# Endomorphisms of the Steenrod algebra and of its odd subalgebra 

Sandling, Robert

2011

MIMS EPrint: 2011.111

Manchester Institute for Mathematical Sciences
School of Mathematics

The University of Manchester

```
Reports available from: http://eprints.maths.manchester.ac.uk/
    And by contacting: The MIMS Secretary
    School of Mathematics
    The University of Manchester
    Manchester, M13 9PL, UK
```


# Endomorphisms of the Steenrod algebra and of its odd subalgebra 

Robert Sandling<br>School of Mathematics<br>University of Manchester


#### Abstract

We characterise those algebra endomorphisms of the Steenrod algebra over the field of two elements, and those of its odd subalgebra, which send Steenrod squares to Steenrod squares or to 0 . Two such maps appear in the literature, an epimorphism of the Steenrod algebra in the book of Steenrod and Epstein which halves superscripts on Steenrod squares and a monomorphism of the odd subalgebra in a paper of Monks. In the latter context a new map, an epimorphism, arises which has contrasting features to those of the endomorphism of Monks. Formulae for the endomorphisms are indicated both for the admissible and the Milnor bases.


## 1. Introduction and preliminaries

An $\mathbf{F}_{2}$-algebra endomorphism of the Steenrod algebra which sent Steenrod squares to Steenrod squares (or to 0 ) would be particularly accessible. Two such maps occur in the literature, one on the full Steenrod algebra and the other on its so-called odd subalgebra. The first, dating at least to the book of Steenrod and Epstein [SE62, p. 24] and called $\gamma$ in Wood's survey article [Wo98, p. 488], halves the superscripts. That is, for $p \geq 0, \gamma\left(\mathrm{Sq}^{2 p}\right)=\mathrm{Sq}^{p}$ and $\gamma\left(\mathrm{Sq}^{2 p+1}\right)=0$.

The second map, called $\lambda$ in [Mo92; Wo98, p. 489], doubles the superscripts and subtracts 1 . We restrict attention to its action on the subalgebra on which it is an algebra endomorphism, namely, the odd subalgebra, the subspace having as basis all admissible $\mathrm{Sq}^{\mathbf{a}}:=\mathrm{Sq}^{a_{1}} \mathrm{Sq}^{a_{2}}, \cdots, \mathrm{Sq}^{a_{\ell}}, \mathbf{a}=\left(a_{1}, a_{2}, \cdots, a_{\ell}\right), a_{i} \geq 0$, for which each superscript $a_{i}$ is odd or 0 (and so including the unit 1 of $A$ ). Thus, for $p \geq 0, \lambda\left(\mathrm{Sq}^{2 p+1}\right)=\mathrm{Sq}^{4 p+1}$. The odd subalgebra $O$ of the Steenrod algebra $A$ and its endomorphism $\lambda$ seem to have been introduced by Monks in his 1989 thesis (see [Mo92]); he used the Milnor basis. In [Mo92] a chain of smaller and smaller subalgebras is defined, each isomorphic to the next and all of them isomorphic to $O$. The isomorphisms are explicitly given and give rise to $\lambda$ and its powers. Here we define a chain of larger and larger ideals whose quotient algebras are each isomorphic to the next and again all are isomorphic to $O$. The isomorphisms give rise to endomorphisms of $O$ which send Steenrod squares to Steenrod squares or to 0 .

For conceptual and notational purposes, we consider our endomorphisms as initially defined on the tensor algebra and then defined on $A$ via a presentation. Let $V$ be a vector space of countable dimension over $\mathbf{F}_{2}$. Fix a basis $S_{n}$, $n \geq 1$. Then the tensor algebra $T(V)$, isomorphic to the polynomial algebra $\mathbf{F}_{2}\left\{S_{1}, S_{2}, \cdots\right\}$ in non-commuting variables, has the Steenrod algebra $A$ as a quotient:

$$
\pi: T(V) \longrightarrow A,
$$

where $\pi$ maps $S_{n}$ to $\mathrm{Sq}^{n}$. The kernel $R$, according to the Adem-Wu relations, is generated as ideal by all

$$
S_{x} S_{y}-\sum \epsilon_{k}(x, y) S_{x+y-k} S_{k}
$$

where $2 y>x \geq 1$ and $\epsilon_{k}(x, y)$ is the binomial coefficient $\binom{y-1-k}{x-2 k}$ modulo 2.
Let $\eta$ be a map from the set of indeterminates $\left\{S_{1}, S_{2}, \cdots\right\}$ to $T(V)$ with the property that, if $\eta\left(S_{n}\right) \neq 0$, then $\eta\left(S_{n}\right)$ is itself an indeterminate. Thus we may write $\eta\left(S_{n}\right)=S_{\eta(n)}$ with the convention that, if $\eta\left(S_{n}\right)=0$, then $\eta(n)=-\infty$, i.e., we also interpret $\eta$ as a function from the set $\mathbf{P}$ of positive integers to $\mathbf{P} \cup\{-\infty\}$. Such a map defines an endomorphism of $T(V)$ as (unital) algebra.

If $\eta(R) \subseteq R$, then $\eta$ induces an algebra endomorphism of $A$. We use the same name $\eta$ so that, if $\eta\left(\mathrm{Sq}^{n}\right) \neq 0$, then $\eta\left(\mathrm{Sq}^{n}\right)$ is itself a Steenrod square and we again write $\eta\left(\mathrm{Sq}^{n}\right)=\mathrm{Sq}^{\eta(n)}$, including 0 in the notation as an honorary Steenrod square $0=\mathrm{Sq}^{-\infty}$. As our algebra endomorphisms are taken to be those of unital algebras, $\eta(0)=0$ (if $n>0$, then $\eta(n) \neq 0$ ). Such endomorphisms of $A$ are those which we wish to characterise and any such arises from a corresponding endomorphism of $T(V)$ as above.

Recall that $A$ is minimally generated as unital algebra by the squares $\mathrm{Sq}^{2^{e}}$ with $0 \leq e$ (see [Wo98, p. 454]), so that an algebra homomorphism on $A$ is determined by its images on these elements. In $O$ the Steenrod squares of odd degree themselves form a minimal generating set so that an algebra homomorphism on $O$ is determined by its images on the elements $\mathrm{Sq}^{n}, n$ odd. As $O$ has the presentation $\mathbf{F}_{2}\left\{S_{1}, S_{3}, S_{5}, \cdots\right\} / R_{\text {odd }}$, where $R_{\text {odd }}$ is the ideal generated by all Adem-Wu relations in which only odd superscripts appear, the considerations above apply as well to defining algebra homomorphisms on $O$. Note that in our treatment we consider $O$ as a unital subalgebra. This differs from the usage in Monks and in Wood for whom the odd subalgebra is $O^{+}$ (in the algebras which appear here the superscript + denotes the augmentation ideal, the subalgebra of elements of positive grading).

Our results depend heavily on the parity of certain binomial coefficients. We begin with lemmas on this topic. The parity of a binomial coefficient can be calculated from the dyadic expansions of its entries. We write $d_{i}(n)$ for the $i$ th binary digit of the non-negative integer $n$ so that $n=\Sigma_{i} d_{i}(n) 2^{i}$. Then, for $x, y \geq 0$,

$$
\binom{x}{y} \equiv \prod_{i}\binom{d_{i}(x)}{d_{i}(y)} \bmod 2
$$

[AS72, 24.1.1].
1.1 Lemma. The binomial coefficient $\binom{2 m+1}{m+2}$ is equivalent to 1 modulo 2 if and only if $m=2^{e}-1$ for some $e \geq 1$ or $m=2^{e}-2$ for some $e \geq 2$. Similarly, $\binom{2 m}{m+2} \equiv 1 \bmod 2$ if and only if $m=2^{e}-2$ for some $e \geq 2$.

