arXiv:2304.00506v1 [math.AT] 2 Apr 2023

¨非交换格罗布纳基与 Ext 群；在Steenrod代数中的应用

WEINAN LIN

Abstract. 我们研究递减滤过代数上的非交换格罗布纳基理论，其中这些代数的伴随分次代数是交换的。我们将许多使用交换格罗布纳基的算法推广到这一背景中。作为一项重要应用，我们实现了高效算法，用于计算素数 2 下 Steenrod代数上的 Ext 群。特别是，我们计算了 Steenrod代数的上同调 $\mathrm{Ext}^{*,*}_{\mathscr{A}}(\mathbb{F}_2,\mathbb{F}_2)$，其在代数拓扑中发挥着重要作用，计算范围达到总次数 261，并包括该范围内的环结构。

Contents

1. 引言 1 2. 过滤交换代数 2 3. 基与单项式序 4 4. 过滤交换代数上的格罗布纳基 6 5. 模 9 6. 自关系 11 7. Ext 群 12 8. Steenrod 代数 14 9. 计算 Steenrod 代数上的 Ext 群 16 参考文献 17

1. Introduction

交换格¨obner基理论 [7] 一直是数学不同领域中非常有力的工具，例如交换代数、代数几何、同调代数和应用数学。已有多项研究致力于将格¨obner基推广到非交换代数，包括 [2] 用于李代数的包络代数的研究、 [3] 以及 [17] 非交换自由代数中双边理想的研究，还有 [10] 对交换与非交换格¨obner基之间关系的探索。

然而，大多数 Gr¨obner 基理论都依赖限制性较强的单项式序，要求当单项式 M 是另一个单项式N的倍数时， $M \geq N$ 。本文介绍了一种不同类型的单项式序（定义 3.1）

中国博士后科学基金资助项目，2021年TQ00151

这使我们能够更有效地将 Gr¨obner 基理论应用于范围更广的非交换代数，包括 Steenrod代数。

我们为一类称为滤过交换代数的代数定义了非交换 Gr¨obner 基理论（定义 2.1）。主要结果如下。

定理 1.1（算法 4.5）。给定滤过交换代数 A 的左理想 J 的有限生成集 H ($0 \notin H$)，存在一种广义布赫伯格算法，可将 H 扩充为 J 的 Gr ¨obner 基。

定理 1.2（算法 7.3）。设 $N = A^r/M$ 是滤过交换分次代数 A 上的分次左模，其中 M 是 A^r 的左子模。存在一种算法，可以构造自由 A-分解的前 $s+1$ 项 $F_0, \ldots, F_s$

$$\cdots \to F_s \xrightarrow{d_s} \cdots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 = A^r \xrightarrow{\epsilon} N$$

对于任意 s。

上述算法有许多应用，我们重点开发一种计算 Ext 群的算法；这在同调代数和代数拓扑中都很重要。随后，我们将该算法应用于模 2 斯坦罗德代数 $\mathscr{A}$，得到以下计算结果。

定理 1.3。双分次代数

$$\bigoplus_{t \le 261} \operatorname{Ext}_{\mathscr{A}}^{s,t}(\mathbb{F}_2, \mathbb{F}_2)$$

在总次数不超过 261 的范围内是一个代数，其中有 2914 个不可分解元、23822 个基元素和 227498 个不可分解关系。完整图表见 [13]。

这个代数是 Adams谱序列的 E_2 页，该谱序列收敛到在素数 2 处完备化的球面的稳定同伦群（见 [1]）。它在稳定同伦论中发挥着基础性作用，并与许多重要问题相关，例如霍普夫不变量一问题和凯尔韦尔不变量一问题。球面的稳定同伦群的计算依赖于这些针对 Adams E_2 页的机器计算结果。关于最新的计算，感兴趣的读者可参阅 Isaksen、Wang 和 Xu [6] 。

此前，最全面且公开可用的 $\operatorname{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2, \mathbb{F}_2)$ 计算由 Bruner 和 Rognes [4], 完成，他们将 Ext 计算至 200 维。Nassau [18] 和 Wang [21] 也编写了其他计算机程序。我们的新算法在内存和运行时间方面都非常高效：在个人计算机上，一天内即可计算出 200 范围内的分解；而为了在 64 核 CPU 机器上获得定理 1.3 所需的分解和乘积，我们耗时 $88{+}63$ 天。这将他们的计算范围扩展了数个数量级。感兴趣的读者可在 GitHub [11], 找到该算法的最新实现；对于定理 1.3，该实现的运行速度是旧版本的两倍。

2. Filtered-Commutative Algebras

设 k 为任意域， A 为下文定义的代数。

定义 2.1. 若代数 A 在 k 上满足以下条件，则称其为（递减）滤过交换代数。

(1) 代数 A 带有一个理想过滤

$$A = F_0A \supset F_1A \supset F_2A \supset \cdots$$

使得

$$F_pA \cdot F_qA \subset F_{p+q}A$$

且 $F_{p_{\text{nul}}}A = 0$ 对于某个数 $p_{\text{nul}} > 0$。

(2) 由下式定义的伴随分次代数 gr(A)

$$\text{gr}_p(A) = F_pA/F_{p+1}A$$

是交换的。

定义 2.2。若非零元素 $a \in A$ 投影到 $f \in \text{gr}_p(A)$，则称之为.....，其中p 是满足 $a \in F_pA$ 且 f 是 a 在映射$F_pA \to F_pA/F_{p+1}A$下的像的最大数。我们记

$$v(a) = p \text{ and } \text{pr}(a) = f.$$

若 a 为零，我们定义

$$v(0) = \infty \text{ and } \text{pr}(0) = 0.$$

我们也称 a 为 f 的一个提升。

容易看出，另一个元素 $a' \in A$ 投影到同一个元素 $f \in \text{gr}_p(A)$，当且仅当 $a - a' \in F_{p+1}A$。投影映射不是向量空间之间的线性映射，因为此处 pr($a - a'$) 可能非零。

命题 2.3. 对于非零元素 a、$b \in A$，有

$$v(ab) \geq v(a) + v(b)$$

或者等价地,

$$|\text{pr}(ab)| \geq |\text{pr}(a)| + |\text{pr}(b)|$$

其中 $|\cdot|$ 是 gr(A) 中元素的次数。等式成立当且仅当

$$\text{pr}(a)\text{pr}(b) \neq 0$$

在 gr(A) 中。

证明。由条件 $F_pA \cdot F_qA \subset F_{p+q}A$ 可直接得出。 □

定义 2.1 中的条件 $F_{p_{\text{nul}}}A = 0$ 确保 gr(A) 的一个基可以提升为 A 的一个基。更准确地说，若 $\mathscr{B} = \{m_i\}$ 是 gr(A) 的一个 k-基，且 $\tilde{m}_i \in \tilde{A}$ 投影到 m_i，则 $\mathscr{B} = \{\tilde{m}_i\}$ 是 A 的一个 k- 基。

注释 2.4。滤过交换代数的定义是交换代数的推广，因为如果 A 是交换的，我们可以用以下方式对它进行滤过

$$A = F_0A \subset F_1A = \{0\}.$$

显然， A 满足定义 2.1 中的条件。也存在非交换的例子。本文将研究的重要例子是素数 2 处的截断 Steenrod 代数。

从现在起，我们研究满足 gr(A) 为有限生成的滤过交换代数 A 。因此，伴随分次代数可以表示为

$$\text{gr}(A) = k[x_1, \ldots, x_n]/I$$

对于某个 n 以及多项式环 $P = k[x_1, \ldots, x_n]$的某个理想 I。由于 gr(A) 是分次的，我们假设 x_i 和 I 都是齐次的。齐次元素 $f \in P$ 的次数记为 $|f|$。

