On the Hopf Ring for the Sphere

by

Yanfei Li

A dissertation submitted to The Johns Hopkins University

in conformity with the requirements for the degree of

Doctor of Philosophy

Baltimore, Maryland

1996

Abstract

In this work we describe the mod p ordinary homology of QS^k for $k \geq 0$ as a Hopf ring. We give the explicit relations for the $\circ$-product and $*$-product which allow us to calculate $H_*(QS^k; \mathbb{F}_p)$ as a Hopf ring. We also give new generators for $H_*(QS^k; \mathbb{F}_p)$ as an algebra for any prime p.

Acknowledgments

I would like to express my deep gratitude to my advisors, Prof. J. Michael Boardman and Prof. W. Stephen Wilson. To Prof. Wilson, for introducing this interesting problem to me and for the constant encouragement and support as well as tremendously useful discussions during my graduate studies at The Johns Hopkins University. To Prof. Boardman, for the very careful reading of my thesis, clarifying the ideas, pointing out many corrections and simplifying the statements and proofs which have greatly improved the final version. I would also like to express my gratitude to Prof. Jack Morava and Prof. Hal Sadofsky for useful discussions about various topological questions. I would also like to express my gratitude to all support staff of the Department of Mathematics, for their kindness and assistance. Last but not least, I would like to express my gratitude to my wife, Bingwen Wu, for her love and support, and I would also like to express my great love to my son, Daniel Li.

Contents

1 Introduction

The homology of the infinite loop space $QS^k = \lim_{n\to\infty} \Omega^n S^{n+k}$ $(k \geq 0)$ is well known and the reader can find detailed information about the calculation in [May] and [CLM] where the answer is given to us as a Hopf algebra. There, only one of the spaces $\{QS^k\}_{k\geq 0}$ is discussed at a time and so the answer is given in terms of the Hopf algebra. In this work we will consider $\{QS^k\}_{k\geq 0}$ as the Ω-spectrum associated to the sphere spectrum S. The sphere spectrum is a ring spectrum and so we can consider the mod p homology Hopf ring $\{H_*QS^k\}_{k\in\mathbb{Z}}$. For an introduction to Hopf rings the reader is refered to [RW] and we will give a brief review with the terminology and conventions established there. In this case the Hopf ring $*$ and $\circ$ products have a more conventional interpretation as those arising from the loop sum and the composition product.

This thesis is organized as follows. Section 2 contributes the necessary preparation for this work. Section 3 gives the relations on the $\circ$-product. In Section 4 we use the results of Section 3 to compute the Hopf ring $\{H_*(QS^k;\mathbb{F}_2)\}_{k\geq 0}$. In Section 5 we give the formulae for the $*$-power in terms of the $\circ$-product. Finally, in Section 6, we compute the Hopf ring $\{H_*(QS^k;\mathbb{F}_p)\}_{k\geq 0}$ for an odd prime p.

2 Preliminaries

In Section 2.1, we introduce Hopf algebras. The standard references for this subject are Milnor and Moore [MMj] and Sweedler [Sw]. In Section 2.2, we introduce Hopf rings and the standard reference for this subject is Ravenel and Wilson [RW]. In Section 2.3, we review the Dyer-Lashof operations, and the reference for these materials is May [May]. In Section 2.4, we recall the the description of the Hopf algebra $H_*(QS^k;\mathbb{F}_p)$ where $k \geq 0$.

2.1 Hopf Algebras

Assume that R is a commutative ring with unit. A *Hopf algebra* over R is a graded R-module $A_* = \{A_k\}_{k\in\Lambda}$ with R-module maps

- Multiplication $\varphi : A_* \otimes A_* \to A_*$
- Unit for multiplication $\eta : R \to A_*$
- Comultiplication $\psi : A_* \to A_* \otimes A_*$
- Counit for comultiplication $\varepsilon : A_* \to R$
- Conjugation $\chi : A_* \to A_*$

such that

(1) (A_*, φ, η) is an algebra over R with augmentation ε,

(2) (A_*, ψ, ε) is a coalgebra over R with coaugmentation η, and

(3) the diagram

$$\begin{array}{ccccc} A_* \otimes A_* & \xrightarrow{\varphi} & A_* & \xrightarrow{\psi} & A_* \otimes A_* \\ \downarrow{\scriptstyle \psi\otimes\psi} & & & & \uparrow{\scriptstyle \varphi\otimes\varphi} \\ A_* \otimes A_* \otimes A_* \otimes A_* & & \xrightarrow[A\otimes T\otimes A]{} & & A_* \otimes A_* \otimes A_* \otimes A_* \end{array}$$

commutes, where $T : A_* \otimes A_* \to A_* \otimes A_*$ is the twist map.

The *dual* of a Hopf algebra $(A_*, \varphi, \eta, \psi, \varepsilon, \chi)$, where A_* is a free R-module of finite type, is the Hopf algebra $((A_*)^*, \psi^*, \varepsilon^*, \phi^*, \eta^*, \chi^*)$; note that $(A_* \otimes A_*)^* = (A_*)^* \otimes (A_*)^*$.

Example 2.1 *The polynomial algebra $P[x]$ and exterior algebra $E[x]$ can be given a Hopf algebra structure by defining the coproduct, counit and conjugation as follows, respectively.*

$$\psi(x) = x \otimes 1 + 1 \otimes x$$

$$\varepsilon(x) = 0$$

$$\chi(x) = -x$$

Note that the above construction can be generalized to n generators by taking tensor products.

Example 2.2 *The divided power algebra $D[x]$ is the dual of the polynomial algebra $P[x]$. The dual basis is $\{v^{[i]}\}$ where $v^{[i]}$ is dual to x^i, and the structure maps are:*

$$\varphi(v^{[i]} \otimes v^{[j]}) = \left(\begin{array}{c} i+j \\ j \end{array} \right) v^{[i+j]}$$

$$\eta(1) = 1 = v^{[0]}$$

$$\psi(v^{[i]}) = \sum_{l=0}^{i} v^{[i-l]} \otimes v^{[l]}$$

$$\varepsilon(v^{[i]}) = 0 \qquad \textit{for } i > 0$$

$$\chi(v^{[i]}) = (-1)^i v^{[i]}$$

Also, we can give the Hopf algebra structure on the divided power algebra with n generators by taking tensor products.

2.2 Hopf Rings

Now we give a brief review of the basics of Hopf rings. Let R be a graded (associative, commutative) ring (with unit). We let $\mathbb{D} = CoAlg_R$ be the category of graded cocommutative coassociative coalgebras with counit over R, henceforth coalgebras. For each object C we have a coproduct $\psi_C : C \to C \otimes_R C$ and a counit $\varepsilon_C : C \to R$. Morphisms are maps of coalgebras with unit. R is in the category in a natural way and is a terminal object. The unique map from C to R is ε_C. The product in the category, $C \Pi D$, is given by $C \otimes_R D = C \otimes D$, where $1 \otimes \varepsilon_D : C \otimes D \to C$ and $\varepsilon_C \otimes 1 : C \otimes D \to D$ are the projections. If $f : B \to C$ and $g : B \to D$ are given. then the map $(f, g) : B \to C \otimes D$ is $(f \otimes g)\psi_B$, i.e., $(f, g)(b) = \sum f(b') \otimes g(b'')$ where $\psi(b) = \sum b' \otimes b''$. We call a ring object over $CoAlg_R$ a (graded) *Hopf ring*. The following lemma is extracted from Ravenel and Wilson [RW].

Lemma 2.3 *Let $H(*) = \{H_*(n)\}_{n \in Z} \in CoAlg_R$ be a Hopf ring. Let $a \in H_i(n)$, $b \in H_j(k)$, $c \in H_q(k)$. Define* $\deg(x)$ *by $x \in H_{\deg(x)}(m)$.*

(a) Each $H_*(n) \in CoAlg_R$.

(i) There is a coassociative cocommutative coproduct for all n

$$\psi : H_*(n) \to H_*(n) \otimes H_*(n)$$

$$\psi(a) = \sum a' \otimes a'' = \sum (-1)^{\deg(a')\,\deg(a'')} a'' \otimes a'$$

(ii) There is a counit, $\varepsilon : H_*(n) \to R$ *such that*

$$H_*(n) \xrightarrow{\psi} H_*(n) \otimes H_*(n) \xrightarrow{1_{H_*(n)} \otimes \varepsilon} H_*(n) \otimes_R R \simeq H_*(n)$$

is the identity, i.e. $a = \sum a' \varepsilon(a'')$.

(b) Each $H_*(k)$ *is an abelian group object of* $CoAlg_R$*, i.e. a bicommutative biassociative Hopf algebra with unit, counit and conjugation:*

(i) There is a product

$$* : H_*(k) \otimes H_*(k) \to H_*(k)$$

which is associative and commutative,

$$b * c = (-1)^{jq} c * b \in H_{j+q}(k)$$

(ii) The map $*$ *is in* $CoAlg_R$

$$\begin{aligned} \psi(b * c) = \psi(b) * \psi(c) &= \sum (b' \otimes b'') * (c' \otimes c'') \\ &= \sum (-1)^{\deg(c')\,\deg(b'')} (b' * c') \otimes (b'' * c'') \end{aligned}$$

(iii) The abelian group object unit, zero, is $\eta : R \to H_*(k)$*. We define* $[0_k] = \eta(1) \neq 0$,

$$[0_k] * b = b$$

(iv) The conjugation $\chi : H_*(k) \to H_*(k)$ *has* $\chi\chi = identity$ *and* $\eta\varepsilon(b) = \sum b' * \chi(b'')$.

(c) There are associative maps

$$\circ : H_*(n) \otimes H_*(k) \to H_*(n+k)$$

such that:

(i) The map $\circ$ *is in* $CoAlg_R$

$$\psi(a \circ b) = \psi(a) \circ \psi(b) = \sum (a' \otimes a'') \circ (b' \otimes b'')$$
$$= \sum (-1)^{\deg(a'')\ \deg(b')} (a' \circ b') \otimes (a'' \circ b'')$$

(ii) Multiplication by zero

$$[0_n] \circ b = \eta\varepsilon(b)$$

(iii) There is a unit map $e : R \to H_*(0)$. *Define* $e(1) = [1] \in H_0(0)$, *then*

$$[1] \circ b = b$$

(iv) Define $\chi([1]) = [-1] \in H_0(0)$. *Then*

$$\chi(a) = [-1] \circ a$$

and

$$\chi(a \circ b) = \chi(a) \circ b = a \circ \chi(b)$$

(v) Commutativity

$$a \circ b = (-1)^{ij}[-1]^{\circ nk} \circ b \circ a = (-1)^{ij} \chi^{nk}(b \circ a) \in H_{i+j}(n+k)$$

(vi) Distributivity

$$a \circ (b * c) = \sum (-1)^{\deg(a'')\ \deg(b)} (a' \circ b) * (a'' \circ c)$$

(vii) Let $[n] = [1]^{*n} = [1 + 1 + \cdots + 1]$, *then*

$$[n] \circ b = \sum b' * b'' * \cdots * b^{(n)}$$

where $\Psi : H_*(k) \longrightarrow H_*(k) \otimes \cdots \otimes H_*(k)$ *denotes the iterated n-fold coproduct and* $\Psi b = \sum b' \otimes b'' \otimes \cdots \otimes b^{(n)}$.

