

\mathcal{A} –générateurs génériques pour l’algèbre polynomiale

Trần Ngọc Nam *

¹ Département de Mathématiques, Université des Sciences à Hanoi

² LAGA, Département de Mathématiques, Université de Paris–Nord

e-mail: trngnam@hotmail.com, tran@math.univ-paris13.fr

Received: 23-XI-2002 / Revised version: date

Dédié au Pr. Nguyễn Duy Tiên à l’occasion de son soixantième anniversaire

Résumé. Nous résolvons génériquement le problème “hit” (posé en 1986 par Franklin P. Peterson) par la découverte en degrés génériques d’un système générateur minimal explicite pour l’algèbre polynomiale comme module sur l’algèbre de Steenrod mod 2. Cette solution implique en particulier un résultat de J. Repka–P. Selick, une partie de celui de M. C. Crabb–J. R. Hubbuck et nous permet en même temps de vérifier une conjecture due à M. Kameko. Ce système générateur sera appliqué à l’étude du transfert algébrique de W. M. Singer et de la représentation modulaire du groupe linéaire général.

1. Introduction

Soient \mathcal{A} l’algèbre de Steenrod mod 2 et $\mathbf{P} := \mathbb{F}_2[x_1, x_2, \dots, x_k]$ l’algèbre polynomiale graduée à k générateurs sur le corps à deux éléments \mathbb{F}_2 , chaque générateur étant de degré 1. En tant que cohomologie modulo 2 du classifiant $B(\mathbb{Z}/2)^k$, l’algèbre \mathbf{P} est dotée d’une structure naturelle de \mathcal{A} –algèbre instable.

Soient $\bar{\mathcal{A}} \subset \mathcal{A}$ l’idéal de l’augmentation et $\bar{\mathcal{A}}\mathbf{P} \subset \mathbf{P}$ le sous-ensemble des éléments “hit”, c’est-à-dire de la forme $\sum \theta P$ avec $\theta \in \bar{\mathcal{A}}$ et $P \in \mathbf{P}$. Nous attaquons le problème “hit” qui consiste à expliciter une base pour l’espace vectoriel $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ (autrement dit, un système générateur minimal pour le \mathcal{A} –module \mathbf{P}). Ce problème est d’une importance significative en topologie algébrique. Parmi ses applications, citons les travaux de Peterson [45] en cobordisme, de Wood [57]

* L’auteur bénéficie d’une bourse de doctorat BDI 2002 du CNRS

en représentation modulaire des groupes linéaires et de Hung [21] sur l'homologie de l'espace de lacets infini QS^0 . D'autres applications sont fournies par les travaux de Singer [52] et de Minami [36] [37].

Singer [52] construit un morphisme \mathbb{F}_2 -linéaire

$$Tr_k^* : Tor_k^A(\mathbb{F}_2, \mathbb{F}_2) \longrightarrow Tor_0^A(\mathbb{F}_2, \mathbf{P})^{\mathrm{GL}(k, \mathbb{F}_2)} \cong (\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})^{\mathrm{GL}(k, \mathbb{F}_2)}.$$

L'importance de ce morphisme pour la théorie de l'homotopie vient de ce que

- (i) son dual Tr_k , baptisé le “transfert algébrique”, est induit “au niveau E_2 ” par le transfert homotopique $\pi_*^S(B(\mathbb{Z}/2)_+^k) \longrightarrow \pi_*^S(S^0)$ (cf. [4] [17] [27] [30] [38] [46]),
- (ii) Tr_k donne des informations sur les groupes $Ext = Ext_{\mathcal{A}}^k(\mathbb{F}_2, \mathbb{F}_2)$, le terme E_2 de la suite spectrale d'Adams stable qui converge vers les groupes d'homotopie de sphères mod 2,
- (iii) Tr_k est un isomorphisme pour $k \leq 3$ [52] [5],
- (iv) Tr_k n'est pas un épimorphisme pour $k = 4, 5$ [7] [52], mais reste un outil intéressant pour l'étude des groupes Ext . Que ce soit un isomorphisme, épimorphisme ou monomorphisme en général est encore une question ouverte.

Cela étant, ajoutons que les efforts [5] [7] [15] [52] pour établir la bijectivité de Tr_k ($k \leq 3$) et la non-surjectivité de Tr_k ($k = 4, 5$) reposent essentiellement sur la connaissance d'une base explicite de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$.

Liés à ceux de Singer, les travaux de Minami [36] [37] touchent aussi le problème “hit” mais portent sur un autre aspect de la théorie d'homotopie. En effet, à la différence de Carlsson [9], Miller [34], Adams–Gunawardena–Miller [1] et Lannes [29] qui étudient $B(\mathbb{Z}/2)^k$ en tant qu'espace source, Minami se propose d'étudier les groupes d'homotopie stable de $B(\mathbb{Z}/2)^k$. En utilisant des techniques venant de la BP -théorie et les travaux de Kameko [25] (voir ci-dessous) et de Boardman [5], Minami a trouvé des résultats intéressants sur l'image de Hurewicz stable de $B(\mathbb{Z}/2)^k$. De plus, ses recherches ont mis à jour les conjectures surnommées “doomsday”, de pleine actualité.

Ces quelques citations donnent une idée assez claire du rôle que joue $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$. Pourtant, malgré son importance significative, la description de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ avait la réputation d'être difficile. Celle-ci est facile pour $k = 1$, connue pour $k = 2$ [19] [44] [58] mais se révèle très compliquée dès que $k \geq 3$. Les premiers calculs complets de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ pour $k = 3$ ont été effectués par Kameko dans sa thèse [25] soutenue à l'Université Johns Hopkins en 1990. Ils constituent une source de référence pour deux autres groupes de topologues: Alghamdi–Crabb–Hubbuck [2] et Boardman [5], qui ont aussi explicité le cas $k = 3$ mais par des approches différentes. Tous ces travaux ont été communiqués au moment de la Conférence à la mémoire d'Adams en 1990. Signalons que même pour le cas $k = 3$, les calculs [25] sont longs et

n'ont été publiés que beaucoup plus tard sous forme réduite [26]. Le problème "hit" demeure non résolu jusqu'ici pour $k \geq 4$.

En raison de la complexité du calcul de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$, souvent on contourne la difficulté: soit on cherche à décrire $\bar{\mathcal{A}}\mathbf{P}$ et les générateurs de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ qui en découlent, soit on examine $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ en degrés petits, soit on mesure sa dimension globale. (Il y a aussi l'approche plus homotopique comme [3], mais on n'en parlera pas ici. Le lecteur pourra consulter [19] [20] [22] [23] [24] [58] pour des problèmes proches de celui que nous traitons.)

Citons d'abord le théorème célèbre de R. M. W. Wood (alias la Conjecture de Peterson—cf. [6] pour son contexte):

Théorème 1.1 (Wood [56]). *En degré d , l'espace vectoriel $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ est nul sauf si d est de la forme*

$$d = (2^{m_1} - 1) + (2^{m_2} - 1) + \cdots + (2^{m_k} - 1)$$

avec $m_1 \geq m_2 \geq \cdots \geq m_k \geq 0$.

Ce théorème est le point de départ de tout un courant de recherche actuel: celui de déterminer les éléments "hit" et les conditions qui les gouvernent. Nombreux sont les chercheurs qui cherchent à raffiner et généraliser la technique de Wood, dont Chen–Shen [10], Crossley [12] [14] [16], Karaca [28], Meyer [32] [33], Monks [39], Silverman [49] [50], Singer [53]... Ajoutons que cet ordre d'idée donne lieu à des systèmes générateurs de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ [16] [57] [58, p. 502] mais qui ne sont pas minimaux et ne constituent donc pas une solution du problème "hit".

Pour l'examen de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ en degrés petits, citons les travaux pionniers de Peterson [44], ceux de Singer [52] et, plus récemment, ceux de Bruner–Hà–Hung [7]. Les calculs explicites de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ en degré 8 pour $k = 4$ ont permis à ces derniers d'affirmer que le transfert algébrique Tr_4 ne détecte pas les éléments $g_{i+1} \in Ext_{\mathcal{A}}^{4, 2^{i+4}+2^{i+3}}(\mathbb{F}_2, \mathbb{F}_2)$ [31].

Quant à l'estimation de la dimension globale de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$, citons d'abord les travaux de Carlisle–Wood [8] qui prouvent qu'il existe une constante $c(k)$ ne dépendant que de k telle que

$$\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d \leq c(k)$$

pour tout d . Une généralisation a été faite par Crossley [12], et des constantes $c(k)$ ont été proposées dans [8] [12] [25] [58]. Il reste cependant à en trouver la valeur exacte (la plus petite possible). À la fin de ses calculs [25], Kameko a proposé la suivante:

Conjecture 1.2 (Kameko [25]). *Soit $d \geq 0$ un entier quelconque. Alors*

$$\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d \leq \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

Cette conjecture est reprise par deux groupes de chercheurs: Crabb–Hubbuck [11] et Repka–Selick [47], qui cherchent tous deux à généraliser les résultats de [2]. Ils ont considéré une certaine sous-algèbre de l’objet dual $(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})^*$ et l’ont étudiée en tant que représentation du groupe linéaire $\mathrm{GL}(k, \mathbb{F}_2)$. En minorant la dimension de cette sous-algèbre, ils ont trouvé une borne minorée générique pour $\dim(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})$:

Théorème 1.3 (Crabb–Hubbuck [11]). *Soit $d = (2^{m_1} - 1) + (2^{m_2} - 1) + \dots + (2^{m_k} - 1)$, avec $2^{m_1 - m_2} > k$, $2^{m_2 - m_3} > k - 1$, \dots , $2^{m_{k-1} - m_k} > 2$ et $m_k \geq 0$. Alors*

$$\dim(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})_d \geq \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

Théorème 1.4 (Repka–Selick [47]). *Soit $d = (2^{m_1} - 1) + (2^{m_2} - 1) + \dots + (2^{m_k} - 1)$ avec $m_1 \geq m_2 \geq \dots \geq m_k \geq 0$. Alors*

$$\dim(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})_d \geq \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

si $m_1 \gg m_2 \gg \dots \gg m_k$. (Cette condition est un peu vague mais elle sera remplie si $m_{\ell-1} - m_\ell \geq k$ pour tout $1 < \ell \leq k$.)

Ayant rétabli le contexte, nous passons maintenant à nos résultats. Vu le Théorème 1.1, résoudre le problème “hit” consiste à expliciter une base de $(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})_d$ pour les degrés d de la forme

$$d = (2^{m_1} - 1) + (2^{m_2} - 1) + \dots + (2^{m_k} - 1)$$

avec $m_1 \geq m_2 \geq \dots \geq m_k \geq 0$. Comme le titre de notre article l’indique, nous faisons cela de manière générique. Par une récurrence sur le nombre de générateurs de \mathbf{P} , nous construisons une base de $(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})_d$ pour les degrés d de cette forme et qui vérifient

$$m_1 - m_2 > 0, m_2 - m_3 \geq 3, \dots, m_{k-1} - m_k \geq k \text{ et } m_k \geq 0.$$

Il s’avère que dans le cas le plus générique, la valeur $\dim(\mathbf{P}/\bar{\mathbf{A}}\mathbf{P})_d$ trouvée par notre méthode coïncide avec la constante qu’on trouve dans la Conjecture 1.2, le Théorème 1.3 et le Théorème 1.4. Ainsi, la construction de notre base (que nous appellerons “générique” suivant la terminologie utilisée dans [11] [47]) non seulement résout de manière générique le problème “hit”, mais aussi redémontre le Théorème 1.4 ainsi qu’une partie du Théorème 1.3, et vérifie la Conjecture 1.2 dans le cas générique. Cette base sera utilisée dans [41], où nous donnons, entre autres, la preuve d’une conjecture de Singer [52] sur le comportement de Tr_k en degrés génériques, puis un analogue du résultat principal de Bruner–Hà–Hung [7] (nous montrons que Tr_4 ne détecte pas l’élément $D_3 \in Ext_{\mathcal{A}}^{4,65}(\mathbb{F}_2, \mathbb{F}_2)$ [55]) et une description de $\mathbf{P}/\bar{\mathbf{A}}\mathbf{P}$ en tant que représentation de $\mathrm{GL}(k, \mathbb{F}_2)$.

L'article est organisé comme suit: pour des raisons techniques, l'énoncé précis de nos résultats est reporté jusqu'en Section 2. L'indépendance linéaire de la base générique est démontrée (avec plus de généralité) dans la Section 3. Cette section peut donc être considérée comme la redécouverte d'une partie des résultats de [11] [47]. La propriété génératrice de la base est établie dans la Section 4 et la preuve finale s'ensuit dans la Section 5. Nos remarques et commentaires sont donnés dans la dernière section: la Section 6.

