TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 353, Number 12, Pages 5029–5040
S 0002-9947(01)02705-2
Article electronically published on May 22, 2001

THE HIT PROBLEM FOR THE DICKSON ALGEBRA

NGUYỄN H. V. HƯNG AND TRẦN NGỌC NAM

Dedicated to Professor Franklin P. Peterson on the occasion of his 70th birthday

Abstract. Let the mod 2 Steenrod algebra, $\mathcal{A}$, and the general linear group, $GL(k,\mathbb{F}_2)$, act on $P_k := \mathbb{F}_2[x_1,...,x_k]$ with $|x_i| = 1$ in the usual manner. We prove the conjecture of the first-named author in *Spherical classes and the algebraic transfer*, (Trans. Amer. Math Soc. **349** (1997), 3893–3910) stating that every element of positive degree in the Dickson algebra $D_k := (P_k)^{GL(k,\mathbb{F}_2)}$ is $\mathcal{A}$-decomposable in P_k for arbitrary $k > 2$. This conjecture was shown to be equivalent to a weak algebraic version of the classical conjecture on spherical classes, which states that the only spherical classes in Q_0S^0 are the elements of Hopf invariant one and those of Kervaire invariant one.

1. Introduction

Let $P_k := \mathbb{F}_2[x_1, \dots, x_k]$ be the polynomial algebra over (the field of two elements) $\mathbb{F}_2$ in k variables, each of degree 1. The general linear group $GL_k := GL(k,\mathbb{F}_2)$ acts on P_k in the usual manner. Dickson proves in [1] that the ring of invariants, $D_k := (P_k)^{GL_k}$, is also a polynomial algebra $D_k \cong \mathbb{F}_2[Q_{k,k-1}, \dots, Q_{k,0}]$, where $Q_{k,s}$ denotes the Dickson invariant of degree $2^k - 2^s$. It can be defined by the inductive formula

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

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

$$V_k = \prod_{\lambda_j \in \mathbb{F}_2} (\lambda_1 x_1 + \cdots + \lambda_{k-1}x_{k-1} + x_k).$$

Let $\mathcal{A}$ be the mod 2 Steenrod algebra. The usual action of $\mathcal{A}$ on P_k commutes with that of GL_k. So D_k is an $\mathcal{A}$-module. One of the authors has been interested in the homomorphism

$$j_k : \mathbb{F}_2 \underset{\mathcal{A}}{\otimes} (P_k)^{GL_k} \to (\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k)^{GL_k},$$

which is induced by the identity map on P_k (see [3]). Observing that j_1 is an isomorphism and j_2 is a monomorphism, he sets up the following

Conjecture 1.1 (Nguyễn H. V. Hu'ng [3]). $j_k = 0$ in positive degrees for $k > 2$.

Let D_k^+ and $\mathcal{A}^+$ denote respectively the submodules of D_k and $\mathcal{A}$ consisting of all elements of positive degree. Then Conjecture 1.1 is equivalent to $D_k^+ \subset \mathcal{A}^+ \cdot P_k$

Received by the editors September 29, 1999 and, in revised form, February 22, 2000.
2000 *Mathematics Subject Classification.* Primary 55S10; Secondary 55P47, 55Q45, 55T15.
Key words and phrases. Steenrod algebra, invariant theory, Dickson algebra.
This work was supported in part by the National Research Project, No. 1.4.2.

for $k > 2$ (see [3]). In other words, it predicts that every GL_k-invariant element of positive degree is hit by the Steenrod algebra acting on P_k for $k > 2$.

Conjecture 1.1 is related to the *hit problem* of determination of $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k$. This problem has first been studied by F. Peterson [9], R. Wood [14], W. Singer [12], and S. Priddy [10], who show its relationships to several classical problems in cobordism theory, modular representation theory, Adams spectral sequence for the stable homotopy of spheres, and stable homotopy type of classifying spaces of finite groups. The tensor product $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k$ has explicitly been computed for $k \leq 3$. The cases $k = 1$ and 2 are not difficult, while the case $k = 3$ is complicated and was solved by M. Kameko [8]. It seems unlikely that a very explicit description of $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k$ for general k will appear in the near future. There is also another approach, the qualitative one, to the problem. By this we mean giving conditions on elements of P_k to show that they go to zero in $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k$, i.e. belong to $\mathcal{A}^+ \cdot P_k$. Peterson's conjecture, which was established by Wood [14], claims that $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} P_k = 0$ in degree d such that $\alpha(d + k) > k$. Here $\alpha(n)$ denotes the number of ones in the dyadic expansion of n. Recently, W. Singer, K. Monks, and J. Silverman have refined the method of R. Wood to show that many more monomials in P_k are in $\mathcal{A}^+ \cdot P_k$. (See Silverman [11] and its references.) *Conjecture 1.1 presents a large family, whose elements are predicted to be in* $\mathcal{A}^+ \cdot P_k$.