Proof. We may assume that $m \geq 1$. The sufficiency of the conditions is straightforward. For their necessity let $e$ be maximal such that $d_{e-1}(m)=1$. We show by reverse induction that $d_{i}(m)=1$ for $e-1 \geq i>0$. Suppose that $d_{i}(m)=1$ for $e-1 \geq i>k>0$. If $d_{k}(m)=0$, then $d_{k+1}(2 m+1)=0$ while $d_{k+1}(m+2)=1$. This has the contradictory implication that each of the binomial coefficients of the statement is 0 modulo 2 . Thus, $m=2^{e}-1$ or $m=2^{e}-2$; as $m$ cannot be odd in the second case, $m=2^{e}-2$ there.
1.2 Lemma. Let a be a positive integer. Then $\mathrm{Sq}^{a} \mathrm{Sq}^{a}=\mathrm{Sq}^{2 a-1} \mathrm{Sq}^{1}+S$, where $S$ is a sum of admissible monomials which do not involve $\mathrm{Sq}^{1}$. Moreover, $S=0$ if and only if $a=1$ or $a=2^{f}+1, f \geq 0$, while $\mathrm{Sq}^{a} \mathrm{Sq}^{a}=0$ if and only if $a=1$.

Proof. The first statement is immediate from the Adem-Wu relations. The second statement is clear if $a \leq 2$ and so we assume $a \geq 3$. For $f \geq 1$ and $k>1$,

$$
\epsilon_{k}\left(2^{f}+1,2^{f}+1\right) \equiv\binom{2^{f}+1-1-k}{2^{f}+1-2 k}=\binom{\left(2^{f}-1\right)-(k-1)}{\left(2^{f}-1\right)-2(k-1)} .
$$

Let $i$ be minimal such that $d_{i}(k-1)=1$. Then $d_{i}\left(\left(2^{f}-1\right)-(k-1)\right)=0$ while $d_{i}\left(\left(2^{f}-1\right)-2(k-1)\right)=1$. It follows that $\epsilon_{k}\left(2^{f}+1,2^{f}+1\right)=0$.

To prove the converse, suppose first that $a$ is odd, $a \neq 2^{f}+1$. Then there exist minimal $i, j, j>i>0$, for which $a=2^{j+1} b+2^{j}+2^{i}+1, b \geq 0$. For $k=2^{j-1}+1, \epsilon_{k}(a, a)=1$, which suffices. If $a$ is even and $a>2$, then there exists $j, j \geq 1$, for which $a=2^{j+1} b+2^{j}+2, b \geq 0$. Again for $k=2^{j-1}+1$, $\epsilon_{k}(a, a)=1$, which concludes the proof.

## 2. Constructions and characterisations

Our classification of endomorphisms like $\gamma$ calls forth a host of much more limited maps. In [Wo98, p. 455] the notation $A(0)$ is used for the subalgebra $\mathbf{F}_{2}+\mathbf{F}_{2} \mathrm{Sq}^{1}$ of $A$. Let $x \geq 1$; using the procedure discussed in the previous section, define the projection $\pi_{x}$ from $A$ to $A(0)$ by $\pi_{x}\left(\mathrm{Sq}^{n}\right)=\delta_{x, n} \mathrm{Sq}^{1}$ for $n \geq 1$ (Kronecker $\delta$ ). The squares $\mathrm{Sq}^{2^{e}}, e \geq 0$, form a minimal generating set for $A$. It follows that, if $n \neq 2^{e}$ for some $e$, then $\mathrm{Sq}^{n} \in\left(A^{+}\right)^{2}$; as $\left(A(0)^{+}\right)^{2}=0$, such $\mathrm{Sq}^{n}$ lie in the kernel of any algebra homomorphism from $A$ to $A(0)$. Indeed, $\pi_{x}$ is an algebra homomorphism if and only if $x$ is a power of 2 . More generally, if $T$ is a set of such powers, finite or infinite, define the map $\pi_{T}$ via

$$
\pi_{T}\left(\mathrm{Sq}^{n}\right):=\left\{\begin{array}{cl}
\mathrm{Sq}^{1} & \text { if } n \in T \\
0 & \text { otherwise }
\end{array}\right.
$$

Then $\pi_{T}\left(\mathrm{Sq}^{n}\right)$ is an algebra homomorphism, which we view here as an algebra endomorphism of $A$. Except for $T=\emptyset$ in which case $\pi_{\emptyset}$ is the projection of $A$ onto the ground field, i.e., $\pi_{\emptyset}=\varepsilon$, the augmentation homomorphism of $A$ as Hopf algebra, $\pi_{T}$ maps $A$ onto $A(0)$. Restricted to $A^{+}$the maps $\pi_{T} \in$ $\operatorname{End}_{\mathbf{F}_{2}}\left(A^{+}\right)$satisfy a Boolean condition: $\pi_{T}+\pi_{U}=\pi_{T \vee U}$, where, so restricted, $\pi_{\emptyset}=0$; in this setting we may write $\pi_{T}=\Sigma_{t \in T} \pi_{t}$.

The endomorphisms of $A$ which we study here form a monoid under composition. Its multiplication table is indicated below. The identity map on $A$ is taken here to be a power of $\gamma, 1_{A}=\gamma^{0}$.

## Multiplication table

|  | $\gamma^{j}$ | $\pi_{U}$ |
| :--- | :--- | :--- |
| $\gamma^{i}$ | $\gamma^{i+j}$ | $\varepsilon$ |
| $\pi_{T}$ | $\pi_{2^{j} T}$ | $\pi_{V}$ |

Here $i, j \geq 1$ and $T, U, V$ are sets of powers of 2 with

$$
V= \begin{cases}U & \text { if } 1 \in T \\ \emptyset & \text { otherwise } .\end{cases}
$$

With the requisite notation now in place, we state our result concerning the endomorphisms of the Steenrod algebra.
2.1 Theorem. Let $\eta$ be an endomorphism of the Steenrod algebra with the property that, if $\eta\left(\mathrm{Sq}^{n}\right) \neq 0, n \geq 1$, then $\eta\left(\mathrm{Sq}^{n}\right)$ is itself a Steenrod square. Then $\eta$ is a power of $\gamma$ or $\eta$ is a map $\pi_{T}$ to $A(0)$ for a set $T$ of powers of 2. If $\eta$ is a monomorphism, then $\eta=1_{A}$.

Proof. The discussion above shows that, if $\operatorname{Im} \eta \subseteq A(0)$, then $\eta$ is a projection $\pi_{T}$. We may thus assume in what follows that there are values of $\eta$ (in its guise as a map defined on $\mathbf{P}$ ) which are strictly greater than 1 . The hypothesis implies that there are few possibilities for the images of $\mathrm{Sq}^{1}$ and $\mathrm{Sq}^{2}$. As $\mathrm{Sq}^{1} \mathrm{Sq}^{1}=0$, applying $\eta$ gives $\mathrm{Sq}^{\eta(1)} \mathrm{Sq}^{\eta(1)}=0$. By Lemma 1.2, $\eta(1) \leq 1$.

