An algebraic introduction to the Steenrod algebra

Larry Smith

The purpose of these notes is to provide an introduction to the Steenrod algebra in an algebraic manner avoiding any use of cohomology operations. The Steenrod algebra is presented as a subalgebra of the algebra of endomorphisms of a functor. The functor in question assigns to a vector space over a Galois field the algebra of polynomial functions on that vector space: the subalgebra of the endomorphisms of this functor that turns out to be the Steenrod algebra if the ground field is the prime field, is generated by the homogeneous components of a variant of the Frobenius map.

Beginning with the paper of Adams–Wilkerson [1] the Steenrod algebra has played a significant role in the development of the invariant theory of finite groups over finite fields (see Smith [20; 22], Neusel–Smith [18] and Neusel [17] and their reference lists). The literature on the Steenrod algebra, in particular its construction, is largely of an algebraic topological nature, making it difficult for non algebraic topologists to gain insights into how and why it is of significance for invariant theory. This presents a challenge for those versent in the Steenrod to explain it to the nonexperts in a concise, motivated, and nontechnical[1] algebraic manner. More than a decade ago as a visiting professor at Yale I was confronted with this problem when teaching a course on invariant theory to an audience consisting primarily of algbraicists, group theorists, and number theorists. My strategy to define the Steenrod algebra for this audience was to regard the total Steenrod operation as a perturbation of the Frobenius map, and to define the Steenrod algebra as the subalgebra generated by the homogeneous components of this perturbation in the endomorphism algebra of a carefully chosen functor.

The purpose of these notes is to expand somewhat on that approach and provide a more complete introduction to the Steenrod algebra in this manner, ie, presented as a subalgebra of the algebra of endomorphisms of a functor. The functor in question assigns to a vector space over a Galois field the algebra of polynomial functions on that vector space: the subalgebra of the endomorphisms of this functor that turns out to be the Steenrod algebra if the ground field is the prime field, is generated by the homogeneous components of a variant of the Frobenius map.

---

[1]No Eilenberg–MacLane spaces, no $\cup_1$ products, etc.

The material presented here is not new: in fact most of the ideas go back to the middle of the last century, and are to be found in papers of H Cartan [6], [7], J-P Serre [19], R Thom [28] and Wu Wen-tsün [34], with one final key ingredient being supplied by S Bullet and I Macdonald [5] (see also T P Bisson [3]). My contribution, if there is one, is to reorganize the presentation of this material so that no algebraic topology is used, nor is it necessary to assume that the ground field is the prime field. This way of presenting things appeared [2] spread through [20, Chapters 10 and 11]. In summary form it also appeared in [21]. For these notes this material is collected in somewhat altered form, stripped of its applications to algebraic topology, and expanded to include the Hopf algebra structure of the Steenrod algebra due to J W Milnor [13] for the prime field. For a discussion of the group of units of the Steenrod algebra regarded as a Hopf algebra from this point of view see Smith [24].

These notes provide a minimal introduction to the use of the Steenrod algebra in modular invariant theory. The reader is encouraged to consult the vast literature on the Steenrod algebra. For orientation in this morass the reader can do no better than to refer to the excellent survey article [31] and Summer School course notes [32; 33] by R M W Wood.

In what follows we adhere to the notations and terminology of [20] and [18]. In particular, if $\mathbb{F}$ is a field and $V = \mathbb{F}^n$ is an n–dimensional vector space over $\mathbb{F}$, then $\mathbb{F}[V]$ denotes the graded algebra of polynomial functions on V. This may be regarded as the symmetric algebra on the dual vector space V^* of V, where the elements of V^*, the linear forms have degree 1. Note carefully we ignore the usual topological sign conventions, since graded commutation rules play no role here. (For a discussion of gradings see eg [18, Appendix A Section 1].) The correspondence $V \rightsquigarrow \mathbb{F}[V]$ defines a contravariant functor from vector spaces over $\mathbb{F}$ to graded connected algebras. This functor is at the center of what follows.

1 The Steenrod algebra

We fix once and for all a Galois field $\mathbb{F}_q$ of characteristic p containing $q = p^\nu$ elements. Denote by $\mathbb{F}_q[V][[\xi]]$ the power series ring over $\mathbb{F}_q[V]$ in an additional variable ξ, and set $\deg(\xi) = 1 - q$. Define an $\mathbb{F}_q$–algebra homomorphism of degree zero

$$\mathcal{P}(\xi)\colon \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V][[\xi]],$$

by requiring

$$\mathcal{P}(\xi)(\ell) = \ell + \ell^q \xi \in \mathbb{F}_q[V][[\xi]], \quad \forall \text{ linear forms } \ell \in V^*.$$

---

[2] The emphasis of [20, Chapter 10] is on certain topological applications.

For an arbitrary polynomial $f \in \mathbb{F}_q[V]$, we have after separating out homogeneous components, [3]

(1)
$$
\mathcal{P}(\xi)(f) = \begin{cases} \sum\limits_{i=0}^{\infty} \mathcal{P}^i(f)\xi^i & q \neq 2 \\ \sum\limits_{i=0}^{\infty} \mathrm{Sq}^i(f)\xi^i & q = 2 \end{cases}
$$

This defines $\mathcal{P}^i$, resp. Sq^i, as $\mathbb{F}_q$–linear maps

$$
\mathcal{P}^i, \mathrm{Sq}^i \colon \mathbb{F}_q[V] \longrightarrow \mathbb{F}_q[V].
$$

These maps are functorial in V. The operations $\mathcal{P}^i$, respectively Sq^i, are called *Steenrod reduced power operations*, respectively *Steenrod squaring operations*, or collectively, *Steenrod operations*. In order to avoid a separate notation for the case $q = 2$, with the indulgence of topologists, [4] we set $\mathrm{Sq}^i = \mathcal{P}^i$ for all $i \in \mathbb{N}_0$.

The sums appearing in (1) are actually finite. In fact $\mathcal{P}(\xi)(f)$ is a *polynomial* in ξ of degree $\deg(f)$ with leading coefficient f^q. This means the Steenrod operations acting on $\mathbb{F}_q[V]$ satisfy the *unstability condition*

$$
\mathcal{P}^i(f) = \begin{cases} f^q & i = \deg(f) \\ 0 & i > \deg(f) \end{cases} \quad \forall f \in \mathbb{F}_q[V].
$$

Note that these conditions express both a triviality condition, viz., $\mathcal{P}^i(f) = 0$ for all $i > \deg(f)$, and, a nontriviality condition, viz., $\mathcal{P}^{\deg(f)}(f) = f^q$. It is the interplay of these two requirements that seems to endow the unstability condition with the power to yield unexpected consequences.

Next, observe that the multiplicativity of the operator $\mathcal{P}(\xi)$ leads to the formulae:

$$
\mathcal{P}^k(f'f'') = \sum_{i+j=k} \mathcal{P}^i(f')\mathcal{P}^j(f''), \quad \forall f', f'' \in \mathbb{F}_q[V].
$$

These are called the *Cartan formulae* for the Steenrod operations. (NB in field theory, a family of operators satisfying these formulae is called a *higher order derivation*. See, eg Jacobsen [12, Chapter 4, Section 9].)

---

[3] Let me emphasize here, that we will have no reason to consider nonhomogeneous polynomials, and implicitly, we are always assuming, unless the contrary is stated, that all algebras are graded, and if nonnegatively graded, also connected. The algebra $\mathbb{F}[V][[\xi]]$ is graded, but no longer connected.

[4] This is not the usual topological convention, which would be to set $\mathcal{P}^i = \mathrm{Sq}^{2i}$. This is only relevant for this algebraic approach when it is necessary to bring in a Bockstein operation.