In [3], one of the authors proves the equivalence of Conjecture 1.1 and a weak algebraic version of the conjecture on spherical classes stating that: *There are no spherical classes in Q_0S^0 except the elements of Hopf invariant one and those of Kervaire invariant one.* He also gives two proofs of Conjecture 1.1 for the case $k = 3$. In this paper, we establish this conjecture for every $k > 2$. That Conjecture 1.1 is no longer valid for $k = 1$ and 2 is respectively an exposition of the existence of Hopf invariant one classes and Kervaire invariant one classes. We have

Main Theorem. *$D_k^+ \subset \mathcal{A}^+ \cdot P_k$ for $k > 2$.*

Recently, F. Peterson and R. Wood privately informed us that they had proved the theorem for $k = 4$ and probably for $k = 5$. The readers are referred to [4] and [5] for some problems, which are closely related to the main theorem. Additionally, the problem of determination of $\mathbb{F}_2 \underset{\mathcal{A}}{\otimes} D_k$ and its applications have been studied by Hu'ng and Peterson [6], [7].

The paper contains five sections. Section 2 is a preparation on the action of the Steenrod squares on the Dickson algebra. We prove the main theorem in Section 3 by means of two lemmata, which are later shown in Section 4 and Section 5 respectively.

2. Preliminaries

The action of the Steenrod squares on D_k is explicitly described as follows.

Theorem 2.1 ([2]).

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

From now on, we denote $Q_{k,s}$ by Q_s for brevity. We get

$$Sq^a(Q_s) = \begin{cases} Q_{s-1} & \text{if } a = 2^{s-1}, \\ 0 & \text{if } 0 < a < 2^{s-1} \text{ or } 2^s \le a < 2^{k-1} \end{cases}$$

for $0 \le s < k$. Combining this with the Cartan formula, one obtains

Corollary 2.2. (a) $Sq^a(Q_sR) = Q_sSq^a(R)$ *if* $0 < a < 2^{s-1}$,
(b) $Sq^a(Q_0R) = Q_0Sq^a(R)$ *if* $0 < a < 2^{k-1}$
for any polynomial $R \in P_k$.

Let $I_n\,(n \ge 0)$ be the right ideal of $\mathcal{A}$ generated by the operations Sq^{2^i} for $i = 0, \dots, n$.

Definition 2.3. Suppose $R_1, R_2 \in P_k$. Then we write $R_1 \equiv R_2 \pmod{I_n}$ if R_1+R_2 belongs to $I_n \cdot P_k$. By convention, $R_1 \equiv R_2 \pmod{I_n}$ means $R_1 = R_2$ for $n < 0$.

This is an equivalence relation.

Lemma 2.4. (a) $Sq^1(R_1)R_2 \equiv R_1Sq^1(R_2) \pmod{I_0}$,
(b) $Sq^2(R_1)R_2 \equiv R_1Sq^2(R_2) \pmod{I_1}$
for any polynomials $R_1, R_2 \in P_k$.

Proof. (a) From the Cartan formula $Sq^1(R_1)R_2+R_1Sq^1(R_2) = Sq^1(R_1R_2)$, we get (a) by Definition 2.3.

(b) We have

$$\begin{aligned} Sq^2(R_1R_2) &= Sq^2(R_1)R_2 + Sq^1(R_1)Sq^1(R_2) + R_1Sq^2(R_2) \\ &\quad \text{(by the Cartan formula)} \\ &\equiv Sq^2(R_1)R_2 + R_1Sq^1Sq^1(R_2) + R_1Sq^2(R_2) \pmod{I_0} \\ &\quad \text{(by Part (a))} \\ &\equiv Sq^2(R_1)R_2 + R_1Sq^2(R_2) \pmod{I_0} \\ &\quad \text{(since } Sq^1Sq^1 = 0). \end{aligned}$$

Hence, $Sq^2(R_1)R_2 + R_1Sq^2(R_2) \in I_1 \cdot P_k$ and (b) follows. ∎

Lemma 2.5. *Let* $R \in P_k$ $(k \ge 1)$. *If* $Sq^1(R) = 0$ *and all the monomials of* R *are of positive degree, then* $R \equiv 0 \pmod{I_0}$.

Proof. The lemma is proved by induction on k. For $k = 1$, it is easy to see that all the monomials of R are of even degree. Since $x_1^{2n} = Sq^1(x_1^{2n-1})$ for $n > 0$, the lemma is proved. Let $k > 1$ and suppose inductively that the lemma holds for polynomials in $k-1$ variables. Let us write

$$R = \sum_{0 \le i \le 2n} x_1^i R_i$$

for some positive integer n and some polynomials R_i $(0 \le i \le 2n)$ in $k-1$ variables $x_2, \dots, x_k$. We get

$$\begin{aligned} Sq^1(R) &= \sum_{0 \le i \le 2n} x_1^i Sq^1(R_i) + \sum_{\substack{0 \le i \le 2n \\ i \text{ odd}}} x_1^{i+1} R_i \\ &= Sq^1(R_0) + \sum_{\substack{0 \le i \le 2n \\ i \text{ odd}}} x_1^i Sq^1(R_i) \\ &\quad + \sum_{\substack{0 \le i \le 2n \\ i \text{ odd}}} x_1^{i+1}[Sq^1(R_{i+1}) + R_i]. \end{aligned}$$

Since $Sq^1(R) = 0$, we have $Sq^1(R_0) = 0$ and $Sq^1(R_{i+1}) = R_i$ for $0 \le i \le 2n$, i odd. Therefore,

$$\begin{aligned} R &= \sum_{\substack{0\le i\le 2n \\ i \text{ even}}} x_1^i R_i + \sum_{\substack{0\le i\le 2n \\ i \text{ odd}}} x_1^i Sq^1(R_{i+1}) \\ &= R_0 + \sum_{\substack{0\le i\le 2n \\ i \text{ odd}}} [x_1^{i+1} R_{i+1} + x_1^i Sq^1(R_{i+1})] \\ &= R_0 + Sq^1(\sum_{\substack{0\le i\le 2n \\ i \text{ odd}}} x_1^i R_{i+1}) \\ &\equiv R_0 \pmod{I_0} \\ &\equiv 0 \pmod{I_0} \qquad \text{(by the inductive hypothesis).} \end{aligned}$$

The lemma is proved. □

This lemma immediately implies that if all monomials of $R \in P_k$ are of positive degree, then $R^2 \equiv 0 \pmod{I_0}$.

