

# DNA 计算的基本代数原理(一)

黄育潜

(江西师范大学计算机信息工程学院 南昌 330022)

**摘 要** 在文中,通过引进  $M$ -粘连代数、 $M$ -剪切代数与  $M$ -重组代数等概念,达到了使与标志集  $M$  相关联的 DNA 计算可按所引进代数中给出的代数定律来推演的目的. 进而研究了这些代数的一系列性质,得到了许多有价值的结果. 它们对 DNA 计算的理论与应用研究必将带来极大的便利.

**关键词** DNA 计算;  $M$ -粘连代数;  $M$ -剪切代数;  $M$ -重组代数; 形式语言

**中图法分类号** TP301

## The Basic Algebraic Principles of DNA Computing (I)

HUANG Yu-Qian

(College of Computer Information and Engineering, Jiangxi Normal University, Nanchang 330022)

**Abstract** By introducing concepts of  $M$ -paste algebra,  $M$ -cut algebra and  $M$ -recombination algebra, the DNA computing associated with mark set  $M$  can be deduced precisely according to the algebraic laws given in the introduced algebras. The author investigates a series of properties of these algebras and obtains many interesting results. These results will give us much convenience in research on the theory and application of DNA computing.

**Keywords** DNA computing;  $M$ -paste algebra;  $M$ -cut algebra;  $M$ -recombination algebra; formal language

## 1 引 言

Head 在其开创性的文献[1]中,通过将每一双链 DNA 分子看作字母表  $D = \{[A/T], [G/C], [G/C], [T/A]\}$  上的一个串,将 DNA 分子在限制性内切酶(它们剪切 DNA 分子为两个带粘性末端的 DNA 片段)和连接酶(它粘连两个具有互补粘性末端的 DNA 片段为一新 DNA 分子)作用下的重组行为抽象为在一定规则控制下的串拼接运算(splicing operation),进而提出拼接系统(splicing system)的概念,用于模拟在一限制性内切酶集与连接酶作用下,一初始有限 DNA 分子集所可能发生的一切重组行为,从而揭示出生命科学领域中的 DNA 重组

现象与理论计算机科学中形式语言理论间的密切关系;DNA 分子重组可用一定的串运算来模拟. 据此,我们可以说,形式语言理论中的 DNA 计算就是现实世界中 DNA 分子重组的形式模型.

近 20 年来,有关 DNA 计算的研究日愈引人注目,成果也层出不穷,归纳起来,主要有如下几个方面:

(1) 对 DNA 计算能力的研究. 由 Head 引进的拼接系统(后人称其为 H-系统)是使用拼接运算作为基本运算的一种语言生成模型,其生成能力与其它计算模型(如 Turing 机)相比,到底强弱如何? Head 在文献[1-2]中证明, NCH(空上下文拼接系统)生成的语言类恰与严格局部可测语言类重合,后者为正则语言类的一个真子类. 其后, Culik 与

Harju<sup>[3]</sup>证明,即使以一正则语言为初始集,按一有限拼接规则集反复迭代(拼接),所生成的语言也仍是一正则语言. Pixton<sup>[4]</sup>对此结果给出了一个本质上更简化的证明. Păun 等(1996)曾模仿 Chomsky 文法在 H-系统中引入在生成过程中起辅助作用的非终极符,称此扩充的系统为扩充 H-系统,但其生成能力仍与 Turing 机相距甚远. 这方面的突破是由 Freund 等在文献[5]中给出的,文中指出,对有限规则集添加一定的控制机制(如引入串的多重性、许可上下文集与禁止上下文集),可得到各种带控制机制的扩充 H-系统,并证明:所有这些扩充 H-系统都是计算完全的(即等价于 Turing 机). 更令人惊喜的是,作者们还证明各类通用 H-系统(它们是具有固定的辅助符集、公理集与拼接规则集的这样一个系统,当给出任一 H-系统  $\gamma$  时,若我们将  $\gamma$  的编码作为此通用系统的一个附加公理时,此通用系统的行为就如同  $\gamma$  的行为)的存在性. 这就向世界宣示,经典计算理论领域中的一切计算都可由一定机制控制下的拼接运算来实现. 近年, Păun<sup>[6]</sup>还引进了双拼接 H-系统、通信分布式 H-系统与变分布式 H-系统,证明了它们也都是计算完全的,并给出有关资源优化方面的若干重要结果. Kobayashi 等<sup>[7]</sup>等则使用带多个谓词符的初等形式系统(一类逻辑方法)来扩充 H-系统,称为 H 形 EFS,证明了它的计算完全性. 并研究了其计算能力与谓词符个数间的联系.

(2) DNA 计算与形式语言理论间的关系的研究,如 DNA 计算与其它语言运算间的关系,各种语言族(特别是,Chomsky 谱系中各语言族)在这些拼接运算下的封闭性及各特殊类 H-系统所生成语言类的特性等. Păun<sup>[8]</sup>首先对拼接运算与其它语言运算的关系进行了细致的讨论,考虑了简单拼接与迭代拼接、有限与无限拼接规则集及规则的半径长等多种情形,得到了若干运算间的相互表示定理及有关语言族封闭性与包含性的定理. 近年, Kobayashi 等<sup>[9]</sup>又引入了 PA-匹配运算及与其对偶的交迭(overlap-ping)运算,研究了在前一运算下的闭包、递归可枚举语言的表示及一些判定问题,讨论了上述两运算的关系及 Chomsky 谱系语言族在非迭代与迭代 PA-匹配与交迭运算下的所有闭包性质. 对特殊类 H-系统的深化研究则首推 Mateescu 等人的成果<sup>[10]</sup>. 他们对所谓简单 H-系统进行了深入的研究,给出了此类 H-系统从有限公理集出发所生成语言

的一系列语言理论性质. 特别是,通过引入跨接(crossover)运算  $\#_M$ ,得到了此类语言的一个用  $\#_M$  表述的代数特征刻画.

(3) DNA 计算的其它特性的研究. 例如,依据现实 DNA 的 Watson-Crick 互补性,将它抽象为一纯语言理论运算. 这方面有 Honkala 等<sup>[11]</sup>和 Mihalache 等<sup>[12]</sup>的方法. 他们据此互补性引进了触发器的概念,并据触发器的复杂性进行了深入研究. 这类研究多与 Lindenmayer 理论中的  $L$ -系统相关. Yokomori 等在文献[13]中则考虑了 DNA 序列的进化问题:① DNA 序列初始如何建立,然后如何进化(长大)成为一复杂的语言;② 进化过程中,最低应要求些什么本原结构. 文中介绍了他们取得的一些结果.

(4) DNA 计算机(或称(生物)分子计算机)的研究. 这方面的突破性成果是 Adleman 在文献[14]中给出的,他使用标准的分子生物学方法,将一个 Hamilton 路径问题的小实例编码为一些 DNA 分子,并在试管中用分子生物学的方法求解,其惊人之处在于,求解步数(即所谓时间复杂性)为  $O(n)$ ,而不是经典计算领域中的  $O(2^n)$ ,奥妙就在于 DNA 计算中巨大的并行机制. 随后, Lipton<sup>[15]</sup>对这种生物计算作了归纳与抽象,提出了由试管集及在其上可作提取、检测与扩增操作组成的 Lipton 生物计算模型. 之后,许多学者开展了用 DNA 计算模拟各种经典算法的实现的研究,发现几乎所有指数级经典算法的 DNA 实现都可降为  $O(n)$  级. Boneh 等在文献[16]中对此有汇总讨论,并提供了所使用的生物计算类型的列表. 文中还提出了一个新的 DNA 计算模型,以试图全面评述有关 DNA 计算能力的许多结果与断言. Adleman 在文献[17]中也勾划了分子计算机的多种抽象模型:非受限模型、受限模型及存储模型. 并给出了分子计算机受限模型的一个基于 DNA 的实现方案,即 DNA 计算机.

欲对 DNA 计算及拼接系统有一全面、系统了解的读者,可参阅文献[18-19]. 本文涉及的形式语言理论中的基本概念与记法,均可在一般教材或论著中找到,此处就不再列参考文献.

本文作者主要受 Mateescu 等在文献[10]中提出的跨接运算  $\#_M$  及其表述的代数特征刻划的启发,对这类与标志集  $M$  相关联的 DNA 计算进行了深入的分析与研究,并提出一字母表  $\Sigma$  上的  $\bullet_M$ -代数( $M$ -粘连代数),  $\langle P_M, S_M, F_M \rangle$ -代数( $M$ -剪切代

数)及 $\#_M$ -代数( $M$ -重组代数)的概念,探讨有关代数运算的特性、规律及相互关联,进而导出这类与标志集 $M$ 相关联的DNA计算的一个完美、精确的代数描述及相关演算系统.这必将对DNA计算的理论与应用研究带来极大的便利.

## 2 $\Sigma$ 上的 $\cdot_M$ -代数( $M$ -粘连代数)

设 $\Sigma$ 是一有限字母表,此后我们总假定它非空. $\Sigma^*$ 记 $\Sigma$ 上所有字(包含空字 $\lambda$ )的集合及 $\Sigma^+$ 是 $\Sigma$ 上所有非空字的集合,即 $\Sigma^+ = \Sigma^* - \{\lambda\}$ . $\Sigma^+$ 的元素记为 $a_1 \cdots a_n$ ,  $a_i \in \Sigma (i=1, 2, \cdots, n)$ .对所有 $w \in \Sigma^*$ ,  $|w|$ 记字 $w$ 的长( $w$ 中出现的字符个数).对 $a \in \Sigma$ ,  $w \in \Sigma^*$ ,  $|w|_a$ 记 $w$ 中字符 $a$ 的出现次数;对 $M \subseteq \Sigma$ ,  $|w|_M$ 记 $M$ 中字符在 $w$ 中的出现次数. $\emptyset$ 记空集.

下面,我们引进本文中第一个重要运算 $\cdot_a$ 与 $\cdot_M$ <sup>①</sup>.

对所有 $x, y \in \Sigma^*$ 及 $a \in \Sigma$ ,我们定义 $\Sigma$ 上的 $a$ -粘连运算 $\cdot_a$ 如下:

$$x \cdot_a y = \begin{cases} x'a y', & \text{若 } x = x'a, y = ay' \\ \text{未定义,} & \text{否则} \end{cases}.$$

此外,应有 $x', y' \in \Sigma^*$ .但是,为了简化叙述,此后在类似情况下,我们也作这种省略.

易见, $x \cdot_a y$ 有定义,记为 $x \cdot_a y \in \Sigma^*$ ,当且仅当 $x \in \Sigma^*a$ 与 $y \in a\Sigma^*$ .

对 $M \subseteq \Sigma$ ,我们定义 $\Sigma$ 上的 $M$ -粘连运算 $\cdot_M$ 如下:

$$x \cdot_M y = \begin{cases} x \cdot_a y, & \text{若存在 } a \in M, \text{使 } x \cdot_a y \in \Sigma^* \\ \text{未定义,} & \text{否则} \end{cases}.$$

由于 $a$ -粘连可看成 $M$ -粘连在 $M = \{a\}$ 时的特殊情形,故后面多是对 $M$ -粘连来讨论,并总假定 $a \in \Sigma$ 及 $M \subseteq \Sigma$ .

**引理 1.** 若 $x \in \Sigma^*a$ ,则 $x \cdot_a a = x$ ;若 $x \in a\Sigma^*$ ,则 $a \cdot_a x = x$ .

证明. 显然.

**引理 2.** 对所有 $x, y \in \Sigma^*$ ,  $M \subseteq \Sigma$ 及 $b \in \Sigma$ ,有

(i)  $x \cdot_M y \in \Sigma^*b$ ,当且仅当存在 $a \in M$ ,使得 $x \in \Sigma^*a$ 与 $y \in a\Sigma^* \cap \Sigma^*b$ ;

(ii)  $x \cdot_M y \in b\Sigma^*$ ,当且仅当存在 $a \in M$ ,使得 $y \in a\Sigma^*$ 与 $x \in b\Sigma^* \cap \Sigma^*a$ .

证明.

(i)

( $\Rightarrow$ )设 $x \cdot_M y \in \Sigma^*b$ .据 $\cdot_M$ 定义,应存在 $a \in M$ ,使得 $x \cdot_M y = x \cdot_a y \in \Sigma^*b$ .设 $x \cdot_a y = wb$ ,  $w \in \Sigma^*$ ,再

据 $\cdot_a$ 定义,应存在 $x', y' \in \Sigma^*$ ,使 $x = x'a \in \Sigma^*a$ ,与 $y = ay' \in a\Sigma^*$ ,且 $x \cdot_a y = x'a \cdot_a ay' = x'ay' = wb \in \Sigma^*b$ .故有, $x \in \Sigma^*a$ 与 $y \in a\Sigma^* \cap \Sigma^*b$ .

( $\Leftarrow$ )设 $a \in M$ ,且 $x \in \Sigma^*a$ 与 $y \in a\Sigma^* \cap \Sigma^*b$ .这时,应存在 $x' \in \Sigma^*$ ,使 $x = x'a$ .又由 $y \in a\Sigma^* \cap \Sigma^*b$ .这时,有以下两种情形:

(a)  $y = a = b$ .从而,利用引理 1,有 $x \cdot_M y = x'a \cdot_a a = x'a = x'b \in \Sigma^*b$ .

(b)  $y \in a\Sigma^*b$ .这时,应存在 $y' \in \Sigma^*$ ,使 $y = ay'b$ .从而,有 $x \cdot_M y = x'a \cdot_a ay'b = x'ay'b \in \Sigma^*b$ .

(ii) 可类似证明.

证毕.

**引理 3.** 对所有 $x, y, z \in \Sigma^*$ 及 $M \subseteq \Sigma$ ,有

(i)  $(x \cdot_M y) \cdot_M z \in \Sigma^*$ ,当且仅当存在 $a, b \in M$ ,使 $(x \cdot_a y) \cdot_b z \in \Sigma^*$ ,且 $x \in \Sigma^*a$ ,  $y \in a\Sigma^* \cap \Sigma^*b$ 及 $z \in b\Sigma^*$ ;

(ii)  $x \cdot_M (y \cdot_M z) \in \Sigma^*$ ,当且仅当存在 $a, b \in M$ ,使 $x \cdot_a (y \cdot_b z) \in \Sigma^*$ ,且 $x \in \Sigma^*a$ ,  $y \in a\Sigma^* \cap \Sigma^*b$ 及 $z \in b\Sigma^*$ .

证明.

(i)

( $\Rightarrow$ )设 $(x \cdot_M y) \cdot_M z = w \in \Sigma^*$ .由 $\cdot_M$ 定义,应存在 $a, b \in M$ ,使 $(x \cdot_a y) \cdot_b z = w \in \Sigma^*$ .从而,据 $\cdot_b$ 的定义,应有 $x \cdot_a y \in \Sigma^*b$ 与 $z \in b\Sigma^*$ .再据引理 2 的(i),应有 $x \in \Sigma^*a$ 与 $y \in a\Sigma^* \cap \Sigma^*b$ .

( $\Leftarrow$ )设存在 $a, b \in M$ ,使 $x \in \Sigma^*a$ ,  $y \in a\Sigma^* \cap \Sigma^*b$ 及 $z \in b\Sigma^*$ .这时,应存在 $x', z' \in \Sigma^*$ ,使 $x = x'a$ ,  $z = bz'$ .而 $y$ 则有以下两种可能:

(a)  $y = a = b$ .从而,利用引理 1,有

$$\begin{aligned} (x \cdot_a y) \cdot_b z &= (x'a \cdot_a a) \cdot_a az' \\ &= x'a \cdot_a az' = x'az' \in \Sigma^*. \end{aligned}$$

(b)  $y \in a\Sigma^*b$ .设 $y = ay'b$ ,  $y' \in \Sigma^*$ .这时,有 $(x \cdot_a y) \cdot_b z = (x'a \cdot_a ay'b) \cdot_b bz' = x'ay'b \cdot_b bz' = x'ay'bz' \in \Sigma^*$ .

(ii) 可类似证明.

证毕.

**推论 1.** 对所有 $x, y, z \in \Sigma^*$ 及 $M \subseteq \Sigma$ ,有

$(x \cdot_M y) \cdot_M z \in \Sigma^*$ ,当且仅当 $x \cdot_M (y \cdot_M z) \in \Sigma^*$ .

证明. 直接由引理 3 的(i)与(ii)推得.