The following description refers to Turner [Tu]. Hopf rings arise in topology in the study of the homology of the spaces of a multiplicative Ω-spectrum. Recall that any unreduced multiplicative cohomology theory $G^*(-)$ can be represented unstably by the infinite loop spaces G_n of its associated Ω-spectrum (i.e. $G^k(X) = [X, G_k]$ and $\Omega G_{k+1} \simeq G_k$, where $[X, Y]$ means homotopy classes of unbased maps from X to Y). To study the homology of these spaces it is convenient to consider all of them simultaneously and regard the collection $G_* = \{G_k\}_{k\in\Lambda}$ as a graded ring space. We have products

$$m : G_k \times G_k \to G_k$$

and

$$\sigma : G_k \times G_l \to G_{k+l}$$

arising from the loop structure on G_k and from the ring map $G \wedge G \to G$. Suppose now we are given another such spectrum, E, for which we have the Künneth isomorphism

$$E_*G_k \otimes_{E_*} E_*G_l \cong E_*(G_k \times G_l)$$

for all k and l. In view of Section 2.1 we then have that E_*G_k is a Hopf algebra. Further, we can use σ to define a circle product

$$\circ : E_*G_k \otimes_{E_*} E_*G_l \cong E_*(G_k \times G_l) \xrightarrow{\sigma_*} E_*G_{k+l}$$

turning $E_*G_* = \{E_*G_k\}_{k\in\Lambda}$ into a Hopf ring.

2.3 Dyer-Lashof Operations

In this section, we review the Dyer-Lashof operations, and most of the materials can be found in May [May]. By an infinite loop space $B = \{B_i \,|\, i \geq 0\}$, we understand a sequence of based spaces such that $B_i = \Omega B_{i+1}$; by a map $g : B \to C$ of infinite loop sequences, we understand a sequence of base-point preserving maps $g_i : B_i \to C_i$ such that $g_i = \Omega g_{i+1}$, $i \geq 0$. We denote $H_*(B) = H_*(B_0; \mathbb{F}_p)$ for some fixed prime p and regard H_* as a functor from the category of infinite loop sequences to that of graded $\mathbb{F}_p$-modules. $H_*(B)$ admits homology operations which are analogous to the Steenrod operations in cohomology. More precisely, there exist homomorphisms

$$Q^i : H_*(B) \longrightarrow H_*(B)$$

for all $i \geq 0$. We state the results for an arbitrary prime p; the modifications needed in the case $p = 2$ are indicated in square brackets.

Theorem 2.4 *The Q^i satisfy the following properties:*

(1) The Q^i are natural with respect to infinite loop maps and have degree $2i(p-1)$ [degree i].

(2) $Q^0(\phi) = \phi$ and $Q^i(\phi) = 0$ for $i > 0$, where $\phi \in H_0(B)$ is the identity element for the loop product in $H_*(B)$.

(3) $Q^i(x) = 0$ if $2i < \deg(x)$ [if $i < \deg(x)$].

(4) $Q^i(x) = x^p$ if $2i = \deg(x)$ [if $i = \deg(x)$].

(5) $\sigma_* Q^i = Q^i \sigma_*$, where $\sigma_* : IH_*(\Omega B) \longrightarrow H_*(B)$ is the homology suspension.

(6) Cartan formula: $Q^s(xy) = \sum_{i=0}^s Q^i(x) Q^{s-i}(y)$ and, if $\psi(x) = \sum x' \otimes x''$, then $\psi Q^s(x) = \sum_{i=0}^s \sum Q^i(x') \otimes Q^{s-i}(x'')$.

(7) If $\chi : H_*(B) \longrightarrow H_*(B)$ is the conjugation (induced from the map $\chi(l)(t) = l(1-t)$, $\chi : \Omega B_1 \longrightarrow \Omega B_1$), then $\chi Q^i = Q^i \chi$.

(8) Adem relations: If $p \geq 2$ and $a > pb$, then

$$Q^aQ^b = \sum_i (-1)^{a+i}(pi-a, a-(p-1)b-i-1)Q^{a+b-i}Q^i$$

If $p > 2$, $a \geq pb$, and β is the mod p *Bockstein, then*

$$\begin{aligned} Q^a\beta Q^b &= \sum_i (-1)^{a+i}(pi-a, a-(p-1)b-i)\beta Q^{a+b-i}Q^i \\ &\quad -\sum_i (-1)^{a+i}(pi-a-1, a-(p-1)b-i)Q^{a+b-i}\beta Q^i \end{aligned}$$

(9) Nishida relations: Let $P^s_* : H_*(B) \longrightarrow H_*(B)$, of degree $-2s(p-1)$, be dual to P^s (i.e. $P^s = \mathrm{Hom}_{\mathbb{F}_p}(P^s_*, 1)$ with $H^*(B) = \mathrm{Hom}_{\mathbb{F}_p}(H_*(B), \mathbb{F}_p)$) if $p > 2$; and let $P^s_* = \mathrm{Sq}^s_*$, of degree $-s$, if $p = 2$. Then

$$P^s_*Q^r = \sum_i (-1)^{i+s}(s-pi, r(p-1)-ps+pi)Q^{r-s+i}P^i_*$$

and if $p > 2$,

$$\begin{aligned} P^s_*\beta Q^r &= \sum_i (-1)^{i+s}(s-pi, r(p-1)-ps+pi-1)\beta Q^{r-s+i}P^i_* \\ &\quad +\sum_i (-1)^{i+s}(s-pi-1, r(p-1)-ps+pi)Q^{r-s+i}P^i_*\beta \end{aligned}$$

In (8) and (9), the binomial coefficient $(i,j) = (i+j)!/i!j!$ if $i > 0$ and $j > 0$, $(i,0) = 1 = (0,i)$ if $i \geq 0$, and $(i,j) = 0$ if $i < 0$ or $j < 0$; the sums are over the integers.

When B is an E_∞ ring space [CLM], we have the following result.

Theorem 2.5 *Let $b \in H_*(B)$ and $f \in H_*(B)$, then*

$$Q^kb \circ f = \sum_i Q^{k+i}(b \circ P^i_*f)$$

and for an odd prime p,

$$\beta Q^kb \circ f = \sum_i \beta Q^{k+i}(b \circ P^i_*f) - \sum_j (-1)^{\deg(b)}Q^{k+j}(b \circ P^j_*\beta f)$$

Let e_k be the image of the generator of $H_k(S^k)$ in $H_k(QS^k)$ by the homomorphism $H_k(S^k) \longrightarrow H_k(QS^k)$ if $k > 0$. By convention, $e_0 = [1]$ denotes the class of the point other than the base-point. Since $P_*^i e_n = 0$ for $i > 0$ and $\beta e_n = 0$, we have

Example 2.6 *For instance,* $Q^i[1] \circ e_k = Q^i e_k$, *and also*

$$P_*^s \beta Q^r e_n = (-1)^s (s,\ r(p-1) - ps - 1) \beta Q^{r-s} e_n$$

2.4 The Homology of QS^k

We review the mod p homology of QS^k for $k \geq 0$. The materials can be found in Cohen, Lada and May [CLM], and May [May]. For $p = 2$, the materials can also be found in Madsen and Milgram [MM], and Turner [T].

Definition 2.7 *(a) For* $p = 2$, *consider the sequence* $I = (s_1, \dots, s_k)$, *where each* $s_j \geq 0$, *and define the* degree $d(I) = \sum_{j=1}^k s_j$, length $l(I) = k$, *and* excess $e(I) = s_k - \sum_{j=2}^k (2s_j - s_{j-1}) = s_1 - \sum_{j=2}^k s_j$. *I is said to be* admissible *if* $2s_j \geq s_{j-1}$ *for* $2 \leq j \leq k$. *Each I determines an element* $Q^I = Q^{s_1} \cdots Q^{s_k}$.

(b) For an odd prime p, consider the sequences $I = (\epsilon_1, s_1, \dots, \epsilon_k, s_k)$ *where every* $\epsilon_j = 0$ *or* 1 *and each* $s_j \geq \epsilon_j$. *Define the* degree, length, *and* excess *of I by*

$$d(I) = \sum_{j=1}^k [2s_j(p-1) - \epsilon_j]$$

$$l(I) = k$$

$$e(I) = 2s_1 - \epsilon_1 - \sum_{j=2}^k [2s_j(p-1) - \epsilon_j]$$

I is said to be admissible *if* $ps_j - \epsilon_j \geq s_{j-1}$ *for* $2 \leq j \leq k$. *Each I determines an element* $Q^I = \beta^{\epsilon_1} Q^{s_1} \cdots \beta^{\epsilon_k} Q^{s_k}$.

Convention The empty sequence I is admissible and satifies $d(I) = 0$, $l(I) = 0$, and $e(I) = \infty$; it determines the identity homology operation $Q^I = 1$.

The following result is extracted from [CLM].

Theorem 2.8 *For any $k > 0$, we have*

$$H_*(QS^k; \mathbb{F}_2) = P[Q^I e_k \,|\, I \text{ admissible and } e(I) > k\,]$$

For $k = 0$, we have

$$H_*(QS^0; \mathbb{F}_2) = P[Q^I[1] \,|\, I \text{ admissible and } e(I) > 0\,] \otimes \mathbb{F}_2[\mathbb{Z}]$$

Every element $Q^I e_k$ of $H_*(QS^k; \mathbb{F}_2)$ can be expressed as a linear combination of products of the form $Q^{s_1}[1] \circ \cdots \circ Q^{s_n}[1] \circ e_k$.