3. Bases and Monomial Orderings

为了在 A上建立 Gr¨obner 基理论，我们希望为 A 选择一组基，并在这组基上定义一个良序。由于 gr(A) 是交换代数，我们先在 gr(A)上进行，再将其提升到 A。

定义 3.1. 对分次多项式环 $P = k[x_1, \dots, x_n]$，次数反向可容许单项式序是指单项式上的一种全序，使得对于任意单项式 M、 N、 L,

(1) $M \le N \iff ML \le NL$,
(2) $|L| = 0 \Longrightarrow M \le ML$。
(3) $|M| > |N| \Longrightarrow M < N$。

注 3.2. 这不是传统单项式序，因为它在所有单项式上不是良序。然而，对于某个 $p_{\mathrm{nul}} > 0$ ，我们有 $F_{p_{\mathrm{nul}}} A = 0$ ，因此对所有 $i \ge p_{\mathrm{nul}}$, $\mathrm{gr}_i(A) = 0$ 。条件 (1)(2) 确保它在每个次数上都是良序，而条件 (3) 确保它在次数小于 p_{nul} 的所有单项式上都是良序。

假设 $P = k[x_1, \dots, x_n]$ 配备了上文定义的次数反向可容许单项式序。我们用 LM(f) 表示 $f \in P$ 的首单项式，它是 f 中最大的单项式。首项 LT(f) 是首单项式及其在 f 中对应系数组成的项。回顾以下关于交换 Gr¨obner 基的定义。

定义 3.3. 理想 I 的 Gr¨obner 基 G 是 P 的有限生成集，且满足 P 中以下两个理想相等:

$$(\mathrm{LM}(f) : f \in I) = (\mathrm{LM}(g) : g \in G).$$

假设 G 是理想 I 的 Gr¨obner 基。令 $\mathscr{M}$ 为 P 中所有单项式构成的集合。Gr¨obner 基的定义表明，集合

$$\mathscr{B} = \{m \in \mathscr{M} : \mathrm{LM}(g) \nmid m \text{ for all } g \in G\}$$

（模 I）是 gr(A) $= P/I$ 作为向量空间的一组基。注意，若 $m \in \mathscr{B}$，则根据定义，所有整除 m 的单项式也都属于 $\mathscr{B}$ 。

定义 3.4. 对任意非零的 $f \in \mathrm{gr}(A) = P/I$，均可唯一地写成

$$f = c_1 m_1 + \cdots + c_l m_l \mod I$$

其中 $c_i \in k$、 $m_i \in \mathscr{B}$ 和 $m_1 > \cdots > m_l$。 f 的首单项式定义为 $\mathrm{LM}_{\mathrm{gr}}(f) = m_1$，而 f 的首项定义为 $\mathrm{LT}_{\mathrm{gr}}(f) = c_1 m_1$。

注意，若 $m \notin \mathscr{B}$，则 $\mathrm{LM}_{\mathrm{gr}}(m) < m$。

我们选定并固定 $X_i \in A$ ，使得对每个 i， X_i 在伴随分次代数中投影为 x_i 。于是对于 $m = x_1^{r_1} \cdots x_n^{r_n} \in \mathscr{B}$，乘积

$$\tilde{m} = X_1^{r_1} \cdots X_n^{r_n} \in A$$

投影为 $m + I$，因为 $m + I$ 在 gr(A) $= P/I$ 中非平凡。因此集合

$$\tilde{\mathscr{B}} = \{\tilde{m} : m \in \mathscr{B}\}$$

˜是 A的一组基。我们通过提升，按照排列 $\mathscr{B}$ 的相同方式排列 $\mathscr{B}$ 。注意， ˜ $\mathscr{B}$ 和 $\mathscr{B}$ 都是良序的。

定义 3.5. 对任意 $f \in \mathbf{gr}(A)$，我们记

$$f = c_1 m_1 + \cdots + c_l m_l \mod I$$

其中 $c_i \in k$ 和 $m_i \in \mathscr{B}$。我们定义

$$\tilde{f} = c_1 \tilde{m}_1 + \cdots + c_l \tilde{m}_l \in A$$

˜它是 f的一个提升。有时我们也写作 $\ell(f) = f$。

定义 3.6. 对任意非零的 $a \in A$，我们可以将 a 写成如下形式

$$a = c_1 \tilde{m}_1 + \cdots + c_l \tilde{m}_l$$

˜其中 $c_i \in k$、 $m_i \in \mathscr{B}$和 $m_1 > \cdots > m_l$。我们称 $\mathbf{LM}_A(a) = \tilde{m}_1 \in \mathscr{B}$为 a的首单项式，并称 $\mathbf{LT}_A(a) = c_1 \tilde{m}_1$ 为 a的首项。为方便起见，我们还定义 $\mathbf{LM}_{\mathscr{B}}(a) = m_1 \in \mathscr{B}$，并且可见 $\mathbf{LM}_{\mathscr{B}} = \mathbf{pr} \circ \mathbf{LM}_A$。

命题 3.7. 对任意非零的 $a \in A$，有

$$\mathrm{LM}_{\mathscr{B}}(a) = \mathrm{pr}(\mathrm{LM}_A(a)) = \mathrm{LM}_{\mathrm{gr}}(\mathrm{pr}(a))$$

或者等价地

$$\mathrm{LM}_A = \ell \circ \mathrm{LM}_{\mathrm{gr}} \circ \mathrm{pr}$$

证明。若

$$a = c_1 \tilde{m}_1 + \cdots + c_l \tilde{m}_l$$

其中 $c_i \in k$、 $m_i \in \mathscr{B}$ 和

$$m_1 > \cdots > m_l,$$

then it is clear that $\mathrm{pr}(a) = \sum_{\substack{1 \le i \le l \\ |m_i| = |m_1|}} m_i$. Therefore $\mathrm{LM}_{\mathrm{gr}}(\mathrm{pr}(a)) = m_1$. □

˜以下命题表明， $\mathscr{B}$ 上的序是“可容许的”，也就是说，它与乘法相容。为方便起见，在上下文明确时，我们有时省略“模 I”，并将 P 的某些元素视为 $\mathbf{gr}(A) = P/I$ 的元素。

命题 3.8。假设 m_1、 $m_2 \in \mathscr{B}$ 和 $\tilde{m}_1 \tilde{m}_2 \neq 0$。我们有

$$\mathrm{LM}_{\mathscr{B}}(\tilde{m}_1 \tilde{m}_2) \le m_1 m_2.$$

当且仅当 $m_1 m_2 \in \mathscr{B}$ 时，等式成立。

证明。由前一个命题可得

$$\mathrm{LM}_{\mathscr{B}}(\tilde{m}_1 \tilde{m}_2) = \mathrm{LM}_{\mathrm{gr}}(\mathrm{pr}(\tilde{m}_1 \tilde{m}_2)).$$

若 $m_1 m_2$ 在 $\mathbf{gr}(A)$ 中平凡，则 $|\mathbf{pr}(\tilde{m}_1 \tilde{m}_2)| > |m_1 m_2|$。因此

$$\mathrm{LM}_{\mathrm{gr}}(\mathrm{pr}(\tilde{m}_1 \tilde{m}_2)) < m_1 m_2.$$

若 $m_1 m_2$ 在 $\mathbf{gr}(A)$ 中非平凡，则有

$$\mathrm{LM}_{\mathrm{gr}}(\mathrm{pr}(\tilde{m}_1 \tilde{m}_2)) = \mathrm{LM}_{\mathrm{gr}}(m_1 m_2) \le m_1 m_2.$$