Corollary 2.6. *Let $k > 1$ and suppose S is a non-empty subset of $\{0, \dots, k-1\}$ such that $1 \notin S$. Then*

$$QR^2 \equiv 0 \pmod{I_0},$$

where $Q = \prod_{s\in S} Q_s$ and R is an arbitrary polynomial in P_k.

Proof. As $k > 1$ and $1 \notin S$, one gets $Sq^1(Q) = 0$. This implies $Sq^1(QR^2) = 0$. Thus $QR^2 \equiv 0 \pmod{I_0}$ by Lemma 2.5. The corollary is proved. □

3. Proof of the Main Theorem

Let Q be a non-zero Dickson monomial. If $Q \neq 1$, it can be written as

$$Q = \prod_{0\le i\le n} A_i^{2^i},$$

where n is some non-negative integer and A_i is some Dickson monomial dividing $\prod_{0\le s<k} Q_s$ for $i = 0, \dots, n$ with $A_n \neq 1$.

Indeed, suppose $Q = \prod_{0\le s<k} Q_s^{\alpha_s}$. Since $Q \neq 1$, there exists at least one $\alpha_s \neq 0$. Consider the 2-adic expansions of all the non-zero α_s's:

$$\alpha_s = \sum_{0\le i\le n(s)} \alpha_{si} 2^i,$$

where $\alpha_{sn(s)} = 1$. Now denoting

$$\begin{aligned} n &:= \max_{\substack{\alpha_s\neq 0, \\ 0\le s<k}} n(s), \\ \alpha_{si} &:= 0 \text{ if } n(s) < i \le n \ (0 \le s < k), \\ A_i &:= \prod_{0\le s<k} Q_s^{\alpha_{si}} \ (0 \le i \le n), \end{aligned}$$

one can easily check that $Q = \prod_{0\le i\le n} A_i^{2^i}$ and each A_i divides $\prod_{0\le s<k} Q_s$. Moreover, there exists an integer r such that $0 \le r < k$, $\alpha_r \neq 0$ and $n = n(r)$. Then $A_n = \prod_{0\le s<k} Q_s^{\alpha_{sn}}$ is divisible by $Q_r^{\alpha_{rn}} = Q_r^{\alpha_{rn(r)}} = Q_r$, so $A_n \neq 1$.

Definition 3.1. (i) We call n the *height* of Q. The monomial $A_i^{2^i} = A_i(Q)^{2^i}$ is called the ith *cut* of Q. It is said to be *full* if A_i is divisible by $\prod_{0<s<k} Q_s$. The monomial Q is called *full* if its cuts are all full.

(ii) A Dickson monomial is called a *based cut* if it is the 0th cut of some $Q \neq 0$ and $\neq 1$.

The main theorem is proved at the end of this section by means of the following two lemmata, whose proofs will be given in the last two sections.

Lemma A. *Let $k > 2$ and suppose R is an arbitrary polynomial in P_k.*

(a) *If $Q = \prod_{0\le i\le n} A_i^{2^i} \neq 1$ and it is not full, then $QR^{2^{n+1}} \in \mathcal{A}^+ \cdot P_k$.*

(b) *If $Q = \prod_{0\le i\le n} A_i^{2^i}$ is full, then $QSq^{2^{m+n+1}}(R^{2^{n+1}}) \in \mathcal{A}^+ \cdot P_k$ for $0 \le m < k-1$.*

Lemma B. *Suppose $k > 2$. If A is a full based cut, then $A \equiv 0 \pmod{I_1}$.*

Proof of the Main Theorem. Suppose $Q = \prod_{0\le i\le n} A_i^{2^i}$ is a Dickson monomial with $A_n \neq 1$.

If Q is not full, then applying Lemma A(a) with $R = 1$, one gets $Q \in \mathcal{A}^+ \cdot P_k$.

If Q is full and $n = 0$, then Q is the full based cut of itself. So using Lemma B, one obtains $Q \equiv 0 \pmod{I_1}$. In particular, $Q \in \mathcal{A}^+ \cdot P_k$.