2. Énoncé des résultats

Dans tout l'article, on adopte les notations:

$$\begin{aligned} E &:= \{1, 2, \dots, k\}, \\ \mathbf{P} &:= \mathbb{F}_2[x_1, x_2, \dots, x_k], \\ X &:= x_1 x_2 \cdots x_k, \\ X_i &:= X/x_i \ (i \in E). \end{aligned}$$

Étant donné un ensemble non vide $I \subset E$, on note $|I|$ son cardinal et $\min I$ son plus petit élément. De plus, si $I = \{i_0 > \dots > i_r\}$ et $m > r$, on pose

$$X(I, m) := \left(\prod_{0 \leq \ell < r} X_{i_\ell}^{2^\ell} \right) X_{i_r}^{2^m - 2^r}.$$

Pour tout $i \in E$, on désigne par $\mathbf{P}(i) \subset \mathbf{P}$ la sous-algèbre engendrée par toutes les variables sauf x_i . Pour tout entier positif n , on note $\alpha(n)$ le nombre de chiffres non nuls dans son développement 2-adique.

Notre premier résultat est le:

Théorème 2.1. *Soient $n, d' \geq 0$ des entiers. Pour chaque $i \in E$, soit $\mathbf{B}(i) \subset \mathbf{P}(i)$ un sous-ensemble dont tous les éléments sont de degré d' . Notons \mathbf{B} l'ensemble des éléments $X^{2^n - 1} X(I, k)^{2^n} P^{2^{k+n}}$, où $\emptyset \neq I = \{i_0 > \dots > i_r\} \subset E$ et $P \in \mathbf{B}(i_r)$.*

- (i) *Si $\mathbf{B}(i)$ est \mathcal{A} -linéairement indépendant pour tout $i \in E$, alors \mathbf{B} l'est également.*
- (ii) *Soit $d := 2^{k+n}(d' + k - 1) + 2^n - k$. Supposons que $\mathbf{B}(i)$ engendre le \mathcal{A} -module $\mathbf{P}(i)$ en degré d' pour tout $i \in E$ et que soit $\alpha(d' + k - 1) = k - 1 > 0$, soit ($n = 0$ et $\alpha(d' + k - 2) \geq k - 2 > 0$). Alors \mathbf{B} engendre le \mathcal{A} -module \mathbf{P} en degré d .*

Soit Ω l'ensemble des suites d'ensembles $\omega := (I_k, J_k, \dots, I_1, J_1)$ définies par: $\emptyset \neq I_k \subset J_k := E$ et $\emptyset \neq I_\ell \subset J_\ell := J_{\ell+1} \setminus \{\min I_{\ell+1}\}$

pour $1 \leq \ell < k$. Si $k > 1$, on désigne par $\bar{\Omega}$ l'ensemble des suites $\bar{\omega} = (I_k, J_k, \dots, I_2, J_2)$ telles que $I_2 \neq J_2$ et

$$(I_k, J_k, \dots, I_2, J_2, J_2 \setminus I_2, J_2 \setminus I_2) \in \Omega.$$

Étant donnés des ensembles non vides $I = \{i_0 > \dots > i_r\} \subset J \subset E$ et un entier $n \geq 0$, on pose

$$\begin{aligned} \Phi(I, J, n) &:= \left(\prod_{j \in J} x_j \right)^{2^n - 1} \left(\prod_{0 \leq \ell < r} \left(\prod_{j \in J \setminus \{i_\ell\}} x_j \right)^{2^{\ell+n}} \right) \\ &\quad \times \left(\prod_{j \in J \setminus \{i_r\}} x_j \right)^{2^{|J|+n} - 2^{r+n}}, \\ \Psi(I, J, n) &:= \left(\prod_{j \in J} x_j \right)^{2^n - 1} x_{i_0}^{2^n} \text{ si } r = 0 \text{ et } |J| = 2 \leq k. \end{aligned}$$

Notre deuxième résultat et la solution générique du problème “hit” est donné par le:

Théorème 2.2. *Soit $d = (2^{m_1} - 1) + (2^{m_2} - 1) + \dots + (2^{m_k} - 1)$ avec $m_k \geq 0$ et $m_{\ell-1} - m_\ell \geq \ell$ pour $2 < \ell \leq k$.*

(i) *Si $k = 1$, alors $\Phi(E, E, m_1) = x_1^{2^{m_1}-1}$ est l'unique générateur non nul du \mathcal{A} -module $\mathbb{F}_2[x_1]$ en degré d . Si $k = 2$ et $m_1 - m_2 = 1$, alors les deux éléments*

$$\begin{aligned} \Psi(\{1\}, E, m_2) &= x_1^{2^{m_1}-1} x_2^{2^{m_2}-1}, \\ \Psi(\{2\}, E, m_2) &= x_1^{2^{m_2}-1} x_2^{2^{m_1}-1}, \end{aligned}$$

forment un système générateur minimal du \mathcal{A} -module $\mathbb{F}_2[x_1, x_2]$ en degré d .

(ii) *Supposons $k > 1$ et $m_1 - m_2 > 1$. Posons*

$$\bar{\Phi}(\omega) := \bar{\Phi}(I_k, J_k, m_k) \prod_{1 < \ell \leq k} \bar{\Phi}(I_{\ell-1}, J_{\ell-1}, m_{\ell-1} - m_\ell - \ell)^{2^{m_\ell + \ell}}$$

pour chaque $\omega \in \Omega$. Alors, l'ensemble $\mathbf{B} := \{\bar{\Phi}(\omega) \mid \omega \in \Omega\}$ forme un système générateur minimal du \mathcal{A} -module \mathbf{P} en degré d . Par conséquent

$$\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d = \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

(iii) *Supposons $k > 2$ et $m_1 - m_2 = 1$. Posons*

$$\begin{aligned} \bar{\Psi}(\bar{\omega}) &:= \bar{\Phi}(I_k, J_k, m_k) \prod_{3 < \ell \leq k} \bar{\Phi}(I_{\ell-1}, J_{\ell-1}, m_{\ell-1} - m_\ell - \ell)^{2^{m_\ell + \ell}} \\ &\quad \times \Psi(I_2, J_2, m_2 - m_3 - 3)^{2^{m_3+3}} \end{aligned}$$

pour chaque $\bar{\omega} \in \bar{\Omega}$. Alors, l'ensemble $\bar{\mathbf{B}} := \{\Psi(\bar{\omega}) \mid \bar{\omega} \in \bar{\Omega}\}$ forme un système générateur minimal du \mathcal{A} -module \mathbf{P} en degré d . Par conséquent

$$\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d = 2 \prod_{3 \leq \ell \leq k} (2^\ell - 1).$$

Remarque 2.3. Signalons qu'une autre écriture des monômes de \mathbf{B} et $\bar{\mathbf{B}}$ pour $k = 3$ est proposée dans [5] [16] [26]. Pour être plus explicite, les trois éléments de \mathbf{B} dans le cas $k = 2$ s'écrivent comme suit:

$$\begin{aligned} \omega_1 &:= (\{1\}, E, \{2\}, \{2\}), & \Phi(\omega_1) &= x_1^{2^{m_2-1}} x_2^{2^{m_1-1}}, \\ \omega_2 &:= (\{2\}, E, \{1\}, \{1\}), & \Phi(\omega_2) &= x_1^{2^{m_1-1}} x_2^{2^{m_2-1}}, \\ \omega_3 &:= (E, E, \{2\}, \{2\}), & \Phi(\omega_3) &= x_1^{2^{m_2+1}-1} x_2^{2^{m_1}-2^{m_2}-1}. \end{aligned}$$

On retrouve donc, sous cette forme, les résultats classiques [44] [58].

3. Démonstration du Théorème 2.1(i)

Pour tout monôme non nul $P \in \mathbf{P}$ et tout $i \in E$, notons $\mu(x_i, P)$ la puissance de x_i dans P . Soit

$$\mu(x_i, P) = 2^0 \mu_0(x_i, P) + 2^1 \mu_1(x_i, P) + 2^2 \mu_2(x_i, P) + \dots$$

(avec $\mu_\ell(x_i, P) \in \{0, 1\}$) le développement 2-adique de $\mu(x_i, P)$.

Définition 3.1. (i) Soit $P \in \mathbf{P}$ un monôme non nul. On appelle étage ℓ -ième de P et on note P_ℓ le monôme

$$P_\ell := \prod_{i \in E} x_i^{\mu_\ell(x_i, P)}.$$

(ii) Soient $m, n \geq 0$ des entiers. On définit $\mathbf{V}(m, n) \subset \mathbf{P}$ comme étant le sous-espace vectoriel engendré par les monômes P tels que

$$\min_{0 \leq \ell < n} \deg P_\ell < k \quad \text{ou} \quad \min_{n \leq \ell < m+n} \deg P_\ell < k - 1.$$

On pose $\mathbf{V}_i(m) := \mathbf{P}(i) \cap \mathbf{V}(m, 0)$ pour chaque $i \in E$.

Remarque 3.2. On a $P = \prod_{\ell > 0} P_\ell^{2^\ell}$, ce qui justifie la Définition 3.1(i). On renvoie à [22] [23] [32] [51] pour des notations analogues. Quant à la Définition 3.1(ii), observons que $\mathbf{V}(0, 0) = \mathbf{V}_i(0) = \{0\}$. On verra dans la Section 6 que $\mathbf{V}(0, n)$ peut être interprété comme le noyau de la puissance n -ième d'un morphisme construit par Kameko [25].

Définition 3.3. Soient $P, Q \in \mathbf{P}$ des éléments quelconques, $m, n \geq 0$ des entiers et $i \in E$. On dit

(i) $P \equiv Q$ ssi $P + Q \in \bar{\mathcal{A}}\mathbf{P}$,

- (ii) $P \equiv Q \pmod{\mathbf{V}(m, n)}$ ssi $P + Q \in \bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(m, n)$,
 (iii) $P \equiv Q \pmod{\mathbf{V}_i(m)}$ ssi $P + Q \in \bar{\mathcal{A}}\mathbf{P} + \mathbf{V}_i(m)$.

Lemme 3.4. Soient $p \geq n \geq 0$ des entiers et $P \in \mathbf{P}$ un élément quelconque.

- (i) Si $P \equiv 0$, alors $QP^{2^n} \equiv 0 \pmod{\mathbf{V}(n, 0)}$ pour tout monôme $Q \in \mathbf{P}$ tel que $Q_\ell = 1 \forall \ell \geq n$.
 (ii) Soit $m \geq 0$ un entier. Si $X^{2^n-1}P^{2^n} \equiv 0 \pmod{\mathbf{V}(m, p)}$, alors $P \equiv 0 \pmod{\mathbf{V}(m, p-n)}$. En particulier $P \equiv 0$ si $m = p-n = 0$.
 (iii) Soit $i \in E$. Supposons $P \in \mathbf{P}(i)$ et $X_i^{2^n-1}P^{2^n} \equiv 0 \pmod{\mathbf{V}_i(p)}$. Alors $P \equiv 0 \pmod{\mathbf{V}_i(p-n)}$. En particulier $P \equiv 0$ si $p = n$.

(cf. [7] [25] [26] [37] [40], où ce lemme est utilisé sous des formes variées.)

Démonstration. (i) Supposons que $P = Sq^1(u_1) + Sq^2(u_2) + \dots$ avec u_1, u_2, \dots des éléments de \mathbf{P} . Rappelons la formule $Sq^{2^i}Sq_0 = Sq_0Sq^i$ (où $Sq_0(u) := Sq^{\deg u}(u) = u^2$ pour tout u) pour l'action de l'algèbre de Steenrod sur les \mathcal{A} -algèbres instables [48]. Puisque \mathbf{P} est une \mathcal{A} -algèbre instable, celle-ci et la formule de Cartan impliquent que

$$Sq^{2^ni}(Qu_i^{2^n}) = Q(Sq^i(u_i))^{2^n} + \sum_{0 < j \leq i} Sq^{j2^n}(Q)(Sq^{i-j}(u_i))^{2^n}$$

pour tout $i > 0$. D'où

$$Q(Sq^i(u_i))^{2^n} \equiv \sum_{0 < j \leq i} Sq^{j2^n}(Q)(Sq^{i-j}(u_i))^{2^n}.$$

Puisque $Q = \prod_{0 \leq \ell < n} Q_\ell^{2^\ell}$ par hypothèse, il s'ensuit que

$$Q(Sq^i(u_i))^{2^n} \equiv \sum_{0 < j \leq i} \sum_{E_j} \prod_{0 \leq \ell < n} (Sq^{j\ell}(Q_\ell))^{2^\ell} (Sq^{i-j}(u_i))^{2^n},$$

où E_j ($0 < j \leq i$) désigne l'ensemble des suites $(j_0, j_1, \dots, j_{n-1})$ d'entiers (≥ 0) tels que $j_0 + j_1 2 + \dots + j_{n-1} 2^{n-1} = j 2^n$.