**引理 4.** 对所有 $x, y, z \in \Sigma^*$ 及 $a, b \in \Sigma$ ,有

① 此处 $\cdot_a$ 与 $\cdot_M$ 运算分别与文献[10]中的 $\diamond_a$ 与 $\diamond_M$ 相同,但文献[10]中仅把它们当作定义后面 $\cdot_M$ 运算的一个过渡来用.无任何像本文所展示的运算性质的研究,且文献[10]中将 $\lambda$ 与 $\{\lambda\}$ 分别看作 $\cdot_M$ 与 $\#_M$ 的单位元,这显然是错误的,因为一般来说, $\lambda \notin M$ ,而对应 $\lambda$ 的 $\cdot_a$ 连接实际上就是通常的自然连接.

$$(x \cdot_a y) \cdot_b z = x \cdot_a (y \cdot_b z).$$

证明. 由上面推论 1 知道,  $(x \cdot_a y) \cdot_b z$  无定义, 当且仅当  $x \cdot_a (y \cdot_b z)$  无定义, 故仅需考虑  $(x \cdot_a y) \cdot_b z \in \Sigma^*$  的情形. 这时, 据引理 3 的(i), 应有  $x \in \Sigma^* a$ ,  $y \in a \Sigma^* \cap \Sigma^* b$  及  $z \in b \Sigma^*$ . 设  $x = x'a$ ,  $z = bz'$ , 并分以下两情形考虑  $y$ :

(a)  $y = a = b$ . 这时有

$$\begin{aligned} (x \cdot_a y) \cdot_b z &= (x'a \cdot_a a) \cdot_a az' = x'a \cdot_a az' = x'az' \\ &= x'a \cdot_a az' = x'a \cdot_a (a \cdot_a az') \\ &= x \cdot_a (y \cdot_a z) = x \cdot_a (y \cdot_b z). \end{aligned}$$

(b)  $y \in a \Sigma^* b$ . 设  $y = ay'b$ ,  $y' \in \Sigma^*$ . 这时有

$$\begin{aligned} (x \cdot_a y) \cdot_b z &= (x'a \cdot_a ay'b) \cdot_b bz' = x'ay'b \cdot_b bz' \\ &= x'ay'bz' = x'a \cdot_a ay'bz' \\ &= x'a \cdot_a (ay'b \cdot_b bz') = x \cdot_a (y \cdot_b z). \end{aligned}$$

证毕.

**定理 1.** 对所有  $x, y, z \in \Sigma^*$  及  $M \subseteq \Sigma$ , 有

$$(x \cdot_M y) \cdot_M z = x \cdot_M (y \cdot_M z),$$

即字间  $\cdot_M$  运算满足结合律.

证明. 事实上, 据推论 1,  $(x \cdot_M y) \cdot_M z$  无定义, 当且仅当  $x \cdot_M (y \cdot_M z)$  也无定义. 现设  $(x \cdot_M y) \cdot_M z \in \Sigma^*$ . 据  $\cdot_M$  定义, 应存在  $a, b \in M$ , 使得  $(x \cdot_M y) \cdot_M z = (x \cdot_a y) \cdot_b z$ . 再由引理 4, 我们有  $(x \cdot_a y) \cdot_b z = x \cdot_a (y \cdot_b z)$ . 由于  $a, b \in M$ , 据  $\cdot_M$  定义, 我们有  $(x \cdot_a y) \cdot_b z = x \cdot_M (y \cdot_M z)$ , 从而, 有  $(x \cdot_M y) \cdot_M z = x \cdot_M (y \cdot_M z)$ .

对  $x \cdot_M (y \cdot_M z) \in \Sigma^*$  的情形可类似证明. 证毕.

$\Sigma$  上的  $\cdot_a$  与  $\cdot_M$  运算可自然地推广为  $\Sigma$  上字集间的运算如下:

设  $A, B \subseteq \Sigma^*$ ,  $a \in \Sigma$  及  $M \subseteq \Sigma$ , 我们定义

$$A \cdot_a B = \{x \cdot_a y \mid x \in A, y \in B\},$$

$$A \cdot_M B = \bigcup_{a \in M} A \cdot_a B.$$

由于,  $x \cdot_M y \in \Sigma^*$ , 当且仅当存在  $a \in M$ , 使  $x \cdot_M y = x \cdot_a y$ , 故我们还有  $A \cdot_M B$  的如下等价定义:

$$A \cdot_M B = \{x \cdot_M y \mid x \in A, y \in B\}.$$

下面是  $\Sigma$  上字集间  $\cdot_M$  运算的一些基本性质.

**引理 5.** 若  $A \subseteq \Sigma^* M$ , 则  $A \cdot_M M = A$ ; 若  $A \subseteq M \Sigma^*$ , 则  $M \cdot_M A = A$ .

证明. 我们仅对前一断言作证明, 后一断言的证明可类似进行. 设  $A \subseteq \Sigma^* M$ , 我们的证明分以下两方向进行.

( $\subseteq$ ) 设  $w \in A \cdot_M M$ . 依定义, 应存在  $a \in M$  及  $x \in A, y \in M$ , 使  $w = x \cdot_a y$ . 从而, 必有  $x \in \Sigma^* a$  与  $y \in a \Sigma^* \cap M$ . 故有  $y = a$  及存在  $x' \in \Sigma^*$ , 使  $x = x'a$ . 于是, 我们有  $w = x \cdot_a y = x'a \cdot_a a = x'a = x \in A$ .

( $\supseteq$ ) 设  $x \in A$ . 由于  $A \subseteq \Sigma^* M$ , 故必存在  $a \in M$ , 使  $x \in \Sigma^* a$ . 设  $x = x'a$ ,  $x' \in \Sigma^*$ , 这时, 有  $x = x'a = x'a \cdot_a a \in A \cdot_a M \subseteq A \cdot_M M$ . 证毕.

**引理 6.** 对所有  $A, B \subseteq \Sigma^*$ ,  $a \in \Sigma$  及  $w \in \Sigma^*$ , 有  $w \in A \cdot_a B$ , 当且仅当存在  $ua \in A$  与  $av \in B$ , 使  $w = uav$ .

证明.

( $\Rightarrow$ ) 设  $w \in A \cdot_a B$ . 依定义, 应存在  $x \in A$  与  $y \in B$ , 使  $w = x \cdot_a y$ . 从而, 依字间  $\cdot_a$  运算的定义, 应有  $x \in \Sigma^* a$  与  $y \in a \Sigma^*$ , 即存在  $u, v \in \Sigma^*$ , 使  $x = ua$ ,  $y = av$  且  $w = x \cdot_a y = ua \cdot_a av = uav$ .

( $\Leftarrow$ ) 设  $ua \in A$  与  $av \in B$ . 依  $\cdot_a$  定义, 这时, 显然有  $w = uav = ua \cdot_a av \in A \cdot_a B$ . 证毕.

**引理 7.** 对所有  $A, B \subseteq \Sigma^*$ ,  $a \in \Sigma$ , 有

$$A \cdot_a B = (A \cap \Sigma^* a) \cdot_a (B \cap a \Sigma^*).$$

证明.

( $\subseteq$ ) 设  $w \in A \cdot_a B$ . 由引理 6, 应存在  $ua \in A$  与  $av \in B$ , 使  $w = uav$ . 但显然有  $ua \in A \cap \Sigma^* a$  与  $av \in B \cap a \Sigma^*$ . 故我们有

$$w = uav = ua \cdot_a av \in (A \cap \Sigma^* a) \cdot_a (B \cap a \Sigma^*).$$

( $\supseteq$ ) 设  $w \in (A \cap \Sigma^* a) \cdot_a (B \cap a \Sigma^*)$ . 由引理 6 应存在  $ua \in A \cap \Sigma^* a$  与  $av \in B \cap a \Sigma^*$ , 使  $w = uav$ . 从而, 必有  $ua \in A$  与  $av \in B$ , 且  $w = uav = ua \cdot_a av \in A \cdot_a B$ . 证毕.

**引理 8.** 对所有  $A, B \subseteq \Sigma^*$  及  $M \subseteq \Sigma$ , 有

$$A \cdot_M B = (A \cap \Sigma^* M) \cdot_M (B \cap M \Sigma^*).$$

证明. 事实上,  $w \in A \cdot_M B$ , 依  $\cdot_M$  定义, 当且仅当存在  $a \in M$ , 使  $w \in A \cdot_a B$ . 再依引理 7, 当且仅当  $w \in (A \cap \Sigma^* a) \cdot_a (B \cap a \Sigma^*)$ . 从而依  $\cdot_M$  定义, 当且仅当  $w \in (A \cap \Sigma^* M) \cdot_M (B \cap M \Sigma^*)$ . 证毕.

下面, 我们再给出  $\cdot_M$  运算与通常集合运算与包含关系间的关联引理.

**引理 9.** 对所有  $A, B, C \subseteq \Sigma^*$ ,  $M \subseteq \Sigma$ , 有

$$(i) A \cdot_M (B \cup C) = A \cdot_M B \cup A \cdot_M C;$$

$$(ii) (A \cup B) \cdot_M C = A \cdot_M C \cup B \cdot_M C;$$

$$(iii) A \cdot_M (B \cap C) \subseteq A \cdot_M B \cap A \cdot_M C;$$

$$(iv) (A \cap B) \cdot_M C \subseteq A \cdot_M C \cap B \cdot_M C;$$

$$(v) \text{ 若 } B \subseteq C, \text{ 则 } A \cdot_M B \subseteq A \cdot_M C;$$

$$(iv) \text{ 若 } A \subseteq B, \text{ 则 } A \cdot_M C \subseteq B \cdot_M C.$$

证明.

(i)

( $\subseteq$ ) 设  $w \in A \cdot_M (B \cup C)$ . 这时, 据  $\cdot_M$  定义, 应存在  $a \in M$  及  $x \in A$  与  $y \in B \cup C$ , 使  $w = x \cdot_a y$ . 从而,

或有  $w \in A \cdot_a B \subseteq A \cdot_M B$  (若  $y \in B$ ), 或有  $w \in A \cdot_a C \subseteq A \cdot_M C$  (若  $y \in C$ ). 即总有  $w \in A \cdot_M B \cup A \cdot_M C$ .

( $\supseteq$ ) 设  $w \in A \cdot_M B \cup A \cdot_M C$ . 不妨设  $w \in A \cdot_M B$  ( $w \in A \cdot_M C$  时可类似证明). 这时, 依  $\cdot_M$  定义, 应存在  $a \in M$  及  $x \in A$  与  $y \in B$ , 使  $w = x \cdot_a y$ . 由于  $B \subseteq B \cup C$ , 故自然有

$$w \in A \cdot_a B \subseteq A \cdot_a (B \cup C) \subseteq A \cdot_M (B \cup C).$$

(ii) 可类似(i)进行证明.

(iii) 设  $w \in A \cdot_M (B \cap C)$ . 这时, 应存在  $a \in M$ ,  $x \in A$  与  $y \in B \cap C$ , 使  $w = x \cdot_a y$ . 由此有  $y \in B$  与  $y \in C$ . 从而, 应同时有  $w \in A \cdot_a B \subseteq A \cdot_M B$  与  $w \in A \cdot_a C \subseteq A \cdot_M C$ . 即  $w \in A \cdot_M B \cap A \cdot_M C$ . 这就证明了  $A \cdot_M (B \cap C) \subseteq A \cdot_M B \cap A \cdot_M C$ .

(iv) 可类似(iii)进行证明.

(v) 设  $B \subseteq C$ . 这时, 有  $C = B \cup C'$ ,  $C' \subseteq \Sigma^*$ . 从而, 利用(i)有

$$A \cdot_M B \subseteq A \cdot_M B \cup A \cdot_M C' = A \cdot_M (B \cup C') = A \cdot_M C.$$

(iv) 可类似(v)进行证明. 证毕.

注意, (iii) 与 (iv) 的反包含未必成立. 如说  $a, b \in M$ ,  $A = \{xa, xayb\}$ ,  $B = \{aybz\}$  及  $C = \{bz\}$ . 这时, 显然有  $xaybz = xa \cdot_a aybz \in A \cdot_M B$  与  $xaybz = xayb \cdot_b z \in A \cdot_M C$ . 从而, 应有  $xaybz \in A \cdot_M B \cap A \cdot_M C$ . 但由于  $B \cap C = \emptyset$ , 故  $xaybz \notin A \cdot_M (B \cap C)$ . 即 (iii) 的反包含在此时不成立. 对 (iv) 读者可类似找到其反包含不成立的实例.

**推论 2.** 对所有  $A_i, B_j \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 其中,  $i = 1, 2, \dots, n, j = 1, 2, \dots, m$ , 有

$$(i) (A_1 \cup A_2 \cup \dots \cup A_n) \cdot_M (B_1 \cup B_2 \cup \dots \cup B_m) = \bigcup_{i=1}^n \bigcup_{j=1}^m (A_i \cdot_M B_j);$$

$$(ii) (A_1 \cap A_2 \cap \dots \cap A_n) \cdot_M (B_1 \cap B_2 \cap \dots \cap B_m) \subseteq \bigcap_{i=1}^n \bigcap_{j=1}^m (A_i \cdot_M B_j).$$

证明. 略.

现在, 我们可以给出字集间  $\cdot_M$  运算满足结合律的一个定理.

**定理 2.** 对所有  $A, B, C \subseteq \Sigma^*$  及  $M \subseteq \Sigma$ , 有

$$(A \cdot_M B) \cdot_M C = A \cdot_M (B \cdot_M C).$$

证明. 事实上, 我们有

$$(A \cdot_M B) \cdot_M C = \{x \cdot_M y \mid x \in A, y \in B\} \cdot_M C$$

据字集  $\cdot_M$  的定义

$$= \{(x \cdot_M y) \cdot_M z \mid x \in A, y \in B, z \in C\}$$

据字集  $\cdot_M$  的定义

$$= \{x \cdot_M (y \cdot_M z) \mid x \in A, y \in B, z \in C\} \quad \text{据定理 1}$$

$$= A \cdot_M \{y \cdot_M z \mid y \in B, z \in C\} \quad \text{据字集 } \cdot_M \text{ 的定义}$$

$$= A \cdot_M (B \cdot_M C) \quad \text{据字集 } \cdot_M \text{ 的定义}$$

证毕.

我们用  $P(\Sigma^*)$  记  $\Sigma^*$  的幂集. 为方便叙述, 我们称代数系  $\langle P(\Sigma^*), \cdot_M, M \rangle$  为  $\Sigma$  上的一个  $M$ -粘连代数, 由定理 2 知, 它是一个半群, 且由引理 5,  $M$  部分地具有  $\cdot_M$  运算单位元的性质.

由于字集  $\cdot_M$  运算满足结合律, 故表达式  $A \cdot_M (B \cdot_M C)$  与  $(A \cdot_M B) \cdot_M C$  将统一简记为  $A \cdot_M B \cdot_M C$ . 一般地, 表达式  $A_1 \cdot_M A_2 \cdot_M \dots \cdot_M A_n$  有意义, 它表示  $n$  个字集  $A_1, A_2, \dots, A_n$  的按此序所作的  $\cdot_M$  积.

下面, 我们再引进后面讨论中起重要作用的字集的幂运算  $i(\cdot_M)$ ,  $i \geq 0$  及闭包运算  $*$  ( $\cdot_M$ ) 与  $+$  ( $\cdot_M$ ), 并介绍其若干有用的基本性质.

设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 我们定义

$$A^{0(\cdot_M)} = M,$$

$$A^{1(\cdot_M)} = A,$$

$$A^{(i+1)(\cdot_M)} = A^{i(\cdot_M)} \cdot_M A, \quad i \geq 1.$$

定义  $A$  的关于  $\cdot_M$  的星闭包  $*$  ( $\cdot_M$ ) 与正闭包  $+$  ( $\cdot_M$ ) 如下:

$$A^*(\cdot_M) = A^{0(\cdot_M)} \cup A^{1(\cdot_M)} \cup \dots \cup A^{i(\cdot_M)} \cup \dots,$$

$$A^+(\cdot_M) = A^{1(\cdot_M)} \cup A^{2(\cdot_M)} \cup \dots \cup A^{i(\cdot_M)} \cup \dots.$$

显然, 我们有  $A^*(\cdot_M) = A^+(\cdot_M) \cup A^{0(\cdot_M)}$ . 此外, 关于幂运算  $i(\cdot_M)$ ,  $i \geq 1$ , 也满足通常的幂运算定律.

**引理 10.**  $A^{i(\cdot_M)} \cdot_M A^{j(\cdot_M)} = A^{(i+j)(\cdot_M)}$ ,  $i, j \geq 1$ .

证明. 对  $j$  作归纳,

基础:  $j = 1$  时, 依定义即有  $A^{i(\cdot_M)} \cdot_M A^{1(\cdot_M)} = A^{(i+1)(\cdot_M)}$ .

归纳: 设  $j = k$  时, 结论成立, 现考虑  $k+1$  的情形. 这时, 我们有

$$A^{i(\cdot_M)} \cdot_M A^{(k+1)(\cdot_M)} = A^{i(\cdot_M)} \cdot_M (A^{k(\cdot_M)} \cdot_M A)$$

依  $(k+1)(\cdot_M)$  定义

$$= (A^{i(\cdot_M)} \cdot_M A^{k(\cdot_M)}) \cdot_M A \quad \text{定理 2}$$

$$= A^{(i+k)(\cdot_M)} \cdot_M A \quad \text{归纳假设}$$

$$= A^{(i+k+1)(\cdot_M)} \quad \cdot_M \text{ 指数定义}$$

证毕.

**引理 11.**  $(A^{i(\cdot_M)})^{j(\cdot_M)} = A^{ij(\cdot_M)}$ ,  $i, j \geq 1$  (写法  $ij$  表示  $i$  与  $j$  的积).

证明. 略.

注意, 引理 10、引理 11 中  $i, j \geq 1$  的限制是因为: 一般未必有  $A^{i(\cdot_M)} \cdot_M A^{0(\cdot_M)} = A^{i(\cdot_M)}$  与  $A^{0(\cdot_M)} \cdot_M A^{i(\cdot_M)} = A^{i(\cdot_M)}$ , 除非分别有  $A \subseteq \Sigma^* M$  与  $A \subseteq M \Sigma^*$ .

为方便后面的讨论, 我们再引进以下若干记号,

并介绍若干有关结果.

设  $M \subseteq \Sigma$ . 我们记  $\Sigma_{\bar{M}} = \Sigma - M$ . 这时,  $\Sigma_{\bar{M}}^*$  为  $\Sigma^*$  中不含  $M$  中符号的所有字的集合, 即  $\Sigma_{\bar{M}}^* = \Sigma^* - \Sigma^* M \Sigma^*$ . 显然, 我们有以下一些结果.