If Q is full and $n > 0$, then A_n is the full based cut of itself. By Lemma B, one has $A_n = Sq^1(R_1) + Sq^2(R_2)$, with some $R_1, R_2 \in P_k$. Noting that $Q' = \prod_{0\le i<n} A_i^{2^i}$ is also full with the height $n-1$, one can apply Lemma A(b) to it and get

$$\begin{aligned} Q'Sq^{2^n}(R_1^{2^n}) &= \prod_{0\le i<n} A_i^{2^i} Sq^{2^n}(R_1^{2^n}) \in \mathcal{A}^+ \cdot P_k, \\ Q'Sq^{2^{n+1}}(R_2^{2^n}) &= \prod_{0\le i<n} A_i^{2^i} Sq^{2^{n+1}}(R_2^{2^n}) \in \mathcal{A}^+ \cdot P_k. \end{aligned}$$

(It should be noted that $1 < k-1$.) Hence

$$Q = \prod_{0\le i<n} A_i^{2^i} \cdot A_n^{2^n} = \prod_{0\le i<n} A_i^{2^i} [Sq^{2^n}(R_1^{2^n}) + Sq^{2^{n+1}}(R_2^{2^n})] \in \mathcal{A}^+ \cdot P_k.$$

The proof is completed. □

4. Proof of Lemma A

In this section, we prove Lemma A by using Lemma 4.1 and Lemma 4.2.

Lemma 4.1. *Suppose k, m, j are integers satisfying $k > 2$, $0 \le m < k-1$ and $0 < j \le 2^m$. Let Q be a full Dickson monomial of height n and B any Dickson monomial of $Sq^{2^{n+1}j}(Q)$. Suppose $B = \prod_{0\le i\le p} B_i^{2^i}$, with $B_i^{2^i}$ the ith cut of B and $B_p \neq 1$. We have*

(a) *$p \ge n$,*

(b) *If* $B' = \prod_{0\le i\le n} B_i^{2^i} \neq 1$, *then it is not full.*

Proof. (a) Suppose to the contrary that $p < n$. We get

$$\begin{aligned}
\deg Q + 2^{n+1}j &= \deg(\prod_{0\le i\le p} B_i^{2^i}) \\
&\le (\sum_{0\le i\le p} 2^i) \deg(\prod_{0\le s<k} Q_s) \\
&\le (2^n - 1) \deg(\prod_{0\le s<k} Q_s)
\end{aligned}$$

and

$$\begin{aligned}
\deg Q + 2^{n+1}j &> \deg Q \\
&\ge (\sum_{0\le i\le n} 2^i) \deg(\prod_{0<s<k} Q_s) \qquad \text{(since } Q \text{ is full)} \\
&= (2^{n+1} - 1) \deg(\prod_{0<s<k} Q_s).
\end{aligned}$$

Therefore,

$$\begin{aligned}
(2^n - 1) \deg(\prod_{0\le s<k} Q_s) &> (2^{n+1} - 1) \deg(\prod_{0<s<k} Q_s), \\
(2^n - 1) \deg Q_0 &> 2^n \deg(\prod_{0<s<k} Q_s), \\
\deg Q_0 &> \deg(\prod_{0<s<k} Q_s).
\end{aligned}$$

The last inequality is false for every $k > 2$. This contradiction shows part (a).

(b) Suppose to the contrary that $\prod_{0\le i\le n} B_i^{2^i}$ is full. Then

$$\begin{aligned}
\deg Q + 2^{n+1}j &= \deg(\prod_{0\le i\le p} B_i^{2^i}) \\
&\equiv \deg(\prod_{0\le i\le n} B_i^{2^i}) \pmod{2^{n+1}}, \\
\deg Q - \deg(\prod_{0\le i\le n} B_i^{2^i}) &\equiv 0 \pmod{2^{n+1}}, \\
\sum_{0\le i\le n} 2^i(\deg A_i - \deg B_i) &\equiv 0 \pmod{2^{n+1}}.
\end{aligned}$$

It is easy to see that $\deg A_i - \deg B_i = \varepsilon_i \deg Q_0$, with $\varepsilon_i \in \{0, 1, -1\}$. Furthermore, if $\varepsilon_i = 0$, then $A_i = B_i$. So $\sum_{0\le i\le n} 2^i \varepsilon_i \deg Q_0 \equiv 0 \pmod{2^{n+1}}$. It should be noted that $\deg Q_0 = 2^k - 1$ has no common divisor with 2^{n+1}. So $\sum_{0\le i\le n} 2^i \varepsilon_i \equiv 0 \pmod{2^{n+1}}$. This implies $\varepsilon_i = 0$ for $i = 0, \dots, n$. In other words, $A_i = B_i$ for

$i = 0, \dots, n$ and $Q = \prod_{0 \le i \le n} B_i^{2^i}$. We have

$$\begin{aligned} \deg Q + 2^{n+1} j &= \deg(\prod_{0 \le i \le n} B_i^{2^i}) + \deg(\prod_{n < i \le p} B_i^{2^i}) \\ &= \deg Q + \deg(\prod_{n < i \le p} B_i^{2^i}), \\ 2^{n+1} j &= \deg(\prod_{n < i \le p} B_i^{2^i}) \ge \deg B_p^{2^p}. \end{aligned}$$

Since $j > 0$, we get $\deg B = \deg Q + 2^{n+1} j > \deg Q$, so $p > n$. Hence

$$\deg B_p^{2^p} \ge \deg B_p^{2^{n+1}} \ge \deg Q_{k-1}^{2^{n+1}} = 2^{n+1} \cdot 2^{k-1}.$$

It implies $j \ge 2^{k-1}$. Combining this and the fact $2^{k-1} > 2^m \ge j$, we obtain $j > j$. This contradiction comes from the hypothesis that B' is full. Therefore, the lemma is proved. $\square$

Lemma 4.2. *Let $A \ne 1$ be an unfull based cut. Denote by s the smallest integer $s \ge 1$ such that $Q_s \nmid A$. If $s > 1$, then there exists for every $R \in P_k$ an expansion*

$$AR^2 = Sq^{2^{s-1}}(R_1) + \sum BR_2^2,$$

where $R_1 \in P_k$, every $R_2 \in P_k$ and every B is a Dickson monomial with $B \mid \prod_{0 \le r < k} Q_r$, $B \ne 1$, $Q_{s-1} \nmid B$.