Soient $0 < j \leq i$ une indice quelconque et $(j_0, j_1, \dots, j_{n-1}) \in E_j$ une suite quelconque. Notons $q \geq 0$ le plus petit entier tel que $j_q > 0$. Alors j_q est un nombre pair, d'où $Sq^{j_q}(Q_q) \in \mathbf{V}(1, 0)$ et

$$\prod_{0 \leq \ell < n} (Sq^{j_\ell}(Q_\ell))^{2^\ell} (Sq^{i-j}(u_i))^{2^n} \in \mathbf{V}(n, 0).$$

Ces arguments montrent que $Q(Sq^i(u_i))^{2^n} \equiv 0 \pmod{\mathbf{V}(n, 0)}$. Par conséquent

$$QP^{2^n} = \sum_{i > 0} Q(Sq^i(u_i))^{2^n} \equiv 0 \pmod{\mathbf{V}(n, 0)}.$$

(ii) Soit $u \in \mathbf{V}(m, p)$ tel que $X^{2^n-1}P^{2^n} + u \equiv 0$. Par hypothèse, on peut trouver des éléments $v \in \mathbf{V}(m, p-n)$, $w \in \mathbf{V}(0, n)$, $v_\ell \in \mathbf{P}$, $w_\ell \in \mathbf{V}(0, n)$ tels que

$$\begin{aligned} u &= X^{2^n-1}v^{2^n} + w, \\ X^{2^n-1}P^{2^n} + u &= \sum_{\ell>0} Sq^\ell(X^{2^n-1}v_\ell^{2^n}) + \sum_{\ell>0} Sq^\ell(w_\ell). \end{aligned}$$

Observons d'abord que $\mathbf{V}(0, n)$ est stable sous l'action de l'algèbre de Steenrod. En particulier, on a

$$\sum_{\ell>0} Sq^\ell(w_\ell) \in \mathbf{V}(0, n).$$

D'autre part, il est facile de vérifier $Sq^i(X^{2^n-1}) \in \mathbf{V}(0, n)$ pour tout $i > 0$. D'où, d'après la formule de Cartan,

$$\begin{aligned} &\sum_{\ell>0} Sq^\ell(X^{2^n-1}v_\ell^{2^n}) + X^{2^n-1} \sum_{\ell>0} Sq^\ell(v_\ell^{2^n}) \\ &= \sum_{\ell>0} \sum_{2^n | (\ell-i) > 0} Sq^i(X^{2^n-1})(Sq^{(\ell-i)/2^n}(v_\ell))^{2^n} \in \mathbf{V}(0, n). \end{aligned}$$

Ces arguments montrent que

$$X^{2^n-1}P^{2^n} = X^{2^n-1}v^{2^n} + X^{2^n-1} \sum_{\ell>0} Sq^\ell(v_\ell^{2^n}),$$

d'où

$$P = v + \sum_{\ell>0} Sq^{\ell/2^n}(v_\ell) \equiv 0 \pmod{\mathbf{V}(m, p-n)}.$$

(iii) Ce lemme n'est autre que le Lemme 3.4(ii) appliqué (avec $m = 0$) à l'algèbre $\mathbf{P}(i)$ au lieu de \mathbf{P} . \square

Lemme 3.5. Soient $m, n \geq 0$ des entiers. Supposons qu'on ait un élément $P_I \in \mathbf{P}(i_r)$ pour chaque sous-ensemble non vide $I = \{i_0 > \dots > i_r\} \subset E$ et que

$$\sum_{\emptyset \neq I \subset E} X^{2^n-1} X(I, |I|)^{2^n} P_I^{2^{n+|I|}} \equiv 0 \pmod{\mathbf{V}(m, n)}.$$

Alors $P_I \equiv 0 \pmod{\mathbf{V}_{i_r}(m - |I|)}$ pour tout sous-ensemble non vide $I \subset E$ tel que $|I| < m$. De plus $P_E \equiv 0$ si $m = k$.

Démonstration. D'abord, par application du Lemme 3.4(ii) on a

$$\sum_{\emptyset \neq I \subset E} X(I, |I|) P_I^{2^{|I|}} \equiv 0 \pmod{\mathbf{V}(m, 0)}.$$

Soit $u \in \mathbf{V}(m, 0)$ un élément tel que

$$\sum_{\emptyset \neq I \subset E} X(I, |I|) P_I^{2^{|I|}} \equiv u. \quad (1)$$

On démontre le lemme par récurrence sur $|I|$. Supposons pour commencer que $I = \{i_0\}$. Soit $\pi : \mathbf{P} \rightarrow \mathbf{P}(i_0) \cong \mathbf{P}/(x_{i_0})$ la projection canonique. Observons que $\pi(\bar{\mathcal{A}}\mathbf{P}) \subset \bar{\mathcal{A}}\mathbf{P}$ et $\pi(\mathbf{V}(m, 0)) \subset \mathbf{V}(m, 0)$. D'autre part, du fait que tous les termes dans la relation (1), sauf $X_{i_0} P_{\{i_0\}}^2$ et u , sont annulés par π , on a $X_{i_0} P_{\{i_0\}}^2 = \pi(X_{i_0} P_{\{i_0\}}^2) \equiv \pi(u)$. Or, par définition $\mathbf{V}_{i_0}(m) = \mathbf{V}(m, 0) \cap \mathbf{P}(i_0)$, il s'ensuit que $X_{i_0} P_{\{i_0\}}^2 \equiv 0 \pmod{\mathbf{V}_{i_0}(m)}$. En appliquant le Lemme 3.4(iii), on obtient $P_{\{i_0\}} \equiv 0 \pmod{\mathbf{V}_{i_0}(m-1)}$.

Supposons maintenant $0 < s < m-1$ et $P_I \equiv 0 \pmod{\mathbf{V}_{i_r}(m-|I|)}$ pour tout $I = \{i_0 > \dots > i_r\} \subset E$ tel que $0 < |I| \leq s$. Soit $J = \{j_0 > \dots > j_s\} \subset E$ un sous-ensemble quelconque. Il faut montrer que $P_J \equiv 0 \pmod{\mathbf{V}_{j_s}(m-|J|)}$.

Soit $\pi_J : \mathbf{P} \rightarrow \mathbf{P}(j_s)$ le morphisme d'algèbres défini par la substitution

$$x_{j_s} := \sum_{\ell \in J \setminus \{j_s\}} x_\ell$$

et qui laisse invariant les autres variables. Il est facile de vérifier que $\pi_J(X_\ell) + X_{j_s} \in \mathbf{V}_{j_s}(1)$ si $\ell \in J$ et $\pi_J(X_\ell) \in \mathbf{V}_{j_s}(1)$ si $\ell \in E \setminus J$.

Soit $I = \{i_0 > \dots > i_r\} \subset E$ un sous-ensemble non vide quelconque. Si $r \geq m-1$, alors $\{i_0, \dots, i_{m-1}\} \cap (E \setminus J) \neq \emptyset$, d'où $\pi_J(X_{i_\ell}) \in \mathbf{V}_{j_s}(1)$ pour un certain $0 \leq \ell < m$. Il en résulte que

$$\begin{aligned} \pi_J(X(I, |I|) P_I^{2^{|I|}}) &= \left(\prod_{0 \leq \ell \leq r} \pi_J(X_{i_\ell})^{2^\ell} \right) \pi_J(P_I)^{2^{|I|}} \\ &\equiv 0 \pmod{\mathbf{V}_{j_s}(m)}. \end{aligned}$$

Si $r < m-1$, alors $\pi_J(X(I, |I|) P_I^{2^{|I|}}) \equiv 0 \pmod{\mathbf{V}_{j_s}(m)}$ sauf si $I \subset J$. De plus, si $I \subset J$ et $I \neq J$, par hypothèse de récurrence on a

$$\begin{aligned} P_I &\equiv 0 \pmod{\mathbf{V}_{i_r}(m-|I|)} \\ &\equiv 0 \pmod{\mathbf{V}(m-|I|, 0)}. \end{aligned}$$

Soit $v \in \mathbf{V}(m-|I|, 0)$ un élément tel que $P_I \equiv v$. Par application du Lemme 3.4(i) on a $X(I, |I|) P_I^{2^{|I|}} \equiv X(I, |I|) v^{2^{|I|}} \pmod{\mathbf{V}(|I|, 0)}$. Clairement $X(I, |I|) v^{2^{|I|}} \in \mathbf{V}(m, 0)$, d'où

$$X(I, |I|) P_I^{2^{|I|}} \equiv 0 \pmod{\mathbf{V}(m, 0)}.$$

Observons que $\pi_J(\bar{\mathcal{A}}\mathbf{P}) \subset \bar{\mathcal{A}}\mathbf{P}$ et $\pi_J(\mathbf{V}(m, 0)) \subset \mathbf{V}_{j_s}(m)$. Il s'ensuit que $\pi_J(X(I, |I|)P_I^{2^{|I|}}) \equiv 0 \pmod{\mathbf{V}_{j_s}(m)}$.

De manière analogue, si $I = J$, on a

$$\begin{aligned} \pi_J(X(J, |J|)P_J^{2^{|J|}}) &= \left(\prod_{0 \leq \ell \leq s} \pi_J(X_{i_\ell})^{2^\ell} \right) \pi_J(P_J)^{2^{|J|}} \\ &\equiv \left(\prod_{0 \leq \ell \leq s} X_{j_s}^{2^\ell} \right) \pi_J(P_J)^{2^{|J|}} \pmod{\mathbf{V}_{j_s}(m)} \\ &\equiv X_{j_s}^{2^{|J|-1}} P_J^{2^{|J|}} \pmod{\mathbf{V}_{j_s}(m)}. \end{aligned}$$

Appliquons π_J aux deux membres de la relation (1). Il résulte des arguments qui précèdent que

$$\begin{aligned} X_{j_s}^{2^{|J|-1}} P_J^{2^{|J|}} &\equiv \pi_J(u) \pmod{\mathbf{V}_{j_s}(m)} \\ &\equiv 0 \pmod{\mathbf{V}_{j_s}(m)}. \end{aligned}$$

D'après le Lemme 3.4(iii), cela implique $P_J \equiv 0 \pmod{\mathbf{V}_{j_s}(m-|J|)}$.

Montrons le reste du lemme. Supposons $m = k$. On a montré plus haut que

$$\sum_{\emptyset \neq I \subset E} X(I, |I|)P_I^{2^{|I|}} \equiv 0 \pmod{\mathbf{V}(k, 0)}.$$

De plus, on a montré que $X(I, |I|)P_I^{2^{|I|}} \equiv 0 \pmod{\mathbf{V}(k, 0)}$ pour tout $|I| < k$, c'est-à-dire pour tout $I \neq E$. Il en résulte que $X(E, k)P_E^{2^k} \equiv 0 \pmod{\mathbf{V}(k, 0)}$.

Soit $\pi_E : \mathbf{P} \rightarrow \mathbf{P}(1)$ le morphisme d'algèbres défini par la substitution $x_1 := x_2 + \dots + x_k$ et qui laisse invariant les autres variables. Il est facile de voir que $\pi_E(X(E, k)P_E^{2^k}) \equiv X_1^{2^k-1}P_E^{2^k} \pmod{\mathbf{V}_1(k)}$, d'où $X_1^{2^k-1}P_E^{2^k} \equiv 0 \pmod{\mathbf{V}_1(k)}$. D'après le Lemme 3.4(iii), cela implique $P_E \equiv 0$. \square

Démonstration du Théorème 2.1(i). Supposons donnée une relation linéaire

$$\sum_{\emptyset \neq I \subset E} X^{2^n-1} X(I, k)^{2^n} P_I^{2^{k+n}} \equiv 0,$$

où P_I est une certaine somme (peut-être vide) d'éléments distincts de $\mathbf{B}(i_r)$ pour chaque sous-ensemble non vide $I = \{i_0 > \dots > i_r\} \subset E$.

