204. On the Dimension of Generators of a Polynomial Algebra over the Mod p Steenrod Algebra

By Ryosuke NAKAGAWA and Shōji OCHIAI
Tokyo University of Education

(Comm. by Kinjirô KUNUGI, M.J.A., Dec. 12, 1967)

1. It is well known that if $H^*(X; Z_2)$ is a polynomial algebra (possibly truncated) on a generator x of dimension m and $x^2 \neq 0$, then $m=1, 2, 4$, or 8 [1]. If $H^*(X; Z_p)$ is a truncated polynomial algebra on one generator with dimension $2k$ of height $q>p$, then k is a divisor of $p-1$ [3]—[5]. In the above cases the cohomology algebra has only one generator. In this paper, we are concerned with a truncated polynomial algebra with two generators over the mod p Steenrod algebra where p is an odd prime. On a finitely generated truncated polynomial algebra over the Steenrod algebra, E. Thomas and A. Clark have obtained some results [2][6].

By an algebra A over the mod p Steenrod algebra, we mean a commutative and associative graded Z_p algebra A on which the reduced powers and the Bockstein coboundary act just as if A were the cohomology algebra of a space.

Our results are the followings.

Theorem. 1. *Let A be a truncated polynomial algebra of height $q>p$ with even dimensional generators a and b over the mod p Steenrod algebra. We put dim $a=m$, dim $b=n$, and we assume that $0<m\leqq n$ holds. Then, such an algebra only possible if the dimensions m, n satisfy one of the following conditions.*

(a) $m=2i$, $n=2j$, $i\leqq j<p$, *and*
  (i) *i, j are divisors of $p-1$,*
  (ii) *i is a divisor of $p-1$ and j is a divisor of $i+p-1$,*
  (iii) *j is a divisor of $p-1$ and i is a divisor of $j+p-1$, or*
  (iv) *i is a divisor of $j+p-1$ and j is a divisor of $i+p-1$.*
(b) $m=2i$, $n=2(p+i-1)$, *i is a divisor of $2(p-1)$.*
(c) $m=2i$, $n=2\varepsilon p^f$, *i, ε are divisors of $p-1$, $f\geqq 1$,*
(d) $m=2(\delta p^f+i)$, $n=2\varepsilon p^f$, *ε is a divisor of $p-1$, $0<\delta<\varepsilon$, $0<i<p$, $f\geqq 1$,*
(e) $m=2\varepsilon p^f$, $n=2(\varepsilon p^f+p-1)$, *ε is a divisor of $p-1$, $f\geqq 1$,*
(f) $m\equiv 0$, $n\equiv 0$ (mod $2p$).

Remark. If A is a finitely generated truncated polynomial algebra whose generators have fixed even dimensions m and n, then the same conclusion as above holds for this algebra A. The similar generalization for Theorem 2 holds also.

Theorem 2. *Suppose that $H^*(X;Z_p)$ is a truncated polynomial algebra of height $q>p$ with two generators a and b which have even dimensions m and n respectively $(m \leqq n)$. Then such a cohomology algebra is only possible if m and n satisfy one of the conditions* (a) *to* (c) *of Theorem* 1.

Throughout the paper, we shall denote by λ, λ', α, α', ... non zero elements in Z_p and by x, y, x', ... polynomials of a and b (possibly 0).

2. Proof of Theorem 1. This is accomplished by considering for each case divided as follows.

(I) $m \not\equiv 0$, $n \not\equiv 0 \pmod{2p}$.

For this case, we can use the subsequent result of A. Clark (Theorem 2[2]).

Lemma. *Let A be a truncated polynomial algebra of height $q>p$ with even dimensional generators over the* mod p *Steenrod algebra. If m is the dimension of a generator of A, then A has a generator with dimension n such that $n \equiv 2(1-p) \pmod{m}$, or else $m \equiv 0 \pmod{2p}$.*

In our case, since A has two generators a and b with dimensions $m \not\equiv 0$ and $n \not\equiv 0 \pmod{2p}$, we have that m or $n \equiv 2(1-p) \pmod{m}$ and m or $n \equiv 2(1-p) \pmod{n}$.

