TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 347, Number 12, December 1995

$\mathscr{A}$-GENERATORS FOR THE DICKSON ALGEBRA

NGUYỄN H. V. HU'NG AND FRANKLIN P. PETERSON

ABSTRACT. Let D_k denote the Dickson algebra in k variables over the field of two elements. We study the problem of determining a minimal set of generators for D_k as a module over the Steenrod algebra $\mathscr{A}$. This is easy for $k = 1$ and 2. In this paper we answer this question for $k = 3$ and 4 and give techniques which may help solve the problem for general k.

1. INTRODUCTION

Let $P^k = H^*(RP^\infty \times \cdots \times RP^\infty; \mathbf{Z}/2)$, k-times, i.e. $P^k = \mathbf{Z}/2[x_1, \ldots, x_k]$, where $|x_i| = 1$. The general linear group $G = GL(k, \mathbf{Z}/2)$ acts on P^k, and the ring of invariants, $(P^k)^G = D_k$, was described by Dickson. He showed that $D_k \cong \mathbf{Z}/2[Q_{k-1}, Q_{k-2}, \ldots, Q_0]$, again a polynomial algebra in k variables, with $|Q_s| = 2^k - 2^s$ ([1]). Note that Q_s depends on k, and when necessary, will be denoted $Q_{k,s}$. An inductive definition of $Q_{k,s}$ is given by

$$Q_{k,s} = (Q_{k-1,s-1})^2 + V_k \cdot Q_{k-1,s},$$

where, by convention, $Q_{k,k} = 1$, $Q_{k,s} = 0$ for $s < 0$ and

$$V_k = \prod_{\lambda_i \in \mathbf{Z}/2} (\lambda_1 x_1 + \cdots + \lambda_{k-1} x_{k-1} + x_k).$$

Since the operations of $GL(k, \mathbf{Z}/2)$ on P^k commute with the action of the Steenrod algebra, D_k is also a module (in fact an algebra) over $\mathscr{A}$. The importance of D_k to topologists was first shown by Madsen [6] who calculated the dual to the Dyer–Lashof operations of length k, and by Mùi [2] who related this to D_k. Furthermore, the cohomology operations derived from the invariants in D_k are exactly the Steenrod–Milnor ones of length k (see Madsen–Milgram [7], Mùi [3]).

In this paper we investigate the structure of $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$, the minimal set of $\mathscr{A}$-generators for D_k. The motivation for this problem is provided by the fact that a calculation of $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for all k also calculates the $\mathscr{A}$-annihilated elements of $PH_*(Q_0 S^0)$ which form the bottom line of the E^2-term of the unstable Adams spectral sequence which converges to $\pi_*(Q_0 S^0)$ $(\cong \pi_*^s(S^0))$ (this has been studied by Wellington [10], who computed this in dimensions

Received by the editors November 26, 1993.
1991 *Mathematics Subject Classification.* Primary 55S10, 55T15, 55P47, 55Q40, 55S12.
Key words and phrases. Steenrod algebra, Dickson invariants.
The research of the first author was supported in part by an NSF grant and a JSPS fellowship.

< 200, and others). This problem is also related to the study of the Hurewicz map $\pi_*(Q_0S^0) \to H_*(Q_0S^0; \mathbf{Z}/2)$ (see Lannes–Zarati [4], [5]).

The paper is organized as follows. The key definitions and the main results are stated in Section 2. Then we give an outline of the proofs in Section 3. Section 4 deals with how to determine inductively all the allowed sequences of length k for any k. In Section 5, the fact that the allowed monomials generate $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for $k \leq 4$ is showed to be equivalent to the main lemma, whose proof is given in the next three sections. The linear independence of the allowed monomials is proved in Section 9 for $k \leq 4$. Finally, we give some remarks and conjectures in Section 10.

Acknowledgment. The authors would like to thank A. Dold and D. Puppe for providing them with an opportunity of working together at Heidelberg University in summer 1993 while the final version of the paper was being prepared and for the hospitality. The first author is grateful to G. Nishida for the hospitality and valuable discussions on the research during his visit to Kyoto University in the academic year 1991–1992. The authors also thank the referee for several suggestions which, they believe, have improved the exposition of this work.

2. Statement of results

Definition 2.1. (i) Let u be an integer. Define $s(u) = s_1(u)$ to be the maximal non-negative integer such that $u+1$ is divisible by $2^{s(u)}$ but not by $2^{s(u)+1}$.

For $u \neq -1$, $s(u)$ is well defined. Convention: $s(-1) = \infty$.

In other words, if $u \neq -1$, $u = 2^{s(u)} - 1 \bmod 2^{s(u)+1}$. That means, for $u \geq 0$, $s(u)$ is the non-negative integer with $2^{s(u)}$ being the first missing 2 power in the dyadic expansion of u.

(ii) Suppose $u \geq 0$. Define $s'(u) = s_2(u)$ to be the positive integer with $2^{s_2(u)}$ being the second missing 2 power in the dyadic expansion of u. That means $s_2(u) = s(u + 2^{s(u)})$.

Thus, if u is a non-negative integer, $u = 2^{s_1(u)} - 1 + 2^{s_1(u)+1} + \cdots + 2^{s_2(u)-1} + 2^{s_2(u)+1} \cdot t$, where t is a non-negative integer.

Definition 2.2. $u \rhd v$ if $v < 2^{s(u)}$. Here u, v are non-negative integers.

Remark 2.3. If $u \rhd v$ then $s(u) \geq s(v)$. The equality happens if and only if $v = 2^{s(u)} - 1$. In particular, $u \rhd u$ if and only if $u = 2^s - 1$ for some s.

Definition 2.4. $u \rhd\!\!\rhd v$ if $2^{s_1(u)} \leq v < 2^{s_2(u)}$ and $s_1(u) = s_1(v) = s_2(v) - 1$.

Let $I = (i_{k-1}, i_{k-2}, \ldots, i_0)$ be a sequence of k non-negative integers, with corresponding monomial $Q^I = Q_{k-1}^{i_{k-1}} \cdots Q_0^{i_0} \in D_k$. Let $h(I) = \sum_{j=0}^{k-1} i_j$, the classical degree of Q^I.

Definition 2.5. (i) I is *strongly allowed* if $h(I) \rhd i_{k-1} \rhd i_{k-2} \rhd \cdots \rhd i_0$.

(ii) I is *weakly allowed* if one or more $\rhd$ in the above definition is replaced by $\rhd\!\!\rhd$.

(iii) I is *allowed* if it is either strongly or weakly allowed.

(iv) Q^I is (strongly, weakly) *allowed* if I is.

Let us consider small values of k. If $k = 1$, then by Remark 2.3 $i_0 \rhd i_0$ if and only if $i_0 = 2^s - 1$. So it is well-known that the strongly allowed monomials form a basis for $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_1$.

If $k = 2$, then it is easy to check that $i_1 + i_0 \rhd i_1 \rhd i_0$ if and only if $i_1 = 2^s - 1$ and $i_0 = 0$. Thus the strongly allowed monomials form a basis of $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_2$ (see, e.g., Singer [9]).

Our first theorem is the following one.

Theorem 2.6. *Let $k = 3$. Then the set of strongly allowed monomials forms a basis for $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_3$.*

We note which I are strongly allowed for $k = 3$:

$$\begin{aligned} &(2^s - 1, 0, 0), && s \geq 0, \\ &(2^r - 2^s - 1, 2^s - 1, 1), && r > s > 0. \end{aligned}$$

The corresponding Q^I is of dimension $2^{s+2} - 4$ and $2^{r+2} + 2^{s+1} - 3$ respectively.

This pattern does not continue, as the set of strongly allowed monomials does not span D_k for $k > 3$. It should also be noted that there is no weakly allowed sequence for $k \leq 3$.

Our second theorem handles the case $k = 4$.

Theorem 2.7. *Let $k = 4$. Then the set of allowed monomials is a basis for $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_4$.*

We show that the only allowed sequences I for $k = 4$ are the following ones:

$$\begin{aligned} &(2^s - 1, 0, 0, 0), && s \geq 0, \\ &(2^r - 2^s - 1, 2^s - 1, 1, 0), && r > s > 0, \\ &(2^t - 2^r - 1, 2^r - 2^s - 1, 2^s - 1, 2), && t > r > s > 1, \\ &(2^r - 2^{s+1} - 2^s - 1, 2^s - 1, 2^s - 1, 2), && r > s + 1 > 2. \end{aligned}$$

The corresponding Q^I is of dimension $2^{s+3} - 8$, $2^{r+3} + 2^{s+2} - 6$, $2^{t+3} + 2^{r+2} + 2^{s+1} - 4$ and $2^{r+3} + 2^{s+1} - 4$ respectively.

Note that the last sequence with $r > s + 2$ is the only weakly allowed one. It has

$$h(I) \rhd\!\!\rhd i_3 \rhd i_2 \rhd i_1 \rhd i_0.$$

We hope to solve this problem for larger k in the future. The proofs of Theorems 2.6 and 2.7 are very long and complicated and involve studying many cases. In Section 3 we give formulae that are needed and describe the global structure of the proofs. The detailed lemmas are then proved in later sections.

3. Outline of the proofs

Many algebraic topologists have studied the Dickson algebra. For background, see the primer by Wilkerson [11].

We will need the action of $\mathscr{A}$ on D_k. This is given by the following theorem (see Hu'ng [8]).

Theorem 3.1 (Hai–Hu'ng).

$$Sq^i(Q_{k,s}) = \begin{cases} Q_{k,r}, & i = 2^s - 2^r,\ r \le s, \\ Q_{k,t}Q_{k,r}, & i = 2^k - 2^t + 2^s - 2^r,\ r \le s < t, \\ Q_{k,s}^2, & i = 2^k - 2^s, \\ 0, & \text{otherwise.} \end{cases}$$

Corollary 3.2. *Suppose q and l are non-negative integers with $0 \le l < k$. The submodule spanned by all Q^I with $i_l + i_{l-1} + \cdots + i_0 \ge q$ is an $\mathscr{A}$-ideal of D_k. Therefore, if $Sq^a(Q^I) = Q^J$ + other terms, then $j_l + j_{l-1} + \cdots + j_0 \ge i_l + i_{l-1} + \cdots + i_0$ for any $l < k$.*

From the definition of strongly allowed, if I is not strongly allowed, then it is easy to find a sequence K and an integer a so that $Sq^a(Q^K) = Q^I +$ other terms. We give here a canonical way to do that.

3.3. *If $i_m \not\vdash i_{m-1}$, $s = s(i_m)$, then*

$$Sq^{2^{s+m-1}} Q^{(\dots, i_m+2^s, i_{m-1}-2^s, \dots)} = Q^I + \text{other terms};$$

3.4. *Also, if $h(I) \not\vdash i_{k-1}$, $s = s(h)$, then*

$$Sq^{2^{s+k-1}} Q^{(i_{k-1}-2^s, i_{k-2}, \dots)} = Q^I + \text{ other terms.}$$

The trouble comes from the fact that a given pair (K, a) might be chosen by two or more different I's. The pair (K, a) is not uniquely determined by I and the proof shows that there are enough (K, a) for all of the I when $k = 3$. When $k = 4$, there are not enough pairs (K, a) and we need to add the weakly allowed generators.

More precisely,

Definition 3.5. Let $I = (i_{k-1}, \dots, i_0)$, define

$$m(I) = \min\{s(h(I)), s(i_{k-2} + \cdots + i_0 - 1), \dots, s(i_1 + i_0 - k + 2)\}.$$

The idea of the proof for $k = 3$ and 4 is to prove the following result. Let I be not allowed for $k = 3$ or 4 and $\bar{\mathscr{A}}$ the augmentation ideal in $\mathscr{A}$. Then we find a pair (K, a) such that $Sq^a(Q^K) = Q^I + \sum Q^J \bmod \operatorname{Im}\bar{\mathscr{A}}$, where either (1) $m(J) < m(I)$ or (2) $m(J) = m(I)$ and $h(J) < h(I)$ or (3) J is weakly allowed. These arguments show that the set of allowed sequences forms a spanning set of $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for $k = 3$ or 4.

One step in the proof of linear independence is to prove the following proposition.

Proposition 3.6. *Let $k = 3$ or 4. Suppose I is strongly allowed and*

$$Sq^a Q^K = Q^I + \text{other terms.}$$

Then $a = 0$ and $K = I$.

We note that this is not true for a weakly allowed I.

The following proposition allows us to focus only to the case of $k = 4$.

Proposition 3.7. *Theorem* 2.7 *implies Theorem* 2.6.

Proof. By means of Theorem 3.1 one easily sees that the map

$$D_k/(Q_{k,0}) \to D_{k-1}, \qquad Q_{k,s} \mapsto Q_{k-1,s-1}$$

is an isomorphism over the "halving" map

$$\mathscr{A} \to \mathscr{A}, \qquad Sq^{2i} \mapsto Sq^i, \quad Sq^{2i+1} \mapsto 0.$$

The proposition follows from the lists of the allowed sequences for $k = 3$ and $k = 4$ given in the previous section.

4. Determination of the allowed sequences

In this section we describe an inductive procedure for getting all the allowed sequences of length k for any k.

Definition 4.1. Suppose $a = \alpha_0(a) + \alpha_1(a)2 + \cdots + \alpha_n(a)2^n$ is the dyadic expansion of a with $\alpha_n(a) = 1$. Define $[a : 2^t]$ to be the non-negative integer less than 2^t with $a \equiv [a : 2^t] \bmod 2^t$. So $[a : 2^t] = \alpha_0(a) + \alpha_1(a)2 + \cdots + \alpha_{t-1}(a)2^{t-1}$ if $t \leq n$, and $[a : 2^t] = a$ if $t > n$.

Theorem 4.2. *The only strongly allowed sequences I's of length k are:*

(1) *either $I = (i_{k-1}, \ldots, i_1, 0)$, where $I' = (i_{k-1}, \ldots, i_1)$ is strongly allowed at length $k-1$.*

(2) *or $I = (i_{k-1}, \ldots, i_1, i_0)$ satisfying the three conditions:*

(2a) $i_0 = [k-2 : 2^{s(i_1)}] > 0$,

(2b) $I'' = (i_{k-2}, \ldots, i_1, i_0 - 1)$ *is strongly allowed at length* $k-1$.

(2c) $i_{k-1} = 2^t - [h' : 2^t] - 1$ *for* $t > \nu(i_{k-2})$, *where* $h' = i_{k-2} + \cdots + i_0$ *and* $\nu(i_{k-2}) = \max\{n | 2^n \leq i_{k-2}\}$.

To prove the theorem we need a couple of lemmas.

Lemma 4.3. *Suppose $u \rhd v$ with $u \geq 0$ and t is an integer with $2^t - 1 \leq v$. Then*

$$u \equiv 2^t - 1 \bmod 2^t \equiv -1 \bmod 2^t.$$

Proof. Suppose the contrary that there exists t with $2^t - 1 \leq v$ and

$$u \not\equiv 1 + 2 + \cdots + 2^{t-1} \bmod 2^t.$$

That means there exists $s < t$ such that $\alpha_s(u) = 0$. So $s(u) \leq s < t$. It implies $v \geq 2^t - 1 > 2^{s(u)} - 1$. Hence $u \not\rhd v$. This is a contradiction. The lemma is proved.

Lemma 4.4. *If $s(a+b) \geq s(a)$ then $s(b-1) \geq s(a)$.*

Proof. See the proof of Lemma 5.1.

Lemma 4.5. *If $I = (i_{k-1}, \ldots, i_1, i_0)$ is strongly allowed, then*

$$i_0 = [k-2 : 2^{s(i_1)}].$$

Proof. Using Lemma 4.3 we have $i_1 \equiv -1 \bmod 2^{s(i_1)}$ (obviously), and

$$\begin{aligned} & i_2 \rhd i_1 \Longrightarrow i_2 && \equiv && -1 \bmod 2^{s(i_1)} \\ & \vdots && \vdots && \vdots \\ & i_{k-1} \rhd i_1 \Longrightarrow i_{k-1} && \equiv && -1 \bmod 2^{s(i_1)} \\ & h \rhd i_1 \Longrightarrow h && \equiv && -1 \bmod 2^{s(i_1)} \\ \text{so } h \;=\; & i_{k-1} + \cdots + i_1 + i_0 && \equiv && -1 \bmod 2^{s(i_1)} \\ & (-1) + \cdots + (-1) + i_0 && \equiv && -1 \bmod 2^{s(i_1)}. \end{aligned}$$

Thus $i_0 \equiv k - 1 - 1 \equiv k - 2 \bmod 2^{s(i_1)}$. Combining this with the fact that $0 \le i_0 < 2^{s(i_1)}$ (because of $i_1 \rhd i_0$) we get $i_0 = [k - 2 : 2^{s(i_1)}]$. The lemma is proved.

Lemma 4.6. *Suppose* $I = (i_{k-1}, \ldots, i_0)$ *is strongly allowed with* $i_0 > 0$. *Then so is* $I' = (i_{k-2}, \ldots, i_0 - 1)$.

Proof. We need only to show that $(i_{k-2} + \cdots + i_0 - 1) \rhd i_{k-2}$. Applying Lemma 4.4 with $a = i_{k-1}$, $b = i_{k-2} + \cdots + i_0$, we get $s(b-1) \ge s(i_{k-1})$. This together with $i_{k-1} \rhd i_{k-2}$ implies $b - 1 \rhd i_{k-2}$. The lemma is proved.

Lemma 4.7. *Suppose* h' *and* s *are non-negative integers.*

(a) *If there exists* i *satisfying* $i + h' \rhd i \rhd 2^s - 1$ *then* h' *is divisible by* 2^s.
(b) *If* h' *is divisible by* 2^s, *then the only* i*'s satisfying* (a) *are* $i = 2^t - [h' : 2^t] - 1$, $t \ge s$.

Proof. If i satisfies (a), then $s(i) \ge s(2^s - 1) = s$. Since $i + h' \rhd i$, by Lemma 4.4, it implies $s(h' - 1) \ge s(i) \ge s$. Because h' is divisible by $2^{s(h'-1)}$, it is divisible by 2^s.

Write $i = 2^t - 1 - u$ for some t and u with $t \ge s(i) \ge s$. We require $u < 2^{t-1}$ so that this expression is *unique*. Now we want to show $u = [h' : 2^t]$. The fact $u < 2^{t-1}$ implies $i \ge 2^{t-1}$. Then we have $h' - u \equiv 0 \bmod 2^t$; otherwise $i + h' = 2^t - 1 + (h' - u) \not\rhd 2^{t-1}$, hence $i + h' \not\rhd i$ (as $i \ge 2^{t-1}$). Combining $h' - u \equiv 0 \bmod 2^t$ and $u < 2^t$ we get $u = [h' : 2^t]$, by Definition 4.1.

It is easy to check that i given by (b) satisfies (a). The lemma is proved.

Proof of Theorem 4.2. Obviously, if $i_0 = 0$, then I is strongly allowed if and only if $I' = (i_{k-1}, \ldots, i_1)$ is.

If $i_0 > 0$, suppose I is strongly allowed. By Lemmas 4.5 and 4.6, I satisfies (2a) and (2b). Furthermore, from $h \rhd i_{k-1} \rhd i_{k-2}$ it implies $i_{k-1} + h' \rhd i_{k-1} \rhd 2^s - 1$, where $s = s(i_{k-2})$. By Lemma 4.7, $i_{k-1} = 2^t - [h' : 2^t] - 1$, for $t \ge s$. The condition $i_{k-1} = 2^t - [h' : 2^t] - 1 \rhd i_{k-2}$ obviously implies $t \ge \nu(i_{k-2}) + 1 \ge s$.

On the other hand, we need to show that if I satisfies (2a), (2b) and (2c), then I is strongly allowed. Indeed, (2a) implies $i_1 \rhd i_0$, (2b) implies $i_{k-2} \rhd \cdots \rhd i_1$. Finally, by Lemma 4.7, (2c) implies $h = i_{k-1} + h' \rhd i_{k-1} \rhd i_{k-2}$. The theorem is proved.