Posons $\bar{P}_I := X_{i_r}^{2^{k-|I|-1}} P_I^{2^{k-|I|}}$. Alors

$$\sum_{\emptyset \neq I \subset E} X^{2^n-1} X(I, |I|)^{2^n} \bar{P}_I^{2^{n+|I|}} \equiv 0.$$

Par application du Lemme 3.5 (avec $m = k$), on en déduit que

$$\bar{P}_I \equiv 0 \pmod{\mathbf{V}_{i_r}(k - |I|)}$$

pour tout $\emptyset \neq I \subset E$. D'après le Lemme 3.4(iii), cela implique à son tour $P_I \equiv 0$. Or, $\mathbf{B}(i_r)$ étant \mathcal{A} -linéairement indépendant par hypothèse, il s'ensuit que P_I est la somme vide pour tout $\emptyset \neq I \subset E$. Le Théorème 2.1(i) est démontré. \square

4. Démonstration du Théorème 2.1(ii)

Lemme 4.1. *Soient $m, n \geq 0$ des entiers, $P \in \mathbf{P}$ et $j_\ell \in E$ ($0 \leq \ell < m$) des éléments quelconques, non nécessairement distincts. Alors, il existe un ensemble unique $\emptyset \neq I = \{i_0 > \dots > i_r\} \subset E$ avec $r < m$ tel que $I = \{j_0, \dots, j_{m-1}\}$. De plus, on a la relation*

$$\begin{aligned} & X^{2^n-1} \left(\prod_{0 \leq \ell < m} X_{j_\ell}^{2^{n+\ell}} \right) P^{2^{m+n}} \\ & \equiv X^{2^n-1} X(I, m)^{2^n} P^{2^{m+n}} \pmod{\mathbf{V}(m, n)}. \end{aligned}$$

Démonstration. L'existence et l'unicité de l'ensemble I sont claires. Montrons la relation linéaire. Pour toute suite $J = (j_0, \dots, j_{m-1})$, soit $[J]$ la classe modulo $\mathcal{A}\mathbf{P} + \mathbf{V}(m, n)$ du monôme

$$X^{2^n-1} \left(\prod_{0 \leq \ell < m} X_{j_\ell}^{2^{n+\ell}} \right) P^{2^{m+n}}.$$

Le lemme résulte de la proposition suivante: la classe $[J]$ ne change pas quand on remplace dans J toute partie de la forme

$$(j_{m'}, \dots, j_{m'+n'-1}) = (\underbrace{i, \dots, i}_{n'-1 > 0}, j)$$

par

$$(\underbrace{j, \dots, j}_{n'-1}, i).$$

En effet, il est facile de vérifier que par ces remplacements, on peut obtenir la suite $I = (i_0, \dots, i_{r-1}, \underbrace{i_r, \dots, i_r}_{m-r})$ à partir de la suite $J =$

(j_0, \dots, j_{m-1}) donnée.

Montrons cette proposition. Soient $0 \leq m' < m' + n' - 1 < m$ et $i, j \in E$ deux éléments distincts quelconques. Soient $j_\ell = i$ pour $m' \leq \ell < m' + n' - 1$ et $j_{m'+n'-1} = j$. Posons

$$\begin{aligned} Q & := X^{2^n-1} \prod_{0 \leq \ell < m'} X_{j_\ell}^{2^{n+\ell}}, \\ R & := \left(\prod_{m'+n' \leq \ell < m} X_{j_\ell}^{2^{\ell-m'-n'}} \right) P^{2^{m+n-m'-n'}}. \end{aligned}$$

Il s'agit de montrer

$$\begin{aligned} & Q(X_i^{2^{n'}-1-1} X_j^{2^{n'}-1})^{2^{m'}} R^{2^{m'}+n'} \\ & \equiv Q(X_j^{2^{n'}-1-1} X_i^{2^{n'}-1})^{2^{m'}} R^{2^{m'}+n'} \pmod{\mathbf{V}(m, n)}. \end{aligned}$$

Soit $Y := X/(x_i x_j)$. D'après la formule de Cartan,

$$\begin{aligned} & Sq^1(X^{2^{n'}-1-1} Y^{2^{n'}-1} R^{2^{n'}}) \\ & = (X_i^{2^{n'}-1-1} X_j^{2^{n'}-1} + X_j^{2^{n'}-1-1} X_i^{2^{n'}-1}) R^{2^{n'}} \\ & \quad + \sum_{\ell \in E \setminus \{i, j\}} X_\ell^{2^{n'}-1-1} (Y x_\ell)^{2^{n'}-1} R^{2^{n'}}. \end{aligned}$$

Puisque $Y x_\ell \in \mathbf{V}(1, 0)$ pour tout $\ell \in E \setminus \{i, j\}$, il s'ensuit que

$$Q\left(\sum_{\ell \in E \setminus \{i, j\}} X_\ell^{2^{n'}-1-1} (Y x_\ell)^{2^{n'}-1} R^{2^{n'}}\right)^{2^{m'}} \in \mathbf{V}(m' + n', 0) \subset \mathbf{V}(m, n).$$

D'autre part, d'après le Lemme 3.4(i) on a

$$\begin{aligned} Q(Sq^1(X^{2^{n'}-1-1} Y^{2^{n'}-1} R^{2^{n'}}))^{2^{m'}} & \equiv 0 \pmod{\mathbf{V}(m' + n, 0)} \\ & \equiv 0 \pmod{\mathbf{V}(m, n)}. \end{aligned}$$

Ces arguments impliquent que

$$\begin{aligned} & Q(X_i^{2^{n'}-1-1} X_j^{2^{n'}-1} + X_j^{2^{n'}-1-1} X_i^{2^{n'}-1})^{2^{m'}} R^{2^{m'}+n'} \\ & \equiv 0 \pmod{\mathbf{V}(m, n)}, \end{aligned}$$

d'où la proposition. \square

Rappelons que $\mu(x_1, P)$ désigne la puissance de x_1 dans P pour tout monôme non nul $P \in \mathbf{P}$.

Lemme 4.2. *Soit $P \in \mathbf{P}$ un monôme non nul quelconque. Alors $P \equiv \sum \bar{P}$ pour certains monômes $\bar{P} \in \mathbf{P}$ tels que $\mu(x_1, \bar{P}) = 2^m - 1$ avec $m = \alpha(\mu(x_1, P))$.*

Démonstration. Si $\mu(x_1, P) = 0$, rien n'est à démontrer. Supposons que $\mu(x_1, P) > 0$. Soit $\mu(x_1, P) = 2^{j_0} + \dots + 2^{j_{m-1}}$ ($j_0 < \dots < j_{m-1}$) son développement 2-adique.

Rappelons d'abord la coaction de Milnor [35] (cf. aussi [18])

$$\begin{aligned} \lambda : \mathbb{F}_2[x_1] & \longrightarrow \mathbb{F}_2[x_1] \otimes \mathcal{A}_*, \\ u & \longmapsto \sum_{\xi^J} Sq(J)(u) \otimes \xi^J, \end{aligned}$$

où les produits tensoriels sont pris sur le corps \mathbb{F}_2 , $\mathcal{A}_* = \mathbb{F}_2[\xi_1, \xi_2, \dots]$ est l'algèbre de Steenrod duale, ξ^J parcourt la base monomiale usuelle

de \mathcal{A}_* et $Sq(J) \in \mathcal{A}$ désigne l'élément dual de ξ^J par rapport à cette base. La coaction λ est multiplicative. Elle est déterminée sur le générateur x_1 par la formule

$$\lambda(x_1) = \sum_{n \geq 0} x_1^{2^n} \otimes \xi_n,$$

où par convention $\xi_0 := 1 \in \mathcal{A}_*$.

Posons $\xi^J := \prod_{0 \leq \ell < m} \xi_{j_\ell}^{2^\ell}$. On vérifie aisément que l'expression $x_1^{\mu(x_1, P)} \otimes \xi^J = x_1^{2^{j_0} + \dots + 2^{j_{m-1}}} \otimes \prod_{0 \leq \ell < m} \xi_{j_\ell}^{2^\ell}$ apparaît dans le développement de

$$\lambda(x_1^{2^m - 1}) = \lambda(x_1)^{2^m - 1} = \left(\sum_{n \geq 0} x_1^{2^n} \otimes \xi_n \right)^{2^m - 1}.$$

D'où $x_1^{\mu(x_1, P)} = Sq(J)(x_1^{2^m - 1})$.

Notons $Q := P/x_1^{\mu(x_1, P)}$. Soit χ l'anti-automorphisme canonique de l'algèbre de Steenrod [35] [54]. Rappelons ensuite le suivant, connu sous le nom de “ χ -technique” [43] [54] [58] :

Lemme 4.3. *Soient $u, v \in \mathbf{P}$ et $\theta \in \mathcal{A}$. Alors $\theta(u)v \equiv u\chi(\theta)(v)$.*

Ceci dit, on applique la χ -technique et obtient que

$$P = x_1^{\mu(x_1, P)} Q = Sq(J)(x_1^{2^m - 1}) Q \equiv x_1^{2^m - 1} \chi(Sq(J))(Q),$$

ce qui implique le lemme. \square

Soit Γ l'ensemble des couples (I, P) , où $I \subset E$ est un sous-ensemble non vide et $P \in \mathbf{P}$ est un monôme non nul. Pour tout couple $(I, P) \in \Gamma$, soit $\mu = \mu(I, P)$ la puissance de $x_{\min I}$ dans P .

Définition 4.4. *Soient $(I, P), (J, Q) \in \Gamma$. On dit $(J, Q) < (I, P)$ ssi $(\min J < \min I)$ ou $(\min J = \min I)$ et $\mu(J, Q) < \mu(I, P)$.*

Les deux lemmes qui suivent sont clefs pour la démonstration du Théorème 2.1(ii).

Lemme 4.5. *Soient $n \geq 0$ un entier et $(I, P) \in \Gamma$ un couple quelconque. Supposons $k > 1$ et $\mu = \mu(I, P) > 0$. Alors, sauf dans le cas $I = E$ et $P = x_1$, on a*

$$\begin{aligned} X^{2^n - 1} X(I, k)^{2^n} P^{2^{n+k}} &\equiv \sum X^{2^n - 1} X(J, k)^{2^n} Q^{2^{n+k}} \\ &\quad + \sum X^{2^n - 1} R^{2^n} \pmod{\mathbf{V}(k, n)} \end{aligned}$$

pour certains monômes $R \in \mathbf{P}$ tels que $\alpha(\mu(x_1, R)) = k - 1$ et certains couples $(J, Q) < (I, P)$ dans Γ .

Démonstration. Soit $I = \{i_0 > \dots > i_r\}$. On prouve le lemme par l'examen de 3 cas suivants:

Cas 1. $I \neq E$.

Posons $P' := P/x_{i_r}$. D'après la formule de Cartan, on a

$$\begin{aligned} X_{i_r} P^2 &= X_{i_r} x_{i_r}^2 P'^2 \\ &= Sq^1(X P'^2) + \sum_{i \in E \setminus \{i_r\}} X_i x_i^2 P'^2 \\ &\equiv \sum_{i \in E \setminus \{i_r\}} X_i x_i^2 P'^2. \end{aligned}$$

Par application du Lemme 3.4(i), cela implique que

$$\begin{aligned} &X^{2^n-1} X(I, k)^{2^n} P^{2^{n+k}} \\ &= X^{2^n-1} X(I, k-1)^{2^n} (X_{i_r} P^2)^{2^{n+k-1}} \\ &\equiv X^{2^n-1} X(I, k-1)^{2^n} \left(\sum_{i \in E \setminus \{i_r\}} X_i x_i^2 P'^2 \right)^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum_{i \in E \setminus \{i_r\}} X^{2^n-1} (X(I, k-1) X_i^{2^{k-1}})^{2^n} (x_i P')^{2^{n+k}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

Soit $i \in E \setminus \{i_r\}$ une indice quelconque. Posons $J := I \cup \{i\}$ et $Q := x_i P'$. Il est facile de vérifier que $(J, Q) < (I, P)$. D'après le Lemme 4.1, on a

$$\begin{aligned} &X^{2^n-1} (X(I, k-1) X_i^{2^{k-1}})^{2^n} (x_i P')^{2^{n+k}} \\ &\equiv X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \pmod{\mathbf{V}(k, n)}, \end{aligned}$$

d'où

$$\begin{aligned} &X^{2^n-1} X(I, k)^{2^n} P^{2^{n+k}} \\ &\equiv \sum_{i \in E \setminus \{i_r\}} X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

Cas 2. $I = E$ et $P \neq x_1^\mu$.