For odd primes p, we have

Theorem 2.9 *For $k > 0$,*

$$\begin{aligned} H_*(QS^{2k}; \mathbb{F}_p) = P[\, Q^I e_{2k} \mid I \text{ admissible, } e(I) > 2k, \; d(I) \text{ is even}\,] \\ \otimes P[\, Q^I e_{2k} \mid I \text{ admissible, } e(I) = 2k \text{ and } \epsilon_1 = 1\,] \\ \otimes E[\, Q^I e_{2k} \mid I \text{ admissible, } e(I) > 2k \text{ and } d(I) \text{ is odd}\,] \end{aligned}$$

For $k = 0$,

$$\begin{aligned} H_*(QS^0; \mathbb{F}_p) = P[\, Q^I[1] \mid I \text{ admissible, } e(I) > 0, \; d(I) \text{ is even}\,] \\ \otimes P[\, Q^I[1] \mid I \text{ admissible, } e(I) = 0 \text{ and } \epsilon_1 = 1\,] \\ \otimes E[\, Q^I e_{2k} \mid I \text{ admissible, } e(I) > 0 \text{ and } d(I) \text{ is odd}\,] \otimes \mathbb{F}_p[\mathbb{Z}] \end{aligned}$$

where P denotes the polynomial algebra, E denotes the exterior algebra and $\mathbb{F}_p[\mathbb{Z}]$ denotes the group algebra of $\mathbb{Z}$.

Theorem 2.10 *For $k > 0$, with the same notation as above,*

$$H_*(QS^{2k-1};\mathbb{F}_p) = P[\, Q^I e_{2k-1} \mid I \;\; admissible, \;\; e(I) > 2k-1 \;\; and \;\; d(I) \;\; is \;\; odd \,]$$

$$\otimes P[\, Q^I e_{2k-1} \mid I \;\; admissible, \;\; e(I) = 2k-1 \;\; and \;\; \epsilon_1 = 1 \,]$$

$$\otimes E[\, Q^I e_{2k-1} \mid I \;\; admissible, \;\; e(I) > 2k-1 \;\; and \;\; d(I) \;\; is \;\; even \,]$$

Theorem 2.11 *For $k \geq 0$, every element $Q^I e_k$ of $H_*(QS^k;\mathbb{F}_p)$ can be written as a linear combination of products of form $Q^{i_1}[1] \circ \cdots \circ Q^{i_n}[1] \circ (\beta Q^{j_1}[1]) \circ \cdots \circ (\beta Q^{j_m}[1]) \circ e_k$ where $i_r \geq 0$ and $j_r > 0$ for any r.*

3 The Relations for the Formal Power Series

The Nishida relations link the actions of the Dyer-Lashof operations Q^i, the Bockstein β, and the duals P^i_* of the Steenrod cohomology operations on $H_*(B;\mathbb{F}_p)$. Let U, V be indeterminates of degree $-2(p-1)$ (degree of -1 if $p=2$) commuting with each other and with anything else that occurs. Put $S = U(1-V^{-1}U)^{p-1}$ and $T = V(1-U^{-1}V)^{p-1}$. For an indeterminate Z, write $Q(Z) = \sum_i Q^i Z^i$, $P_*(Z) = \sum_i P^i_* Z^i$. Following Steiner [S], we have

Lemma 3.1 *For any prime* p

$$P_*(U^{-1})Q(V) = Q(T)P_*(S^{-1})$$

and for an odd prime p

$$P_*(U^{-1})\beta Q(V) = (1-U^{-1}V)^{-1}[\,\beta Q(T)P_*(S^{-1}) - U^{-1}VQ(T)P_*(S^{-1})\beta\,]$$

Definition 3.2 *Define* $X_i = Q^i[1]$ *for* $i \geq 0$ *and, for odd* p, $Y_j = \beta Q^j[1]$, *where* $j > 0$.

Let $X(s) = \sum_{i=0}^{\infty} X_i\, s^{(p-1)i}$ *for any prime* p, *where* s *is an indeterminate of degree* -2 *(degree* -1 *if* $p=2$*),* $Y(s) = \sum_{i=1}^{\infty} Y_i\, s^{(p-1)i-1}$ *for an odd prime* p, $\overline{Y}(s) = \sum_{i=1}^{\infty} Y_i\, s^{(p-1)i} = sY(s)$.

We have the following theorem. For $p=2$, see Turner [T], where he proved it using coinvariants of rings and transfer.

Theorem 3.3 $$X(s)\circ X(t) = X(s)\circ X(s+t)$$

Proof: For the sake of simplicity, let $S = s^{p-1}$, $T = t^{p-1}$, $L = (s+t)^{p-1}$, $U = T(1-S^{-1}T)^{p-1}$, $V = S(1-T^{-1}S)^{p-1}$, and $\overline{U} = L(1-S^{-1}L)^{p-1}$. By

Theorem 2.6 and Lemma 3.1,

$$\begin{aligned} X(s)\circ X(t) &= \sum_{i,j} Q^i[1]\circ Q^j[1]S^iT^j \\ &= \sum_{i,j,k} Q^{i+k}P_*^kQ^j[1]S^iT^j \\ &= Q(S)P_*(S^{-1})Q(T)[1] \\ &= Q(S)Q(U)P_*(V^{-1})[1] \\ &= Q(S)Q(U)[1] \end{aligned}$$

since $P_*(V^{-1})[1]=[1]$ as $[1]$ is in degree 0. Here $U=u^{p-1}$, where $u=t(1-s^{-(p-1)}t^{p-1})$. Similarly, replacing t by $s+t$, we find

$$X(s)\circ X(s+t)=Q(S)Q(\overline{U})[1]$$

where $\overline{U}=\overline{u}^{p-1}$ and $\overline{u}=(s+t)(1-s^{-(p-1)}(s+t)^{p-1})$. Recall that we are working over the ring $\mathbb{F}_p$, so we have

$$\begin{aligned} u &= t(1-s^{-(p-1)}t^{p-1}) \\ &= t-s^{-(p-1)}t^p \\ &= s+t-s^{-(p-1)}(s^p+t^p) \\ &= (s+t)(1-s^{-(p-1)}(s+t)^{p-1}) \\ &= \overline{u} \end{aligned}$$

Thus $U=\overline{U}$, and we have proved our theorem. □

The following results concern the odd prime situation.

Theorem 3.4 $\quad Y(s)\circ X(t)=Y(s+t)\circ X(t)$

Proof: With the same notation as in the proof of Theorem 3.3,

$$\begin{aligned} X(t) \circ \overline{Y}(s) &= \sum_{i,j} Q^i[1] \circ \beta Q^j[1] T^i S^j \\ &= \sum_{i,j,k} Q^{i+k} P_*^k \beta Q^j[1] T^i S^j \\ &= Q(T) P_*(T^{-1}) \beta Q(S)[1] \\ &= Q(T) \frac{1}{1 - T^{-1}S} \beta Q(U) P_*(V^{-1})[1] \\ &= Q(T) \frac{1}{1 - T^{-1}S} \beta Q(U)[1] \end{aligned}$$

since $\beta[1] = 0$. Similarly,

$$X(t) \circ \overline{Y}(s+t) = Q(T) \frac{1}{1 - T^{-1}L} \beta Q(\overline{U})[1]$$

As in the proof of Theorem 3.3, we have $U = \overline{U}$. Also

$$\begin{aligned} 1 - T^{-1}L &= 1 - t^{-(p-1)}(s+t)^{p-1} \\ &= \frac{s + t - t^{-(p-1)}(s^p + t^p)}{s+t} \\ &= \frac{s - t^{-(p-1)} s^p}{s+t} \\ &= \frac{s}{s+t}(1 - t^{-(p-1)} s^{p-1}) \\ &= \frac{s}{s+t}(1 - T^{-1}S) \end{aligned}$$

so we have

$$X(t) \circ \overline{Y}(s+t) = \frac{s+t}{s} X(t) \circ \overline{Y}(s)$$

and we have proved our theorem. □

Applying the Bockstein β to the above theorem, we get

Theorem 3.5 $$Y(s) \circ Y(t) = Y(s+t) \circ Y(t)$$

Expanding the relation

$$0 = X(s) \circ X(s+t) - X(s) \circ X(t) = X(s) \circ [X(s+t) - X(t)]$$

we have

$$\begin{aligned} 0 &= \sum_{i,j} X_i \circ X_j \, s^{(p-1)i}((s+t)^{(p-1)j} - t^{(p-1)j}) \\ &= \sum_{i,j} X_i \circ X_j \sum_{b=0}^{(p-1)j-1} \binom{(p-1)j}{b} s^{(p-1)i} s^{(p-1)j-b} t^b \end{aligned}$$

Considering the coefficients of $s^{(p-1)N-b}t^b$ for a fixed b, so that we must take $i = N - j$, we get

Theorem 3.6 *For any positive integer N and $b \geq 0$, we have*

$$\sum_{(p-1)j>b} \binom{(p-1)j}{b} X_{N-j} \circ X_j = 0$$

Now assume p is odd. Similarly expanding the relation

$$0 = Y(s+t) \circ X(t) - Y(s) \circ X(t) = [Y(s+t) - Y(s)] \circ X(t)$$

yields

$$\begin{aligned} 0 &= \sum_{i,j} Y_i \circ X_j ((s+t)^{(p-1)i-1} - s^{(p-1)i-1}) t^{(p-1)j} \\ &= \sum_{i,j} Y_i \circ X_j \sum_{b=0}^{(p-1)i-2} \binom{(p-1)i-1}{b} s^b t^{(p-1)i-1-b} t^{(p-1)j} \end{aligned}$$

Considering the coefficients of $s^b t^{(p-1)N-1-b}$, we get

Theorem 3.7 *For any positive integer N and $b \geq 0$, we have*

$$\sum_{(p-1)i-1>b} \binom{(p-1)i-1}{b} Y_i \circ X_{N-i} = 0$$

Analogously from Theorem 3.5, we have

Theorem 3.8 *For any positive integer* N *and* $0 \leq b$*, we have*

$$\sum_{(p-1)i-1>b} \binom{(p-1)i-1}{b} Y_i \circ Y_{N-i} = 0$$

By convention, $X_i = 0$ for $i < 0$ and $Y_j = 0$ for $j \leq 0$ in all these formulae.