Proof. From the hypothesis we can write $A = \bar{A} \prod_{0 < r < s} Q_r$ with a certain Dickson monomial $\bar{A} \mid \prod_{s < r < k} Q_r Q_0$. By the Cartan formula

$$\begin{aligned} Sq^{2^{s-1}}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r R^2) &= Sq^{2^{s-1}}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) R^2 \\ &+ \sum_{0 \le j < 2^{s-2}} Sq^{2j}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) Sq^{2^{s-1}-2j}(R^2). \end{aligned}$$

Denoting $R_1 := \bar{A} Q_s \prod_{0 < r < s-1} Q_r R^2$, we get

$$\begin{aligned} Sq^{2^{s-1}}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) R^2 &= Sq^{2^{s-1}}(R_1) \\ &+ \sum_{0 \le j < 2^{s-2}} Sq^{2j}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) Sq^{2^{s-1}-2j}(R^2). \end{aligned}$$

We will prove that (a) $A = Sq^{2^{s-1}}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r)$ and that (b) every polynomial $Sq^{2j}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) Sq^{2^{s-1}-2j}(R^2)$ for $0 \le j < 2^{s-2}$ can be written in the form $\sum BR_2^2$, where B, R_2 satisfy the conclusions of Lemma 4.2. Thus, the required expansion will be obtained.

First we prove (a). By Corollary 2.2, we have

$$Sq^{2^{s-1}}(\bar{A} Q_s \prod_{0 < r < s-1} Q_r) = \bar{A} Sq^{2^{s-1}}(Q_s \prod_{0 < r < s-1} Q_r).$$

So it suffices to show that $Sq^{2^{s-1}}(Q_s \prod_{0<r<s-1} Q_r) = \prod_{0<r<s} Q_r$. By the Cartan formula

$$\begin{aligned}
Sq^{2^{s-1}}(Q_s \prod_{0<r<s-1} Q_r) &= Q_s Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) \\
&\quad + \sum_{0<a\leq 2^{s-1}} Sq^a(Q_s) Sq^{2^{s-1}-a}(\prod_{0<r<s-1} Q_r) \\
&= Q_s Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) + Q_{s-1} \prod_{0<r<s-1} Q_r \\
&\quad \text{(since } Sq^a(Q_s) = 0 \text{ for } 0 < a < 2^{s-1} \\
&\quad \text{and } Sq^{2^{s-1}}(Q_s) = Q_{s-1}) \\
&= Q_s Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) + \prod_{0<r<s} Q_r.
\end{aligned}$$

It is sufficient to prove $Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) = 0$. Note that, by the Cartan formula,

$$Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) = \sum \prod_{0<r<s-1} Sq^{a_r}(Q_r),$$

where the sum is taken over all $(a_r)_{0<r<s-1}$ satisfying $\sum_{0<r<s-1} a_r = 2^{s-1}$ and $a_r \geq 0$. It is easy to show that there exists an r such that $0 < r < s-1$ and $a_r > 2^r$. Since $a_r \leq 2^{s-1} < 2^{k-1}$, we have $2^r < a_r < 2^{k-1}$. So, by Theorem 2.1, $Sq^{a_r}(Q_r) = 0$. Hence $\prod_{0<r<s-1} Sq^{a_r}(Q_r) = 0$. This is true for every $(a_r)_{0<r<s-1}$, so $Sq^{2^{s-1}}(\prod_{0<r<s-1} Q_r) = 0$. Part (a) is shown.

Next we prove (b). From Corollary 2.2 and since $2j < 2^{s-1} < 2^{k-1}$ we have

$$Sq^{2j}(\bar{A}Q_s \prod_{0<r<s-1} Q_r) = \bar{A}Q_s Sq^{2j}(\prod_{0<r<s-1} Q_r).$$

By the Cartan formula we get

$$Sq^{2j}(\prod_{0<r<s-1} Q_r) = \sum \prod_{0<r<s-1} Sq^{j_r}(Q_r),$$

where the sum is taken over all sequences $(j_r)_{0<r<s-1}$ satisfying $\sum_{0<r<s-1} j_r = 2j$ and $j_r \geq 0$. From Theorem 2.1 and since $j_r \leq 2j < 2^{k-1}$ we have $Sq^{j_r}(Q_r) =$ either 0 or Q_t with $0 \leq t \leq r$. So $\prod_{0<r<s-1} Sq^{j_r}(Q_r)$ is not divisible by $Q_{s-1}, Q_s, \ldots, Q_{k-1}$. Therefore, the 0th cut of every Dickson monomial in $Sq^{2j}(\prod_{0<r<s-1} Q_r)$ is not divisible by $Q_{s-1}, Q_s, \ldots, Q_{k-1}$. Let us write $Sq^{2j}(\prod_{0<r<s-1} Q_r)$ as the sum of its Dickson monomials $Sq^{2j}(\prod_{0<r<s-1} Q_r) = \sum \prod_{0\leq i\leq p} C_i^{2^i}$, where $C_i^{2^i}$ is an ith cut. Then

$$\begin{aligned}
Sq^{2j}(\bar{A}Q_s \prod_{0<r<s-1} Q_r) &= \bar{A}Q_s Sq^{2j}(\prod_{0<r<s-1} Q_r) \\
&= \sum \bar{A}Q_s C_0 \prod_{0<i\leq p} C_i^{2^i}.
\end{aligned}$$