Therefore the following four cases are possible.

(i) $m \equiv 2(1-p) \pmod{m}$ and $n \equiv 2(1-p) \pmod{n}$. That is, m and n divides $2(p-1)$.

(ii) $m \equiv 2(1-p) \pmod{m}$ and $m \equiv 2(1-p) \pmod{n}$. That is, m divides $2(p-1)$ and n divides $m+2(p-1)$.

(iii) $n \equiv 2(1-p) \pmod{m}$ and $n \equiv 2(1-p) \pmod{n}$. That is, n divides $2(p-1)$ and m divides $n+2(p-1)$.

(iv) $n \equiv 2(1-p) \pmod{m}$ and $m \equiv 2(1-p) \pmod{n}$. This implies that $n+2(p-1)=sm$ and $m+2(p-1)=tn$

for some positive integers s and t. If $n>2p$, $2(p-1)=tn-m=(t-1)n+n-m>2(t-1)p$. Thus we have $t=1$ and $4(p-1)=(s-1)m$ that is, m divides $4(p-1)$. If $p=3$ and $m=4(p-1)$, then $n=6(p-1)\equiv 0 \pmod{2p}$. This contradicts the assumption $n \not\equiv 0 \pmod{2p}$. Therefore we have obtained that the cases (a) and (b) mentioned in Theorem 1 are only possible in the case (I).

(II) $m \not\equiv 0$, $n \equiv 0 \pmod{2p}$.

We put $m=2(kp+i)$, $n=2\,lp$, $0<i<p$.

(1) $k \geqq 1$. From the property of the cyclic reduced powers we have $a^p=\mathcal{P}^{kp+i}a=\lambda(\mathcal{P}^1)^i\mathcal{P}^{kp}a$. Since $\dim \mathcal{P}^{kp}\,a \equiv 2\,i$, $\dim a^u b^v \equiv 2\,i\,u \pmod{2\,p}$ and $\mathcal{P}^{kp}\,a \neq 0$, we have that $\mathcal{P}^{kp}\,a = \alpha\,a\,b^v$. This implies that

(i) $kp(p-1)=lpv$.

Next, we shall consider about $\mathcal{P}^1 a$. Since $\dim \mathcal{P}^1 a < \dim a^2$, we get $\mathcal{P}^1 a=0$ or $\alpha' b$. Suppose that $\mathcal{P}^1 a=\alpha' b$. Then $2(kp+i)+2(p-1)=2\,lp$ holds and this implies that $i=1$. Therefore, $m=2(kp+1)$, $n=2(k+1)p$. Thus we have that if $k\geqq 2$, $\dim \mathcal{P}^1 b<\dim a^2$, and if $k=1$ and $p\geqq 5$, $\dim a^2<\dim \mathcal{P}^1 b<\dim a^3$. Therefore, we can conclude $\mathcal{P}^1 b=0$ with an exception of $p=3$ and $k=1$, (that is $m=8$ and $n=12$). The exceptional case is included in (b) in this theorem and hereafter we shall not consider about this case. Since we get $\mathcal{P}^1 b=0$, we have $a^p=\mathcal{P}^1\mathcal{P}^{kp}a=\mathcal{P}^1(\alpha\, a\, b^v)=\alpha\,\alpha'\ b^{v+1}$. This is a contradiction. Then we get $\mathcal{P}^1 a=0$. We know that any $\mathcal{P}^k (k\neq p^i)$ is decomposable, and so, from the fact that $\mathcal{P}^{kp}a\neq 0$ there is an integer f such that $\mathcal{P}^{p^f}a\neq 0$. Since we have proved $\mathcal{P}^1 a=0$, f is positive. Since $\dim \mathcal{P}^{p^f}a\equiv 2\ i$ and $\dim a^u b^v\equiv 2\ i\, u \pmod{2p}$, we have that $\mathcal{P}^{p^f}a=\alpha'' a b^{v'}$. Thus we get $p^f(p-1)=lp\, v'$. This shows (ii) $l=\varepsilon\, p^{f-1}$ where ε is a divisor of $p-1$ and $f\geqq 1$. We get $k=\delta\, p^{f-1}$ from (i) and (ii). Therefore we can conclude that $m=2(\delta p^f+i)$, $n=2\varepsilon p^f$, where ε is a divisor of $p-1$, $0<\delta<\varepsilon$, and $f\geqq 1$.