**引理 12.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

(i) 若  $B \subseteq \Sigma_{\bar{M}}^*$ , 则  $A \cdot_M B = \emptyset$ ;

(ii) 若  $B \subseteq \Sigma^* \Sigma_{\bar{M}}$ , 则  $B \cdot_M A = \emptyset$ .

证明. 显然.

此引理表明, 对任一  $A \subseteq \Sigma^*$ , 用非  $M$  字符开头的字集作  $\cdot_M$  右乘, 或用非  $M$  字符结尾的字集作  $\cdot_M$  左乘, 其积均为空集. 下面, 我们再引进记号

$$A_M^{(0)} = \{w \mid w \in A, \text{ 且 } |w|_M = 0\}.$$

易见, 有  $A_M^{(0)} = A \cap \Sigma_{\bar{M}}^*$ . 这时, 我们令  $A_M = A - A_M^{(0)}$ . 于是, 由上面引理及推论 2(i), 我们可得以下结果.

**引理 13.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有  $A \cdot_M A = A_M \cdot_M A_M$ .

证明. 事实上, 我们有

$$\begin{aligned} A \cdot_M A &= (A_M \cup A_M^{(0)}) \cdot_M (A_M \cup A_M^{(0)}) \stackrel{\text{推论 2(i)}}{=} A_M \cup A_M^{(0)} \\ &= A_M \cdot_M A_M \cup A_M \cdot_M A_M^{(0)} \cup A_M^{(0)} \cdot_M A_M \cup A_M^{(0)} \cdot_M A_M^{(0)} \\ &= A_M \cdot_M A_M. \end{aligned}$$

证毕.

### 3 $\Sigma$ 上的 $\langle P_M, S_M, F_M \rangle$ -代数 ( $M$ -剪切代数)

设  $\Sigma$  是一有限字母表,  $w \in \Sigma^*$  与  $a \in \Sigma$ . 我们定义  $w$  的  $a$  尾前缀 (简称  $a$ -前缀) 集  $P_a(w)$  与  $a$  头后缀 (简称  $a$ -后缀) 集  $S_a(w)$  如下:

$$P_a(w) = \{ua \mid w = uav, u, v \in \Sigma^*\},$$

$$S_a(w) = \{av \mid w = uav, u, v \in \Sigma^*\}.$$

特别地, 有  $P_a(a) = S_a(a) = \{a\}$ .

对  $w \in \Sigma^*$  与  $a \in \Sigma$ , 我们定义

$$P_a(A) = \bigcup_{x \in A} P_a(x),$$

$$S_a(A) = \bigcup_{x \in A} S_a(x).$$

对  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ ,  $w$  的  $M$ -前缀集  $P_M(w)$  与  $M$ -后缀集  $S_M(w)$  定义为

$$P_M(w) = \bigcup_{a \in M} P_a(w),$$

$$S_M(w) = \bigcup_{a \in M} S_a(w).$$

设  $A \subseteq \Sigma^*$ ,  $A$  的  $M$ -前缀集  $P_M(A)$  与  $M$ -后缀集  $S_M(A)$  定义为

$$P_M(A) = \bigcup_{w \in A} P_M(w),$$

$$S_M(A) = \bigcup_{w \in A} S_M(w).$$

特别地, 有  $P_M(M) = M = S_M(M)$ , 且若  $A \subseteq \Sigma_{\bar{M}}^*$ , 则有  $P_M(A) = S_M(A) = \emptyset$ . 此外, 易见, 若  $|w|_a \neq 0$ , 则有  $P_a(w) \subseteq \Sigma^* a$  与  $S_a(w) \subseteq a \Sigma^*$ , 及若  $A \neq A_M^{(0)}$ , 则有  $P_M(A) \subseteq \Sigma^* M$  与  $S_M(A) \subseteq M \Sigma^*$ . 后面, 我们有时泛称  $P_a$  与  $P_M$  为  $P$  运算, 称  $S_a$  与  $S_M$  为  $S$  运算.

下面, 我们来介绍  $P$  与  $S$  运算的若干基本性质.

**引理 14.** 对所有  $w \in \Sigma^*$  与  $a \in \Sigma$ , 有

$$P_a(P_a(w)) = P_a(w),$$

$$S_a(S_a(w)) = S_a(w).$$

证明. 先证  $P_a(P_a(w)) = P_a(w)$ .

( $\subseteq$ ) 设  $ua \in P_a(P_a(w))$ . 依定义, 应存在  $w'a \in P_a(w)$ , 使  $ua \in P_a(w'a)$ . 这时, 有以下两种可能:

(a)  $|u| = |w'|$ . 从而, 有  $ua = w'a \in P_a(w)$ ;

(b)  $|u| < |w'|$ . 这时, 应存在  $y' \in \Sigma^*$ , 使  $w'a = uay'a$ . 又由  $w'a \in P_a(w)$ , 依定义, 应存在  $y \in \Sigma^*$ , 使  $w = w'ay = uay'ay$ , 故有  $ua \in P_a(w)$ .

( $\supseteq$ ) 设  $ua \in P_a(w)$ . 依定义, 必有  $ua \in \Sigma^* a$ . 从而,  $ua \in P_a(ua) \subseteq P_a(P_a(w))$ .

对  $S_a(S_a(w)) = S_a(w)$  可类似证明. 证毕.

**推论 3.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

$$P_M(P_M(A)) = P_M(A),$$

$$S_M(S_M(A)) = S_M(A).$$

证明. 显然.

**引理 15.** 对所有  $w, u \in \Sigma^*$  与  $a, b \in \Sigma$ , 有

(i)  $u \in P_a(S_b(w))$ , 当且仅当存在  $x, z \in \Sigma^*$ , 使得  $w = xuz$ , 且  $u \in \Sigma^* a \cap b \Sigma^*$ ;

(ii)  $u \in S_b(P_a(w))$ , 当且仅当存在  $x, z \in \Sigma^*$ , 使得  $w = xuz$ , 且  $u \in \Sigma^* a \cap b \Sigma^*$ .

证明.

(i)

( $\Rightarrow$ ) 设  $u \in P_a(S_b(w))$ . 这时, 据  $P_a$  定义, 应存在  $w' \in S_b(w) \subseteq b \Sigma^*$ , 使得  $w' = u'a z$ , 且  $u = u'a \in \Sigma^* a$ . 再由  $w' \in S_b(w) \subseteq b \Sigma^*$  及  $S_b$  定义, 应有  $w = xw'$ ,  $x \in \Sigma^*$ . 考虑到  $w' = u'a z \in b \Sigma^*$ , 我们应有  $w = xw' = xu'a z = xuz$ . 故再据  $w' = u'a z = uz \in S_b(w) \subseteq b \Sigma^*$ , 有  $u \in b \Sigma^*$ , 从而, 有  $u \in \Sigma^* a \cap b \Sigma^*$ .

( $\Leftarrow$ ) 设存在  $x, z \in \Sigma^*$ , 使  $w = xuz$ , 且  $u \in \Sigma^* a \cap b \Sigma^*$ . 这时, 有以下两种情形:

(a)  $|u| = 1$ . 从而, 由  $u \in \Sigma^* a \cap b \Sigma^*$  知, 必有  $u =$

$a=b$ . 这时, 有  $w=xaz$ . 据  $S_a$  的定义, 有  $az \in S_a(w)$ . 再据  $P_a$  定义, 有  $u=a \in P_a(az) \subseteq P_a(S_a(w)) = P_a(S_b(w))$ .

(b)  $|u| \geq 2$ . 这时, 必存在  $y \in \Sigma^*$ , 使  $u=bya$ ,  $w=xbyaz$ . 据  $S_a$  与  $P_a$  定义, 应有  $byaz \in S_b(w)$  及  $u=bya \in P_a(byaz) \subseteq P_a(S_b(w))$ .

(ii) 可类似证明.

证毕.

### 定理 3.

(i) 对所有  $a, b \in \Sigma$  与  $w \in \Sigma^*$ ,  $P_a(S_b(w)) = S_b(P_a(w))$ ;

(ii) 对所有  $a, b \in \Sigma$  与  $A \subseteq \Sigma^*$ ,  $P_a(S_b(A)) = S_b(P_a(A))$ .

证明.

(i) 事实上, 设  $u \in P_a(P_b(w))$ . 据引理 15 的 (i), 即当且仅当存在  $x, z \in \Sigma^*$ , 使得  $w=xuz$ , 且  $u \in \Sigma^*a \cap b\Sigma^*$ . 又据同一引理的 (ii), 即当且仅当  $u \in S_b(P_a(w))$ , 故有  $P_a(S_b(w)) = S_b(P_a(w))$ .

(ii) 显然.

证毕.

关于字与字集的(通常)连接、 $a$ -粘连、 $M$ -粘连,  $P$  与  $S$  运算有如下一些结果.

**引理 16.** 对所有  $x, y \in \Sigma^*$  与  $a \in \Sigma$ , 有

(i)  $P_a(xy) = P_a(x) \cup xP_a(y)$ ;

(ii)  $S_a(xy) = S_a(y) \cup S_a(x)y$ .

证明.

(i)

( $\subseteq$ ) 设  $ua \in P_a(xy)$ . 据  $P_a$  定义, 应存在  $z \in \Sigma^*$ , 使  $xy=uaz$ . 这时, 若  $|x| \geq |ua|$ , 则有  $x=uax'$ ,  $x' \in \Sigma^*$ , 从而, 有  $ua \in P_a(x)$ ; 若  $|x| < |ua|$ , 设  $ua=xu'a$ ,  $u' \in \Sigma^*$ , 于是, 我们有  $xy=uaz=xu'az$ . 从而, 有  $y=u'az$  及  $u'a \in P_a(y)$ . 故有  $ua=xu'a \in xP_a(y)$ .

( $\supseteq$ ) 设  $ua \in P_a(x) \cup xP_a(y)$ . 这时, 若  $ua \in P_a(x)$ , 则依定义, 应存在  $z \in \Sigma^*$ , 使  $x=uaz$ . 从而, 有  $xy=uaz$ , 故  $ua \in P_a(xy)$ . 若  $ua \in xP_a(y)$ , 则应存在  $u'a \in P_a(y)$ , 使  $ua=xu'a$ . 又据  $u'a \in P_a(y)$ , 依  $P_a$  定义, 应存在  $v \in \Sigma^*$ , 使  $y=u'av$ . 这时, 有  $xy=xu'av=uav$ . 故有  $ua \in P_a(xy)$ .

(ii) 可类似证明.

证毕.

**引理 17.** 对所有  $x, y \in \Sigma^*$  与  $a, b \in \Sigma$ , 若  $x \cdot_b b \in \Sigma^*$ , 则有

(i)  $P_a(x \cdot_b y) = P_a(x) \cup x \cdot_b P_a(y)$ ;

(ii)  $S_a(x \cdot_b y) = S_a(y) \cup S_a(x) \cdot_b y$ .

证明.

(i)

( $\subseteq$ ) 设  $ua \in P_a(x \cdot_b y)$ , 且  $x \cdot_b y = x'by'$ , 其中,

$x=x'b, y=by', x', y' \in \Sigma^*$ . 由  $P_a$  定义, 应存在  $v \in \Sigma^*$ , 使得  $x'by' = x \cdot_b y = uav$ . 这时, 有以下两种情形:

(a)  $ua \in P_a(x'b) = P_a(x)$ . 由此, 显然有  $ua \in P_a(x) \subseteq P_a(x) \cup x \cdot_b P_a(y)$ .

(b)  $ua \notin P_a(x'b)$ . 从而, 应有  $|ua| > |x'b|$ . 据此, 应存在  $z \in \Sigma^*$ , 使得  $ua=x'bza$ . 从而, 有  $x'by' = x'bzav$ . 于是, 我们有  $y=by' = bzaav$ . 据  $P_a$  定义, 将有  $bza \in P_a(y)$ . 由此有  $ua=x'bza = x'b \cdot_b bza \in x \cdot_b P_a(y) \subseteq P_a(x) \cup x \cdot_b P_a(y)$ .

( $\supseteq$ ) 设  $ua \in P_a(x) \cup x \cdot_b P_a(y)$ , 且  $x \cdot_b y = x'by'$ , 其中,  $x=x'b, y=by', x', y' \in \Sigma^*$ . 这时, 有以下两种情形:

(a)  $ua \in P_a(x)$ . 由于  $x \cdot_b y = x'by' = xy'$ . 据引理 16 的 (i), 应有  $ua \in P_a(x) \cup x \cdot_b P_a(y') = P_a(xy') = P_a(x \cdot_b y)$ .

(b)  $ua \in x \cdot_b P_a(y)$ . 据此, 应存在  $z \in P_a(y)$ , 使得  $ua = x \cdot_b z$ . 设  $z=bz', z' \in \Sigma^*$ . 于是, 有  $ua = x'bz'$ . 又由于  $z \in P_a(y)$ , 据定义, 应存在  $v \in \Sigma^*$ , 使得  $y=zv$ . 于是, 我们有  $x \cdot_b y = x'by' = x'y = x'zv = x'bz'v = x'b \cdot_b bz'v = x \cdot_b zv$ . 从而, 据  $P_a$  定义, 我们有  $ua = x \cdot_b z \in P_a(x \cdot_b zv) = P_a(x \cdot_b y)$ .

(ii) 可类似证明.

证毕.

**推论 4.** 对所有  $x, y \in \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $x \cdot_M y \in \Sigma^*$ , 则对所有  $a \in M$ , 有

(i)  $p_a(x \cdot_M y) = p_a(x) \cup x \cdot_M p_a(y)$ ;

(ii)  $S_a(x \cdot_M y) = S_a(y) \cup S_a(x) \cdot_M y$ .

证明.

(i) 由于  $x \cdot_M y \in \Sigma^*$ , 当且仅当存在  $b \in M$ , 使得  $x \cdot_M y = x \cdot_b y$ . 利用引理 17 的 (i), 显然有

$$p_a(x \cdot_M y) = p_a(x \cdot_b y) = p_a(x) \cup x \cdot_b p_a(y) = p_a(x) \cup x \cdot_M p_a(y).$$

(ii) 可类似证明.

证毕.

**推论 5.** 对所有  $x, y \in \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $x \cdot_M y \in \Sigma^*$ , 则有

(i)  $P_M(x \cdot_M y) = P_M(x) \cup x \cdot_M P_M(y)$ ;

(ii)  $S_M(x \cdot_M y) = S_M(y) \cup S_M(x) \cdot_M y$ .

证明.

(i) 事实上, 据  $P_M$  定义及推论 4, 我们有

$$\begin{aligned} P_M(x \cdot_M y) &= \bigcup_{a \in M} p_a(x \cdot_M y) \\ &= \bigcup_{a \in M} (p_a(x) \cup x \cdot_M p_a(y)) \\ &= \bigcup_{a \in M} p_a(x) \cup \bigcup_{a \in M} (x \cdot_M p_a(y)) \\ &= P_M(x) \cup x \cdot_M P_M(y). \end{aligned}$$

(ii) 可类似证明.

证毕.

关于  $P$  与  $S$  运算与集合运算和包含关系间的关联,由以下引理给出.

**引理 18.** 对所有  $A, B \subseteq \Sigma^*$  与  $a \in \Sigma$ , 有

(i)  $P_a(AB) = P_a(A) \cup AP_a(B)$ ;  $S_a(AB) = S_a(B) \cup S_a(A)B$ .

(ii)  $P_a(A \cup B) = P_a(A) \cup P_a(B)$ ;  $S_a(A \cup B) = S_a(A) \cup S_a(B)$ .

(iii)  $P_a(A \cap B) \subseteq P_a(A) \cap P_a(B)$ ;  $S_a(A \cap B) \subseteq S_a(A) \cap S_a(B)$ .

(iv) 若  $A \subseteq B$ , 则  $P_a(A) \subseteq P_a(B)$  及  $S_a(A) \subseteq S_a(B)$ .

证明.

(i) 先证  $P_a(AB) = P_a(A) \cup AP_a(B)$ .

( $\subseteq$ ) 设  $ua \in P_a(AB)$ . 由定义, 应存在  $x \in A$  与  $y \in B$ , 使  $ua \in P_a(xy)$ . 于是, 据引理 16 的 (i), 有  $ua \in P_a(x) \cup xP_a(y) \subseteq P_a(A) \cup AP_a(B)$ .

( $\supseteq$ ) 设  $ua \in P_a(A) \cup AP_a(B)$ . 这时, 有以下两种情形:

(a)  $ua \in P_a(A)$ . 从而, 应存在  $x \in A$ , 使  $ua \in P_a(x)$ . 于是, 据引理 16 的 (i), 对任何  $y \in \Sigma^*$ , 都有  $ua \in P_a(x) \subseteq P_a(x) \cup xP_a(y) = P_a(xy)$ . 故若取  $y \in B$ , 则自然有  $ua \in P_a(xy) \subseteq P_a(AB)$ ;

(b)  $ua \in AP_a(B)$ . 从而, 应存在  $x \in A$  与  $y \in B$ , 使  $ua \in xP_a(y)$ . 同样, 据引理 16 的 (i), 有  $ua \in xP_a(y) \subseteq P_a(x) \cup xP_a(y) = P_a(xy) \subseteq P_a(AB)$ .

对  $S_a(AB) = S_a(B) \cup S_a(A)B$  可类似证明.