As a simple example of how one can compute with these operations consider the quadratic form

$$Q = x^2 + xy + y^2 \in \mathbb{F}_2[x, y].$$

Let us compute how the Steenrod operations Sq^i act on Q by using linearity, the Cartan formula, and unstability.

$$\begin{aligned}
\text{Sq}^1(Q) &= \text{Sq}^1(x^2) + \text{Sq}^1(xy) + \text{Sq}^1(y^2) \\
&= 2x\text{Sq}^1(x) + \text{Sq}^1(x) \cdot y + x \cdot \text{Sq}^1(y) + 2y\text{Sq}^1(y) \\
&= 0 + x^2 y + xy^2 + 0 = x^2 y + xy^2 \\
\text{Sq}^2(Q) &= Q^2 = x^4 + x^2 y^2 + y^4 \\
\text{Sq}^i(Q) &= 0 \text{ for } i > 2.
\end{aligned}$$

Since the Steenrod operations are natural with respect to linear transformations between vector spaces they induce endomorphisms of the functor

$$\mathbb{F}_q[-]: \mathit{Vect}_{\mathbb{F}_q} \longrightarrow \mathit{Alg}_{\mathbb{F}_q}$$

from $\mathbb{F}_q$–vector spaces to commutative graded $\mathbb{F}_q$–algebras.

They therefore commute with the action of $\text{GL}(V)$ on $\mathbb{F}_q[V]$. If $G \hookrightarrow \text{GL}(n, \mathbb{F}_q)$ is a faithful representation of a finite group G then the Steenrod operations restrict to the ring of invariants $\mathbb{F}_q[V]^G$, ie map invariant forms to invariant forms. Hence they can be used to produce new invariants from old ones. This is a new feature of invariant theory over finite fields as opposed to arbitrary fields (but do see in this connection Glenn [10]). Here is an example to illustrate this. It is based on a result, and the methods of [23].

Example 1 Let $\mathbb{F}_q$ be the Galois field with q elements of odd characteristic p, and consider the action of the group $\text{SL}(2, \mathbb{F}_q)$ on the space of binary quadratic forms over $\mathbb{F}_q$ by change of variables. A typical such form is $Q(x, y) = ax^2 + 2bxy + cy^2$.

$$\mathbf{T}_Q = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$$

The space of such forms can be identified with the vector space $\text{Mat}_{2,2}^{\text{sym}}(\mathbb{F}_q)$ of 2×2 symmetric matrices over $\mathbb{F}_q$. Under this identification the form Q corresponds to the matrix $\mathbf{T}_Q$ above, and the action of $\text{SL}(2, \mathbb{F}_q)$ is given by $\mathbf{T}_Q \mapsto \mathbf{S}\mathbf{T}_Q\mathbf{S}^{\text{tr}}$, where $\mathbf{S} \in \text{SL}(2, \mathbb{F}_q)$, with $\mathbf{S}^{\text{tr}}$ the transpose of $\mathbf{S}$. The element $-\mathbf{I} \in \text{SL}(2, \mathbb{F}_q)$ acts trivially. By dividing out the subgroup it generates, we receive a faithful representation of $\text{PSL}(2, \mathbb{F}_q) = \text{SL}(2, \mathbb{F}_q)/\{\pm\mathbf{I}\}$ on the space of binary quadratic forms. This group has order $q(q^2 - 1)/2$.

The action of $\mathrm{PSL}(2, \mathbb{F}_q)$ on $\mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)$ preserves the nonsingular quadratic form defined by $\det\colon \mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q$ and since there is only one such nonsingular quadratic form in 3 variables over $\mathbb{F}_q$, at least up to isomorphism, (cf Dickson [9, pages 169–173]), we receive an unambiguous faithful representation $\rho\colon \mathrm{PSL}(2, \mathbb{F}_q) \hookrightarrow \mathbb{O}(3, \mathbb{F}_q)$. Denote by

$$\begin{bmatrix} x & y \\ y & z \end{bmatrix} \in \mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)^*$$

a generic linear form on the dual space of the 2×2 symmetric matrices over $\mathbb{F}_q$. Per definition the quadratic form

$$\det = xz - y^2 \in \mathbb{F}_q[\mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)] = \mathbb{F}_q[x, y, z]$$

is $\mathbb{O}(3, \mathbb{F}_q)$–invariant. If we apply the first Steenrod operation to this form we receive the new invariant form of degree $q + 1$, viz.,

$$\mathcal{P}^1(\det) = x^q z + xz^q - 2y^{q+1} \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3, \mathbb{F}_q)}.$$

The full ring of invariants of the orthogonal group $\mathbb{O}(3, \mathbb{F}_q)$ is known (see eg Cohen [8] or [23]). To wit

$$\mathbb{F}_q[x, y, z]^{\mathbb{O}(3, \mathbb{F}_q)} \cong \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathbf{E}_{\det}].$$

Here $\mathbf{E}_{\det}$ is the Euler class (see eg Smith–Strong [26] or Neusel–Smith [18, Chapter 4]) associated to the configuration of linear forms defining the set of external lines to the projective variety $\mathfrak{X}_{\det}$ in the projective plane $\mathbb{PF}_q(2)$ over $\mathbb{F}_q$ defined by the vanishing of the determinant [5] (see Hirschfeld [11, Section 8.2] and [23]). The form $\mathbf{E}_{\det}$ has degree $q(q - 1)$. The three forms $\det, \mathcal{P}^1(\det), \mathbf{E}_Q \in \mathbb{F}_q[x, y, z]^{\mathbb{O}(3, \mathbb{F}_q)}$ are a system of parameters [23]. Since the product of their degrees is $|\mathbb{O}(3, \mathbb{F}_q)|$ it follows from [20, Proposition 5.5.5] that $\mathbb{F}_q[x, y, z]^{\mathbb{O}(3, \mathbb{F}_q)}$ must be a polynomial algebra as stated.

The pre-Euler class $\mathbf{e}_{\det}$ of the set of external projective lines to $\mathfrak{X}_{\det}$ is an $\mathbb{O}(3, \mathbb{F}_q)$ $\det$–relative invariant, so is $\mathbb{SO}(3, \mathbb{F}_q)$–invariant. It has degree $\binom{q}{2}$, and together with the forms $\det$ and $\mathcal{P}^1(\det)$ it forms a system of parameters for $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3, \mathbb{F}_q)}$, so again we may apply [20, Proposition 5.5.5] and conclude that $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3, \mathbb{F}_q)}$ is a polynomial algebra, viz., $\mathbb{F}_q[x, y, z]^{\mathbb{SO}(3, \mathbb{F}_q)} = \mathbb{F}_q[\det, \mathcal{P}^1(\det), \mathbf{e}_{\det}]$.

---

[5] The projective plane of $\mathbb{F}_q$ is defined by $\mathbb{PF}_q(2) = \left(\mathbb{F}_q^3 \setminus \{0\}\right)^{\mathbb{F}^\times}$ where $\mathbb{F}^\times$ acts via scalar multiplication on the vectors of $\mathbb{F}_q^3$. In this discussion we are identifying $\mathbb{F}_q^3$ with $\mathrm{Mat}_{2,2}^{\mathrm{sym}}(\mathbb{F}_q)$, so this is the same as the set of lines through the origin in $\mathrm{Mat}_{2,2}^{\mathrm{sym}}$. The pre-Euler class $\mathbf{e}_{\det}$ may be taken to be the product of a set of linear forms $\{\ell_L\}$, indexed by the $\binom{q}{2}$ external lines $\{L\}$ to $\mathfrak{X}_{\det}$, and satisfying $\ker(\ell_L) = L$. The Euler class $\mathbf{E}_{\det}$ is its square.