(2) $k=0$. We can see that $\mathcal{P}^1 a=\alpha a^u$, by considering their dimensions. This implies that $2(p-1)=2i(u-1)$. Therefore, i is a divisor of $p-1$, and furthermore, we have that $\mathcal{P}^j a=\alpha_j a^{uj}$ for $j\leqq i$, and $\mathcal{P}^j a=0$ for $j>i$. Since $b^p=\mathcal{P}^{lp}b\neq 0$, there is an integer $f\geqq 0$ such that $\mathcal{P}^{p^f}b\neq 0$. Suppose that $\mathcal{P}^{p^f}b=0$ for any $f>0$. Then $\mathcal{P}^1 b\neq 0$. Since $\dim \mathcal{P}^1 b<\dim\ b^2$, we have $\mathcal{P}^1 b=a\cdot y$. Therefore $b^p=\mathcal{P}^{lp}b=\sum \mathcal{P}^{p^{f_1}}\cdots \mathcal{P}^{p^{f_r}}\mathcal{P}^1_b=a\cdot y'$. This is a contradiction. Thus there exists a positive integer f such that $\mathcal{P}^{p^f}b\neq 0$. Then we get $\dim \mathcal{P}^{p^f}b\not\equiv \dim\ a^u b^v \pmod{2p}$ for any $u>0$. Hence we can conclude that $\mathcal{P}^{p^f}b=\alpha' b^v$. Therefore $2(p-1)p^f=2(v-1)lp$. Consequently, $l=\varepsilon p^{f-1}$, where ε is a divisor of $p-1$. Thus we have proved in this case that $m=2\, i$, $n=2\varepsilon p^f$, where i, ε are divisors of $p-1$ and $f\geqq 1$.

(III) $m\equiv 0$, $n\not\equiv 0 \pmod{2p}$.

We put $m=2kp$, $n=2(lp+j)$, $0<j<p$. Since $\dim \mathcal{P}^1 a<\dim a^2$, $\mathcal{P}^1 a=0$ or αb. Suppose that $\mathcal{P}^1 a=0$. Since $\mathcal{P}^{lp}b=\beta a^u b$, then we get $b^p=\lambda'(\mathcal{P}^1)^j\, p^{lp}b=a\cdot y$. This is a contradiction. Thus we have $\mathcal{P}^1 a=\alpha b$ and this implies that $m=2kp$ and $n=2(kp+p-1)$. Now there is an integer f such that $\mathcal{P}^{p^f}b\neq 0$, $p^f\leqq kp$. Since $\dim \mathcal{P}^1 b<\dim b^2$, and $\dim \mathcal{P}^1 b\equiv -4$, $\dim a^u\equiv 0$ and $\dim a^u b\equiv -2 \pmod{2p}$, we obtain $\mathcal{P}^1 b=0$. Therefore $f>0$. Since $\dim \mathcal{P}^{p^f}b\equiv -2$ and $a^u b^v\equiv -2v \pmod{2p}$, we can get $\mathcal{P}^{p^f}b=\alpha' a^{u'} b$. From this equation, we can conclude $k=\varepsilon p^{f-1}$. Thus we have $m=2\varepsilon p^f$, $n=2(\varepsilon p^f+p-1)$, where ε is a divisor of $p-1$ and $f\geqq 1$.

(IV) $m\equiv 0$, $n\equiv 0 \pmod{2p}$

We have some results for m and n in this case. However they are somewhat complicated and so we omitt them.

Thus we complete the proof of Theorem 1.

3. Proof of Theorem 2. To prove Theorem 2, we need the results about the factrization of cyclic reduced powers by secondary cohomology operations [3] [4].