Observons d'abord que $m := \alpha(\mu) = \alpha(\mu(x_1, P)) > 0$ par hypothèse. Si $\mu \neq 2^m - 1$, alors $\mu > 2^m - 1$. D'après le Lemme 4.2 on a $P \equiv \sum \bar{P}$ pour certains monômes \bar{P} avec $\mu(x_1, \bar{P}) = 2^m - 1 < \mu$. D'après le Lemme 3.4(i), ceci implique que

$$\begin{aligned} &X^{2^n-1} X(I, k)^{2^n} P^{2^{n+k}} \\ &\equiv X^{2^n-1} X(I, k)^{2^n} \sum \bar{P}^{2^{n+k}} \pmod{\mathbf{V}(n+k, 0)} \\ &\equiv X^{2^n-1} X(I, k)^{2^n} \sum \bar{P}^{2^{n+k}} \pmod{\mathbf{V}(k, n)}, \end{aligned}$$

ce qui entraîne le lemme.

Supposons $\mu = 2^m - 1$. Soit $i > 1$ le plus petit entier tel que $x_i | P$. Posons $P'' := P/x_i$ et $I' := E \setminus \{i\}$. Puisque $I = I' \cup \{i\}$, d'après le Lemme 4.1 on a

$$\begin{aligned} & X^{2^n-1} X(I, k)^{2^n} P^{2^{n+k}} \\ & \equiv X^{2^n-1} X(I', k-1)^{2^n} (X_i P^2)^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

D'après la formule de Cartan

$$\begin{aligned} X_i P^2 &= X_i (x_i P'')^2 \\ &= Sq^1(X P''^2) + \sum_{j \in E \setminus \{i\}} X_j (x_j P'')^2 \\ &\equiv \sum_{j \in E \setminus \{i\}} X_j (x_j P'')^2. \end{aligned}$$

Par application du Lemme 3.4(i), cela implique que

$$\begin{aligned} & X^{2^n-1} X(I', k-1)^{2^n} (X_i P^2)^{2^{n+k-1}} \\ & \equiv \sum_{j \in E \setminus \{i\}} X^{2^n-1} (X(I', k-1) X_j^{2^{k-1}})^{2^n} (x_j P'')^{2^{n+k}} \pmod{\mathbf{V}(k, n)} \\ & \equiv X^{2^n-1} X(I', k)^{2^n} (x_j P'')^{2^{n+k}} \pmod{\mathbf{V}(k, n)}, \end{aligned}$$

ceci étant à cause du Lemme 4.1 et du fait que $I' = I' \cup \{j\}$ pour tout $j \in E \setminus \{i\}$.

Soit $j \in E \setminus \{i\}$ une indice quelconque. Si $j > 1$, alors $\mu(I', x_j P'') = \mu$. Puisque $I' \neq E$, le Cas 1 précédent implique que

$$\begin{aligned} & X^{2^n-1} X(I', k)^{2^n} (x_j P'')^{2^{n+k}} \\ & \equiv \sum X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \pmod{\mathbf{V}(k, n)} \end{aligned}$$

pour certains couples $(J, Q) < (I', x_j P'')$. Il suit du fait $\min I' = 1$ que $\min J = \min I'$ pour tout couple (J, Q) dans cette somme. D'où $\mu(J, Q) < \mu(I', x_j P'') = \mu$ et $(J, Q) < (I, P)$.

Si $j = 1$, alors $\mu(x_1, x_j P'') = \mu + 1 = 2^m$ et

$$\begin{aligned} \alpha(\mu(x_1, X(I', k)(x_j P'')^{2^k})) &= \alpha(\mu(x_1, X(I', k))) + \alpha(\mu(x_1, x_j P'')) \\ &= \alpha(\mu(x_1, X(I', k))) + 1 \\ &= k - 1. \end{aligned}$$

On conclut en posant $R := X(I', k)(x_1 P'')^{2^k}$.

Cas 3. $I = E$ et $P = x_1^\mu$ avec $\mu > 1$.

Ce cas-ci étant plus calculatoire que les autres, nous n'en avons pas trouvé une démonstration plus compacte. Observons tout de suite qu'on peut toujours supposer que $\mu = 2^m - 1$ avec $m = \alpha(\mu) > 1$ (voir le début du Cas 2).

Posons $\bar{I} := E \setminus \{1\}$. D'après la formule de Cartan, on a

$$\begin{aligned} X_1 x_1^{2\mu} &= Sq^1(X x_1^{2\mu-2}) + \sum_{i \in E \setminus \{1\}} X_i x_i^2 x_1^{2\mu-2} \\ &\equiv \sum_{i \in E \setminus \{1\}} X_i x_i^2 x_1^{2\mu-2}. \end{aligned}$$

Par application du Lemme 3.4(i), cela implique que

$$\begin{aligned} &X^{2^n-1} X(\bar{I}, k)^{2^n} P^{2^{n+k}} \\ &= X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_1 x_1^{2\mu})^{2^{n+k-1}} \\ &\equiv X^{2^n-1} X(\bar{I}, k-1)^{2^n} \left(\sum_{i \in E \setminus \{1\}} X_i x_i^2 x_1^{2\mu-2} \right)^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum_{i \in E \setminus \{1\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_i x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)}, \end{aligned}$$

ceci étant à cause du Lemme 4.1 et du fait que $\bar{I} = \bar{I} \cup \{i\} \forall i \in E \setminus \{1\}$.

Considérons le terme qui correspond à l'indice $i = 2$. Il est clair que $x_2 x_1^{\mu-1} \equiv x_2^2 x_1^{\mu-2}$. Il en résulte d'après le Lemme 3.4(i) que

$$\begin{aligned} &X^{2^n-1} X(\bar{I}, k)^{2^n} (x_2 x_1^{\mu-1})^{2^{n+k}} \\ &\equiv X^{2^n-1} X(\bar{I}, k)^{2^n} (x_2^2 x_1^{\mu-2})^{2^{n+k}} \pmod{\mathbf{V}(k, n)} \\ &\equiv X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_2 x_2^4 x_1^{2\mu-4})^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

D'autre part, d'après la formule de Cartan, on a

$$\begin{aligned} X_2 x_2^4 x_1^{2\mu-4} &= Sq^1(X x_2^2 x_1^{2\mu-4}) + \sum_{j \in E \setminus \{2\}} X_j x_j^2 x_2^2 x_1^{2\mu-4} \\ &\equiv \sum_{j \in E \setminus \{2\}} X_j x_j^2 x_2^2 x_1^{2\mu-4}. \end{aligned}$$

Par application du Lemme 3.4(i), cela implique que

$$\begin{aligned} &X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_2 x_2^4 x_1^{2\mu-4})^{2^{n+k-1}} \\ &\equiv X^{2^n-1} X(\bar{I}, k-1)^{2^n} \sum_{j \in E \setminus \{2\}} (X_j x_j^2 x_2^2 x_1^{2\mu-4})^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum_{j \in E \setminus \{1,2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_j x_2 x_1^{\mu-2})^{2^{n+k}} \\ &\quad + X^{2^n-1} X(E, k)^{2^n} (x_2 x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)}, \end{aligned}$$

ceci étant à cause du Lemme 4.1 et du fait que $\bar{I} \cup \{j\} = \bar{I}$ pour toute indice $j \in E \setminus \{1, 2\}$ et $\bar{I} \cup \{j\} = E$ pour $j = 1$.

Puisque $\min \bar{I} = 2$, pour toute indice $j \in E \setminus \{1, 2\}$ on a

$$\begin{aligned} & X^{2^n-1} X(\bar{I}, k)^{2^n} (x_j x_2 x_1^{\mu-2})^{2^{n+k}} \\ &= X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_2 x_j^2 x_2^2 x_1^{2\mu-4})^{2^{n+k-1}}. \end{aligned}$$

D'après la formule de Cartan:

$$\begin{aligned} X_2 x_j^2 x_2^2 x_1^{2\mu-4} &= Sq^1(X x_j^2 x_1^{2\mu-4}) + \sum_{\ell \in E \setminus \{2\}} X_\ell x_\ell^2 x_j^2 x_1^{2\mu-4} \\ &\equiv \sum_{\ell \in E \setminus \{2\}} X_\ell x_\ell^2 x_j^2 x_1^{2\mu-4}. \end{aligned}$$

Par application du Lemme 3.4(i), ceci implique que

$$\begin{aligned} & X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_2 x_j^2 x_2^2 x_1^{2\mu-4})^{2^{n+k-1}} \\ &\equiv \sum_{\ell \in E \setminus \{2\}} X^{2^n-1} X(\bar{I}, k-1)^{2^n} (X_\ell x_\ell^2 x_j^2 x_1^{2\mu-4})^{2^{n+k-1}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum_{\ell \in E \setminus \{1, 2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_\ell x_j x_1^{\mu-2})^{2^{n+k}} \\ &\quad + X^{2^n-1} X(E, k)^{2^n} (x_j x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

Prenant la somme sur toutes les indices $j \in E \setminus \{1, 2\}$, on a

$$\begin{aligned} & \sum_{j \in E \setminus \{1, 2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_j x_2 x_1^{\mu-2})^{2^{n+k}} \\ &\equiv \sum_{j \in E \setminus \{1, 2\}} \sum_{\ell \in E \setminus \{1, 2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_\ell x_j x_1^{\mu-2})^{2^{n+k}} \\ &\quad + \sum_{j \in E \setminus \{1, 2\}} X^{2^n-1} X(E, k)^{2^n} (x_j x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum_{j \in E \setminus \{1, 2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_j^2 x_1^{\mu-2})^{2^{n+k}} \\ &\quad + \sum_{j \in E \setminus \{1, 2\}} X^{2^n-1} X(E, k)^{2^n} (x_j x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)}. \end{aligned}$$

En résumé, on obtient la relation suivante:

$$\begin{aligned} & X^{2^n-1} X(I, k)^{2^n} P^{2^{n+k}} \\ &\equiv \sum_{i \in E \setminus \{1, 2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_i x_1^{\mu-1})^{2^{n+k}} \end{aligned}$$

$$\begin{aligned}
 &+ \sum_{j \in E \setminus \{1,2\}} X^{2^n-1} X(\bar{I}, k)^{2^n} (x_j^2 x_1^{\mu-2})^{2^{n+k}} \\
 &+ \sum_{j \in E \setminus \{1,2\}} X^{2^n-1} X(E, k)^{2^n} (x_j x_1^{\mu-1})^{2^{n+k}} \\
 &+ X^{2^n-1} X(E, k)^{2^n} (x_2 x_1^{\mu-1})^{2^{n+k}} \pmod{\mathbf{V}(k, n)}.
 \end{aligned}$$

Observons que $x_i x_1^{\mu-1} \equiv x_i^2 x_1^{\mu-2}$ pour tout $i \in E \setminus \{1,2\}$. Il suit de là d'après le Lemme 3.4(i) que la somme de deux premiers termes dans le membre de droite de cette relation est nulle modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$. Pour les deux termes qui restent, il suffit de retourner au Cas 2 pour conclure. □

Lemme 4.6. *Supposons $n \geq 0$ et $1 < k \leq 4$. Alors*

$$\begin{aligned}
 X^{2^n-1} X(E, k)^{2^n} x_1^{2^{n+k}} &\equiv \sum X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \\
 &+ \sum X^{2^n-1} R^{2^n} \pmod{\mathbf{V}(k, n)}
 \end{aligned}$$

pour certains monômes $R \in \mathbf{P}$ tels que $\alpha(\mu(x_1, R)) < k$ et certains couples $(J, Q) \in \Gamma$ tels que $\mu(J, Q) = 0$.

Démonstration. En fait, on a la relation

$$X^{2^n-1} X(E, k)^{2^n} x_1^{2^{n+k}} \equiv X^{2^n-1} X(E, k)^{2^n} (x_2 + \cdots + x_k)^{2^{n+k}},$$

qui est démontrée dans [25] [40] pour $k \leq 3$. Il suffit donc de montrer le lemme pour $k = 4$. Notons que ce cas-ci n'est pas indispensable pour la démonstration du Théorème 2.2, mais il est essentiel pour celle [41] de l'analogie du résultat principal de [7] dont nous avons parlé dans l'Introduction. Ajoutons que les arguments qui suivent peuvent être légèrement modifiés pour s'adapter au cas $k \leq 3$.

