1

Steenrod squares and the hit problem

1.0 Introduction

In this chapter we introduce our main subject, the algebra of polynomials in n variables over the field of two elements $\mathbb{F}_2$ under the left action of linear operations called **Steenrod squares** and the right action of $n \times n$ matrices. We denote this polynomial algebra by $\mathsf{P}(n) = \mathbb{F}_2[x_1, \ldots, x_n]$, in variables x_i for $1 \leq i \leq n$. For small n it is convenient to use x, y, z for variables. The algebra $\mathsf{P}(n)$ is graded by the vector spaces $\mathsf{P}^d(n)$ of homogeneous polynomials of degree $d \geq 0$. In particular, the variables x_i have degree 1, and form a basis of the n-dimensional vector space $\mathsf{P}^1(n)$.

In Section 1.1 the Steenrod squaring operations $Sq^k : \mathsf{P}^d(n) \to \mathsf{P}^{d+k}(n)$ are defined for $k \geq 0$, and their basic properties, such as the **Cartan formula**, are established. In Section 1.2 we explain how $\mathsf{P}^d(n)$ is a right module over the monoid algebra $\mathbb{F}_2\mathsf{M}(n)$, where $\mathsf{M}(n) = \mathsf{M}(n, \mathbb{F}_2)$ is the multiplicative monoid of $n \times n$ matrices over $\mathbb{F}_2$. This right action commutes with the left action of the Steenrod squares. By restricting to non-singular matrices, $\mathsf{P}^d(n)$ gives a modular representation of the general linear group $\mathsf{GL}(n) \subset \mathsf{M}(n)$, and the Steenrod squares are maps of $\mathbb{F}_2\mathsf{GL}(n)$-modules. Further properties of the Steenrod squares are developed in Section 1.3.

In Section 1.4 we introduce the **hit problem**. We call a polynomial 'hit' if it is a linear combination of elements in the images of positive Steenrod squares. The hit polynomials form a $\mathbb{F}_2\mathsf{M}(n)$-submodule $\mathsf{H}(n)$ of $\mathsf{P}(n)$. The corresponding quotient $\mathsf{Q}(n) = \mathsf{P}(n)/\mathsf{H}(n)$ is the **cohit module**, and the hit problem is to determine $\mathsf{Q}^d(n)$ for each n and degree d. Although this problem arose in algebraic topology, we treat it simply as a problem in algebra. We shall see later that the cohit modules are also of interest in group representation theory.

In the 1-variable case, the hit problem is a straightforward exercise in handling binomial coefficients mod 2. We give the solution in Section 1.4. For

all n, certain monomials called **spikes** cannot appear in the image of a positive Steenrod square. We introduce these in Section 1.5. In the rest of the chapter we focus on the 2-variable case. In Sections 1.6 and 1.7, we introduce the **Kameko** and **duplication** maps, which connect the cohit modules $\mathsf{Q}^d(2)$ in different degrees d. Section 1.8 completes the solution of the hit problem for $\mathsf{P}(2)$.

1.1 The total square Sq

Most of our calculations will be carried out with polynomials whose coefficients are in the field of two elements $\mathbb{F}_2 = \{0,1\}$. Such a polynomial can be written as a sum without repetitions of monomials called its **terms**. That is to say, we do not write down monomials with coefficient 0, except in the case of the zero polynomial 0, which has no terms, and we do not write the coefficient 1. The joy in working with these polynomials is that there are no explicit coefficients or signs to worry about. Further, since we are working mod 2, $(x+y)^2 = x^2 + y^2$.

Definition 1.1.1 For $n \geq 1$, $\mathsf{P}(n) = \mathbb{F}_2[x_1, \ldots, x_n]$ is the polynomial algebra in n variables $x_1, \ldots, x_n$ over the field $\mathbb{F}_2$. For $n = 0$, $\mathsf{P}(0) = \mathbb{F}_2$.