There exist stable secondary operations R, Ψ_g $(g=1, 2, \cdots)$ such that

$$R: H^r(X; Z_p) \cap \mathrm{Ker}\, \Delta \cap \mathrm{Ker}\, \mathcal{P}^1 \longrightarrow$$
$$H^{r+4(p-1)}(X; Z_p)/\mathcal{P}^2 H^r(X; Z_p) + \left(\frac{1}{2}\ \Delta\mathcal{P}' - \mathcal{P}'\Delta\right) H^{r-1+2(p-1)}(X; Z_p)$$

$$\Psi_g: H^r(X; Z_p) \cap \mathrm{Ker}\, \Delta \cap \mathrm{Ker}\, \mathcal{P}^1 \cap \mathrm{Ker}\, \mathcal{P}^p \cap \cdots \mathrm{Ker}\, \mathcal{P}^{p^g} \longrightarrow$$
$$H^{r+2p^g(p-1)}(X; Z_p)/\mathcal{P}^{p^g} H^r(X; Z_p) + \sum \vartheta_h H^{r-1+2p^h(p-1)}(X; Z_p)$$

where ϑ_h are homogeneous elements of the Steenrod algebra A_p with odd degrees. We quote from [3] the following:

Theorem A. *There exists a constant ν_{f-1}, non zero in Z_p, elements $a_{f-1,g}$, b_{f-1}, $c_{f-1,\gamma}$ with possitive degrees in A_p and secondary cohomology operations Γ_γ with odd degree, such that*

$$\{\nu_{f-1}\,\mathcal{P}^{p^f}\} \equiv \sum_{g=1}^{f-1} a_{f-1,g}\,\Psi_g + b_{f-1}\,R + \sum c_{f-1,\,\gamma}\Gamma_\gamma.$$

modulo the total indeterminacy of the right-hand side.

From this, we have the following:

Lemma 3. *Let Δ and $\mathcal{P}^1$ operate trivially on a cohomology group $H^*(X; Z_p)$ Then $\mathcal{P}^i$ operates trivially on $H^*(X; Z_p)$ for any i.*

Proof. If a monomial c in A_p has odd degree, c contains Δ as its factor. From the assumption, we have that if an element c in A_p has odd degree, c operates trivially on $H^*(X; Z_p)$. We know that $\mathcal{P}^i$, $i \neq p^f$, is decomposable. Hence if $\mathcal{P}^{p^{f'}}=0$ for $0 \leqq f' \leqq f-1$, $\mathcal{P}^i=0$ for $i<p^f$. We shall show that under the assumption of $\mathcal{P}^i=0$ for $i<p^f$, $\mathcal{P}^{p^f}=0$ holds. By Theorem A, there exists a non zero constant $\nu_{f-1} \in Z_p$ such that $\{\nu_{f-1}\mathcal{P}^{p^f}\} \equiv \sum_{g=1}^{f-1} a_{f-1,g}\,\Psi_g + b_{f-1}\,R.$ modulo $a_{f-1,f-1}\,\mathcal{P}^{p^{f-1}}\,H^r(X; Z_p) + \cdots + a_{f-1,1}\,\mathcal{P}^p H^r(X; Z_p) + b_{f-1}\,\mathcal{P}^2 H^r(X; Z_p)$. It is noted that the above equation holds on $H^*(X; Z_p)$. Since $0<\dim a_{f-1,g}$, $\dim b_{f-1} < \dim \mathcal{P}^{p^f}$, $a_{f-1,g}=0$, $g=1, 2, \cdots, f-1$, and $b_{f-1}=0$. This shows that $\mathcal{P}^{p^f}=0$ and the proof is completed.

Now we shall prove the impossibility of (d), (e), and (f) in Theorem 1 under the assumption of Theorem 2.

(1) Case (f).

Since $m=2kp$ and $n=2lp$, we have that $\dim \mathcal{P}^1 a \equiv -2$ and $\dim \mathcal{P}^1 b \equiv -2 \pmod{2p}$. On the other hand, $\dim a^u b^v \equiv 0 \pmod{2p}$. This implies that $\mathcal{P}^1 a=0$ and $\mathcal{P}^1 b=0$, that is, $\mathcal{P}^1=0$. By Lemma 3, $\mathcal{P}^i=0$ for any i. This contradicts to the fact that $\mathcal{P}^{kp} a = a^p \neq 0$

and $\mathcal{P}^{1p}b=b^p\neq 0$.