最后一个等式成立当且仅当 $m_1 m_2 \in \mathscr{B}$。 □

该命题直接推出以下结论。

推论 3.9。假设 $a \in A$，$\mathbf{LM}_A(a) = \tilde{m}$ 且 $q \in \mathscr{B}$。若 $qm \in \mathscr{B}$，则 $\mathbf{LM}_{\mathscr{B}}(\tilde{q}a) = qm$。否则，$\mathbf{LM}_{\mathscr{B}}(\tilde{q}a) < qm$。

4. Gröbner bases over Filtered-Commutative Algebras

设 A 是一个滤过交换代数，并沿用上一节定义的记号。我们首先关注 A 的左理想。下一节将考虑 A 上的左模。

定义 4.1. 左理想 J 的 Gröbner 基 H 是 J 的有限生成集，使得 P 的以下两个理想相等:

$$(\mathrm{LM}_{\mathscr{B}}(a) : a \in J) = (\mathrm{LM}_{\mathscr{B}}(h) : h \in H).$$

为了给出一种算法，从给定的 J 生成集出发计算 $J \subset A$ 的 Gröbner 基，我们需要定义 A 中的约化。

定义 4.2. 给定 a、$b \in A$，记

$$a = c_1\tilde{m}_1 + \cdots + c_l\tilde{m}_l$$

其中 $c_i \in k$、$m_i \in \mathscr{B}$ 和 $m_1 > \cdots > m_l$。设对某个 $c \in k$ 和 $m \in \mathscr{B}$，有 $c\tilde{m} = \mathrm{LT}_A(b)$。若 a 可被 b 约化，即对于某个 i，m_i 可被 m 整除，则称 a 可约化。在这种情况下，我们选取最小的 i，并将 a 被 b 的单步约化定义为

$$\mathrm{red}_1(a, b) = a - \frac{c_i}{c}\widetilde{\Big(\frac{m_i}{m}\Big)}b.$$

注意，与 a 相比，$\mathrm{red}_1(a, b)$ 将 a 中的 $c_i\tilde{m}_i$ 替换为严格小于 $\tilde{m}_i$ 的其他项，因为

$$\mathrm{LT}_{\mathrm{gr}}(\mathrm{pr}(\frac{c_i}{c}\widetilde{\Big(\frac{m_i}{m}\Big)}b)) = \frac{c_i}{c}\frac{m_i}{m}cm = c_im_i.$$

定义 4.3. 对于 $a \in A$ 和一个有限的有序子集 $H \subset A$，我们称 a 可由 H 约化，如果 a 可由某个 $h \in H$ 约化。在这种情况下，我们假设 $\tilde{m}$ 是 a 中可由 H 约化的最大项，而 $h \in H$ 是 H 中第一个能约化 $\tilde{m}$ 的元素。我们将 a 按 H 进行的单步约化定义为

$$\mathrm{red}_1(a, H) = \mathrm{red}_1(a, h).$$

我们用 $\mathrm{red}_1(a, H)$ 替换 a，并重复此过程，直到 a 不能由 H 约化为止。这个过程会终止，因为单项式序在 $\mathscr{B}$ 上是良序的。我们称最终结果为 a 按 H 的约化，记作 $\mathrm{red}(a, H)$。

注 4.4. 根据约化的定义，如果 $\mathrm{red}(a, H) = 0$，我们可以写成

$$a = c_1\tilde{m}_1h_1 + \cdots + c_l\tilde{m}_lh_l$$

其中 $c_i \in k$、$m_i \in \mathscr{B}$ 和 $h_i \in H$ 使得 $m_i\mathrm{LM}_{\mathscr{B}}(h_i) \in \mathscr{B}$ 且

$$m_1\mathrm{LM}_{\mathscr{B}}(h_1) > \cdots > m_l\mathrm{LM}_{\mathscr{B}}(h_l).$$

我们可以看到 $\mathrm{LM}_{\mathscr{B}}(a) = m_1\mathrm{LM}_{\mathscr{B}}(h_1)$。

下面给出一种广义 Buchberger 算法，用于计算 A 的理想的 Gr¨obner 基。

算法 4.5. 给定左理想 J of A 的有限有序生成集 H ($0 \notin H$)，我们可以通过以下步骤将 H 扩展为 J 的 Gr ¨obner 基

(1) 对于 $a \in H$ 和 $g \in G$，令 L 为最小公倍数

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathscr{B}}(a), \mathrm{LM}(g))$$

and

$$q = \frac{L}{\mathrm{LM}_{\mathscr{B}}(a)}.$$

如果 $\mathrm{red}(\tilde{q}a, H)$ 非平凡，则将其追加到 H。

(2) 对于 $a, b \in H$，令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathscr{B}}(a), \mathrm{LM}_{\mathscr{B}}(b))$$

and

$$t_1 = \frac{L}{\mathrm{LT}_{\mathrm{gr}}(\mathrm{pr}(a))},\ t_2 = \frac{L}{\mathrm{LT}_{\mathrm{gr}}(\mathrm{pr}(b))}.$$

如果 $\mathrm{red}(\tilde{t}_1 a - \tilde{t}_2 b, H)$ 非平凡，则将其追加到 H。

(3) 重复 (1)(2)，直到无法再向 H中添加元素。

我们通过以下两个命题验证该算法的正确性。

命题 4.6. 算法 4.5 总是会终止。

证明. 显然，添加到 H 中的新元素属于 J。由于每个新元素在添加到 H 之前都会先化简，因此理想

$$(\mathrm{LM}_{\mathscr{B}}(h) : h \in H)$$

P 的理想在添加该元素后会严格变大。由于 $P = k[x_1, \ldots, x_n]$ 是诺特环，这种情况不可能无限持续下去。□

命题 4.7. 当算法 4.5 终止时，对于任意 $a \in J$，我们有

$$\mathrm{LM}_{\mathscr{B}}(a) \in (\mathrm{LM}_{\mathscr{B}}(h) : h \in H).$$

证明. 由于 H 是 J 的生成集，只需证明对于所有 $c_i \in k$、$m_i \in \mathscr{B}$ 和 $h_i \in H$、$1 \le i \le l$，满足

$$m_1 \mathrm{LM}_{\mathscr{B}}(h_1) \ge \cdots \ge m_l \mathrm{LM}_{\mathscr{B}}(h_l),$$

该命题对以下情形成立

$$a = c_1 \tilde{m}_1 h_1 + \cdots + c_l \tilde{m}_l h_l. \tag{4.8}$$

不失一般性，我们假设任意 $h \in H$的首项系数均为 1，这意味着 $\mathrm{LT}_A(h) = \mathrm{LM}_A(h)$。

若 $l = 0$，则证明完成，因为这只会在 $a = 0$时发生。

若 $m_1 \mathrm{LM}_{\mathscr{B}}(h_1) \notin \mathscr{B}$，则存在 $g \in G$ 使得 $\mathrm{LM}(g) \mid m_1 \mathrm{LM}_{\mathscr{B}}(h_1)$。令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathscr{B}}(h_1), \mathrm{LM}(g))$$

and

$$q = \frac{L}{\mathrm{LM}_{\mathscr{B}}(h_1)}.$$

我们有 $q | m_1$ ，并且根据算法 4.5 的终止性，

$$\mathrm{red}(\tilde{q}h_1, H) = 0.$$

因此，根据注 4.4，我们可以写成

$$\tilde{q}h_1 = c_1' \tilde{m}_1' h_1' + \cdots + c_s' \tilde{m}_s' h_s'$$

其中存在某些 $c'_i \in k$、 $m'_i \in \mathscr{B}$ 和 $h'_i \in H$，使得

$$m'_1 \mathrm{LM}_{\mathscr{B}}(h'_1) > \cdots > m'_s \mathrm{LM}_{\mathscr{B}}(h'_s).$$