(ii) 显然.

(iii) 先证  $P_a(A \cap B) \subseteq P_a(A) \cap P_a(B)$ .

设  $ua \in P_a(A \cap B)$ . 由定义, 应存在  $w \in A \cap B$ , 使  $ua \in P_a(w)$ . 由此, 有  $w \in A$  与  $w \in B$ . 故应有  $ua \in P_a(w) \subseteq P_a(A)$  与  $ua \in P_a(w) \subseteq P_a(B)$ . 所以,  $ua \in P_a(A) \cap P_a(B)$ .

对  $S_a(A \cap B) \subseteq S_a(A) \cap S_a(B)$  可类似证明.

(iv) 显然. 证毕.

注意, 本引理 (iii) 中的反包含一般并不成立. 例如, 设  $A = ab^+$ ,  $B = ac^+$ . 这时  $A \cap B = \emptyset$ . 显然, 我们有  $P_a(A) = P_a(B) = \{a\}$ , 故  $P_a(A) \cap P_a(B) = \{a\}$ . 但  $P_a(A \cap B) = \emptyset$ . 对  $S_a$  的情形, 可考虑  $A = b^+a$  与  $B = c^+a$  的结果.

显然, 对  $M \subseteq \Sigma$ , 在本引理中, 用  $P_M$  代替  $P_a$  及用  $S_M$  代替  $S_a$ , (i) ~ (iv) 的结论必仍成立. 读者有兴趣可证之. 此外, (ii) 与 (iii) 中的结论也易推广到

$\bigcup_{i=1}^n A_i$  及  $\bigcap_{i=1}^n A_i$  的情形.

下面, 我们再给出有关  $P$  与  $S$  间关系的若干结果.

**定理 4.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ ,  $P_M(S_M(A)) = S_M(P_M(A))$ .

证明. 事实上, 我们有

$$\begin{aligned} P_M(S_M(A)) &= P_M\left(\bigcup_{a \in M} S_a(A)\right) \quad \text{据 } S_M \text{ 定义} \\ &= \bigcup_{a \in M} (P_M(S_a(A))) \quad \text{引理 18(ii) 的推广版} \\ &= \bigcup_{a \in M} \left(\bigcup_{b \in M} P_b(S_a(A))\right) \quad \text{据 } P_M \text{ 的定义} \\ &= \bigcup_{a \in M} \left(\bigcup_{b \in M} S_a(P_b(A))\right) \quad \text{定理 3 的 (ii)} \\ &= \bigcup_{a \in M} (S_a(\bigcup_{b \in M} P_b(A))) \quad \text{引理 18(ii) 的推广版} \\ &= \bigcup_{a \in M} S_a(P_M(A)) \quad \text{据 } P_M \text{ 的定义} \\ &= S_M(P_M(A)) \quad \text{据 } S_M \text{ 定义} \end{aligned}$$

证毕.

**引理 19.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 这时, 对所有  $a \in M$  与  $x \in \Sigma^*$ ,  $xa \in P_M(A)$ , 当且仅当存在  $y \in \Sigma^*$ , 使得  $ay \in S_M(A)$ .

证明.

( $\Rightarrow$ ) 设  $xa \in P_M(A)$ . 依定义, 应存在  $w \in A$  及  $y \in \Sigma^*$ , 使  $w = xay$ . 从而, 存在  $y \in \Sigma^*$ , 使  $ay \in S_M(w) \subseteq S_M(A)$ ;

( $\Leftarrow$ ) 设存在  $y \in \Sigma^*$ , 使得  $ay \in S_M(A)$ . 依定义, 应存在  $w \in A$  及  $x \in \Sigma^*$ , 使得  $w = xay$ . 从而, 存在  $x \in \Sigma^*$ , 使  $xa \subseteq P_a(w) \subseteq P_M(A)$ . 证毕.

**引理 20.** 设  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 对所有  $w \in \Sigma^*$ , 有  $w \in P_M(A) \cdot_M S_M(B)$ , 当且仅当存在  $a \in M$ ,  $ua \in P_M(A)$  与  $av \in S_M(A)$ , 使得  $w = uav$ .

证明.

( $\Rightarrow$ ) 设  $w \in P_M(A) \cdot_M S_M(B)$ . 依定义, 应存在  $a \in M$ ,  $ua \in P_M(A)$  与  $av \in S_M(A)$ , 使得  $w = ua \cdot_a av = uav$ .

( $\Leftarrow$ ) 设存在  $a \in M$ ,  $ua \in P_M(A)$  与  $av \in S_M(A)$ , 使得  $w = uav$ . 这时, 显然有  $w = uav = ua \cdot_a av \in P_M(A) \cdot_M S_M(B)$ . 证毕.

**引理 21.** 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

(i)  $P_M(A \cdot_M B) \subseteq P_M(A) \cup A \cdot_M P_M(B)$ ;

(ii)  $S_M(A \cdot_M B) \subseteq S_M(B) \cup S_M(A) \cdot_M B$ .

证明.

(i) 对每一  $a \in M$ , 设  $ua \in P_a(A \cdot_M B)$ . 据  $P_a$  定义, 应存在  $w \in A \cdot_M B$  与  $v \in \Sigma^*$ , 使得  $w = uav$ . 由  $w \in A \cdot_M B$  知, 应存在  $b \in M$ ,  $x \in A$  与  $y \in B$ , 使得  $w = x \cdot_b y$ . 从而, 有  $ua \in P_a(w) = P_a(x \cdot_b y)$ . 由引理 17 的 (i) 知, 有  $ua \in P_a(x) \cup x \cdot_b P_a(y) \subseteq P_M(A) \cup$



$A \cdot_M P_M(B)$ .

(ii) 可类似证明. 证毕.

注意,本引理的“ $\subseteq$ ”如改成“ $\supseteq$ ”,结论一般並不成立. 例如,设  $\Sigma = \{a, b, c, d\}$ ,  $M = \{a, b\}$ ,  $A = \{cacb, dbda\}$  与  $B = \{acc, add\}$ . 这时,有

$$\begin{aligned} A \cdot_M B &= A \cdot_a B \cup A \cdot_b B \\ &= \{cacb, dbda\} \cdot_a \{acc, add\} \cup \\ &\quad \{cacb, dbda\} \cdot_b \{acc, add\} \\ &= \{dbdacc, dbdadd\} \cup \emptyset \\ &= \{dbdacc, dbdadd\}, \end{aligned}$$

$$\begin{aligned} P_M(A \cdot_M B) &= P_M(\{dbdacc, dbdadd\}) \\ &= \{db, dbda\}, \end{aligned}$$

及  $P_M(A) = \{ca, cacb, db, dbda\}$ ,

$$P_M(B) = \{a\}.$$

这时,我们有

$$P_M(A) \cup A \cdot_M P_M(B) = \{ca, cacb, db, dbda\}.$$

显然有  $P_M(A) \cup A \cdot_M P_M(B)$  不包含于  $P_M(A \cdot_M B)$  中. 对  $S$  操作的反例,读者可仿此构造. 此外,我们有以下引理.

**引理 22.** 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ ,有

(i)  $A \cdot_M P_M(B) \subseteq P_M(A \cdot_M B)$ ;

(ii)  $S_M(A) \cdot_M B \subseteq S_M(A \cdot_M B)$ .

证明.

(i) 对每一  $a \in M$ , 设  $ua \in A \cdot_M P_a(B)$ . 依  $\cdot_M$  定义,应存在  $b \in M$ ,  $x'b \in A$  与  $by' \in P_a(B)$ ,  $x', y' \in \Sigma^*$ , 使得  $ua = x'by'$ . 这时,有以下两种情形:

(a)  $y' = \lambda$ . 从而,有  $u = x'$  与  $a = b$ . 由此,有  $a = b = by' \in P_a(B)$ . 据此,应存在  $y \in B$  及  $v \in \Sigma^*$ , 使得  $y = av = by'v$ . 于是,我们有  $x'by'v = x'b \cdot_b by'v \in A \cdot_b B \subseteq A \cdot_M B$ . 从而,有  $ua = x'by' \in P_a(x'by'v) \subseteq P_M(A \cdot_M B)$ .

(b)  $y' \neq \lambda$ . 由  $by' \in P_a(B)$  知,可设  $y' = za$ ,  $z \in \Sigma^*$ . 从而,有  $ua = x'by' = x'bza$ . 由  $bza = by' \in P_a(B)$ , 据  $P_a$  定义,应存在  $y \in B$  与  $v \in \Sigma^*$ , 使得  $y = bzav$ . 由此,我们有  $uav = x'bzav = x'b \cdot_b bzav \in A \cdot_b B$ . 最后,我们有  $ua = P_a(uav) \subseteq P_a(A \cdot_M B) \subseteq P_M(A \cdot_M B)$ .

(ii) 可类似证明. 证毕.

为了探讨  $P_M(A) \subseteq P_M(A \cdot_M B)$  与  $S_M(B) \subseteq S_M(A \cdot_M B)$  成立的条件,我们需要引进以下一些概念和记法.

设  $A \subseteq \Sigma^*$ , 我们定义

$$\text{tail}(A) = \{t \in \Sigma \mid \text{存在 } x \in \Sigma^*, \text{ 使得 } xt \in A\},$$

$$\text{head}(A) = \{h \in \Sigma \mid \text{存在 } x \in \Sigma^*, \text{ 使得 } hx \in A\}.$$

易见,  $\text{tail}(A)$  与  $\text{head}(A)$  分别为字集  $A$  中非空字之尾符与首符集.

对任意  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 我们说  $A$  与  $B$  关于  $\cdot_M$  是完全的, 记为  $M(\cdot, A, B)$ , 假如对每一  $x \in A$ , 存在  $y \in B$  及对每一  $y \in B$ , 存在  $x \in A$ , 使得  $x \cdot_M y \in \Sigma^*$ .

由于  $x \cdot_M y \in \Sigma^*$ , 当且仅当存在  $a \in M$ , 使得  $x \cdot_M y = x \cdot_a y$ . 从而,我们有  $M(\cdot, A, B)$  成立, 当且仅当对每一  $x \in A$ , 存在  $a \in M$  与  $y \in B$  及对每一  $y \in B$ , 存在  $a \in M$  与  $x \in A$ , 使得  $x \cdot_a y \in \Sigma^*$ .

下面,我们来建立上述概念的一些有用性质.

**引理 23.** 对任意  $x \in \Sigma^*$ ,  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

(i)  $\text{tail}(P_M(x)) = \text{head}(S_M(x))$ ;

(ii)  $\text{tail}(P_M(A)) = \text{head}(S_M(A))$ .

证明.

(i)

( $\subseteq$ ) 对任一  $a \in \text{tail}(P_M(x))$ , 据  $\text{tail}$  定义, 应存在  $u \in \Sigma^*$ , 使得  $ua \in P_M(x)$ . 再据  $P_M$  定义, 应存在  $v \in \Sigma^*$ , 使得  $x = uav$ . 由此, 有  $av \in S_M(x)$ . 再据  $\text{head}$  定义, 我们就有  $a \in \text{head}(S_M(x))$ .

( $\supseteq$ ) 可类似证明.

(ii) 事实上, 考虑到  $\text{tail}$  与  $\text{head}$  对集合并的可分配性(读者自证), 并利用上述引理, 我们有

$$\begin{aligned} \text{tail}(P_M(A)) &= \text{tail}\left(\bigcup_{x \in A} P_M(x)\right) \\ &= \bigcup_{x \in A} \text{tail}(P_M(x)) \\ &= \bigcup_{x \in A} \text{head}(S_M(x)) \\ &= \text{head}\left(\bigcup_{x \in A} S_M(x)\right) \\ &= \text{head}(S_M(A)). \end{aligned}$$

证毕.

**引理 24.** 对任意  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $M(\cdot, A, B)$  成立, 则必有  $A \subseteq \Sigma^* M$  与  $B \subseteq M \Sigma^*$ .

证明. 设  $x \in A$ . 由于  $M(\cdot, A, B)$  成立, 故应存在  $y \in B$ , 使得  $x \cdot_M y \in \Sigma^*$ . 据  $\cdot_M$  定义, 当且仅当存在  $a \in M$ , 使得  $x \cdot_M y = x \cdot_a y$ . 据  $\cdot_a$  定义, 当且仅当存在  $x', y' \in \Sigma^*$ , 使得  $x = x'a$ ,  $y = ay'$ , 且  $x \cdot_a y = x'ay'$ . 于是, 有  $x \in \Sigma^* a \subseteq \Sigma^* M$ .

对  $B \subseteq M \Sigma^*$  可类似证明.

证毕.

**引理 25.** 对任意  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $M(\cdot, A, B)$  成立, 则有

(i) 对每一  $a \in M$ , 假如存在  $x' \in \Sigma^*$ , 使得  $x'a \in A$ , 则必存在  $y' \in \Sigma^*$ , 使得  $ay' \in B$ ;

(ii) 对每一  $a \in M$ , 假如存在  $y' \in \Sigma^*$ , 使得  $ay' \in B$ , 则必存在  $x' \in \Sigma^*$ , 使得  $x'a \in A$ .

证明.

(i) 设  $a \in M$ , 且  $x'a \in A, x' \in \Sigma^*$ . 由于  $M(\cdot, A, B)$  成立, 故应存在  $y \in B$ , 使得  $x'a \cdot_M y \in \Sigma^*$ . 依  $\cdot_M$  定义, 应存在  $b \in M$ , 使得  $x'a \cdot_M y = x'a \cdot_b y$ . 显然应有  $b = a$ , 及存在  $y' \in \Sigma^*$ , 使得  $ay' = y \in B$ .

(ii) 可类似证明. 证毕.

**引理 26.** 对任意  $M \subseteq \Sigma, A \subseteq \Sigma^* M$  与  $B \subseteq M\Sigma^*, M(\cdot, A, B)$  成立, 当且仅当  $\text{tail}(A) = \text{head}(B)$ .

证明.

( $\Rightarrow$ ) 设  $M \subseteq \Sigma, A \subseteq \Sigma^* M$  与  $B \subseteq M\Sigma^*$ , 且  $M(\cdot, A, B)$  成立. 我们来证明  $\text{tail}(A) = \text{head}(B)$ .

( $\subseteq$ ) 设  $a \in \text{tail}(A)$ . 依  $\text{tail}$  定义, 应存在  $x' \in \Sigma^*$ , 使得  $x'a \in A \subseteq \Sigma^* M$ . 故有  $a \in M$ . 又由  $M(\cdot, A, B)$  成立, 据引理 25 的(i), 应存在  $y' \in \Sigma^*$ , 使得  $ay' \in B$ . 从而, 有  $a \in \text{head}(B)$ .

( $\supseteq$ ) 设  $a \in \text{head}(B)$ . 依  $\text{head}$  定义, 应存在  $y' \in \Sigma^*$ , 使得  $y' \in B \subseteq M\Sigma^*$ . 故有  $a \in M$ . 又由  $M(\cdot, A, B)$  成立, 据引理 25 的(ii), 应存在  $x' \in \Sigma^*$ , 使得  $x'a \in A$ . 从而, 有  $a \in \text{tail}(A)$ .

( $\Leftarrow$ ) 设  $M \subseteq \Sigma, A \subseteq \Sigma^* M$  与  $B \subseteq M\Sigma^*$ , 且  $\text{tail}(A) = \text{head}(B)$ . 我们来证明  $M(\cdot, A, B)$  成立.

事实上, 设  $x \in A \subseteq \Sigma^* M$ . 我们令  $x = x'a, x' \in \Sigma^*, a \in M$ . 由此, 有  $a \in \text{tail}(A)$ . 再据  $\text{tail}(A) = \text{head}(B)$ , 应有  $a \in \text{head}(B)$ . 从而, 应存在  $y' \in \Sigma^*$ , 使得  $ay' \in B$ . 取  $y = ay'$ , 就有在所设条件下, 对每一  $x \in A$ , 存在  $a \in M$  与  $y \in B$ , 使得  $x \cdot_a y = x'ay' \in \Sigma^*$ . 类似地, 可证明, 对每一  $y \in B$  存在  $a \in M$  与  $x \in A$ , 使得  $x \cdot_a y \in \Sigma^*$ . 故我们有  $M(\cdot, A, B)$ . 证毕.

**推论 6.** 对任意  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 总有  $M(\cdot, P_M(A), S_M(A))$  成立.

证明. 事实上, 对任意  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 据引理 20 的(ii), 我们有  $\text{tail}(P_M(A)) = \text{head}(S_M(A))$ . 故据引理 26, 有  $M(\cdot, P_M(A), S_M(A))$  成立.

下面, 在  $M(\cdot, A, B)$  成立的条件下, 我们证明包含关系  $P_M(A) \subseteq P_M(A \cdot_M B)$  与  $S_M(B) \subseteq S_M(A \cdot_M B)$  成立.

**引理 27.** 对任意  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $M(\cdot, A, B)$  成立, 则有

(i)  $P_M(A) \subseteq P_M(A \cdot_M B)$ ;

(ii)  $S_M(B) \subseteq S_M(A \cdot_M B)$ .

证明.

(i) 对每一  $a \in M$ , 设  $ua \in P_a(A)$ . 据  $P_a$  定义, 应存在  $x \in A$  与  $v \in \Sigma^*$ , 使得  $x = uav$ . 由于  $M(\cdot, A, B)$  成立, 故应存在  $y \in B$ , 使得  $x \cdot_M y \in \Sigma^*$ . 显然, 我们有

$x \cdot_M y \in A \cdot_M B$ . 据推论 4, 对每一  $a \in M$ , 我们有  $P_a(x \cdot_M y) = P_a(x) \cup x \cdot_M P_a(y)$ . 从而, 有  $ua \in P_a(x) \subseteq P_a(x \cdot_M y) \subseteq P_a(A \cdot_M B) \subseteq P_M(A \cdot_M B)$ .