From $\mathrm{Sq}^{2} \mathrm{Sq}^{2}=\mathrm{Sq}^{3} \mathrm{Sq}^{1}$, we obtain

$$
\mathrm{Sq}^{\eta(2)} \mathrm{Sq}^{\eta(2)}=\mathrm{Sq}^{\eta(3)} \mathrm{Sq}^{\eta(1)}
$$

If $\eta(1)=-\infty$, then, as before, $\eta(2) \leq 1$. Suppose that $\eta(1)=1$. As $\mathrm{Sq}^{3}=$ $\mathrm{Sq}^{1} \mathrm{Sq}^{2}$, we have

$$
\mathrm{Sq}^{\eta(2)} \mathrm{Sq}^{\eta(2)}=\mathrm{Sq}^{1} \mathrm{Sq}^{\eta(2)} \mathrm{Sq}^{1}
$$

If $\eta(2) \geq 2$, then the left-hand side is not 0 so that $\eta(2)$ is even and the righthand side is $\mathrm{Sq}^{1+\eta(2)} \mathrm{Sq}^{1}$, an admissible. Comparison of degrees shows that $\eta(2)=2$. In conclusion, $\eta(2) \leq 2$.

Suppose first that $\eta(1)=1$. If $\eta(2)=2$, then $\eta=1_{A}$. For this we prove by induction that $\eta(n)=n$ for all $n$ by applying $\eta$ to the identity

$$
\mathrm{Sq}^{2} \mathrm{Sq}^{n-1}=\epsilon_{0}(2, n-1) \mathrm{Sq}^{n+1}+\mathrm{Sq}^{n} \mathrm{Sq}^{1}
$$

for $n \geq 3$. If $\eta(2) \leq 1$, then $\eta(n) \leq 1$ for all $n, n \geq 1$, the condition which implies that $\eta$ is a projection $\pi_{T}$. This follows by induction, the induction step proceeding by applying $\eta$ to the previous identity for $n \geq 3$. Now the lefthand side is sent to 0 while the image of the right-hand side includes the term $\mathrm{Sq}^{\eta(n)} \mathrm{Sq}^{1}$ and so $\mathrm{Sq}^{\eta(n)}=0$. In conclusion, if $\eta(1)=1$, then $\eta=1_{A}$.

As $\eta(1) \neq 0$, the remaining possibility is $\eta(1)=-\infty$. Now $\eta(n)=-\infty$ for all odd $n, n \geq 3$, as can be seen by applying $\eta$ to $\mathrm{Sq}^{n}=\mathrm{Sq}^{1} \mathrm{Sq}^{n-1}$. Since $A \mathrm{Sq}^{1} A$, the two-sided ideal generated by $\mathrm{Sq}^{1}$, is in the kernel of $\eta$, it follows that $\eta$ induces a homomorphism from $A / A \mathrm{Sq}^{1} A$ to $A$. Moreover this ideal has as basis all admissibles of the form $\mathrm{Sq}^{\mathrm{a}}$ for which at least one entry in $\mathbf{a}$ is odd. It thus coincides with Ker $\gamma$ [SE62, p. 24].

Imitating [Wo98, p. 488], we define an endomorphism of the algebra $T(V)$ called $\gamma^{-1}$ by setting $\gamma^{-1}\left(S_{n}\right)=S_{2 n}$, which, however, does not induce an algebra endomorphism of $A$. It does induce an algebra homomorphism from $A$ onto $A / A \mathrm{Sq}^{1} A$ which is indeed the inverse of the isomorphism which $\gamma$ induces from $A / A \mathrm{Sq}^{1} A$ onto $A$. For ease of notation, we use the same names of the mappings in the context of the quotient algebras.

We now use the fact that $\eta$ is determined by its action on the elements $\mathrm{Sq}^{2}{ }^{e}$ for $e \geq 0$. To conclude the proof, we induct on $e, e \geq 0$, that, if

$$
\eta(1)=\eta(2)=\cdots=\eta\left(2^{e-1}\right)=-\infty
$$

and if $\eta\left(2^{e}\right) \geq 1$, then $\eta=\gamma^{e}$. We have seen earlier that this is so for $e=0$, i.e., that $\eta(1)=1$ implies that $\eta=1_{A}=\gamma^{0}$. For $e>0$, the composite homomorphism $\eta \gamma^{-1}$ is an algebra endomorphism of $A$ for which

$$
\eta \gamma^{-1}(1)=\eta \gamma^{-1}(2)=\cdots=\eta \gamma^{-1}\left(2^{e-2}\right)=-\infty
$$

and $\eta \gamma^{-1}\left(2^{e-1}\right) \geq 1$. By induction it follows that $\eta \gamma^{-1}=\gamma^{e-1}$ and so $\eta=\gamma^{e}$, as required.

We now turn our attention to the odd subalgebra. Again there is a host of projections to $A(0)$, a subalgebra of $O$, now obtained from the minimal generators $\mathrm{Sq}^{x}, x$ odd. The maps $\pi_{x}$ for odd $x$ restrict to algebra endomorphisms of $O$. Here we have a map $\pi_{M}$ for each set $M$ of odd numbers which, except for $M=\emptyset$, maps $O$ onto $A(0)\left(\pi_{\emptyset}\right.$ is again the augmentation homomorphism, here in the context of $O$ ). The other remarks about the projections from $A$ apply in this setting.

In the next result we apply to $O$ the same considerations and conventions set out in the introduction for $A$ concerning linear maps defined initially only on Steenrod squares.
2.2 Proposition. Let $m$ be a positive odd integer, and $f \geq 1$. Define a linear transformation $\mu$ from the odd subalgebra $O$ to itself by letting

$$
\mu\left(\mathrm{Sq}^{n}\right):=\left\{\begin{array}{cl}
1 & \text { if } n=0 \\
\mathrm{Sq}^{2 f}(p-1)+1 & \text { if } n=(m+1) p-1 \text { for } p \geq 1 \\
0 & \text { otherwise } .
\end{array}\right.
$$

If $\mu$ is an algebra endomorphism, then there is $e \geq 1$ such that $m=2^{e}-1$.

Proof. By replacing $\mu$ by $\lambda^{-(f-1)} \mu$, we may assume that $f=1$.
Suppose now that $\mu$ is an algebra endomorphism. By the assumption and the hypotheses,

$$
\mu\left(\mathrm{Sq}^{3(m+1)-1}\right) \mu\left(\mathrm{Sq}^{3(m+1)-1}\right)=\mathrm{Sq}^{5} \mathrm{Sq}^{5}=\mathrm{Sq}^{9} \mathrm{Sq}^{1} .
$$

As $\mu(x)=-\infty$ if $x \neq(m+1) p-1$ for some $p$, modulo $\operatorname{Ker} \mu$ and with $\epsilon:=$ $\epsilon_{m}(3 m+2,3 m+2)$,

$$
\mathrm{Sq}^{3 m+2} \mathrm{Sq}^{3 m+2} \equiv \epsilon \mathrm{Sq}^{5 m+4} \mathrm{Sq}^{m}=\epsilon \mathrm{Sq}^{5(m+1)-1} \mathrm{Sq}^{m}
$$

whose image under $\mu$ is $\epsilon \mathrm{Sq}^{9} \mathrm{Sq}^{1}$. Thus,

$$
\epsilon=\binom{3 m+2-1-m}{3 m+2-2 m}=\binom{2 m+1}{m+2} \equiv 1 \bmod 2 .
$$

By Lemma 1.1, $m=2^{e}-1$ for some $e \geq 1$ as required.