We have shown that C_0 is not divisible by $Q_{s-1}, Q_s, \dots, Q_{k-1}$. Note that $\deg Q_0$ is odd, while $\deg Q_r$ is even for every $r > 0$. Thus, the 0th cut C_0 of every term in $Sq^{2j}(\prod_{0<r<s-1} Q_r)$ is not divisible by Q_0. Recall that $\bar{A}$ is a divisor of $\prod_{s<r<k} Q_r Q_0$. So $\bar{A}Q_sC_0$ is not divisible by Q_{s-1}. Moreover, it is a Dickson monomial, which is different from 1 and divides $\prod_{0\le r<k} Q_r$.

Putting $B := \bar{A}Q_sC_0$ and $R_2 := \prod_{0<i\le p} C_i^{2^{i-1}} Sq^{2^{s-2}-j}(R)$ for each C_0, we get

$$\begin{aligned} Sq^{2j}(\bar{A}Q_s \prod_{0<r<s-1} Q_r)Sq^{2^{s-1}-2j}(R^2) &= \sum \bar{A}Q_sC_0 \prod_{0<i\le p} C_i^{2^i} Sq^{2^{s-1}-2j}(R^2) \\ &= \sum BR_2^2. \end{aligned}$$

It has been shown that $B = \bar{A}Q_sC_0$ satisfies the conclusions of Lemma 4.2. Hence, part (b) and therefore Lemma 4.2 is proved. $\square$

Proof of Lemma A. The proof is divided into 2 steps.

Step 1. *If Lemma* A(a) *is true for every* $n \le N$*, then so is Lemma* A(b) *for every* $n \le N$.

Indeed, suppose $Q = \prod_{0\le i\le n} A_i^{2^i}$ (with $n \le N$) is full and m satisfies $0 \le m < k-1$. One needs to prove $QSq^{2^{m+n+1}}(R^{2^{n+1}}) \in \mathcal{A}^+ \cdot P_k$, where $R \in P_k$. Recall that

$$Sq^a(R^{2^n}) = \begin{cases} [Sq^{a/2^n}(R)]^{2^n} & \text{if } 2^n \mid a, \\ 0 & \text{otherwise.} \end{cases}$$

Then, by the Cartan formula, one gets

$$\begin{aligned} Sq^{2^{m+n+1}}(QR^{2^{n+1}}) &= \sum_{0\le j\le 2^m} Sq^{2^{n+1}j}(Q)Sq^{2^{n+1}(2^m-j)}(R^{2^{n+1}}) \\ &= QSq^{2^{m+n+1}}(R^{2^{n+1}}) + \sum_{0<j\le 2^m} Sq^{2^{n+1}j}(Q)R_j^{2^{n+1}}, \end{aligned}$$

where $R_j := Sq^{2^m-j}(R)$ for $j = 1, \dots, 2^m$.

In order to prove that $QSq^{2^{m+n+1}}(R^{2^{n+1}})$ is $\mathcal{A}$-decomposable, it suffices to show that each $Sq^{2^{n+1}j}(Q)R_j^{2^{n+1}}$ is $\mathcal{A}$-decomposable. We do this by showing $BR_j^{2^{n+1}} \in \mathcal{A}^+ \cdot P_k$ for every Dickson monomial B of $Sq^{2^{n+1}j}(Q)$. Let $B = \prod_{0\le i\le p} B_i^{2^i}$, with $B_i^{2^i}$ the ith cut of B. By Lemma 4.1(a), we have $p \ge n$. If $\prod_{0\le i\le n} B_i^{2^i} = 1$, then $p > n$, so $BR_j^{2^{n+1}} = (\prod_{n<i\le p} B_i^{2^{i-1}} R_j^{2^n})^2 \equiv 0 \pmod{I_0}$. If $\prod_{0\le i\le n} B_i^{2^i} \ne 1$, then it is not full by Lemma 4.1(b). So we can choose an integer q such that $B_q \ne 1\,(0 \le q \le n \le N)$ and $\prod_{0\le i\le q} B_i^{2^i}$ is not full. Applying Lemma A(a) to $\prod_{0\le i\le q} B_i^{2^i}$, we obtain

$$BR_j^{2^{n+1}} = \prod_{0\le i\le q} B_i^{2^i}(\prod_{q<i\le p} B_i^{2^{i-q-1}} R_j^{2^{n-q}})^{2^{q+1}} \in \mathcal{A}^+ \cdot P_k.$$

Therefore, Step 1 is shown.

Step 2. *Lemma* A(a) *holds for every non-negative integer* n.