(ii) 可类似证明. 证毕.

**定理 5.** 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $M(\cdot, A, B)$  成立, 则有

(i)  $P_M(A \cdot_M B) = P_M(A) \cup A \cdot_M P_M(B)$ ;

(ii)  $S_M(A \cdot_M B) = S_M(B) \cup S_M(A) \cdot_M B$ .

证明.

(i)

( $\subseteq$ ) 据引理 21 的(i).

( $\supseteq$ ) 据引理 22 的(i)与引理 27 的(i).

(ii) 可类似证明.

这里, 我们还要介绍一个下面要用到的结果.

**引理 28.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

(i)  $P_M(A) = P_M(A_M)$ ;

(ii)  $S_M(A) = S_M(A_M)$ .

证明.

(i) 由  $A = A_M \cup A_M^{(0)}$  及  $P_M(A_M^{(0)}) = \emptyset$ , 再据引理 18 的(ii)  $M$  版即得.

(ii) 可类似证明. 证毕.

最后, 我们再引进  $M$ -剪切代数  $\langle P(\Sigma^*), \{P_M, S_M, F_M\}, M \rangle$  中的另一运算  $F_M$ . 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma, F_M$  为取  $M$ -因子的运算, 它定义为

$F_M(A) = \{axb \mid a, b \in M, \text{存在 } w \in A, \text{使 } w = uaxbv\}$ .

此处我们不准备对运算  $F_M$  的性质作探讨, 因为, 在后面, 我们将对  $F_M$  的一类更实用的特殊形式  $F_M^{(i)}, i \geq 0$  作深入研究.

## 4 $\Sigma$ 上的 $\#_M$ -代数 ( $M$ -重组代数或称 $M$ -桥接代数)

本节中, 我们来讨论  $\Sigma$  上的  $\#_M$ -代数, 亦称  $M$ -重组代数或  $M$ -桥接代数, 它对应于简单  $H$ -系统<sup>[10]</sup>. 它们是由运算  $\#_a$  与  $\#_M$  导出的. 现在, 我们就来给出它们的定义.

设  $x, y \in \Sigma^*$  与  $a \in \Sigma$ . 我们定义

$x \#_a y = \{x_1 a y_2 \mid \text{若 } x = x_1 a x_2, y = y_1 a y_2\}$ .

并称  $\#_a$  为字间的  $a$ -重组运算或  $a$ -桥接运算. 对  $M \subseteq \Sigma$ , 我们定义

$$x \#_M y = \bigcup_{a \in M} x \#_a y,$$

并称  $\#_M$  为字间的  $M$ -重组运算或  $M$ -桥接运算. 运算  $\#_a$  与  $\#_M$  可如下自然地定义为字集间的运算. 设

$A, B \subseteq \Sigma^*$ ,  $a \in \Sigma$  及  $M \subseteq \Sigma$ . 我们定义

$$A \#_a B = \bigcup_{\substack{x \in A \\ y \in B}} x \#_a y;$$

$$A \#_M B = \bigcup_{a \in M} A \#_a B.$$

注意,在文献[10]中仅定义了字集间的  $\#_M$  运算,且它定义为

$$L_1 \#_M L_2 = \text{Pref}(L_1) \diamond_M \text{Suf}(L_2).$$

其中,  $\text{Pref}(L_1)$  与  $\text{Suf}(L_2)$  分别为  $L_1$  的所有前缀的集合及  $L_2$  的所有后缀的集合,  $\diamond_M$  的意义与本文中的  $\cdot_M$  相同. 由后面的定理 6 可知,我们的  $\#_M$  定义与文献[10]中  $\#_M$  的定义等价,且我们仅考虑运算中真正起作用的  $M$ -前缀与  $M$ -后缀,从而简化了计算.

我们首先给出有关  $A \#_M B$  另一种表示的一个引理.

**引理 29.** 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

$$\bigcup_{a \in M} A \#_a B = \bigcup_{\substack{x \in A \\ y \in B}} x \#_M y,$$

$$\text{即有 } A \#_M B = \bigcup_{\substack{x \in A \\ y \in B}} x \#_M y.$$

证明.

( $\subseteq$ ) 设  $w \in \bigcup_{a \in M} A \#_a B$ . 依定义,应存在  $a \in M$ , 使得  $w \in A \#_a B$ . 从而,应存在  $x \in A, y \in B$ , 使得  $w \in x \#_a y \subseteq x \#_M y \subseteq \bigcup_{\substack{x \in A \\ y \in B}} x \#_M y$ .

( $\supseteq$ ) 设  $w \in \bigcup_{\substack{x \in A \\ y \in B}} x \#_M y$ . 依定义,应存在  $x \in A$  与  $y \in B$ , 使  $w \in x \#_M y = \bigcup_{a \in M} x \#_a y$ . 从而,应存在  $a \in M$ , 使得  $w \in x \#_a y \subseteq A \#_a B \subseteq \bigcup_{a \in M} A \#_a B$ . 证毕.

下面的定理及推论提示了  $\#_a, \#_M$  运算与  $P, S$  及  $\cdot_a, \cdot_M$  运算间的密切关系,并证明了我们给出的  $\#_M$  运算与文献[10]中  $\#_M$  定义是等价的.

**定理 6.**

(i) 对所有  $x, y \in \Sigma^*$  与  $a \in \Sigma$ ,  $x \#_a y = P_a(x) \cdot_a S_a(y)$ ;

(ii) 对所有  $x, y \in \Sigma^*$  与  $M \subseteq \Sigma$ ,  $x \#_M y = P_M(x) \cdot_M S_M(y)$ ;

(iii) 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ ,  $A \#_M B = P_M(A) \cdot_M S_M(B)$ ;

(iv) 对所有  $A, B \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ ,  $A \#_M B = A_M \#_M B_M$ .

证明.

(i)

( $\subseteq$ ) 设  $w \in x \#_a y$ . 依定义,应存在  $x_1, x_2, y_1, y_2 \in \Sigma^*$ , 使  $x = x_1 a x_2, y = y_1 a y_2$  及  $w = x_1 a y_2$ . 于是,

应有  $x_1 a \in P_a(x)$  与  $a y_2 \in S_a(y)$ . 从而,有  $w = x_1 a y_2 = x_1 a \cdot_a a y_2 \in P_a(x) \cdot_a S_a(y)$ .

( $\supseteq$ ) 设  $w \in P_a(x) \cdot_a S_a(y)$ . 据此,应存在  $x_1 a \in P_a(x)$  与  $a y_2 \in S_a(y)$ , 使  $w = x_1 a \cdot_a a y_2 = x_1 a y_2$ . 再由  $x_1 a \in P_a(x)$ , 依定义应存在  $x_2 \in \Sigma$ , 使  $x = x_1 a x_2$ . 据  $a y_2 \in S_a(y)$ , 依定义,应存在  $y_1 \in \Sigma^*$ , 使  $y = y_1 a y_2$ . 从而,据  $\#_a$  定义,有  $w = x_1 a y_2 \in x \#_a y$ .

(ii) 事实上,我们有

$$\begin{aligned} x \#_M y &= \bigcup_{a \in M} x \#_a y = \bigcup_{a \in M} (P_a(x) \cdot_a S_a(y)) \\ &= P_M(x) \cdot_M S_M(y). \end{aligned}$$

(iii) 由定义及引理 29, 再据(ii), 我们有

$$\begin{aligned} A \#_M B &= \bigcup_{a \in M} A \#_a B = \bigcup_{\substack{x \in A \\ y \in B}} (x \#_M y) \\ &= \bigcup_{\substack{x \in A \\ y \in B}} (P_M(x) \cdot_M S_M(y)) \\ &= P_M(A) \cdot_M S_M(B). \end{aligned}$$

(iv) 据(iii) 及引理 28, 我们有

$$\begin{aligned} A \#_M B &= P_M(A) \cdot_M S_M(B) = P_M(A_M) \cdot_M S_M(B_M) \\ &= A_M \#_M B_M. \end{aligned} \quad \text{证毕.}$$

下面引理给出了  $\#_M$  与通常集合运算与包含关系间的关联.

**引理 30.** 设  $A, B, C \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

(i)  $A \#_M (B \cup C) = A \#_M B \cup A \#_M C$ ;

(ii)  $(A \cup B) \#_M C = A \#_M C \cup B \#_M C$ ;

(iii)  $A \#_M (B \cap C) \subseteq A \#_M B \cap A \#_M C$ ;

(iv)  $(A \cap B) \#_M C \subseteq A \#_M C \cap B \#_M C$ ;

(v) 若  $A \subseteq B$ , 则  $A \#_M C \subseteq B \#_M C$ ; 若  $B \subseteq C$ , 则  $A \#_M B \subseteq A \#_M C$ .

证明.

(i) 事实上,我们有

$$\begin{aligned} A \#_M (B \cup C) &= P_M(A) \cdot_M S_M(B \cup C) \\ &\quad \text{据定理 6 的(iii)} \\ &= P_M(A) \cdot_M (S_M(B) \cup S_M(C)) \\ &\quad \text{据引理 18(ii)的 } S_M \text{ 版} \\ &= P_M(A) \cdot_M S_M(B) \cup P_M(A) \cdot_M S_M(C) \\ &\quad \text{据引理 9 的(i)} \\ &= A \#_M B \cup A \#_M C \quad \text{据定理 6 的(iii)} \end{aligned}$$

(ii) 可类似证明.

$$\begin{aligned} A \#_M (B \cap C) &= P_M(A) \cdot_M S_M(B \cap C) \\ &\quad \text{据定理 6 的(iii)} \\ &\subseteq P_M(A) \cdot_M (S_M(B) \cap S_M(C)) \\ &\quad \text{据引理 18 的(iii)及引理 9 的(v)} \end{aligned}$$

(iii) 事实上,我们有

$$\begin{aligned} A \#_M (B \cap C) &= P_M(A) \cdot_M S_M(B \cap C) \\ &\quad \text{据定理 6 的(iii)} \\ &\subseteq P_M(A) \cdot_M (S_M(B) \cap S_M(C)) \\ &\quad \text{据引理 18 的(iii)及引理 9 的(v)} \end{aligned}$$

(ii) 可类似证明.

(iii) 事实上,我们有

$$\begin{aligned} A \#_M (B \cap C) &= P_M(A) \cdot_M S_M(B \cap C) \\ &\quad \text{据定理 6 的(iii)} \\ &\subseteq P_M(A) \cdot_M (S_M(B) \cap S_M(C)) \\ &\quad \text{据引理 18 的(iii)及引理 9 的(v)} \end{aligned}$$

(iv) 可类似证明.

$$\subseteq P_M(A) \cdot_M S_M(B) \cap P_M(A) \cdot_M S_M(C)$$

据引理 9 的 (iii)

$$= A \#_M B \cap A \#_M C \quad \text{据定理 6 的 (iii)}$$

(iv) 可类似 (iii) 证明.

(v) 我们仅对前一断言进行证明, 后一断言可类似证明.

设  $A \subseteq B$ . 据引理 18 (iv) 的  $M$  版, 我们有  $P_M(A) \subseteq P_M(B)$ . 再据引理 9 的 (vi), 我们有  $P_M(A) \cdot_M S_M(C) \subseteq P_M(B) \cdot_M S_M(C)$ . 从而, 据定理 6 的 (iii), 我们有  $A \#_M C \subseteq B \#_M C$ . 证毕.

**推论 7.** 设  $A_i, B_j \subseteq \Sigma^*, i = 1, 2, \dots, n, j = 1, 2, \dots, m$  及  $M \subseteq \Sigma$ . 这时, 有

$$(i) (A_1 \cup A_2 \cup \dots \cup A_n) \#_M (B_1 \cup B_2 \cup \dots \cup B_m) = \bigcup_{i=1}^n \bigcup_{j=1}^m (A_i \#_M B_j);$$

$$(ii) (A_1 \cap A_2 \cap \dots \cap A_n) \#_M (B_1 \cap B_2 \cap \dots \cap B_m) \subseteq \bigcup_{i=1}^n \bigcup_{j=1}^m (A_i \#_M B_j).$$

证明. 略.

下面, 我们来研究运算  $\#_M$  的结合性. 出于实用的目的, 我们仅考虑字集间的  $\#_M$  运算. 首先, 我们要指出的是 Mateescu 等在文献 [10] 中给出的引理 6 (关于  $\#_M$  的结合性) 是错误的. 这通过我们下面给出的实例就可看出.

**例.** 设  $\Sigma = \{a, b, c, d\}, M = \{a, b\}, A = \{cacb, dbda\}, B = \{acc, add\}$  与  $C = \{bdc\}$ .

利用定理 6 的 (iii), 通过计算, 我们有

$$\begin{aligned} (A \#_M B) \#_M C &= (P_M(A) \cdot_M S_M(A)) \#_M C \\ &= (\{ca, cacb, db, dbda\} \cdot_M \{acc, add\}) \#_M C \\ &= \{cacc, cadd, dbdacc, dbdadd\} \#_M C \\ &= P_M(\{cacc, cadd, dbdacc, dbdadd\}) \cdot_M S_M(C) \\ &= \{ca, db, dbda\} \cdot_M \{bdc\} \\ &= \{dbdc\}, \end{aligned}$$

$$\begin{aligned} A \#_M (B \#_M C) &= A \#_M (P_M(B) \cdot_M S_M(C)) \\ &= A \#_M (a \cdot_M bdc) \\ &= A \#_M \emptyset \\ &= \emptyset. \end{aligned}$$

从而有  $(A \#_M B) \#_M C \neq A \#_M (B \#_M C)$ .

Mateescu 等关于  $\#_M$  满足结合律的断言错误的关键在于, 他们误认为  $P_M(A) \subseteq P_M(A \cdot_M B)$  与  $S_M(B) \subseteq S_M(A \cdot_M B)$  两包含关系的成立是无条件的. 但是, 像我们在引理 21 后给出的实例所证实的, 事实并非如此. 为此, 我们着力于寻求两包含关系成立的充分条件, 这就是  $M(\cdot, A, B)$  成立. 从而, 也就有了下面的  $\#_M$  结合性定理.

**定理 7.** 对所有  $A, B, C \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 假如  $M(\cdot, P_M(A), S_M(B))$  与  $M(\cdot, P_M(B), S_M(C))$  成立, 则我们有

$$(A \#_M B) \#_M C = A \#_M (B \#_M C).$$

证明. 首先注意到, 据引理 14 的推论, 我们有  $P_M(P_M(A)) = P_M(A)$  与  $S_M(S_M(A)) = S_M(A)$ . 从而, 易检验, 假如  $M(\cdot, P_M(A), S_M(B))$  成立, 则  $M(\cdot, P_M(P_M(A)), S_M(B))$  与  $M(\cdot, P_M(A), S_M(S_M(B)))$  成立. 同样,  $M(\cdot, P_M(B), S_M(C))$  成立将蕴含  $M(\cdot, P_M(P_M(B)), S_M(C))$  与  $M(\cdot, P_M(B), S_M(S_M(C)))$  成立. 于是, 我们有

$$\begin{aligned} (A \#_M B) \#_M C &= (P_M(A) \cdot_M S_M(B)) \#_M C \quad \text{定理 6 的 (iii)} \\ &= P_M(P_M(A) \cdot_M S_M(B)) \cdot_M S_M(C) \quad \text{同上} \\ &= [P_M(P_M(A)) \cup P_M(A) \cdot_M P_M(S_M(B))] \cdot_M S_M(C) \quad \text{定理 5} \\ &= [P_M(A) \cup P_M(A) \cdot_M S_M(P_M(B))] \cdot_M S_M(C) \quad \text{前面说明与定理 4} \\ &= P_M(A) \cdot_M S_M(C) \cup P_M(A) \cdot_M S_M(P_M(B)) \cdot_M S_M(C) \quad \text{引理 9} \\ &= P_M(A) \cdot_M [S_M(C) \cup S_M(P_M(B)) \cdot_M S_M(C)] \quad \text{同上} \\ &= P_M(A) \cdot_M S_M(P_M(B) \cdot_M S_M(C)) \quad \text{定理 5} \\ &= P_M(A) \cdot_M S_M(B \#_M C) \quad \text{定理 6 的 (iii)} \\ &= A \#_M (B \#_M C). \quad \text{同上} \end{aligned}$$

证毕.

**推论 8.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 总有

$$(A \#_M A) \#_M A = A \#_M (A \#_M A).$$

证明. 据推论 6, 对任意  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 我们总有  $M(\cdot, P_M(A), S_M(A))$  成立. 在本定理证明中, 取  $A = B = C$ , 即得本推论.

下面, 我们再指出,  $M$  在局部范围内也起作运算  $\#_M$  的单位元作用.

**定理 8.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

- (i)  $A \#_M M = A$ , 当且仅当  $A = P_M(A)$ ;
- (ii)  $M \#_M A = A$ , 当且仅当  $A = S_M(A)$ ;
- (iii) 若  $B \in \Sigma_M^*$ , 则  $A \#_M B = B \#_M A = \emptyset$ .

证明.