As an algebra over $\mathbb{F}_2$, $\mathsf{P}(n)$ is graded by integers $d \geq 0$. That is, $\mathsf{P}(n)$ is the direct sum $\sum_{d\geq 0} \mathsf{P}^d(n)$, where $\mathsf{P}^d(n)$ is the vector space of homogeneous polynomials of degree d. We identify $\mathsf{P}^0(n)$ with $\mathbb{F}_2$ for all $n \geq 0$. The monomials $x_1^{d_1} \cdots x_n^{d_n}$ such that $d_1 + \cdots + d_n = d$ and $d_i \geq 0$ for $1 \leq i \leq n$ form a basis for $\mathsf{P}^d(n)$ as a vector space over $\mathbb{F}_2$. As usual, $x_i^0 = 1$ and $x_i^1 = x_i$. By considering a monomial as a string of symbols and separators (e.g. $xxx \cdot x \cdot xx$ for x^3yz^2), we see that the dimension of $\mathsf{P}^d(n)$ is

$$\dim \mathsf{P}^d(n) = \binom{d+n-1}{n-1}. \tag{1.1}$$

Since $\mathsf{P}(n)$ is freely generated as a commutative algebra by the variables x_i, an algebra map $\phi : \mathsf{P}(n) \to \mathsf{P}(n)$ is defined uniquely by assigning a value $\phi(x_i)$ to each variable x_i, $1 \leq i \leq n$. We shall always assume that $\phi(1) = 1$. We use a particular map of this kind to define the Steenrod squaring operations on $\mathsf{P}(n)$.

Definition 1.1.2 The **total Steenrod square** $\mathsf{Sq} : \mathsf{P}(n) \to \mathsf{P}(n)$ is the algebra map defined by

$$\mathsf{Sq}(1) = 1, \quad \mathsf{Sq}(x_i) = x_i + x_i^2, \ 1 \leq i \leq n.$$

The **Steenrod squares** $Sq^k : \mathsf{P}^d(n) \to \mathsf{P}^{d+k}(n)$ are the linear maps defined for $k,d \geq 0$ by restricting Sq to $\mathsf{P}^d(n)$ and projecting on to $\mathsf{P}^{d+k}(n)$. Thus $\mathsf{Sq} = \sum_{k\geq 0} Sq^k$ is the formal sum of its graded parts.

Proposition 1.1.3 *For all $x \in \mathsf{P}^1(n)$, $\mathsf{Sq}(x) = x + x^2$. Thus $Sq^0(x) = x$, $Sq^1(x) = x^2$ and $Sq^k(x) = 0$ for all $k > 1$.*

Proof Let $x = \sum_{i=1}^n a_i x_i$, where $a_i \in \mathbb{F}_2$. Then $\mathsf{Sq}(x) = \sum_{i=1}^n a_i \mathsf{Sq}(x_i) = \sum_{i=1}^n a_i(x_i + x_i^2) = \sum_{i=1}^n a_i x_i + \sum_{i=1}^n (a_i x_i)^2 = x + x^2$. The second statement follows by equating graded parts. □

The most important rule for calculating with Steenrod squares is as follows.

Proposition 1.1.4 (Cartan formula) *For polynomials $f, g \in \mathsf{P}(n)$ and $k \geq 0$,*

$$Sq^k(fg) = \sum_{i+j=k} Sq^i(f) Sq^j(g).$$

Proof This follows from the multiplicative property $\mathsf{Sq}(fg) = \mathsf{Sq}(f)\mathsf{Sq}(g)$ by equating terms of degree k. □

Proposition 1.1.5 *Sq^0 is the identity map of $\mathsf{P}(n)$.*

Proof Setting $k = 0$ in Proposition 1.1.4, Sq^0 is an algebra map of $\mathsf{P}(n)$. Since $Sq^0(1) = 1$ and $Sq^0(x_i) = x_i$ for $1 \leq i \leq n$, $Sq^0(f) = f$ for all $f \in \mathsf{P}(n)$. □

Definition 1.1.6 A **Steenrod operation** is a linear map $\theta : \mathsf{P}(n) \to \mathsf{P}(n)$ which can be obtained from the operations Sq^k by addition and composition. Thus θ is a finite sum of operations of the form $Sq^{k_1} Sq^{k_2} \cdots Sq^{k_s}$.

In principle, any Steenrod operation can be evaluated on a polynomial by means of Propositions 1.1.3 and 1.1.4.

Example 1.1.7 In $\mathsf{P}(2) = \mathbb{F}_2[x,y]$ we have

$$Sq^1(xy) = Sq^1(x)Sq^0(y) + Sq^0(x)Sq^1(y) = x^2 y + xy^2.$$

The next two results show how to evaluate a Steenrod square on a monomial. All binomial coefficients which appear in formulae such as the following are understood to be reduced mod 2.

Proposition 1.1.8 *For all $x \in \mathsf{P}^1(n)$,*

$$Sq^k(x^d) = \binom{d}{k} x^{d+k}.$$

In particular, $Sq^1(x^d) = x^{d+1}$ if d is odd and $Sq^1(x^d) = 0$ if d is even.