我们有

$$m'_j \mathrm{LM}_{\mathscr{B}}(h'_j) \le m'_1 \mathrm{LM}_{\mathscr{B}}(h'_1) = \mathrm{LM}_{\mathscr{B}}(\tilde{q} h_1) < q \mathrm{LM}_{\mathscr{B}}(h_1)$$

对所有 $1 \le j \le s$。

现在我们考虑

$$\begin{aligned} \tilde{m}_1 h_1 &= \Big(\tilde{m}_1 - \widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{q}\Big) h_1 + \widetilde{\Big(\frac{m_1}{q}\Big)} (\tilde{q} h_1) \\ &= \Big(\tilde{m}_1 - \widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{q}\Big) h_1 + \sum_{j=1}^{s} c'_j \widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{m}'_j h'_j. \end{aligned} \tag{4.9}$$

由于 $\mathsf{gr}(A)$ 是交换的，我们有

$$v\Big(\tilde{m}_1 - \widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{q}\Big) > v(\tilde{m}_1).$$

Thus

$$\mathrm{LM}_{\mathscr{B}}\Big(\tilde{m}_1 - \widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{q}\Big) \cdot \mathrm{LM}_{\mathscr{B}}(h_1) < m_1 \mathrm{LM}_{\mathscr{B}}(h_1).$$

我们还有

$$\begin{aligned} \mathrm{LM}_{\mathscr{B}}\Big(\widetilde{\Big(\frac{m_1}{q}\Big)} \tilde{m}'_j\Big) \cdot \mathrm{LM}_{\mathscr{B}}(h'_j) &\le \frac{m_1}{q} \cdot m'_j \mathrm{LM}_{\mathscr{B}}(h'_j) \\ &< \frac{m_1}{q} \cdot q \mathrm{LM}_{\mathscr{B}}(h_1) \\ &= m_1 \mathrm{LM}_{\mathscr{B}}(h_1) \end{aligned}$$

对所有 $1 \le j \le s$。上述两个等式和 (4.9) 表明，$\tilde{m}_1 h_1$ 可以重写为形如 $\tilde{m} h$ 的元素的线性组合，其中 $m \in \mathscr{B}$、$h \in H$ 和 $m\mathrm{LM}_{\mathscr{B}}(h) < m_1 \mathrm{LM}_{\mathscr{B}}(h_1)$。只要 $m_1 \mathrm{LM}_{\mathscr{B}}(h_1) \notin \mathscr{B}$，我们就可以继续对 (4.8) 进行重写；由于 $|m_1 \mathrm{LM}_{\mathscr{B}}(h_1)| < 2p_{\mathrm{nul}}$，且单项式序在有限次数的单项式上总是良序，因此这一过程必定会在某个时候停止。

现在我们总可以假设，在 (4.8) 中 $m_1 \mathrm{LM}_{\mathscr{B}}(h_1) \in \mathscr{B}$。如果 $l > 1$ 并且

$$m_1 \mathrm{LM}_{\mathscr{B}}(h_1) = m_2 \mathrm{LM}_{\mathscr{B}}(h_2),$$

我们可以用与本证明前一部分类似的方式重写 (4.8)。事实上，令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathscr{B}}(h_1), \mathrm{LM}_{\mathscr{B}}(h_2))$$

and

$$q_1 = \frac{L}{\mathrm{LM}_{\mathscr{B}}(h_1)}, \ q_2 = \frac{L}{\mathrm{LM}_{\mathscr{B}}(h_2)}.$$

容易看出，存在 $m' \in \mathscr{B}$ 使得 $m_1 = m' q_1$ 且 $m_2 = m' q_2$。B y 算法 4.5 的终止，

$$\mathrm{red}(\tilde{q}_1 h_1 - \tilde{q}_2 h_2, H) = 0.$$

因此我们可以写成

$$\tilde{q}_1 h_1 - \tilde{q}_2 h_2 = c'_1 \tilde{m}'_1 h'_1 + \cdots + c'_s \tilde{m}'_s h'_s$$

对于某些满足以下条件的 $c'_i \in k$、 $m'_i \in \mathscr{B}$ 和 $h'_i \in H$

$$m'_1\mathrm{LM}_{\mathscr{B}}(h'_1) > \cdots > m'_s\mathrm{LM}_{\mathscr{B}}(h'_s).$$

我们有

$$m'_j\mathrm{LM}_{\mathscr{B}}(h'_j) \leq m'_1\mathrm{LM}_{\mathscr{B}}(h'_1) = \mathrm{LM}_{\mathscr{B}}(\tilde{q}_1h_1 - \tilde{q}_2h_2) < q_1\mathrm{LM}_{\mathscr{B}}(h_1)$$

对所有 $1 \leq j \leq s$ 均成立。

现在我们考虑

$$\begin{aligned}
&\tilde{m}_1h_1 - \tilde{m}_2h_2 \\
=&\Big(\tilde{m}_1 - \tilde{m}'\tilde{q}_1\Big)h_1 - \Big(\tilde{m}_2 - \tilde{m}'\tilde{q}_2\Big)h_2 + \tilde{m}'(\tilde{q}_1h - \tilde{q}_2h) \\
=&\Big(\tilde{m}_1 - \tilde{m}'\tilde{q}_1\Big)h_1 - \Big(\tilde{m}_2 - \tilde{m}'\tilde{q}_2\Big)h_2 + \sum_{j=1}^{s} c'_j\tilde{m}'\tilde{m}'_jh'_j.
\end{aligned} \tag{4.10}$$

同样，对于 $i = 1$，我们有 2

$$v\Big(\tilde{m}_i - \tilde{m}'\tilde{q}_i\Big) > v(\tilde{m}_i).$$

Thus

$$\mathrm{LM}_{\mathscr{B}}\Big(\tilde{m}_i - \tilde{m}'\tilde{q}_i\Big) \cdot \mathrm{LM}_{\mathscr{B}}(h_i) < m_i\mathrm{LM}_{\mathscr{B}}(h_i) = m_1\mathrm{LM}_{\mathscr{B}}(h_1).$$

我们还有

$$\begin{aligned}
\mathrm{LM}_{\mathscr{B}}\Big(\tilde{m}'\tilde{m}'_j\Big) \cdot \mathrm{LM}_{\mathscr{B}}(h'_j) &\leq \frac{m_1}{q} \cdot m'_j\mathrm{LM}_{\mathscr{B}}(h'_j) \\
&< \tilde{m}' \cdot q\mathrm{LM}_{\mathscr{B}}(h_1) \\
&= m_1\mathrm{LM}_{\mathscr{B}}(h_1)
\end{aligned}$$

对所有 $1 \leq j \leq s$。上述两个等式和 (4.10) 表明， $\tilde{m}_1h_1$ 可以重写为 $\tilde{m}_2h_2$ 与形如 $\tilde{m}h$ 的元素的线性组合，其中$m \in \mathscr{B}$、 $h \in H$，且 $m\mathrm{LM}_{\mathscr{B}}(h) < m_1\mathrm{LM}_{\mathscr{B}}(h_1)$。只要 $m_1\mathrm{LM}_{\mathscr{B}}(h_1) = m_2\mathrm{LM}_{\mathscr{B}}(h_2)$，我们就可以继续对 (4.8) 进行重写，直到某个时刻停止。