Remark 4.8. A strongly allowed sequence $I = (i_{k-1}, \ldots, i_0)$ is called *main* if $i_0 > 0$. Making use of the theorem, we list here all the main strongly allowed

sequences for $k \leq 4$:

$$\begin{array}{lll} \text{For } k=1 : & (2^s-1), & s>0, \\ \text{For } k=2 : & \text{None} & \\ \text{For } k=3 : & (2^r-2^s-1, 2^s-1, 1), & r>s>0, \\ \text{For } k=4 : & (2^s-1, 2^s-1, 2^s-1, 2), & s>1, \\ & (2^t-2^r-1, 2^r-2^s-1, 2^s-1, 2), & t>r>s>1. \end{array}$$

Here is a generalization of Lemma 4.5.

Remark 4.9. Set $S(I) = (s_k, \dots, s_1) = (s(h), s(i_{k-1}), \dots, s(i_1))$ for $I = (i_{k-1}, \dots, i_1, i_0)$. Then S is injective on the set of all strongly allowed sequences.

Clearly, in $\operatorname{Im} S$, $s_k \geq s_{k-1} \geq \cdots \geq s_1$, but not all such appear.

Now let us turn to investigate the weakly allowed sequences. We will show that they can be given as "deformations" of the strongly allowed sequences.

Definition 4.10. Let $J = (j_{k-1}, \dots, j_0)$. We set $j_k = h(J)$.

(i) By a *deformation of* J *at* k we mean

$$I = (j_{k-1} - 2^{s(j_{k-1})-1}, j_{k-2}, \dots, j_0) \quad \text{with} \quad 2^{s(j_{k-1})-1} - 1 \geq j_{k-2}.$$

(ii) By a *deformation of* J *at* $m < k$ we mean

$$I = (j_{k-1}, \dots, j_m - 2^s, j_{m-1} + 2^s, \dots, j_0)$$

with $s(j_{m-1}) \geq s+2$, $2^s - 1 \geq j_{m-2}$, $j_m \rhd j_{m-1} + 2^s$.

We call j_m, j_{m-1} the initial and the terminal of the deformation at m $(1 \leq m \leq k)$.

Proposition 4.11. *Every weakly allowed sequence I can be obtained from a strongly allowed sequence J by applying some deformations with the condition that the terminal of any deformation is not the initial of another deformation.*

Proof. By definition of $\rhd\!\!\rhd$, there do not exist u, v, w such that $u \rhd\!\!\rhd v \rhd\!\!\rhd w$. Therefore, in a weakly allowed sequence I a $\rhd\!\!\rhd$ cannot stand just after another $\rhd\!\!\rhd$.

Suppose I is weakly allowed. Applying the reverse procedure of deformation at any place where a $\rhd\!\!\rhd$ stands, we get a strongly allowed sequence J.

Remark 4.12. Making use of the proposition for $k \leq 4$ we conclude: For $k \leq 3$, there are no weakly allowed sequences. For $k = 4$, the only weakly allowed sequences are

$$I = (2^r - 2^{s+1} - 2^s - 1, 2^s - 1, 2^s - 1, 2), \quad r > s+2 > 3.$$

In this sequence $h \rhd\!\!\rhd i_3 \rhd i_2 \rhd i_1 \rhd i_0$.

Combining this result with Remark 4.8 we get the lists of allowed sequences for $k \leq 4$, which are shown in Section 2.

5. The span of the allowed monomials

From now on, we always work at $k = 4$ unless otherwise specified. Let us begin with a generalization of Lemma 4.4.

Lemma 5.1. *For any integers* a, b,

$$\min\{s(a), s(b-1)\} = \min\{s(a+b), s(a)\} = \min\{s(a+b), s(b-1)\}.$$

Proof. If either $a = -1$ or $b = -1$, then one can directly check the conclusion by using Definition 2.1 and the remark that $s(\text{even number}) = 0$.

Suppose $a \neq -1, b \neq -1$. Set $s(a) = s, s(b-1) = r$. So $a \equiv 2^s - 1 \bmod 2^{s+1}$, $b - 1 \equiv 2^r - 1 \bmod 2^{r+1}$. Consider the three cases:

Case 1: $r < s$. $a + b \equiv 2^s + 2^r - 1 \bmod 2^{r+1} \equiv 2^r - 1 \bmod 2^{r+1}$. Hence $s(a+b) = r$.

$$\begin{aligned}\min\{s(a), s(b-1)\} &= \min\{s(a+b), s(a)\} \\ &= \min\{s(a+b), s(b-1)\} = r.\end{aligned}$$

Case 2: $r > s$. $a + b \equiv 2^s + 2^r - 1 \bmod 2^{s+1} \equiv 2^s - 1 \bmod 2^{s+1}$. Hence $s(a+b) = s$.

$$\begin{aligned}\min\{s(a), s(b-1)\} &= \min\{s(a+b), s(a)\} \\ &= \min\{s(a+b), s(b-1)\} = s.\end{aligned}$$

Case 3: $r = s$. $a + b \equiv 2^{r+1} - 1 \bmod 2^{r+1}$. So $s(a+b) > r$.

$$\begin{aligned}\min\{s(a), s(b-1)\} &= \min\{s(a+b), s(a)\} \\ &= \min\{s(a+b), s(b-1)\} = r = s.\end{aligned}$$

The lemma is proved.

Making use of the lemma we get

$$\begin{aligned}\min\{s(i_2), s(i_1+i_0-2)\} &= \min\{s(i_2), s(i_2+i_1+i_0-1)\} \\ &= \min\{s(i_2+i_1+i_0-1), s(i_1+i_0-2)\}, \\ \min\{s(i_3), s(i_2+i_1+i_0-1)\} &= \min\{s(i_3), s(h)\} \\ &= \min\{s(h), s(i_2+i_1+i_0-1)\}.\end{aligned}$$

Definition 5.2. If I is of length 4, by $m(I)$ we mean the common value

$$\begin{aligned}m(I) &= \min\{s(i_3), s(i_2), s(i_1+i_0-2)\} \\ &= \min\{s(i_3), s(i_2+i_1+i_0-1), s(i_1+i_0-2)\} \\ &= \min\{s(h), s(i_3), s(i_1+i_0-2)\} \\ &= \min\{s(h), s(i_2+i_1+i_0-1), s(i_1+i_0-2)\}.\end{aligned}$$

Main Lemma 5.3. *If I is not allowed, then*

(a) *either* $Q^I \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < m(I)\}$ *(the strong form of the main lemma),*

(b) *or* $Q^I \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | \text{either } m(J) < m(I) \text{ or } m(J) = m(I) \text{ and } h(J) < h(I)\}$ *(the weak form of the main lemma),*

(c) *or there exists a weakly allowed sequence I' with $m(I) = m(I')$, $h(I) < h(I')$ and*

$$Q^I + Q^{I'} \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < m(I)\}$$

(the exceptional form of the main lemma).

The main lemma is proved by showing several lemmas. We state them here, but postpone their proofs until the next three sections.

Lemma 5.4. *Suppose I satisfies $s(h), s(i_3), s(i_2)$ all $\geq s(i_1)$, $i_1 \not\rhd i_0$. Then the **strong** form of the main lemma holds for I.*

Lemma 5.5. *Suppose I satisfies either $s(h), s(i_3)$ all $\geq s(i_2) \neq s(i_1)$, $i_2 \not\rhd i_1$, or $s(h), s(i_3)$ all $\geq s(i_2) = s(i_1)$, $i_2 \not\rhd i_1 \rhd i_0$. Then the **strong** form of the main lemma holds for I.*

Lemma 5.6. *Suppose I satisfies $s(h) \geq s(i_3) \geq s(i_2)$, $i_3 \not\rhd i_2 \rhd i_1 \rhd i_0$. Then either the **weak** form or the **exceptional** form of the main lemma holds for I.*

Lemma 5.7. *Suppose I satisfies $s(h) \geq s(i_3) < s(i_2)$. Then the **strong** form of the main lemma holds for I.*

Lemma 5.8. *Suppose I satisfies $s(h) \geq s(i_3)$, $h \not\rhd i_3 \rhd i_2 \rhd i_1 \rhd i_0$, and $h \not\trianglerighteq i_3$. Then the **weak** form of the main lemma holds for I.*

Lemma 5.9. *Suppose I satisfies $s(h) < s(i_3)$. Then the **weak** form of the main lemma holds for I.*

It should be noted that we have to distinguish the strong form of the main lemma in Lemmas 5.4, 5.5 and 5.7 because it will essentially be used in the proofs of Lemmas 7.5, 7.7, which are parts of Lemma 5.6.

According to the results of Section 4, the main lemma is equivalent to these six lemmas, whose proofs will be given in the next three sections . Now we show how the main lemma leads to Theorem 2.7.

Proof of Theorem 2.7. The linear independence of the allowed monomials will be showed in Section 9.

Suppose that the main lemma is true. To prove the allowed monomials generate $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_4$ we need only to show

Lemma 5.10. *Let $k = 4$. Suppose I is not allowed, with $m(I) = 0$. Then $Q^I \in \operatorname{Im}\bar{\mathscr{A}}$.*

Proof. For abbreviation, from now on we sometimes let I stand for Q^I. So, for instance, the statements like $I \in D_k$ or $Sq^i I$... make sense.

Recall $m(I) = \min\{s(h(I)), s(i_3), s(i_1 + i_0 - 2)\}$. We will consider the following three cases, with many subcases.

1. $s(h(I)) = 0$.
2. $s(h(I)) > 0$ and $s(i_3) = 0$.
3. $s(h(I)) > 0$, $s(i_3) > 0$, and $s(i_1 + i_0 - 2) = 0$.

In this proof, we will abbreviate the expression $i \equiv 0 \mod 2^t$ by $i \equiv 0(2^t)$.

There are three easy ways to show that $I \in \operatorname{Im}\bar{\mathscr{A}}$, and we will call I simple if it can be handled in one of the following three ways.

(a) $i_1 \equiv 0(2)$ and $i_0 \geq 1$, because $Sq^1(i_3, i_2, i_1 + 1, i_0 - 1) = I$, or

(b) $i_j \equiv 0(2)$ all j, because then I is a square, or

(c) $i_2 \equiv 0(2)$ and $i_1 \equiv 1(2)$, because

$$Sq^2(i_3, i_2 + 1, i_1 - 1, i_0) = I + \binom{i_1 - 1}{2}(i_3, i_2 + 1, i_1 - 3, i_0 + 2)$$

and this last term is of type **(a)** above.

Case 1: $s(h(I)) = 0$.

(a) Assume $i_3 > 0$. Then $Sq^8(i_3 - 1, i_2, i_1, i_0) = I + \sum J$. Here $h(J) < h(I)$ for all such J and we must show $m(J) = 0$. For most of these terms, $s(j_3) = 0$. The ones left are

$$\binom{i_3 - 1}{2}(i_3 - 3, i_2 + 2, i_1, i_0), \quad \binom{i_2}{4}(i_3 - 1, i_2 - 4, i_1 + 4, i_0),$$

and

$$\binom{i_1}{8}(i_3 - 1, i_2, i_1 - 8, i_0 + 8)$$

with $i_3 \equiv 0(2)$, $i_1 + i_0 \equiv 1(2)$, $i_2 \equiv 1(2)$. In this case we get

$$Sq^4(i_3 + 1, i_2 - 1, i_1, i_0) = I + \binom{i_2 - 1}{2}(i_3 + 1, i_2 - 3, i_1 + 2, i_0) + \binom{i_1}{4}(i_3 + 1, i_2 - 1, i_1 - 4, i_0 + 4).$$

Note that $i_1 \equiv 1(2)$ or I is simple. Hence both the later terms are simple.

(b) Assume $i_3 = 0$ and $i_2 > 0$.

(i) If $i_2 \equiv 1(2)$, then $i_1 \equiv 1(2)$ or it is simple.

$$Sq^4(1, i_2 - 1, i_1, i_0) = I + \binom{i_2 - 1}{2}(1, i_2 - 3, i_1 + 2, i_0) + (i_2 - 1)\binom{i_1}{2}(1, i_2 - 2, i_1 - 1, i_0 + 2) + \binom{i_1}{4}(1, i_2 - 1, i_1 - 4, i_0 + 4)$$

works as the other terms are 0 or simple.

(ii) If $i_2 \equiv 0(2)$, then $i_1 + i_0 \equiv 0(2)$. If $i_1 \equiv 0(2)$, then I is simple. If $i_1 \equiv 1(2)$, then I is also simple.

(c) Assume $i_3 = 0$ and $i_2 = 0$. Then $i_1 \equiv 1(2)$ or I is simple. Then I is also simple.

Case 2: $s(h(I)) > 0$, $s(i_3) = 0$.

(a) Assume $i_2 \equiv 0(2)$. If $i_1 \equiv 0(2)$, then $i_0 > 0$ and I is simple. If $i_1 > 0$, then I is also simple.

(b) Assume $i_2 \equiv 1(2)$.

$$Sq^4(i_3 + 1, i_2 - 1, i_1, i_0) = I + \binom{i_2 - 1}{2}(i_3 + 1, i_2 - 3, i_1 + 2, i_0)$$

and

$$Sq^2(i_3 + 1, i_2 - 2, i_1 + 1, i_0) = (i_3 + 1, i_2 - 3, i_1 + 2, i_0) + \binom{i_1 + 1}{2}(i_3 + 1, i_2 - 2, i_1 - 1, i_0 + 2).$$

If $i_1 \equiv 1(2)$, then $i_0 + 2 > 0$ and it is simple. If $i_1 \equiv 0(2)$, then $i_0 \equiv 1(2)$. I is simple.

Case 3: $s(h(I)) > 0$, $s(i_3) > 0$, $s(i_1 + i_0 - 2) = 0$.

(a) Assume $i_0 > 0$. If $i_1 \equiv 0(2)$, then I is simple. If $i_1 \equiv 1(2)$, then $i_2 \equiv 0(2)$ and $i_1 > 0$, so I is simple.

(b) Assume $i_0 = 0$, $i_1 > 0$. Then $i_2 \equiv 0(2)$.

$$Sq^2(i_3, i_2+1, i_1-1, 0) = I + \binom{i_1-1}{2}(i_3, i_2+1, i_1-3, 2)$$

which handles all cases but $i_1 \equiv 0(4)$.

(i) $i_2 \not\equiv 4, 6(8)$, $i_1 \equiv 0(4)$

$$Sq^8(i_3, i_2+4, i_1-4, 0) = I + \text{simple terms.}$$

(ii) $i_2 \equiv 4(8)$, $i_1 \equiv 0(4)$, $i_1 \geq 8$.

$$\begin{aligned} Sq^4(i_3, i_2+3, i_1-5, 2) &= (i_3, i_2+1, i_1-3, 2) \\ &+ \binom{i_1-5}{4}(i_3, i_2+3, i_1-9, 6) + (i_3-1, i_2+4, i_1-5, 2) \\ &+ \text{simple terms} \end{aligned}$$

and the two latter terms are simple.

(iii) $i_2 \equiv 4(8)$, $i_1 = 4$.

$$Sq^4(i_3, i_2+2, 2, 0) = I + (i_3-1, i_2+3, 2, 0)$$

which is in Case 2.

(iv) $i_2 \equiv 6(8)$, $i_3 \equiv 3(4)$. Then $h(I) \equiv 1(4)$.

$$\begin{aligned} Sq^{16}(i_3-2, i_2, i_1, 0) &= I + \binom{i_3-2}{4}(i_3-6, i_2+4, i_1, 0) \\ &+ \binom{i_2}{8}(i_3-2, i_2-8, i_1+8, 0) + \binom{i_2}{2}(i_3-2, i_2-1, i_1+2, 0) \\ &+ \text{simple terms.} \end{aligned}$$

All $h(J) < h(I)$ and only need check $m(J) = 0$. In all cases, $s(j_1 + j_0 - 2) = 0$.

(v) $i_2 \equiv 6(8)$, $i_3 \equiv 1(4)$, $i_1 \equiv 4(8)$.

$$\begin{aligned} Sq^8(i_3+2, i_2-2, i_1, 0) &= I + (i_3+2, i_2-6, i_1+4, 0) \\ &\quad + \text{simple terms.} \\ Sq^2(i_3+2, i_2-5, i_1+3, 0) &= (i_3+2, i_2-6, i_1+4, 0) \\ &\quad + (i_3+2, i_2-5, i_1+1, 2). \\ Sq^4(i_3+2, i_2-3, i_1-1, 2) &= (i_3+2, i_2-5, i_1+1, 2) \\ &\quad + (i_3+1, i_2-2, i_1-1, 2) + \text{simple terms,} \end{aligned}$$

and $(i_3+1, i_2-2, i_1-1, 2)$ is simple.

(vi) $i_2 \equiv 6(8)$, $i_3 = 5(8)$, $i_1 \equiv 0(8)$, $i_1 > 0$.

$$Sq^8(i_3+2, i_2-2, i_1, 0) = I + (i_3+2, i_2-6, i_1+4, 0) + \text{simple terms.}$$

$$Sq^4(i_3+2, i_2-4, i_1+2, 0) = (i_3+2, i_2-6, i_1+4, 0) + (i_3+1, i_2-3, i_1+2, 0).$$

$$Sq^{2^{s(h(I))}\cdot 8}(i_3+1-2^s, i_2-3, i_1+2, 0) = (i_3+1, i_2-3, i_1+2, 0) + \sum J$$

with $h(J) < h(I)$ and all have $j_1 + j_0 - 2 \equiv 0(2)$. Here we denote $s = s(h(I))$ and use $i_3 \equiv 5(8)$ to show $i_3 + 1 \geq 2^{s(h(I))}$.

(vii) $i_2 \equiv 6(8)$, $i_3 = 1(8)$, $i_1 \equiv 0(8)$, $i_1 > 0$.

$$Sq^{16}(i_3+4, i_2-4, i_1, 0) = I + (i_3+6, i_2-4, i_1, 0) + \binom{i_2-4}{8}(i_3+4, i_2-12, i_1+8, 0).$$

$$Sq^{32}(i_3+2, i_2-4, i_1, 0) = (i_3+6, i_2-4, i_1, 0) + \sum J$$

with $h(J) < h(I)$ and all $m(J) = 0$.

$$Sq^8(i_3+4, i_2-8, i_1+4, 0) = (i_3+4, i_2-12, i_1+8, 0) + (i_3+3, i_2-9, i_1+6, 0) + \text{simple terms.}$$

$$Sq^4(i_3+3, i_2-7, i_1+4, 0) = (i_3+3, i_2-9, i_1+6, 0) + \text{simple terms.}$$

(c) Assume $i_1 = i_0 = 0$, $h(I) \not\rhd i_3$.

$$Sq^{2^{s(h(I))}\cdot 8}(i_3 - 2^{s(h(I))}, i_2, 0, 0) = I + \sum J.$$

All $h(J) < h(I)$ and since $\dim I \equiv 0(4)$, we have that $j_1 \equiv j_0 \equiv 0(2)$ and $m(J) = 0$.

(d) Assume $i_1 = i_0 = 0$, $h(I) \rhd i_3$. Then $i_3 \not\rhd i_2$ as I is not allowed. Let $s = s(i_3)$. Hence

$$Sq^{2^s\cdot 4}(i_3+2^s, i_2-2^s, 0, 0) = I + (i_3+2^s+2^{s-1}, i_2-2^s, 0, 0) + \binom{i_2-2^s}{2^{s+1}}(i_3+2^s, i_2-2^s-2^{s+1}, 2^{s+1}, 0).$$

Denote the two extra terms by J and K respectively. Obviously, $m(K) = 0$, $s(h(K)) > 0$, $s(k_3) > 0$, $k_1 > 0$. So K is handled by Case 3(b). Note remarkably that while handling K, one still has the inductive procedure for lowering $h(K)$ in Case 1(a) or Case 2(b). In all possibilities, every extra term L has $l_1 + l_0 \geq k_1 + k_0 > 0$ by Corollary 3.2. Therefore, no extra term needs to be handled by Case 2(c) or (d). So the inductive procedure works.