Next, we give another formula concerning the product $X_i \circ Y_j$. Applying the Bockstein β to the relation

$$X(s) \circ X(t) = X(s) \circ X(s+t)$$

and using $\beta X(s) = sY(s)$, we have

$$sY(s) \circ X(t) + tY(t) \circ X(s) = sY(s) \circ X(s+t) + (s+t)Y(s+t) \circ X(s)$$

By Theorem 3.4, we can write $Y(s+t) \circ X(s) = Y(s) \circ X(s)$, so the relation becomes

$$sY(s) \circ X(t) = sY(s) \circ X(s+t) + sY(t) \circ X(s)$$

so we have

Lemma 3.9 $$Y(s) \circ X(s+t) = Y(s) \circ X(t) - Y(t) \circ X(s)$$

Switching s with t, we have

$$Y(t) \circ X(s+t) = Y(t) \circ X(s) - Y(s) \circ X(t)$$

and hence

$$(Y(s) + Y(t)) \circ X(s+t) = 0$$

Let us work on the relation

$$Y(s) \circ (\, X(s+t) - X(t)\,) + Y(t) \circ X(s) = 0$$

from Lemma 3.9. Expanding in terms of power series, we have

$$0 = \sum_{i,j} Y_i \circ X_j \, s^{(p-1)i-1}((s+t)^{(p-1)j} - t^{(p-1)j}) + \sum_{k,l} Y_k \circ X_l \, t^{(p-1)k-1} s^{(p-1)l}$$

$$= \sum_{i,j} Y_i \circ X_j \sum_{b=0}^{(p-1)j-1} \binom{(p-1)j}{b} s^{(p-1)i-1} s^{(p-1)j-b} t^b + \sum_{k,l} Y_k \circ X_l \, t^{(p-1)k-1} s^{(p-1)l}$$

Considering the coefficients of $t^b s^{(p-1)N-1-b}$, we must take $i = N - j$ in the first sum, and hence we get

Theorem 3.10 *For any positive integer N and $b \geq 0$, we have*

(a) If $(b+1) \not\equiv 0 \bmod (p-1)$,

$$\sum_{(p-1)j>b} \binom{(p-1)j}{b} Y_{N-j} \circ X_j = 0$$

(b) If $(b+1) \equiv 0 \bmod (p-1)$, say $b = (p-1)s - 1$ for some $s > 0$,

$$X_{N-s} \circ Y_s + \sum_{j \geq s} \binom{(p-1)j}{(p-1)s-1} Y_{N-j} \circ X_j = 0$$

4 The Generators of the Hopf Ring $H_*(QS^k;\mathbb{F}_2)$

Now we are going to construct the generator set for the Hopf ring $H_*(QS^k;\mathbb{F}_2)$.

Given a set $S = \{s_1, s_2, \ldots, s_n\}$ of integers, where $s_1 > s_2 > \cdots > s_n \geq 0$, write $2^S = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_n}$, then $\alpha(2^S)$ is defined as n. If $M = 2^S$ and $N = 2^T$, $M \subset N$ means that $S \subset T$.

Lemma 4.1 *For any positive integers k and b such that $k > b$, $\binom{k}{b} \not\equiv 0 \bmod 2$ if and only if $b \subset k$.*

Given a positive integer M (to be chosen later), write $M = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_n}$ as above, with $s_1 > s_2 > \cdots > s_n \geq 0$. We define $K_t = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_t}$ for $1 \leq t \leq n$, $K_0 = 0$, and $L_t = (K_t + M)/2$ (note that L_t need not be an integer). Then we have $K_t = K_{t-1} + 2^{s_t}$, $M < K_t + 2^{s_t}$, $L_t = L_{t-1} + 2^{s_t - 1}$, $M - L_t = (M - K_t)/2 < 2^{s_{t+1}}$, $L_{t-1} = (M + K_{t-1})/2 < K_t$. Thus

$$K_0 = 0 < L_0 = M/2 < K_1 < L_1 < \cdots < K_n = L_n = M$$

Define the sets of integers $A_t = \{j \in \mathbb{Z} : K_t \leq j \leq L_t\}$ for $0 \leq t \leq n$ and $B_t = \{j \in \mathbb{Z} : L_t < j < K_{t+1}\}$ for $0 \leq t < n$. This defines a partition of the set $\{j \in \mathbb{Z} : 0 \leq j \leq M\}$.

Recall what we have proved in the last section in Theorem 3.6.

Lemma 4.2 *For any positive integer N, we have*

$$\sum_{j > b} \binom{j}{b} X_{N-j} \circ X_j = 0$$

Here $0 \leq b \leq N - 1$.

In the statements and proofs of the following results, c_j or c_J denotes an unknown coefficient in which we are not interested. We first consider the case of length 2.

Lemma 4.3 *Assume that $j \in A_t$ where $0 < t \leq n$. Taking $b = j - 2^{s_t}$ in Lemma 4.2, we have*

$$X_{N-j} \circ X_j = \sum_{\alpha(l)=\alpha(j)} \binom{l}{b} X_{N-l} \circ X_l + \sum_{\alpha(k)>\alpha(j)} c_k\, X_{N-k} \circ X_k$$

where $l \in A_{t-1}$ whenever l satisfies $l \neq j$, $l \leq M$ and $\binom{l}{b} \not\equiv 0 \bmod 2$.

Proof: By Lemma 4.1, $\binom{l}{b} \not\equiv 0 \bmod 2$ gives $l = b + 2^v$, where $v \neq s_t$. Then $M \geq l = j - 2^{s_t} + 2^v \geq K_t - 2^{s_t} + 2^v$ gives $2^v \leq M - K_t + 2^{s_t} < 2^{s_t} + 2^{s_t}$, and we get $v < s_t$. So we have $l > b = j - 2^{s_t} \geq K_t - 2^{s_t} = K_{t-1}$ and $l = b + 2^v \leq L_t - 2^{s_t} + 2^{s_t - 1} = L_t - 2^{s_t-1} = L_{t-1}$. □

Lemma 4.4 *Assume that $j \in B_t$ where $0 \leq t < n$. Then taking $b = j - 2^{s_{t+1}-1}$ in Lemma 4.2, we have*

$$X_{N-j} \circ X_j = \sum_{\alpha(l)=\alpha(j)} \binom{l}{b} X_{N-l} \circ X_l + \sum_{\alpha(k)>\alpha(j)} c_k\, X_{N-k} \circ X_k$$

where $l \in A_h \cup B_h$ for some $h > t$ or $l \in A_t$ whenever $\binom{l}{b} \not\equiv 0 \bmod 2$ and $l \leq M$, $l \neq j$.

Proof: Note that $2^{s_{t+1}-1}$ does appear in the binary expansion of j, since

$$K_t + 2^{s_{t+1}-1} \leq (K_t + M)/2 = L_t < j < K_{t+1} = K_t + 2^{s_{t+1}}$$

and also, $s_{t+1} \geq 1$ if B_t is non-empty. By Lemma 4.1, $\binom{l}{b} \not\equiv 0 \bmod 2$ gives $l = b + 2^v$. So if $l \leq M$,

$$2^v = l - j + \frac{1}{2} 2^{s_{t+1}} \leq M - L_t + \frac{1}{2} 2^{s_{t+1}} < \frac{3}{2} 2^{s_{t+1}}$$

and we get $v \le s_{t+1}$. But $v \ne s_{t+1} - 1$, since $l \ne j$.

Case $v = s_{t+1}$. Claim: $l \in A_h \cup B_h$ with $h \ge t+1$.

The reason is that $l = b + 2^{s_{t+1}} = j + 2^{s_{t+1}-1} > L_t + 2^{s_{t+1}-1} = L_{t+1}$.

Case $v \le s_{t+1} - 2$. Claim: $l \in A_t$.

If $\begin{pmatrix} l \\ b \end{pmatrix} \not\equiv 0 \bmod 2$, we must have $2^v \not\subset j$. This, with $j < K_{t+1}$, gives $j + 2^v < K_{t+1}$. Then

$$l = b + 2^v < K_{t+1} - 2^{s_{t+1}-1} = (K_t + K_{t+1})/2 \le (M + K_t)/2 = L_t$$

but

$$l > b > L_t - 2^{s_{t+1}-1} = (K_t + M - 2^{s_{t+1}})/2 \ge K_t$$

□

By applying Lemmas 4.3 and 4.4 as necessary, finitely many times, and noting that $l \le M/2$ if $l \in A_0$, we obtain the crucial step in our reduction.

Corollary 4.5 *We have*

$$X_{N-j} \circ X_j = \sum_l c_l X_{N-l} \circ X_l$$

where $c_l \ne 0$ *only if* $\alpha(l) > \alpha(j)$ *or* $l > M$ *or* $l \le M/2$.

By induction on $\alpha(j)$, we deduce

Corollary 4.6 *We have*

$$X_{N-j} \circ X_j = \sum_l c_l X_{N-l} \circ X_l$$

where $c_l \ne 0$ *only if* $l > M$ *or* $l \le M/2$.

Proposition 4.7 *For any integers i and j, we have*

$$X_i \circ X_{2j+1} = \sum_{s>0} \binom{j+s}{s} X_{i+1-2s} \circ X_{2(j+s)}$$

Proof: Let $i + 2j + 1 = N$. Taking $b = 2j$ in Lemma 4.2, we have

$$\sum_{k>j} \binom{2k}{2j} X_{N-2k} \circ X_{2k} + \sum_{k\geq j} \binom{2k+1}{2j} X_{N-(2k+1)} \circ X_{2k+1} = 0$$

Taking $b = 2j + 1$ in Lemma 4.2, we get

$$\sum_{k>j} \binom{2k+1}{2j+1} X_{N-(2k+1)} \circ X_{2k+1} = 0$$

But

$$\binom{2k}{2j} = \binom{2k+1}{2j} = \binom{2k+1}{2j+1} = \binom{k}{j}$$

Comparing the above two equalities and writing $k = j + s$, we get our result. □

Definition 4.8 *Given $I = (i_0, i_1, \ldots, i_{l-1})$ with $i_{l-1} > 0$, define the* length *of I by $l(I) = l$, and the* degree *of I by $d(I) = \sum_{k=0}^{l-1} i_k$. We call I* allowable *if $I = (j_0, 2j_1, \ldots, 2^{l-1}j_{l-1})$ with $j_k \leq j_{k+1}$ for all $0 \leq k < l-1$. Given I and J with $i_0 \leq i_1 \leq \cdots \leq i_{l-1}$ and $j_0 \leq j_1 \leq \cdots \leq j_{l-1}$, define $I > J$ lexicographically: there exists m with $0 \leq m < l$ such that $i_k = j_k$ for all $0 \leq k < m$, and $i_m > j_m$. Denote $X_I = X_{i_0} \circ X_{i_1} \circ \cdots \circ X_{i_{l-1}}$.*

We combine these results to obtain our theorem for length 2.

Theorem 4.9 *For any k and l, we have*

$$X_k \circ X_l = \sum_{i\leq k} c_i X_i \circ X_{2j}$$

where $i + 2j = k + l$ and in each nonzero term, $i \leq j$.

Proof: Write $N = k+l$, and choose $M = \lfloor (2N-1)/3 \rfloor$. First, we apply Corollary 4.6 to express $X_k \circ X_l$ in terms of monomials $X_i \circ X_j$ with $j > M$ or $j \leq M/2$.

Second, if $j \leq M/2$, we write $X_i \circ X_j = X_j \circ X_i$. This ensures only terms $X_i \circ X_j$ with $j \geq 2i$ and $i \leq k$.

Third, if j is odd, we apply Proposition 4.7. □

Theorem 4.10 *(a) Given I with $i_0 \leq i_1 \leq \cdots \leq i_{l-1}$ which is not allowable, we have*

$$X_I = \sum_{J<I} c_J \, X_J$$

summing over J with $l(J) = l(I)$ and $d(I) = d(J)$.