最终我们得到 $l = 0$，或者 $m_1\mathrm{LM}_{\mathscr{B}}(h_1) \in \mathscr{B}$，且 $m_1\mathrm{LM}_{\mathscr{B}}(h_1) > m_2\mathrm{LM}_{\mathscr{B}}(h_2)$（当 $l > 1$ 时）。在第二种情况下

$$\mathrm{LM}_{\mathscr{B}}(a) = m_1\mathrm{LM}_{\mathscr{B}}(h_1) \in (\mathrm{LM}_{\mathscr{B}}(h) : h \in H).$$

□

在 A 上的 Gr¨obner 基与交换 Gr¨obner 基的表现非常相似。很容易看出， H 是 $J \subset A$ 的 Gr¨obner 基，当且仅当对于任意 $a \in J$，$\mathrm{red}(a, H) = 0$，并且集合

$$\{\tilde{m} \in \tilde{\mathscr{B}} : \mathrm{LM}_{\mathscr{B}}(h) \nmid m \text{ for all } h \in H\}$$

（模 J）是左 A-模 A/J 的 k-基。

5. Modules

在前几节中，我们研究了 A 的左理想的 Gr¨obner 基。现在考虑 A 上的有限生成左模 N。我们可以找到一个数 r 和 A^r 的左子模 M，使得 $N \cong A^r/M$。因此，为了研究 A 上的有限生成左模，我们可以研究 A^r 的左子模。

考虑截断分次环 $\mathbb{A} = \mathbb{A}_0 \oplus \mathbb{A}_1 = A \oplus A^r$，其乘法定义如下：

$$(a_1, x_1) \cdot (a_2, x_2) = (a_1 a_2, a_1 x_2 + a_2 x_1)$$

对于 $a_i \in A$、$x_i \in A^r$、$i = 1, 2$。我们可以看到，A^r 关于 A 的左子模与包含在 $\mathbb{A}_1$ 中的 $\mathbb{A}$ 的左理想一一对应。我们可以按以下方式过滤 $\mathbb{A}$

$$F_p\mathbb{A} = F_pA \oplus (F_pA)^r \subset \mathbb{A}.$$

那么 $\mathbb{A}$ 实际上是一个过滤分次交换代数，并且

$$\mathrm{gr}(\mathbb{A}) = \mathrm{gr}(A) \oplus \mathrm{gr}(A)^r \cong k[x_1, \ldots, x_n, e_1, \ldots, e_r]/(I, e_i e_j : 1 \le i \le j \le r)$$

其中，$\{\tilde{e}_i\}$ 是自由 A 模 $\mathbb{A}_1 = A^r$ 的 A 基，且 $\mathbf{pr}(\tilde{e}_i) = e_i$。

由于 $M \subset \mathbb{A}_1$，我们只关注以下集合中的单项式

$$\mathbb{B} = \{me_i : m \in \mathscr{M}, 1 \le i \le r\}.$$

这些单项式上的单项式序应满足

$$m_1 e_i < m_2 e_i \Longleftrightarrow m_1 < m_2 \text{ for all } i.$$

这类序的一个例子是

$$m_1 e_i < m_2 e_j \Longleftrightarrow i > j \text{ or } (i = j \text{ and } m_1 < m_2). \tag{5.1}$$

还有许多其他例子，但我们假设已经为 $\mathbb{B}$选定了其中一种~。注意，集合 $\mathbb{B} = \{\tilde{m}\tilde{e}_i : m \in \mathscr{M}、1 \le i \le r\}$ 是 A^r的一个 k基。如果 $\tilde{m}\tilde{e}_i$是 $x \in A^r$的首单项式，我们记作 $\mathbf{LM}_{\mathbb{B}}(x) = me_i$。

定义 5.2. 左子模 $M \subset A^r$ 在 A 上的 Gr¨öbner 基 H，是 $M \subset \mathbb{A}_1$ 作为滤过交换代数 $\mathbb{A}$的左理想的一个 Gr¨öbner 基。

如果我们用 A展开定义，就得到如下结果。

命题 5.3. 左子模 $M \subset A^r$ 在 A 上的 Gr ¨öbner 基 H 是 M的一个有限生成集，并且 $k[x_1, \ldots, x_n, e_1, \ldots, e_r]$ 的以下两个理想相等：

$$(\mathrm{LM}_{\mathbb{B}}(x) : x \in M) = (\mathrm{LM}_{\mathbb{B}}(h) : h \in H).$$

由于 $M \subset A^r$ 可以视为 $\mathbb{A}$的一个理想，因此若将 A 替换为 $\mathbb{A}$，便可使用算法 4.5 计算 M 的 Gr¨obner 基。这里我们用 A 以及辅助符号 e_1、……、e_r来重述该算法。

算法 5.4. 给定 A上的左子模 $M \subset A^r$ 的有限有序生成集 H ($0 \notin H$)，我们可以通过以下步骤将 H 扩展为 M 的 Gr ¨obner 基。

(1) 对于 $a \in H$ 和 $g \in G$，令 L 为最小公倍数

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathbb{B}}(a), \mathrm{LM}(g))$$

and

$$q = \frac{L}{\mathrm{LM}_{\mathbb{B}}(a)}.$$

如果 $\mathbf{red}(\tilde{q}a, H)$ 非平凡，则将其追加到 H。

（2）对于满足 $\mathrm{LM}_{\mathbb{B}}(a)$ 和 $\mathrm{LM}_{\mathbb{B}}(b)$ 含有相同 e_i 因子的 $a, b \in H$，令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathbb{B}}(a), \mathrm{LM}_{\mathbb{B}}(b))$$

and

$$t_1 = \frac{L}{\mathrm{LT}_{\mathrm{gr}(\mathbb{A})}(\mathrm{pr}(a))},\ t_2 = \frac{L}{\mathrm{LT}_{\mathrm{gr}(\mathbb{A})}(\mathrm{pr}(b))}.$$

如果 $\mathrm{red}(\tilde{t}_1 a - \tilde{t}_2 b, H)$ 非平凡，就将其添加到 H 中。

(3) 重复 (1)(2)，直到无法再向 H 中添加元素。

6. Syzygies

定义 6.1. 设 $(x_1, \cdots, x_s)$ 是 A^r 中的一个元素组。

(1) $(x_1, \ldots, x_s)$ 的一个 Syzygy 是一个满足 $a_1 x_1 + \cdots + a_s x_s = 0$ 的元组 $(a_1, \ldots, a_s) \in A^s$。(2) $(x_1, \cdots, x_s)$ 的所有 Syzygy 构成 $(x_1, \cdots, x_s)$ 的（第一）关系模，记作 $\mathrm{Syz}(x_1, \cdots, x_s)$。

显然，$\mathrm{Syz}(x_1, \cdots, x_s)$ 是 A^s 的一个左子模。本节的目标是求出 $\mathrm{Syz}(x_1, \cdots, x_s)$ 的一个生成集。