Proof By the multiplicative property of Sq, we have

$$\mathsf{Sq}(x^d) = (\mathsf{Sq}(x))^d = (x+x^2)^d = x^d(1+x)^d = \sum_{k=0}^{d} \binom{d}{k} x^{d+k}.$$

The result follows by equating terms of degree $d+k$. □

Proposition 1.1.9 *Let $f = x_1^{d_1} \cdots x_n^{d_n}$ be a monomial in $\mathsf{P}(n)$. Then*

$$Sq^k(f) = \sum_{k_1+\cdots+k_n=k} Sq^{k_1}(x_1^{d_1}) \cdots Sq^{k_n}(x_n^{d_n}).$$

Proof This follows by induction on n using the Cartan formula 1.1.4. □

The next result explains why Sq^k is called a squaring operation.

Proposition 1.1.10 *For $f \in \mathsf{P}^d(n)$, $Sq^k(f) = 0$ for $k > d$ and $Sq^d(f) = f^2$.*

Proof Since Sq^k is linear and $(f+g)^2 = f^2 + g^2$, we may assume that f is a monomial of degree d. We use induction on d. The base case $d = 0$ holds since $\mathsf{Sq}(1) = 1$. For $d > 0$, let $f = xg$, where x is one of the variables x_i and g is a monomial of degree $d-1$. By the Cartan formula, $Sq^k(f) = xSq^k(g) + x^2Sq^{k-1}(g)$ for $k > 0$. If $k > d$, then $Sq^k(g) = 0$ and $Sq^{k-1}(g) = 0$ by the inductive hypothesis, so $Sq^k(f) = 0$. If $k = d$, then $Sq^k(g) = 0$ and $Sq^{k-1}(g) = g^2$ by the inductive hypothesis, so $Sq^k(f) = x^2g^2 = f^2$. This completes the induction. □

Proposition 1.1.11 *If $f \in \mathsf{P}(n)$ is a monomial and $k \geq 0$, then every term of $Sq^k(f)$ involves exactly the same variables as f does.*

Proof The monomial $f = x_1^{d_1} \cdots x_n^{d_n}$ involves x_i if and only if $d_i > 0$. If $d_i > 0$, then $k + d_i > 0$ for all k. If $d_i = 0$, then $\mathsf{Sq}(x_i^{d_i}) = \mathsf{Sq}(1) = 1$. The result follows from Proposition 1.1.9. □

1.2 The action of matrices on $\mathsf{P}(n)$

As well as algebra operations in $\mathsf{P}(n)$, we can substitute polynomials for the variables x_i in a polynomial $f \in \mathsf{P}(n)$. In this section, we show that the Steenrod operations on $\mathsf{P}(n)$ commute with linear substitutions of the variables. For $n \geq 1$, we write $\mathsf{GL}(n) = GL(n, \mathbb{F}_2)$ for the general linear group of non-singular $n \times n$ matrices over $\mathbb{F}_2$, and $\mathbb{F}_2\mathsf{GL}(n)$ for its group algebra over $\mathbb{F}_2$. We also write $\mathsf{M}(n) = M(n, \mathbb{F}_2)$ for the multiplicative monoid of all $n \times n$ matrices over $\mathbb{F}_2$, and $\mathbb{F}_2\mathsf{M}(n)$ for its monoid algebra.

Definition 1.2.1 For $A = (a_{i,j}) \in \mathsf{M}(n)$ and $1 \leq i \leq n$, let

$$x_i \cdot A = \sum_{j=1}^{n} a_{i,j} x_j,$$

and extend this action of A to all polynomials $f \in \mathsf{P}(n)$ by substitution, so that $f \cdot A$ is the polynomial $f(x_1 \cdot A, \ldots, x_n \cdot A)$. If $f \in \mathsf{P}^0(n)$ is constant, then $f \cdot A = f$.