(b) For any I, we have

$$X_I = \sum_{J \leq I} c_J \, X_J$$

where J is allowable, $l(J) = l(I)$ and $d(J) = d(I)$.

Proof: We will use induction on the length to prove this theorem. The case of length 2 is Theorem 4.9. Next we discuss the case of length 3 to clarify the key idea of the proof, which we can make explicit.

Given any monomial $X_u \circ X_v \circ X_w$, we apply Theorem 4.9 to $X_u \circ X_v$ if this is not allowable, or to $X_v \circ X_w$ if this is not allowable. We repeat until we have only terms $X_{u'} \circ X_{v'} \circ X_{w'}$ with both $X_{u'} \circ X_{v'}$ and $X_{v'} \circ X_{w'}$ allowable. Then we have

$$X_u \circ X_v \circ X_w = \sum_{i \leq j \leq k} c \, X_i \circ X_{2j} \circ X_{4k+2} + \sum_K X_K$$

for certain K, where K is allowable and $K \leq (u,v,w)$, and certain triples (i,j,k) that satisfy $(i, 2j, 4k+2) \leq (u,v,w)$ if $c \neq 0$. Of course, all terms have the same degree and length.

Now taking $b = 4k$ in Lemma 4.2, we have

$$X_i \circ X_{2j} \circ X_{4k+2} = X_i \circ X_{2j+1} \circ X_{4k+1} + \sum_{j'<2j} c\, X_i \circ X_{j'} \circ X_{k'}$$

The first term does not have the required form, but by Proposition 4.7,

$$X_i \circ X_{2j+1} \circ X_{4k+1} = \sum_{s>0} \binom{j+s}{s} X_{i+1-2s} \circ X_{2(j+s)} \circ X_{4k+1}$$

This proves (a) for length 3, and (b) follows by repeatedly applying (a) to each non-allowable term on the right. The process terminates because there are only finitely many monomials with given length and degree.

Suppose we have proved the theorem for the length less than $n+2$, now we deal with length $n+2$. Again, for any $U = (u_0, u_1, \ldots, u_{n+1})$ with $u_0 \leq u_1 \leq \cdots \leq u_{n+1}$, we get the following result if we apply part (b) of our theorem for length $n+1$, as often as possible:

$$X_U = \sum_{I \leq U} c_I\, X_I + \sum_{K \leq U} c_K\, X_K$$

where (1) each K is allowable, and (2) each I has the form $(i_0, 2i_1, \ldots, 2^n i_n, 2^{n+1} i_{n+1} + 2^n)$ with $i_0 \leq i_1 \leq \cdots \leq i_{n+1}$.

Now taking $b = 2^{n+1} i_{n+1}$ in Lemma 4.2, we have

$$\begin{aligned} & X_{i_0} \circ X_{2i_1} \circ \cdots \circ X_{2^{n-1} i_{n-1}} \circ X_{2^n i_n} \circ X_{2^{n+1} i_{n+1} + 2^n} \\ = & \sum_{s=1}^{2^n - 1} c_s\, X_{i_0} \circ X_{2i_1} \circ \cdots \circ X_{2^{n-1} i_{n-1}} \circ X_{2^n i_n + 2^n - s} \circ X_{2^{n+1} i_{n+1} + s} \\ & + \sum_{j' < 2^n i_n} c_{j'}\, X_{i_0} \circ X_{2i_1} \circ \cdots \circ X_{2^{n-1} i_{n-1}} \circ X_{j'} \circ X_{k'} \end{aligned}$$

The terms in the second sum are acceptable. Applying part (b) of our theorem for length $n+1$ to a typical term in the first sum, we get

$$X_{i_0} \circ X_{2i_1} \circ \cdots \circ X_{2^n i_n + 2^n - s} \circ X_{2^{n+1} i_{n+1} + s} = \sum_{I'} c_{I'}\, X_{I'} \circ X_{2^{n+1} i_{n+1} + s}$$

where $I' = (i'_0, 2i'_1, \ldots, 2^n i'_n) \leq (i_0, 2i_1, \ldots, 2^n i_n + 2^n - s)$. If $i'_k = i_k$ for all $k \leq n-1$, the equation

$$\sum_{k=0}^{n} 2^k {i'}_k = \sum_{k=0}^{n} 2^k i_k + 2^n - s$$

gives a contradiction, as $0 < s < 2^n$. Hence there exists an integer $m \leq n-1$ such that $i'_k = i_k$ for all $0 \leq k < m$ and $i'_m < i_m$. Thus $I' < (i_0, 2i_1, \ldots, 2^{n-1} i_{n-1}, 2^n i_n)$. This proves part (a) of the theorem, and again, part (b) follows from part (a). □

With our notation, and Theorem 4.10, we have

Theorem 4.11 *Every element $Q^I e_k$ of $H_*(QS^k)$ can be written as a linear combination of elements of the form $X_I \circ e_k$, where I is allowable.*

Theorem 4.12 *As an algebra*

$$H_*(QS^0) = P[\, X_I \mid I \;\; is \;\; allowable, \;\; i_0 > 0 \,] \otimes \mathbb{F}_2[\mathbb{Z}]$$

$$H_*(QS^k) = P[\, X_I \circ e_k \mid I \;\; is \;\; allowable \;\; i_0 > k \,]$$

Proof: Note that $X_0 = [2]$. Then $X_0 \circ X_{2I} = {X_I}^{*2}$ is not needed. Again, $e_k \circ X_k = Q^k e_k = e_k^{*2}$ and $e_k \circ X_k \circ X_{2I} = e_k^{*2} \circ X_{2I} = (e_k \circ X_I)^{*2}$ is not needed. For $i < k$, Example 2.6 and Theorem 2.4(3) give us $e_k \circ X_i = 0$.

We next give a counting argument to show that we have the correct number of generators in each degree. Given $I = (i_0, i_1, \ldots, i_{n-1})$ admissible, we take

$$j_0 = e(I), \;\; j_1 = 2i_1 - i_0, \;\; \ldots, \;\; j_{n-1} = 2i_{n-1} - i_{n-2}$$

then $I' = (j_0, 2(j_0 + j_1), \ldots, 2^{n-1}(i_0 + i_1 + \cdots + i_{n-1}))$ is allowable and $\deg(Q^I) = \deg(X_{I'})$. It follows that the X_I must be polynomial generators. □

We should point out that Turner had proved the first part of Theorem 4.12 with Dickson coinvariants and transfer [T], but his method cannot be applied to the odd prime situation. And the second part of Theorem 4.12 has been proved by Wilson et al. [ETW] using bar spectral sequences.

5 The Formulae for the p-th Power

In this section, we only discuss odd primes p.

Definition 5.1 *Consider elements written in the form*

$$y = \beta Q^t x$$

where $\beta x = 0$. *Define the* pseudo-excess *of* y *as*

$$\mathrm{pex}(y) = 2t - \deg(x)$$

Lemma 5.2 *If* $\mathrm{pex}(y) \leq 0$, *then* $y = 0$.

This is a direct conclusion of Theorem 2.4(3) and (4).

Applying Theorem 2.6 to the spaces $B = \{QS^k\}$ for $k \geq 0$ by taking $b = [1]$, we have

Lemma 5.3

$$Y_k \circ f = \sum_i \beta Q^{k+i} P_*^i f$$

for any f *such that* $\beta f = 0$. *Also*

$$X_k \circ f = \sum_i Q^{k+i} P_*^i f$$

For instance, we have $Y_k \circ e_n = \beta Q^k e_n$.

In the following results, c, c_i and c' etc. denote numerical coefficients in which we are not interested.

Lemma 5.4 *Assume* $t \leq m+1$ *and* $\beta x = 0$. *Put* $h = \mathrm{pex}(\beta Q^t x)$. *Then*

$$Y_{mp-1} \circ \beta Q^t x = \beta Q^{(p-1)m+t-1}(Y_m \circ x) + \sum c' y'$$

where the first term has pseudo-excess $h-1$ *and each* y' *has the form* $\beta Q^{t'} x'$ *with* $\mathrm{pex}(\beta Q^{t'} x') \leq h-2$, $t' < pm$ *and* $\beta x' = 0$.

Proof: By Lemma 5.3, and applying the Nishida relation, we have

$$\begin{aligned} Y_{mp-1} \circ \beta Q^t x &= \sum_i \beta Q^{mp-1+i} P_*^i \beta Q^t x \\ &= \sum_{i,i'} c' \beta Q^{mp-1+i} \beta Q^{t-i+i'} P_*^{i'} x \end{aligned}$$

where $i \geq pi'$ i.e., $i/p \geq i'$, and $c' = 1$ if $i = p\, i'$.

Now we apply the Adem relation

$$\beta Q^{mp-1+i} \beta Q^{t-i+i'} = \sum_s c_s \beta Q^{pm-1+t+i'-s} \beta Q^s$$

where $ps \geq pm - 1 + i + 1$, i.e, $s \geq m + i/p$, and $c_s = 1$ in case $s = m + i/p$. Write

$$t_1 = pm - 1 + t + i' - s$$

and we have the following summation

$$Y_{mp-1} \circ \beta Q^t x = \sum_{i,i',s} c \beta Q^{t_1} \beta Q^s P_*^{i'} x = \sum_{i,i',s} c \beta Q^{t_1} x_1$$

where $x_1 = \beta Q^s P_*^{i'} x$. Then we have

$$t_1 \leq (p-1)m + t - 1$$

and

$$\deg(x_1) = 2(p-1)s + \deg(x) - 1 - 2(p-1)i' \geq 2(p-1)m + \deg(x) - 1$$

Thus $\operatorname{pex}(\beta Q^{t_1} x_1) \leq h - 1$, with equality only if $s = m + i'$ and $i = p\, i'$, in which case $c = 1$.

By now, the result of our lemma is obvious, with the help of Lemma 5.3. □

Lemma 5.5 *Assume $\beta x = 0$, $t \leq m$, and $\operatorname{pex}(\beta Q^t x) = 1$. Then*

$$X_{pm-1} \circ \beta Q^t x = (Y_m \circ x)^{*p}$$

Proof: The proof is similar to the proof of Lemma 5.4. By Lemma 5.3, and applying the Nishida relation, we have

$$\begin{aligned} X_{mp-1} \circ \beta Q^t x &= \sum_i Q^{mp-1+i} P_*^i \beta Q^t x \\ &= \sum_{i,i'} c' Q^{mp-1+i} \beta Q^{t-i+i'} P_*^{i'} x \end{aligned}$$

where $i \geq pi'$ i.e., $i/p \geq i'$, and $c' = 1$ if $i = p\, i'$.