(i)

( $\Rightarrow$ ) 若  $A \#_M M = A$ , 则依定理 6 的 (iii) 及引理 5, 我们有

$$\begin{aligned} A &= A \#_M M = P_M(A) \cdot_M S_M(M) \\ &= P_M(A) \cdot_M M = P_M(A). \end{aligned}$$

( $\Leftarrow$ ) 若  $A = P_M(A)$ , 这时, 我们有

$$\begin{aligned} A &= P_M(A) = P_M(A) \cdot_M M \\ &= P_M(A) \cdot_M S_M(M) = A \#_M M. \end{aligned}$$

(ii) 可类似证明.

(iii) 由于若  $B \in \Sigma_M^*$ , 则有  $P_M(B) = S_M(B) = \emptyset$ ,

从而, 有  $A \#_M B = P_M(A) \cdot_M S_M(B) = \emptyset \cdot_M \emptyset = \emptyset$ .

证毕.

至此, 易见, 代数系  $\langle P(\Sigma^*), \#_M, M \rangle$  仅是一个亚半群( $\#_M$  的结合性是有条件的, 故不是如 Mateescu 等所断言的为半群), 且具有  $M$  为部分单位元. 为方便叙述, 我们称其为  $\Sigma$  上的一个  $M$ -重组代数, 或  $M$ -桥接代数(它们将剪切后具有  $M$  中同一符标记作尾与头的两段重组为一新字). 有意思的是, 据推论 8, 对任意  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 我们可将  $(A \#_M A) \#_M A$  与  $A \#_M (A \#_M A)$  统一记为  $A \#_M A \#_M A$ . 由此, 我们就可引入关于字集  $A \subseteq \Sigma^*$  的幂运算  $i(\#_M)$ ,  $i \geq 0$  及闭包运算  $*$ ( $\#_M$ ) 与  $+$ ( $\#_M$ ). 下面我们来作介绍, 并给出它们的一些基本性质.

设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 我们定义:

$$A^{0(\#_M)} = M,$$

$$A^{1(\#_M)} = A,$$

$$A^{(i+1)(\#_M)} = A^{i(\#_M)} \#_M A, i \geq 1.$$

像前面一样, 如下引进  $A$  关于  $\#_M$  的星闭包  $*$ ( $\#_M$ ) 与正闭包  $+$ ( $\#_M$ ) 如下:

$$A^{* (\#_M)} = A^{0(\#_M)} \cup A^{1(\#_M)} \cup \dots \cup A^{i(\#_M)} \cup \dots;$$

$$A^{+ (\#_M)} = A^{1(\#_M)} \cup A^{2(\#_M)} \cup \dots \cup A^{i(\#_M)} \cup \dots.$$

显然, 我们有  $A^{* (\#_M)} = A^{+ (\#_M)} \cup A^{0(\#_M)}$ . 此外, 我们还有下面引理.

**引理 31.** 对所有  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 有

$$(i) A^{i(\#_M)} \#_M A^{j(\#_M)} = A^{(i+j)(\#_M)}, i, j \geq 1;$$

$$(ii) (A^{i(\#_M)})^{j(\#_M)} = A^{ij(\#_M)}, i, j \geq 1.$$

证明.

(i) 对  $j$  作归纳.

基础:  $j = 1$  时, 依定义, 有  $A^{i(\#_M)} \#_M A^{1(\#_M)} = A^{i(\#_M)} \#_M A = A^{(i+1)(\#_M)}$ .

归纳: 设  $j = k$  时, 结论成立, 现考虑  $k+1$  的情形. 这时, 有

$$A^{i(\#_M)} A^{(k+1)(\#_M)} = A^{i(\#_M)} \#_M (A^{k(\#_M)} \#_M A)$$

据  $\#_M$  指数定义

$$= (A^{i(\#_M)} \#_M A^{k(\#_M)}) \#_M A \quad \text{据 } \#_M \text{ 结合性}$$

$$= A^{(i+k)(\#_M)} \#_M A \quad \text{归纳假设}$$

$$= A^{(i+k+1)(\#_M)} \quad \text{据 } \#_M \text{ 指数定义}$$

(ii) 略.

证毕.

注意, 引理中  $i, j \geq 1$  的限制是因为, 一般未必有  $A^{i(\#_M)} \#_M A^{0(\#_M)} = A^{i(\#_M)}$  与  $A^{0(\#_M)} \#_M A^{i(\#_M)} = A^{i(\#_M)}$ , 除非有  $P_M(A^{i(\#_M)}) = A^{i(\#_M)}$  与  $S_M(A^{i(\#_M)}) = A^{i(\#_M)}$ .

下面, 再介绍几个涉及  $A_M^{(0)}$  与  $A_M$  的结果.

**定理 9.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 这时, 若  $A_M^{(0)} = \emptyset$ , 则必有

$$A \subseteq P_M(A) \cdot_M S_M(A) = A^{2(\#_M)}.$$

证明. 设  $A_M^{(0)} = \emptyset$ . 这时, 若  $w \in A$ , 则有  $|w|_M \geq 1$ . 从而, 应存在  $a \in M$  及  $x, y \in \Sigma^*$ , 使  $w = xay$ . 由此, 有  $xa \in P_a(w) \subseteq P_M(A)$  与  $ay \in S_a(w) \subseteq S_M(A)$ . 从而有

$$w = xay = xa \cdot_a ay \in P_M(A) \cdot_M S_M(A)$$

$$= A \#_M A = A^{2(\#_M)}.$$

证毕.

**推论 9.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$  及  $i \geq 1$ . 若  $A_M^{(0)} = \emptyset$ , 则有  $A^{i(\#_M)} \subseteq A^{(i+1)(\#_M)}$ .

证明. 对  $i$  作归纳即可证明(略).

**定理 10.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 若  $i \neq 1$ , 则有  $A^{i(\#_M)} = A_M^{i(\#_M)}$ .

证明. 对  $i=0$ , 我们有  $A^{0(\#_M)} = M = A_M^{0(\#_M)}$ .

对  $i > 1$  的情形, 我们对  $i$  作归纳来证明.

基础:  $i=2$  时, 注意到  $A = A_M \cup A_M^{(0)}$ ,  $A_M^{(0)} \subseteq \Sigma_M^*$  及定理 8 的(iii), 我们有

$$A^{2(\#_M)} = A \#_M A = (A_M \cup A_M^{(0)}) \#_M (A_M \cup A_M^{(0)})$$

$$= A_M \#_M A_M \cup A_M \#_M A_M^{(0)} \cup$$

$$A_M^{(0)} \#_M A_M \cup A_M^{(0)} \#_M A_M^{(0)}$$

$$= A_M \#_M A_M = A_M^{2(\#_M)}.$$

归纳: 设  $i \geq 2$  时, 结论成立. 现考虑  $i+1$  时情形. 这时, 我们有

$$A^{(i+1)(\#_M)} = A^{i(\#_M)} \#_M A \quad \text{据 } \#_M \text{ 指数定义}$$

$$= A_M^{i(\#_M)} \#_M (A_M \cup A_M^{(0)}) \quad \text{归纳假设与 } A = A_M \cup A_M^{(0)}$$

$$= A_M^{i(\#_M)} \#_M A_M \cup A_M^{i(\#_M)} \#_M A_M^{(0)} \quad \text{据引理 30 的(i)}$$

$$= A_M^{(i+1)(\#_M)} \quad \text{据 } \#_M \text{ 指数定义及定理 8 的(iii)}$$

证毕.

最后, 我们来介绍一个关于闭包运算  $*$ ( $\#_M$ ) 与  $+$ ( $\#_M$ ) 的简单结果. 为此, 我们引进一个术语.

我们称  $A \subseteq \Sigma^*$  关于  $M \subseteq \Sigma$  是  $\#_M$  封闭的, 若  $A^{2(\#_M)} \subseteq A$ .

**定理 11.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 这时,  $A^{* (\#_M)}$  与  $A^{+ (\#_M)}$  均是  $\#_M$  封闭的.

证明. 事实上, 由于对任意  $i, j \geq 1$  有

$$A^{i(\#_M)} \#_M A^{j(\#_M)} = A^{(i+j)(\#_M)}.$$

故只须对  $i, j$  作归纳. 易证, 有

$$A^{+(\#_M)} \#_M A^{+(\#_M)} = A^{+(\#_M)},$$

$$A^{*(\#_M)} \#_M A^{*(\#_M)} = A^{*(\#_M)}.$$

细节此处从略.

证毕.

## 5 素 $M$ -前缀、素 $M$ -后缀和素 $M$ -因子

在本节中,我们首先引进一些更精细的概念,进而探讨其性质.为简便计,以下讨论都仅对字集进行,倘若把独项集 $\{w\}$ 与字 $w$ 等同,则有关字集的许多结果自然对字也成立.

设 $A \subseteq \Sigma^*$ 与 $M \subseteq \Sigma$ .对任意 $i \geq 1$ ,我们如下定义 $A$ 的 $i$ 次 $M$ -前缀集 $P_M^{(i)}(A)$ , $i$ 次 $M$ -后缀集 $S_M^{(i)}(A)$ 与 $i$ 次 $M$ -因子集 $F_M^{(i)}(A)$ :

$$P_M^{(i)}(A) = \{ua \mid a \in M, \text{存在 } w = uav \in A, \text{且} \\ |u|_M = i-1\},$$

$$S_M^{(i)}(A) = \{av \mid a \in M, \text{存在 } w = uav \in A, \text{且} \\ |v|_M = i-1\},$$

$$F_M^{(i)}(A) = \{axb \mid a, b \in M, \text{存在 } w = uaxbv \in A, \text{且} \\ |x|_M = i-1\}.$$

特别地,我们将 $P_M^{(1)}(A)$ , $S_M^{(1)}(A)$ 与 $F_M^{(1)}(A)$ 分别称为 $A$ 的素 $M$ -前缀集、素 $M$ -后缀集与素 $M$ -因子集,因为它们中的 $M$ -前缀、 $M$ -后缀与 $M$ -因子分别都不包含真子 $M$ -前缀、真子 $M$ -后缀与真子 $M$ -因子,它们在后面的讨论中有着特别重要的作用.

此外,为了方便,对所有 $A \subseteq \Sigma^*$ 及 $M \subseteq \Sigma$ ,我们将约定, $F_M^{(0)}(A) = M$ .对任一 $w \in \Sigma^*$ , $w$ 的示 $M$ -表示是具有如下特性的一个表达式:

$$w = w_0 a_1 w_1 a_2 w_2 \cdots w_{n-1} a_n w_n,$$

$$a_i \in M, w_0, w_i \in \Sigma_M^*, i = 1, 2, \cdots, n.$$

易见,对任一 $w \in \Sigma^*$ ,其示 $M$ -表示存在且唯一.且我们有以下引理.

**引理 32.** 对任意 $M \subseteq \Sigma$ 与 $w \in \Sigma^*$ .若 $w$ 的示 $M$ -表示为 $w = w_0 a_1 w_1 a_2 w_2 \cdots w_{n-1} a_n w_n$ , $a_i \in M$ , $w_0, w_i \in \Sigma_M^*$ , $i = 1, 2, \cdots, n$ .这时,有

$$(i) P_M^{(i)}(w) = \{w_0 a_1 w_1 \cdots a_{i-1} w_{i-1} a_i\}, 1 \leq i \leq n;$$

$$(ii) S_M^{(i)}(w) = \{a_{n-i} w_{n-i} \cdots a_{n-1} w_{n-1} a_n w_n\}, 1 \leq i \leq n;$$

$$(iii) F_M^{(i)}(w) = \{a_k w_k \cdots a_{k+i-1} w_{k+i-1} a_{k+i} \mid k \geq 1, \text{且 } k+i \leq n\}, 1 \leq i \leq n-1.$$

此处,我们将 $w$ 等同于 $\{w\}$ .

证明. 显然.

下面,我们首先来看有关 $P_M^{(1)}(A)$ , $S_M^{(1)}(A)$ 与

$F_M^{(1)}(A)$ 的基本定理.

**定理 12.** 设 $A \subseteq \Sigma^*$ , $M \subseteq \Sigma$ 及 $i \geq 1$ ,有

$$(i) P_M^{(1)}(A^{i(\#_M)}) = P_M^{(1)}(A);$$

$$(ii) S_M^{(1)}(A^{i(\#_M)}) = S_M^{(1)}(A);$$

$$(iii) F_M^{(1)}(A^{i(\#_M)}) = F_M^{(1)}(A).$$

证明.

(i)

( $\subseteq$ ) 对 $i$ 作归纳.

基础: $i=1$ 时,有 $A^{i(\#_M)} = A^{1(\#_M)} = A$ ,故有

$$P_M^{(1)}(A^{i(\#_M)}) = P_M^{(1)}(A).$$

归纳:假设对 $i \geq 1$ ,结论成立.现考虑 $i+1$ 的情形.设 $ua \in P_M^{(1)}(A^{(i+1)(\#_M)})$ , $a \in M$ .依定义,应存在 $w \in A^{(i+1)(\#_M)}$ ,使 $w = uav$ , $v \in \Sigma^*$ ,且 $|u|_M = 0$ .又由 $w \in A^{(i+1)(\#_M)} = A^{i(\#_M)} \#_M A$ 推知,应存在 $b \in M$ ,使 $w = xby$ ,其中, $xb \in P_M(A^{i(\#_M)})$ , $by \in S_M(A)$ .从而,有 $w = uav = xby$ .由于 $|u|_M = 0$ ,故必有 $|u| \leq |x|$ (否则,将有 $u = xbx'$ ,与 $|u|_M = 0$ 矛盾).这时,有以下两种情形:

(a)  $|u| = |x|$ .从而,有 $u = x$ , $a = b$ .由此,据 $ua = xb \in P_M(A^{i(\#_M)})$ 及 $|u|_M = 0$ ,应有 $ua \in P_M^{(1)}(A^{i(\#_M)})$ .由归纳假设,有 $ua \in P_M^{(1)}(A)$ .

(b)  $|u| < |x|$ .设 $x = uau'$ , $u' \in \Sigma^*$ .从而,有 $ua \in P_M(xb) \subseteq P_M(A^{i(\#_M)})$ .由归纳假设,应有 $ua \in P_M^{(1)}(A)$ .

( $\supseteq$ ) 注意到 $A = A_M^{(0)} \cup A_M$ ,应用推论 9 可得

$$A = A_M^{(0)} \cup A = A_M^{(0)} \cup A^{1(\#_M)} \\ \subseteq A_M^{(0)} \cup A^{2(\#_M)} \subseteq \cdots \subseteq A_M^{(0)} \cup A^{i(\#_M)}.$$

从而有

$$P_M^{(1)}(A) \subseteq P_M^{(1)}(A_M^{(0)} \cup A^{i(\#_M)}) \\ = P_M^{(1)}(A_M^{(0)}) \cup P_M^{(1)}(A^{i(\#_M)}) \\ = P_M^{(1)}(A^{i(\#_M)}).$$

(ii) 可类似证明.

(iii) ( $\subseteq$ ) 对 $i$ 作归纳.

基础: $i=1$ 时,有 $A^{i(\#_M)} = A^{1(\#_M)} = A$ ,故有

$$F_M^{(1)}(A^{i(\#_M)}) = F_M^{(1)}(A).$$

归纳:假设对 $i \geq 1$ ,结论成立.现考虑 $i+1$ 的情形.设 $axb \in F_M^{(1)}(A^{(i+1)(\#_M)})$ , $a, b \in M$ .依定义,应存在 $w \in A^{(i+1)(\#_M)}$ ,使 $w = uaxbv$ , $u, v \in \Sigma^*$ .又由于 $A^{(i+1)(\#_M)} = P_M(A^{i(\#_M)}) \cdot_M S_M(A)$ ,故有 $w = uaxbv \in P_M(A^{i(\#_M)}) \cdot_M S_M(A)$ .由于 $|x|_M = 0$ ,故这时必为以下两种情形之一:

(a)  $uaxb \in P_M(A^{i(\#_M)})$ ,从而必有

$$axb \in P_M^{(1)}(A^{i(\#_M)}).$$

由归纳假设,应有  $axb \in F_M^{(1)}(A)$ .

(b)  $axbv \in S_M(A)$ , 据此, 应存在  $w' \in A$ , 使得  $w' = u'axbv$ ,  $u' \in \Sigma^*$ , 从而, 必有  $axb \in F_M^{(1)}(A)$ .

( $\supseteq$ ) 由于  $A = A_M^{(0)} \cup A_M$  及  $A_M^{(0)} \subseteq \Sigma_M^*$ , 易见有  $F_M^{(1)}(A_M^{(0)}) = \emptyset$ . 据推论 9, 作简归纳可推得, 当  $i \geq 1$  时, 有

$$A = A_M^{(0)} \cup A = A_M^{(0)} \cup A^{1(\#_M)} \subseteq A_M^{(0)} \cup A^{i(\#_M)}.$$

从而, 有

$$\begin{aligned} F_M^{(1)}(A) &\subseteq F_M^{(1)}(A_M^{(0)} \cup A^{i(\#_M)}) \\ &= F_M^{(1)}(A_M^{(0)}) \cup F_M^{(1)}(A^{i(\#_M)}) \\ &= F_M^{(1)}(A^{i(\#_M)}). \end{aligned}$$

证毕.

下面, 我们来介绍有关  $P_M, S_M$  与  $P_M^{(1)}, S_M^{(1)}$  和  $F_M^{(1)}$  间关系的若干结果.