Proposition 1.2.2 *For $d \geq 0$, $\mathsf{P}^d(n)$ is a right $\mathbb{F}_2\mathsf{M}(n)$-module, and so also a right $\mathbb{F}_2\mathsf{GL}(n)$-module. For $A \in \mathsf{M}(n)$, the map $f \mapsto f \cdot A$ is an algebra map of $\mathsf{P}(n)$.*

Proof Let $f, g \in \mathsf{P}(n)$ and $A, B \in \mathsf{M}(n)$, and let $I_n \in \mathsf{M}(n)$ be the identity matrix. We have $f \cdot I_n = f$, and we check that $f \cdot (AB) = (f \cdot A) \cdot B$. Since linear substitutions preserve degree, this proves the first statement. For the second statement, we check that $1 \cdot A = 1$, $(f + g) \cdot A = f \cdot A + g \cdot A$ and $(fg) \cdot A = (f \cdot A)(g \cdot A)$. □

Example 1.2.3 The group $\mathsf{GL}(2)$ is generated by S and U, where

$$S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \; U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

which act on the variables x, y by $x \cdot S = y$, $y \cdot S = x$ and $x \cdot U = x + y$, $y \cdot U = y$. Evaluating in degree 2, we obtain $x^2 \cdot S = y^2$, $xy \cdot S = xy$, $y^2 \cdot S = x^2$ and $x^2 \cdot U = x^2 + y^2$, $xy \cdot U = xy + y^2$, $y^2 \cdot U = y^2$.

By choosing a basis for $\mathsf{P}^d(n)$, we obtain a matrix representation ρ of $\mathsf{GL}(n)$, i.e. a homomorphism $\rho : \mathsf{GL}(n) \to \mathsf{GL}(m)$, where $m = \dim \mathsf{P}^d(n)$. Thus with respect to the basis $\{x^2, xy, y^2\}$ of $\mathsf{P}^2(2)$, S and U are represented by

$$\rho(S) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \rho(U) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

The module $\mathsf{P}^1(n)$ gives the **defining representation** of $\mathsf{GL}(n)$ or $\mathsf{M}(n)$. It is equivalent to the representation $\mathsf{V}(n)$ given by matrix multiplication $v \cdot A$, where v is a row vector regarded as a element of $\mathbb{F}_2^n$. The defining representation is irreducible both as a $\mathbb{F}_2\mathsf{GL}(n)$-module and as a $\mathbb{F}_2\mathsf{M}(n)$-module, meaning that it has no submodules other than itself and 0. In general, the module structure of $\mathsf{P}^d(n)$ is complicated, as the following observation shows.

Proposition 1.2.4 *For $n \geq 1$ and $d \geq 0$, the squaring map $f \mapsto f^2$ embeds $\mathsf{P}^d(n)$ as a $\mathbb{F}_2\mathsf{M}(n)$-submodule in $\mathsf{P}^{2d}(n)$.*

Proof Since $(f+g)^2 = f^2 + g^2$ in $\mathsf{P}(n)$, the squaring map is linear, and it is clearly injective. It is also an $\mathbb{F}_2\mathsf{M}(n)$-module map, since $f^2 \cdot A = (f \cdot A)^2$. □

We shall usually consider $\mathsf{P}^d(n)$ only as a $\mathbb{F}_2\mathsf{GL}(n)$-module. The difference between this and its (even more complicated) $\mathbb{F}_2\mathsf{M}(n)$-module structure can be seen as follows. There are two non-equivalent 1-dimensional representations of $\mathsf{M}(n)$, the 'trivial' representation $\mathsf{I}(n)$, where all matrices act as the identity, and the determinant representation det. Singular matrices act as the identity map for $\mathsf{I}(n)$, and as the zero map for det. The $\mathbb{F}_2\mathsf{M}(1)$-module $\mathsf{P}^d(1)$ is $\mathsf{I}(1)$ if $d = 0$, det if $d > 0$. In $\mathsf{P}(2)$, $\mathsf{GL}(2)$ permutes x, y and $x+y$. Hence $f = xy(x+y)$ is an invariant, and generates a $\mathbb{F}_2\mathsf{GL}(2)$-submodule I of $\mathsf{P}^3(2)$ which is isomorphic to $\mathsf{I}(2)$. Since a singular matrix maps f to 0, I is isomorphic to det as a $\mathbb{F}_2\mathsf{M}(2)$-module. This difference affects higher-dimensional modules as well. For example, the $\mathbb{F}_2\mathsf{GL}(2)$-submodule of $\mathsf{P}^4(2)$ with basis $\{xf, yf\}$ is isomorphic to $\mathsf{P}^1(2)$. As every singular matrix acts as zero on xf and yf, while only the zero matrix acts as zero on $\mathsf{P}^1(2)$, these modules are not isomorphic as $\mathbb{F}_2\mathsf{M}(2)$-modules.

The next result is central to our whole subject.