Now we apply the Adem relation

$$Q^{mp-1+i} \beta Q^{t-i+i'} = \sum_s c_s Q^{pm-1+t+i'-s} \beta Q^s + \sum_u c_u \beta Q^{pm-1+t+i'-u} Q^u$$

where $ps \geq pm - 1 + i + 1$, i.e, $s \geq m + i/p$, and $pu \geq pm - 1 + i$. Write

$$t_1 = pm - 1 + t + i' - s$$

$$t_2 = pm - 1 + t + i' - u$$

and we have the following summation

$$\begin{aligned} X_{mp-1} \circ \beta Q^t x &= \sum_{i,i',s} c' c_s\, Q^{t_1} \beta Q^s P_*^{i'} x + \sum_{i,i',u} c' c_u\, \beta Q^{t_2} Q^u P_*^{i'} x \\ &= \sum_{i,i',s} c' c_s\, Q^{t_1} x_1 + \sum_{i,i',u} c' c_u\, \beta Q^{t_2} x_2 \end{aligned}$$

where $x_1 = \beta Q^s P_*^{i'} x$ and $x_2 = Q^u P_*^{i'} x$. For the first summation, with the same discussion as above, taking $h = 1$, Lemma 5.2 shows that the only surviving terms are

$$\sum_{i,i',s} c\, Q^{t_1} x_1 = (Y_m \circ x)^{*p}$$

For the second summation, we have

$$\begin{aligned} pt_2 &= p^2 m - p + pt + pi' - pu \\ &\leq p^2 - p + pt + pi' - pm + 1 - i \\ &\leq p^2 m - p + pt - pm + 1 \end{aligned}$$

So again we have

$$t_2 \leq (p-1)m + t - 1$$

and

$$\begin{aligned} p\deg(x_2) &= 2(p-1)pu + p\deg(x) - 2(p-1)pi' \\ &\geq 2(p-1)(pm-1) + p\deg(x) \\ &= 2p^2m - 2pm - 2p + 2 + p\deg(x) \end{aligned}$$

So we get

$$\deg(x_2) \geq 2(p-1)m + \deg(x) - 1$$

Thus $\text{pex}(\beta Q^{t_2} x_2) \leq 0$, and we get $\beta Q^{t_2} x_2 = 0$ from Lemma 5.2. □

By induction, we get

Theorem 5.6 *Given* $m_1, m_2, \ldots, m_{k+1}$ *where* $m_{l+1} \geq n + (p-1)[m_1 + \cdots + m_l] - l$ *for all* $l \geq 1$ *and* $m_1 \geq n-1$, *we have*

$$\begin{aligned} &X_{pm_{k+1}-1} \circ Y_{pm_k - 1} \circ \cdots \circ Y_{pm_2-1} \circ Y_{pm_1-1} \circ Y_n \circ e_{2n-k-1} \\ &\quad = (Y_{m_{k+1}} \circ Y_{m_k} \circ \cdots \circ Y_{m_2} \circ Y_{m_1} \circ e_{2n-k-1})^{*p} \end{aligned}$$

Proof: By induction on l for $0 \leq l \leq k$,

$$\begin{aligned} &Y_{pm_l-1} \circ \cdots \circ Y_{pm_2-1} \circ Y_{pm_1-1} \circ Y_n \circ e_{2n-k-1} \\ &= \beta Q^{n+(p-1)(m_1+m_2+\cdots+m_l)-l}(Y_{m_l} \circ \cdots \circ Y_{m_2} \circ Y_{m_1} \circ e_{2n-k-1}) + \sum c'y' \end{aligned}$$

where the first term has pseudo-excess $k+1-l$, each y' has the form $y' = \beta Q^{t'} x'$ with $\text{pex}(y') \leq k - l$, and $t' < n + (p-1)(m_1 + m_2 + \cdots + m_l) - l$.

The induction starts from $l = 0$, which is

$$Y_n \circ e_{2n-k-1} = \beta Q^n e_{2n-k-1}$$

Lemma 5.4 gives the induction step.

When $l = k$, apply Lemma 5.5 and note that there are no terms $c'y'$ by Lemma 5.2. □

Denote $\Delta_l = 1 + p + p^2 + \cdots + p^{l-1}$ for $l \geq 1$, and $\Delta_0 = 0$. The following two results are the special cases of this Theorem that we need.

Theorem 5.7 *When $i_0 \geq n - k$ and $i_j > 0$ for all $j \geq 1$,*

$$\begin{aligned}
&(e_{2n-1} \circ Y_{i_0+2k} \circ Y_{p[i_0+i_1+(2k-1)]-\Delta_1} \circ \cdots \circ Y_{p^{2k}[i_0+\cdots+i_{2k}]-\Delta_{2k}})^{*p} \\
&= \quad e_{2n-1} \circ Y_{n+k} \circ Y_{p[i_0+2k]-\Delta_1} \circ Y_{p^2[i_0+i_1+(2k-1)]-\Delta_2} \\
&\quad \circ \cdots \circ Y_{p^{2k}[i_0+\cdots+i_{2k-1}+1]-\Delta_{2k}} \circ X_{p^{2k+1}[i_0+\cdots+i_{2k}]-\Delta_{2k+1}}
\end{aligned}$$

Theorem 5.8 *When $i_0 \geq n - k$ and $i_j > 0$ for all $j \geq 1$,*

$$\begin{aligned}
&(e_{2n} \circ Y_{i_0+(2k-1)} \circ Y_{p[i_0+i_1+(2k-2)]-\Delta_1} \circ \cdots \circ Y_{p^{2k-1}[i_0+\cdots+i_{2k-1}]-\Delta_{2k-1}})^{*p} \\
&= \quad e_{2n} \circ Y_{n+k} \circ Y_{p[i_0+(2k-1)]-\Delta_1} \circ Y_{p^2[i_0+i_1+(2k-2)]-\Delta_2} \\
&\quad \circ \cdots \circ Y_{p^{2k-1}[i_0+\cdots+i_{2k-2}+1]-\Delta_{2k-1}} \circ X_{p^{2k}[i_0+\cdots+i_{2k-1}]-\Delta_{2k}}
\end{aligned}$$

6 The Generators of the Hopf Ring $H_*(QS^k;\mathbb{F}_p)$

Now we are going to construct the generator set for the Hopf ring $H_*(QS^k;\mathbb{F}_p)$ for $k \geq 0$, with p an odd prime, by analogy with the case $p = 2$.

Let $S = (s_1, s_2 \ldots, s_n)$ with $s_1 > s_2 > \cdots > s_n \geq 0$ and $A = (a_1, a_2, \ldots, a_n)$ with $0 < a_k < p$ for all $1 \leq k \leq n$. Then any integer M can be written uniquely in the form $M = Ap^S = a_1 p^{s_1} + a_2 p^{s_2} + \cdots + a_n p^{s_n}$. Then $\alpha(M)$ is defined as $\sum_{k=1}^{n} a_k$. And also if $T = (t_1, t_2 \ldots, t_m)$ with $t_1 > t_2 > \cdots > t_m \geq 0$ and $B = (b_1, b_2, \ldots, b_m)$ with $0 < b_k < p$ for all $1 \leq k \leq m$, we define $Ap^S \subset Bp^T$ to mean that for each $k\,(1 \leq k \leq n)$ there is an $h\,(1 \leq h \leq m)$ such that $s_k = t_h$ and $a_k \leq b_h$.

Recall that

Lemma 6.1 *For any positive integers k and b such that $k > b$, $\binom{k}{b} \not\equiv 0 \bmod p$ if and only if $\alpha(k) > \alpha(b)$ and $b \subset k$.*

Let M be a positive integer (to be chosen later). Write $M = a_1 p^{s_1} + a_2 p^{s_2} + \cdots + a_n p^{s_t}$ with $s_1 > s_2 > \cdots > s_n \geq 0$ and $0 < a_k < p$ for each $k\,(1 \leq k \leq n)$, as above.

Definition 6.2 *For any $i\,(1 \leq i \leq n)$, define*

$$K_t^i = \sum_{k=1}^{i-1} a_k p^{s_k} + t p^{s_i}$$

where $0 \leq t \leq a_i$, and

$$L_t^i = K_t^i + \frac{M - K_t^i}{p}$$

We define sets of integers

$$A_t^i = \{j \in \mathbb{Z} : K_t^i \leq j \leq L_t^i\}$$

for $0 \leq t \leq a_i$, *and*

$$B_t^i = \{j \in \mathbb{Z} : L_t^i < j < K_{t+1}^i\}$$

for $0 \leq t < a_i$.

From the above definition, we have

Proposition 6.3 *(1)* $K_0^1 = 0, \quad L_0^1 = M/p, \quad K_{a_n}^n = L_{a_n}^n = M.$

(2) For any i $(1 \leq i \leq n)$, *if* $u > s_i$

$$K_{a_i}^i + p^u > M$$

(3) For any i $(1 \leq i < n)$,

$$K_{a_i}^i = K_0^{i+1}, \quad L_{a_i}^i = L_0^{i+1}, \quad A_{a_i}^i = A_0^{i+1}$$

(4) The sets A_0^1, $\{A_t^i : 1 \leq i \leq n,\ 1 \leq t \leq a_i\}$, *and* $\{B_t^i : 1 \leq i \leq n,\ 0 \leq t < a_i\}$ *form a partition of the set* $\{j \in \mathbb{Z} : 0 \leq j \leq M\}$.

(5) $A_0^1 = \{j \in \mathbb{Z} : 0 \leq j \leq M/p\}$

We give the analogues of Lemmas 4.3 and 4.4.

Lemma 6.4 *Assume that* $j \in A_t^i$, *where* $1 \leq t \leq a_i$. *Suppose* $l \neq j$, $l \leq M$, *and* $l \neq j - p^{s_i}$. *Then* $\begin{pmatrix} l \\ j - p^{s_i} \end{pmatrix} \not\equiv 0 \bmod p$ *only when*

(i) $\alpha(l) > \alpha(j)$ *or*

(ii) $\alpha(l) = \alpha(j)$ *and* $l \in A_{t-1}^i$.

Proof: From Lemma 6.1, we have $\alpha(l) \geq \alpha(j)$. If $\alpha(l) = \alpha(j)$, we must have $l = j - p^{s_i} + p^u$. Then $l \leq M$ implies that $u \leq s_i$. Since $l \neq j_1$, we must have $u < s_i$, hence $K_{t-1}^i \leq l \leq L_{t-1}^i$. $\square$

Lemma 6.5 *Assume that* $j \in B^i_t$, *where* $0 \le t < a_i$. *Suppose* $l \ne j$, $l \le M$, *and* $l \ne j - p^{s_i - 1}$. *Then* $\binom{l}{j-p^{s_i-1}} \not\equiv 0 \bmod p$ *only when*

(i) $\alpha(l) > \alpha(j)$ *or*

(ii) $\alpha(l) = \alpha(j)$ *and one of the following is true:*

(a) $l \in A^v_k \cup B^v_k$ *where* $v > i$

(b) $l \in A^i_k \cup B^i_k$ *where* $k > t$

(c) $l \in A^i_t$

(d) $l \in B^i_t$ *and* $l < j$.