**引理 33.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 这时, 有

(i) 若  $a \in M$  且  $ua \in P_M(A)$ , 则存在  $k \geq 0$ , 使  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)}$ ;

(ii) 若  $a \in M$  且  $av \in S_M(A)$ , 则存在  $k \geq 0$ , 使  $av \in (F_M^{(1)}(A))^{k(\cdot_M)} \cdot_M S_M^{(1)}(A)$ .

证明.

(i) 设  $a \in M$  且  $ua \in P_M(A)$ . 依定义, 应存在  $w \in A$ , 使  $w = uav$ ,  $v \in \Sigma^*$ . 设  $w$  的示  $M$ -表示为

$$w = w_0 a_1 w_1 \cdots a_k w_k \cdots a_n w_n,$$

$$a_i \in M, w_0, w_i \in \Sigma_M^*, i = 1, 2, \cdots, n.$$

这时, 必存在  $j, 1 \leq j \leq n$ , 使  $ua = w_0 a_1 w_1 \cdots w_{j-1} a_j$ . 由示  $M$ -表示的定义, 必有

$$w_0 a_1 \in P_M^{(1)}(A), a_1 w_1 a_2, \cdots, a_{j-1} w_{j-1} a_j \in F_M^{(1)}(A).$$

从而, 我们有

$$\begin{aligned} ua &= w_0 a_1 \cdot_{a_1} a_1 w_1 a_2 \cdot_{a_2} \cdots \cdot_{a_{j-1}} a_{j-1} w_{j-1} a_j \in \\ &P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{(j-1)(\cdot_M)}. \end{aligned}$$

取  $k = j - 1$ , 即得所要结果.

(ii) 可类似证明.

证毕.

**定理 13.** 设  $A \subseteq \Sigma^*, M \subseteq \Sigma$  与  $i \geq 1$ . 这时, 有

(i) 若  $a \in M$  且  $ua \in P_M(A^{i(\#_M)})$ , 则存在  $k \geq 0$ , 使  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)}$ ;

(ii) 若  $a \in M$  且  $av \in S_M(A^{i(\#_M)})$ , 则存在  $k \geq 0$ , 使  $av \in (F_M^{(1)}(A))^{k(\cdot_M)} \cdot_M S_M^{(1)}(A)$ .

证明.

(i) 对  $i$  作归纳.

基础:  $i = 1$  时, 有  $A^{i(\#_M)} = A$ . 由引理 33 的(i), 结论成立.

归纳: 设  $i \geq 1$  时, 结论成立. 现考虑  $i + 1$  的情形. 设  $a \in M$  且  $ua \in P_M(A^{(i+1)(\#_M)})$ . 依定义, 应存在  $w \in A^{(i+1)(\#_M)}$ , 使  $w = uav$ ,  $v \in \Sigma^*$ . 再由  $A^{(i+1)(\#_M)} = A^{i(\#_M)} \#_M A = P_M(A^{i(\#_M)}) \cdot_M S_M(A)$  知, 应存在  $b \in M, xb \in P_M(A^{i(\#_M)})$  与  $by \in S_M(A)$ , 使  $w = xby$ . 从而, 有  $uav = xby$ . 分 3 种情形讨论:

(a)  $|u| = |x|$ . 这时, 有  $u = x, a = b$  与  $v = y$ . 从而, 有  $ua = xb \in P_M(A^{i(\#_M)})$ . 由归纳假设, 存在  $k \geq 0$ , 使  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)}$ .

(b)  $|u| < |x|$ . 设  $x = uau'$ . 由此, 有  $ua \in P_M(xb) \subseteq P_M(A^{i(\#_M)})$  (据推论 3, 应有  $P_M(P_M(A^{i(\#_M)})) = P_M(A^{i(\#_M)})$ ). 由归纳假设, 存在  $k \geq 0$ , 使  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)}$ .

(c)  $|u| > |x|$ . 设  $u = xbx'$ . 由此, 有  $ua = xbx'a$ . 由  $xb \in P_M(A^{i(\#_M)})$  及归纳假设, 存在  $k' \geq 0$ , 使  $xb \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k'(\cdot_M)}$ . 又设  $bx'a$  的示  $M$ -表示为  $bx'a = bx'_0 a_1 x'_1 \cdots a_s x'_s a$ . 从而有  $bx'_0 a_1, \cdots, a_s x'_s a \in F_M^{(1)}(w) \subseteq F_M^{(1)}(A^{(i+1)(\#_M)})$ . 再据定理 12 的(iii), 应有  $F_M^{(1)}(A^{(i+1)(\#_M)}) = F_M^{(1)}(A)$ . 故若取  $k = k' + s + 1$ , 我们就有

$$ua = xbx'_0 a_1 x'_1 \cdots a_s x'_s a \in$$

$$\begin{aligned} &P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k'(\cdot_M)} \cdot_M (F_M^{(1)}(A))^{(s+1)(\cdot_M)} \\ &= P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)}. \end{aligned}$$

(ii) 可类似证明.

证毕.

在讨论定理 13 的逆定理之前, 我们还需要以下几个结果. 在以下各定(引)理表述与证明中, 为简化叙述, 凡未标明出处的  $w, x, u, v$  (可能带有下标) 均为  $\Sigma^*$  中的字.

**引理 34.** 若  $w_j = u_j a_j x_j a_{j+1} v_j \in A, a_j, a_{j+1} \in M, j = 1, 2, \cdots, n$ . 这时有

$$w = u_1 a_1 x_1 a_2 x_2 \cdots a_n x_n a_{n+1} v_n \in A^{n(\#_M)}.$$

证明. 对  $n$  作归纳.

基础:  $n = 1$  时, 有  $w = w_1 = u_1 a_1 x_1 a_2 v_1 \in A = A^{1(\#_M)}$ .

归纳: 假设对  $n \geq 1$ , 结论成立, 现考虑  $n + 1$  情形. 设有  $w_j = u_j a_j x_j a_{j+1} v_j \in A, a_j, a_{j+1} \in M, j = 1, 2, \cdots, n, n + 1$ . 由归纳假设, 应有  $w' = u_1 a_1 x_1 a_2 x_2 \cdots a_n x_n a_{n+1} v_n \in A^{n(\#_M)}$ . 从而有

$$u_1 a_1 x_1 a_2 x_2 \cdots a_n x_n a_{n+1} \in P_M(w') \subseteq P_M(A^{n(\#_M)})$$

及有

$$a_{n+1} x_{n+1} a_{n+2} v_{n+1} \in S_M(w_{n+1}) \subseteq S_M(A).$$

据此, 就有

$$w = u_1 a_1 x_1 \cdots a_n x_n a_{n+1} x_{n+1} a_{n+2} v_{n+1}$$

$$= u_1 a_1 x_1 \cdots a_n x_n a_{n+1} \cdot_{a_{n+1}} a_{n+1} x_{n+1} a_{n+2} v_{n+1} \in P_M(A^{n(\#_M)}) \cdot_M S_M(A).$$

但  $P_M(A^{n(\#_M)}) \cdot_M S_M(A) = A^{(n+1)(\#_M)}$ . 故有  $w \in A^{(n+1)(\#_M)}$ . 证毕.

**定理 14.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ , 则对所有  $i \geq 1$ , 有  $(F_M^{(1)}(A))^{i(\#_M)} = F_M^{(i)}(A^{i(\#_M)})$ .

证明.

( $\subseteq$ ) 设  $a, b \in M$  及  $axb \in (F_M^{(1)}(A))^{i(\#_M)}$ . 据此, 应存在  $a_j x_j a_{j+1} \in F_M^{(1)}(A)$ ,  $j=1, 2, \dots, i$ , 使得  $a=a_1$ ,  $b=a_{i+1}$ , 且  $axb=a_1 x_1 a_2 \cdot_{a_2} a_2 x_2 a_3 \cdot_{a_3} \cdots \cdot_{a_i} a_i x_i a_{i+1}$ . 又由于对  $j=1, 2, \dots, i$ ,  $a_j x_j a_{j+1} \in F_M^{(1)}(A)$ , 依  $F_M^{(1)}$  定义, 应存在  $w_j = u_j a_j x_j a_{j+1} v_j \in A$ . 据引理 34, 我们有  $w = u_1 a_1 x_1 \cdots a_i x_i a_{i+1} v_i \in A^{i(\#_M)}$ .

由于有  $|x_1 a_2 x_2 \cdots a_i x_i|_M = i-1$ . 故我们有  $axb = a_1 x_1 a_2 \cdots a_i x_i a_{i+1} \in F_M^{(i)}(A^{i(\#_M)})$ .

( $\supseteq$ ) 设  $a, b \in M$  及  $axb \in F_M^{(i)}(A^{i(\#_M)})$ . 从而, 有  $|x|_M = i-1$ . 再据  $F_M$  的定义, 应存在  $w = uaxbv \in A^{i(\#_M)}$ . 这时, 设  $axb$  的示  $M$ -表示为

$$axb = a_1 x_1 a_2 \cdots a_i x_i a_{i+1},$$

$$a_j, a_{j+1} \in M, x_j \in \Sigma_M^*, j=1, 2, \dots, i.$$

这里当然有  $a=a_1$ ,  $b=a_{i+1}$ . 据  $|x_j|_M=0$ ,  $j=1, 2, \dots, i$ , 我们有  $a_j x_j a_{j+1} \in F_M^{(1)}(w) \subseteq F_M^{(1)}(A^{i(\#_M)}) = F_M^{(1)}(A)$  (据定理 12 的 (iii)),  $j=1, 2, \dots, i$ . 于是有  $axb = a_1 x_1 a_2 \cdot_{a_2} a_2 x_2 a_3 \cdot_{a_3} \cdots \cdot_{a_i} a_i x_i a_{i+1} \in (F_M^{(1)}(A))^{i(\#_M)}$ .

证毕.

**定理 15.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$  与  $s, i, j \geq 1$ . 这时, 有

$$(i) P_M^{(s+j)}(A^{i(\#_M)}) \subseteq P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}) \subseteq P_M^{(s+j)}(A^{2i(\#_M)});$$

$$(ii) S_M^{(s+j)}(A^{i(\#_M)}) \subseteq F_M^{(j)}(A^{i(\#_M)}) \cdot_M S_M^{(s)}(A^{i(\#_M)}) \subseteq S_M^{(s+j)}(A^{2i(\#_M)});$$

$$(iii) F_M^{(s+j)}(A^{i(\#_M)}) \subseteq F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}) \subseteq F_M^{(s+j)}(A^{2i(\#_M)}).$$

证明.

$$(i) \text{ 先证 } P_M^{(s+j)}(A^{i(\#_M)}) \subseteq P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}).$$

设  $ua \in P_M^{(s+j)}(A^{i(\#_M)})$ ,  $a \in M$ . 依定义, 应存在  $b \in M$ , 使  $ua = u_1 b u_2 a$ . 其中,  $|u_1|_M = s-1$  与  $|u_2|_M = j-1$ , 并应存在  $w \in A^{i(\#_M)}$ , 使  $w = uav = u_1 b u_2 av$ ,  $v \in \Sigma^*$ . 由此, 有  $u_1 b \in P_M^{(s)}(w) \subseteq P_M^{(s)}(A^{i(\#_M)})$  及  $b u_2 a \in F_M^{(j)}(w) \subseteq F_M^{(j)}(A^{i(\#_M)})$ . 从而有

$$ua = u_1 b u_2 a$$

$$= u_1 b \cdot_b b u_2 a \in P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}).$$

$$\text{次证 } P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}) \subseteq P_M^{(s+j)}(A^{2i(\#_M)}).$$

设  $w \in P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)})$ . 依定义, 应存在  $a, b \in M$ , 使  $w = uaxb$ , 其中  $ua \in P_M^{(s)}(A^{i(\#_M)})$ ,  $axb \in F_M^{(j)}(A^{i(\#_M)})$ . 再依  $P_M^{(s)}$  与  $F_M^{(j)}$  的定义, 应存在  $w_1 = uav_1 \in A^{i(\#_M)}$  与  $w_2 = u_2 axbv_2 \in A_M^{i(\#_M)}$ , 其中  $v_1, u_2, v_2 \in \Sigma^*$ . 由此, 应有  $ua \in P_M(w_1) \subseteq P_M(A^{i(\#_M)})$  及  $axbv_2 \in S_M(w_2) \subseteq S_M(A^{i(\#_M)})$ . 从而有

$$\begin{aligned} uaxbv_2 &= ua \cdot_a axbv_2 \in P_M(A^{i(\#_M)}) \cdot_M S_M(A^{i(\#_M)}) \\ &= A^{2i(\#_M)}. \end{aligned}$$

由此, 我们有

$$w = uaxb \in P_M(uaxbv_2) \subseteq P_M(A^{2i(\#_M)}).$$

又因为

$$\begin{aligned} |uax|_M &= |u|_M + |a|_M + |x|_M \\ &= s-1+1+j-1 = s+j-1. \end{aligned}$$

故依定义, 有  $w \in P_M^{(s+j)}(A^{2i(\#_M)})$ .

(ii) 可类似(i)证明.

(iii) 先证

$$F_M^{(s+j)}(A^{i(\#_M)}) \subseteq F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}).$$

设  $a, b \in M$  及  $axb \in F_M^{(s+j)}(A^{i(\#_M)})$ . 从而, 有  $|x|_M = s+j-1$ , 及依定义, 应存在  $w \in A^{i(\#_M)}$ , 使  $w = uaxbv$ ,  $u, v \in \Sigma^*$ . 由于有  $s, j \geq 1$ , 故有  $|x|_M \geq 1$ . 据此, 应存在  $c \in M$ , 使  $x = x_1 c x_2$ ,  $x_1, x_2 \in \Sigma^*$ , 且使  $|x_1 c|_M = s$  及  $|x_2|_M = j-1$ . 于是有

$$w = uaxbv = ua x_1 c x_2 b v \in A^{i(\#_M)}.$$

由此, 必有  $ax_1 c \in F_M^{(s)}(A^{i(\#_M)})$  与  $c x_2 b \in F_M^{(j)}(A^{i(\#_M)})$ . 从而有

$$\begin{aligned} axb &= ax_1 c x_2 b \\ &= ax_1 c \cdot_c c x_2 b \in F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}). \end{aligned}$$

$$\text{次证 } F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)}) \subseteq F_M^{(s+j)}(A^{2i(\#_M)}).$$

设  $w \in F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(j)}(A^{i(\#_M)})$ . 依定义, 应存在  $a, b, c \in M$ , 使得  $w = axb \cdot_b b y c$ , 其中,  $axb \in F_M^{(s)}(A^{i(\#_M)})$  与  $b y c \in F_M^{(j)}(A^{i(\#_M)})$ . 于是我们有  $|x|_M = s-1$  及  $|y|_M = j-1$ , 且依  $F_M$  定义, 还应存在  $w_1 = u_1 axb v_1 \in A^{i(\#_M)}$  与  $w_2 = u_2 b y c v_2 \in A^{i(\#_M)}$ . 由此, 应有  $u_1 axb \in P_M(A^{i(\#_M)})$  与  $b y c v_2 \in S_M(A^{i(\#_M)})$ . 从而有  $u_1 axb y c v_2 = u_1 axb \cdot_b b y c v_2 \in P_M(A^{i(\#_M)}) \cdot_M S_M(A^{i(\#_M)}) = A^{2i(\#_M)}$ .

再由  $|x b y|_M = |x|_M + |b|_M + |y|_M = s-1+1+j-1 = s+j-1$ . 据  $F_M^{(s+j)}$  定义, 即得

$$w = axb y c \in F_M^{(s+j)}(A^{2i(\#_M)}). \quad \text{证毕.}$$

**定理 16.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$  与  $i, s \geq 1$ . 这时, 有



$$\begin{aligned}
 & \text{(i)} P_M^{(s+1)}(A^{i(\#_M)}) \subseteq P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A) \subseteq \\
 & P_M^{(s+1)}(A^{(i+1)(\#_M)}); \\
 & \text{(ii)} S_M^{(s+1)}(A^{i(\#_M)}) \subseteq F_M^{(1)}(A) \cdot_M S_M^{(s)}(A^{i(\#_M)}) \subseteq \\
 & S_M^{(s+1)}(A^{(i+1)(\#_M)}); \\
 & \text{(iii)} F_M^{(s+1)}(A^{i(\#_M)}) \subseteq F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A) \subseteq \\
 & F_M^{(s+1)}(A^{(i+1)(\#_M)}).
 \end{aligned}$$

证明.

$$\text{(i)} \text{ 先证 } P_M^{(s+1)}(A^{i(\#_M)}) \subseteq P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A).$$

设  $a \in M$  且  $ua \in P_M^{(s+1)}(A^{i(\#_M)})$ . 依定义, 应存在  $b \in M$ , 使  $ua = u_1 bu_2 a$ , 其中  $|u_1|_M = s-1$  与  $|u_2|_M = 0$ . 并应存在  $w \in A^{i(\#_M)}$ , 使  $w = uav = u_1 bu_2 av$ ,  $v \in \Sigma^*$ . 由此, 有  $u_1 b \in P_M^{(s)}(w) \subseteq P_M^{(s)}(A^{i(\#_M)})$  及  $bu_2 a \in F_M^{(1)}(w) \subseteq F_M^{(1)}(A^{i(\#_M)}) = F_M^{(1)}(A)$  (据定理 12 的 (iii)). 从而有  $ua = u_1 bu_2 a = u_1 b \cdot_M bu_2 a \in P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A)$ .

$$\text{次证 } P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A) \subseteq P_M^{(s+1)}(A^{(i+1)(\#_M)}).$$

设  $w \in P_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A)$ . 依定义, 应存在  $a, b \in M$ , 使  $w = uaxb$ , 其中  $ua \in P_M^{(s)}(A^{i(\#_M)})$ ,  $axb \in F_M^{(1)}(A)$ . 于是我们有  $|u|_M = s-1$  及  $|x|_M = 0$ . 再据  $P$  与  $F$  的定义, 应存在  $w_1 = uav \in A^{i(\#_M)}$  与  $w_2 = u_2 axbv_2 \in A$ . 由此, 应有  $ua \in P_M(w_1) \subseteq P_M(A^{i(\#_M)})$  及  $axbv_2 \in S_M(w_2) \subseteq S_M(A)$ . 从而有

$$\begin{aligned}
 uaxbv_2 &= ua \cdot_M axbv_2 \in P_M(A^{i(\#_M)}) \cdot_M S_M(A) \\
 &= A^{i(\#_M)} \cdot_M A = A^{(i+1)(\#_M)}.
 \end{aligned}$$

再由  $|uax|_M = |u|_M + |a|_M + |x|_M = s-1+1-0=s$  知, 有  $w = uaxb \in P_M^{(s+1)}(A^{(i+1)(\#_M)})$ .