Proposition 1.2.5 *The right action of $\mathbb{F}_2\mathsf{M}(n)$ on $\mathsf{P}(n)$ commutes with the left action of the Steenrod squares Sq^k. That is to say*

(i) $\mathsf{Sq}(f) \cdot A = \mathsf{Sq}(f \cdot A)$, *for $f \in \mathsf{P}(n)$ and $A \in \mathsf{M}(n)$,*
(ii) $Sq^k : \mathsf{P}^d(n) \to \mathsf{P}^{k+d}(n)$ *is a map of $\mathbb{F}_2\mathsf{M}(n)$-modules.*

Proof Since Sq and $f \mapsto f \cdot A$ are algebra maps of $\mathsf{P}(n)$, we need only check (i) when f is one of the variables x_i. Let $A = (a_{i,j})$. Then $\mathsf{Sq}(x_i) \cdot A = (x_i + x_i^2) \cdot A = x_i \cdot A + (x_i \cdot A)^2$, while $\mathsf{Sq}(x_i \cdot A) = \mathsf{Sq}(\sum_{j=1}^n a_{i,j}x_j) = \sum_{j=1}^n a_{i,j}\mathsf{Sq}(x_j) = \sum_{j=1}^n a_{i,j}(x_j + x_j^2)$. But $\sum_{j=1}^n a_{i,j}x_j^2 = (\sum_{j=1}^n a_{i,j}x_j)^2 = (x_i \cdot A)^2$, so $\mathsf{Sq}(x_i) \cdot A = \mathsf{Sq}(x_i \cdot A)$. Statement (ii) follows by taking the graded parts of Sq. □

We may also consider the set of rectangular $m \times n$ matrices $\mathsf{M}(m,n)$ over $\mathbb{F}_2$, which define linear maps $\mathsf{P}(m) \to \mathsf{P}(n)$ as in Definition 1.2.1. The proof of (i) shows more generally that $\mathsf{Sq}(f) \cdot A = \mathsf{Sq}(f \cdot A)$, for $f \in \mathsf{P}(m)$ and $A \in \mathsf{M}(m,n)$. Although we shall mainly consider $\mathsf{P}(n)$ as a representation of $\mathsf{GL}(n)$ rather than $\mathsf{M}(n)$, it is important to be aware that Steenrod operations commute with specializations of the variables given by singular matrices. For example, since the action of $\left(\begin{smallmatrix}0&0\\0&1\end{smallmatrix}\right)$ sets $x = 0$, and that of $\left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right)$ sets $y = x$, $Sq^1(xy^2 + y^3) = x^2y^2 + y^4$ implies $Sq^1(x^3) = x^4$, by first setting $x = 0$ and then $y = x$.

It is convenient to fix notation for some matrices in $\mathsf{GL}(n)$.

Definition 1.2.6 The **switch matrix** obtained from the identity matrix I_n by exchanging rows i and j will be denoted by $S_{i,j}$, or by S_i in the case $j = i+1$.

The **transvection** obtained from I_n by replacing the entry 0 in position (i,j) by 1 will be denoted by $T_{i,j}$. We also write $U_i = T_{i,i+1}$ and $L_i = T_{i+1,i}$.

Thus S in Example 1.2.3 is also denoted by $S_{1,2}$ or S_1, and U by $T_{1,2}$ or U_1.

1.3 Some properties of Sq^k

The action of Steenrod operations on polynomials is reproduced on squares of polynomials by doubling exponents of the operations.

Proposition 1.3.1 *For $f \in \mathsf{P}(n)$ and $k \geq 0$,*

$$Sq^k(f^2) = \begin{cases} (Sq^j(f))^2, & \text{if } k = 2j \text{ is even,} \\ 0, & \text{if } k \text{ is odd.} \end{cases}$$

Proof By the Cartan formula, $Sq^k(f^2) = \sum_{i+j=k} Sq^i(f)Sq^j(f)$. By exchanging i and j, the terms in the sum with $i \neq j$ cancel in pairs. □

Proposition 1.3.2 *For $f \in \mathsf{P}(n)$ and $s,k \geq 0$,*

$$Sq^k(f^{2^s}) = \begin{cases} (Sq^j(f))^{2^s}, & \text{if } k = 2^s j, \\ 0, & \text{otherwise.} \end{cases}$$

In particular, $Sq^k(x^{2^s})$ is x^{2^s} if $k = 0$, $x^{2^{s+1}}$ if $k = 2^s$, and is 0 otherwise.