Soit $\mathbf{V} \subset \mathbf{P}$ le sous-espace vectoriel engendré par les monômes $X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}}$ avec $\mu(J, Q) = 0$ et les monômes $X^{2^n-1} R^{2^n}$ avec $\alpha(\mu(x_1, R)) < k$. (On s'apercevra que les générateurs dans le Théorème 2.1 sont précisément ceux de \mathbf{V} .) Si $P, P' \in \mathbf{P}$, définissons $P \equiv P' \pmod{\mathbf{V}}$ comme étant la relation $P + P' \in \mathbf{V} + \bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$. Il s'agit alors de montrer que

$$X^{2^n-1} X(E, k)^{2^n} x_1^{2^{n+k}} \equiv 0 \pmod{\mathbf{V}}.$$

Rappelons que $X(E, 4) = X_4 X_3^2 X_2^4 X_1^8$. Il est clair que $X_1 x_1^2 = Sq^1(X) + X_2 x_2^2 + X_3 x_3^2 + X_4 x_4^2 \equiv X_2 x_2^2 + X_3 x_3^2 + X_4 x_4^2$. D'après les

Lemmes 3.4(i) et 4.1, on a

$$\begin{aligned}
& X^{2^n-1} X(E, 4)^{2^n} x_1^{2^{n+4}} \\
&= X^{2^n-1} (X_4 X_3^2 X_2^4)^{2^n} (X_1 x_1^2)^{2^{n+3}} \\
&\equiv X^{2^n-1} (X_4 X_3^2 X_2^4)^{2^n} (X_2 x_2^2 + X_3 x_3^2 + X_4 x_4^2)^{2^{n+3}} \pmod{\mathbf{V}(4, n)} \\
&\equiv X^{2^n-1} (X_4 X_3^2 X_2^{12})^{2^n} (x_2 + x_3 + x_4)^{2^{n+4}} \pmod{\mathbf{V}(4, n)} \\
&\equiv X^{2^n-1} (X_4 X_3^2)^{2^n} (X_2^3 x_2^4)^{2^{n+2}} \pmod{\mathbf{V}}.
\end{aligned}$$

D'après la formule de Cartan, on a

$$\begin{aligned}
X_2^3 x_2^4 &= Sq^1(X^3) + X_1^3 x_1^4 + X_3^3 x_3^4 + X_4^3 x_4^4 \\
&\equiv X_1^3 x_1^4 + X_3^3 x_3^4 + X_4^3 x_4^4.
\end{aligned}$$

Par application du Lemme 3.4(i), cela implique que

$$\begin{aligned}
& X^{2^n-1} (X_4 X_3^2)^{2^n} (X_2^3 x_2^4)^{2^{n+2}} \\
&\equiv X^{2^n-1} (X_4 X_3^2)^{2^n} (X_1^3 x_1^4 + X_3^3 x_3^4 + X_4^3 x_4^4)^{2^{n+2}} \pmod{\mathbf{V}(4, n)} \\
&\equiv X^{2^n-1} X_4^{2^n} (X_3^7 x_3^8)^{2^{n+1}} \pmod{\mathbf{V}},
\end{aligned}$$

ceci étant à cause du Lemme 4.1 et du fait que

$$\alpha(\mu(x_1, X_4 X_3^2 X_1^{12} x_1^{16})) = 3 < k = 4.$$

Appliquons encore la formule de Cartan:

$$\begin{aligned}
X_3^7 x_3^8 &= Sq^1(X^7) + X_1^7 x_1^8 + X_2^7 x_2^8 + X_4^7 x_4^8 \\
&\equiv X_1^7 x_1^8 + X_2^7 x_2^8 + X_4^7 x_4^8.
\end{aligned}$$

D'après le Lemme 3.4(i), on a

$$\begin{aligned}
& X^{2^n-1} X_4^{2^n} (X_3^7 x_3^8)^{2^{n+1}} \\
&\equiv X^{2^n-1} X_4^{2^n} (X_1^7 x_1^8 + X_2^7 x_2^8 + X_4^7 x_4^8)^{2^{n+1}} \pmod{\mathbf{V}(4, n)} \\
&\equiv X^{2^n-1} (X_4 X_2^6)^{2^n} (X_2 x_2^2)^{2^{n+3}} + X^{2^n-1} (X_4^{15} x_4^{16})^{2^n} \pmod{\mathbf{V}}.
\end{aligned}$$

Observons que $X_2 x_2^2 \equiv X_1 x_1^2 + X_3 x_3^2 + X_4 x_4^2$. Il s'ensuit d'après les Lemmes 3.4(i) et 4.1 que

$$\begin{aligned}
& X^{2^n-1} (X_4 X_2^6)^{2^n} (X_2 x_2^2)^{2^{n+3}} \\
&\equiv X^{2^n-1} (X_4 X_2^6)^{2^n} (X_1 x_1^2 + X_3 x_3^2 + X_4 x_4^2)^{2^{n+3}} \pmod{\mathbf{V}(4, n)} \\
&\equiv X^{2^n-1} X_4^{2^n} (X_2 X_1^6 x_1^8 + X_3 X_2^6 x_3^8 + X_2^7 x_4^8)^{2^{n+1}} \pmod{\mathbf{V}(4, n)} \\
&\equiv 0 \pmod{\mathbf{V}}.
\end{aligned}$$

En résumé, on a montré jusqu'ici que

$$X^{2^n-1} X(E, 4)^{2^n} x_1^{2^{n+4}} \equiv X^{2^n-1} (X_4^{15} x_4^{16})^{2^n} \pmod{\mathbf{V}}.$$

Pour l'examen de ce dernier terme, appliquons la formule de Cartan:

$$\begin{aligned} X_4^{15}x_4^{16} &= Sq^1(X^{15}) + X_1^{15}x_1^{16} + X_2^{15}x_2^{16} + X_3^{15}x_3^{16} \\ &\equiv X_1^{15}x_1^{16} + X_2^{15}x_2^{16} + X_3^{15}x_3^{16}. \end{aligned}$$

D'après le Lemme 3.4(i), on a

$$\begin{aligned} &X^{2^n-1}(X_4^{15}x_4^{16})^{2^n} \\ &\equiv X^{2^n-1}(X_1^{15}x_1^{16} + X_2^{15}x_2^{16} + X_3^{15}x_3^{16})^{2^n} \pmod{\mathbf{V}(4, n)} \\ &\equiv X^{2^n-1}(X_2^7)^{2^n}(X_2x_2^2)^{2^{n+3}} + X^{2^n-1}(X_3^7)^{2^n}(X_3x_3^2)^{2^{n+3}} \pmod{\mathbf{V}}. \end{aligned}$$

Puisque $X_2x_2^2 \equiv X_1x_1^2 + X_3x_3^2 + X_4x_4^2$, d'après les Lemmes 3.4(i) et 4.1 on a

$$\begin{aligned} &X^{2^n-1}(X_2^7)^{2^n}(X_2x_2^2)^{2^{n+3}} \\ &\equiv X^{2^n-1}(X_2^7)^{2^n}(X_1x_1^2 + X_3x_3^2 + X_4x_4^2)^{2^{n+3}} \pmod{\mathbf{V}(4, n)} \\ &\equiv X^{2^n-1}(X_2X_1^{14}x_1^{16} + X_3X_2^{14}x_3^{16} + X_4X_2^{14}x_4^{15})^{2^n} \pmod{\mathbf{V}(4, n)} \\ &\equiv 0 \pmod{\mathbf{V}}. \end{aligned}$$

De manière analogue, en utilisant le fait $X_3x_3^2 \equiv X_1x_1^2 + X_2x_2^2 + X_4x_4^2$ et les Lemmes 3.4(i) et 4.1, on obtient que

$$\begin{aligned} &X^{2^n-1}(X_3^7)^{2^n}(X_3x_3^2)^{2^{n+3}} \\ &\equiv X^{2^n-1}(X_3^7)^{2^n}(X_1x_1^2 + X_2x_2^2 + X_4x_4^2)^{2^{n+3}} \pmod{\mathbf{V}(4, n)} \\ &\equiv X^{2^n-1}(X_3X_1^{14}x_1^{16} + X_3X_2^{14}x_2^{16} + X_4X_3^{14}x_4^{15})^{2^n} \pmod{\mathbf{V}(4, n)} \\ &\equiv X^{2^n-1}(X_3X_2^6)^{2^n}(X_2x_2^2)^{2^{n+3}} \pmod{\mathbf{V}} \\ &\equiv X^{2^n-1}(X_3X_2^6)^{2^n}(X_1x_1^2 + X_3x_3^2 + X_4x_4^2)^{2^{n+3}} \pmod{\mathbf{V}} \\ &\equiv X^{2^n-1}(X_3X_2^2X_1^{12}x_1^{16} + X_3X_2^{14}x_3^{16} + X_4X_3^2X_2^{12}x_4^{16})^{2^n} \pmod{\mathbf{V}} \\ &\equiv 0 \pmod{\mathbf{V}}. \end{aligned}$$

Le lemme est complètement démontré. \square

Démonstration du Théorème 2.1(ii). D'après le Lemme 4.2, pour montrer qu'en degré d , le \mathcal{A} -module \mathbf{P} est engendré par l'ensemble \mathbf{B} , il suffit de montrer que: modulo $\bar{\mathcal{A}}\mathbf{P}$, tout monôme $P \in \mathbf{P}$ tel que $\deg P = d$ et $\mu(x_1, P) = 2^m - 1$ ($m \geq 0$ un entier) est engendré par \mathbf{B} sur \mathbb{F}_2 .

Soit P un tel monôme. Montrons d'abord que modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, P est engendré par \mathbf{B} sur \mathbb{F}_2 . Ceci est clair si $P \in \mathbf{V}(k, n)$. Supposons $P \notin \mathbf{V}(k, n)$. Rappelons que $\mathbf{V}(k, n)$ désigne l'espace vectoriel engendré par les monômes P tels que

$$\min_{0 \leq \ell < n} \deg P_\ell < k \quad \text{ou} \quad \min_{n \leq \ell < n+k} \deg P_\ell < k - 1.$$

Il suit du fait

$$d = \sum_{\ell \geq 0} 2^\ell \deg P_\ell \equiv 2^n - k \pmod{2^{n+k}}$$

que $\deg P_\ell = k$ pour $0 \leq \ell < n$ et $\deg P_\ell = k - 1$ pour $n \leq \ell < n + k$. D'où $P_\ell = X$ pour $0 \leq \ell < n$ et il existe un unique ensemble non vide $I = \{i_0 > \dots > i_r\} \subset E$ tel que $\{P_\ell \mid n \leq \ell < n + k\} = \{X_{i_0}, \dots, X_{i_r}\}$. Posons

$$\bar{P} := \prod_{\ell \geq n+k} P_\ell^{2^{\ell-n-k}}.$$

Alors $\deg \bar{P} = d'$ et par application du Lemme 4.1 :

$$P \equiv X^{2^n-1} X(I, k)^{2^n} \bar{P}^{2^{n+k}} \pmod{\mathbf{V}(k, n)}.$$

Si $\mu(I, \bar{P}) = 0$ ou $m = \alpha(\mu(x_1, P)) < n + k$, alors $\bar{P} \in \mathbf{P}(i_r)$. Par hypothèse, \bar{P} étant engendré par $\mathbf{B}(i_r)$, on a $\bar{P} \equiv \sum Q$ pour certains éléments $Q \in \mathbf{B}(i_r)$. D'après le Lemme 3.4(i),

$$\begin{aligned} P &\equiv X^{2^n-1} X(I, k)^{2^n} \bar{P}^{2^{n+k}} \pmod{\mathbf{V}(k, n)} \\ &\equiv \sum X^{2^n-1} X(I, k)^{2^n} Q^{2^{n+k}} \pmod{\mathbf{V}(n+k, 0)}. \end{aligned}$$

Puisque $\mathbf{V}(n+k, 0) \subset \mathbf{V}(k, n)$, il s'ensuit que modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, le monôme P est engendré par \mathbf{B} sur \mathbb{F}_2 .

Supposons maintenant que $\mu(I, \bar{P}) > 0$ et $m \geq n+k$. On va raisonner par l'absurde. Supposons le contraire qu'il existe des monômes P qui, modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, ne soient pas engendrés par \mathbf{B} sur \mathbb{F}_2 . Soit P un tel monôme avec (I, \bar{P}) minimal par rapport à la relation $<$ dans Γ définie plus haut. Si $I \neq E$ ou $\bar{P} \neq x_1$, alors d'après le Lemme 4.5 :

$$\begin{aligned} X^{2^n-1} X(I, k)^{2^n} \bar{P}^{2^{n+k}} &\equiv \sum X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \\ &\quad + \sum X^{2^n-1} R^{2^n} \pmod{\mathbf{V}(k, n)} \end{aligned}$$

pour certains monômes $R \in \mathbf{P}$ tels que $\alpha(\mu(x_1, R)) = k - 1$, et certains couples $(J, Q) < (I, \bar{P})$ dans Γ . Puisque $\alpha(\mu(x_1, X^{2^n-1} R^{2^n})) = n + k - 1 < n + k$, d'après ce qui précède, $X^{2^n-1} R^{2^n}$ est engendré par \mathbf{B} pour tout R dans le membre de droite. D'autre part, à cause de la minimalité du couple (I, \bar{P}) , modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, tous les monômes qui restent dans le membre de droite sont engendrés par \mathbf{B} . Il en est donc de même de l'autre membre et de P , ce qui est une contradiction !