Next, note that $s(h(J)) = s(h(I) + 2^{s-1}) = s - 1 = s(j_3)$ and $\alpha_t(j_2) = \alpha_t(i_2 - 2^s) = 0$ for $t < s$ as $h \rhd i_3$. If $j_2 \geq 2^{s-1}$, we handle J by downward induction on s using $Sq^{2^{s-1}\cdot 4}(j_3 + 2^{s-1}, j_2 - 2^{s-1}, 0, 0)$. Otherwise, if $j_2 < 2^{s-1}$, combining this with the fact that $\alpha_t(j_2) = 0$ for $t < s$ we get $j_2 = 0$. Then we cannot use Case 3(c) to handle J because of $h(J) > h(I)$. Let t be a number with $\alpha_t(j_3) = 0$, $\alpha_{t+1}(j_3) = 1$. Such a t exists as $h(J) \not\rhd j_3 = h(J)$. Then $Sq^{2^t\cdot 8}(j_3 - 2^t, 0, 0, 0) = J$.

In order to start the induction, we need the following case.

Case 4: $h(I) = 1$. $(1, 0, 0, 0)$ is allowed, $Sq^4(1, 0, 0, 0) = (0, 1, 0, 0)$, $Sq^6(1, 0, 0, 0) = (0, 0, 1, 0)$, and $Sq^7(1, 0, 0, 0) = (0, 0, 0, 1)$.

6. Proofs of Lemma 5.4 and Lemma 5.5

We need the following terminology:

Definition 6.1. Let s be a natural number. Q^I (or I) is *s-killed* if

$$Q^I \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J \mid m(J) < s\}.$$

Therefore, the strong form of the main lemma holds for I if and only if I is $m(I)$-killed.

Proof of Lemma 5.4. Set $s = s(i_1)$. By Lemma 5.1,

$$s(h), s(i_3) \text{ all } \geq s \Rightarrow \left.\begin{array}{r} s(i_2 + i_1 + i_0 - 1) \geq s \\ \text{also } \ s(i_2) \geq s \end{array}\right\} \Rightarrow \ s(i_1 + i_0 - 2) \geq s.$$

As a consequence: $m(I) = \min\{s(i_3), s(i_2), s(i_1 + i_0 - 2)\} \geq s$.

We kill Q^I by

$$Sq^{2^s}(Q_3^{i_3} Q_2^{i_2} Q_1^{i_1 + 2^s} Q_0^{i_0 - 2^s}) = \underbrace{\binom{i_1 + 2^s}{2^s}}_{1} Q^I + \sum_J Q^J.$$

For any J in the sum we have

(a) $|h(J) - h(I)| \leq \frac{2^s}{\dim Q_3} = 2^{s-3} < 2^s$,

(b) $|j_3 - i_3| \leq \frac{2^s}{\dim Q_2 - \dim Q_3} = 2^{s-2} < 2^s$,

(c) $|j_2 - i_2| \leq \frac{2^s}{\dim Q_1 - \dim Q_2} = 2^{s-1} < 2^s$.

If $h(J) \neq h(I)$, combine (a) with the fact $s(h(I)) \geq s$ and we get $s(h(J)) < s$. So $m(J) \leq s(h(J)) < s \leq m(I)$. Similarly, if either $j_3 \neq i_3$ or $j_2 \neq i_2$, then $m(J) < s \leq m(I)$.

Suppose now $h(J) = h(I)$, $j_3 = i_3$, $j_2 = i_2$. The dimensional information shows

(d) $14(j_1 - (i_1 + 2^s)) + 15(j_0 - (i_0 - 2^s)) = 2^s$.

As $j_0 - (i_0 - 2^s) \geq 0$, so $14[j_1 - (i_1 + 2^s) + j_0 - (i_0 - 2^s)] \leq 2^s$, hence $0 \leq [(j_1 + j_0 - 2) - (i_1 + i_0 - 2)] \leq \frac{2^s}{14} < 2^s$.

If $(j_1 + j_0 - 2) - (i_1 + i_0 - 2) = 0$, then $(j_1 - i_1) = -(j_0 - i_0) = x$ (say).

Now, (d) becomes $14(x - 2^s) + 15(-x + 2^s) = 2^s$. So $x = 0$, $j_1 = i_1$, $j_0 = i_0$. The corresponding term is Q^I but not a term of the sum.

Otherwise $0 < (j_1 + j_0 - 2) - (i_1 + i_0 - 2) < 2^s$. This together with $s(i_1 + i_0 - 2) \geq s$ implies $m(J) \leq s(j_1 + j_0 - 2) < s \leq m(I)$.

The lemma follows.

In order to prove Lemma 5.5, we need the following two technical lemmas.

Let us first state a strong version of Lemma 5.4, which can be proved by the same argument.

Lemma 6.2. *Let* $I = (i_3, i_2, i_1, i_0)$. *Suppose there exists* s *such that*

$$\binom{i_1 + 2^s}{2^s} \equiv 1 \bmod 2, \quad i_0 \geq 2^s, \quad m(I) \geq s.$$

Then I *is* s*-killed.*

Next we show:

Lemma 6.3. *Suppose* I *satisfies* $s(h), s(i_3)$ *all* $\geq s(i_2)$, $i_2 \not\rhd i_1$. *Then, for* $s = s(i_2)$:

$$Q^I + \binom{i_1 - 2^s}{2^{s+1}} Q^{(i_3, i_2 + 2^s, i_1 - 2^s - 2^{s+1}, i_0 + 2^{s+1})} \in \operatorname{Im} \bar{\mathscr{A}} + \operatorname{Span}\{Q^J \mid m(J) < m(I)\}.$$

Proof. We kill Q^I by the usual way

$$Sq^{2^{s+1}}(Q_3^{i_3} Q_2^{i_2 + 2^s} Q_1^{i_1 - 2^s} Q_0^{i_0}) = Q^I + \sum_J Q^J.$$

Similarly as in the proof of Lemma 5.4, for any J in the sum, we have

$$|h(J) - h(I)| \leq 2^{s+1}/2^3 = 2^{s-2} < 2^s, \; |j_3 - i_3| \leq 2^{s+1}/2^2 < 2^s.$$

Thus, if either $h(J) \neq h(I)$ or $j_3 \neq i_3$ then $m(J) < s \leq m(I)$. We need only to consider the case where $h(J) = h(I)$, $j_3 = i_3$. Note that

$$j_1 + j_0 = (i_1 - 2^s) + i_0 + t \quad \text{with } 0 \leq t < 2^s.$$

(The only term with $t = 2^s$ is Q^I according to the dimensional information.)

If $0 < t < 2^s$: Using Lemma 5.1, one has

$$\begin{array}{rcl} s(h), s(i_3) \text{ all } \geq s(i_2) & \Rightarrow & s(i_1 + i_0 - 2) \geq s = s(i_2). \\ \left.\begin{array}{l} \Rightarrow s(i_1 - 2^s + i_0 - 2) \geq s \\ \text{meanwhile } 0 < t < 2^s \end{array}\right\} & \Rightarrow & s(j_1 + j_0 - 2) = s(i_1 - 2^s + i_0 + t - 2) < s. \\ & \Rightarrow & m(J) < s \leq m(I). \end{array}$$

If $t = 0$: One gets

$$\begin{cases} j_1 + j_0 &= (i_1 - 2^s) + i_0 \\ 14\, j_1 + 15\, j_0 &= 14(i_1 - 2^s) + 15\, i_0 + 2^{s+1} \text{ (dim. information).} \end{cases}$$

So $j_0 = i_0 + 2^{s+1}$, $j_1 = i_1 - 2^s - 2^{s+1}$, $j_2 = h - (j_3 + j_1 + j_0) = i_0 + 2^s$. The coefficient of the resulting term Q^J in the sum is $\binom{i_1 - 2^s}{2^{s+1}}$. The lemma is proved.

Proof of Lemma 5.5. Using actually the argument in the proof of Lemma 4.5, one observes that if $s(h), s(i_3), s(i_2)$ all $\geq s(i_1)$, $i_1 \rhd i_0$, then either $i_0 = 0$ or $i_0 = 2$. Combining this with Remark 4.12, we need only to consider the four cases:

Case A: $s(h), s(i_3)$ all $\geq s(i_2)$, $i_2 \not\rhd i_1$ and at least one from the following three equalities is broken: $s(i_2) = s(i_1)$, $s_2(i_1) = s(i_1) + 1$, $i_0 = 2$.

Case B: $s(h), s(i_3)$ all $\geq s(i_2)$, $i_2 \not\rhd i_1 \rhd i_0$, $s(i_2) = s(i_1) = s_2(i_1) - 1$, $i_0 = 2$, $i_2 \not\gg i_1$ (or equivalently $i_2 + 2^{s(i_2)} \not\rhd i_1$).

Case C: $s(h), s(i_3)$ all $\geq s(i_2)$, $i_3 \not\rhd i_2 \gg i_1 \rhd i_0 = 2$.

Case D: $s(h), s(i_3)$ all $\geq s(i_2)$, $h \not\rhd i_3 \rhd i_2 \gg i_1 \rhd i_0 = 2$.

Proof of Lemma 5.5 *in Case* A. Using Lemma 6.3 it suffices to study the case of $\binom{i_1 - 2^s}{2^{s+1}} \equiv 1 \bmod 2$, where $s = s(i_2)$. First, we note that:

$$\begin{aligned} s(i_1 - 2^s - 2^{s+1}) = s+1 &\Leftrightarrow i_1 - 2^s - 2^{s+1} \equiv 2^{s+1} - 1 \bmod 2^{s+2} \\ &\Leftrightarrow i_1 \equiv 2^s - 1 \bmod 2^{s+2} \Leftrightarrow \begin{cases} s(i_1) = s \\ s_2(i_1) = s+1. \end{cases} \end{aligned}$$

(1) If $s(i_1 - 2^s - 2^{s+1}) \neq s+1$, since $\binom{i_1 - 2^s}{2^{s+1}} = 1$, so $r = s(i_1 - 2^s - 2^{s+1}) < s+1$. We have $s(h) \geq s(i_2) = s \geq r$. Since $s(i_3), s(h)$ all $\geq s(i_2)$ so $s(i_1 + i_0 - 2) \geq s(i_2) = s$. Then

$$s(i_1 - 2^s - 2^{s+1} + i_0 + 2^{s+1} - 2) = s(i_1 + i_0 - 2 - 2^s) \geq s \geq r.$$

Now we can apply Lemma 6.2 for

$$Q^T = Q^{(i_3, i_2 + 2^s, i_1 - 2^s - 2^{s+1}, i_0 + 2^{s+1})}$$

with r playing the role of s. So we get

$$Q^T \in \operatorname{Im}\tilde{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < r\} \subset \operatorname{Im}\tilde{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < m(I) = s\}.$$

Combining this with Lemma 6.3, it implies Q^I is s-killed.

(2) Suppose $s(i_1 - 2^s - 2^{s+1}) = s+1$. By the hypothesis of Lemma 5.5 Case A: $i_0 \neq 2$.

$$\left.\begin{array}{c} s(i_1) = s \Rightarrow 2^s \,|\, (i_1 + 1) \\ \text{By Lemma 4.3}: s(i_1 + i_0 - 2) \geq s \Rightarrow 2^s \,|\, (i_1 + i_0 - 1) \end{array}\right\} \Rightarrow 2^s \,|\, (i_0 - 2).$$

(a) If $i_0 - 2 > 0$, then $i_0 > 2^s$. On the other hand: $s(h), s(i_3), s(i_1 + i_0 - 2)$ all $\geq s$. We can apply Lemma 6.2 and I is s-killed.

(b) If $i_0 - 2 < 0$, then either $i_0 = 1$ (so $s = 0$ as $2^s | -1 = i_0 - 2$), or $i_0 = 0$ (and $s = 0$ or 1 because of $2^s | -2 = i_0 - 2$).

The case $s = m(I) = 0$ has been considered in the proof of Theorem 2.7 at the end of Section 5. Now it sufficies to study the case $s = 1$, $i_0 = 0$.

By hypothesis $i_0 = 0$, $i_1 = 1 + c$, $i_2 = 1 + b$, $i_3 = 1 + a$. Here $c \equiv 0 \bmod 8$, $c > 0$, $b \equiv 0 \bmod 4$ and $a \equiv 0 \bmod 2$. The following computations are modulo $\operatorname{Span}\{Q^J | m(J) = 0\}$.

- If $a \equiv 0 \bmod 4$,

$$\begin{aligned} Sq^4(1+a, 3+b, 1+c-2, 0) &= (1+a, 1+b, 1+c, 0) \\ &\quad + (1+a, 3+b, 1+c-6, 4), \\ Sq^8(3+a, 1+b, 1+c-6, 4) &= (1+a, 3+b, 1+c-6, 4) + \sum J. \end{aligned}$$

Here every J in the sum satisfies

$$j_3 \equiv 3 \bmod 4,\ j_2 \equiv 1 \bmod 4,\ j_1 \equiv 3 \bmod 4,\ j_0 \geq 4.$$

Such a J satisfies the hypothesis of Case 1 above, hence it is 1-killed.

- If $a \equiv 2 \bmod 4$,

$$Sq^{16}(1+a-2, 1+b, 1+c, 0) = (1+a, 1+b, 1+c, 0) + \sum J.$$

Here any J satisfies either the hypothesis of Lemma 5.4 with $m(J) = 1$ or $J = (1+a', 1+b', 1+c', 0)$ with $a' \equiv b' \equiv 0 \pmod 4$, $c' \equiv 0 \bmod 8$, $c' > 0$. Thus J is 1-killed by means of either Lemma 5.4 or the previous item.

Proof of Lemma 5.5 *in Cases* B, C, D *supposing that Lemma* 5.7 *is true.* (We will prove Lemma 5.7 by a direct computation in the next section.)

To this end, the use of $m(I)$ is not enough. We need one more control variable defined as follows.

Definition 6.4. For $I = (i_3, i_2, i_1, i_0)$, we define

$$m'(I) = \min\{s(i_3), s'(i_2)\}.$$

Set

$$S(s) = \{I | s(h), s(i_3) \text{ all } \geq s(i_2) = s(i_1) = s > 1, i_0 = 2\}.$$

Note that $m(I) = s$ for any $I \in S(s)$. Making use of $m'(I)$, we get

Lemma 6.5. *If* $I \in S(s)$, *and* I *is in Cases* B, C *or* D, *then*

$$\begin{aligned} I \in \operatorname{Im}\bar{\mathscr{A}} &+ \operatorname{Span}\{J | m(J) < m(I) = s\} \\ &+ \operatorname{Span}\{J \in S(s) | m'(J) < m'(I), \ I \text{ in Cases B, C or D}\} \\ &+ \operatorname{Span}\{J \text{ satisfying Lemma 5.7's hypothesis and } s(j_3) = s\}. \end{aligned}$$

Corollary 6.6. *If Lemma* 5.7 *is true, then so is Lemma* 5.5 *in Cases* B, C, D.

To prove the above lemma we need the technical lemma:

Lemma 6.7. *If* $H \in S(s)$, *then for any* i *we have*

$$Sq^{2^i} H = \sum_J J \mod \operatorname{Span}\{L | m(L) < s\},$$

where

(a) *either* J *satisfies the hypothesis of Lemma* 5.7 *with* $s(j_3) = s$,
(b) *or* $J \in S(s)$.

Proof. This proof looks very much like the beginning part of that of Lemma 7.7. It is easy to see that $m(H) = s$.

$$\begin{aligned} Sq^{2^i} H &= \sum J \\ &= \sum (Sq^{k_0} Q_3)^{a_0} \cdots (Sq^{k_\alpha} Q_3)^{2^\alpha a_\alpha} \\ &\quad \cdot (Sq^{l_0} Q_2)^{b_0} \cdots (Sq^{l_\beta} Q_2)^{2^\beta b_\beta} \\ &\quad \cdot (Sq^{m_0} Q_1)^{c_0} \cdots (Sq^{m_\gamma} Q_1)^{2^\gamma c_\gamma} \\ &\quad \cdot (Sq^n Q_0)^2. \end{aligned}$$

Here a_i, b_i, c_i are the coefficients of 2^i in the dyadic expansions of h_3, h_2, h_1 respectively. Convention: $k_i = 0$ if $a_i = 0$, $l_i = 0$ if $b_i = 0$, $m_i = 0$ if $c_i = 0$. Consider a J in the sum. We need only to study the case $m(J) \geq s$. That means $s(j_3), s(j_2), s(j_1 + j_0 - 2)$ all $\geq s$.

Case 1: $s(j_3) \geq s$, $s(j_2) > s$. These imply $k_s = 4$ and $s(j_3) = s$. Hence $m(J) \leq s \leq m(J)$, so $m(J) = s \leq s(h')$. Here $h' = h(J)$. Therefore J satisfies the hypothesis of Lemma 5.7 with $s(j_3) = s$.

Case 2: $s(j_3) \geq s$, $s(j_2) = s$, $s(j_1) > s$. Then $m(J) \leq s(j_2) = s$. So $m(J) = s$. Then $s(h') \geq m(J) = s$. Since $s(j_2) < s(j_1)$ so $j_2 \not\rhd j_1$, we can apply Case A of Lemma 5.5 to show J is s-killed.

Case 3: $s(j_3) \geq s$, $s(j_2) = s$, $s(j_1) = t < s$. Similarly as before $m(J) = s$. Hence $s(j_1 + j_0 - 2) \geq s$. This together with $s(j_1) = t < s$ implies $j_0 > 2^t$. Therefore, $j_1 \not\rhd j_0$. We also have $s(h') \geq m(J) = s > t$. Hence, by Lemma 5.4, J is s-killed.

Case 4: $s(j_3) \geq s$, $s(j_2) = s(j_1) = s$. We also have $m(J) = s$. Then $s(h') \geq s$.

If $j_1 \not\rhd j_0$, then we can apply Lemma 5.4 to show J is s-killed.

Otherwise, if $j_1 \rhd j_0$, this together with $s(h')$, $s(j_3)$ all $\geq s(j_2) = s(j_1) = s$ implies $j_0 = 2$ (by an argument similar to that in the proof of Lemma 4.5). That means $J \in S(s)$. The lemma is proved.

Proof of Lemma 6.5. In the three parts of this proof, we find some i and $H \in S(s)$ such that $Sq^{2^i} H = I + \sum J$. Using Lemma 6.7, it suffices to consider $J \in S(s)$. We will show that either such a J satisfies $m'(J) < m'(I)$ and $j_2 \not\rhd j_1$ or it is a linear combination of some sequences with these properties modulo Im $\bar{\mathscr{A}}$. Note that if $J \in S(s)$ with $j_2 \not\rhd j_1$, then either it is s-killed by Lemma 5.4 or it is in Cases A, B, C or D of Lemma 5.5. If J is in Case A, it is also s-killed as showed above. Then the lemma follows.

(1) I **is in Case B with** $s(i_3) \geq s'(i_2)$: Set $s' = s'(i_2)$. Let a_i, b_i, c_i be the coefficients of 2^i in the dyadic expansions of i_3, $i_2 + 2^{s'}$, $i_1 - 2^{s'}$ respectively. Then, we have

$$\begin{aligned} Sq^{2^{s'+1}}(i_3, i_2 + 2^{s'}, i_1 - 2^{s'}, 2) &= I + \sum J \\ &= \sum (Sq^{k_0} Q_3)^{a_0} \cdots (Sq^{k_\alpha} Q_3)^{2^\alpha a_\alpha} \\ &\quad \cdot (Sq^{l_0} Q_2)^{b_0} \cdots (Sq^{l_\beta} Q_2)^{2^\beta b_\beta} \\ &\quad \cdot (Sq^{m_0} Q_1)^{c_0} \cdots (Sq^{m_\gamma} Q_1)^{2^\gamma c_\gamma} \\ &\quad \cdot (Sq^n Q_0)^2. \end{aligned}$$

Take a J in the sum. By Lemma 6.7 we can suppose $J \in S(s)$. Compare j_2 and $i_2 + 2^{s'}$.