Proof This follows from Proposition 1.3.1 by induction on s. □

Proposition 1.3.3 *For $f,g \in \mathsf{P}(n)$ and $s,k \geq 0$,*

$$\text{(i) } Sq^k(gf^{2^s}) = \sum_{i+2^s j=k} Sq^i(g)(Sq^j(f))^{2^s}, \text{ (ii) } Sq^k(gf^{2^s}) = Sq^k(g)f^{2^s} \text{ if } k < 2^s.$$

Proof (i) follows from the Cartan formula and Proposition 1.3.2, and (ii) is immediate from (i) and Proposition 1.1.10. □

Proposition 1.3.4 *For $f \in \mathsf{P}(n)$ and $k \geq 0$,*

$$\text{(i) } Sq^1Sq^{2k}(f) = Sq^{2k+1}(f), \text{ (ii) } Sq^1Sq^{2k+1}(f) = 0.$$

Proof By linearity, we may assume that f is a monomial of degree d. We use induction on d. The case $d = 0$ is true since $\mathsf{Sq}(1) = 1$. For $d > 0$, let $f = xg$ where $x = x_i$ is one of the variables. By the Cartan formula, $Sq^j(f) = xSq^j(g) + x^2Sq^{j-1}(g)$ and $Sq^1Sq^j(f) = xSq^1Sq^j(g) + x^2Sq^j(g) + x^2Sq^1Sq^{j-1}(g)$. The inductive hypothesis for (i) gives $Sq^1Sq^{2k}(g) = Sq^{2k+1}(g)$, and the

inductive hypothesis for (ii) gives $Sq^1Sq^{2k-1}(g) = 0$ and $Sq^1Sq^{2k+1}(g) = 0$. Hence $Sq^1Sq^{2k}(f) = xSq^{2k+1}(g) + x^2Sq^{2k}(g) = Sq^{2k+1}(f)$ and $Sq^1Sq^{2k+1}(f) = x^2Sq^{2k+1}(g) + x^2Sq^{2k+1}(g) = 0$. This completes the induction. □

Proposition 1.3.5 *Given $f \in \mathsf{P}^d(n)$ for $d \geq 1$, $Sq^1(f) = 0$ if and only if $f = Sq^1(g)$ for some $g \in \mathsf{P}^{d-1}(n)$.*

Proof Since $Sq^1Sq^1(g) = 0$ for all polynomials g, the 'if' part follows from Proposition 1.3.4. To prove the 'only if' part, we use induction on n. The case $n = 1$ is true by Proposition 1.1.8. Assume the result for $\mathsf{P}(n-1)$, and let $f \in \mathsf{P}(n)$ with $Sq^1(f) = 0$. Then $f = xf_1 + f_2$, where $x = x_n$, $f_1 \in \mathsf{P}^{d-1}(n)$ and $f_2 \in \mathsf{P}^d(n-1)$. Hence $0 = Sq^1(f) = Sq^1(xf_1) + Sq^1(f_2) = x^2f_1 + xSq^1(f_1) + Sq^1(f_2)$. Since f_2 is independent of x, setting $x = 0$ and using Proposition 1.1.11 we have $Sq^1(f_2) = 0$. Hence $f_2 = Sq^1(g_2)$ for some $g_2 \in \mathsf{P}^{d-1}(n-1)$ by the inductive assumption. Then $x^2f_1 + xSq^1(f_1) = 0$ and so $Sq^1(f_1) = xf_1$. Thus $f = xf_1 + f_2 = Sq^1(f_1 + g_2)$. This completes the induction. □

Since $Sq^1(fg) = Sq^1(f)g + fSq^1(g)$, the operation Sq^1 on $\mathsf{P}(n)$ is a differential. In Section 1.9 we explain how the Steenrod squares may be interpreted in terms of differential operators with polynomial coefficients. Here we show that the action of a Steenrod square commutes with partial differentiation.

Proposition 1.3.6 *Let $f \in \mathsf{P}^d(n)$, $x = x_i$, $1 \leq i \leq n$, and $k \geq 0$. Then*

$$Sq^k\left(\frac{\partial f}{\partial x}\right) = \frac{\partial}{\partial x}(Sq^k(f)).$$