The converse of this proposition is also true, as can be seen by applying the method described in the previous section. Hereafter $\mu$ will denote the one specific linear transformation of $O$ defined as in the proposition by

$$
\mu\left(\mathrm{Sq}^{4 p-1}\right)=\mathrm{Sq}^{2 p-1}, p \geq 1
$$

and $\mu\left(\mathrm{Sq}^{n}\right)=0$ for all other positive $n$. In the next section we also provide a detailed proof that $\mu$ is an endomorphism, which is incidental to establishing the formulae for the action of $\mu$ on the Milnor basis. For $e \geq 0, \mu^{e}$ is the endomorphism of $O$ given as

$$
\mu^{e}\left(\mathrm{Sq}^{2^{e+1} p-1}\right)=\mathrm{Sq}^{2 p-1}, p \geq 1,
$$

and $\mu^{e}\left(\mathrm{Sq}^{n}\right)=0$ for all other positive $n$. Its kernel is is an admissible ideal, i.e., one with a basis of admissible monomials. In the statement, $\ell(\mathbf{x})$ denotes the length of a vector $\mathbf{x}$.
2.3 Proposition. The ideal $\operatorname{Ker} \mu^{e}, e \geq 0$, is the subspace spanned by all monomials $\mathrm{Sq}^{\mathbf{x}}$ of $O$ for which there is an index $j$, with $1 \leq j \leq \ell(\mathbf{x})$, for which $x_{j} \not \equiv-1 \bmod 2^{e+1}$. The same statement holds when the monomials are restricted to being admissible. The quotient space $\operatorname{Coim} \mu^{e}$, isomorphic to $O$,
is spanned by the cosets of all admissible $\mathrm{Sq}^{\mathbf{a}}$ for which $a_{j} \equiv-1 \bmod 2^{e+1}$, $1 \leq j \leq \ell(\mathbf{a})$.

Proof. We may take $e$ positive. Let $U$ denote the subspace described; it is clear that it is contained in $\operatorname{Ker} \mu^{e}$ and that it is an ideal. We show first that it is admissible. Our proof that each of the defining monomials $\mathrm{Sq}^{\mathbf{x}}$ of $U$ is a linear combination of admissibles which satisfy the defining condition of $U$, is by induction, first on $\ell(\mathbf{x})$, and then on $\mathbf{x}$ in the right lexicographic order. The base cases are trivial: $\ell(\mathbf{x})=1$, and, for fixed $\ell>1, x_{i}=1$ for all $i, 1 \leq i \leq \ell=\ell(\mathbf{x})$.

Let $\mathbf{x}=\left(x_{1}, x_{2}, \cdots, x_{\ell}\right)$ be strictly greater than $(1,1, \cdots, 1)$, and suppose that $\mathrm{Sq}^{\mathbf{x}}$ satisfies the defining condition of $U$. If there is an index $i$ such that $x_{i} \not \equiv-1 \bmod 2^{e}$ and $i \leq \ell-1$, then, by induction on length, we may assume that $\left(x_{1}, x_{2}, \cdots, x_{\ell-1}\right)$ is admissible. If there is no such index, then, by expressing $\left(x_{1}, x_{2}, \cdots, x_{\ell-1}\right)$ as a sum of admissibles (which in $O$ still have length $\ell-1$ ), we may again assume that $\left(x_{1}, x_{2}, \cdots, x_{\ell-1}\right)$ is admissible.

If $\mathbf{x}$ is not admissible, then $x_{\ell-1}<2 x_{\ell}$. Writing $x=x_{\ell-1}$ and $y=x_{\ell}$, we see from the Adem-Wu relations that

$$
\mathrm{Sq}^{x} \mathrm{Sq}^{y}=\sum_{k \text { odd }, 1 \leq k<x / 2} \epsilon_{k}(x, y) \mathrm{Sq}^{x+y-k} \mathrm{Sq}^{k} .
$$

If there is an index $i, 1 \leq i \leq \ell-2$, with $x_{i} \not \equiv-1 \bmod 2^{e}$, then we are done by induction on right lexicographic order. If not then either $x$ or $y$ is not equivalent to $-1 \bmod 2^{e}$.

If there is $k, 1 \leq k<x / 2$, for which both $k$ and $x+y-k$ are equivalent to -1 $\bmod 2^{e}$, then $\epsilon_{k}(x, y)=0$. To see this, write $x=2^{e} p+u, y=2^{e} q+v$, and $k=$ $2^{e} r+\left(2^{e}-1\right)$, where $1 \leq u, v \leq 2^{e}-1$. By hypothesis, $u+v \leq\left(2^{e}-1\right)+\left(2^{e}-3\right)$. As $u+v \equiv-2$, it follows that $(u+2)+v=2^{e}$. Thus, $d_{j}(u+2)=1-d_{j}(v)$ if $1 \leq j \leq e-1$. Now

$$
\epsilon_{k}(x, y) \equiv\binom{y-1-k}{x-2 k}=\binom{2^{e}(q-(r+1))+v}{2^{e}(p-2(r+1))+u+2} .
$$

Since $q-(r+1) \geq 0$ and $p-2(r+1) \geq 0$, we may write

$$
\epsilon_{k}(x, y) \equiv\binom{q-(r+1)}{p-2(r+1)}\binom{d_{e-1}(v)}{1-d_{e-1}(v)} \cdots\binom{d_{1}(v)}{1-d_{1}(v)}\binom{1}{1}
$$

As $v \leq 2^{e}-3$, there is an index $j, 1 \leq j \leq e-1$, for which $d_{j}(v)=0$. It follows that $\epsilon_{k}(x, y)=0$.

We thus see that either $\mathbf{x}$ is admissible or $\mathrm{Sq}^{\mathbf{x}}$ is a sum of monomials in $U$, each of whose vectors of superscripts is strictly below $\mathbf{x}$ in the right lexicographic order, so that the argument concludes on applying the second induction.

The cosets of the admissibles described in the last assertion of the proposition comprise a basis for $O / U$. To finish the proof of the proposition it suffices to show that a sum of such admissibles is not sent to 0 by $\mu^{e}$. Let $\mathrm{Sq}^{\text {a }}$ be such that $a_{j} \equiv-1 \bmod 2^{e+1}, 1 \leq j \leq \ell=\ell(\mathbf{a})$. Then

$$
\mu^{e}\left(\mathrm{Sq}^{\mathbf{a}}\right)=\mathrm{Sq}^{2 a_{1}-1} \cdots \mathrm{Sq}^{2 a_{\ell}-1}
$$

an admissible. Moreover, different such admissibles $\mathrm{Sq}^{\mathbf{a}}$ are sent to distinct admissible images $\mu^{e}\left(\mathrm{Sq}^{\mathbf{a}}\right)$. This establishes the proposition.

These ideals form a strictly increasing chain: $\operatorname{Ker} \mu^{0}=\operatorname{Ker} 1_{O}=0$ and, for $e \geq 1$, $\operatorname{Ker} \mu^{e-1} \subset \operatorname{Ker} \mu^{e}$. The maps $\mu^{e}$ can be factored through the coimages. For example, using the cosets of the admissible basis we define an algebra isomorphism from $\operatorname{Coim} \mu^{e}$ to $\operatorname{Coim} \mu^{e-1}$ for $e \geq 1$ by sending the coset of $\mathrm{Sq}^{2^{e+1} p-1}, p \geq 1$, to the coset of $\mathrm{Sq}^{2^{e} p-1}$. We have thus constructed a sequence of isomorphisms

$$
\operatorname{Coim} \mu^{e} \longrightarrow \operatorname{Coim} \mu^{e-1} \longrightarrow \cdots \longrightarrow \operatorname{Coim} \mu \longrightarrow \operatorname{Coim} 1_{O}=O .
$$

When preceded by the natural projection the composite gives the epimorphism $\mu^{e}: O \rightarrow O$.

Before stating our result concerning the endomorphisms of $O$ we describe the monoid of those non-zero endomorphisms so far considered. We begin with a multiplication table of the non-identity endomorphisms.