Let $q = q(Q)$ be the smallest integer so that A_q is not full ($0 \le q \le n$). Setting $\bar{R} := \prod_{q<i\le n} A_i^{2^{i-q-1}} R^{2^{n-q}}$, we have $QR^{2^{n+1}} = \prod_{0\le i\le q} A_i^{2^i} \bar{R}^{2^{q+1}}$.

Let s be the smallest integer with $0 < s < k$ such that $Q_s \not| A_q$.

We first notice that Lemma A(a) is true if $q(Q) = 0$. This is proved by induction on s. For $s = 1$, we have $A_q\bar{R}^2 \equiv 0 \pmod{I_0}$. Indeed, if $A_q = 1$, then every monomial of $\bar{R}$ is of positive degree, so $A_q\bar{R}^2 = \bar{R}^2 \equiv 0 \pmod{I_0}$; if $A_q \ne 1$, then $A_q\bar{R}^2 \equiv 0 \pmod{I_0}$ by Corollary 2.6. Therefore, $QR^{2^{n+1}} = A_q\bar{R}^2 \in \mathcal{A}^+ \cdot P_k$. The case $s = 1$ is proved. Suppose $s > 1$ and the assertion holds for $s-1$. Then $A_q \ne 1$. By Lemma 4.2, we get

$$QR^{2^{n+1}} = A_q\bar{R}^2 = Sq^{2^{s-1}}(R_1) + \sum BR_2^2.$$

Since $Q_{s-1} \not| B$, by the inductive hypothesis on s, we have $BR_2^2 \in \mathcal{A}^+ \cdot P_k$. This is true for every term BR_2^2, so $QR^{2^{n+1}} \in \mathcal{A}^+ \cdot P_k$.

We now prove Step 2 by induction on n. For $n = 0$, we have $q(Q) = 0$, so Lemma A(a) is true by the above remark. Suppose $n > 1$ and Lemma A(a) holds for every smaller value of n. Using the above remark, it suffices to consider the case $q = q(Q) > 0$. Again, the proof proceeds by induction on s.

For $s = 1$, we have seen that $A_q\bar{R}^2 \equiv 0 \pmod{I_0}$. In other words, $A_q\bar{R}^2 = Sq^1(R_1)$ for some $R_1 \in P_k$. Then

$$QR^{2^{n+1}} = \prod_{0\le i<q} A_i^{2^i}(A_q\bar{R}^2)^{2^q} = \prod_{0\le i<q} A_i^{2^i} Sq^{2^q}(R_1^{2^q}).$$

Note that $\prod_{0\le i<q} A_i^{2^i}$ is full. By Step 1 and the inductive hypothesis on n, we can apply Lemma A(b) to the element $\prod_{0\le i<q} A_i^{2^i}$ of height $q-1 < n$. This gives

$$\prod_{0\le i<q} A_i^{2^i} Sq^{2^q}(R_1^{2^q}) \in \mathcal{A}^+ \cdot P_k.$$

Thus, the case $s = 1$ is proved.

Suppose $s > 1$ and the assertion holds for every smaller value of s. Since $A_q \ne 1$, by Lemma 4.2, we get $A_q\bar{R}^2 = Sq^{2^{s-1}}(R_1) + \sum BR_2^2$. So

$$\begin{aligned} QR^{2^{n+1}} &= \prod_{0\le i<q} A_i^{2^i}(A_q\bar{R}^2)^{2^q} \\ &= \prod_{0\le i<q} A_i^{2^i} Sq^{2^{q+s-1}}(R_1^{2^q}) + \sum \prod_{0\le i<q} A_i^{2^i} B^{2^q} R_2^{2^{q+1}}. \end{aligned}$$

By Step 1 and the inductive hypothesis on n, we have

$$\prod_{0\le i<q} A_i^{2^i} Sq^{2^{q+s-1}}(R_1^{2^q}) \in \mathcal{A}^+ \cdot P_k.$$

On the other hand, as B is a cut that is not divisible by Q_{s-1}, by using the inductive hypothesis on s we get

$$\prod_{0\le i<q} A_i^{2^i} B^{2^q} R_2^{2^{q+1}} \in \mathcal{A}^+ \cdot P_k.$$

Step 2 is proved. Then, Lemma A follows. $\square$

5. Proof of Lemma B

By the hypothesis, $A = \prod_{0<s<k} Q_s Q_0^{\alpha}$, with $\alpha \in \{0,1\}$. We need to prove $A \equiv 0 \pmod{I_1}$. To this end, by means of Corollary 2.2 and the hypothesis $k > 2$, it suffices to show $Q_2 Q_1 \equiv 0 \pmod{I_1}$. From [7, Theorem 2.2], we get

$$\begin{aligned} Q_1 &= \sum_{\substack{\alpha_1+\cdots+\alpha_k=2^k-2,\\ \alpha_i=0 \text{ or power of } 2}} x_1^{\alpha_1}\dots x_k^{\alpha_k} \\ &= \sum_{\text{sym}} x_1x_2x_3^4\dots x_k^{2^{k-1}} + \sum_{\text{sym}} x_1^2x_2^2x_3^2x_4^8\dots x_k^{2^{k-1}} + R^2, \end{aligned}$$

where $\sum_{\text{sym}}$ denotes the sum of all symmetrized terms in $x_1,\dots,x_k$, and R is some polynomial, whose monomials are all of positive degree. By Lemma 2.5, $R^2 \equiv 0 \pmod{I_0}$. We obtain