定义 6.2. 设 $H = (h_1, \ldots, h_s)$ 是 $M \subset A^r$ 的一个有序 Gr¨obner 基。对于 $1 \le i \le s$ 和 $g \in G$，令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathbb{B}}(h_i), \mathrm{LM}(g))$$

and

$$q = \frac{L}{\mathrm{LM}_{\mathbb{B}}(h_i)}.$$

我们有 $\mathrm{red}(\tilde{q} h_i, H) = 0$，并且它展开为

$$\tilde{q} h_i = a_1 h_1 + \cdots + a_s h_s$$

对于某些 $a_l \in A$、$1 \le l \le s$。这意味着

$$(-a_1, \ldots, -a_{i-1}, \tilde{q} - a_i, -a_{i+1}, \ldots, -a_s)$$

是 H 的一个 Syzygy。我们将 H 的这个 Syzygy 记为 $\sigma_{i,\ g}$。

定义 6.3. 设 $H = (h_1, \ldots, h_s)$ 是 $M \subset A^r$ 的一个有序 Gr¨obner 基。对于 $1 \le i < j \le s$，令

$$L = \mathrm{lcm}(\mathrm{LM}_{\mathbb{B}}(h_i), \mathrm{LM}_{\mathbb{B}}(h_j))$$

and

$$t_i = \frac{L}{\mathrm{LT}_{\mathrm{gr}(\mathbb{A})}(\mathrm{pr}(h_i))},\ t_j = \frac{L}{\mathrm{LT}_{\mathrm{gr}(\mathbb{A})}(\mathrm{pr}(h_j))}.$$

我们有 $\mathrm{red}(\tilde{t}_i h_i - \tilde{t}_j h_j, H) = 0$，并且它展开为

$$\tilde{t}_i h_i - \tilde{t}_j h_j = a_1 h_1 + \cdots + a_s h_s$$

对于某些 $a_l \in A$、$1 \le l \le s$。这意味着

$$(-a_1, \ldots, -a_{i-1}, \tilde{t}_i - a_i, a_{i+1}, \ldots, -a_{j-1}, -\tilde{t}_j - a_j, -a_{j+1}, \ldots, -a_s)$$

是 H 的 Syzygy。我们将 H 的这个 Syzygy 记为 $\sigma_{i,\ j}$。

下面的命题给出了 Gr¨obne 的 $\mathrm{Syz}(h_1, \ldots, h_s)$ 的一个生成集 r
基（$h_1, \ldots, h_s$）。

定理 6.4. 若 $H=(h_1,\dots,h_s)$ 是某个左子模 $M\subset A^r$ 的有序 Gr¨obner 基，则关系模 Syz(H) 由以下两组元素生成。

$$\{\sigma_{i,g}\}_{1\le i\le s,g\in G},\ \{\sigma_{i,j}\}_{1\le i\le s,1\le j\le s}.$$

证明。实际上，只要将 A 替换为 $\mathbb{A}$，并考虑 (4.8) 中 $a=0$ 的情形，就可由命题 4.7 的证明得出这一结论。我们可以看到，将 (4.8) 的右侧改写为 H 之间的线性关系后，它就变为零；这些线性关系对应于某些 $m\in\mathscr{M}$ 的 $m\sigma_{i,\ g}$ 或 $m\sigma_{i,\ j}$。□

对于 A^r 中任意一组元素 $X=(h_1,\dots,h_t)$，我们可以使用广义布赫伯格算法，计算由 $h_1,..,h_t\,(s\ge t)$ 生成的 A^r 子模的 Gr¨格布纳基 $H=(h_1,..,h_s)$。由于 H 的所有元素都属于该子模，因此我们可以找到一个矩阵 $Q=\begin{pmatrix}I_t\\Q'\end{pmatrix}\in M_{s\times t}(A)$，使得

$$H^T=QX^T.$$

其中 I_t 是 $t\times t$ 单位矩阵，而 $(\cdot)^T$ 表示矩阵转置。

定理 6.5. 若 S 是一个矩阵，且 S 的行向量张成关系模 Syz(H)，则 SQ的行向量张成 Syz(X)。

证明. 由于 $SQX^T=SH^T=0$，我们知道 SQ 的行向量属于$Syz(X)$。另一方面，设 $vX^T=0$，其中 $v\in R^t$是某个行向量。令

$$P=\begin{pmatrix}I_t & 0\end{pmatrix}\in M_{t\times s}(A).$$

于是我们有 $X^T=PX^T$和 $PQ=I_t$。因此

$$0=vX^T=(vPQ)X^T=vPH^T\implies vP\in\mathrm{Syz}(H).$$

因此，vP属于 S 的行向量的张成空间，而 $v=vPQ$ 属于 SQ的行向量的张成空间。□

结合上述两个定理，即可计算任意元组 X的 Syz(X)。

7. Ext Groups

在本节中，我们进一步假设 $A=\oplus_{i\ge0}A_i$ 是一个连通分次代数，这意味着 $A_0=k$。(齐次)元素 $a\in A$的次数记为 deg(a)。我们要求滤过 $F_\bullet A$ 是齐次的。因此，伴随分次代数 gr(A)具有两种分次。为避免混淆，由 A 的分次所诱导的 gr(A)上的次数函数也记为 deg(·)，而由滤过诱导的次数函数仍记为 $|\cdot|$。

设 $N=A^r/M$ 是一个分次左 A-模。这里 $A^r=A\{\tilde v_i:\ 1\le i\le r\}$ 是 A 的若干移位的直和，其中基的次数 deg($\tilde v_i$)为整数。本节的目标是通过构造 N 的极小自由分解来计算 Ext 群 $\mathrm{Ext}^*_A(N,k)$。大多数算法改编自交换 Gr¨obner 基理论（参见 [8]）。唯一的不同之处在于构造非交换 Gr¨obner 基的步骤。

首先，我们必须确保表示 $N=A^r/M$ 中的数目 r 尽可能小。令 A 的“分次极大理想”为 $A_+=\oplus_{i>0}A_i$。由中山引理可知，分次左模的极小生成集

A 的 N 对应于 k-向量空间 N/A_+N 的一组基。因此，我们可以使用以下算法来最小化 r。

算法 7.1. 设 N 是 A 上的分次左子模，其表示如下

$$N = A\{\tilde{v}_1, \ldots, \tilde{v}_r\}/(Ax_1 + \cdots + Ax_l)$$

其中，x_i 是 A中 $\tilde{v}_j$的线性组合。我们可以通过以下步骤最小化表示中的 r 。

(1) 对于 $1 \leq i \leq l$，令 y_i 为 x_i 中对于某个 j等于 $\tilde{v}_j$的所有单项式之和。换言之，我们从 x_i的各个和式中移除 $A_+\{\tilde{v}_1, \ldots, \tilde{v}_r\}$ 中的单项式。于是有

$$N/A_+N \cong k\{\tilde{v}_1, \ldots, \tilde{v}_r\}/(ky_1 + \cdots + ky_l).$$

(2) 假设对于某个 $r' \leq r$，$\dim_k(N/A_+N) = r'$。对 y_i进行行约简，以找出生成 N/A_+N的 $\{\tilde{v}_1, \ldots, \tilde{v}_r\}$的一个子集。不失一般性，假设 $\{\tilde{v}_1, \ldots, \tilde{v}_{r'}\}$生成 N/A_+N，并且对于 $j > r'$中的 N/A_+N，我们可以将 $\tilde{v}_j$写成 k中 $\tilde{v}_1$、.....、$\tilde{v}_{r'}$的线性组合。

(3) 对 x_i 执行完全相同的行约简，而不是对 y_i执行。这样，在 N 中，我们可以将 $\tilde{v}_j$ 写成 $\tilde{v}_1$、.....、$\tilde{v}_{r'}$ 以及 $A_+\{\tilde{v}_1, \ldots, \tilde{v}_r\}$ 中其他单项式的 k-线性组合，其中 $j > r'$。重复这一过程后，$\tilde{v}_j$ 可进一步改写为 $\tilde{v}_1$、.....、$\tilde{v}_{r'}$ 的 A-线性组合。因此，我们可以用以下内容替换 x_i

$$x_i' \in Av_1 + \cdots + Av_{r'}$$

使得

$$N \cong A\{\tilde{v}_1, \ldots, \tilde{v}_{r'}\}/(Ax_1' + \cdots + Ax_l')$$

其中 $\{\tilde{v}_1, \ldots, \tilde{v}_{r'}\}$ 是 N 的极小生成集。

接下来，我们需要以下简单算法，用于计算子模 $M \subset A^r$ 的极小生成集。

算法 7.2. 设 M 是由 x_1、.....、x_l 生成的 A^r 的分次左子模。我们可以通过以下步骤，从 $\{x_1, \ldots, x_l\}$ 中找出一个子集，使其成为 M 的极小生成集。