(2) Case (e).

We have already obtained that $m=2\varepsilon p^f$ and $n=2(\varepsilon p^f+p-1)$, where ε is a divisor of $p-1$ and $f\geqq 1$. We have also shown in the proof (III) of Theorem 1, that $\mathcal{P}^1a=\alpha b$ and $\mathcal{P}^1b=0$.

Since $b^p=\mathcal{P}^{(\varepsilon p^f+(p-1))}b\neq 0$, there exists an integer $f'\leqq f$ such that $\mathcal{P}^{p^{f'}}b\neq 0$. If $\mathcal{P}^{p^{f'}}b$, $1\leqq f'\leqq f$, contains a term a^ub^v, we can see $v=1$ from the fact that $\dim \mathcal{P}^{p^{f'}}b\equiv -2$, $\dim a^ub^v\equiv -2v (\mathrm{mod}\ 2p)$ and $v<p$ and we have that $2(p-1)p^{f'}=2\varepsilon p^f u$. This means that $f'=f$ and $u=\dfrac{p-1}{\varepsilon}$. Consequently $\mathcal{P}^{p^{f'}}b=0$ for $f'<f$, $\mathcal{P}^{p^f}b=\beta' a^{\frac{p-1}{\varepsilon}}\cdot b$.

Therefore we can apply Theorem A to b. There exists a non-zero element ν_{f-1} in Z_p such that $\{\nu_f\,\mathcal{P}^{p^f}b\}\equiv\sum_{g=1}^{f-1}a_{f-1,g}\Psi_g b+b_{f-1}Rb \bmod a_{f-1,f-1}\mathcal{P}^{p^{f-1}}H^n(X;Z_p)+\cdots+a_{f-1,1}\mathcal{P}^pH^n(X;Z_p)+b_{f-1}\mathcal{P}^2H^n(X;Z_p)$. It is easily seen that the above indeterminacy is zero. If Rb contains a term a^ub^v, we get $v=3$ from the fact that $\dim Rb\equiv -6$ and $\dim a^ub^v\equiv -2v (\mathrm{mod}\ 2p)$. However, $\dim Rb<\dim b^3$. Hence we have that $Rb=0$. By the similar way as above, we can see that $\Psi_g b=0$ for $1\leqq g\leqq f-1$. Thus, we have that $\mathcal{P}^{p^f}b=0$. This is a contradiction and it is shown that the case (e) is not realized.

(3) Case (d).

We have already obtained that $m=2(\delta p^f+i)$, and $n=2\varepsilon p^f$, where ε is a divisor of $p-1$, $0<\delta<\varepsilon$, $0<i<p$, and $f\geqq 1$. We have also shown that unless $p=3$, $m=8$, and $n=12$, $\mathcal{P}^1a=0$, $\mathcal{P}^{\delta p^f}a=\alpha ab^v$, $\mathcal{P}^{p^f}a=\alpha'' ab^{v'}$. By the similar way as above, we can obtain that $\mathcal{P}^{p^{f'}}a=0$ for any $f'<f$ and by using Theorem A, we have $\mathcal{P}^{p^f}a=0$. This is a contradiction. Thus it is shown that this case (d) is not realized. It is noted that the case $p=3$, $m=8$, and $n=12$ is possible and is contained in (b). Thus the proof is completed.

References

[1] J. F. Adams: On the non-existence of elements of Hopf invariant one. Ann. Math., **72**, 20-104 (1960).

[2] A. Clark: On Π_3 of finite dimensional H-spaces. Ann. Math., **78**, 193-196 (1963).

[3] Liulevicius: The factorization of cyclic reduced powers by secondary cohomology operations. Proc. Nat. Acad. Sci. U.S.A., **46**, 978-981 (1960).

[4] N. Shimada and T. Yamanoshita: On triviarity of the mod p Hopf invariant. Japanese Journal, **31**, 1-26 (1961).

[5] N. Steenrod: Cohomology operations. Princeton Univ. Press (1962).

[6] E. Thomas: Steenrod squares and H-spaces. Ann. Math., **77**, 306-317 (1963).