Proof: From Lemma 6.1, we have $\alpha(l) \ge \alpha(j)$. If $\alpha(l) = \alpha(j)$, $l = j - p^{s_i-1} + p^u$, with $u \ne s_i - 1$. Then $l \le M$ implies that $u \le s_i$. If $u = s_i$, $l \ge K^i_{t+1}$ so $l \in A^v_k \cup B^v_k$ as in (a) or (b). If $u \le s_i - 2$, we have $l < j$ and $l \ge K^i_t$ as in (c) or (d). □

Recall that we have proved the formulae in Section 3.

Lemma 6.6 *For any positive integer* N *and* $0 \le b$, *we have*

(a)

$$\sum_{(p-1)j>b} \binom{(p-1)j}{b} X_{N-j} \circ X_j = 0$$

(b)

$$\sum_{(p-1)j-1>b} \binom{(p-1)j-1}{b} Y_j \circ X_{N-j} = 0$$

(c) If $(b+1) \not\equiv 0 \bmod (p-1)$,

$$\sum_{(p-1)j>b} \binom{(p-1)j}{b} Y_{N-j} \circ X_j = 0$$

(d) If $(b+1) \equiv 0 \bmod (p-1)$, *say* $b = (p-1)s - 1$ *for some* $s > 0$,

$$X_{N-s} \circ Y_s + \sum_{j \ge s} \binom{(p-1)j}{(p-1)s-1} Y_{N-j} \circ X_j = 0$$

Definition 6.7 *Let* $I = (i_0, i_1, \ldots, i_{l-1})$ *be a sequence of non-negative integers. Define the* length $L(I)$ *of* I *to be* l, *the* degree *of* I *by* $D(I) = \sum_{k=0}^{l-1} i_k$. I *is called* X-allowable *if* $I = (j_0, pj_1, \ldots, p^{l-1}j_{l-1})$ *with* $j_k \leq j_{k+1}$ *for all* $0 \leq k < l-1$. *We order the sequences lexicographically, as before, and write* $I < J$. *Denote* $X_I = X_{i_0} \circ X_{i_1} \circ \cdots \circ X_{i_{l-1}}$.

In the statements and proofs of the following results, c or c_J denotes an unknown coefficient in which we are not interested. We first consider the case of length 2.

Lemma 6.8 *If* j *is not a multiple of* p, *we can write*

$$X_i \circ X_j = \sum_{k<i} c_k \, X_k \circ X_{i+j-k}$$

Proof: Write $(p-1)j = pm + a$ with $0 < a < p$. We take $b = (p-1)j - 1 = pm + a - 1$ in Lemma 6.6(a) and find

$$jX_i \circ X_j = \sum_{l>j} c_l \, X_{i+j-l} \circ X_l$$

□

Theorem 6.9 *For any* i *and* j, *we have*

$$X_i \circ X_j = \sum c_k \, X_k \circ X_{pl}$$

where in each term, $k + pl = i + j$, $k \leq i$, *and* $l \geq k$.

Proof: We put $N = i + j$ and choose

$$M = \lfloor [(p-1)(pN - p + 1)]/(p+1) \rfloor$$

If $j \in A_t^m$, with $0 < t \leq a_m$, we take $b = (p-1)j - p^{s_m}$ in Lemma 6.6(a) and use Lemma 6.4 to write

$$X_{N-j} \circ X_j = \sum_l c_l \, X_{N-l} \circ X_l$$

where $c_l \neq 0$ only if $(p-1)l > M$ or $\alpha((p-1)l) > \alpha((p-1)j)$ or $\alpha((p-1)l) = \alpha((p-1)j)$ and $l \in A_{t-1}^m$.

If $j \in B_t^m$, with $0 \leq t < a_m$, we take $b = (p-1)j - p^{s_m - 1}$ in Lemma 6.6(a) and similarly use Lemma 6.5 to write

$$X_{N-j} \circ X_j = \sum_l c_l \, X_{N-l} \circ X_l$$

where $c_l \neq 0$ only if $(p-1)l > M$ or $(p-1)l$ satisfies any of the conditions of Lemma 6.5.

Keeping in mind that $A_0^{m+1} = A_{a_m}^m$, we see that after applying these Lemmas finitely many times, we can express any $X_{N-j} \circ X_j$ in terms of monomials $X_{N-l} \circ X_l$ for which $(p-1)l > M$ or $(p-1)l \in A_0^1$. If $(p-1)l \in A_0^1$, we have $(p-1)l \leq M/p$, and write $X_{N-l} \circ X_l = X_l \circ X_{N-l}$. In either case, our choice of M ensures that we have only terms $X_{N-l} \circ X_l$ for which $l \geq p(N-l)$. If l is not a multiple of p we apply Lemma 6.8 as often as necessary. □

Recall $\Delta_n = 1 + p + p^2 + \cdots + p^{n-1} = (p^n - 1)/(p-1)$ for $n > 0$, thus $(p-1)\Delta_n = p^n - 1$.

Theorem 6.10 *(a) For any I which is not X-allowable, we have*

$$X_I = \sum_{J<I} c_J \, X_J$$

summing over J with $D(J) = D(I)$ and $L(J) = L(I)$.

(b) For any I, we have

$$X_I = \sum_{J \le I} c_J \, X_J$$

where J is X-allowable and $D(J) = D(I)$ and $L(J) = L(I)$.

Proof: We will use induction on the length to prove this theorem. We have already proved the case of length of 2. Next we discuss the case of length 3 for illustration.

For any positive integers u, v and w, we get the following result if we apply Theorem 6.9 to $X_u \circ X_v$ or $X_v \circ X_w$ as often as possible:

$$X_u \circ X_v \circ X_w = \sum_{i \le j \le k} X_i \circ X_{pj} \circ X_{p^2k+mp} + \sum_K c_K \, X_K$$

where (1) each K is X-allowable, $K \le (u, v, w)$, (2) $(i, pj, p^2k + mp) \le (u, v, w)$, $0 < m < p$.

We take

$$b = (p-1)(p^2k + mp) - p = [(p-1)k + (m-1)]p^2 + (p - m - 1)p$$

in part (a) of Lemma 6.6. Since

$$(p-1)(p^2k + mp) - p < (p-1)l < (p-1)(p^2k + mp)$$

gives

$$p^2k + mp - 1 \le l < p^2k + mp$$

we have

$$(p - m) \, X_{pj} \circ X_{p^2k+mp} = c \, X_{pj+1} \circ X_{p^2k+mp-1} + \sum_{j' < pj} c_{j'} \, X_{j'} \circ X_{k'}$$

where $j' + k' = pj + p^2k + mp$, and so

$$X_i \circ X_{pj} \circ X_{p^2k+mp} = c\, X_i \circ X_{pj+1} \circ X_{p^2k+mp-1} + \sum_{j'<pj} c_{j'}\, X_i \circ X_{j'} \circ X_{k'}$$

To put the first term in the desired form, we apply Theorem 6.9

$$X_i \circ X_{pj+1} \circ X_{p^2k+mp-1} = \sum_{s\geq 1} c_s\, X_{i+1-ps} \circ X_{p(j+s)} \circ X_{p^2k+mp-1}$$

We have proved (a) for length 3, and (b) follows by applying (a) finitely many times.

Suppose that we have proved the theorem for the case of length $n+1$, now we deal with the case of length $n+2$. As in Section 4, for any $U = (u_0, u_1, \ldots, u_{n+1})$, we get the following result if we iterate part (b) of our theorem for length $n+1$ as often as possible:

$$X_U = \sum_{I\leq U} c_I\, X_I + \sum_{K\leq U} c_K\, X_K$$

where each K is X-allowable, and each I has the form $I = (i_0, pi_1, \ldots, p^n i_n, p^{n+1} i_{n+1} + mp^n)$ with $i_0 \leq i_1 \leq \cdots \leq i_n \leq i_{n+1}$, $0 < m < p$.

We take

$$b = (p-1)(p^{n+1} i_{n+1} + mp^n) - p^n = [(p-1)i_{n+1} + (m-1)]p^2 + (p-m-1)p^n$$

in part (a) of the Lemma 6.6. Since

$$b = (p-1)(p^{n+1} i_{n+1} + mp^n) - p^n < (p-1)j < (p-1)(p^{n+1} i_{n+1} + mp^n)$$

gives

$$(p^{n+1} i_{n+1} + mp^n) - \Delta_n \leq j < p^{n+1} i_{n+1} + mp^n$$

we have

$$(p-m)\, X_{p^n i_n} \circ X_{p^{n+1} i_{n+1} + mp^n} = \sum_{s=1}^{\Delta_n} c_s\, X_{p^n i_n + s} \circ X_{p^{n+1} i_{n+1} + mp^n - s} + \sum_{j'<p^n i_n} c_{k'}\, X_{j'} \circ X_{k'}$$

For the typical term in the first sum, we apply part (b) of our theorem for length $(n+1)$ to get

$$X_{i_0} \circ X_{pi_1} \circ \cdots \circ X_{p^n i_n + s} \circ X_{p^{n+1} i_{n+1} + mp^n - s} = \sum_{I'} X_{I'} \circ X_{p^{n+1} i_{n+1} + mp^n - s}$$

where $I' = (i'_0, pi'_1, \ldots, p^n i'_n) \leq (i_0, pi_1, \ldots, p^n i_n + s)$.

So $I' < (i_0, pi_1, \ldots, p^n i_n)$ unless $i'_0 = i_0, \ldots, i'_{n-1} = i_{n-1}$, which cannot happen since all terms have the same degree, and this would imply

$$p^n i'_n + (p^{n+1} i_{n+1} + mp^n - s) = p^n i_n + (p^{n+1} i_{n+1} + mp^n)$$

which is absurd.

So we have successfully proved part (a) of our theorem for the case $n+2$. Again, part (b) follows. □

Now we discuss the reduction of terms $Y_j \circ X_{N-j}$.

Theorem 6.11 *For any positive integers k and l, we have*

$$Y_k \circ X_l = \sum_{j \geq i > 0} c_i \, Y_i \circ X_{pj} + \sum_{j' \geq i' > 0} c_{i'} Y_{i'} \circ X_{pj'-1}$$

where $i + pj = i' + pj' - 1 = k + l$, $i \leq k$, and $i' \leq k$.