Finally, $\mathrm{PSL}(2, \mathbb{F}_q)$ is the commutator subgroup of, and has index 2 in, the special orthogonal group $\mathbb{SO}(3, \mathbb{F}_q)$, so by a Proposition in Smith [25] the ring of invariants of $\mathrm{PSL}(2, \mathbb{F}_q)$ acting on the space of binary quadratic forms is a hypersurface. It has generators $\det, \mathcal{P}^1(\det), \mathbf{e}_{\det}$ and a certain form ω which satisfies a monic quadratic equation over the subalgebra generated by the first three. A choice for ω is the pre-Euler class of the configuration of external projective lines to the variety $\mathfrak{X}_{\det} \subset \mathbb{PF}(3)$.

The Steenrod operations can be collected together to form an algebra, in fact a Hopf algebra (see Section 4), over the Galois field $\mathbb{F}_q$.

Definition The *Steenrod algebra* $\mathcal{P}^*(\mathbb{F}_q)$ is the $\mathbb{F}_q$–subalgebra of the endomorphism algebra of the functor $\mathbb{F}_q[-]$, generated by $\mathcal{P}^0 = 1, \mathcal{P}^1, \mathcal{P}^2, \ldots$.

Notation In most situations, such as here, the ground field $\mathbb{F}_q$ is fixed at the outset, and we therefore abbreviate $\mathcal{P}^*(\mathbb{F}_q)$ to $\mathcal{P}^*$.

The next sections develop the basic algebraic structure of the Steenrod algebra.

2   The Adem–Wu relations

The Steenrod algebra is by no means freely generated by the Steenrod reduced powers. For example, when $p = 2$ it is easy to check that $\mathrm{Sq}^1 \mathrm{Sq}^1 = 0$ by verifying this is the case for monomials $z^E = z_1^{e_1}, \ldots, z_n^{e_n}$. To do so one needs the formula, valid for any linear form, $\mathrm{Sq}^1(z^k) = k z^{k+1}$, which follows by induction immediately from the Cartan formula.[6]

Traditionally, relations between the Steenrod operations are expressed as commutation rules for $\mathcal{P}^i \mathcal{P}^j$, respectively $\mathrm{Sq}^i \mathrm{Sq}^j$. These commutation relations are called *Adem–Wu relations*. In the case of the prime field $\mathbb{F}_p$ they were originally conjectured by Wu based on his study of the mod p cohomology of Grassmann manifolds [34] and proved by J Adem in [2], H Cartan in [6], and for $p = 2$ by J P Serre in [19]. These relations are usually written as follows:

$$\mathcal{P}^i \mathcal{P}^j = \sum_{k=0}^{[i/q]} (-1)^{(i-qk)} \cdot \binom{(q-1)(j-k)-1}{i-qk} \mathcal{P}^{i+j-k} \mathcal{P}^k \quad \forall i, j \geq 0, i < qj.$$

Note for any Galois field $\mathbb{F}_q$ the coefficients are still elements in the prime subfield $\mathbb{F}_p$ of $\mathbb{F}_q$.

---

[6]In fact every element in the Steenrod algebra is nilpotent, but the index of nilpotence is known only in a few cases, see eg Monks [15; 16], Walker–Wood [29; 30] and Wood [31] for a resumé of what is known.

The proof of these relations is greatly simplified by the *Bullett–Macdonald identity*, which provides us with a well-wrapped description of the relations among the Steenrod operations, Bullett–Macdonald [5]. To describe this identity, as in [5], extend $\mathcal{P}(\xi)$ to a ring homomorphism $\mathcal{P}(\xi)\colon \mathbb{F}[V][\eta] \longrightarrow \mathbb{F}[V][\eta][\xi]$ by setting $\mathcal{P}(\xi))(\eta) = \eta$. Next, set $u = (1-t)^{q-1} = 1+t+\cdots+t^{q-1}$ and $s = tu$. Then the Bullett–Macdonald identity is

$$\mathcal{P}(s) \circ \mathcal{P}(1) = \mathcal{P}(u) \circ \mathcal{P}(t^q).$$

Since $\mathcal{P}(\xi)$ is additive and multiplicative, it is enough to check this equation for the basis elements of V^*, which is indeed a short calculation. Rumor says Macdonald, like most of us, could not remember the coefficients that appear in the Adem relations, so devised this identity so that he could derive them on the spot when J F Adams came to talk with him.

Remark For $p = 2$, T P Bisson has pointed out (see Bisson–Joyal [4]) that the Bullett–Macdonald identity may be viewed as a commutation rule, viz., $\mathcal{P}(\xi)\mathcal{P}(\eta) = \mathcal{P}(\eta)\mathcal{P}(\xi)$. For a general Galois $\mathbb{F}_q$, one needs to demand $\mathrm{GL}(2, \mathbb{F}_q)$–invariance of $\mathcal{P}(\zeta)$, where $\zeta \in \mathrm{Span}_{\mathbb{F}_q}\{\xi, \eta\}$.

To derive the Adem–Wu relations we provide details for the residue computation[7] sketched in [5]. First of all, direct calculation gives:

$$\mathcal{P}(s)\mathcal{P}(1) = \sum_{a,\, k} s^a \mathcal{P}^a \mathcal{P}^k$$

$$\mathcal{P}(u)\mathcal{P}(t^q) = \sum_{a,\, b,\, j} u^{a+b-j} t^{qj} \mathcal{P}^{a+b-j} \mathcal{P}^j,$$

which the Bullett–Macdonald identity says are equal. Recall from complex analysis that

$$\frac{1}{2\pi\iota} \oint_\gamma z^m dz = \begin{cases} 1 & m = -1 \\ 0 & \text{otherwise,} \end{cases}$$

---

[7]The following discussion is based on conversations with E H Brown Jr. The author is also grateful to J Hartmann for correcting some errors in his version of the computation. I do hope for once the indices are close to being correct.

where γ is a small circle around $0 \in \mathbb{C}$. Therefore we obtain

$$\sum_k \mathcal{P}^a \mathcal{P}^k = \frac{1}{2\pi\iota} \oint_\gamma \frac{\mathcal{P}(s)\mathcal{P}(1)}{s^{a+1}} ds$$

$$= \frac{1}{2\pi\iota} \oint_\gamma \frac{\mathcal{P}(u)\mathcal{P}(t^q)}{s^{a+1}} ds$$

$$= \frac{1}{2\pi\iota} \sum_{a,\,b,\,j} \oint_\gamma \frac{u^{a+b-j}t^{qj}}{s^{a+1}} ds \mathcal{P}^{a+b-j}\mathcal{P}^j.$$

The formula $s = t(1-t)^{q-1}$ gives $ds = (1-t)^{q-2}(1-qt)dt$, so substituting gives

$$\frac{u^{a+b-j}t^{qj}}{s^{a+1}} ds = \frac{(1-t)^{(q-1)(a+b-j)}t^{qj}(1-t)^{q-2}(1-qt)}{\left[t(1-t)^{q-1}\right]^{a+1}} dt$$

$$= (1-t)^{(b-j-1)(q-1)+(q-2)}t^{qj-a-1}(1-qt)dt$$

$$= (1-t)^{((b-j)(q-1)-1)}t^{qj-a-1}(1-qt)dt$$

$$= \left[\sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} t^k\right] t^{qj-a-1}(1-qt)dt$$

$$= \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - qt^{k+qj-a}\right] dt.$$

Therefore

$$\mathcal{P}^a \mathcal{P}^b = \sum_j \left[\frac{1}{2\pi\iota} \oint_\gamma \frac{u^{a+b-j}t^{qj}}{s^{a+1}} ds\right] \mathcal{P}^{a+b-j}\mathcal{P}^j$$

$$= \sum_j \frac{1}{2\pi\iota} \oint \sum_k (-1)^k \binom{(b-j)(q-1)-1}{k} \left[t^{k+qj-a-1} - qt^{k+qj-a}\right] dt \mathcal{P}^{a+b-j}\mathcal{P}^j.$$

Only the terms where

$$k + qj - a - 1 = -1 \quad (k = a - qj)$$
$$k + qj - a = -1 \quad (k = a - qj - 1),$$

contribute anything to the sum, so

$$\mathcal{P}^a \mathcal{P}^b = \sum_j \left[(-1)^{(a-qj)} \cdot \binom{(b-j)(q-1)-1}{a-qj}\right.$$

$$\left. + (-1)^{a-qj-1} q \binom{(b-j)(q-1)-1}{a-qj-1}\right] \mathcal{P}^{a+b-j}\mathcal{P}^j,$$

and since

$$\binom{(b-j)(q-1)-1}{a-qj} - q\binom{(b-j)(q-1)-1}{a-qj-1} \equiv \binom{(b-j)(q-1)-1}{a-qj} \mod p,$$

we conclude

$$\mathcal{P}^a\mathcal{P}^b = \sum_j (-1)^{(a-qj)} \cdot \binom{(b-j)(q-1)-1}{a-qj}\mathcal{P}^{a+b-j}\mathcal{P}^j,$$

which are the Adem–Wu relations.