$$\begin{aligned} Q_1 &\equiv \sum_{\text{sym}}(x_1x_2x_3^4\dots x_k^{2^{k-1}} + x_1^2x_2^2x_3^2x_4^8\dots x_k^{2^{k-1}}) \pmod{I_0} \\ &\equiv Sq^2\Big(\sum_{\text{sym}} x_1x_2x_3^2x_4^8\dots x_k^{2^{k-1}}\Big) \pmod{I_0} \\ &\equiv Sq^2Sq^1\Big(\sum_{\text{sym}} x_1x_2x_3x_4^8\dots x_k^{2^{k-1}}\Big) \pmod{I_0} \\ &\equiv Sq^2Sq^1(R_1) \pmod{I_0}, \end{aligned}$$

where $R_1 := \sum_{\text{sym}} x_1x_2x_3x_4^8\dots x_k^{2^{k-1}}$. Writing $Q_1 = Sq^2Sq^1(R_1) + Sq^1(R_2)$ for some $R_2 \in P_k$, we get

$$\begin{aligned} Q_2Q_1 &= Q_2Sq^2Sq^1(R_1) + Q_2Sq^1(R_2) \\ &\equiv R_1Sq^1Sq^2(Q_2) + R_2Sq^1(Q_2) \pmod{I_1} \qquad \text{(by Lemma 2.4)} \\ &\equiv R_1Q_0 \pmod{I_1} \qquad \text{(by Corollary 2.2).} \end{aligned}$$

On the other hand, by [7, Theorem 2.2], we have

$$\begin{aligned} Q_0 &= \sum_{\text{sym}} x_1x_2^2x_3^4\dots x_k^{2^{k-1}} = Sq^2\Big(\sum_{\text{sym}} x_1x_2^2x_3^2x_4^8\dots x_k^{2^{k-1}}\Big) \\ &= Sq^2Sq^2\Big(\sum_{\text{sym}} x_1x_2x_3x_4^8\dots x_k^{2^{k-1}}\Big) = Sq^2Sq^2(R_1). \end{aligned}$$

Therefore,

$$\begin{aligned} Q_2Q_1 &\equiv R_1Q_0 \pmod{I_1} \equiv R_1Sq^2Sq^2(R_1) \pmod{I_1} \\ &\equiv Sq^2(R_1)Sq^2(R_1) \pmod{I_1} \qquad \text{(by Lemma 2.4(b))} \\ &\equiv [Sq^2(R_1)]^2 \pmod{I_1} \equiv 0 \pmod{I_1}. \end{aligned}$$

Lemma B is proved. □

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. CMP 95:18

[2] 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. MR **92c:**55018

[3] Nguyễn H. V. Hu'ng, *Spherical classes and the algebraic transfer*, Trans. Amer. Math. Soc. **349** (1997), 3893–3910. MR **98e:**55020

[4] Nguyễn H. V. Hu'ng, *The weak conjecture on spherical classes*, Math. Zeit. **231** (1999), 727–743. MR **2000g:**55019

[5] Nguyễn H. V. Hu'ng, *Spherical classes and the lambda algebra*, Trans. Amer. Math. Soc. **353** (2001), 4447–4460.

[6] Nguyễn H. V. Hu'ng and F. P. Peterson, *$\mathcal{A}$-generators for the Dickson algebra*, Trans. Amer. Math. Soc. **347** (1995), 4687–4728. MR **96c:**55022

[7] Nguyễn H. V. Hu'ng and F. P. Peterson, *Spherical classes and the Dickson algebra*, Math. Proc. Camb. Phil. Soc. **124** (1998), 253–264. MR **99i:**55021

[8] M. Kameko, *Products of projective spaces as Steenrod modules*, Thesis, Johns Hopkins University 1990.

[9] F. P. Peterson, *Generators of $H^*(\mathbf{RP}^\infty \wedge \mathbf{RP}^\infty)$ as a module over the Steenrod algebra,* Abstracts Amer. Math. Soc., No **833**, April 1987.

[10] S. Priddy, *On characterizing summands in the classifying space of a group, I*, Amer. Jour. Math. **112** (1990), 737–748. MR **91i:**55020

[11] J. H. Silverman, *Hit polynomials and the canonical antiautomorphism of the Steenrod algabra*, Proc. Amer. Math. Soc. **123** (1995), 627–637. MR **95c:**55023

[12] W. M. Singer, *The transfer in homological algebra*, Math. Zeit. **202** (1989), 493–523. MR **90i:**55035

[13] N. E. Steenrod and D. B. A. Epstein, *Cohomology operations*, Ann. of Math. Studies, No. **50**, Princeton Univ. Press, 1962. MR **26:**3056

[14] R. M. W. Wood, *Modular representations of $GL(n, \mathbb{F}_p)$ and homotopy theory*, Lecture Notes in Math. **1172**, Springer Verlag (1985), 188–203. MR **88a:**55007

Department of Mathematics, Vietnam National University, Hanoi, 334 Nguyên Trãi Street, Hanoi, Vietnam

E-mail address: nhvhung@hotmail.com

Department of Mathematics, Vietnam National University, Hanoi, 334 Nguyên Trãi Street, Hanoi, Vietnam

E-mail address: trngnam@hotmail.com