## Multiplication table

|  | $\lambda^{i^{\prime}}$ | $\mu^{j^{\prime}}$ | $\lambda^{i^{\prime}} \mu^{j^{\prime}}$ | $\pi_{M^{\prime}}$ |
| :--- | :--- | :--- | :--- | :--- |
| $\lambda^{i}$ | $\lambda^{i+i^{\prime}}$ | $\lambda^{i} \mu^{j^{\prime}}$ | $\lambda^{i+i^{\prime}} \mu^{j^{\prime}}$ | $\pi_{M^{\prime}}$ |
| $\mu^{j}$ | 0 | $\mu^{j+j^{\prime}}$ | 0 | 0 |
| $\lambda^{i} \mu^{j}$ | 0 | $\lambda^{i} \mu^{j+j^{\prime}}$ | 0 | 0 |
| $\pi_{M}$ | $\pi_{M_{1}}$ | $\pi_{M_{2}}$ | $\pi_{M_{3}}$ | $\pi_{M_{4}}$ |

Here $i, i^{\prime}, j, j^{\prime} \geq 1$ and $M, M^{\prime}$ are sets of positive odd numbers while

$$
\begin{array}{cc}
M_{1}= & \left\{2 p+1 \mid 2^{i^{\prime}+1} p+1 \in M, p \geq 0\right\} \\
M_{2}= & \left\{2^{j^{\prime}+1} p-1 \mid 2 p-1 \in M, p \geq 1\right\}, \\
M_{3}= & \left\{2^{j^{\prime}+1} p-1 \mid 2^{i^{\prime}+1}(p-1)+1 \in M, p \geq 1\right\}, \\
& M_{4}= \begin{cases}M^{\prime} & \text { if } 1 \in M \\
\emptyset & \text { otherwise }\end{cases}
\end{array}
$$

and

As shown in the next theorem, the monoid of endomorphisms of $O$ which send squares to squares or to 0 comprises precisely the set of products $\lambda^{i} \mu^{j}$ for $i, j \geq 0$ (by convention, $\lambda^{0}=\mu^{0}=1_{O}$ ), the set of projections and the 0 map.

Next we give a table of the values of these endomorphisms, suppressing those which are zero, i.e., if, for an endomorphism $\eta$ and an odd integer $n$, no value for $\eta\left(\mathrm{Sq}^{n}\right)$ appears in the table, then $\eta\left(\mathrm{Sq}^{n}\right)=0$ (recall that $\eta\left(\mathrm{Sq}^{0}\right)=\eta\left(1_{O}\right)=1$ as $\eta$ is a homomorphism of unital algebras). For an example, a notable one, if $p \geq 0, \lambda \mu\left(\mathrm{Sq}^{4 p+3}\right)=\mathrm{Sq}^{4 p+1}$ while $\lambda \mu\left(\mathrm{Sq}^{4 p+1}\right)=0$.

## Table of non-zero values

$$
\left.\begin{array}{ll}
\lambda^{i}\left(\mathrm{Sq}^{2 p+1}\right) & =\mathrm{Sq}^{2^{i+1} p+1}, i, p \geq 0 \\
\mu^{j}\left(\mathrm{Sq}^{2^{j+1} p-1}\right) & =\mathrm{Sq}^{2 p-1}, p \geq 1, j \geq 0 \\
\lambda^{i} \mu^{j}\left(\mathrm{Sq}^{2+1} p-1\right.
\end{array}\right)=\mathrm{Sq}^{2^{i+1}(p-1)+1}, p \geq 1, i, j \geq 0, ~\left(\mathrm{Sq}^{1}, p \geq 0,2 p+1 \in M .\right.
$$

Thus, $\operatorname{Ker} \lambda^{i}=0$ and

$$
\operatorname{Im} \lambda^{i}=\Sigma\left\{\mathbf{F}_{2} \mathrm{Sq}^{\mathbf{x}} \mid x_{j} \equiv 1 \bmod 2^{i+1}, 1 \leq j \leq \ell(\mathbf{x})\right\}
$$

while
$\operatorname{Ker} \mu^{i}=\Sigma\left\{\mathbf{F}_{2}\right.$ Sq $^{\mathbf{x}} \mid$ there exists $j, 1 \leq j \leq \ell(\mathbf{x})$, with $\left.x_{j} \not \equiv-1 \bmod 2^{i+1}\right\}$,
as already noted, and $\operatorname{Im} \mu^{i}=O$. In the descriptions of $\operatorname{Im} \lambda^{i}$ and of $\operatorname{Ker} \mu^{i}$, admissible vectors of superscripts can be taken in place of arbitrary ones; thus, these subspaces have bases of admissible monomials.
2.4 Theorem. Let $\eta$ be an endomorphism of the odd subalgebra $O$ of the Steenrod algebra with the property that, if $\eta\left(\mathrm{Sq}^{n}\right) \neq 0$, then $\eta\left(\mathrm{Sq}^{n}\right)$ is itself a Steenrod square. Then $\eta$ lies in the monoid generated by $\mu, \lambda$ and the projections $\pi_{M}$, where $M$ is a set of odd numbers.

Proof. Assume that $\eta \neq 0$ and that $\eta$ is not a projection. Let $m$ be minimal such that $\eta(m)>0$. Applying $\eta$ to the Adem-Wu expansion

$$
\mathrm{Sq}^{m} \mathrm{Sq}^{m}=\sum_{k} \epsilon_{k}(m, m) \mathrm{Sq}^{2 m-k} \mathrm{Sq}^{k}
$$

we find that $\mathrm{Sq}^{\eta(m)} \mathrm{Sq}^{\eta(m)}=0$ since $\eta(k)=-\infty$ if $k<m$. By Lemma 1.2 $\eta(m)=1$. A similar argument shows that, for $m<n<2 m+1, \mathrm{Sq}^{\eta(n)} \mathrm{Sq}^{1}=0$ so that $\eta(n) \leq 1$.

As $\eta$ is not a projection, it takes values strictly greater than 1 . But then the least element on which $\eta$ takes such a value is of the form $n+(m+1), m \leq n$. If $m<n$, applying $\eta$ to the Adem-Wu expansion

$$
\mathrm{Sq}^{2 m+1} \mathrm{Sq}^{n}=\sum_{k} \epsilon_{k}(2 m+1, n) \mathrm{Sq}^{2 m+1+n-k} \mathrm{Sq}^{k}
$$

we find that $\mathrm{Sq}^{\eta(2 m+1)} \mathrm{Sq}^{\eta(n)}=\mathrm{Sq}^{\eta(n+(m+1))} \mathrm{Sq}^{1}$ since $\epsilon_{m}(2 m+1, n)=1$. But the assumption that $\eta(2 m+1) \leq 1$ implies that the left-hand side is 0 whereas the right-hand side is not. Thus, $\eta(2 m+1)>1$.

The previous equation for the case $n=2 m+1$ yields $\mathrm{Sq}^{\eta(2 m+1)} \mathrm{Sq}^{\eta(2 m+1)}=$ $\mathrm{Sq}^{\eta(3 m+2)} \mathrm{Sq}^{1}$. By Lemma 1.2, $\eta(2 m+1)=2^{f}+1, f>0$. Comparison of degrees in that same equation shows that $\eta(n+(m+1))=\eta(n)+2^{f}$ if $\eta(n)>0$. Thus, $\operatorname{Im} \eta=\operatorname{Im} \lambda^{f-1}$, and, as in the proof of Proposition 2.2, we may replace $\eta$ by
$\lambda^{-(f-1)} \eta$, i.e., we may assume that $f=1$. In particular, we may assume that $\eta(2 m+1)=3$ and $\eta(n+(m+1))=\eta(n)+2$ whenever $n>m$ and $\eta(n)>0$.