(a) If $|j_2 - (i_2 + 2^{s'})| \equiv 2^{s'} \bmod 2^{s'+1}$, then $j_2 = i_2$ and $J = I$ by dimensional information.

(b) If $|j_2 - (i_2 + 2^{s'})| \equiv 0 \bmod 2^{s'+1}$, then $j_2 = i_2 + 2^{s'}$ by dimensional information.

- If $j_3 = i_3$, since $J \in S(s)$, so $(j_3, j_2, j_0) = (i_3, i_2 + 2^{s'}, i_0)$. It is contradictory to the fact that $2^{s'+1} = \dim Sq^{2^{s'+1}}$ is not divisible by $\dim Q_1 = 14$.
- If $j_3 \neq i_3$, also by dimensional information we have

$$j_3 - i_3 \equiv 2^u \bmod 2^{u+1}, \qquad u < s'.$$

From $s(i_3) \geq s'(i_2) = s'$, it implies $s(j_3) = u < s'$.

That means $m'(J) < m'(I)$. If $j_2 \not\rhd j_1$ then J has the properties which we want.

Otherwise, $j_2 \rhd j_1$ hence $j_1 = 2^s - 1$ (as $J \in S(s)$). We have

$$(*) \qquad Sq^{2^{s(j_3)+2}}(j_3 + 2^{s(j_3)}, i_2 + 2^{s'} - 2^{s(j_3)}, 2^s - 1, 2) = J + \sum K.$$

By Lemma 6.7, it suffices to consider the case $K \in S(s)$. If $k_2 \not\rhd k_1$ then K has the properties we want. Otherwise, $k_2 \rhd k_1$ hence $k_1 = 2^s - 1$, $k_0 = 2$ (as $K \in S(s)$). Then, by Corollary 3.2, $k_2 \geq i_2 + 2^{s'} - 2^{s(j_3)}$. On the other hand $s(k_3) < s(j_3)$, otherwise $K = J$ by dimensional information. So $k_3 \not\rhd k_2$. We can use an equality that is similar to $(*)$ to handle K by induction on $s(k_3)$. Emphasize that in the inductive procedure, we always have

$$m(K) = m(I) = s,\ m'(K) \leq s(k_3) < s' = m'(I).$$

(c) If $|j_2 - (i_2 + 2^{s'})| \equiv 2^t \bmod 2^{t+1} (t < s')$ ($t > s$ since $s(j_2) = s(i_2) = s$), then $\alpha_t(j_2) = 0$ because of $\alpha_t(i_2) = 1$. Hence

$$s'(j_2) \leq t < s' = \min\{s(i_3), s'(i_2)\}.$$

Let us consider all the possibilities to get $\alpha_t(j_2) = 0$.

- If $Q_2^{2^t}$ moves to $Q_0^{2^t}$ $(l_t = 3)$, then it contradicts the fact that $J \in S(s)$. This possibility does not occur.
- If $Q_2^{2^t}$ moves to $Q_1^{2^t}$ $(l_t = 2)$, then $j_2 \not\rhd j_1$.
- If it raises the power of Q_2 from 2^t then $\binom{i_2+i_1+i_0}{2^t} = 1$. Since $i_0 = 2$, $i_2 = 2^{s'} - 2^s - 1 \bmod 2^{s'+1}$ and $s(i_1) = s$, so $\alpha_t(i_1) = 1$. Then $j_2 \not\rhd j_1$.
- If $Q_2^{2^t}$ moves to either $Q_3^{2^t}Q_0^{2^t}$ or $Q_3^{2^t}Q_1^{2^t}$ $(l_t = 11$ or $10)$, then the situation looks like that in the first two cases. The first possibility does not happen and in the second one, $j_2 \not\rhd j_1$.
- If $Q_3^{2^t}$ moves to $Q_2^{2^t}$ $(k_t = 4)$, then $s(j_3) \leq t < s'$, $j_2 > 2^t$. If $j_2 \not\rhd j_1$, then J has the properties we want. Otherwise, if $j_2 \rhd j_1$ then $j_1 = 2^s - 1$ (as $J \in S(s)$). We handle J by

$$Sq^{2^{s(j_3)+2}}(j_3 + 2^{s(j_3)}, j_2 - 2^{s(j_3)}, 2^s - 1, 2) = J + \sum K$$

and by using a similar argument as in the last item of (b).

(2) I is in either Case B or Case C with $s(i_3) < s'(i_2)$: Put $r = s(i_3) = m'(I)$.

(a) Suppose $r = s = s(i_2)$. Using $Sq^{2^{s+1}}(i_3, i_2 + 2^s, i_1 - 2^s, 2)$ we get as in the proof of Lemma 6.3:

$$I = I' := (i_3, i_2 + 2^s, i_1 - 2^s - 2^{s+1}, 2 + 2^{s+1})$$

modulo $\operatorname{Im}\tilde{\mathscr{A}} + \operatorname{Span}\{J | m(J) < s\}$. It is easy to check that I' satisfies the hypothesis of Lemma 5.7 with $s(i_3') = s$.

(b) Suppose $r > s = s(i_2)$.

$$Sq^{2^{r+2}}(i_3 + 2^r, i_2 - 2^r, i_1, 2) = I + \sum J.$$

$(i_3 + 2^r, i_2 - 2^r, i_1, 2) \in S(s)$. We apply Lemma 6.7 to it. Take a $J \neq I$ in the sum. We can assume $J \in S(s)$. It suffices to prove that $m'(J) < m'(I)$ and $j_2 \not\rhd j_1$. By dimensional information: $J \neq I \Leftrightarrow 0 \leq |j_3 - (i_3 + 2^r)| < 2^r$.

• If $j_3 \neq i_3 + 2^r$: $|j_3 - (i_3 + 2^r)| = 2^u \bmod 2^{u+1}$ so $s(j_3) = u < r$. Then $m'(J) < m'(I)$.

By Corollary 3.2, $j_1 \geq i_1$. Meanwhile, $s(j_2) = s(i_2) = s$, $i_2 \not\triangleright i_1$. Therefore, $j_2 \not\triangleright j_1$.

• If $j_3 = i_3 + 2^r$: From $s'(i_2 - 2^r) = r$ it implies $s'(j_2) \leq r$. If $j_2 = i_2 - 2^r$, then $(i_3 + 2^r, i_2 - 2^r, i_0) = (j_3, j_2, j_0)$. As seen in part (1), it contradicts the fact that $\dim Q_1$ does not divide 2^{r+2}. Now we consider $j_2 \neq i_2 - 2^r$. By dimensional information we get

$$|j_2 - (i_2 - 2^r)| \leq 2^{r+1}.$$

If the equality happens, also by means of dimensional information we have

$$J = (i_3 + 2^r, i_2 - 2^r - 2^{r+1}, i_1 + 2^{r+1}, 2).$$

Note that $m(J) = m(I) = s$, $m'(J) = m'(I) = r$ and J is in Case B with $s(j_3) > r = s'(j_2)$. So J can be controlled by part (1) of this proof.

If $|j_2 - (i_2 - 2^r)| < 2^{r+1} \leq 2^{s'}$. Put $|j_2 - (i_2 - 2^r)| \equiv 2^t \bmod 2^{t+1}$, $t < s'$. Using a similar argument to that of (c) in part (1) we can control J.

(3) I is in Case C with $s(i_3) \geq s'(i_2)$ or I is in Case D: First we show that in the both cases $s(h) < \min\{s(i_3), s'(i_2))\} = s'(i_2)$. Indeed, suppose $i_1 \equiv (2^s - 1) + 2^u \bmod 2^{u+1} (s < u < s')$. In the two cases: $s(i_3) \geq s'(i_2) > u$. So

$$\begin{aligned} h &\equiv (2^{s(i_3)} - 1) + (2^{s'(i_2)} - 2^s - 1) + [(2^s - 1) + 2^u] + 2 \bmod 2^{u+1} \\ &\equiv 2^u - 1 \bmod 2^{u+1}. \end{aligned}$$

Hence $s(h) = u < s'(i_2) \leq s(i_3)$.

Now we can apply Lemma 6.7 to $K = (i_3 - 2^u, i_2, i_1, i_0) \in S(s)$.

$$Sq^{2^{u+3}}(i_3 - 2^u, i_2, i_1, i_0) = I + \sum_J J.$$

By dimensional information, $j_3 \equiv i_3 \bmod 2^{u+1} \Leftrightarrow J = I$.

Otherwise, $|j_3 - i_3| \equiv 2^v \bmod 2^{v+1} (v \leq u)$. Thus

$$s(j_3) = v \leq u < s'(i_2), \text{ hence } m'(J) < m'(I).$$

Moreover,

$$\begin{aligned} &j_0 = i_0 = 2 \quad (J \in S(s)) \\ &j_1 + j_0 \geq i_1 + i_0 \qquad \Rightarrow \quad j_1 \geq i_1 > 2^u. \end{aligned}$$

This together with the fact that $J \in S(s)$ implies $j_2 \not\triangleright j_1$.

The lemma is completely proved.

7. Proofs of Lemma 5.6 and Lemma 5.7

First, suppose that Lemma 5.7 is true. Basing ourself on Lemma 7.1, we prove Lemma 5.6 by combining Lemmas 7.2, 7.3, 7.5, 7.7 below. Then, Lemma 5.7 will be proved at the end of the section.

Lemma 7.1. *Suppose I satisfies the hypothesis of Lemma 5.6, which means $s(h) \geq s(i_3) \geq s(i_2)$, and $i_3 \not\triangleright i_2 \triangleright i_1 \triangleright i_0$. Then*

(a) *either $i_0 = i_1 = 0$, i_2 is even > 0, i_3 is even,*

(b) *or $i_0 = i_1 = 0$, i_2 is even > 0, i_3 is odd, $s(i_2 - 1) \geq s(i_3)$,*

(c) *or* $i_0 = 0, i_1 = 1, s(i_2) = s(i_3) = m(I)$,

(d) *or* $i_0 = 2, i_1 = 2^s - 1 \ (s > 1), s(i_2) = s(i_1) = s = m(I), s \le s(i_3) \le s'(i_2), s(h) \ge s(i_3)$.

Proof. Using actually the argument of Lemma 4.5 we get $i_0 = [2 : 2^{s(i_1)}] = 0$ or 2.

(a) If $i_0 = 0$, then $s(i_1) = 0$ or 1. Considering the reduced sequence (i_3, i_2, i_1) at length 3 and repeating the argument mentioned above we obtain $i_1 = 0$ or 1. If $i_1 = 0$, and $s(h) = 0$, then $s(i_3) = s(i_2) = 0$. That means i_2, i_3 are even. Since $i_3 \not\rhd i_2$, so $i_2 > 0$.

(b) If $i_0 = i_1 = 0$ and $s(h) > 0$, then either i_2 or i_3 is odd, the other is even. But $s(i_3) \ge s(i_2)$ so i_3 is odd and i_2 is even. By $s(h) \ge s(i_3)$ we get $s(i_2 - 1) = s(i_2 + i_1 + i_0 - 1) \ge s(i_3)$.

(c) If $i_0 = 0, i_1 = 1$, from $s(h) \ge s(i_3)$ it implies $s(i_2 + i_1 - 1) = s(i_2) \ge s(i_3)$, so $s(i_3) = s(i_2)$.

(d) If $i_0 = 2$, then $s(i_1) > 1$. The hypothesis $s(h) \ge s(i_3) \ge s(i_2)$ implies $s(i_1 + i_0 - 2) = s(i_1) \ge s(i_2)$, so $s(i_2) = s(i_1) = s$ (say). This equality together with $i_2 \rhd i_1$ implies $i_1 = 2^s - 1$. Set $s' = s'(i_2)$, that means $i_2 \equiv 2^{s'} - 2^s - 1 \bmod 2^{s'+1}$. Since $s(h) \ge s(i_3)$ so $s(i_2 + i_1 + i_0 - 1) \ge s(i_3)$, or equivalently

$$s(2^{s'} - 2^s - 1 + 2^s - 1 + 2 - 1 \bmod 2^{s'+1}) = s' \ge s(i_3).$$

The lemma follows.

Now we prove Lemma 5.6 by showing Lemmas 7.2, 7.3, 7.5, 7.7 below.

Lemma 7.2. *Suppose I belongs to case* (a) *of Lemma* 7.1, *that means $i_0 = i_1 = 0$, i_2 is even and positive, i_3 is even. Then I is absolutely killed.* (*That means $I \in \operatorname{Im}\bar{\mathscr{A}}$.*)

Lemma 7.3. *Suppose I belongs to case* (b) *of Lemma* 7.1, *that means $i_0 = i_1 = 0$, i_2 is even > 0, i_3 is odd, $s(i_2 - 1) \ge s(i_3)$. Then I is absolutely killed.* (*That means $I \in \operatorname{Im}\bar{\mathscr{A}}$.*)

In the previous two lemmas $m(I) = 0$. So they are special cases of Lemma 5.10.

In order to prove the main lemma in case (c) of Lemma 7.1 we need the following technical lemma.

Lemma 7.4. *Let $H = (h_3, h_2, 1, 0)$. If $s(h_3) = s(h_2) = s$, then for any a*

$$Sq^{2^a}(h_3, h_2, 1, 0) = \sum_J J,$$

with $m(J) \le m(H) = s$ for every J in the sum.

Proof.

$$\begin{aligned} Sq^{2^a}(h_3, h_2, 1, 0) &= \sum J \\ &= \sum (Sq^{k_0}Q_3)^{a_0} \cdots (Sq^{k_n}Q_3)^{2^n a_n} \\ &\quad \cdot (Sq^{l_0}Q_2)^{b_0} \cdots (Sq^{l_\beta}Q_2)^{2^\beta b_\beta} \\ &\quad \cdot (Sq^m Q_1). \end{aligned}$$

Here a_i, b_i are the coefficients of 2^i in the dyadic expansions of h_3, h_2 respectively, and $k_i = 0$ if $a_i = 0$, $l_i = 0$ if $b_i = 0$.

Take a sequence J in the sum. Define

$$x = \sum_{k_i=4,6,7} 2^i a_i, \quad y = \sum_{l_j=12} 2^j b_j + \begin{cases} 1 & \text{if } m = 12 \text{ or } 13 \text{ or } 14, \\ 0 & \text{otherwise.} \end{cases}$$

So we have $j_2 + j_1 + j_0 - 1 = h_2 + h_1 + h_0 - 1 + x + y$.

Case A: $h(J) > h(H)$. We need only to consider J with $s(j_2 + j_1 + j_0 - 1) > s = m(H)$.

(1) We show $x \not\equiv 2^s \bmod 2^{s+1}$. Indeed, if $x \equiv 2^s \bmod 2^{s+1}$, by definition of x then $a_s = 1$. However, $a_s = 0$ since $s(h_3) = s$. This is a contradiction.

(2) Suppose $x \equiv 0 \bmod 2^{s+1}$. One gets

$$j_2 + j_1 + j_0 - 1 \equiv h_2 + h_1 + h_0 - 1 + y \bmod 2^{s+1}.$$

Combining this with $s(j_2 + j_1 + j_0 - 1) > s = s(h_2 + h_1 + h_0 - 1)$ we obtain $y \equiv 2^s \bmod 2^{s+1}$. Recall that $b_s = 0$, so $l_s = 0$. Hence

$$\begin{cases} l_j = 12 & \text{for any } j \text{ with } 0 \le j < s \text{ (note } b_j = 1 \text{ for any } j < s), \\ m = 12 \text{ or } 14. \end{cases}$$

(Note that $m \neq 13$ since 2^a is even if $2^a \ge 13$.) Consider $u = \min\{i | k_i = 8\}$ (u may not exist).

(a) We claim $u \neq s$. Indeed, from $a_s = 0$ it implies $k_s = 0$.

(b) If $u < s$, combining this with the facts that $x \equiv 0 \bmod 2^{s+1}$, $l_j = 12$ for $j < s$, $m = 12$ or 14 we get $j_3 \equiv 2^u - 1 \bmod 2^{u+1}$. So $m(J) \le s(j_3) = u < s$.

(c) If $u > s$ or there does not exist u, combining this with the facts that $x \equiv 0 \bmod 2^{s+1}$, $l_j = 12$ for $j < s$, $m = 12$ or 14 we have $j_3 \equiv 2^s - 1 \bmod 2^{s+1}$. So $m(J) \le s(j_3) = s = m(H)$.

(3) Suppose $x \equiv 2^v \bmod 2^{v+1}$, $v < s$. It is easy to see

$$j_2 + j_1 + j_0 - 1 \equiv h_2 + h_1 + h_0 - 1 + y \bmod 2^v.$$

As $s(j_2 + j_1 + j_0 - 1) > s = s(h_2 + h_1 + h_0 - 1)$, so $y \equiv 0 \bmod 2^v$.

(a) There exists $i < v$ with $k_i = 8$. Then $m(J) \le s(j_3) = i < v < s$.

(b) Otherwise, if there does not exist $i < v$ with $k_i = 8$, then $m(J) \le s(j_3) = v < s$.

Case B: $h(J) = h(H)$. Then $y = 0$ by definition.

(1) We show $x \not\equiv 2^s \bmod 2^{s+1}$ by the same argument as in (1) of Case A.

(2) If $x \equiv 0 \bmod 2^{s+1}$, then the fact that $j_2 + j_1 + j_0 - 1 = h_2 + h_1 + h_0 - 1 + x$ implies

$$m(J) \le s(j_2 + j_1 + j_0 - 1) = s(h_2 + h_1 + h_0 - 1) = s.$$

(3) Suppose $x \equiv 2^v \bmod 2^{v+1}$, $v < s$. As $h(J) = h(H)$, so $j_3 = h_3 - x$. Hence $m(J) \le s(j_3) = v < s$.

The lemma is proved.

Lemma 7.5. *Suppose I belongs to case* (c) *of Lemma* 7.1. *That means*

$$i_0 = 0,\ i_1 = 1,\ s(i_2) = s(i_3) = s = m(I), \text{ and } i_3 \not\rhd i_2.$$

(a) *Further if $h \not\rhd i_3$, then the weak form of the main lemma holds for I.*

(b) *If $h \rhd i_3$, then the strong form of the main lemma holds for I.*

Proof. **(a)** $h \not\rhd i_3$. Set $t = s(h) > s$, we kill I by the usual method

$$Sq^{2^{t+3}}(i_3 - 2^t, i_2, 1, 0) = I + \sum_J J.$$

By Lemma 7.4, $m(J) \leq m(i_3 - 2^t, i_2, 1, 0) = s$. By dimensional information $h(J) < h(I)$.

(b) $h \rhd i_3 \not\rhd i_2$.

This case is treated in the following lemma.

Lemma 7.6. *Suppose* $I = (i_3, i_2, i_1, i_0)$ *satisfies* $i_3 \not\rhd i_2 \rhd i_1 = 1, i_0 = 0, s(i_3) = s(i_2) = s$, $i_3 + 2^s \not\rhd i_2$. *Then*

$$Q^I \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < m(I) = s\}.$$

Proof. Note that the hypothesis of the lemma is valid at least when

$$h \rhd i_3 \not\rhd i_2 \rhd i_1 = 1, \quad i_0 = 0, s(i_3) = s(i_2) = s.$$

Suppose $s < r$. Consider the submodule

$$R(s, r) = \operatorname{Span}\{Q^J | j_3 \not\rhd j_2 \rhd j_1 = 1, j_0 = 0, s(j_3) = s(j_2) = s, \\ j_3 + 2^s \not\rhd j_2, s'(j_3) \leq r\}.$$

Now we show that if I is as in the lemma, and $r = s'(i_3)$, then

$$Q^I \in \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < m(I) = s\} + R(s, r-1).$$

Furthermore, one could see

$$R(s, s+1) \subset \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < s\}.$$

So, the lemma follows.

From $i_3 + 2^s \not\rhd i_2$, it implies $i_2 \geq 2^r$, where $r = s'(i_3)$. One gets

$$Sq^{2^{r+2}}(i_3 + 2^r, i_2 - 2^r, 1, 0) = I + \sum_J J.$$

Let J be a term in the right-hand side.