Thus there is a surjective map from the free associative algebra $\mathcal{B}^*$ with 1 generated by the Steenrod operations modulo the ideal generated by the Adem–Wu relations,

$$\mathcal{P}^a\mathcal{P}^b - \sum_j (-1)^{(a-qj)} \cdot \binom{(b-j)(q-1)-1}{a-qj}\mathcal{P}^{a+b-j}\mathcal{P}^j \quad a, b \in \mathbb{N} \text{ and } a < qb,$$

onto the Steenrod algebra. In fact, this map, $\mathcal{B}^* \longrightarrow \mathcal{P}^*$ is an isomorphism, so the Adem–Wu relations are a complete set of defining relations for the Steenrod algebra. The proof of this, and some of its consequences, is the subject of the next section.

3 The basis of admissible monomials

In this section we show that the relations between Steenrod operations that are universally valid all follow from the Adem–Wu relations. To do so we extend some theorems of of H Cartan [6], J-P Serre [19] and Wu Wen-tsün [34] from the case of the prime field to arbitrary Galois fields. Their proofs have been rearranged so that no direct use is made of algebraic topology.

An *index sequence* is a sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ of nonnegative integers, almost all of which are zero. If I is an index sequence we denote by $\mathcal{P}^I \in \mathcal{P}^*$ the monomial $\mathcal{P}^{i_1} \cdot \mathcal{P}^{i_2} \cdots \mathcal{P}^{i_k} \cdots$ in the Steenrod operations $\mathcal{P}^i$, with the convention that trailing 1s are ignored. The degree of the element $\mathcal{P}^I$ is $(q-1)(i_1+i_2+\cdots+i_k+\cdots)$. These iterations of Steenrod operations are called *basic monomials*. An index sequence I is called admissible if $i_s \geq qi_{s+1}$ for $s = 1, \ldots$. We call k the *length* of I if $i_k \neq 0$ but $i_s = 0$ for $s > k$. Write $\ell(I)$ for the length of I. It is often convenient to treat an index sequence as a finite sequence of nonnegative integers by truncating it to $\ell(I)$ entries.

A basic monomial is defined to be *admissible* if the corresponding index sequence is admissible. The strategy of H Cartan and J-P Serre to prove that the Adem–Wu relations are a complete set of defining relations for the Steenrod algebra of the prime

field is to prove that the admissible monomials are an $\mathbb{F}_p$ basis for $\mathcal{P}^*$. We follow the same strategy for an arbitrary Galois field.

Recall that $\mathcal{B}^*$ denotes the free, graded, associative algebra generated by the symbols $\mathcal{P}^k$ modulo the ideal spanned by the Adem–Wu relations in those symbols. We have a surjective map $\mathcal{B}^* \longrightarrow \mathcal{P}^*$, and so with his notation our goal is to prove:

Theorem 3.1 *The admissible monomials span $\mathcal{B}^*$ as an $\mathbb{F}_q$–vector space. The images of the admissible monomials in the Steenrod algebra are linearly independent.*

Proof We begin by showing that the admissible monomials span $\mathcal{B}^*$.

For a sequence $I = (i_1, i_2, \ldots, i_k)$, the *moment* of I, denoted by $m(I)$, is defined by $m(I) = \sum_{s=1}^k s \cdot i_s$. We first show that an inadmissible monomial is a sum of monomials of smaller moment. Granted this it follows by induction over the moment that the admissible monomials span $\mathcal{B}^*$.

Suppose that $\mathcal{P}^I$ is an inadmissible monomial. Then there is a smallest s such that $i_s < q i_{s+1}$, ie,

$$\mathcal{P}^I = \mathcal{Q}' \mathcal{P}^{i_s} \mathcal{P}^{i_{s+1}} \mathcal{Q}'',$$

where $\mathcal{Q}'$, $\mathcal{Q}''$ are basic monomials, and $\mathcal{Q}'$ is admissible. It is therefore possible to apply an Adem–Wu relation to $\mathcal{P}^I$ to obtain

$$\mathcal{P}^I = \sum_j a_j \mathcal{Q}' \mathcal{P}^{i_s + i_{s+1} - j} \mathcal{P}^j \mathcal{Q}'',$$

for certain coefficients $a_j \in \mathbb{F}_p$. The terms on the right hand side all have smaller moment than $\mathcal{P}^I$ and so, by induction on s, we may express $\mathcal{P}^I$ as a sum of admissible monomials. (NB The admissible monomials are *reduced* in the sense that no Adem–Wu relation can be applied to them.)

We next show that the admissible monomials are linearly independent as elements of the Steenrod algebra $\mathcal{P}^*$. This we do by adapting an argument of J-P Serre [19] and H Cartan [6] which makes use of a formula of Wu Wen-tsün.

Let $e_n = x_1 x_2 \cdots x_n \in \mathbb{F}_q[x_1, \ldots, x_n]$ be the nth elementary symmetric function. Then,

$$\mathcal{P}(\xi)(e_n) = \mathcal{P}(\xi)(\prod_{i=1}^n x_i) = \prod_{i=1}^n \mathcal{P}(\xi)(x_i)$$

$$= \prod_{i=1}^n (x_i + x_i^q \xi) = \prod_{i=1}^n x_i \cdot \prod_{i=1}^n (1 + x_i^{q-1} \xi)$$

$$= e_n(x_1, \ldots, x_n) \cdot \left(\sum_{i=1}^{n} e_i(x_1^{q-1}, \ldots, x_n^{q-1}) \xi^i \right),$$

where $e_i(x_1, \ldots, x_n)$ denotes the ith elementary symmetric polynomial in $x_1, \ldots, x_n$. So we have obtained a formula of Wu Wen-tsün:

$$\mathcal{P}^i(e_n) = e_n \cdot e_i(x_1^{q-1}, \ldots, x_n^{q-1})$$

We claim that the monomials

$$\{\mathcal{P}^I | \mathcal{P}^I \text{ admissible and } \deg(\mathcal{P}^I) \leq 2n\}$$

are linearly independent in $\mathbb{F}_q[x_1, \ldots, x_n]$. To see this note that in case $\ell(I) \leq n$, each entry in I is at most n (so the following formula makes sense), and

$$\mathcal{P}^I(e_n) = e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1}) + \cdots$$

where $I = (i_1, \ldots, i_s)$, $\mathcal{P}^I = \mathcal{P}^{i_1} \cdots \mathcal{P}^{i_s}$ and the remaining terms are lower in the lexicographic ordering on monomials. So $e_n \cdot \prod_{j=1}^{s} e_{i_j}(x_1^{q-1}, \ldots, x_n^{q-1})$ is the largest monomial in $\mathcal{P}^I(e_n)$ in the lexicographic order. Thus

$$\{\mathcal{P}^I(e_n) \mid \mathcal{P}^I \text{ admissible and } \deg(\mathcal{P}^I) \leq 2n\},$$

have distinct largest monomials, so are linearly independent.