Si $I = E$ et $\bar{P} = x_1$, alors $k \leq 4$. (Rappelons que $\alpha(k-1) = \alpha(d'+k-2) \geq k-2$ par hypothèse!) D'après le Lemme 4.6, on a

$$\begin{aligned} X^{2^n-1} X(I, k)^{2^n} \bar{P}^{2^{n+k}} &\equiv \sum X^{2^n-1} X(J, k)^{2^n} Q^{2^{n+k}} \\ &\quad + \sum X^{2^n-1} R^{2^n} \pmod{\mathbf{V}(k, n)} \end{aligned}$$

pour certains monômes $R \in \mathbf{P}$ tels que $\alpha(\mu(x_1, R)) < k$, et certains couples $(J, Q) \in \Gamma$ tels que $\mu(J, Q) = 0$. Vu ce qui précède, modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, tous les termes dans cette écriture sont engendrés par \mathbf{B} sur \mathbb{F}_2 . D'où P l'est, ce qui est encore une contradiction!

On a montré que modulo $\bar{\mathcal{A}}\mathbf{P} + \mathbf{V}(k, n)$, le monôme P est engendré par l'ensemble \mathbf{B} sur \mathbb{F}_2 . Le Théorème 2.1(ii) résulte maintenant de la proposition suivante:

Proposition 4.7. *Si $0 \leq m \leq k$ et $0 \leq n' \leq n$, alors $\mathbf{V}(m, n') \subset \bar{\mathcal{A}}\mathbf{P}$ en degré d . En particulier, les relations $P \equiv Q$ et $P \equiv Q \pmod{\mathbf{V}(k, n)}$ sont équivalentes en degré d . (On trouve des variantes de cette proposition dans [25] [37].)*

Montrons cette proposition par récurrence sur $m + n'$. Il n'y a rien à faire si $m + n' = 0$. Supposons $m + n' > 0$ et qu'elle est vraie pour toute valeur inférieure de $m + n'$. Soit $R \in \mathbf{V}(m, n')$ un monôme quelconque. Supposons d'abord $R \in \mathbf{V}(0, m+n') \cap \mathbf{V}(0, n)$. Soit $q \geq 0$ le plus petit entier tel que l'étage q -ième $R_q \neq X$. Par définition $q < \min\{n, m+n'\}$. Posons

$$\bar{R} := \prod_{\ell \geq q} R_\ell^{\ell-q},$$

alors $2^q \deg \bar{R} = d - (2^q - 1)k$, d'où

$$\deg \bar{R} + k = (d+k)/2^q = 2^{n+k-q}(d'+k-1) + 2^{n-q}.$$

À ce point, rappelons le:

Théorème 4.8 (Wood [56]). *Soit $P \in \mathbf{P}$ un monôme. Alors $P \equiv 0$ si $\alpha(\deg P + \deg P_0) > \deg P_0$.*

Puisque $\deg \bar{R}_0 = \deg R_q < k$ et $q < n$, il s'ensuit que $\deg \bar{R}_0 \equiv k \pmod{2}$ et $\deg \bar{R}_0 \leq k-2$. Observons que $n > 0$ dans le cas qu'on considère. D'où $\alpha(d'+k-1) = k-1 > 0$ par hypothèse. On en déduit sans peine que $\alpha(\deg \bar{R} + \deg \bar{R}_0) > \deg \bar{R}_0$ (voir la Section 6). D'après le Théorème 4.8, le monôme $\bar{R} \equiv 0$. Par application du Lemme 3.4(i), on a

$$R = \left(\prod_{0 \leq \ell < q} R_\ell^{2^\ell} \right) \bar{R}^{2^q} \equiv 0 \pmod{\mathbf{V}(q, 0)}.$$

Il est clair que $\mathbf{V}(q, 0) \subset \mathbf{V}(0, q)$. Du fait que $q < m + n'$, par hypothèse de récurrence $\mathbf{V}(0, q) \subset \bar{\mathcal{A}}\mathbf{P}$. D'où $\tilde{R} \equiv 0$.

Supposons maintenant $R \notin \mathbf{V}(0, m + n') \cap \mathbf{V}(0, n)$. Ceci implique que $m + n' > n$ et $R \notin \mathbf{V}(0, n)$, car $\mathbf{V}(m, n') \subset \mathbf{V}(0, m + n')$. D'où $R_\ell = X$ pour $0 \leq \ell < n$. Soit $s \geq 0$ le plus petit entier tel que $\deg R_s < k - 1$. Par définition $n \leq s < m + n' \leq n + k$. Il est facile de vérifier que $\deg R_\ell = k - 1$ pour $n \leq \ell < s$. Posons

$$\tilde{R} := \prod_{\ell \geq s} R_\ell^{\ell-s}.$$

alors $2^s \deg \tilde{R} = d - (2^n - 1)k - (2^s - 2^n)(k - 1)$, d'où

$$\deg \tilde{R} + k - 1 = (d + k - 2^n)/2^s = 2^{n+k-s}(d' + k - 1).$$

Puisque $\deg \tilde{R}_0 = \deg R_s < k - 1$ et $s < n + k$, il s'ensuit que $\deg \tilde{R}_0 \equiv k - 1 \pmod{2}$ et $\deg \tilde{R}_0 \leq k - 3$. Du fait que soit $\alpha(d' + k - 1) = k - 1$, soit $\alpha(d' + k - 2) \geq k - 2 > 0$, on vérifie aisément que $\alpha(\deg \tilde{R} + \deg \tilde{R}_0) > \deg \tilde{R}_0$ (voir la Section 6). D'après le Théorème 4.8, le monôme $\tilde{R} \equiv 0$. Par application du Lemme 3.4(i), on a

$$R = \left(\prod_{0 \leq \ell < s} R_\ell^{2^\ell} \right) \tilde{R}^{2^s} \equiv 0 \pmod{\mathbf{V}(s, 0)}.$$

Il est clair que $\mathbf{V}(s, 0) \subset \mathbf{V}(0, s)$. Du fait que $s < m + n'$, par hypothèse de récurrence $\mathbf{V}(0, s) \subset \bar{\mathcal{A}}\mathbf{P}$. D'où de nouveau $R \equiv 0$. \square

5. Démonstration du Théorème 2.2

Le Théorème 2.2(i) est classique, on renvoie à [25] [40] [44] [58] etc. pour les détails.

La première partie du Théorème 2.2(ii) se vérifie facilement par récurrence à partir du cas $k = 1$ du Théorème 2.2(i). Il en est de même de la première partie du Théorème 2.2(iii), qui se démontre par récurrence à partir du cas $k = 2$ du Théorème 2.2(i).

Il reste à vérifier les affirmations concernant $\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d$ dans ces théorèmes. Il est facile de voir que $|\mathbf{B}|$ est égal au nombre de suites $(I_k, I_{k-1}, \dots, I_1)$. Il y a $2^k - 1$ choix de I_k . Une fois I_k choisi, il ne reste que $2^{k-1} - 1$ choix de I_{k-1} . Si I_k et I_{k-1} ont déjà été choisis, il ne reste que $2^{k-2} - 1$ choix de I_{k-2} et ainsi de suite. D'où

$$|\mathbf{B}| = \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

En raisonnant de la même manière, on obtient

$$|\bar{\mathbf{B}}| = 2 \prod_{3 \leq \ell \leq k} (2^\ell - 1).$$

□

6. Remarques finales

6.1. Exemples

Nous tenons d'abord à signaler que l'idée d'une base de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ pour $k = 3$ a déjà été conçue dans notre mémoire [40]. À ce moment-là (1999), le problème "hit" général nous semblait inaccessible et l'idée d'une construction générique nous était inconcevable. Par chance, nous avons réussi au fil du temps à généraliser notre construction du moment et formuler ainsi le Théorème 2.1. Les exemples qui suivent expliciteront ce théorème dans le cas $2 \leq k \leq 4$.

Soient $n \geq 0$, $d' \geq 0$ et $d := 2^{n+k}(d' + k - 1) + 2^n - k$. Donnons-nous un système générateur minimal quelconque $\mathbf{B}[x_1, \dots, x_{k-1}]$ du \mathcal{A} -module $\mathbb{F}_2[x_1, \dots, x_{k-1}]$ en degré d' . Supposons que soit $\alpha(d' + k - 1) = k - 1 > 0$, soit $(n = 0 \text{ et } \alpha(d' + k - 2) \geq k - 2 > 0)$. Alors, l'ensemble des produits $(x_1 x_2 \cdots x_k)^{2^n - 1} P^{2^n}$, où P parcourt les éléments suivants, forme un système générateur minimal du \mathcal{A} -module $\mathbb{F}_2[x_1, x_2, \dots, x_k]$ en degré d (pour être plus commode, les variables s'écriront x, y, z, t au lieu de x_1, x_2, x_3, x_4) :

Pour $k = 2$:

- (I) $x^3 Q^4$, où $Q \in \mathbf{B}[x]$,
- (II) $y^3 Q^4$, $xy^2 Q^4$, où $Q \in \mathbf{B}[y]$.

Pour $k = 3$:

- (I) $(xy)^7 Q^8$, où $Q \in \mathbf{B}[x, y]$,
- (II) $(xz)^7 Q^8$, $(xy)(xz)^6 Q^8$, où $Q \in \mathbf{B}[x, z]$,
- (III) $(yz)^7 Q^8$, $(xy)(yz)^6 Q^8$, $(xz)(yz)^6 Q^8$,
 $(xy)(xz)^2 (yz)^4 Q^8$, où $Q \in \mathbf{B}[y, z]$.

Pour $k = 4$:

- (I) $(xyz)^{15} Q^{16}$, où $Q \in \mathbf{B}[x, y, z]$,
- (II) $(xyt)^{15} Q^{16}$, $(xyz)(xyt)^{14} Q^{16}$, où $Q \in \mathbf{B}[x, y, t]$,
- (III) $(xzt)^{15} Q^{16}$, $(xyz)(xzt)^{14} Q^{16}$, $(xyt)(xzt)^{14} Q^{16}$,
 $(xyz)(xyt)^2 (xzt)^{12} Q^{16}$, où $Q \in \mathbf{B}[x, z, t]$,
- (IV) $(yzt)^{15} Q^{16}$, $(xyz)(yzt)^{14} Q^{16}$, $(xyt)(yzt)^{14} Q^{16}$,
 $(xzt)(yzt)^{14} Q^{16}$, $(xyz)(xyt)^2 (yzt)^{12} Q^{16}$,
 $(xyz)(xzt)^2 (yzt)^{12} Q^{16}$, $(xyt)(xzt)^2 (yzt)^{12} Q^{16}$,
 $(xyz)(xyt)^2 (xzt)^4 (yzt)^8 Q^{16}$, où $Q \in \mathbf{B}[y, z, t]$.

6.2. Une propriété arithmétique

Soit $m \geq 2$ un entier. La propriété suivante est implicitement utilisée dans la démonstration du Théorème 2.1(ii): $\alpha(m-1) \geq \alpha(m) - 1$ et $\alpha(m-2) > \alpha(m) - 2$. Cette propriété est pourtant triviale et nous nous dispensons d'en inclure la preuve.

6.3. Interprétation de $\mathbf{V}(0, n)$

Dans sa thèse [25], Kameko a construit le morphisme suivant (baptisé depuis le “ Sq^0 de Kameko” – voir [5] [7] [11] [37]):

$$Sq^0 : \mathbf{P}/\bar{\mathcal{A}}\mathbf{P} \longrightarrow \mathbf{P}/\bar{\mathcal{A}}\mathbf{P},$$

$$Sq^0([P]) := \begin{cases} [Q] & \text{si } P = XQ^2, \\ 0 & \text{sinon.} \end{cases}$$

($[P]$ désigne la classe modulo $\bar{\mathcal{A}}\mathbf{P}$ de l'élément $P \in \mathbf{P}$.)

Il montre que Sq^0 est toujours surjectif et que ce morphisme est, en plus, bijectif en certains degrés. Cette propriété suggère une méthode de descente pour attaquer le problème “hit”. Kameko s'en est largement servi pour mener à bout ses calculs de $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ (mais seulement) pour $k = 3$.

Poussant cette remarque un peu plus loin, nous disons que $\mathbf{P}/\bar{\mathcal{A}}\mathbf{P}$ sera déterminé de manière récursive si on arrive à expliciter le noyau de Sq^0 en tout degré. Nous suivons ce principe et résolvons complètement le problème “hit” pour $k = 4$ dans [42].