If $j_0 > 0$: Then j_0 is even (dim information). By Lemma 7.4, it suffices to consider $m(J) = m(I)$. First we show that $s(h(J)) \geq s(j_3)$. In fact, if $h(J) = h(I)$, combine this with $s(i_3 + 2^r) = s$ and get $s(j_3) \leq s$. On the other hand, $s(h(J)) = s(h(I)) > s$. So $s(h(J)) \geq s(j_3)$. Suppose $h(J) > h(I)$ and $m(J) = m(I)$. Going through the proof of Lemma 7.4 we observe that in this case $s(h(J)) \geq s(j_3) = s = m(I)$.

• If $j_0 \neq 2$: It is easy to check that J is s-killed by Lemma 5.4, Case A in Lemma 5.5 and Lemma 5.7.

• If $j_0 = 2$: Since $i_0 = 0$, j_0 is moved from either $i_3 + 2^r$, $i_2 - 2^r$ or $i_1 = 1$. Hence

$$\text{either } j_3 \not\rhd j_0, \quad \text{or } j_2 \not\rhd j_0 \quad \text{or } j_1 \not\rhd j_0.$$

– If $j_1 \not\rhd j_0$: $s(j_1) \leq 1$. We can assume $s(h), s(j_3), s(j_2)$ all ≥ 1. (Otherwise, $m(J) = 0$, then J is absolutely killed as seen in the proof of Theorem 2.7 at the end of Section 5.) Now we can apply Lemma 5.4 and J is s-killed.

– If $j_1 \rhd j_0, j_2 \not\rhd j_0$: $s(j_2) \leq 1 < s(j_1)$. Again, it suffices to consider $s(h), s(j_3)$ all ≥ 1. We can apply Case A of Lemma 5.5 and J is s-killed.

– If $j_2 \rhd j_0$, $j_1 \rhd j_0$, $j_3 \not\rhd j_0$: $s(j_3) \leq 1 < s(j_2)$. Again, we need only to consider the case $s(h) \geq 1 \geq s(j_3) < s(j_2)$. J is s–killed by Lemma 5.7.

If $j_0 = 0$: According to Lemma 7.4 it suffices to consider J with $m(J) = m(I) = s$.

Case A: $h(J) = h(I) = h$, $m(J) = m(I) = s$.

Since $s(i_3) = s(i_2 + i_1 + i_0 - 1) = s$, so $s(h) > s = m(J)$. Hence $s(j_3) = s(j_2 + j_1 + j_0 - 1) = s$.

(1) If $s(j_2) > s$, then we can apply Lemma 5.7 to show J is s–killed.

(2) If $s(j_2) < s$, as $h(J) = h(I)$ we have

$$z = \sum_{l_j=2} 2^j b_j \not\equiv 0 \bmod 2^s \equiv 2^u \bmod 2^{u+1}, \quad \text{for some } u < s.$$

Here we use the notations given in the proof of Lemma 7.4 with $h_3 = i_3 + 2^r$, $h_2 = i_2 - 2^r$. Hence $j_1 = i_1 + z \bmod 2^s$. Combining this with the fact that $s(j_2) = u$ we get $j_2 \not\rhd j_1$. We can apply Lemma 5.5 to show J is s–killed.

(3) $s(j_2) = s$.

(a) $j_1 > 1$. Combine $s(j_2 + j_1 + j_0 - 1) = s$, $s(j_2) = s$, $j_1 > 1$, $j_0 = 0$ and get $j_1 > 1 + 2^s$. So $j_2 \not\rhd j_1$. Then Q^J is s–killed by Lemma 5.5 again.

(b) $j_1 = 1$. We show that either $J = I$ or $J \in R(s, r-1)$.

Because of $h(J) = h(I)$, $j_0 = i_0 = 0$, $j_1 = i_1 = 1$, so $j_3 + j_2 = i_3 + i_2$.

Recall $s(j_3) = s(j_2) = s$. We will prove that $j_3 + 2^s \not\rhd j_2$. Indeed $j_3 = i_3 - \sum_{k_i=4} a_i 2^i$. Combine this with $s(j_3) = s(i_3) = s$ and get $s(j_3 + 2^s) \leq s(i_3 + 2^s)$. That means $s'(j_3) \leq s'(i_3) = r$.

On the other hand, $j_2 \geq i_2$ by Corollary 3.2, $i_3 + 2^s \not\rhd i_2$. Hence $j_3 + 2^s \not\rhd j_2$.

If $s'(j_3) = s'(i_3)$, then $j_3 \equiv i_3 \bmod 2^{r+1}$. Note that $|Sq^{2^{r+2}}| = 4 \cdot 2^r$. By dimensional information we get $J = I$.

Otherwise, if $s'(j_3) < s'(i_3) = r$, then $J \in R(s, r-1)$.

Case B: $h(J) > h(I)$, $m(J) = m(I) = s$.

Going though the proof of Lemma 7.4, we see that the hypotheses $h(J) > h(I)$, $m(J) = m(I) = s$ happen only if $s(j_3) = s$. Consider the following two cases.

(1) $s(j_3) = s$, $s(j_2 + j_1 + j_0 - 1) > s$.

(a) $s(j_2) \leq s$. Combine this with $s(j_2 + j_1 + j_0 - 1) > s$, $j_0 = 0$ and get $j_1 \geq 1 + 2^s$. So $j_2 \not\rhd j_1$. Then Q^J is s–killed by Lemma 5.5.

(b) $s(j_2) > s$. Then $j_3 \not\rhd j_2$. So Q^J is s–killed by Lemma 5.7.

(2) $s(j_3) = s$, $s(j_2 + j_1 + j_0 - 1) = s$. It implies that $s(h(J)) > s$.

(a) $s(j_2) < s$. So $j_1 \geq 1 + 2^{s(j_2)}$. Hence $j_2 \not\rhd j_1$. Meanwhile $s(h(J)) > s(j_3) \geq s(j_2)$. Then Q^J is s–killed by Lemma 5.5.

(b) $s(j_2) > s$. So $s(h(J)) > s(j_3) < s(j_2)$. Then Q^J is s–killed by Lemma 5.7.

(c) $s(j_2) = s$. If $j_1 > 1$, then $j_1 \geq 1 + 2^{s(j_2)}$. So Q^J is also s–killed by Lemma 5.5. Suppose $j_1 = 1$. Note that $j_3 \geq i_3 + 2^r - 2^{r+2}/4 = i_3$.

If $j_3 = i_3$, then $J = I$ (by dimensional information). This contradicts the fact that $h(J) > h(I)$.

If $j_3 > i_3$, then $i_3 < j_3 \leq i_3 + 2^r + 2^{r-1}$. So $s'(j_3) \leq r - 1$.

There are two possibilities:

- $j_3 + 2^s \not\rhd j_2$, then $Q^J \in R(s, r-1)$.

- $j_3 + 2^s \rhd j_2$, then $j_2 < 2^{s'(j_3)} \leq 2^{r-1}$. Set

$$u = \max\{i | \alpha_i(j_3) = 0,\ \alpha_{i+1}(j_3) = 1\} \geq s'(j_3).$$

Then $j_3 - 2^u = \alpha_0 \cdot 2^0 + \cdots + 2^u + 0 \cdot 2^{u+1} + j$, where $j \equiv 0 \bmod 2^{u+2}$. Since $j_3 + 2^s \rhd j_2$, so $j_2 < 2^{s'(j_3)} \leq 2^u$.

$$Sq^{2^{u+3}}(Q_3^{j_3-2^u} Q_2^{j_2} Q_1) = Q_3^j Sq^{2^{u+3}}(Q_3^{j_3-2^u-j} Q_2^{j_2} Q_1).$$

Therefore, we can reduce to the case $j = 0$, i.e., we have

$$j_3 - 2^u = \alpha_0 \cdot 2^0 + \cdots + 2^u.$$

$$\begin{aligned} Sq^{2^{u+3}}(Q_3^{j_3-2^u} Q_2^{j_2} Q_1) = {} & (Sq^8 Q_3)^{2^u}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1) \\ & + (Sq^7 Q_3)^{2^u} Sq^{2^u}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1) \\ & + (Sq^6 Q_3)^{2^u} Sq^{2^{u+1}}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1) \\ & + (Sq^4 Q_3)^{2^u} Sq^{2^{u+2}}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1) \\ & + (Q_3)^{2^u} Sq^{2^{u+3}}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1). \end{aligned}$$

The first term is obviously Q^J.

Let the second term be $\sum Q^T$. Since $Sq^7 Q_3 = Q_0$, then $t_0 \geq 2^u$ for any T in the sum. One can repeat the argument for the previous cases of this lemma to show that Q^T is s-killed by Lemma 5.4 or Lemma 5.5.

Let the third term be $\sum Q^T$. Since $Sq^6 Q_3 = Q_1$, so $t_1 \geq 2^u$ for any T in the sum. Using Lemma 5.5 one can s-kill Q^T by the same way that is used for the second term.

Let the fourth term be $\sum Q^T$. Since $Sq^4 Q_3 = Q_2$, so $t_2 \geq 2^u$ for any T in the sum. One can repeat the argument for the previous cases of this lemma to show that, studying modulo $\operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^K | m(K) < s = m(J)\}$, one needs only to consider T with $s(t_3) = s$, $s'(t_3) \leq s'(j_3) - 1 \leq r - 2$. So $t_3 + 2^s \not\rhd 2^{s'(t_3)} \leq 2^u$. Hence $t_3 + 2^s \not\rhd t_2$. Therefore, Q^T is s-killed modulo $R(s, r-1)$ by Lemmas 5.4, 5.5 and 5.7.

Suppose the last term is $\sum Q^T$. Again, using the argument for the previous cases of this lemma, it suffices to consider T's satisfying

$$m(T) = s(t_3) = s(t_2) = s,\ t_3 + 2^s \rhd t_2,\ t_1 = 1,\ t_0 = 0.$$

However, we will arithmetically prove that there is no such a T.

Let us apply Lemma 7.4 to $Sq^{2^{u+3}}(Q_3^{j_3-2^{u+1}} Q_2^{j_2} Q_1)$ and use the notations given in its proof $(a_i, b_i, k_i, l_i, m...)$.

Fix such a T and take a corresponding sequence $\{k_i, l_i, m\}$.

(*) First, we show that there exists i such that $l_i \neq 0$. Otherwise, if $l_i = 0$ for any i, then combining this with the fact that $m = 0$ (because of $t_1 = 1$, $t_0 = 0$) we claim Q^T is a term of

$$Sq^{2^{u+3}}(Q_3^{j_3-2^{u+1}}) Q_2^{j_2} Q_1 = 0,$$

(as $j_3 - 2^{u+1} < 2^u$).

(**) Next, we show that one can choose a sequence $\{k_i, l_i, m\}$ among those corresponding to Q^T so that, if $l_x \neq 0$ then $k_i = 0$ for any $i \leq x$. Suppose the contrary. Let $v = \min\{i | i \leq x, k_i \neq 0\}$. As $s(t_3) = s(t_2) = s$, we get $v > s$. Note that $k_v = 4$ or 8 (because of $t_1 = 1, t_0 = 0$). If either $k_v = 4$ or 8, and $l_v = 0$ or 12, then $\alpha_v(t_3) = \alpha_v(t_3 + 2^s) = 0$, so $s(t_3 + 2^s) \leq v$. Meanwhile, $l_x \neq 0$ hence $l_x = 8$ or 12 (because of $t_1 = 1, t_0 = 0$). It implies $t_2 \geq 2^x \geq 2^v$. Thus $t_3 + 2^s \not\rhd t_2$. This contradicts the hypothesis on T.

If $k_v = 4$ and $l_v = 8$, we choose another sequence $\{k_i', l_i', m\}$ which corresponds to Q^T as well as $\{k_i, l_i, m\}$ as follows:

$$k_i' = \begin{cases} k_i & \text{if } i \neq v, \\ 0 & \text{if } i = v, \end{cases} \qquad l_i' = \begin{cases} l_i & \text{if } i \neq v, \\ 12 & \text{if } i = v. \end{cases}$$

The new sequence satisfies the property we state at the beginning of the item.

(***) Finally, set $j = \min\{i | l_i \neq 0\}$. From $s(t_3) = s(t_2) = s$, $t_1 = 1$, $t_0 = 0$ it implies that $j > s$, $m = 0$ and if $k_i \neq 0$ then $k_i = 4$ or 8, also if $l_i \neq 0$ then $l_i = 8$ or 12. They all are divisible by 4. Since $l_j \neq 0$ so $b_j = 1$ (by definition of l_j). Furthermore,

$$2^j l_j = 2^j l_j b_j = 2^{u+3} - \sum_{i>j} 2^i k_i a_i - \sum_{i>j} 2^i l_i b_i \equiv 0 \bmod 2^{j+3}.$$

It implies $l_j = 8$ (but not 12).

If $l_{j+1} = 0$, then $2^j l_j = 2^{j+3} \equiv 2^{j+1} k_{j+1} a_{j+1} \bmod 2^{j+4}$. Then $k_{j+1} = 4$ ($a_{j+1} = 1$). So $s(t_3 + 2^s) \leq j + 1$, $t_2 \geq 2^{j+1}$. Hence $t_3 + 2^s \not\rhd t_2$ (contradiction).

If $l_{j+1} = 8$, then $k_{j+1} = 0$ (see (**)). Thus $2^{j+3} \equiv 0 \bmod 2^{j+4}$. This cannot happen.

Therefore, $l_{j+1} = 12$. So $b_{j+1} = \alpha_{j+1}(j_2) = 1$. That means $j_2 \geq 2^{j+1}$. Combining this with $j_3 + 2^s \rhd j_2$ we get $a_{s+1} = \cdots = a_{j+1} = 1$ (recall that $a_i = \alpha_i(j_3 - 2^{u+1})$).

Meanwhile, $l_j = 8$, $a_j = 1$ implies $\alpha_j(t_3) = 0$, so $s(t_3 + 2^s) \leq j$.

On the other hand, $l_{j+1} = 12$ implies $t_2 \geq 2^{j+1} \cdot 2 = 2^{j+2}$. Therefore $t_3 + 2^s \not\rhd t_2$ (contradiction).

The fact that $R(s, s+1) \subset \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{Q^J | m(J) < s\}$ can be read off from the inductive procedure on r.

In the proof of the lemma we need only to use Lemmas 5.4, 5.5 and 5.7, so the strong form of the main lemma holds for I. The lemma, and so Lemma 7.5, is proved.

Lemma 7.7. *Suppose I belongs to case* (d) *of Lemma* 7.1. *That means*

$$i_0 = 2, \quad i_1 = 2^s - 1 \ (s > 1), \quad s(i_2) = s(i_1) = s = m(I),$$

$$s \leq s(i_3) \leq s'(i_2), \quad s(h) \geq s(i_3).$$

Then either the strong form or the exceptional form of the main lemma holds for I.

Proof. In this proof, one can see how the strong form of the main lemma is needed.

Set $r = s(i_3)$. We kill I by the usual method using $(i_3 + 2^r, i_2 - 2^r, i_1, i_0)$.

$$\begin{aligned} Sq^{2^{r+2}}(i_3 + 2^r, i_2 - 2^r, i_1, i_0) &= I + \sum J \\ &= \sum (Sq^{k_0}Q_3)^{a_0} \cdots (Sq^{k_\alpha}Q_3)^{2^\alpha a_\alpha} \\ &\quad \cdot (Sq^{l_0}Q_2)^{b_0} \cdots (Sq^{l_\beta}Q_2)^{2^\beta b_\beta} \\ &\quad \cdot (Sq^{m_0}Q_1)^{c_0} \cdots (Sq^{m_\gamma}Q_1)^{2^\gamma c_\gamma} \\ &\quad \cdot (Sq^n Q_0)^2. \end{aligned}$$

Here a_i, b_i, c_i are the coefficients of 2^i in the dyadic expansions of $i_3 + 2^r, i_2 - 2^r, i_1$ respectively. Convention: $k_i = 0$ if $a_i = 0$, $l_i = 0$ if $b_i = 0$, $m_i = 0$ if $c_i = 0$. Consider a J in the sum with $h' = h(J)$. We need only to study the case $m(J) \geq m(I) = s$. That means $s(j_3), s(j_2)$, and $s(j_1 + j_0 - 2)$ all $\geq s$.

Case 1: $s(j_3) \geq s, s(j_2) > s$. These imply $k_s = 4$ and $s(j_3) = s$. Hence $m(J) \leq s = m(I) \leq m(J)$, so $m(J) = s \leq s(h')$. We can apply Lemma 5.7 and J is s-killed.

Case 2: $s(j_3) \geq s, s(j_2) = s, s(j_1) > s$. Then $m(J) \leq s(j_2) = s = m(I)$. So $m(J) = s$. Then $s(h') \geq m(J) = s$. Since $s(j_2) < s(j_1)$ so $j_2 \not\rhd j_1$, we can apply Case A of Lemma 5.5: J is s-killed.

Case 3: $s(j_3) \geq s, s(j_2) = s, s(j_1) = t < s$. Similarly as before $m(J) = s$. Hence $s(j_1 + j_0 - 2) \geq s$. This together with $s(j_1) = t < s$ implies $j_0 > 2^t$. Therefore, $j_1 \not\rhd j_0$. We also have $s(h') \geq m(J) = s > t$. Hence, by Lemma 5.4, J is s-killed.

Case 4: $s(j_3) \geq s, s(j_2) = s(j_1) = s$. We also have $m(J) = s$. Then $s(h') \geq s$.

If $j_2 \not\rhd j_1$ or $j_1 \not\rhd j_0$: then we can apply Lemma 5.4 or Lemma 5.5: J is s-killed.

If $j_2 \rhd j_1 \rhd j_0$: we will show $s(h') \geq s(j_3)$. In fact, $s(j_3) \geq s(j_2) = s(j_1) = s \leq s(h')$ and $j_2 \rhd j_1 \rhd j_0$ imply $j_0 = 2 = i_0, j_1 = 2^s - 1 = i_1$ (by the same argument as in the proof of Lemma 4.5). So $j_3 \neq i_3 + 2^r$. Otherwise,

$$2^{r+2} = \dim Q_2 \cdot \{j_2 - (i_2 - 2^r)\} \equiv 0 \mod 12.$$

This cannot happen. We note that $s(j_3) < r$. (The only J with $s(j_3) \geq r$ is I, by dimensional information.)

Suppose the contrary that $s(h') < s(j_3)$ or equivalently $s(j_3) > s'(j_2) := u$. Dimensional information shows

$$\begin{aligned} 2^{r+2} &= \dim Q_3\{j_3 - (i_3 + 2^r)\} + \dim Q_2\{j_2 - (i_2 - 2^r)\} \\ &\equiv 12 \cdot 2^u \mod 2^{u+3}. \end{aligned}$$

This contradicts $u < r - 1$. So we get $s(h') \geq s(j_3) \geq s(j_2) \geq s(j_1)$.

Assume in addition $j_3 \rhd j_2 \rhd j_1 \rhd j_0$: Recall $s(h') \geq s(j_3)$, and $j_0 \geq i_0 = 2$. By the method in Lemma 4.5 and Remark 4.9, we get:

(a) either $j_0 = 2, j_1 = 2^s - 1, j_2 = 2^s - 1, j_3 \equiv 2^s - 1 \mod 2^{s+1}$.

(b) or $j_0 = 2, j_1 = 2^s - 1, j_2 = 2^t - 2^s - 1, j_3 \equiv 2^t - 1 \mod 2^{t+1} (t > s)$.

In the both cases, J should be $(i_3 + 2^r + 2^{r-1}, i_2 - 2^r, i_1, i_0)$. Actually case (b) cannot happen. If so, $t = s(j_3) = r - 1$, and $j_2 = 2^t - 2^s - 1 = i_2 - 2^r$. Hence, $i_2 = 2^{t+1} + 2^t - 2^s - 1, s'(i_2) = t < s(i_3)$. This contradicts the hypothesis of the lemma: $s(i_3) \leq s'(i_2)$.