By letting $n \longrightarrow \infty$ we obtain the assertion, completing the proof. $\square$

Thus the Steenrod algebra may be regarded (this is one traditional definition) as the graded free associative algebra with 1 generated by the Sq^i respectively $\mathcal{P}^i$ modulo the ideal generated by the Adem–Wu relations. This means we have proven:

Theorem 3.2 *The Steenrod algebra $\mathcal{P}^*$ is the free associative $\mathbb{F}_q$–algebra generated by the reduced power operations $\mathcal{P}^0, \mathcal{P}^1, \mathcal{P}^2, \ldots$ modulo the Adem–Wu relations.*

Corollary 3.3 *The admissible monomials are an $\mathbb{F}_q$–basis for the Steenrod algebra $\mathcal{P}^*$.*

Since the coefficients of the Adem–Wu relations lie in the prime field $\mathbb{F}_p$, the operations $\mathcal{P}^{p^i}$ for $i \geq 0$ are indecomposable in $\mathcal{P}^*$. In particular, over the Galois field $\mathbb{F}_q$, the Steenrod algebra $\mathcal{P}^*$ is *not* generated by the operations $\mathcal{P}^{q^i}$ for $i \geq 0$: one needs all $\mathcal{P}^{p^i}$ for $i \geq 0$. This will become even clearer after we have developed the Hopf algebra structure of $\mathcal{P}^*$ in the next section.

Example 2 Consider the polynomial algebra $\mathbb{F}_2[Q, T]$ over the field with 2 elements, where the indeterminate Q has degree 2 and T has degree 3. If the Steenrod algebra were to act unstably on this algebra then the unstability condition would determine $\mathrm{Sq}^i(Q)$ and $\mathrm{Sq}^j(T)$ apart from $i = 1$ and $j = 1$ and 2. If we specify these as follows

$$\mathrm{Sq}^1(Q) = T, \quad \mathrm{Sq}^1(T) = 0, \quad \mathrm{Sq}^2(T) = QT,$$

and demand that the Cartan formula hold, then using these formulae we can compute Sq^k on any monomial, and hence by linearity, on any polynomial in Q and T. For example

$$\mathrm{Sq}^1(QT) = \mathrm{Sq}^1(Q) \cdot T + Q \cdot \mathrm{Sq}^1(T) = T^2 + 0 = T^2,$$

and so on. Note that since $\mathrm{Sq}^1 \cdot \mathrm{Sq}^1 = 0$ is an Adem–Wu relation, $\mathrm{Sq}^1(T) = 0$ is forced from $\mathrm{Sq}^1(Q) = T$. To verify the unstability conditions, suppose that

$$\mathrm{Sq}^a \mathrm{Sq}^b = \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c} \mathrm{Sq}^c, \quad 0 < a < 2b,$$

is an Adem–Wu relation. We need to show that

$$\left(\mathrm{Sq}^a \mathrm{Sq}^b - \sum_{c=0}^{[\frac{a}{2}]} \binom{b-1-c}{a-2c} \mathrm{Sq}^{a+b-c} \mathrm{Sq}^c \right) (Q^i T^j) = 0$$

for all $i, j \in \mathbb{N}_0$. By a simple argument using the Cartan formulae, see eg [27, Lemma 4.1], it is enough to verify that these hold for the generators Q and T and this is routine. It is a bit more elegant to identify Q with $x^2 + xy + y^2$ and T with $x^2 y + xy^2 \in \mathbb{F}_2[x, y]$. The action of the Steenrod operations on Q and T then coincides with the restriction of the action from $\mathbb{F}_2[x, y]$. This way, it is then clear that $\mathbb{F}_2[Q, T]$ is an unstable algebra over the Steenrod algebra, because,

(1) with some topological background we recognize this as just $H^*(B\mathbb{SO}(3); \mathbb{F}_2)$, or,

(2) with some invariant theoretic background we recognize this as the Dickson algebra $\mathbf{D}(2) = \mathbb{F}_2[x, y]^{\mathrm{GL}(2, \mathbb{F}_2)}$.

4 The Hopf algebra structure of the Steenrod algebra

Our goal in this section is to complete the traditional picture of the Steenrod algebra by proving that $\mathcal{P}^*(\mathbb{F}_q)$ is a Hopf algebra [8] and extending Milnor's Hopf algebra [13] structure theorems from the prime field $\mathbb{F}_p$ to an arbitrary Galois field. It should be emphasized that this requires no new ideas, only a careful reorganization of Milnor's proofs, so as to avoid reference to algebraic topology and cohomology operations, and, where appropriate carefully replacing p by q.

Proposition 4.1 *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Then the Steenrod algebra of $\mathbb{F}_q$ is a cocommutative Hopf algebra over $\mathbb{F}_q$ with respect to the coproduct*

$$\nabla \colon \mathcal{P}^* \longrightarrow \mathcal{P}^* \otimes \mathcal{P}^*,$$

defined by the formulae

$$\nabla(\mathcal{P}^k) = \sum_{i+j=k} \mathcal{P}^i \otimes \mathcal{P}^j, \quad k = 1, 2, \dots.$$

Proof Consider the functor $V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the commutative graded algebra $\mathbb{F}_q[V] \otimes \mathbb{F}_q[V]$ over $\mathbb{F}_q$. There is a natural map of algebras

$$\mathcal{P}^* \otimes \mathcal{P}^* \longrightarrow \operatorname{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]),$$

given by the tensor product of endomorphisms. Since there is an isomorphism

$$\mathbb{F}_q[V] \otimes \mathbb{F}_q[V] \cong \mathbb{F}_q[V \oplus V],$$

that is natural in V, the functor $\operatorname{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])$ is a subfunctor of the functor $\operatorname{End}(V \rightsquigarrow \mathbb{F}_q[V])$ that assigns to a finite dimensional vector space V over $\mathbb{F}_q$ the polynomial algebra $\mathbb{F}_q[V]$. Hence restriction defines a map of algebras

$$\mathcal{P}^* \longrightarrow \operatorname{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V]),$$

---

[8]One quick way to do this is to write down as comultiplication map

$$\nabla(\mathcal{P}^k) = \sum_{i+j=k} \mathcal{P}^i \otimes \mathcal{P}^j, \quad k = 1, 2, \dots,$$

and verify that it is compatible with the Bullett–Macdonald identity, and hence also with the Adem–Wu relations.

and we obtain a diagram of algebra homomorphisms

$$
\begin{array}{ccc}
& & \mathcal{P}^* \otimes \mathcal{P}^* \\
& \nearrow & \downarrow \tau \\
\mathcal{P}^* & \xrightarrow[\rho]{} & \operatorname{End}(V \rightsquigarrow \mathbb{F}_q[V] \otimes \mathbb{F}_q[V])
\end{array}
$$

What we need to show is that $\operatorname{Im}(\rho) \subseteq \operatorname{Im}(\tau)$, for since τ is monic $\nabla = \tau^{-1}\rho$ would define the desired coproduct. Since the reduced power operations $\mathcal{P}^k$ for $k = 1, 2, \ldots,$ generate $\mathcal{P}^*$ it is enough to check that $\rho(\mathcal{P}^k) \in \operatorname{Im}(\tau)$ for $k = 1, 2, \ldots,.$ But this is immediate from the Cartan formula. Since ∇ is a map of algebras the Hopf condition is satisfied, so $\mathcal{P}^*$ is a Hopf algebra. $\qquad\square$

If J is an admissible index sequence then

$$
e(J) = \sum_{s=1}^{\infty} (j_s - q j_{s+1}),
$$

is called the *excess* of J. For example, the sequences

$$
M_k = (q^{k-1}, \ldots, q, 1), \quad k = 1, 2, \ldots,
$$

are all the admissible sequences of excess zero. Note that

$$
\deg(\mathcal{P}^{M_k}) = \sum_{j=1}^{k} q^{k-j}(q-1) = q^k - 1, \text{ for } k = 1, 2, \ldots.
$$

Recall by Corollary 3.3 that the admissible monomials are an $\mathbb{F}_q$–vector space basis for $\mathcal{P}^*$.