Le morphisme Sq^0 ayant été rappelé, il est clair maintenant que modulo $\bar{\mathcal{A}}\mathbf{P}$, l'espace vectoriel $\mathbf{V}(0, n)$ défini dans la Section 3 n'est autre que $\text{Ker}(Sq^0)^n$. C'est là l'interprétation que nous voulons donner à $\mathbf{V}(0, n)$. En général, une description explicite de $\text{Ker}(Sq^0)^n$ est, bien sûr, difficile à obtenir. Mais dans les degrés génériques que nous traitons dans cet article, ce noyau est simplement nul, comme en témoigne la Proposition 4.7. Cela contribue de manière substantielle à l'aboutissement de notre approche.

6.4. Raffinement du théorème de Crabb–Hubbuck

Récemment, en utilisant une idée de Crabb–Hubbuck (exposée dans leur travaux [11]) et nos propres techniques, nous avons réussi à raffiner leur théorème 1.3. Nous nous contentons pour le moment d'annoncer ce raffinement et reporter sa démonstration jusqu'au [41]:

Théorème 6.1 (Nam [41]). *Soit $d = (2^{m_1} - 1) + (2^{m_2} - 1) + \dots + (2^{m_k} - 1)$ avec $m_1 - m_2 > 1$, $m_2 - m_3 > 1, \dots, m_{k-1} - m_k > 1$ et $m_k \geq 0$. Alors*

$$\dim(\mathbf{P}/\bar{\mathcal{A}}\mathbf{P})_d \geq \prod_{1 \leq \ell \leq k} (2^\ell - 1).$$

N. B.: Peu après notre envoi de la première version de cet article, Pr. Wood nous a informé qu'il connaît notre base générique depuis quelques années, mais qu'il n'a pas de prépublication à ce propos.

Remerciements. L'auteur tient à remercier les Professeurs Nguyễn Hữu Việt Hưng (Université des Sciences à Hanoï) et Lionel Schwartz (Université de Paris-Nord) pour avoir accepté de diriger sa thèse. Il tient à remercier le Pr. Hung pour l'avoir instruit au cours de ses études à l'Université des Sciences à Hanoï, et le Pr. Schwartz pour l'avoir intégré dans le laboratoire LAGA de l'Université de Paris-Nord. L'auteur aimerait profiter de cette occasion pour remercier également le Pr. Frédéric Pham (Université de Nice) et le Programme ForMath Vietnam, qui ont rendu possibles ses études de DEA à l'Université de Paris-Nord dans l'année scolaire 2000-2001. Ses remerciements vont finalement à l'Institut de Mathématiques à Hanoï pour le financement qu'il lui a fourni durant la période fin 1999-début 2000.

References

1. J. F. Adams, J. H. Gunawardena and H. R. Miller: The Segal conjecture for elementary abelian p -groups, *Topology* **24**, 435–460 (1985)
2. M. A. Alghamdi, M. C. Crabb and J. R. Hubbuck: Representations of the homology of BV and the Steenrod algebra I, Adams Memorial Symposium on Algebraic Topology, Vol. II, London Math. Soc. Lecture Note Ser. **176**, 217–234 (1992)
3. D. J. Anick and F. P. Peterson: \mathcal{A}_2 -annihilated elements in $H_*(\Omega\Sigma\mathbb{R}P^2)$, *Proc. Amer. Math. Soc.* **117**, 243–250 (1993)
4. M. G. Barratt and S. Priddy: On the homology of non-connected monoids and their associated groups, *Comment. Math. Helv.* **47**, 1–14 (1972)
5. J. M. Boardman: Modular representations on the homology of powers of real projective spaces, *Algebraic Topology: Oaxtepec 1991* (M. C. Tangora ed.), *Contemp. Math.* **146**, 49–70 (1993)
6. E. H. Brown, F. R. Cohen, F. W. Gehring, H. R. Miller and B. A. Taylor: Franklin Peterson (1930-2000), *Notices Amer. Math. Soc.* **48**, 1161–1168 (2001)
7. R. Bruner, L. M. Hà and N. H. V. Hung: On behavior of the algebraic transfer, preprint
8. D. P. Carlisle and R. M. W. Wood: The boundedness conjecture for the action of the Steenrod algebra on polynomials, Adams Memorial Symposium on Algebraic Topology, Vol. II, London Math. Soc. Lecture Note Ser. **176**, 203–216 (1992)
9. G. Carlsson: G. B. Segal's Burnside ring conjecture for $(\mathbb{Z}/2)^k$, *Topology* **22**, 83–103 (1983)
10. S. M. Chen and X. Y. Shen: On the action of Steenrod powers on polynomial algebras, *Lecture Notes in Math.*, vol. 1059, Springer-Verlag 1991, pp. 326–330
11. M. C. Crabb and J. R. Hubbuck: Representations of the homology of BV and the Steenrod algebra II, *Algebraic Topology: new trends in localization and periodicity*, *Progr. Math.* **136**, 143–154 (1996)
12. M. D. Crossley: $H^*(V)$ is of bounded type over $\mathcal{A}(p)$, *Proc. Sympos. Pure Math.* **63**, 183–190 (1998)
13. M. D. Crossley: $\mathcal{A}(p)$ -annihilated elements in $H_*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty)$, *Math. Proc. Cambridge Philos. Soc.* **120**, 441–453 (1996)

14. M. D. Crossley: Monomial bases for $H_*(\mathbb{C}P^\infty \times \mathbb{C}P^\infty)$ over $\mathcal{A}(p)$, *Trans. Amer. Math. Soc.* **351**, 171–192 (1999)
15. M. D. Crossley: $\mathcal{A}(p)$ generators for H^*V and Singer’s homological transfer, *Math. Z.* **230**, 401–411 (1999)
16. M. D. Crossley: On the cohomology of an elementary abelian p -group as a module over the Steenrod algebra, preprint
17. E. Dyer and R. K. Lashof: Homology of iterated loopspaces, *Amer. J. Math.* **84**, 35–88 (1962)
18. V. Franjou and L. Schwartz: Reduced unstable \mathcal{A} -modules and the modular representation theory of the symmetric groups, *Ann. Sci. École Norm. Sup. (4)* **23**, 593–624 (1990)
19. V. Giambalvo, N. H. V. Hung and F. P. Peterson: $H^*(\mathbb{R}P^\infty \times \cdots \times \mathbb{R}P^\infty)$ as a module over the Steenrod algebra, *The Hilton Symposium 1993 (Montreal)*, CRM Proc. Lecture Notes **6**, 133–140 (1994)
20. V. Giambalvo and F. P. Peterson: The annihilator ideal for the action of the Steenrod algebra on $H^*(\mathbb{R}P^\infty)$, *Topology Appl.* **65**, 105–122 (1995)
21. N. H. V. Hung: Spherical classes and the algebraic transfer, *Trans. Amer. Math. Soc.* **349**, 3893–3910 (1997)
22. N. H. V. Hung and T. N. Nam: The hit problem for the Dickson algebra, *Trans. Amer. Math. Soc.* **353**, 5029–5040 (2001)
23. N. H. V. Hung and T. N. Nam: The hit problem for the modular invariants of linear groups, *J. Algebra* **246**, 367–384 (2001)
24. A. S. Janfada and R. M. W. Wood: The hit problem for symmetric polynomials over the Steenrod algebra, *Math. Proc. Cambridge Philos. Soc.* **133**, 295–303 (2002)
25. M. Kameko: Products of projective spaces as Steenrod modules, Thesis, Johns Hopkins University, May 1990
26. M. Kameko: Generators of the cohomology of BV_3 , *J. Math. Kyoto Univ.* **38**, 587–593 (1998)
27. D. S. Kahn and S. B. Priddy: The transfer and stable homotopy theory, *Math. Proc. Cambridge Philos. Soc.* **83**, 103–111 (1978)
28. I. Karaca: On the action of Steenrod operations on polynomial algebras, *Turkish J. Math.* **22**, 163–170 (1998)
29. J. Lannes: Sur les espaces fonctionnels dont la source est le classifiant d’un p -groupe abélien élémentaire, *Inst. Hautes Études Sci. Publ. Math.* **75**, 135–244 (1992)
30. B. M. Mann, E. Y. Miller and H. R. Miller: S^1 -equivariant function spaces and characteristic classes, *Trans. Amer. Math. Soc.* **295**, 233–256 (1986)
31. J. P. May: The cohomology of restricted Lie algebras and Hopf algebras, applications to the Steenrod algebra, Thesis, Princeton University, 1964
32. D. M. Meyer: Hit polynomial and excess in the mod p Steenrod algebra, *Proc. Edinburgh Math. Soc.* **44**, 323–350 (2001)
33. D. M. Meyer and J. H. Silverman: Corrigendum to “Hit polynomials and conjugation in the dual Steenrod algebra”, *Math. Proc. Cambridge Philos. Soc.* **129**, 277–289 (2000)
34. H. R. Miller: The Sullivan conjecture on maps from classifying spaces, *Ann. of Math.* **120**, 39–87 (1984)
35. J. Milnor: The Steenrod algebra and its dual, *Ann. of Math.* **67**, 150–171 (1958)
36. N. Minami: The Adams spectral sequence and the triple transfer, *Amer. J. Math.* **117**, 965–985 (1995)
37. N. Minami: The iterated transfer analogue of the new doomsday conjecture, *Trans. Amer. Math. Soc.* **351**, 2325–2351 (1999)
38. S. A. Mitchell: Splitting $B(\mathbb{Z}/p)^n$ and $B\mathbb{T}^n$ via modular representation theory, *Math. Z.* **189**, 1–9 (1985)

39. K. G. Monks: Polynomial modules over the Steenrod algebra and conjugation in the Milnor basis, *Proc. Amer. Math. Soc.* **122**, 625–634 (1994)
40. T. N. Nam: Système générateur minimal de $\mathbb{F}_2[x, y, z]$ comme module sur l'algèbre de Steenrod, Mémoire de fin d'études universitaires (en langue vietnamienne), Université des Sciences à Hanoï, Juin 1999
41. T. N. Nam: Le transfert algébrique et représentation modulaire du groupe linéaire général, en préparation
42. T. N. Nam: Base monomiale pour $\mathbb{F}_2[x, y, z, t]$ sur l'algèbre de Steenrod et applications, en préparation
43. S. Papastavridis: A formula for the obstruction to transversality, *Topology* **11**, 415–416 (1972)
44. F. P. Peterson: Generators of $H^*(\mathbb{R}P^\infty \wedge \mathbb{R}P^\infty)$ as a module over the Steenrod algebra, *Abstracts Amer. Math. Soc.* 833–55–89, April 1987
45. F. P. Peterson: \mathcal{A} -generators for certain polynomial algebras, *Math. Proc. Cambridge Philos. Soc.* **105**, 311–312 (1989)
46. D. Quillen: On the completion of a simplicial monoid, preprint
47. J. Repka and P. Selick: On the subalgebra of $H_*((\mathbb{R}P^\infty)^n; \mathbb{F}_2)$ annihilated by Steenrod operations, *J. Pure Appl. Algebra* **127**, 273–288 (1998)
48. L. Schwartz: Unstable modules over the Steenrod algebra and Sullivan's fixed point set conjecture, *Chicago Lectures in Math.*, 1994
49. J. H. Silverman: Hit polynomials and the canonical antiautomorphism of the Steenrod algebra, *Proc. Amer. Math. Soc.* **123**, 627–637 (1995)
50. J. H. Silverman: Hit polynomials and conjugation in the dual Steenrod algebra, *Math. Proc. Cambridge Philos. Soc.* **123**, 531–547 (1998)
51. J. Silverman and W. M. Singer: On the action of Steenrod squares on polynomial algebras II, *J. Pure Appl. Algebra* **98**, 95–103 (1995)
52. W. M. Singer: The transfer in homological algebra, *Math. Z.* **202**, 493–523 (1989)
53. W. M. Singer: On the action of Steenrod squares on polynomial algebras, *Proc. Amer. Math. Soc.* **111**, 577–583 (1991)
54. N. E. Steenrod and D. B. A. Epstein: *Cohomology operations*, *Ann. of Math. Stud.*, Vol. **50**, Princeton Univ. Press, 1962
55. M. C. Tangora: On the cohomology of Steenrod algebra, *Math. Z.* **116**, 18–64 (1970)
56. R. M. W. Wood: Steenrod squares of polynomials and the Peterson conjecture, *Math. Proc. Cambridge Philos. Soc.* **105**, 307–309 (1989)
57. R. M. W. Wood: Steenrod squares of polynomials, *Advances in Homotopy Theory*, *London Math. Soc. Lecture Note Ser.* **139**, 173–177 (1989)
58. R. M. W. Wood: Problems in the Steenrod algebra, *Bull. London Math. Soc.* **146**, 449–517 (1998)