(1) 按次数对 $x_1, \ldots, x_l$ 排序，使得

$$\deg(x_1) \leq \cdots \leq \deg(x_l).$$

(2) 计算由 $x_1, \ldots, x_i$ 生成的子模的 Gröbner 基 H_i，用于 $0 \leq i \leq l$ ($H_0 = \emptyset$)。我们可以对 $H_{i-1} \cup \{\text{red}(x_i, H_{i-1})\}$ 应用算法 5.4，以得到 H_i。(3) 当 $\text{red}(x_i, H_{i-1}) = 0$ 时，将 x_i 标记为 $1 \leq i \leq l$ 的冗余元素。(4) 从 $x_1, \ldots, x_l$ 中移除冗余元素。剩余元素构成 M 的一个极小生成集。

现在，我们已经具备了构造 $N = A^r/M$ 的极小分解所需的全部要素。

算法 7.3。设 $N = A^r/M$ 是一个分次左 A-模，其中 $M \subset A^r$ 由 $x_1, \ldots, x_l$ 生成。我们构造自由分解的前 $s+1$ 项 $F_0, \ldots, F_s$

$$\cdots \to F_s \xrightarrow{d_s} \cdots \xrightarrow{d_3} F_2 \xrightarrow{d_2} F_1 \xrightarrow{d_1} F_0 = A^r \xrightarrow{\epsilon} N$$

通过以下步骤。

(1) 在 N 的表示中应用算法 7.1，将 r 化为极小。 (2) 令 $d_0 = \epsilon$: $F_0 = A^r \to N$ 为商映射。对 $M = \ker(d_0)$ 应用算法 7.2，得到 M 的极小生成集 $\{x_{11}, \dots, x_{1l_1}\}$。 (3) 对于 $i = 1$、2、.....、s，假设 $\{x_{i1}, \dots, x_{il_i}\}$ 是 $\ker(d_{i-1})$ 的极小生成集。定义

$$F_i = A\{v_{i1}, \dots, v_{il_i}\},\ \deg(v_{ij}) = \deg(x_{ij})$$

and

$$d_i(v_{ij}) = x_{ij},\ \textit{for } 1 \le j \le l_i.$$

应用定理 6.5，计算 $\ker(d_i) \cong \mathrm{Syz}(x_{i1}, \dots, x_{il_i})$ 的极小生成集。

通过执行该算法，我们可以发现

$$\mathrm{Ext}_A^i(N, k) \cong \begin{cases} k^r & i = 0, \\ k^{l_i} & 1 \le i \le s. \end{cases}$$

我们称该算法为计算极小分解的垂直方法。我们可以写出该算法的水平版本，按次数逐次执行该算法（依据 A 的分次）。这一版本留待读者编写。关于结合消元算法作为优化手段的水平方法的交换版本，请参阅 [8, 定理 4.8.16]；该方法可以直接移植到我们的情形中。

8. The Steenrod Algebra

在本文余下部分，我们将把非交换 Grobner 基应用于素数 2 下的 Steenrod 代数，并计算其上的 Ext 群。本节回顾 Steenrod代数的一些事实。

令 $\mathscr{A}$ 为素数 2 处的 Steenrod代数。它是一个 Hopf 代数，由次数为 n 的符号 Sq^n，$n \ge 1$ 生成，其关系由下式给出

$$Sq^i Sq^j = \sum_{k=0}^{[i/2]} \binom{j-k-1}{i-2k} Sq^{i+j-k} Sq^k \qquad (Sq^0 = 1)$$

对所有满足 $i < 2j$的 $i, j > 0$ 均成立。它们称为 Adem关系。余乘由下式给出

$$\psi(Sq^n) = \sum_{i=0}^{n} Sq^i \otimes Sq^{n-i}.$$

为了给 $\mathscr{A}$定义一个合适的滤过，我们首先考虑 $\mathscr{A}$的对偶。根据 Milnor [15], 的研究，Steenrod代数 $\mathscr{A}_*$ 的对偶可由下式刻画

$$\mathscr{A}_* = \mathbb{F}_2[\xi_1, \xi_2, \dots], \qquad \deg(\xi_i) = 2^i - 1$$

其余乘由下式给出

$$\psi(\xi_n) = \sum_{i=0}^{n} \xi_{n-i}^{2^i} \otimes \xi_i. \qquad (\xi_0 = 1)$$

$\mathscr{A}_*$ 的单项式基的对偶基记为 $\{P(R)\}$，其中 $R = (r_1, r_2, \dots)$ 遍历所有几乎处处为零的非负整数序列，而 $P(R)$ 与之对偶

$$\xi(R) = \xi_1^{r_1} \xi_2^{r_2} \cdots .$$

Milnor 给出了一个乘积公式，用线性组合的形式计算乘积 $P(R_1)\cdot P(R_2)$，结果仍由 $P(R)$ 表示。

我们在 $\mathscr{A}$ 上定义权函数 w

$$w(P(r_1,r_2,\dots))=\sum_{k,i}(2k-1)a_{k,i}$$

其中$r_k=\sum_i a_{k,\ i}2^i$ 为2进展开。我们在$\mathscr{A}$ 上定义递降滤过

$$F_p\mathscr{A}=k\{P(R):w(P(R))\geq p\}.$$

利用对偶中的余乘积公式不难验证， $F_\bullet\mathscr{A}$ 满足

$$F_p\mathscr{A}\cdot F_q\mathscr{A}\subset F_{p+q}\mathscr{A}$$

并且对每个次数 n，当 p 充分大时，我们有 $F_p\mathscr{A}_n=0$ 。

命题 8.1。Steenrod代数的伴随分次代数同构于一个外代数

$$\mathrm{gr}(\mathscr{A})\cong E[P_j^i:i\geq 0,j>0]$$

其中符号 P_j^i 是.....的投影

$$\tilde{P}_j^i=P(0,\dots,0,\overset{j}{2^i},0,\dots)$$

它与 $\xi_j^{2^i}$ 对偶。gr($\mathscr{A}$) 的分次由下式给出

$$\deg(P_j^i)=2^i(2^j-1),\ |P_j^i|=2j-1.$$

读者可从 [20, 定理 3.2.2] 的证明中找到该定理的证明。

注 8.2。这里的伴随分次代数实际上与 May 的 Steenrod代数伴随分次代数的伴随齐次 Koszul代数（由 Priddy [19] 定义）相同（见 [14]）。

注 8.3。对于素数 $p>2$，Steenrod代数在素数 p 处有类似的滤过，使得其伴随分次代数是高度为 p 的外代数和截断多项式代数的乘积（见 [20, 引理 3.2.4] 之前的注释）。因此，我们也可以将这些算法应用于奇素数下的 Steenrod代数。然而，作者尚未将这些算法编写成计算机程序。

虽然 gr($\mathscr{A}$) 不是有限生成的交换代数，但截断分次代数 $\mathscr{A}_{\leq n}$ 是有限生成的，因此 gr($\mathscr{A}_{\leq n}$) 也是如此。若要计算左 $\mathscr{A}$-模在次数 n 以内的极小分解，只需使用 $\mathscr{A}_{\leq n}$ ，而不必使用 $\mathscr{A}$。