Let $\mathcal{P}_*(\mathbb{F}_q)$ denote the Hopf algebra dual to the Steenrod algebra $\mathcal{P}^*(\mathbb{F}_q)$. We define $\xi_k \in \mathcal{P}_*(\mathbb{F}_q)$ to be dual to the monomial $\mathcal{P}^{M_k} = \mathcal{P}^{q^{k-1}} \cdots \mathcal{P}^q \cdot \mathcal{P}^1$ with respect to the basis of admissible monomials for $\mathcal{P}^*$. This means that we have:

$$
\langle \mathcal{P}^J \mid \xi_k \rangle = \begin{cases} 1 & J = M_k \\ 0 & \text{otherwise,} \end{cases}
$$

where we have written $\langle \mathcal{P} \mid \xi \rangle$ for the value of an element $\mathcal{P} \in \mathcal{P}^*(\mathbb{F}_q)$ on an element $\xi \in \mathcal{P}_*(\mathbb{F}_q)$. Note that $\deg(\xi_k) = q^k - 1$ for $k = 1, \ldots.$

If $I = (i_1, i_2, \ldots, i_k, \ldots)$ is an index sequence we call ℓ the *length* of I, denoted by $\ell(I)$, if $i_k = 0$ for $k > \ell$, but $i_\ell \neq 0$. We associate to an index sequence $I =$

$(i_1, i_2, \ldots, i_k, \ldots)$ the element $\xi^I = \xi_1^{i_1} \cdot \xi_2^{i_2} \cdots \xi_\ell^{i_\ell} \in \mathcal{P}_*(\mathbb{F}_q)$, where $\ell = \ell(I)$. Note that

$$\deg(\xi^I) = \sum_{s=1}^{\ell(I)} i_s(q^s - 1).$$

To an index sequence $I = (i_1, i_2, \ldots, i_k, \ldots)$ we also associate an admissible sequence $J(I) = (j_1, j_2, \ldots, j_k, \ldots)$ defined by

$$(2) \qquad j_1 = \sum_{s=1}^{\infty} i_s q^{s-1}, \quad j_2 = \sum_{s=2}^{\infty} i_s q^{s-2}, \ldots, \quad j_k = \sum_{s=k}^{\infty} i_s q^{s-k}, \ldots.$$

It is easy to verify that as I runs over all index sequences that $J(I)$ runs over all admissible sequences. Finally, note that $\deg(\mathcal{P}^{J(I)}) = \deg(\xi^I)$ for any index sequence I.

The crucial observation used by Milnor to prove the structure theorem of $\mathcal{P}_*(\mathbb{F}_q)$ is that the pairing of the admissible monomial basis for $\mathcal{P}^*(\mathbb{F}_q)$ against the monomials in the ξ_k is upper triangular. To formulate this precisely we order the index sequences lexicographically from the right so for example $(1, 2, 0, \ldots) \prec (0, 0, 1, \ldots)$.

Lemma 4.2 (J W Milnor) *With the preceding notations we have that the inner product matrix* $\langle \mathcal{P}^{J(I)} \mid \xi^K \rangle$ *is upper triangular with* 1 *s on the diagonal, ie,*

$$\langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = \begin{cases} 1 & I = K \\ 0 & I < K. \end{cases}$$

Proof Let the length of K be ℓ and define $K' = (k_1, k_2, \ldots, k_{\ell-1})$, so

$$\xi^K = \xi^{K'} \cdot \xi_\ell \in \mathcal{P}_*(\mathbb{F}_q).$$

If ∇ denotes the coproduct in $\mathcal{P}^*(\mathbb{F}_q)$, then we have the formula

$$(3) \qquad \langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = \langle \mathcal{P}^{J(I)} \mid \xi^{K'} \cdot \xi_\ell \rangle = \langle \nabla(\mathcal{P}^{J(I)}) \mid \xi^{K'} \otimes \xi_\ell \rangle$$

If $J(I) = (j_1, j_2, \ldots, j_k, \ldots)$ then one easily checks that

$$\nabla(\mathcal{P}^{J(I)}) = \sum_{J' + J'' = J(I)} \mathcal{P}^{J'} \otimes \mathcal{P}^{J''}.$$

Substituting this into (3) gives

$$(4) \qquad \langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = \sum_{J' + J'' = J(I)} \langle \mathcal{P}^{J'} \mid \xi^{K'} \rangle \cdot \langle \mathcal{P}^{J''} \mid \xi_\ell \rangle.$$

By the definition of ξ_ℓ we have

$$\langle \mathcal{P}^{J''} \mid \xi_\ell \rangle = \begin{cases} 1 & J'' = M_\ell \\ 0 & \text{otherwise.} \end{cases}$$

If $J'' = M_\ell$ then unravelling the definitions shows that $J' = J(I')$, for a suitable I', so if K and I have the same length ℓ, we have shown

$$\langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = \langle \mathcal{P}^{J(I')} \mid \xi^{K'} \rangle,$$

and hence it follows from induction over the degree that

$$\langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = \begin{cases} 1 & I = K \\ 0 & I < K. \end{cases}$$

If, on the other hand, $\ell(I) < \ell$ then all the terms

$$\langle \mathcal{P}^{J''} \mid \xi_\ell \rangle$$

in the sum (4) are zero and hence that $\langle \mathcal{P}^{J(I)} \mid \xi^K \rangle = 0$ as required. $\qquad\square$

Theorem 4.3 *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. Let $\mathcal{P}_*(\mathbb{F}_q)$ denote the dual Hopf algebra to the Steenrod algebra of the Galois field $\mathbb{F}_q$. Then, as an algebra*

$$\mathcal{P}_* \cong \mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots],$$

where $\deg(\xi_k) = q^k - 1$ for $k \in \mathbb{N}$. The coproduct is given by the formula

$$\nabla_*(\xi_k) = \sum_{i+j=k} \xi_i^{q^j} \otimes \xi_j, \quad k = 1, 2, \ldots.$$

Proof By Milnor's Lemma (Lemma 4.2) the monomials $\{\xi^I\}$ where I ranges over all index sequences are linearly independent in $\mathcal{P}_*(\mathbb{F}_q)$. Hence $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] \subseteq \mathcal{P}_*(\mathbb{F}_q)$. The algebras $\mathcal{P}_*(\mathbb{F}_q)$ and $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots]$ have the same Poincaré series, since $\deg(\mathcal{P}^{J(I)}) = \deg(\xi^I)$ for all index sequences I, and the admissible monomials $\mathcal{P}^{J(I)}$ are an $\mathbb{F}_q$–vector space basis for $\mathcal{P}^*(\mathbb{F}_q)$. So $\mathbb{F}_q[\xi_1, \ldots, \xi_k, \ldots] = \mathcal{P}_*(\mathbb{F}_q)$, and it remains to verify the formula for the coproduct.