In case (a): $r-1=s$, $s(i_3)=r=s+1$, $i_3\equiv 2^{s+1}-1 \bmod 2^{s+2}$. Thus $j_3=i_3+2^{s+1}+2^s\equiv 2^s-1 \bmod 2^{s+2}$. Since $j_3>2^s-1$, we set $j_3=2^t-2^{s+2}+2^s-1+x$, where $x\equiv 0 \bmod 2^{t+1}$, $t>s+2$. We get

$$i_3=2^t-2^{s+2}-2^{s+1}-1+x,\ h'=h(J)=2^t-2^s-1+x.$$

Note: $h'\rhd\!\rhd j_3$ if and only if $x=0$.

If $x\neq 0$: then $x>2^t$, $\alpha_t(j_3)=0$. Let v be a number $\geq t$ such that $\alpha_v(j_3)=0$, $\alpha_{v+1}(j_3)=1$. (v exists as $x>2^t$.) Hence $\alpha_v(h)=0$.

$$Sq^{2^{v+3}}(j_3-2^v, j_2, j_1, j_0)=J+0\cdot(j_3-2^v-2^{v+1}, j_2+2^{v+1}, j_1, j_0)$$
$$+\operatorname{Span}\{K|m(K)<m(J)=s\}.$$

Indeed, any change at j_2, j_1 or j_0 makes the function $m(\cdot)$ smaller.

If $x=0$: $J=I'=(2^t-2^{s+1}-2^s-1, 2^s-1, 2^s-1, 2)$ is a weakly allowed sequence (as $t>s+2$). We observe $I=(2^t-2^{s+2}-2^{s+1}-1, 2^{s+1}+2^s-1, 2^s-1, 2)$. So $h(I)=2^t-2^{s+1}-1<h(I')=2^t-2^s-1$, $m(I)=m(I')=s$.

Finally assume that $j_3\not\rhd j_2\rhd j_1\rhd j_0$: Using Lemma 4.5, from these and $j_0\geq i_0=2$, it implies $j_0=2$. Now J satisfies the hypothesis of Lemma 7.7 (see Lemma 7.1). Recall that $s(j_3)<s(i_3)$. So we can repeat the above procedure to handle J inductively on $s(j_3)$.

(*Remark.* h' could be greater than h. But it does not damage the proof because we are concerned only with the strong form of the main lemma.)

In the inductive procedure we might meet a weakly allowed sequence of the form $J=I'=(2^t-2^{s+1}-2^s-1, 2^s-1, 2^s-1, 2)$, when $x=0$. We cannot meet more than one sequence of this form because of dimensional information. That means either the strong form or the exceptional form of the main lemma holds for I. The lemma is completely proved.

Example 7.8. Let $I=(2^{t-1}-1, 2^t-2^s-1, 2^s-1, 2)$. The above inductive procedure shows modulo $\operatorname{Im}\bar{\mathscr{A}}+\operatorname{Span}\{K|m(K)<s\}$:

$$\begin{aligned} I &= (2^t+2^{t-2}-1, 2^{t-1}-2^s-1, 2^s-1, 2)\\ &= (2^t+2^{t-1}+2^{t-3}-1, 2^{t-2}-2^s-1, 2^s-1, 2)\\ &= \cdots=\cdots\\ &= (2^{t+1}-2^{s+1}-2^s-1, 2^s-1, 2^s-1, 2).\end{aligned}$$

The last sequence is weakly allowed.

Now we give a direct proof for Lemma 5.7.

Proof of Lemma 5.7. According to Lemma 5.1 and Definition 5.2, $m(I)=s:=s(i_3)$, and

$$I+\binom{i_2-2^s}{2^{s+1}}I'+\binom{i_1}{2^{s+2}}I''\in\operatorname{Im}\bar{\mathscr{A}}+\operatorname{Span}\{J|m(J)<s\},$$

where

$$I'=(i_3+2^s, i_2-2^s-2^{s+1}, i_1+2^{s+1}, i_0),$$
$$I''=(i_3+2^s, i_2-2^s, i_1-2^{s+2}, i_0+2^{s+2}).$$

It is easy to check that I'' is s-killed by Lemma 5.4 or Case A of Lemma 5.5, since $i_0'' = i_0 + 2^{s+2} > 2$. We need only to study I' with $\binom{i_2 - 2^s}{2^{s+1}} = 1$ or equivalently $\alpha_{s+1}(i_2 - 2^s - 2^{s+1}) = 0$. So $s(i_2 - 2^s - 2^{s+1}) = s$, and

$$s'(i_2 - 2^s - 2^{s+1}) = s + 1.$$

We can concentrate on the case

$$s(i_1 + 2^{s+1}) = s, \quad s'(i_1 + 2^{s+1}) = s + 1, \quad i_0 = 2.$$

Otherwise, I' is s-killed by Lemma 5.4 or Case A of Lemma 5.5 as before. Hence,

$$i_2 - 2^s - 2^{s+1} \not\geqslant i_1 + 2^{s+1}.$$

I' turns out to be a very special case in Case B of Lemma 5.5 with $s'(i_2') = s(i_2') + 1$. We have

$$\begin{aligned} &Sq^{2^{s+1}}(i_3 + 2^s, i_2 - 2^{s+1}, i_1 + 2^s, 2) \\ &\quad = I' + (i_3 + 2^s, i_2 - 2^{s+1}, i_1 + 2^s - 2^{s+1}, 2 + 2^{s+1}) \\ &\qquad\qquad \text{modulo Span}\{K | m(K) < s\}. \end{aligned}$$

Denote the second term by J. We note that

$$s(i_2 - 2^{s+1}) = s(i_1 + 2^s - 2^{s+1}) = s + 1,$$

and either $s(i_3 + 2^s) = s + 1$, hence s $(h(J)) > s + 1$, or $s(h(J)) = s + 1$, hence $s(i_3 + 2^s) > s + 1$. From here to the end of this section, all the computations are modulo Span$\{L | m(L) < s\}$. We always try to show $J = K$ modulo $\operatorname{Im}\bar{\mathscr{A}} +$ Span$\{L | m(L) < s\}$, for some K with $s(k_3) = s(k_2) = s(k_1) = s$ in the remaining part of the section.

We need the technical lemma:

Lemma 7.9. *Suppose* $s(i_3) = s(i_2) = s(i_1) = s$, $s'(i_2) = s + 1$, $i_1 > 2^{s+1}$. *Then* I *is* s*-killed.*

Proof.

$$Sq^{2^{s+2}}(i_3, i_2 + 2^{s+1}, i_1 - 2^{s+1}, i_0) = I \quad \text{modulo Span}\{J | m(J) < s\}.$$

(Use Lemma 5.4.) The lemma is proved.

Come back to the proof of Lemma 5.7.

Let us consider the two possibilities for J as seen above.

(1) $J = (2^{s+1} - 1 + a, 2^{s+1} - 1 + b, 2^{s+1} - 1 + c, 2 + 2^{s+1})$, with $a \equiv b \equiv c \equiv 0 \bmod 2^{s+2}$.

$$\begin{aligned} &Sq^{2^{s+1}}(2^{s+1} - 1 + a, 2^{s+1} - 1 + b, 2^{s+2} - 1 + c, 2) \\ &\quad = J + \underbrace{(2^{s+1} - 1 + a, 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2)}_{K}. \end{aligned}$$

(a) If $\alpha_{s+2}(b) = 0$, then

$$Sq^{2^{s+3}}(2^{s+1} - 1 + a, 2^{s+2} + 2^s - 1 + b, 2^s - 1 + c, 2)$$
$$= K + \underbrace{(2^{s+1} + \boxed{2^s} - 1 + a, 2^{s+2} + 2^s - 1 + b, 2^s - 1 + c, 2)}_{L}.$$

- *If* $c \neq 0$: L is s-killed by Lemma 7.9.
- *If* $c = 0$: Note that $\alpha_{s+1}(h(L)) = 0$.

$$Sq^{2^{s+4}}(2^s - 1 + a, 2^{s+2} + 2^s - 1 + b, 2^s - 1, 2)$$
$$= L + \alpha_{s+2}(a)\underbrace{(2^s - 1 + a - 2^{s+2}, 2^{s+3} + 2^s - 1 + b, 2^s - 1, 2)}_{M}$$
$$+ \{\text{a term, which is } s\text{-killed by Lemma 7.9}\}.$$

$$Sq^{2^{s+3}}(2^s - 1 + a - 2^{s+1}, 2^{s+3} - 2^{s+1} + 2^s - 1 + b, 2^s - 1, 2)$$
$$= M + \underbrace{(2^s - 1 + a - 2^{s+1}, 2^{s+1} + 2^s - 1 + b, 2^{s+2} + 2^s - 1, 2)}_{N}.$$

$$Sq^{2^{s+2}}(a - 1, 2^{s+1} - 1 + b, 2^{s+2} + 2^s - 1, 2)$$
$$= N + (a - 1, 2^{s+1} - 1 + b, 2^s - 1, 2 + 2^{s+2}).$$

The last term is s-killed by Lemma 5.4.

(b) If $\alpha_{s+2}(b) = 1$, K can be handled as follows:

$$Sq^{2^{s+3}}(2^{s+2} - 1 + a, 2^s - 1 + b - 2^{s+1}, 2^{s+2} + 2^s - 1 + c, 2)$$
$$= K + \underbrace{(2^{s+2} + \boxed{2^s} - 1 + a, 2^s - 1 + b - 2^{s+1}, 2^{s+2} + 2^s - 1 + c, 2)}_{P}$$
$$+ \alpha_{s+3}(c)(2^{s+2} - 1 + a, 2^s - 1 + b - 2^{s+1},$$
$$2^{s+2} + 2^s - 1 + c - 2^{s+3}, 2 + 2^{s+3}).$$

The last term is s-killed by Lemma 5.4.

Since $\alpha_{s+2}(b - 2^{s+1}) = 0$, so we get

$$Sq^{2^{s+3}}(2^{s+2} + 2^s - 1 + a, 2^{s+1} + 2^s - 1 + b, 2^s - 1 + c, 2)$$
$$= P + \alpha_{s+3}(c)(2^{s+2} + 2^s - 1 + a, 2^{s+1} + 2^s - 1 + b,$$
$$2^s - 1 + c - 2^{s+3}, 2 + 2^{s+3}).$$

This term is s-killed by Lemma 5.4.

Note: The last equality is based on the fact that

$$\alpha_{s+1}(2^{s+2} + 2^s - 1 + a) = 0 = \alpha_s(h(Q)),$$

where

$$Q = (2^{s+2} + 2^s - 1 + a, 2^{s+1} + 2^s - 1 + b, 2^s - 1 + c, 2).$$

(2) $J = (2^t - 1 + a, 2^{s+1} - 1 + b, 2^{s+1} - 1 + c, 2 + 2^{s+1})$, with $a \equiv 0 \bmod 2^{t+1}$ and $b \equiv c \equiv 0 \bmod 2^{s+2}$, $t > s+1$.

$$Sq^{2^{s+1}}(2^t - 1 + a, 2^{s+1} - 1 + b, 2^{s+2} - 1 + c, 2)$$
$$= J + (\underbrace{2^t - 1 + a, 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2}_{K}).$$

Note that $s(h(K)) = s + 1$. So

$$Sq^{2^{s+4}}(2^t - 2^{s+1} - 1 + a, 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2)$$
$$= K + (\underbrace{2^t - 2^{s+2} - 2^{s+1} - 1 + a, 2^{s+2} + 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2}_{L_1})$$
$$+ \alpha_{s+3}(b)(\underbrace{2^t - 2^{s+1} - 1 + a, 2^s - 1 + b - 2^{s+3}, 2^{s+3} + 2^{s+2} + 2^s - 1 + c, 2}_{L_2})$$
$$+ \alpha_{s+4}(c)(2^t - 2^{s+1} - 1 + a, 2^s - 1 + b,$$
$$2^{s+2} + 2^s - 1 + c - 2^{s+4}, 2 + 2^{s+4}).$$

The last term is s-killed by Lemma 5.4.

(a) If $\alpha_{s+2}(b) = 0$, *first we kill* L_1:

$$Sq^{2^{s+3}}(2^t - 2^{s+2} - 1 + a, 2^{s+1} + 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2)$$
$$= L_1 + (\underbrace{2^t - 2^{s+2} + \boxed{2^s} - 1 + a, 2^{s+1} + 2^s - 1 + b, 2^{s+2} + 2^s - 1 + c, 2}_{M_1})$$
$$+ \alpha_{s+3}(c)(2^t - 2^{s+2} - 1 + a, 2^{s+1} + 2^s - 1 + b,$$
$$2^{s+2} + 2^s - 1 + c - 2^{s+3}, 2 + 2^{s+3}).$$

The last term is s-killed by Lemma 5.4.

$$Sq^{2^{s+2}}(2^t - 2^{s+2} + 2^{s+1} - 1 + a, 2^{s+1} - 1 + b, 2^{s+2} + 2^s - 1 + c, 2)$$
$$= M_1 + \alpha_{s+2}(c + 2^{s+2})(2^t - 2^{s+2} + 2^{s+1} - 1 + a,$$
$$2^{s+1} - 1 + b, 2^s - 1 + c, 2 + 2^{s+2}).$$

Again, the last term is s-killed by Lemma 5.4.

Now we kill L_2:

$$Sq^{2^{s+3}}(2^t - 2^{s+1} - 1 + a, 2^s - 1 + b - 2^{s+2}, 2^{s+3} + 2^s - 1 + c, 2)$$
$$= L_2 + (2^t - 2^{s+1} + \boxed{2^s} - 1 + a, 2^s - 1 + b - 2^{s+2},$$
$$2^{s+3} + 2^s - 1 + c, 2)$$
$$+ (2^t - 2^{s+1} - 1 + a, 2^s - 1 + b - 2^{s+2},$$
$$2^s - 1 + c, 2 + 2^{s+3}).$$

The last two terms are s-killed by Lemma 7.9 and Lemma 5.4, respectively.

(b) If $\alpha_{s+2}(b)=1$, *we kill* L_1 :

$$Sq^{2^{s+3}}(2^t-2^{s+2}-2^{s+1}-1+a,\,2^{s+3}+2^s-1+b,\,2^s-1+c,\,2)$$
$$=L_1+\underbrace{(2^t-2^{s+2}-2^{s+1}+\boxed{2^s}-1+a,\,2^{s+3}+2^s-1+b,\,2^s-1+c,\,2)}_{M_1}$$
$$+\alpha_{s+3}(c)(2^t-2^{s+2}-2^{s+1}-1+a,\,2^{s+3}+2^s-1+b,$$
$$2^s-1+c-2^{s+3},\,2+2^{s+3}).$$

The last term is s–killed by Lemma 5.4.

$$Sq^{2^{s+3}}(2^t-2^{s+2}+2^s-1+a,\,2^{s+3}+2^s-1+b-2^{s+1},\,2^s-1+c,\,2)$$
$$=M_1+\alpha_{s+3}(c)(2^t-2^{s+2}-2^s-1+a,\,2^{s+3}+2^s-1+b-2^{s+1},$$
$$2^s-1+c-2^{s+3},\,2+2^{s+3}).$$

The last term is also s–killed by Lemma 5.4. Note that the last equality is based on the fact that

$$\alpha_s(h(M_1))=0=\alpha_{s+2}(b-2^{s+1}).$$

We kill L_2 :

$$Sq^{2^{s+3}}(2^t-1+a,\,2^s-1+b-2^{s+3}-2^{s+1},\,2^{s+3}+2^{s+2}+2^s-1+c,\,2)$$
$$=L_2+\underbrace{(2^t+\boxed{2^s}-1+a,\,2^s-1+b-2^{s+3}-2^{s+1},\,2^{s+3}+2^{s+2}+2^s-1+c,\,2)}_{M_2}$$
$$+\alpha_{s+3}(c+2^{s+3})(2^t-1+a,\,2^s-1+b-2^{s+3}-2^{s+1},$$
$$2^{s+2}+2^s-1+c,\,2+2^{s+3}).$$

The last term is s–killed by Lemma 5.4.

$$Sq^{2^{s+3}}(2^t+2^s-1+a,\,2^s-1+b-2^{s+2}-2^{s+1},\,2^{s+3}+2^s-1+c,\,2)$$
$$=M_2+(2^t-2^{s+1}+2^s-1+a,\,2^s-1+b-2^{s+2},$$
$$2^{s+3}+2^s-1+c,\,2)$$
$$+\alpha_{s+3}(c+2^{s+3})(2^t+2^s-1+a,\,2^s-1+b-2^{s+2}-2^{s+1},$$
$$2^s-1+c,\,2+2^{s+3}).$$

The last two terms are s–killed by Lemma 7.9 and Lemma 5.4, respectively.

Lemma 5.7 is completely proved.

8. Proofs of Lemma 5.8 and Lemma 5.9

Lemma 8.1. *Suppose* I *satisfies the hypothesis of Lemma* 5.8. *That means* $s(h)\geq s(i_3)$, $i_3\rhd i_2\rhd i_1\rhd i_0$, $h\not\rhd i_3$ *and* $h\not\trianglerighteq i_3$. *Then*

(a) *either* $i_0=i_1=i_2=0$, $m(I)=0$, $i_3>2^{s(i_3)}$,

(b) *or* $i_0=0$, $i_1=1$, $i_2=2^s-1$, $s(i_3)=s=m(I)$,

(c) *or* $i_0=2$, $i_1=2^s-1$, $i_2=2^{s'}-2^s-1(s'>s+1)$, $s(i_3)=s'$, $m(I)=s$,

(d) *or* $i_0=2$, $i_1=2^s-1=i_2$, $s(i_3)=$ *either* s *or* $s+1$, $m(I)=s$.

Proof. Using the same argument as in the proof of Lemma 4.5, one gets $i_0 = [2 : 2^{s(i_1)}] = 0$ or 2.

(a) If $i_0 = 0$, consider the reduced sequence (i_3, i_2, i_1) and we get $i_1 = 0$ or 1. A possibility is $i_0 = i_1 = i_2 = 0$. The fact that $i_3 > 2^{s(i_3)}$ follows from the hypothesis $h \not\rhd i_3$.

If $i_0 = i_1 = 0$, $i_2 > 0$, then i_3 and h are odd since $h \rhd i_3 \rhd i_2$. Hence i_2 is even, and $s(i_2 - 1) \geq s(i_3)$. So $i_2 \geq 2^{s(i_3)}$. This contradicts $i_3 \rhd i_2$.

(b) If $i_0 = 0$, $i_1 = 1$, since $s(h) \geq s(i_3)$ so $s(i_2) = s(i_2 + i_1 + i_0 - 1) \geq s(i_3)$. Then $s(i_2) = s(i_3) = s$ (say). From $i_3 \rhd i_2$ we have $i_2 = 2^s - 1$.

(c) If $i_0 = 2$, set $s = s(i_1) > 1$. By $s(h) \geq s(i_3) \geq s(i_2)$ we get $s(i_1 + i_0 - 2) = s(i_1) \geq s(i_2) \geq s(i_1)$, thus $s(i_2) = s(i_1) = s$. This together with $i_2 \rhd i_1$ implies $i_1 = 2^s - 1$.

Set $s' = s'(i_2)$, $i_2 \equiv 2^{s'} - 2^s - 1 \bmod 2^{s'+1}$. Because $s(h) \geq s(i_3)$, we have

$$s(i_2 + i_1 + i_0 - 1) = s(2^{s'} - 1 \bmod 2^{s'+1}) = s' \geq s(i_3) \geq s(i_2).$$

If $s' > s + 1$, then the fact $s(h) \geq s(i_3)$ implies $s(i_3) = s'$. So $i_2 = 2^{s'} - 2^s - 1$ as $i_3 \rhd i_2$.

(d) Finally, if $i_0 = 2$, $i_1 = 2^s - 1$, $i_2 \equiv 2^{s'} - 2^s - 1 \bmod 2^{s'+1}$, and $s' = s + 1$, then $s(i_3)$ could be one of the two possible values s and $s + 1$. In the both cases, we have $i_2 = 2^s - 1$ because of $i_3 \rhd i_2$. The lemma is proved.

According to Lemma 8.1, we now prove Lemma 5.8 by showing Lemmas 8.2, 8.3, 8.4 and 8.5 below.