Proof: We put $N = k + l$ and choose $M = \lfloor [(p-1)pN - 1]/(p+1) \rfloor$. We imitate the proof of Theorem 6.9, except that we use the other three parts of Lemma 6.6 instead of part (a), to express $Y_k \circ X_l$ in terms of monomials of the following types:

(i) $Y_{i_0} \circ X_{i_1}$ where $(p-1)i_0 - 1 \leq M/p$. Then $(p-1)i_0 - 1 \leq [(p-1)N - 1]/(p+1)$, so

$$(p-1)(p+1)i_0 - (p+1) \leq (p-1)N - 1$$

$$(p+1)i_0 \leq N + \frac{p}{p-1} = N + 1 + \frac{1}{p-1}$$

Thus

$$(p+1)i_0 \leq N+1 = i_0 + i_1 + 1$$

and

$$pi_0 \leq i_1 + 1 < i_1 + p - 1$$

If $i_1 \equiv 0 \bmod p$ or $i_1 \equiv -1 \bmod p$, we are done. Otherwise we put $b = (p-1)i_1 - 2$ in Lemma 6.6 (c) and get

$$\binom{(p-1)i_1}{(p-1)i_1 - 2} Y_{i_0} \circ X_{i_1} = -\sum_{t<i_0} c_t Y_t \circ X_{N-t}$$

(ii) $Y_{i_0} \circ X_{i_1}$ where $(p-1)i_0 - 1 > M$. Then $(p-1)i_0 - 1 \geq [(p-1)pN]/(p+1)$, so

$$(p-1)(p+1)i_0 - (p+1) \geq (p-1)pN$$

$$(p+1)i_0 \geq pN + \frac{p+1}{p-1} > pN - 1$$

Then part (d) of Lemma 6.6 reduces this case to the previous case. □

Now we discuss the reduction of terms Y_I.

Proposition 6.12 *For any positive integers k and l, we have*

$$Y_k \circ Y_l = \sum_{j \geq i > 0} c_j \, Y_i \circ Y_{pj-1}$$

where in each term, $i + pj - 1 = k + l$ and $i \leq k$.

Proof: We put $N = k + l$ and choose $M = \lfloor [(p-1)pN - 1]/(p+1) \rfloor$ as before. Again, we imitate the proof of Theorem 6.11, except that we use Theorem 3.8 instead of Lemma 6.6, to express $Y_k \circ Y_l$ in terms of monomials of the following types:

(i) $Y_{i_0} \circ Y_{i_1}$ where $(p-1)i_0 - 1 \leq M/p$. As in the previous result, this implies

$$pi_0 \leq i_1 + 1 < i_1 + p - 1$$

If $i_1 \not\equiv -1 \bmod p$, we take $b = (p-1)i_1 - 2$ in Theorem 3.8 and obtain

$$Y_{i_0} \circ Y_{i_1} = -\sum_{t<i_0} c_t Y_t \circ Y_{N-t}$$

(ii) $Y_{i_0} \circ Y_{i_1}$ with $(p-1)i_0 - 1 > M$. As before, this implies $i_0 + 1 \geq pi_1$. Then $Y_{i_0} \circ Y_{i_1} = -Y_{i_1} \circ Y_{i_0}$ reduces this case to the previous case. □

Definition 6.13 *Given $I = (i_0, i_1, \ldots, i_{l-1})$ with every i_k positive, I is called* Y-allowable *when $I = (i_0, i_1 + \Delta_1, \ldots, i_{l-1} + \Delta_{l-1})$ is* X-allowable.

Denote $Y_I = Y_{i_0} \circ Y_{i_1} \circ \cdots \circ Y_{i_{l-1}}$.

Theorem 6.14 *(a) For any I which is not Y-allowable, we have*

$$Y_I = \sum_{J<I} c_J \, Y_J$$

summing over J with $D(J) = D(I)$ and $L(J) = L(I)$.

(b) For any I, we have

$$Y_I = \sum_{J<I} c_J \, Y_J$$

where J is Y-allowable and $D(J) = D(I)$.

Proof: We will use induction on the length to prove this theorem. We have already proved the case of length of 2. Next we discuss the case of length 3.

For any positive integers u, v and w, we get the following result if we iterate the above proposition finitely many times when necessary,

$$Y_u \circ Y_v \circ Y_w = \sum_{0<i\leq j<k} c_{ijk} Y_i \circ Y_{pj-1} \circ Y_{p^2k-mp-1} + \sum_K c_K \, Y_K$$

where each K is Y-allowable, $K \le (u,v,w)$, and $(i, pj-1, p^2k-mp-1) \le (u,v,w)$ with $2 \le m \le p$.

We take

$$b = (p-1)(p^2k - mp - 1) - 1 - p = [(p-1)k - m]p^2 + (m-2)p$$

in Theorem 3.8. Since

$$b = (p-1)(p^2k - mp - 1) - 1 - p < (p-1)l - 1 < (p-1)(p^2k - mp - 1) - 1$$

gives

$$p^2k - mp - 2 \le l < p^2k - mp - 1$$

we have

$$(m-1)\, Y_{pj-1} \circ Y_{p^2k-mp-1} = c\, Y_{pj} \circ Y_{p^2k-mp-2} + \sum_{j' < pj-1} c_{k'}\, X_{j'} \circ X_{k'}$$

and so

$$(m-1)\, Y_i \circ Y_{pj-1} \circ Y_{p^2k-mp-1} = c\, Y_i \circ Y_{pj} \circ Y_{p^2k-mp-2} + \sum_{j' < pj-1} c_{k'}\, Y_i \circ Y_{j'} \circ Y_{k'}$$

Then applying Proposition 6.12, we have

$$Y_i \circ Y_{pj} \circ Y_{p^2k-mp-2} = \sum_{s \ge 1} c_s\, Y_{i+1-ps} \circ Y_{p(j+s)-1} \circ Y_{p^2k-mp-2}$$

Every term now has the desired form, and we have proved (a) for length 3. As before, (b) follows from (a). The general case follows analogously, as in Theorem 6.10. □

With our notation and previous results, we have

Theorem 6.15 *Every element $Q^I e_k$ of $H_*(QS^k; \mathbb{F}_p)$ can be written as a linear combination of elements of the form $e_k \circ Y_J \circ X_I$ and $*$-decomposable elements,* *where J is Y-allowable of length l, I is X-allowable, $i_0 + 1 \geq pj_l$ if $l > 0$ with $i_0 = 0 \bmod p$ or $i_0 + \Delta_l = 0 \bmod p^l$ if l is odd, and $i_0 = 0 \bmod p$ if l is even.*

Theorem 6.16 *As an algebra*

$$H_*(QS^0; \mathbb{F}_p) = P[X_I] \otimes P[Y_J \circ X_{I'}] \otimes E[Y_{J'} \circ X_{I''}] \otimes \mathbb{F}_p[\mathbb{Z}]$$

$$H_*(QS^k; \mathbb{F}_p) = P[e_k \circ X_I] \otimes P[e_k \circ Y_J \circ X_{I'}] \otimes E[e_k \circ Y_{J'} \circ X_{I''}]$$

where $I = (i_0, i_1, \ldots, i_{n-1})$ is X-allowable and $i_0 > k/2$, and

(a) *If k is even, $J = (j_0, j_1, \ldots, j_{2l-1})$ is Y-allowable and $j_0 \geq k/2 + l - 1$ and $I' = (i'_0, i'_1, \ldots, i'_{n-1})$ is X-allowable, $i'_0 = p(j_{2l-1} + s)$ for some non-negative s, $J' = (j'_0, j'_1, \ldots, j'_{2m})$ is Y-allowable and $j'_0 \geq k + m$ and $I'' = (i''_0, i''_1, \ldots, i''_{n-1})$ is X-allowable, $i''_0 + 1 \geq pj_{2m}$ and $i''_0 = 0$ or $p - 1 \bmod p$.*

(b) *If k is odd, $J = (j_0, j_1, \ldots, j_{2l})$ is Y-allowable and $j_0 \geq k/2 + l$ and $I' = (i'_0, i'_1, \ldots, i'_{n-1})$ is X-allowable, $i'_0 = p(j_{2l} + s)$ for some non-negative s, $J' = (j'_0, j'_1, \ldots, j'_{2m-1})$ is Y-allowable and $j'_0 \geq k/2 + m + 1$ and $I'' = (i''_0, i''_1, \ldots, i''_{n-1})$ is X-allowable, $i''_0 + 1 \geq pj_{2m-1}$ and $i''_0 = 0$ or $p - 1 \bmod p$.*

References

[A] J. F. Adams, *Infinite Loop Spaces*, Annals of Math. Studies **90**, Princeton University Press, 1978.

[CLM] Fred R. Cohen, T. J. Lada and J. Peter May, *The Homology of Iterated Loop Spaces*, Lecture Notes in Mathematics **533**, Springer-Verlag, 1976.

[DL] Eldon Dyer and Richard K. Lashof, *Homology of Iterated Loop Spaces*, Amer. J. Math. **84** (1962), 35-88.

[ETW] Peter J. Eccles, Paul R. Turner and W. Stephen Wilson, *On the Hopf Ring for the Sphere*, to appear in Math. Z.

[May] J. Peter May, *Homology Operations on Infinite Loop Spaces*, Proc. Symp. in Pure Math., Amer. Math. Soc. **22** (1971), 171–185.

[MM] Ib Madsen and R. James Milgram, *The Classifying Spaces for Surgery and Cobordism of Manifolds*, Annals of Math. Studies **92**, Princeton University Press, 1979.

[MMj] John W. Milnor and John C. Moore, *On the Structure of Hopf Algebras*, Annals of Math. **81(2)**, (1965) 211–264.

[RW] Douglas C. Ravenel and W. Stephen Wilson, *The Hopf Ring for Complex Cobordism*, Jour. of Pure and Applied Algebra **9** (1977), 241–280.

[S] Richard Steiner, *Homology Operations and Power Series*, Glasgow Math. J. **24** (1983), 161–168.

[Sw] M. Sweedler, *Hopf Algebras*, Benjamin Inc. 1969.

[T] Paul R. Turner, *Dickson Coinvariants and the Homology of QS^0*, to appear in Math. Z.

[Tu] Paul R. Turner, *On the Homology of Certain Infinite Loop Spaces*, Ph.D Thesis, Manchester, 1993.

[TW] Robert W. Thomason and W. Stephen Wilson, *Hopf Rings in the Bar Spectral Sequence*, Quarterly J. Math. Oxford **31** (1980), 507–511.

Vita

Yanfei Li was born in Hebei province, China, on March 1, 1962. He received his Master of Sciences from Nankai University, Tianjin, China, in 1986. Afterwards, he worked in Beijing Normal Univeristy, China, as an instructor of mathematics. He started his doctoral studies at The Johns Hopkins University in 1990.