To this end we use the test algebra $\mathbb{F}_q[u]$, the polynomial algebra on one generator, as in [13]. Note that for admissible sequences we have

$$(5) \qquad\qquad \mathcal{P}^J(u) = \begin{cases} u^{q^k} & J = M_k \\ 0 & \text{otherwise.} \end{cases}$$

Define the map

$$\lambda^*\colon \mathbb{F}_q[u] \longrightarrow \mathbb{F}_q[u] \otimes \mathcal{P}_*,$$

by the formula

$$\lambda^*(u^i) = \sum \mathcal{P}^{J(I)}(u^i) \otimes \xi^I,$$

where the sum is over all index sequences I. Note that in any given degree the sum is finite and that λ^* is a map of algebras. Moreover

$$(\lambda^* \otimes 1)\lambda^*(u) = (1 \otimes \nabla_*)\lambda^*(u),$$

ie the following diagram

(6)

$$
\begin{array}{ccc}
\mathbb{F}_q[u] \otimes \mathcal{P}_*(\mathbb{F}_q) \otimes \mathcal{P}_*(\mathbb{F}_q) & \xleftarrow{\quad 1\otimes\nabla_* \quad} & \mathbb{F}_q[u] \otimes \mathcal{P}_* \\
\Big\uparrow{\scriptstyle \lambda^*\otimes 1} & & \Big\uparrow{\scriptstyle \lambda^*} \\
\mathbb{F}_q[u] \otimes \mathcal{P}_* & \xleftarrow{\quad \lambda^* \quad} & \mathbb{F}_q[u]
\end{array}
$$

is commutative.

From (5) it follows that

$$\lambda^*(u) = \sum u^{q^k} \otimes \xi_k,$$

which when raised to the q^r th power gives

$$\lambda^*(u^r) = \sum u^{q^{k+r}} \otimes \xi_k^{q^r},$$

and leads to the formula

$$(\lambda^* \otimes 1)\big(\lambda^*(u)\big) = \big(\lambda^* \otimes 1\big)\Big(\sum_k u^{q^k} \otimes \xi_k\Big) = \sum_r \sum_k u^{q^{k+r}} \otimes \xi_r^{q^k} \otimes \xi_k.$$

Whereas, the other way around the diagram (6) yields

$$\big(1 \otimes \nabla_*\big)(\lambda^*(u)) = \sum_j u^{q^j} \otimes \nabla_*(\xi_k),$$

and equating these two expressions leads to the asserted formula for the coproduct. $\square$

As remarked at the end of the previous section the operations $\mathcal{P}^{p^i}$ for $i > 0$ are indecomposables in $\mathcal{P}^*$, so $\mathcal{P}^*$ is not generated by the operations $\mathcal{P}^{q^i}$ for $i \geq 0$; we need all the $\mathcal{P}^{p^i}$ for $i > 0$. This can be readily seen on hand from the dual Hopf algebra, where, since $\mathbb{F}_q$ has characteristic p, the elements $\xi_1^{p^i}$ for $i \geq 0$ are all primitive, [14]. The following corollary also indicates that passing from the prime field $\mathbb{F}_p$ to a general Galois field $\mathbb{F}_q$ is not just a simple substitution of q for p.

Corollary 4.4 *Let p be a prime integer, $q = p^\nu$ a power of p s and $\mathbb{F}_q$ the Galois field with q elements. The indecomposable module $Q(\mathcal{P}^*)$ of the Steenrod algebra of $\mathbb{F}_q$ has a basis consisting of the elements $\mathcal{P}^{p^i}$ for $i \in \mathbb{N}_0$, and the primitive elements $P(\mathcal{P}^*)$ has a basis consisting of the elements $\mathcal{P}^k$ for $k \in \mathbb{N}$, where, for $k \in \mathbb{N}$, $\mathcal{P}^k$ is dual to ξ_k with respect to the monomial basis for $\mathcal{P}_*$.*

5 The Milnor basis and embedding one Steenrod algebra in another

If $I = (i_1, i_2, \ldots, i_k, \ldots)$ is an index sequence we denote by $\mathcal{P}(I) \in \mathcal{P}^*(\mathbb{F}_q)$ the element in the Steenrod algebra that is dual to the corresponding monomial ξ^I in $\mathcal{P}_*(\mathbb{F}_q)$ with respect to the monomial basis for $\mathcal{P}_*(\mathbb{F}_q)$. This is not the same as the monomial $\mathcal{P}^I = \mathcal{P}^{i_1} \cdot \mathcal{P}^{i_2} \cdots \mathcal{P}^{i_k} \cdots$, these two elements do not even have the same degrees. As I ranges over all index sequences the collection $\mathcal{P}(I)$ ranges over an $\mathbb{F}_q$–basis for $\mathcal{P}^*(\mathbb{F}_q)$ called the *Milnor basis*.

To give some examples of elements written in the Milnor basis introduce the index sequence Δ_k which has a 1 in the kth position and otherwise 0s. Then $\mathcal{P}^k$ is $\mathcal{P}(k \cdot \Delta_1)$, and, as noted at the end of Section 4, *the Milnor primitive elements $\mathcal{P}^{\Delta_k} = \mathcal{P}(\Delta_k)$, for $k > 0$, form a basis for the subspace of all primitive elements*. In terms of the reduced power operations these elements can also be defined by the inductive formulae

$$\mathcal{P}^{\Delta_k} = \begin{cases} \mathcal{P}^1 & k = 1 \\ [\mathcal{P}^{q^{k-1}}, \mathcal{P}^{\Delta_k}] & k > 0, \end{cases}$$

where $[\mathcal{P}', \mathcal{P}'']$ denotes the commutator $\mathcal{P}' \cdot \mathcal{P}'' - \mathcal{P}'' \cdot \mathcal{P}'$ of $\mathcal{P}'$ and $\mathcal{P}''$. In Milnor's paper one can also find a formula for the product $\mathcal{P}(I) \cdot \mathcal{P}(J)$ of two elements in the Milnor basis. The basis transformation matrix from the admissible to the Milnor basis and its inverse is quite complicated, so we will say nothing more about it.

To each index sequence I we can make correspond both an admissible sequence over $\mathbb{F}_p$ and one over $\mathbb{F}_q$ via the equations (2) from the previous section. This correspondence gives us a map $\theta \colon \mathcal{P}^*(\mathbb{F}_q) \longrightarrow \mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$.

Theorem 5.1 *Let p be a prime integer, $q = p^\nu$ a power of p, and $\mathbb{F}_q$ the Galois field with q elements. The map*

$$\theta \colon \mathcal{P}^*(\mathbb{F}_q) \longrightarrow \mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q,$$

embeds the Steenrod algebra $\mathcal{P}^*(\mathbb{F}_q)$ of $\mathbb{F}_q$ as a Hopf subalgebra in the Steenrod algebra of $\mathbb{F}_p$ extended from $\mathbb{F}_p$ up to $\mathbb{F}_q$.

Proof It is much easier to verify that the dual map

$$\theta_* \colon \mathcal{P}_*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q \longrightarrow \mathcal{P}_*(\mathbb{F}_q),$$

which is defined by the requirement that it be a map of algebras, and take the values

$$\theta_*(\xi_k(p) \otimes 1) = \begin{cases} \xi_m(q) & k = mv \text{ (so } p^k - 1 = q^m - 1) \\ 0 & \text{otherwise,} \end{cases}$$

on algebra generators, is a map of Hopf algebras. This is a routine computation. □

The Steenrod algebra over the prime field $\mathbb{F}_p$ has a well known interpretation as the mod p cohomology of the Eilenberg–MacLane spectrum. By flat base change $\mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ may be regarded as the $\mathbb{F}_q$–cohomology of the same. By including the Eilenberg–MacLane spectrum $K(\mathbb{F}_p)$ for the prime field into the Eilenberg–MacLane spectrum $K(\mathbb{F}_q)$ we may view the elements of $\mathcal{P}^*(\mathbb{F}_p) \otimes_{\mathbb{F}_p} \mathbb{F}_q$ as defining stable cohomology operations in $\mathbb{F}_q$–cohomology. By Theorem 5.1 this also allows us to interpret elements of $\mathcal{P}^*(\mathbb{F}_q)$ as stable cohomology operations acting on the $\mathbb{F}_q$–cohomology of a topological space. Which elements appear in this way is described in cohomological terms in [24].