为方便起见，在本节余下部分中，我们默认所有内容都截断到某个次数，使 Gr¨obner 基仍然有定义。

当 $A=\mathscr{A}$ 时，考虑

$$\mathrm{gr}(\mathscr{A})=k[P_j^i:i\geq 0,j>0]/I$$

其中理想由平方元素构成的集合生成

$$G=\{(P_j^i)^2:i\geq 0,j>0\}.$$

显然， G 是 I的Gr¨obner基。我们按次数对生成元 P_j^i 排序。换句话说，我们有

$$P_j^i < P_t^s \Longleftrightarrow \deg(P_j^i) < \deg(P_t^s).$$

由于所有 P_j^i 的次数各不相同，因此这是良定义的。我们对 P_j^i 的单项式排序如下:

$$\begin{aligned} m < m' \Longleftrightarrow & |m| < |m'| \text{ or} \\ & |m| = |m'| \text{ and } m \text{ is } \textit{greater} \text{ than } m' \text{ lexicographically.} \end{aligned}$$

作者采用这种特定的单项式序，是因为相应的计算机程序比作者迄今尝试过的其他版本运行得更快。对于 $\mathscr{A}^r$ 的左子模，我们使用 (5.1) 作为单项式序。

集合

$$\mathscr{B} = \{\text{square-free monomials in variables } P_j^i\}$$

是 gr($\mathscr{A}$) 的一个 $\mathbb{F}_2$-基，而集合

$$\tilde{\mathscr{B}} = \{\tilde{P}_{j_1}^{i_1} \cdots \tilde{P}_{j_l}^{i_l} : \tilde{P}_{j_1}^{i_1} < \cdots < \tilde{P}_{j_l}^{i_l}, l \geq 0\}$$

˜是 $\mathscr{A}$ 的一个 $\mathbb{F}_2$-基。基 $\mathscr{B}$ 与 Monks [16] 中的“P_t^s基”相似，只是生成元的序不同。

9. Computing the Ext Groups over the Steenrod Algebra

在上一节中，我们已经证明，截断分次代数 $\mathscr{A}_{\leq n}$ 是一个有限生成的滤过交换代数。因此，我们可以应用非交换 Gr¨obner 基，计算有限生成分次左 $\mathscr{A}$-模 N 的 Ext 群 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(N,k)$。

作者已将这些算法编写成计算机程序，用于计算各种 N 在一定次数以内的 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(N,k)$。程序代码可在 GitHub [11] 上找到。除了算法 7.3 外，这些计算机程序还采用了交换代数中的以下优化方法，这些方法很容易适用于我们的非交换情形。

(1) 使用 Buchberger 三元组，减少计算 Gr¨obner 基所需的步骤。（参见 [9, 教程 25]）(2) 逐次按次数构造分解，并使用消去。（参见 [8, 定理 4.8.16]）

由于 $\mathscr{A}$ 是一个 Hopf 代数，$\mathrm{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2,\mathbb{F}_2)$ 实际上是 $\mathbb{F}_2$ 上的交换代数。利用上述程序得到分解后，我们可以使用 [5, 6] 中所述的方法，计算 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2,\mathbb{F}_2)$ 中的乘积，以及 A-模 N 上 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(N,\mathbb{F}_2)$ 相对于 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2,\mathbb{F}_2)$ 的模结构。不过，我们总是使用 Gr¨obner 基进行线性代数运算，而不是枚举自由 $\mathscr{A}$-模的 $\mathbb{F}_2$-基。上文提到的消元算法在构造链复形之间的映射时尤其高效，这些映射用于计算 Ext 中的乘积。

我们已经计算出 Steenrod代数 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2,\mathbb{F}_2)$ 的上同调，其结果见定理 1.3。计算范围非常大，包含h_7^2和 h_8。读者可在网页[12]上查看 $\mathrm{Ext}_{\mathscr{A}}^{*,*}(\mathbb{F}_2,\mathbb{F}_2)$ 的图示。

References

[1] J. F. Adams. 关于 Steenrod代数的结构及其应用。 *Comment. Math. Helv.* 32 180 214, 1958 , : – .

[2] J. Apel and W. Lassner. Buchberger 算法及其在李代数包络域计算中的扩展。第 6 卷，第 361–370 页。1988年。交换代数的计算方面。[3] George M. Bergman. 环论的菱形引理。 *Adv. in Math.* 29 2 178 218, , ( ): – 1978 .[4] R. R. Bruner and J. Rognes. 模 2 Steenrod 代数的上同调。*arXiv:2109.13117*. [5] Robert R. Bruner. 大型Ext模的计算。载于 *Computers in geometry and topology (Chicago, IL, 1986)* 114 *Lecture Notes in Pure and Appl. Math.* 79 104 ，第 卷，页码 – 。Dekker，纽约，1989年。[6] Robert R. Bruner. 九十年代的Ext。载于 *Algebraic topology (Oaxtepec, 1991)*， *Contemp. Math.*第 146 卷，页码 71–90。美国数学会，普罗维登斯，罗得岛州，1993年。[7] Bruno Buchberger. 求零维多项式理想剩余类环基元素的算法。 *J. Symbolic Comput.*, 41(3-4):475–511，2006年。由 Michael P. Abramson 从1965年德文原版翻译。[8] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra 2*. 施普林格出版社，柏林，2005年。[9] Martin Kreuzer and Lorenzo Robbiano. *Computational commutative algebra 1*. 施普林格出版社，柏林，2008年。2000年原版的修订重印本。[10] Huishi Li. *Noncommutative Gröbner bases and filtered-graded transfer* 1795 *Lec-* , 第 *ture Notes in Mathematics* 2002 卷。施普林格出版社，柏林，。[11] Weinan Lin. GitHub 仓库。 `https://github.com/WayneLin92/SSeqCpp`. [12] Weinan Lin. Adams谱序列交互图。 `https://waynelin92.github.io/ss/index.html`. [13] Weinan Lin. 模2 斯坦罗德代数的上同调 (t261.0) [数据集], 2023年3月。可从 Zenodo 获取， `https://doi.org/10.5281/zenodo.7786290`. [14] J. Peter May. *The cohomology of restricted lie algebras and of hopf algebras: application to the steenrod algebra* 1964 .

ProQuest LLC，密歇根州安娜堡，。学位论文（博士）——普林斯顿大学。[15] John Milnor. Steenrod代数及其对偶。 *Ann. of Math. (2)*, 67:150–171，1958年。[16] Kenneth G. Monks. Steenrod代数的基变换、单项式关系和 P^s_t基。 *J. Pure Appl. Algebra*, 125(1-3):235–260，1998年。[17] Teo Mora. 交换与非交换 Gr¨obner 基简介。第 134 卷，第 131–173 页。1994年。第二届国际词、语言与组合学讨论会（京都，1992年）。[18] Christian Nassau. `https://www.nullhomotopie.de`. [19] Stewart B. Priddy. Koszul分解与 Steenrod代数。 *Bull. Amer. Math. Soc.*, 76 834 839, 1970 : – .[20] Douglas C. Ravenel. *Complex cobordism and stable homotopy groups of spheres*, *Pure and Applied Mathematics*第 121 卷。学术出版社，奥兰多，佛罗里达州，1986年。[21] Guozhen Wang. `https://github.com/pouiyter/morestablestems`.

Weinan Lin, School of Mathematical Sciences, Peking University, 5 Yi He Yuan Road, Haidian District, Beijing, 100871, China.
电子邮件地址：lwnpku@math.pku.edu.cn