Proof By linearity, we may assume that f is a monomial of degree d. We use induction on d. If f does not involve x, then nor does $Sq^k(f)$ by Proposition 1.1.11. Hence we may assume that $f = xg$, where g is a monomial of degree $d-1$. By the Cartan formula, $Sq^k(\partial(xg)/\partial x) = Sq^k(g + x\partial g/\partial x) = Sq^k(g) + xSq^k(\partial g/\partial x) + x^2Sq^{k-1}(\partial g/\partial x)$ for $k > 0$. On the other hand, $\partial/\partial x(Sq^k(xg)) = \partial/\partial x(xSq^k(g) + x^2Sq^{k-1}(g)) = Sq^k(g) + x\partial/\partial x(Sq^k(g)) + x^2\partial/\partial x(Sq^{k-1}(g))$. By the induction hypothesis, Sq^k and Sq^{k-1} commute with the operator $\partial/\partial x$ on g, and so $Sq^k(\partial f/\partial x) = \partial/\partial x(Sq^k(f))$. This completes the induction. □

1.4 The hit problem

The Steenrod squaring operations allow us to express many elements of $\mathsf{P}^d(n)$ in terms of polynomials of lower degree. For example, $x^5 = Sq^2(x^3)$, $x^4y = Sq^2(x^2y)$ and $x^3y^2 = Sq^1(x^3y) + Sq^2(x^2y)$. By exchanging the variables x and y

and taking sums, it is clear that every element of $\mathsf{P}^5(2)$ can be written in this form.

Definition 1.4.1 A polynomial $f \in \mathsf{P}^d(n)$ is **hit** if it satisfies a **hit equation**

$$f = \sum_{i>0} Sq^i(f_i),\ f_i \in \mathsf{P}^{d-i}(n).$$

By Proposition 1.1.10, $Sq^i(f_i) = 0$ if $i > d/2$, so the sum has $\leq d/2$ terms.

Proposition 1.4.2 *For all $f \in \mathsf{P}^d(n)$, where $d > 0$, f^2 is hit.*

Proof By Proposition 1.1.10, $Sq^d(f) = f^2$. If $d > 0$, this is a hit equation. □

The hit polynomials in $\mathsf{P}^d(n)$, together with the zero polynomial, form a vector subspace $\mathsf{H}^d(n)$. For $f, g \in \mathsf{P}^d(n)$ we write $f \sim g$ if $f - g$ is hit. (Since we are working mod 2, $f - g = f + g$.) This is an equivalence relation, the equivalence classes being cosets of $\mathsf{H}^d(n)$ in $\mathsf{P}^d(n)$.

Proposition 1.4.3 *For $n \geq 1$ and $d \geq 0$, $\mathsf{H}^d(n)$ is an $\mathbb{F}_2\mathsf{M}(n)$-submodule of $\mathsf{P}^d(n)$.*

Proof Let $f = \sum_{i>0} Sq^i(f_i)$ be a hit equation for f, and let $A \in \mathsf{M}(n)$. Then $f \cdot A = \sum_{i>0}(Sq^i(f_i) \cdot A) = \sum_{i>0} Sq^i(f_i \cdot A)$ by Proposition 1.2.5. This is a hit equation for $f \cdot A$. □

When d is even, Proposition 1.4.2 shows that $\mathsf{H}^d(n)$ contains the submodule whose elements are squares (Proposition 1.2.4). The next result gives a related submodule of $\mathsf{H}^d(n)$ when d is odd.

Proposition 1.4.4 *Let $g \in \mathsf{P}^d(n)$ be hit and let $x \in \mathsf{P}^1(n)$. Then xg^2 is hit.*

Proof Let $g = \sum_{i>0} Sq^i(g_i)$ be a hit equation for g. By Proposition 1.3.2, $Sq^{2i}(xg_i^2) = x(Sq^i(g_i))^2$. Hence $xg^2 = x(\sum_{i>0} Sq^i(g_i))^2 = \sum_{i>0} x(Sq^i(g_i)^2) = \sum_{i>0} Sq^{2i}(xg_i^2)$. □

Definition 1.4.5 The **hit problem** is to determine the **cohit module**

$$\mathsf{Q}^d(n) = \mathsf{P}^d(n)/\mathsf{H}^d(n),\ n \geq 1,\ d \geq 0.$$

The hit problem can be put at different levels. The most basic question is to ask whether or not all homogeneous polynomials of degree d in $\mathsf{P}(n)$ are hit. At the next level, we can ask for the dimension of $\mathsf{Q}^d(n)$ as a vector space over $\mathbb{F}_2$. Further, we can ask for a basis of $\mathsf{Q}^d(n)$. For example, as a quotient space of $\mathsf{P}^d(n)$, a basis can be chosen from the equivalence classes of monomials. Finally, we can seek information about $\mathsf{Q}^d(n)$ as a $\mathbb{F}_2\mathsf{GL}(n)$-module, or as a $\mathbb{F}_2\mathsf{M}(n)$-module.

