, s_{12}, s_{24}, s_{124}\}.$$ 

Then take products of iterated commutators, in increasing order; this will yield the 64 basis elements. E.g., in dimension 10:

$$(s_1 s_2 s_{124}, s_{12} s_{124}, s_4 s_{24}, s_1 s_{12} s_{24}, s_1 s_2 s_4 s_{12})$$

They don’t restrict well to arbitrary sub-Hopf algebras of $A$: there is a sub-Hopf algebra $B$ with dim $B = 4$ but which contains only 3 commutator basis elements.
Sketch of proof.
Filter $A$ by powers of the augmentation ideal (the May filtration). The associated graded algebra $\text{gr} A$ is a restricted enveloping algebra on the restricted Lie algebra generated by certain classes $\overline{P_s^t}$, $s \geq 0$ and $t \geq 1$, with trivial restriction. (Here $\overline{P_t^s}$ is the image in $\text{gr} A$ of an element $P_t^s$ in $A$.)

The Poincaré-Birkhoff-Witt theorem says if you choose an ordering on the $\overline{P_t^s}$’s and then form all monomials

$$\overline{P_t^{s_1}} \cdots \overline{P_t^{s_n}}$$

where $\overline{P_t^{s_1}} < \cdots < \overline{P_t^{s_n}}$, you get a basis for $\text{gr} A$. 
To prove our theorem, then:

- show that $s_{2^i,\ldots,2^i+j}$ is congruent to $P_{j+1}^i$ modulo the May filtration (a straightforward computation)

**Example**

- $s_{2^i} = Sq(2^i) = P_1^i$
- $s_{1,2} = Sq(0,1) = P_2^0$
- $s_{1,2,\ldots,2^i} = Sq(0,\ldots,0,1) = P_{j+1}^0$
- $s_{2,4} = Sq(0,2) = P_2^1$
- $s_{4,8} = Sq(0,4) + Sq(3,3) = P_2^2 + Sq(3,3)$

- observe that any basis for $\text{gr } A$ lifts to one for $A$.

(One also obtains Monks’ $P_i^s$-bases from this.)
Application: computations in \( A(2) \)
The iterated commutators in \( A(2) \):

\[
\{ s_1, s_{12}, s_2, s_4, s_{24}, s_{124} \}.
\]

There are 21 relations among them:

- the restriction: \( s_1^2 = 0, s_{12}^2 = 0, s_{24}^2 = 0, s_{124}^2 = 0, s_2^2 = s_1 s_{12}, \) and \( s_4^2 = s_2 s_{24} \)
- “defining” relations: \( s_{12} = [s_1, s_2], s_{24} = [s_2, s_4], \) and \( s_{124} = [s_{12}, s_4] \)
- other nonzero commutators:

\[
[s_1, s_4] = s_{12} s_2, \quad [s_1, s_{24}] = s_{124},
\]
\[
[s_2, s_{24}] = s_1 s_{124}, \quad [s_4, s_{24}] = s_1 s_2 s_{124} + s_{12} s_{124}.
\]

- all other commutators are zero.
Application, continued

Summary of commutators and relations:

\[ \{s_1, s_{12}, s_2, s_4, s_{24}, s_{124}\} \]

\[ s_2^2 = s_1 s_{12}, \quad s_4^2 = s_2 s_{24}, \]

\[ [s_1, s_4] = s_{12} s_2, \quad [s_1, s_{24}] = s_{124}, \]

\[ [s_2, s_{24}] = s_1 s_{124}, \quad [s_4, s_{24}] = s_1 s_2 s_{124} + s_{12} s_{124}. \]

**Example**

\[ (s_2 s_{24})(s_1) = s_2 s_{124} + s_2 s_1 s_{24} \quad \text{(using \([s_1, s_{24}]\))} \]

\[ = s_2 s_{124} + s_1 s_2 s_{24} + s_{12} s_{24} \quad \text{(using \([s_1, s_2]\))} \]

(Things get more complicated with \(A(3):\) there are 55 relations instead of 21.)
The odd prime case.
Fix an odd prime $p$ and let $A$ be the mod $p$ Steenrod algebra. Define elements $s_{p^i,...,p^{i+j}}$ of $A$ as above, replacing $Sq^{2^n}$ with $\mathcal{P} p^n$. More precisely,

- $s_{p^i} = \mathcal{P} p^i$ and
- $s_{p^i,...,p^{i+j}} = [\mathcal{P} p^{i+j}, s_{p^i,...,p^{i+j-1}}].$

**Theorem**

Choose a linear ordering on the set of iterated commutators. Then the set of products

$$Q_{i_1} \cdots Q_{i_m} s_{p_{i_1},...,p_{i_1+j_1}}^{e_1} \cdots s_{p_{i_n},...,p_{i_n+j_n}}^{e_n},$$

where $i_1 < \cdots < i_m$, $s_{p_{i_1},...,p_{i_1+j_1}} < \cdots < s_{p_{i_n},...,p_{i_n+j_n}}$, and $1 \leq e_k \leq p - 1$ for each $k$, forms a basis for $A$.

The proof is the same as when $p = 2$. 