6   Closing comments

Algebraic topologists will of course immediately say *"but that isn't the Steenrod algebra, it is only the algebra of reduced power operations; there is no Bockstein operator unless $q = 2$."* This is correct, the full Steenrod algebra, with the Bockstein, has not yet played a significant role in invariant theory, so it has not been treated here. But, if one wishes to have a definition of the full Steenrod algebra in the same style as the one presented here, all one needs to do for $q \neq 2$ is to replace the functor $V \rightsquigarrow \mathbb{F}[V]$ with the functor $V \rightsquigarrow H(V)$, where $H(V)$ is defined to be $H(V) = \mathbb{F}[V] \otimes E[V]$, with $E[V]$ the exterior algebra on the dual vector space V^* of V. Since V^* occurs *twice* as a subspace of $H(V)$, once as $V^* \otimes \mathbb{F} \subset \mathbb{F}[V] \otimes \mathbb{F}$ and once as $\mathbb{F} \otimes V^* \subset E[V]$, we need a way to distinguish these two copies. One way to do this is to write z for a linear form $z \in V^*$ when it is to be regarded as a polynomial function, and dz for the same linear form when it is to be regarded as an alternating linear form. This amounts to identifying $H(V)$ with the algebra of polynomial differential forms on V.

Next introduce the Bockstein operator $\beta \colon H(V) \longrightarrow H(V)$ by requiring it to be the unique derivation with the property that for an alternating linear form dz one has $\beta(dz) = z$, where z is the corresponding polynomial linear form, and for any polynomial linear form z one has $\beta(z) = 0$. The operators $\mathcal{P}^k$ for $k \in \mathbb{N}_0$ together with

β generate a subalgebra of the algebra of endomorphisms of the functor $V \rightsquigarrow H(V)$, and this subalgebra is the full Steenrod algebra of the Galois field $\mathbb{F}_q$.

Finally, there is a universal algebra approach to both the Dyer–Lashof algebra and the Steenrod algebra in [4]. The interested reader should consult this paper which contains many informative facts.

References

[1] **J F Adams**, **C W Wilkerson**, *Finite H–spaces and algebras over the Steenrod algebra*, Ann. of Math. (2) 111 (1980) 95–143   MR558398

[2] **J Adem**, *The relations on Steenrod powers of cohomology classes. Algebraic geometry and topology*, from: "A symposium in honor of S. Lefschetz", Princeton University Press, Princeton, NJ (1957) 191–238   MR0085502

[3] **T P Bisson**, *Divided Sequences and Bialgebras of Homology Operations*, PhD thesis, Duke University (1977)

[4] **T P Bisson**, **A Joyal**, *Q–rings and the homology of the symmetric groups*, from: "Operads: Proceedings of Renaissance Conferences (Hartford, CT/Luminy, 1995)", Contemp. Math. 202, Amer. Math. Soc., Providence, RI (1997) 235–286   MR1436923

[5] **S R Bullett**, **I G Macdonald**, *On the Adem relations*, Topology 21 (1982) 329–332   MR649764

[6] **H Cartan**, *Sur l'itération des opérations de Steenrod*, Comment. Math. Helv. 29 (1955) 40–58   MR0068219

[7] **H Cartan**, *Algèbres d'Eilenberg–Mac Lane et Homotopie*, from: "Séminaire Henri Cartan, 7e Année 1954/55", W A Benjamin, New York (1967)

[8] **S D Cohen**, *Rational functions invariant under an orthogonal group*, Bull. London Math. Soc. 22 (1990) 217–221   MR1041133

[9] **L E Dickson**, *Linear groups: With an exposition of the Galois field theory*, Dover Publications, New York (1958)   MR0104735

[10] **O E Glenn**, *Modular invariant processes*, Bull. Amer. Math. Soc. 21 (1914–1915) 167–173

[11] **J W P Hirschfeld**, *Projective geometries over finite fields*, second edition, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York (1998)   MR1612570

[12] **N Jacobson**, *Lectures in abstract algebra III: Theory of fields and Galois theory*, Graduate Texts in Mathematics 32, Springer, New York (1975)   MR0392906

[13] **J W Milnor**, *The Steenrod algebra and its dual*, Ann. of Math. (2) 67 (1958) 150–171   MR0099653

[14] **J W Milnor**, **J C Moore**, *On the structure of Hopf algebras*, Ann. of Math. (2) 81 (1965) 211–264   MR0174052

[15] **K G Monks**, *Nilpotence in the Steenrod algebra*, Bol. Soc. Mat. Mexicana (2) 37 (1992) 401–416   MR1317590

[16] **K G Monks**, *The nilpotence height of P_t^s* , Proc. Amer. Math. Soc. 124 (1996) 1297–1303   MR1301039

[17] **M D Neusel**, *Inverse invariant theory and Steenrod operations*, Mem. Amer. Math. Soc. 146 (2000)   MR1693799

[18] **M D Neusel**, **L Smith**, *Polynomial Invariants of Finite Groups*, Math. Surveys and Monographs 94, American Mathematical Society, Providence (2002)

[19] **J-P Serre**, *Cohomologie modulo* 2 *des complexes d'Eilenberg–Mac Lane*, Comment. Math. Helv. 27 (1953) 198–232   MR0060234

[20] **L Smith**, *Polynomial invariants of finite groups*, Research Notes in Mathematics 6, A K Peters Ltd., Wellesley, MA (1995)   MR1328644

[21] **L Smith**, $\mathcal{P}^*$*–invariant ideals in rings of invariants*, Forum Math. 8 (1996) 319–342   MR1387699

[22] **L Smith**, *Polynomial invariants of finite groups. A survey of recent developments*, Bull. Amer. Math. Soc. (N.S.) 34 (1997) 211–250   MR1433171

[23] **L Smith**, *The ring of invariants of* $O(3, \mathbb{F}_q)$, Finite Fields Appl. 5 (1999) 96–101   MR1667106

[24] **L Smith**, *Cohomology automorphisms over Galois fields and group-like elements in the Steenrod algebra*, AG-Invariantentheorie preprint (2000)

[25] **L Smith**, *Invariants of* 2×2 *matrices over finite fields*, Finite Fields Appl. 8 (2002) 504–510   MR1933621

[26] **L Smith**, **R E Stong**, *On the invariant theory of finite groups: orbit polynomials and splitting principles*, J. Algebra 110 (1987) 134–157   MR904185

[27] **N Steenrod**, *Polynomial algebras over the algebra of cohomology operations*, from: "H–spaces (Actes Réunion Neuchâtel, 1970)", Lecture Notes in Mathematics 196, Springer, Berlin (1971) 85–99   MR0286100

[28] **R Thom**, *Quelques propriétés globales des variétés différentiables*, Comment. Math. Helv. 28 (1954) 17–86   MR0061823

[29] **G Walker**, **R M W Wood**, *The nilpotence height of* Sq^{2^n} , Proc. Amer. Math. Soc. 124 (1996) 1291–1295   MR1307571

[30] **G Walker**, **R M W Wood**, *The nilpotence height of* P^{p^n} , Math. Proc. Cambridge Philos. Soc. 123 (1998) 85–93   MR1474867

[31] **R M W Wood**, *Problems in the Steenrod algebra*, Bull. London Math. Soc. 30 (1998) 449–517   MR1643834

[32] **R M W Wood**, *Hit Problems and the Steenrod Algebra*, Notes from a lecture course at the University of Ioannina (2000)

[33] **R M W Wood**, *Invariant theory and the Steenrod algebra*, Course notes from the lecture series at the conference "Invariant theory and its interactions with related fields", Göttingen (2003)

[34] **W-t Wu**, *Sur les puissances de Steenrod*, from: "Colloque de Topologie de Strasbourg, 1951, no. IX", La Bibliothèque Nationale et Universitaire de Strasbourg (1952) 9 MR0051510

AG-Invariantentheorie, Mittelweg 3, D 37133 Friedland, Federal Republic of Germany

larry@uni-math.gwdg.de