Note that we shall normally write (and refer to) elements of $\mathsf{Q}^d(n)$ as polynomials, although strictly speaking they are equivalence classes of polynomials.

Example 1.4.6 As $Sq^2(x) = 0$ and $Sq^1(x^2) = 0$, x^3 is not hit in $\mathsf{P}(1) = \mathbb{F}_2[x]$. Hence $\mathsf{Q}^3(1)$ is 1-dimensional, generated by x^3. In $\mathsf{P}(2) = \mathbb{F}_2[x,y]$ we have $Sq^1(x) = x^2$ and $Sq^1(y) = y^2$. Hence x^2 and y^2 are hit, but xy is not hit and so $\mathsf{Q}^2(2)$ is 1-dimensional, generated by xy. The discussion at the start of this section shows that $\mathsf{Q}^5(2) = 0$.

As far as the vector space structure of $\mathsf{Q}(n)$ is concerned, the hit problem can be decomposed into smaller problems. Let $Z[n]$ denote the set $\{1,\dots,n\}$ of the first n positive integers. For $Y \subseteq Z[n]$, let $\mathsf{P}(Y)$ be the subspace of $\mathsf{P}(n)$ spanned by monomials which are divisible by x_i if and only if $i \in Y$. If $Y = \emptyset$, then $\mathsf{P}(Y) = \mathsf{P}(0) = \mathbb{F}_2$. By Proposition 1.1.11, $\mathsf{P}(Y)$ is preserved by the action of the Steenrod squares, and so we have a corresponding vector space $\mathsf{H}(Y)$ of hit polynomials and quotient space $\mathsf{Q}(Y) = \mathsf{P}(Y)/\mathsf{H}(Y)$. Then there are direct sum decompositions $\mathsf{P}(n) = \bigoplus_Y \mathsf{P}(Y)$, $\mathsf{H}(n) = \bigoplus_Y \mathsf{H}(Y)$ and $\mathsf{Q}(n) = \bigoplus_Y \mathsf{Q}(Y)$ as vector spaces over $\mathbb{F}_2$, where the sums are over all 2^n subsets Y of $Z[n]$. If $|Y| = |Y'|$ then $\mathsf{Q}(Y) \cong \mathsf{Q}(Y')$, by permuting variables and using Proposition 1.2.5. Since there are $\binom{n}{k}$ k-element subsets Y, this gives the following result.

Proposition 1.4.7 $\dim \mathsf{Q}^d(n) = \sum_{k=1}^{n} \binom{n}{k} \dim \mathsf{Q}^d(Z[k])$ *for* $d > 0$. □

Example 1.4.8 We compute $\dim \mathsf{Q}^3(3)$. Since x^3 is not hit in $\mathsf{P}(1)$ by Example 1.4.6, $\dim \mathsf{Q}^3(Z[1]) = 1$. By Example 1.1.7, $xy^2 \sim x^2y$, but clearly these monomials are not hit, so $\dim \mathsf{Q}^3(Z[2]) = 1$. Finally $\dim \mathsf{Q}^3(Z[3]) = 1$, since the only monomial in $\mathsf{P}^3(Z[3])$ is xyz. Hence $\dim \mathsf{Q}^3(3) = 7$.

In general it is not easy to determine whether a monomial is hit. However, the 1-variable case can be solved using Proposition 1.1.8. For this, we need to evaluate binomial coefficients $\binom{a+b}{a}$ mod 2. This is done by comparing the binary expansions of a and b.

Definition 1.4.9 For $d > 0$, $\mathrm{bin}(d) = \{2^{d_1},\dots,2^{d_r}\}$, where $d = 2^{d_1} + \cdots + 2^{d_r}$ with distinct terms, and $\mathrm{bin}(0) = \emptyset$. For $d \geq 0$, $\alpha(d) = |\mathrm{bin}(d)|$.

Example 1.4.10 $\mathrm{bin}(11) = \{1,2,8\}$, $\alpha(11) = 3$; $\mathrm{bin}(12) = \{4,8\}$, $\alpha(12) = 2$; $\mathrm{bin}(27) = \{1,2,8,16\}$, $\alpha(27) = 4$.

Thus the elements of the set $\mathrm{bin}(d)$ correspond to the 1s in the binary expansion of d, and $\alpha(d)$ is the total number of 1s. By considering binary addition of a and b, it is clear that $\alpha(a+b) \leq \alpha(a) + \alpha(b)$, with equality if and