Lemma 8.2. *Suppose I belongs to case* (a) *of Lemma* 8.1, *that means $i_0 = i_1 = i_2 = 0$, $h \not\rhd i_3$ or equivalently $i_3 > 2^{s(i_3)}$. Then I is absolutely killed, that means $Q^I \in \operatorname{Im}\bar{\mathscr{A}}$.*

Since $m(I) = 0$, the lemma is a special case of Lemma 5.10.

Lemma 8.3. *Suppose I belongs to case* (b) *of Lemma* 8.1, *that means $i_0 = 0$, $i_1 = 1$, $i_2 = 2^s - 1$, $s(i_3) = s = m(I)$, $h \not\rhd i_3$. Then (the weak form of) the main lemma holds for I.*

Proof. Let $s(h) = r > s$. We kill I by the usual method:

$$Sq^{2^{r+3}}(i_3 - 2^r, 2^s - 1, 1, 0) = I + \sum_J J.$$

We use the notations similar as given in the proof of Lemma 7.7 with a_i, b_i, c_i being respectively the coefficients of 2^i in the dyadic expansions of $i_3 - 2^r$, i_2, i_1.

By dimensional information, $h(J) < h(I)$ for all the J's. So it suffices to show $m(J) \leq m(I)$ for any J. Suppose the contrary that $m(J) > m(I) = s$. Then $s(j_2) > s$. In particular, $\alpha_s(j_2) = 1$ meanwhile $\alpha_s(i_2) = 0$. Since $\alpha_s(i_3 - 2^r) = 0$, $i_2 = 2^s - 1$, $i_1 = 1$, $i_0 = 0$, the only way to fulfil the gap at 2^s of i_2 (in order to make j_2) is

$$l_0 = \cdots = l_s = m_0 = 12 = |Q_2|.$$

Under this circumstance, $s(j_3) \leq s(i_3 - 2^r) = s$. Thus $m(J) \leq s$. This is a contradiction. The lemma is proved.

Lemma 8.4. *Suppose I belongs to case* (c) *of Lemma* 8.1, *that means* $i_0 = 2, i_1 = 2^s - 1, i_2 = 2^{s'} - 2^s - 1 \ (s' > s+1), s(i_3) = s', h \not\rhd i_3$. *Then* (*the weak form of*) *the main lemma holds for* I.

Remark. Looking at the list of the allowed sequences for $k = 4$, we note that if $i_0 = 2, i_1 = 2^s - 1, i_2 = 2^{s'} - 2^s - 1 \ (s' > s+1), s(i_3) = s'$, then one does not have $h \rhd\!\!\rhd i_3$.

Proof. Let $r = s(h) \geq s(i_3) = s'$, then $i_3 = 2^r - 2^{s'} - 1 + x$, with $x \neq 0$ but $x \equiv 0 \bmod 2^{r+1}$. We kill I by the usual method

$$Sq^{2^{r+3}}(i_3 - 2^r, 2^{s'} - 2^s - 1, 2^s - 1, 2) = I + \sum_J J.$$

By dimensional information, $h(J) < h(I)$ for all the J's. We need only to check that $m(J) \leq m(I)$ for any J. Suppose the contrary that there is a J with $m(J) > m(I) = s$.

Let us use the notations given in the proof of Lemma 9.7. In order to get J with $m(J) > s$, one has to fulfil the two gaps of i_2 and i_1 at 2^s. There are exactly three ways to do that:

(1) $\alpha_s(h_1) = \alpha_s(h_2) = 1$,
(2) $\alpha_s(t_{31}) = 1, \alpha_s(h_2) = \alpha_s(h_3) = 1$,
(3) $\alpha_s(t_{32}) = 1, \alpha_s(h_1) = \alpha_s(h_3) = 1$.

Similarly as in the end of the proof of Lemma 9.7, one can see that the corresponding coefficients are 0. The lemma follows.

Lemma 8.5. *Suppose I belongs to case* (d) *of Lemma* 8.1. *That means* $i_0 = 2, i_1 = 2^s - 1 = i_2, s(i_3) =$ *either* s *or* $s+1, h \not\rhd i_3$. *Then* (*the weak form of*) *the main lemma holds for* I.

Proof. If $s(i_3) = s+1$, case (d) of Lemma 8.1 can be considered as a special case of case (c) with $s' = s'(i_2) = s+1$. Actually, we did not use the hypothesis $s' > s+1$ in the proof of Lemma 8.4. That proof still works for this lemma in the both cases $s(i_3) =$ either s or $s+1$.

Comment. Suppose $r > s+2$. The sequence $I = (2^r - 2^{s+1} - 2^s - 1, 2^s - 1, 2^s - 1, 2)$ with $h \rhd\!\!\rhd i_3 \rhd i_2 \rhd i_1 \rhd i_0$ is also controlled by Lemma 8.5. However, $I = I' := (2^r - 2^{s+2} - 2^{s+1} - 1, 2^{s+1} + 2^s - 1, 2^s - 1, 2) \bmod \operatorname{Im}\bar{\mathscr{A}} + \operatorname{Span}\{J | m(J) < s\}$, with $m(I) = m(I') = s, h(I) > h(I')$. Note that I' belongs to case (d) of Lemma 7.1 and satisfies only the exceptional form of the main lemma. Lemma 9.6 will show that $I = I'$ in $\mathbf{Z}/2 \otimes_{\mathscr{A}} D_4$ is an $\mathscr{A}$-generator for D_4.

Finally, we have

Proof of Lemma 5.9. Let $s = s(h)$. We kill $Q(I)$ by the usual method:

$$Sq^{2^{s+3}}(i_3 - 2^s, i_2, i_1, i_0) = I + \sum_J J.$$

Obviously, $h(J) < h(I)$ for every J in the sum. So it suffices to show that $m(J) \leq m(I)$ for any J. Consider the two possibilities.

Case 1: $m(I) \geq s$. By the definition of $m(I)$,

$$m(I) = s = \min\{s(h), s(i_3), s(i_2), s(i_1 + i_0 - 2)\}.$$

Let a_i, b_i, c_i, d_i be the coefficients of 2^i in the 2-adic expansions of $i_3 - 2^s, i_2, i_1, i_0$ respectively. We have

$$\begin{aligned} Sq^{2^{s+3}}(i_3 - 2^s, i_2, i_1, i_0) \;=\; & \sum (Sq^{k_0}Q_3)^{a_0} \cdots (Sq^{k_\alpha}Q_3)^{2^\alpha a_\alpha} \\ & \cdot (Sq^{l_0}Q_2)^{b_0} \cdots (Sq^{l_\beta}Q_2)^{2^\beta b_\beta} \\ & \cdot (Sq^{m_0}Q_1)^{c_0} \cdots (Sq^{m_\gamma}Q_1)^{2^\gamma c_\gamma} \\ & \cdot (Sq^{n_0}Q_0)^{d_0} \cdots (Sq^{n_\delta}Q_0)^{2^\delta d_\delta}. \end{aligned}$$

Let J be a term in the above sum $(J \neq I)$, so

$$j_3 = i_3 - 2^s - \sum_i a_i 2^i + y.$$

Here the sum runs over all i with $k_i = 4, 6$ or 7 and $0 \leq y < 2^s$ by dimensional information. Note that $a_s = \alpha_s(i_3 - 2^s) = 0$. Hence $m(J) \leq s(j_3) \leq s = m(I)$.

Case 2: $m := m(I) < s$. Since $s(h) < s(i_3)$, by Lemma 5.1,

$$s(h) = s(i_2 + i_1 + i_0 - 1).$$

Suppose $s(i_2) \neq s(i_1 + i_0 - 2)$ then $s(h) = \min\{s(i_2), s(i_1 + i_0 - 2)\} = m(I)$. This contradicts $m(I) < s$.

So $s(i_2) = s(i_1 + i_0 - 2) = m(I)$, as a consequence $s(h) = m + 1 = s$, where $m = m(I)$. We have $h(J) = h - 2^s + x$ $(0 \leq x < 2^s)$.

(a) If $x \not\equiv 0 \bmod 2^{m+1}$, then $m(J) \leq s(h(J)) \leq m = m(I)$.

(b) Suppose $x \equiv 0 \bmod 2^{m+1}$.

(So $x = 0$. Otherwise $x \geq 2^{m+1} = 2^s$. However, we do not use this fact below.)

If $\alpha_m(j_2) = 0$, then $m(J) \leq s(j_2) \leq m = m(I)$.

Otherwise, $\alpha_m(j_2) = 1$. Combining this with the facts $s(i_2) = m, x \equiv 0 \bmod 2^{m+1}$, we see that 2^m is moved from $i_3 - 2^s$ to j_2. That means $k_m = 4, \alpha_m(j_3) = 0$. Therefore $m(J) \leq s(j_3) \leq m = m(I)$. The lemma is proved.

9. The linear independence of the allowed monomials

The purpose of this section is to show the linear independence of the allowed monomials in $\bar{D}_k = \mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for $k = 3$ or 4.

Definition 9.1. Suppose a is a non-negative integer. Set

$$\ell(a) = \begin{cases} \min\{i | \alpha_i(a) \neq 0\} & \text{for } a > 0, \\ +\infty & \text{for } a = 0. \end{cases}$$

Proposition 9.2. *Let $k = 3$. Then the allowed monomials are linearly independent in $\bar{D}_3 = \mathbf{Z}/2 \otimes_{\mathscr{A}} D_3$.*

Proof. Suppose I, J are of length 3 with I allowed, and

$$Sq^{2^t}Q^J = c \cdot Q^I + \text{other terms}.$$

Then we will show that $c = 0$. The proposition follows.

We are going to describe theoretically the coefficient c. Let a_i, b_i, c_i be the coefficients of 2^i in the dyadic expansions of j_2, j_1, j_0 respectively. We have

$$\begin{aligned} Sq^{2^t}Q^J = \sum & (Sq^{k_0}Q_2)^{a_0}\cdots(Sq^{k_\alpha}Q_2)^{2^\alpha a_\alpha} \\ & \cdot(Sq^{l_0}Q_1)^{b_0}\cdots(Sq^{l_\beta}Q_1)^{2^\beta b_\beta} \\ & \cdot(Sq^{m_0}Q_0)^{c_0}\cdots(Sq^{m_\gamma}Q_0)^{2^\gamma c_\gamma}. \end{aligned}$$

Here the sum runs over all the decompositions

$$2^t = \sum_i k_i 2^i + \sum_i l_i 2^i + \sum_i m_i 2^i,$$

with $k_i = 0$ if $a_i = 0$, $l_i = 0$ if $b_i = 0$ and $m_i = 0$ if $c_i = 0$.

Pick up a term Q^I in the sum. Define for this term:

t_{ij} to be the number of Q_i, which is sent to Q_j $(i > j)$,

d^l_{ij} to be the number of Q_l, which is sent to Q_iQ_j $(i > l > j)$,

h_i to be the number of Q_j, which is sent to Q_iQ_j for any $j < i$.

Obviously one gets

$$(\sigma)\begin{cases} i_2 = j_2 + h_2 + d^1_{20} - t_{21} - t_{20} \\ i_1 = j_1 + h_1 - d^1_{20} + t_{21} - t_{10} \\ i_0 = j_0 + h_0 + d^1_{20} + t_{20} + t_{10}, \end{cases}$$

where all the variables are non-negative integers. They satisfy the Dimensional Equation:

$$\text{(DE)} \qquad 2^t = 4h_2 + 6h_1 + 7h_0 + 5d^1_{20} + 2t_{21} + 3t_{20} + t_{10}.$$

By an easy argument of combination, the coefficient c is determined by $c = \sum_\sigma c(\sigma)$, where

$$\begin{aligned} c(\sigma) = & \binom{j_0}{h_0}\binom{j_1}{t_{10}}\binom{j_1 - t_{10}}{d^1_{20}}\binom{j_0 + j_1 - h_0 - t_{10} - d^1_{20}}{h_1}\binom{j_2}{t_{20}} \\ & \cdot\binom{j_2 - t_{20}}{t_{21}}\binom{j_0 + j_1 + j_2 - h_0 - t_{10} - d^1_{20} - h_1 - t_{20} - t_{21}}{h_2}. \end{aligned}$$

Here the sum runs over all the partitions (σ) satisfying (DE).

The list of the allowed sequences is given just after Theorem 2.6. According to this, as I is allowed, $i_0 = 0$ or 1. By Corollary 3.2, $j_0 \le i_0$. So we need only to consider the three cases.

Case 1: $i_1 = i_0 = 0$. By Corollary 3.2, from $i_0 = 0$ it implies $j_0 = 0$ and $h_0 = d^1_{20} = t_{20} = t_{10} = 0$. Also by the corollary, $j_1 + j_0 \le i_1 + i_0 = 0$, hence $j_1 = 0$, $h_1 = t_{21} = 0$. We get $i_2 = j_2 + h_2 = 2^s - 1$. Then

$$c(\sigma) = \binom{j_0 + j_1 + j_2}{h_2} = \binom{i_2 - h_2}{h_2} = \binom{2^s - 1 - h_2}{h_2} = 0,$$

as $h_2 \neq 0$ (otherwise, $I = J$, $2^t = 0$, a contradiction).

Case 2: $i_0 = 1$, $j_0 = 0$. Note that Q_0 is the only invariant among Q_2, Q_1, Q_0, which is of odd dimension. So $2^t \equiv 1 \bmod 2$. That means $2^t = 1$. Also by dimensional information, the only solution J in this case is $J = (i_2, i_1 + 1, i_0 - 1)$. We have

$$Sq^1 Q^{(i_2, i_1+1, i_0-1)} = \binom{i_1+1}{1} Q^I = \binom{2^s}{1} Q^I = 0,$$

because of $2^s > 1$ as $i_1 = 2^s - 1 \rhd i_0 = 1$.

Case 3: $i_0 = 1$, $j_0 = 1$. Obviously $h_0 = d_{20}^1 = t_{20} = t_{10} = 0$, $j_1 = i_1 - h_1 - t_{21}$, $j_2 = i_2 - h_2 + t_{21}$.

$$\begin{aligned} c(\sigma) &= \binom{j_0+j_1}{h_1}\binom{j_2}{t_{21}}\binom{j_0+j_1+j_2-h_1-t_{21}}{h_2} \\ &= \binom{2^s-h_1-t_{21}}{h_1}\binom{2^r-2^s-1-h_2+t_{21}}{t_{21}}\binom{2^r-1-2h_1-h_2-t_{21}}{h_2}. \end{aligned}$$

Now (DE) becomes $2^t = 4h_2 + 6h_1 + 2t_{21}$. Suppose the contrary that $c(\sigma) \neq 0$. Since $\binom{2^s-h_1-t_{21}}{h_1} \neq 0$, then either $h_1 = 0$ or $\ell(h_1) \neq \ell(t_{21})$. This together with (DE) shows either $h_2 = 0$, or $\ell(h_2) < \min\{\ell(h_1), \ell(t_{21})\}$. If $h_2 \neq 0$ and $\ell(h_2) < \min\{\ell(h_1), \ell(t_{21})\}$, then $\binom{2^r-1-2h_1-h_2-t_{21}}{h_2} = 0$. Otherwise, if $h_2 = 0$, a necessary condition for $\binom{2^r-2^s-1-h_2+t_{21}}{t_{21}} \neq 0$ is either $t_{21} = 0$ or $t_{21} = 2^s$. However, the second possibility is cancelled as it contradicts the fact that $t_{21} \leq i_1 = 2^s - 1$. So $h_2 = t_{21} = 0$, and $2^t = 6h_1$. This is a contradiction.

The proposition is proved.

From now on, we deal with the length $k = 4$ only.

Proposition 9.3. *The allowed monomials are linearly independent in* $\bar{D}_k = \mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ *for* $k = 4$.

According to the list of the allowed sequences for $k = 4$ given just after Theorem 2.7, the proposition is proved by showing Lemmas 9.4 and 9.6 below.

Lemma 9.4. *Suppose* I *is strongly allowed with* $i_0 = 0$ *and*

$$Sq^{2^t} Q^J = c \cdot Q^I + \textit{other terms}.$$

Then $c = 0$.

Proof. From $i_0 = 0$ it implies $j_0 = 0$. Then $I = (I', 0)$, $J = (J', 0)$ with I', J' are of length 3. By dimensional information, 2^t is even. The lemma follows from the proof of Proposition 9.2 and the fact that $D_4/(Q_0) \cong D_3$ over the "halving" map of the Steenrod algebra, which sends Sq^{2i} to Sq^i and Sq^{2i+1} to 0.

Definition 9.5. Let M be an $\mathscr{A}$-module. Suppose

$$Sq^i(x) = a + \text{other terms},$$

for $x, a \in M$. Then we say a is *hit by* Sq^i.

Suppose given $r > s + 1 > 2$. Set

$$I_n = (2^r - 2^{s+n} - 2^{s+n-1} - 1, 2^{s+n} - 2^s - 1, 2^s - 1, 2),$$

for $1 \leq n < r - s$. Note that it is weakly allowed for $n = 1$, $r > s + 2$.

Lemma 9.6. (a) *If I is strongly allowed with $i_0 = 2$, then there is no way to hit I by any Steenrod square of positive dimension.*

(b) *There are exactly two ways to hit I_n for $1 < n < r - s - 1$, namely*

(i) $Sq^{2^{s+n+1}}(2^r - 2^{s+n} - 1, 2^{s+n-1} - 2^s - 1, 2^s - 1, 2) = I_{n-1} + I_n + \text{other terms}$,

(ii) $Sq^{2^{s+n+2}}(2^r - 2^{s+n-1} - 1, 2^{s+n} - 2^s - 1, 2^s - 1, 2) = I_n + I_{n+1} + \text{other terms}$.

There is exactly one way to hit I_n for $n = 1$ or $n = r - s - 1$. It is (ii) *for $n = 1$ and* (i) *for $n = r - s - 1$.*

In order to prove Lemma 9.6, we need

Lemma 9.7. *Suppose either I is allowed with $i_0 = 2$ or $I = I_n (1 \le n < r - s)$. If*

$$Sq^{2^t} Q^J = Q^I + \text{other terms},$$

then $j_0 = i_0 = 2$, $j_1 = i_1 = 2^s - 1$.

Now suppose that Lemma 9.7 has been proved. Then we show Lemma 9.6 as follows.

Proof of Lemma 9.6 (supposing Lemma 9.7 is proved).

We prove part (b) only. Part (a) can similarly be showed.

Suppose $I = I_n$ and $Sq^{2^t} Q^J = c \cdot Q^I + \text{other terms}$. If $c = 1$, then according to Lemma 9.7, $j_0 = i_0 = 2$, $j_1 = i_1 = 2^s - 1$. Define h_i, t_{ij}, d^l_{ij} as in the proof of Proposition 9.2 and have:

$$(\sigma)\begin{cases} i_3 = j_3 + h_3 + d^2_{31} + d^2_{30} + d^1_{30} - t_{32} - t_{31} - t_{30} \\ i_2 = j_2 + h_2 + d^1_{20} - d^2_{31} - d^2_{30} + t_{32} - t_{21} - t_{20} \\ i_1 = j_1 + h_1 + d^2_{31} - d^1_{30} - d^1_{20} + t_{31} + t_{21} - t_{10} \\ i_0 = j_0 + h_0 + d^1_{30} + d^1_{20} + d^2_{30} + t_{30} + t_{20} + t_{10}. \end{cases}$$

However, we do not need to use this equation system in the general form. In fact, when $j_0 = i_0 = 2$, $j_1 = i_1 = 2^s - 1$, we get $h_0 = h_1 = t_{10} = t_{20} = t_{21} = t_{30} = t_{31} = d^1_{20} = d^1_{30} = d^2_{30} = d^2_{31} = 0$, and $i_3 = j_3 + h_3 - t_{32}$, $i_2 = j_2 + h_2 + t_{32}$.