We next show that $\eta(n)>0$ implies that $n \equiv-1 \bmod m+1$. Let $n$ be minimal not of this form for which $\eta(n)>0$. We have already shown above that, if $m<n<2 m+1$, then $\eta(n)=1$. If $n>2 m+1$ and so $\eta(n-(m+1))=-\infty$, then $\eta(n)=1$ since then $\mathrm{Sq}^{\eta(2 m+1)} \mathrm{Sq}^{\eta(n-(m+1))}=0$. Now apply $\eta$ to the Adem-Wu expansion

$$
\mathrm{Sq}^{n+(m+1)} \mathrm{Sq}^{n}=\sum_{k} \epsilon_{k}(n+(m+1), n) \mathrm{Sq}^{2 n+(m+1)-k} \mathrm{Sq}^{k}
$$

to obtain
$\mathrm{Sq}^{3} \mathrm{Sq}^{1}=\sum \epsilon_{i(m+1)-1}(n+(m+1), n) \mathrm{Sq}^{\eta(2 n+(m+1)-(i(m+1)-1))} \mathrm{Sq}^{\eta(i(m+1)-1)}$,
where the sum is over all $i \geq 1$ for which $i(m+1)<n$. But $\eta(i(m+1)-1)=$ $2 i-1$ so that, for $i>2$, the $i$ th term, if non-zero, is of degree $\geq 5$, which is incompatible with the left-hand side of degree 4 . For $i=2$, to be of degree 4 the second term would have to be $\mathrm{Sq}^{1} \mathrm{Sq}^{3}$ which is 0 . For $i=1$,

$$
\epsilon_{m}(n+(m+1), n) \equiv\binom{n-1-m}{n+(m+1)-2 m}=\binom{n-(m+1)}{n-(m+1)+2}=0,
$$

the final contradiction to the supposition. By Proposition 2.2, there is $e \geq 0$ for which $\eta=\mu^{e}$, as required.

## 3. Milnor basis

While Monks developed his map $\lambda$ in order to investigate nilpotence degrees of elements, our result shows that it could have been uncovered simply by studying its defining property. It may be that there are similarly useful maps, even on $A$ itself, to be called into being by positing weaker properties such as sending admissibles to admissibles. A potential difficulty in such an approach, underplayed here, is establishing that such a map is a homomorphism. The method for doing so which is described in Sect. 1, i.e., in the circle of ideas of the admissible basis, is straightforward to apply in the cases discussed. This section provides an alternative and direct approach as a corollary of the following proposition which states the formulae for our endomorphisms in terms of the Milnor basis. Details are given only in the case of $\mu$.

We begin by stating the formulae which define our maps in the Milnor basis. The formulae agree with the previous definitions on Steenrod squares, multiplicative generators of our algebras. Showing in each case that the formulae define a multiplicative mapping thus establishes the correctness of the formulae in addition to the fact that the map is an endomorphism.
3.1 Proposition. On the Milnor basis, the maps $\gamma, \pi_{T}, \lambda, \mu$, and $\pi_{N}$ send $1=\mathrm{Sq}(\mathbf{0})$ to 1 and all other Milnor basis elements in $A$ and $O$, respectively, to 0 with the following exceptions:
$\gamma$ sends each element

$$
\mathrm{Sq}\left(2 p_{1}, \cdots, 2 p_{\ell}\right) \text { to } \operatorname{Sq}\left(p_{1}, \cdots, p_{\ell}\right),
$$

where $p_{i} \geq 0,1 \leq i \leq \ell$;
$\pi_{T}$ sends each element $\mathrm{Sq}(t)$ to $\mathrm{Sq}(1)$, where $T$ is a set of powers of 2 and $t \in T$;
$\lambda$ sends each element

$$
\mathrm{Sq}\left(2 p_{1}+1, \cdots, 2 p_{\ell-1}+1,2 p_{\ell}+1\right) \text { to } \operatorname{Sq}\left(4 p_{1}+3, \cdots, 4 p_{\ell-1}+3,4 p_{\ell}+1\right),
$$

where $p_{i} \geq 0,1 \leq i \leq \ell$;
$\mu$ sends each element

$$
\mathrm{Sq}\left(4 p_{1}+1, \cdots, 4 p_{\ell-1}+1,4 p_{\ell}+3\right) \text { to } \mathrm{Sq}\left(2 p_{1}+1, \cdots, 2 p_{\ell-1}+1,2 p_{\ell}+1\right)
$$

where $p_{i} \geq 0,1 \leq i \leq \ell$;
$\pi_{M}$ sends each element $\mathrm{Sq}(m)$ to $\mathrm{Sq}(1)$, where $M$ is a set of positive odd numbers and $m \in M$.

The formulae for composites are readily derived. That for $\lambda \mu$ is particularly striking. Namely, $\lambda \mu$ sends each element

$$
\operatorname{Sq}\left(4 p_{1}+1, \cdots, 4 p_{\ell-1}+1,4 p_{\ell}+3\right) \text { to } \mathrm{Sq}\left(4 p_{1}+3, \cdots, 4 p_{\ell-1}+3,4 p_{\ell}+1\right)
$$

where $p_{i} \geq 0,1 \leq i \leq \ell$, and all other non-identity Milnor basis elements to 0 . As with the admissible basis, the subspaces associated with these endomorphisms have bases of Milnor basis elements. For example,

$$
\operatorname{Im} \lambda^{i}=\Sigma\left\{\mathbf{F}_{2} \operatorname{Sq}(\mathbf{r}) \mid r_{j} \equiv 1 \bmod 2^{i}, 1 \leq j \leq \ell(\mathbf{r})\right\}
$$

while
$\operatorname{Ker} \mu^{i}=\Sigma\left\{\mathbf{F}_{2} \operatorname{Sq}(\mathbf{r}) \mid\right.$ there exists $j, 1 \leq j \leq \ell(\mathbf{r})$, with $\left.r_{j} \not \equiv-1 \bmod 2^{i+1}\right\}$.

Proof of 3.1. The formula for $\gamma$ is well-known. It can be established by the same lengthy argument given below for the more complicated formula holding for the endomorphism $\mu$. Note that [SE62, p. 24] only gives the formula for $\gamma$ in terms of the admissible basis - and calls the map $\lambda^{*}$.

That for $\lambda$ is given in [Mo92; Wo98, p. 489]. For $\lambda$, establishing multiplicativity has required a fair amount of effort when defined using the Milnor basis, much more so than a proof of multiplicativity based on the universal property of the tensor algebra.

The formulae for $\pi_{T}$ follow from the fact that all Milnor basis elements $\mathrm{Sq}(\mathbf{r}) \in A^{+}$lie in $\left(A^{+}\right)^{2}$ except for those of the form $\mathrm{Sq}\left(2^{e}\right)$, where $e \geq 0$. Those for $\pi_{M}$ rely on the fact that $\mathrm{Sq}(\mathbf{r}) \notin\left(O^{+}\right)^{2}$ if and only if $\ell(\mathbf{r})=1$.