Now the Dimensional Equation becomes

$$(\text{DE}) \qquad 2^t = 12h_2 + 8h_3 + 4t_{32}.$$

We also have $c = \sum_\sigma c(\sigma)$, with

$$c(\sigma) = \binom{2 + i_1 + i_2 - h_2 - t_{32}}{h_2} \binom{i_3 - h_3 + t_{32}}{t_{32}} \cdot \binom{2 + i_1 + i_2 + i_3 - 2h_2 - h_3 - t_{32}}{h_3}.$$

As $c = 1$, there exists at least one σ with $c(\sigma) \neq 0$. Fix such a σ.

Since $\binom{2+i_1+i_2-h_2-t_{32}}{h_2} = \binom{2^{s+n}-h_2-t_{32}}{h_2} \neq 0$, so either $h_2 = 0$ or $\ell(h_2) \neq \ell(t_{32})$. Combine this with (DE) and get either $h_3 = 0$ or $\ell(h_3) < \min\{\ell(h_2), \ell(t_{32})\}$.

(1) Suppose $h_3 = 0$. Combining $\binom{i_3-h_3+t_{32}}{t_{32}} = \binom{2^r-2^{s+n}-2^{s+n-1}-1+t_{32}}{t_{32}} \neq 0$ with the fact that $t_{32} \le i_2 = 2^{s+n} - 2^s - 1$, we get either $t_{32} = 0$ or $t_{32} = 2^{s+n-1}$.

- If $t_{32} = 0$, then $h_3 = t_{32} = 0$, $2^t = 12h_2$. This is a contradiction.

• Suppose $t_{32} = 2^{s+n-1}$. Note that $\binom{2+i_1+i_2-h_2-t_{32}}{h_2} = \binom{2^{s+n}-h_2-2^{s+n-1}}{h_2} = \binom{2^{s+n-1}-h_2}{h_2} \neq 0$ implies $h_2 < t_{32} = 2^{s+n-1}$. Combining this with (DE) $2^t = 12h_2 + 4t_{32}$, we get $h_2 = 0$.

The solution $h_2 = h_3 = 0$, $t_{32} = 2^{s+n-1}$ gives rise to equation (i), provided $n > 1$.

(2) If $h_3 \neq 0$, then as showed before $\ell(h_3) < \min\{\ell(h_2), \ell(t_{32})\}$.

Combine this with $\binom{2+i_1+i_2+i_3-2h_2-h_3-t_{32}}{h_3} = \binom{2^r-2^{s+n-1}-1-2h_2-h_3-t_{32}}{h_3} \neq 0$ and get $\ell(h_3) = s + n - 1$.

If either $h_2 > 0$ or $t_{32} > 0$, then by using $\ell(h_3) < \min\{\ell(h_2), \ell(t_{32})\}$ one obtains $h_2 \geq 2^{s+n} > i_2$ or $t_{32} \geq 2^{s+n} > i_2$ respectively. They both are contradictions.

Thus $h_2 = t_{32} = 0$. Combining (DE) and $\ell(h_3) = s + n - 1$ one gets $h_3 = 2^{s+n-1}$. This solution gives rise to equation (ii), provided that $n < r - s - 1$. The lemma is proved.

Proof of Lemma 9.7.

Step 1: To prove $j_0 = i_0 = 2$.

We start with a very simple but useful observation that if I is as in the lemma, then $s(i_3) \geq s = s(i_2) = s(i_1) > 1$. Consider the two cases:

(1) $i_0 = 2$, $j_0 = 1$. Again, by dimensional information we get $2^t = \dim Q^I - \dim Q^J \equiv 1 \bmod 2$. That means, $2^t = 1, t = 0$. The unique solution is $J = (i_3, i_2, i_1 + 1, i_0 - 1)$. However,

$$Sq^1 Q^J = \binom{i_1+1}{1} Q^I = \binom{2^s}{1} Q^I = 0,$$

because of $2^s - 1 \rhd 2$ or equivalently $2^s > 3$. This is a contradiction.

(2) $i_0 = 2$, $j_0 = 0$. First, we claim that $\alpha_0(j_1) = \alpha_0(i_1) = 1$.

Suppose the contrary that $\alpha_0(j_1) = 0$. It implies $\alpha_0(t_{10}) = \alpha_0(d^1_{20}) = \alpha_0(d^1_{30}) = 0$. We observe $\alpha_0(h_1) = 0$ as $\alpha_0(j_0 + j_1) = \alpha_0(0 + 2) = 0$ or equivalently $\binom{j_0+j_1}{2^0} = 0$. We get

$$1 = \alpha_0(i_1) \equiv \underbrace{\alpha_0(j_1)}_{0} + \underbrace{\alpha_0(h_1)}_{0} + \alpha_0(d^2_{31}) + \alpha_0(t_{21}) + \alpha_0(t_{31}) \bmod 2.$$

If $\alpha_0(t_{21}) = 1$, then $\alpha_0(h_2) = 0$. The only way to hit the new gap of j_2 at 2^0 is $\alpha_0(j_3) = \alpha_0(t_{32}) = 1$. However, it makes $\alpha_0(i_3) = 0$. It contradicts the fact that $s(i_3) \geq s > 1$. Therefore, $\alpha_0(t_{21}) = 0$. Thus $\alpha_0(d^2_{31}) + \alpha_0(t_{31}) = 1$.

(a) If $\alpha_0(t_{31}) = 1$, then $\alpha_0(d^2_{31}) = \alpha_0(t_{21}) = 0$. The only way to hit the new gap of j_3 at 2^0 is $\alpha_0(j_2) = 1$, $\alpha_0(h_3) = 1$. Now we claim that $\alpha_1(j_1) = 0 \neq \alpha_1(i_1) = 1$. Otherwise, if $\alpha_1(j_1) = 1$, one easily gets

$$\begin{aligned}
\dim Q_0^{i_0} - \dim Q_0^{j_0} &\equiv 2(2^4 - 1) \equiv 2^5 - 2 \bmod 2^3, \\
\dim Q_1^{i_1} - \dim Q_1^{j_1} &\equiv 2^4 - 2 \bmod 2^3, \\
\dim Q_2^{i_2} - \dim Q_2^{j_2} &\equiv 0 \bmod 2^3, \\
\dim Q_3^{i_3} - \dim Q_3^{j_3} &\equiv 0 \bmod 2^3.
\end{aligned}$$

So $2^t = \dim Q^I - \dim Q^J \equiv 2^5 + 2^4 - 2^2 \bmod 2^3$. Hence $2^t = 2^2 = 4$. On the other hand, $2^t \geq 6\alpha_0(t_{31}) = 6$. This is a contradiction.

Now we have $\alpha_1(j_1) = 0$. It implies $\alpha_1(d^1_{20}) = \alpha_1(d^1_{30}) = \alpha_1(t_{10}) = 0$. Besides, since $j_0 = 0$, so $\alpha_1(h_0) = 0$. Then

$$1 = \alpha_1(i_0) - \alpha_1(j_0) = 0 + 0 + 0 + 0 + \alpha_1(t_{20}) + \alpha_1(t_{30}) + \alpha_1(d^2_{30}).$$

Hence, either $\alpha_1(t_{20}) = 1$ or $\alpha_1(t_{30}) = 1$ or $\alpha_1(d^2_{30}) = 1$.

- $\alpha_1(t_{20}) = 1$: The only way to hit the gap 2^1 of j_1 is $\alpha_1(j_3) = \alpha_1(t_{31}) = 1$. It makes a gap of i_3 at 2^1, a contradiction.
- $\alpha_1(t_{30}) = 1$: The only way to hit the gap 2^1 of j_1 is $\alpha_1(j_2) = \alpha_1(t_{21}) = 1$. It makes a gap of i_2 at 2^1, a contradiction.
- $\alpha_1(d^2_{30}) = 1$: The only ways to hit the gaps 2^1 of j_2 and j_1 are respectively $\alpha_1(t_{32}) = 1$, $\alpha_1(t_{31}) = 1$. However, each from these equalities damages the other, a contradiction.

(b) If $\alpha_0(d^2_{31}) = 1$, then $\alpha_0(t_{21}) = \alpha_0(t_{31}) = 0$. The only possibility to hit the new gap of j_2 at 2^0 is $\alpha_0(j_3) = \alpha_0(t_{32}) = 1$.

Again, we claim that $\alpha_1(j_1) = 0$. Essentially, we can repeat the argument in (a) to get a contradiction for this case.

We have just showed that $\alpha_0(j_1) = \alpha_0(i_1) = 1$. Combine this with $i_0 = 2$, $j_0 = 0$ and get $2^t = \dim Q^I - \dim Q^J \equiv 2 \bmod 4$. So $2^t = 2$. The unique solution is $J = (i_3, i_2, i_1 + 2, 0)$. However,

$$Sq^2 Q^J = \binom{i_1 + 2}{2} Q^I = \binom{2^s + 1}{2} Q^I = 0,$$

as $2^s - 1 \rhd 2$ or equivalently $2^s > 3$.

Step 2: To prove that $j_1 = i_1 = 2^s - 1$.

Suppose the contrary that $j_1 \neq i_1$, that means $j_1 < i_1$ (as $j_1 + j_0 \leq i_1 + i_0$ by Corollary 3.2 and $j_0 = i_0$). Set $a = s(j_1) < s$. (Indeed, if $a = s$, then $j_1 \geq 2^s - 1 = i_1$, hence $j_1 = i_1$.)

Now we claim that $s(j_2) \geq a$. Suppose the contrary $s(j_2) = u < a$. Let us compare $s(j_3)$ and $s(j_2)$.

If $s(j_3) < s(j_2)$, then the only way to hit the gap $2^{s(j_3)}$ of j_3 is to increase h_3 by $2^{s(j_3)}$. However, the coefficient should be a multiple of

$$\binom{2^{s(j_3)} - 1 + 2^{s(j_2)} - 1 + 2^{s(j_1)} - 1 + 2}{2^{s(j_3)}} = \binom{2^{s(j_3)} - 1 + 2^u + 2^a}{2^{s(j_3)}} = 0,$$

as $s(j_3) < u < a$, a contradiction.

If $s(j_3) = s(j_2) = u$, then the only way to hit the gaps 2^u of j_3 and j_2 is to increase h_2, h_3 both by 2^u. The coefficient should be a multiple of

$$\binom{2^u - 1 + 2^a - 1 + 2}{2^u}\binom{2^u - 1 + 2^u - 1 + 2^a - 1 + 2 - 2^u}{2^u} = \binom{2^u + 2^a}{2^u}\binom{2^u - 1 + 2^a}{2^u} = 0,$$

as $u < a$, a contradiction.

We have just showed that if $s(j_2) < s(j_1)$, then $s(j_3) > s(j_2)$. Recall that $s(i_3) \geq s = s(i_2) = s(i_1) > a$. Consider the differences of dimensions:

$$\begin{aligned} \dim Q_1^{i_1} - \dim Q_1^{j_1} &\equiv 2^{a+1} \bmod 2^{a+2}, \\ \dim Q_2^{i_2} - \dim Q_2^{j_2} &\equiv 2^{u+2} \bmod 2^{u+3}, \\ \dim Q_3^{i_3} - \dim Q_3^{j_3} &\equiv 0 \bmod 2^{u+3}. \end{aligned}$$

However, $2^t = \dim Q^I - \dim Q^J$, so $2^{u+2} = 2^{a+1}$, or equivalently $u = a - 1$.

(1) If $\alpha_{a+1}(j_1) = \alpha_{a+1}(i_1) = 1$, we show that $\alpha_a(j_2) \neq \alpha_a(i_2) = 1$. Otherwise, if $\alpha_a(j_2) = \alpha_a(i_2) = 1$, then

$$\begin{aligned} 2^t = \dim Q^I - \dim Q^J &\equiv 2^a(2^4 - 2) + 2^{a-1}(2^4 - 2^2) \bmod 2^{a+3} \\ &\equiv 2^{a+4} + 2^{a+2} \bmod 2^{a+3}. \end{aligned}$$

It implies $2^t = 2^{a+2}$. On the other hand $2^t > \dim Q_1^{i_1} - \dim Q_1^{j_1} \geq 2^a(2^4 - 2) > 2^{a+2}$. This is a contradiction.

Since $i_0 = j_0$, so $d_{20}^1 = d_{30}^2 = 0$, and $i_2 = j_2 + h_2 - d_{31}^2 + t_{32} - t_{21} - t_{20}$. At level 2^{a-1} we have $\alpha_{a-1}(d_{31}^2) = \alpha_{a-1}(t_{21}) = \alpha_{a-1}(t_{20}) = 0$, as $\alpha_{a-1}(j_2) = 0$. Hence $1 = \alpha_{a-1}(i_2) = \alpha_{a-1}(h_2) + \alpha_{a-1}(t_{32})$. There are two possibilities:

(A) $\alpha_{a-1}(h_2) = 0$, $\alpha_{a-1}(t_{32}) = 1$ it requires $\alpha_{a-1}(h_3) = 1$,

(B) $\alpha_{a-1}(h_2) = 1$, $\alpha_{a-1}(t_{32}) = 0$.

At level 2^a, there are three possibilities to hit the two gaps of j_1 and j_2:

(a) $\alpha_a(t_{32}) = 1$, $\alpha_a(h_1) = 1$, $\alpha_a(h_2) = 0$, $\alpha_a(h_3) = 1$,

(b) $\alpha_a(t_{31}) = 1$, $\alpha_a(h_1) = 0$, $\alpha_a(h_2) = 1$, $\alpha_a(h_3) = 1$,

(c) $\alpha_a(t_{31}) = 0$, $\alpha_a(t_{32}) = 0$, $\alpha_a(h_1) = 1$, $\alpha_a(h_2) = 1$.

($\alpha_a(j_3)$ is either 0 or 1.) Now we have to compute the coefficient c in the combined six cases: (Aa) (Ab) (Ac) (Ba) (Bb) (Bc). In each case, c is a multiple of the following number:

(Aa) $\binom{2^a-1+2}{2^a}\binom{2^{a-1}-1+2^{a-1}-1+2^a-1+2-2^a}{2^{a-1}+2^a} = \binom{2^a+1}{2^a}\binom{2^a-1}{2^{a-1}+2^a} = 0.$

(Ab) $\binom{2^{a-1}-1+2^a-1+2}{2^a}\binom{2^{a-1}-1+2^{a-1}-1+2^a-1+2-2^a}{2^{a-1}+2^a} = \binom{2^{a-1}+2^a}{2^a}\binom{2^a-1}{2^{a-1}+2^a} = 0.$

(Ac) $\binom{2^a-1+2}{2^a}\binom{2^{a-1}-1+2^a-1+2-2^a}{2^a} = \binom{2^a+1}{2^a}\binom{2^{a-1}}{2^a} = 0.$

(Ba) $\binom{2^a-1+2}{2^a}\binom{2^{a-1}-1+2^a-1+2-2^a}{2^{a-1}}\binom{2^{a-1}-1+2^a-1+2-2^a-2^{a-1}+j_3-2^a}{2^a} = \binom{j_3-2^a}{2^a} = 0,$

as $\alpha_a(j_3) = 1$.

(Bb) $\binom{2^a-1+2^{a-1}-1+2}{2^{a-1}+2^a}\binom{2^a-1+2^{a-1}-1+2-2^a-2^{a-1}+j_3-2^a}{2^a} = \binom{j_3-2^a}{2^a} = 0.$

(Bc) $\binom{2^a-1+2}{2^a}\binom{2^{a-1}-1+2^a-1+2-2^a}{2^{a-1}+2^a} = 0.$

(2) If $\alpha_{a+1}(j_1) = 0 \neq \alpha_{a+1}(i_1) = 1$, then similarly as in (1), by computing the difference of dimensions mod 2^{a+3}, one gets $\alpha_a(j_2) = \alpha_a(i_2) = 1$. Also by an argument similar to that in (1), one can see the coefficients of all the possibilities are 0.

In any case, the hypothesis $s(j_2) < s(j_1)$ leads to a contradiction. Therefore, if $s(j_1) = a < s$, then $s(j_2) \geq a$.

Next, we claim that $s(j_3) \geq a$. This can be showed by the same argument as in the proof that if $s(j_2) < s(j_1)$, then $s(j_3) > s(j_2)$.

By dimensional information $2^t = \dim Q^I - \dim Q^J \equiv 2^a(2^4 - 2) \bmod 2^{a+2} \equiv 2^{a+1} \bmod 2^{a+2}$. So $2^t = 2^{a+1}$. On the other hand, $2^t > \dim Q_1^{i_1} - \dim Q_1^{j_1} \geq 2^a(2^4 - 2)$. This contradiction finishes the proof of Lemma 9.7.

10. Final remarks

Conjecture on gaps 10.1. Suppose $Sq^r Q^J = Q^I +$ other terms. One gets
(a) $m(J) \geq m(I)$.
(b) If additionally

$$j_0 = i_0, \ldots, j_{n-1} = i_{n-1} \qquad (2 \leq n < k),$$

then

$$\min\{s(h(J)), s(j_{k-1}), \ldots, s(j_n)\} \geq \min\{s(h(I)), s(i_{k-1}), \ldots, s(i_n)\}.$$

Lemma 7.4 is a special case of this conjecture.

If the conjecture is true, then we can simplify the proofs of some lemmas, for instance, Lemmas 7.4, 9.6 and 9.7. Furthermore, it would allow us to show that the allowed monomials are linearly independent in $\bar{D}_k = \mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for any k.

In general, the allowed monomials do not generate $\bar{D}_k$ for $k > 4$.

Example 10.2. If $k = 12$, the sequence

$$I = (2^{s+4} - 1, 2^{s+1} + 2^s - 1, 2^{s+2} + 2^s - 1, 2^s - 1, \ldots, 2^s - 1, 10) \qquad (\text{with } s > 3)$$

is not allowed as $2^{s+1} + 2^s - 1 \not< 2^{s+2} + 2^s - 1$ and also $2^{s+1} + 2^s - 1 \not\geqslant 2^{s+2} + 2^s - 1$. However, a complicated computation shows that, I does not belong to the subspace spanned by the allowed sequences. It should be considered as a new generator.

Conjecture 10.3. The allowed monomials form a basis for $\bar{D}_k = \mathbf{Z}/2 \otimes_{\mathscr{A}} D_k$ for $k < 12$.

References

1. L. E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. **12** (1911), 75–98.
2. Huỳnh Mùi, *Modular invariant theory and cohomology algebras of symmetric groups*, J. Fac. Sci. Univ. Tokyo **22** (1975), 310–369.
3. ———, *Dickson invariants and Milnor basis of the Steenrod algebra*, Eger Internat. Colloq. Topology (1983), 345–355.
4. J. Lannes and S. Zarati, *Invariants de Hopf d'ordre supérieur eet suite spectrale d'Adams*, C. R. Acad. Sci. **296** (1983), 695–698.
5. ———, *Sur les foncteurs dérivés de la déstabilisation*, Math. Z. **194** (1987), 25–59.
6. I. Madsen, *On the action of the Dyer–Lashof algebra in* $H_*(G)$, Pacific J. Math. **60** (1975), 235–275.
7. I. Madsen and J. Milgram, *The classifying spaces for surgery and cobordism of manifolds*, Ann. of Math. Stud., no. 92, Princeton Univ. Press, Princeton, NJ, 1979.
8. Nguyễn H. V. Hu'ng, *The action of the Steenrod squares on the modular invariants of linear groups*, Proc. Amer. Math. Soc. **113** (1991), 1097–1104.
9. W. Singer, *The transfer in homological algebra*, Math. Z. **202**(1989), 493–523.

10. R. Wellington, *The unstable Adams spectral sequence for free iterated loop spaces*, Mem. Amer. Math. Soc. **258** (1982).

11. C. Wilkerson, *A primer on the Dickson invariants*, Contemp. Math., vol. 19, Amer. Math. Soc., Providence, RI, 1983, pp. 421–434.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HANOI, 90 NGUYỄN TRÃI STREET, HANOI, VIETNAM

Current address: Centre de Recerca Matemàtica, Institut d'Estudis Catalans, Apartat 50, E-08193 Bellaterra, Barcelona, Espana

E-mail address: hung@cadi.crm.es

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MASSACHUSETTS 01239

E-mail address: fpp@math.mit.edu