It remains to deal with $\mu$. Let $B$ be an algebra and let $\phi: A \longrightarrow B$ be a linear transformation whose values on the Milnor basis are given. Then $\phi$ is an algebra homomorphism if, for all $\mathbf{r}$ and $s$,

$$
\phi(\operatorname{Sq}(\mathbf{r}) \operatorname{Sq}(s))=\phi(\operatorname{Sq}(\mathbf{r})) \phi(\operatorname{Sq}(s))
$$

Each of our mappings $\phi$ preserve the identity, i.e., $\phi(\operatorname{Sq}(\mathbf{0}))=\phi(1)=1$, and so we may assume that $\mathbf{r} \neq \mathbf{0}$ and $s>0$. But if $\mathbf{r}=\left(r_{1}, \cdots, r_{\ell}\right), \ell>0$, and $s>0$, then the product $\mathrm{Sq}(\mathbf{r}) \mathrm{Sq}(s)$ is a sum of Milnor basis elements $\mathrm{C}(\mathbf{r}, s, \mathbf{g})$, or simply $\mathrm{C}(\mathbf{g})$ when $\mathbf{r}$ and $s$ are understood, corresponding to vectors $\mathbf{g}=\left(g_{1}, \cdots, g_{\ell}\right), g_{i} \geq 0$, such that $r_{i} \geq 2 g_{i}, 1 \leq i \leq \ell$, and $s \geq \sum_{1 \leq i \leq \ell} g_{i}$. The element $\mathrm{C}(\mathbf{g})$ is defined as
$\mathrm{Sq}\left(r_{1}-2 g_{1}+s-\sum_{1 \leq i \leq \ell} g_{i}, r_{2}-2 g_{2}+g_{1}, \cdots, r_{i+1}-2 g_{i+1}+g_{i}, \cdots, r_{\ell}-2 g_{\ell}+g_{\ell-1}, g_{\ell}\right)$.
Write $\mathrm{NZ}=\mathrm{NZ}(\mathbf{r}, s)$ for the set of those $\mathbf{g}$ for which each of the multinomial coefficients

$$
\left(r_{1}-2 g_{1}, s-\sum_{1 \leq i \leq \ell} g_{i}\right),\left(r_{2}-2 g_{2}, g_{1}\right), \cdots,\left(r_{i+1}-2 g_{i+1}, g_{i}\right), \cdots,\left(r_{\ell}-2 g_{\ell}, g_{\ell-1}\right)
$$

is 1 ; the expression $(a, b)$ denotes the multinomial coefficient interpreted modulo 2 and is 1 if and only if the dyadic expansions of $a$ and $b$ have no 1 's in common [Ma83, p. 230] (i.e., $(a, b)=\binom{a+b}{b}$ modulo 2). Then the product is obtained as

$$
\mathrm{Sq}(\mathbf{r}) \mathrm{Sq}(s)=\sum_{\mathbf{g} \in \mathrm{NZ}} \mathrm{C}(\mathbf{g}) .
$$

Note that, as $\mathbf{g}$ is determined by $\mathrm{C}(\mathbf{r}, s, \mathbf{g})$, there is no cancellation in this sum.
For products of Milnor basis elements in the subalgebra $O$, there are strong restrictions on the vectors $\mathbf{g}$ in NZ. Let $\mathrm{Sq}(\mathbf{r})$ and $\mathrm{Sq}(s)$ be in $O$ so that, if $\mathbf{r}=\left(r_{1}, \cdots, r_{\ell}\right)$, then $r_{1}, \cdots, r_{\ell}$ and $s$ are odd according to Monks' original definition of $O$ [Mo92, p. 402]. Let $\mathbf{g} \in \mathrm{NZ}(\mathbf{r}, s)$. As $1=\left(r_{i+1}-2 g_{i+1}, g_{i}\right)$ for $1 \leq i \leq \ell-1, g_{i}$ is even in this range. Also, since $1=\left(r_{1}-2 g_{1}, s-\sum_{1 \leq i \leq \ell} g_{i}\right)$, $g_{\ell}$ is odd.

We now prove that $\mu(\operatorname{Sq}(\mathbf{r}) \operatorname{Sq}(s))=\mu(\operatorname{Sq}(\mathbf{r})) \mu(\operatorname{Sq}(s))$. First assume that $\mathbf{r}=\left(4 p_{1}+1, \cdots, 4 p_{\ell-1}+1,4 p_{\ell}+3\right)$ and $s=4 q+3$, where $p_{i} \geq 0,1 \leq i \leq \ell$, and $q \geq 0$. Thus $\mu(\operatorname{Sq}(\mathbf{r}))=\operatorname{Sq}\left(\mathbf{r}^{\prime}\right)$, where $\mathbf{r}^{\prime}=\left(2 p_{1}+1, \cdots, 2 p_{\ell-1}+1,2 p_{\ell}+1\right)$, and $\mu(\mathrm{Sq}(s))=\operatorname{Sq}\left(s^{\prime}\right)$, where $s^{\prime}=2 q+1$.

Suppose that $\mathbf{g} \in \mathrm{NZ}(\mathbf{r}, s)$ and that $\mu(\mathrm{C}(\mathbf{g})) \neq 0$. Then $g_{\ell}=4 a_{\ell}+3$ for some $a_{\ell} \geq 0$. Further $g_{i}=4 a_{i}$ for some $a_{i} \geq 0$ if $1 \leq i \leq \ell-1$. For, if there is such an $i$ for which $g_{i} \equiv 2 \bmod 4$, then $r_{i+1}-2 g_{i+1}+g_{i} \equiv 3 \bmod 4$; consequently, $\mu(\mathrm{C}(\mathbf{g}))=0$, contrary to assumption. Thus, if $\ell>1$, then

$$
1=\left(4\left(p_{1}-2 a_{1}\right)+1,4\left(q-\sum a_{i}\right)\right)
$$

and, if $1 \leq i \leq \ell-2$, then $1=\left(4\left(p_{i+1}-2 a_{i+1}\right)+1,4 a_{i}\right)$ and, lastly, $1=$ $\left(4\left(p_{\ell}-2 a_{\ell}-1\right)+1,4 a_{\ell-1}\right)$ while, if $\ell=1$, then $1=\left(4\left(p_{1}-2 a_{1}-1\right)+1,4\left(q-a_{1}\right)\right)$. Moreover, if $\ell>1$, then

$$
\begin{gathered}
\mathrm{C}(\mathbf{g})=\mathrm{Sq}\left(4\left(p_{1}-2 a_{1}+q-\sum a_{i}\right)+1,4\left(p_{2}-2 a_{2}+a_{1}\right)+1, \cdots\right. \\
\cdots, 4\left(p_{i+1}-2 a_{i+1}+a_{i}\right)+1, \cdots, 4\left(p_{\ell-1}-2 a_{\ell-1}+a_{\ell-2}\right)+1 \\
\left.4\left(p_{\ell}-2 a_{\ell}-1+a_{\ell-1}\right)+1,4 a_{\ell}+3\right)
\end{gathered}
$$

while, if $\ell=1$, then

$$
\mathrm{C}(\mathbf{g})=\operatorname{Sq}\left(\left(4\left(p_{1}-3 a_{1}+q-1\right)+1,4 a_{1}+3\right) .\right.
$$

By the formula for $\mu$, if $\ell>1$, then

$$
\begin{gathered}
\mu(\mathrm{C}(\mathbf{g}))=\mathrm{Sq}\left(2\left(p_{1}-2 a_{1}+q-\sum a_{i}\right)+1,2\left(p_{2}-2 a_{2}+a_{1}\right)+1, \cdots\right. \\
\cdots, 2\left(p_{i+1}-2 a_{i+1}+a_{i}\right)+1, \cdots, 2\left(p_{\ell-1}-2 a_{\ell-1}+a_{\ell-2}\right)+1, \\
\left.2\left(p_{\ell}-2 a_{\ell}-1+a_{\ell-1}\right)+1,2 a_{\ell}+1\right)
\end{gathered}
$$

while, if $\ell=1$, then

$$
\mu(\mathrm{C}(\mathbf{g}))=\mathrm{Sq}\left(\left(2\left(p_{1}-3 a_{1}+q-1\right)+1,2 a_{1}+1\right)\right.
$$

Thus, $\mu(\mathrm{Sq}(\mathbf{r}) \mathrm{Sq}(s))$ is the sum over $\mathrm{NZ}(\mathbf{r}, s)$ of these expressions.
We next calculate

$$
\operatorname{Sq}\left(\mathbf{r}^{\prime}\right) \operatorname{Sq}\left(s^{\prime}\right)=\operatorname{Sq}\left(2 p_{1}+1, \cdots, 2 p_{\ell-1}+1,2 p_{\ell}+1\right) \operatorname{Sq}(2 q+1) .
$$

As the product is taken in $O$, we know that, for $\mathbf{h} \in \mathrm{NZ}\left(\mathbf{r}^{\prime}, s^{\prime}\right)$, there are integers $b_{i} \geq 0,1 \leq i \leq \ell$, such that $h_{i}=2 b_{i}, 1 \leq i \leq \ell-1$, and $h_{\ell}=2 b_{\ell}+1$. Thus, if $\ell>1$, then

$$
1=\left(2\left(p_{1}-2 b_{1}\right)+1,2\left(q-\sum b_{i}\right)\right)
$$

and, if $1 \leq i \leq \ell-2$, then $1=\left(2\left(p_{i+1}-2 b_{i+1}\right)+1,2 b_{i}\right)$ and, lastly, $1=$ $\left(2\left(p_{\ell}-2 b_{\ell}-1\right)+1,2 b_{\ell-1}\right)$ while, if $\ell=1$, then $1=\left(2\left(p_{1}-2 b_{1}-1\right)+1,2\left(q-b_{1}\right)\right)$. Furthermore, if $\ell>1$, then

$$
\begin{gathered}
\mathrm{C}(\mathbf{h})=\mathrm{Sq}\left(2\left(p_{1}-2 b_{1}+q-\sum b_{i}\right)+1,2\left(p_{2}-2 b_{2}+b_{1}\right)+1, \cdots\right. \\
\cdots, 2\left(p_{i+1}-2 b_{i+1}+b_{i}\right)+1, \cdots, 2\left(p_{\ell-1}-2 b_{\ell-1}+b_{\ell-2}\right)+1 \\
\left.2\left(p_{\ell}-2 b_{\ell}-1+b_{\ell-1}\right)+1,2 b_{\ell}+1\right)
\end{gathered}
$$

while, if $\ell=1$, then

$$
\mathrm{C}(\mathbf{h})=\mathrm{Sq}\left(2\left(p_{1}-3 b_{1}+q-1\right)+1,2 b_{1}+1\right) .
$$

Thus, $\mu(\operatorname{Sq}(\mathbf{r})) \mu(\operatorname{Sq}(s))$ is the sum over $\mathrm{NZ}\left(\mathbf{r}^{\prime}, s^{\prime}\right)$ of these matching expressions.

It remains to set up a bijective correspondence $\sigma$ between $\mathrm{NZ}(\mathbf{r}, s)$ and $\mathrm{NZ}\left(\mathbf{r}^{\prime}, s^{\prime}\right)$ such that $\mu(\mathrm{C}(\mathbf{g}))=\mathrm{C}(\sigma(\mathbf{g}))$ for $\mathbf{g} \in \mathrm{NZ}(\mathbf{r}, s)$.

We have seen above that $\mathbf{g}$ is of the form $\mathbf{g}=\left(4 a_{1}, \cdots, 4 a_{\ell-1}, 4 a_{\ell}+3\right)$ for non-negative integers $a_{i}$ and so we take $\sigma(\mathbf{g})=\left(2 a_{1}, \cdots, 2 a_{\ell-1}, 2 a_{\ell}+1\right)$. As $1=(4 x+1,4 y)=(2 x+1,2 y)$ for $x, y \geq 0$, we may deduce that $\sigma(\mathbf{g}) \in \mathrm{NZ}\left(\mathbf{r}^{\prime}, s^{\prime}\right)$. It is straightforward to check that $\mathrm{C}(\sigma(\mathbf{g}))=\mu(\mathrm{C}(\mathbf{g}))$ both when $\ell>1$ and when $\ell=1$.

Conversely, for $\mathbf{h} \in \mathrm{NZ}\left(\mathbf{r}^{\prime}, s^{\prime}\right), \mathbf{h}=\left(2 b_{1}, \cdots, 2 b_{\ell-1}, 2 b_{\ell}+1\right)$ for non-negative integers $b_{i}$ and so we take $\mathbf{g}=\left(4 b_{1}, \cdots, 4 b_{\ell-1}, 4 b_{\ell}+3\right)$. As before we may deduce that $\mathbf{g} \in \mathrm{NZ}(\mathbf{r}, s)$. Moreover, $\sigma(\mathbf{g})=\mathbf{h}$. Again one may check that $\mu(\mathrm{C}(\mathbf{g}))=\mathrm{C}(\mathbf{h})$ in both cases.

Finally we assume that $\mu(\mathrm{Sq}(\mathbf{r}))=0$ or that $\mu(\mathrm{Sq}(s))=0$ so that we must show that $\mu(\operatorname{Sq}(\mathbf{r}) \mathrm{Sq}(s))=0$. Assume that there is an $i, 1<i<\ell$, for which $r_{i} \equiv 3 \bmod 4$ so that $\mu(\mathrm{Sq}(\mathbf{r}))=0$. Take $\mathbf{g} \in \mathrm{NZ}(\mathbf{r}, s)$. As $g_{i}$ is even, $r_{i}-2 g_{i} \equiv$ $3 \bmod 4$ and it follows that $g_{i-1} \equiv 0 \bmod 4$. But then $r_{i}-2 g_{i}+g_{i-1} \equiv 3 \bmod 4$ whence $\mu(\mathrm{C}(\mathbf{g}))=0$ and so $\mu(\mathrm{Sq}(\mathbf{r}) \mathrm{Sq}(s))=0$. The proof is completed by working through other such cases in a similar manner.

## Coalgebra endomorphisms

As the subspace spanned by the Steenrod squares forms a subcoalgebra of $A$, a linear transformation from $A$ to itself, which sends each Steenrod square to another or to 0 and which respects the coproduct, determines only a coalgebra endomorphism of this subcoalgebra. It is not hard to answer the more appropriate question, namely: which are the bialgebra endomorphisms with this property?

Proposition. The only bialgebra endomorphisms of $A$ which send a Steenrod square $\mathrm{Sq}^{n}$ either to 0 or to another Steenrod square are $\gamma$ and its powers and the augmentation $\varepsilon$. They are all Hopf algebra endomorphisms.

## References

[AS72] Abramowitz, M.; Stegun, I.A. (eds.): Handbook of mathematical functions. New York: Dover (1972)
[Ma83] Margolis, H.R.: Spectra and the Steenrod algebra. Amsterdam: Elsevier 1983
[Mo92] Monks, K.G.: Nilpotence of the Steenrod algebra. Bol. Soc. Mat. Mexicana 37, 401-416 (1992)
[SE6] Steenrod, N.E., Epstein, D.B.A.: Cohomology operations. (Ann. Math. Stud. 50) Princeton: Princeton University Press 1962
[Wo98] Wood, R.M.W.: Problems in the Steenrod algebra. Bull. London Math. Soc. 30, 449-517 (1998)