(ii) 可类似(i)证明.

$$\text{(iii)} \text{ 先证 } F_M^{(s+1)}(A^{i(\#_M)}) \subseteq F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A).$$

设  $a, b \in M$  及  $axb \in F_M^{(s+1)}(A^{i(\#_M)})$ . 于是, 有  $|x|_M = s \geq 1$ , 且依定义, 应存在  $w = uaxbv \in A^{i(\#_M)}$ ,  $u, v \in \Sigma^*$ . 由于  $|x|_M = s \geq 1$ , 故应存在  $c \in M$ , 使  $x = cx_1cx_2$ , 且有  $|x_1c|_M = s$  与  $|x_2|_M = 0$ . 由此, 有  $w = uax_1cx_2bv \in A^{i(\#_M)}$ . 从而, 应有  $ax_1c \in F_M^{(s)}(w) \subseteq F_M^{(s)}(A^{i(\#_M)})$  与  $cx_2b \in F_M^{(1)}(w) \subseteq F_M^{(1)}(A^{i(\#_M)}) = F_M^{(1)}(A)$  (据定理 12 的 (iii)), 由此, 我们就得到

$$\begin{aligned}
 axb &= ax_1cx_2b \\
 &= ax_1c \cdot_M cx_2b \in F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A).
 \end{aligned}$$

$$\text{次证 } F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A) \subseteq F_M^{(s+1)}(A^{(i+1)(\#_M)}).$$

设  $w \in F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A)$ . 依定义, 应存在  $a, b, c \in M$ , 使得  $w = axbyc$ . 其中,  $axb \in F_M^{(s)}(A^{i(\#_M)})$  与  $byc \in F_M^{(1)}(A)$ . 于是应有  $|x|_M = s-1$  及  $|y|_M = 0$ . 再依  $F_M^{(s)}$  与  $F_M^{(1)}$  定义, 应存在  $w_1 = u_1 axbv_1 \in A^{i(\#_M)}$  与存在  $w_2 = u_2 bycv_2 \in A$ . 从而, 应有  $u_1 axb \in$

$$P_M(w_1) \subseteq P_M(A^{i(\#_M)}) \text{ 与 } bycv_2 \in S_M(w_2) \subseteq S_M(A).$$

由此推得有

$$\begin{aligned}
 u_1 axbycv_2 &= u_1 axb \cdot_M bycv_2 \in P_M(A^{i(\#_M)}) \cdot_M S_M(A) \\
 &= A^{(i+1)(\#_M)}.
 \end{aligned}$$

再由  $|xb|_M = |x|_M + |b|_M + |y|_M = s-1+1+0=s$  知, 应有

$$w = axbyc \in F_M^{(s+1)}(u_1 axbycv_2) \subseteq F_M^{(s+1)}(A^{(i+1)(\#_M)}).$$

这里我们指出一点, 即读者可以证明:

$$F_M^{(s)}(A^{i(\#_M)}) \cdot_M F_M^{(1)}(A) = F_M^{(s)}(A) \cdot_M F_M^{(s)}(A^{i(\#_M)}).$$

从而, 还有以下 (iii') 成立.

$$\text{(iii')} F_M^{(s+1)}(A^{i(\#_M)}) \subseteq F_M^{(1)}(A) \cdot_M F_M^{(s)}(A^{i(\#_M)}) \subseteq F_M^{(s+1)}(A^{(i+1)(\#_M)}).$$

证毕.

现在, 我们可以来建立定理 13 的如下逆定理.

**定理 17.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$  与  $k \geq 0$ . 这时, 有

(i) 若  $a \in M$  且  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\#_M)}$ , 则存在  $i \geq 1$ , 使  $ua \in P_M(A^{i(\#_M)})$ ;

(ii) 若  $a \in M$  且  $av \in (F_M^{(1)}(A))^{k(\#_M)} \cdot_M S_M^{(1)}(A)$ , 则存在  $i \geq 1$ , 使  $av \in S_M(A^{i(\#_M)})$ .

证明.

(i) 设  $a \in M$  且  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\#_M)}$ . 据定理 14, 我们有  $(F_M^{(1)}(A))^{k(\#_M)} = F_M^{(k)}(A^{k(\#_M)})$  及据定理 12 的 (i), 我们有  $P_M^{(1)}(A) = P_M^{(1)}(A^{k(\#_M)})$ . 从而有

$$\begin{aligned}
 ua &\in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\#_M)} = \\
 &P_M^{(1)}(A^{k(\#_M)}) \cdot_M F_M^{(k)}(A^{k(\#_M)}).
 \end{aligned}$$

再据定理 15 (i) 的后一包含, 我们就有  $ua \in P_M^{(k+1)}(A^{2k(\#_M)}) \subseteq P_M(A^{2k(\#_M)})$ . 从而, 取  $i = 2k$ , 就得所需结果.

(ii) 可类似证明.

证毕.

最后, 我们来介绍一个有关  $A^{+(\#_M)}$  的重要表示定理(素分解定理).

**定理 18.** 设  $A \subseteq \Sigma^*$  与  $M \subseteq \Sigma$ . 我们有

$$A^{+(\#_M)} = P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{*(\#_M)} \cdot_M S_M^{(1)}(A) \cup A_M^{(0)}.$$

证明.

( $\subseteq$ ) 设  $w \in A^{+(\#_M)}$ . 依定义, 应存在  $i \geq 1$ , 使  $w \in A^{i(\#_M)}$ . 这时, 若  $|w|_M = 0$ , 则应有  $w \in A_M^{(0)}$ . 若  $|w|_M \neq 0$ , 则应存在  $a \in M$ , 使  $w = uav$ ,  $u, v \in \Sigma^*$ . 从而, 有  $ua \in P_M(A^{i(\#_M)})$  与  $av \in S_M(A^{i(\#_M)})$ . 这时, 据定理 13 的 (i) 与 (ii), 应分别存在  $k_1, k_2 \geq 0$ , 使得分别有  $ua \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k_1(\#_M)}$  与  $av \in (F_M^{(1)}(A))^{k_2(\#_M)} \cdot_M S_M^{(1)}(A)$ . 由此可推得有

$$\begin{aligned} w &= uav = ua \cdot_a av \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k_1(\cdot_M)} \\ &\quad \cdot_M (F_M^{(1)}(A))^{k_2(\cdot_M)} \cdot_M S_M^{(1)}(A) \\ &= P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{(k_1+k_2)(\cdot_M)} \cdot_M S_M^{(1)}(A) \\ &\subseteq P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^*(\cdot_M) \cdot_M S_M^{(1)}(A), \end{aligned}$$

( $\supseteq$ ) 设  $w \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^*(\cdot_M) \cdot_M S_M^{(1)}(A) \cup A_M^{(0)}$ . 这时, 若  $w \in A_M^{(0)}$ , 则由  $A_M^{(0)} \subseteq A \subseteq A^{+(\cdot_M)}$  可知, 有  $w \in A^{+(\cdot_M)}$ . 若  $w \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^*(\cdot_M) \cdot_M S_M^{(1)}(A)$ , 依定义, 应存在  $k \geq 0$ , 使

$$w \in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)} \cdot_M S_M^{(1)}(A),$$

这时, 我们有

$$\begin{aligned} w &\in P_M^{(1)}(A) \cdot_M (F_M^{(1)}(A))^{k(\cdot_M)} \cdot_M S_M^{(1)}(A) \\ &= P_M^{(1)}(A) \cdot F_M^{(k)}(A^{k(\cdot_M)}) \cdot_M S_M^{(1)}(A) \quad \text{定理 14} \\ &= P_M^{(1)}(A^{k(\cdot_M)}) \cdot_M F_M^{(k)}(A^{k(\cdot_M)}) \cdot_M S_M^{(1)}(A) \\ &\quad \text{定理 12(i)} \\ &\subseteq P_M^{(k+1)}(A^{2k(\cdot_M)}) \cdot_M S_M^{(1)}(A) \quad \text{定理 15(i)} \\ &\subseteq P_M(A^{2k(\cdot_M)}) \cdot_M S_M(A) = A^{2k(\cdot_M)} \#_M A \\ &= A^{(2k+1)(\cdot_M)} \subseteq A^{+(\cdot_M)}. \quad \text{证毕.} \end{aligned}$$

## 6 结束语

本文通过引入  $M$ -粘连代数、 $M$ -剪切代数与  $M$ -重组代数(也称  $M$ -桥接代数)等概念, 达到了将与标志集  $M$  相关联的 DNA 计算(文献[10]中称为简单拼接)精确到可按一定代数定律来演算的目的. 我们研究了这些代数的一系列性质, 得到许多有成效的结果. 它们对 DNA 计算的理论与应用的进一步研究, 必将带来极大的方便, 并加深我们对 DNA 计算的理解. 事实上, 像我们在前面看到的,  $M$ -剪切运算可看作现实中限制性内切酶对 DNA 分子作剪切的一个抽象;  $M$ -粘连运算则是剪切后所得片段在连接酶作用下匹配粘连成新 DNA 分子的一个抽象; 而  $M$ -重组运算则组合地应用剪切与粘连, 它恰可作为现实中 DNA 重组的一个抽象.

文献[10]中利用其所引入的跨接运算  $\#_M$ , 曾得到简单拼接语言的如下一个代数特征刻画.

**定理 19.** 设  $V$  是一字母表及  $L$  是  $V$  上一个语言, 这时,  $L \in SH$ , 当且仅当存在  $M \subseteq V$  及一有限语言  $L_0 \subseteq V^*$ , 使得  $L = set(L_0^{\#_M})$ .

定理中  $SH$  指简单拼接语言类,  $L_0^{\#_M}$  记写在幺半群  $\langle P(V^*), \#_M, \{\lambda\} \rangle$  (文献[10]中的断言. 实际上, 像我们前面脚注中指出的  $\{\lambda\}$  不是  $\#_M$  的单位元, 且像前面指出的它也不是半群, 只是我们称做的亚半群)中由  $\{L_0\}$  所生成的子半群. 按我们本文中的

记法就是

$$L_0^{\#_M} = \{L_0, L_0^{2(\cdot_M)}, \dots, L_0^{n(\cdot_M)}, \dots\}.$$

$set(L_0^{\#_M})$  则是求  $L_0^{\#_M}$  中所有集合之并. 在我们记法下应是

$$set(L_0^{\#_M}) = L_0^{+(\cdot_M)} = L_0 \cup L_0^{2(\cdot_M)} \cup \dots \cup L_0^{n(\cdot_M)} \cup \dots.$$

然而, 利用上面介绍的  $M$ -粘连代数、 $M$ -剪切代数与  $M$ -重组代数,  $SH$  中语言可作如下特征刻画.

**定理 20.** 设  $\Sigma$  是一字母表,  $L \subseteq \Sigma^*$ . 这时,  $L \in SH$ , 当且仅当存在  $M \subseteq \Sigma$ , 使得有

$$L = P_M^{(1)}(L) \cdot_M (F_M^{(1)}(L))^*(\cdot_M) \cdot_M S_M^{(1)}(L) \cup L_M^{(0)},$$

且  $P_M^{(1)}(L), S_M^{(1)}(L), F_M^{(1)}(L)$  与  $L_M^{(0)}$  均有限.

显然, 我们的刻画更细致、更清晰, 且更易于操作. 因为计算与检验  $P_M^{(1)}(L), S_M^{(1)}(L), F_M^{(1)}(L)$  与  $L_M^{(0)}$  比求找满足所需条件的  $L_0$  更明确, 更易于进行.

定理 20 的证明将另文给出.

## 参 考 文 献

- [1] Head T. Formal language theory and DNA: An analysis of the generative capacity of specific recombinant behaviours. *Bulletin of Mathematical Biology*, 1987, 49: 737-759
- [2] Head T. Splicing representations of strictly locally testable languages. *Discrete Applied Mathematics*, 1998, 87: 139-147
- [3] Culik I I K, Harju T. Splicing semigroups of dominoes and DNA. *Discrete Applied Mathematics*, 1991, 31: 261-277
- [4] Pixton D. Regularity of splicing languages. *Discrete Applied Mathematics*, 1996, 69: 101-124
- [5] Freund R, Kari L, Păun Gh. DNA computing based on splicing: The existence of universal computers. *Theory of Computing Systems*, 1999, 32: 69-112
- [6] Păun Gh. DNA computing based on splicing: Universality results. *Theoretical Computer Science*, 2000, 231(2): 275-296
- [7] Kobayashi S, Sakakibara Y. Multiple splicing systems and the universal computability. *Theoretical Computer Science*, 2001, 264(1): 3-23
- [8] Păun Gh. On the splicing operation. *Discrete Applied Mathematics*, 1996, 70: 57-79
- [9] Kobayashi S, Mitrana V, Păun Gh, Rozenberg G. Formal properties of PA-matching. *Theoretical Computer Science*, 2001, 262(1-2): 117-131
- [10] Mateescu A, Păun Gh, Rozenberg G, Salomaa A. Simple splicing systems. *Discrete Applied Mathematics*, 1998, 84: 145-163
- [11] Honkala J, Salomaa A. Watson-crick DOL systems with regular triggers. *Theoretical Computer Science*, 2001, 259(1-2): 689-698

[12] Mihalache V, Salomaa A. Language-theoretic aspects of DNA complementarity. *Theoretical Computer Science*, 2001, 250(1-2): 163-178

[13] Yokomori T, Kabayashi S. DNA evolutionary linguistics and RNA structure modeling: A computational approach//*Proceedings of the 1st International IEEE Symposium on Intelligence in Neural and Biological System*, 1995: 38-45

[14] Adleman L. Molecular computation of solution to combinatorial problems. *Science*, 1994, 266: 1021-1024

[15] Lipton R. Speeding up computations via molecular biology. Draft, Dec. 9, 1994(/ftp/pub/people/rjl/bio.ps on ftp.cs.princeton.edu)

[16] Boneh D, Dunworth C, Lipton R, Sgall Jiri. On the computational power of DNA. *Discrete Applied Mathematics*, 1996, 71: 79-94

[17] Adleman L. On constructing a molecular computer. Department of Computer Science, University of Southern California, USA: Technical Report TR79-387, 1995

[18] Head T, Păun Gh, Pixton D. Language theory and molecular genetics: Generative mechanisms suggested by DNA recombination//Rozenberg G, Salomaa A eds. *Handbook of Formal Languages*. Heidelberg: Springer, 1997, 2: 295-360

[19] Păun Gh, Rozenberg G, Salomaa A. *DNA Computing: New Computing Paradigms*. Berlin: Springer, 1998(in Chinese) (许进, 王淑栋, 潘林强译. *DNA 计算: 一种新的计算模式* (中译本). 北京:清华大学出版社, 2004)



**HUANG Yu-Qian**, born in 1938, professor. His research interests include formal language and automata theory, DNA computing.

Background

In his pioneering paper [Head,1987], Head had introduced the splicing system concept as a formal device for the generation of languages and as a formal model of specific forms of DNA recombination. Thus he established the close relationship between the recombinant behavior of DNA in the field of life science and formal language theory in theoretical computer science. The splicing operation raises a large number of appealing problems for formal language theorists: Producing new splicing systems and studying it's power as well as properties of corresponding languages, looking for the relation between splicing operations and usual operations in formal language theory and for the closure of families of languages (in Chomsky hierarchy) under such operations, etc. After this, one developed varied splicing systems, such as, H-systems, extended H-systems, extended H-systems with certain control mechanisms (multiset, permitting context, forbidding context, double splicing, or distributed architectures), multiple splicing systems, etc. Some systems among those was proved that they are computation complete (equivalent to Turing machine), and constructed corresponding universal

splicing systems. Mateescu et al. considered simple splicing systems [Mateescu,1998]. They investigated the properties of the corresponding family: Representation, closure properties, descriptiveal complexity, decidability, relationships with other subfamilies of the family of regular languages etc. Specifically, they gave an algebraic characterization for languages in this family by introduced operation  $\#_M$ . But, except indicating that  $\#_M$  is an associative operation (expression and proof both are wrong), they haven't do any further researches of properties for introducing operations  $\Diamond_M$  and  $\#_M$ . In this paper, the author replaces  $\Diamond_M$  by  $\bullet_M$ , and improves the definition of the operation  $\#_M$ . Moreover, the author also introduces new operations  $P_M$ ,  $S_M$  and  $F_M$ . Specifically, he investigates a series of properties of those operations, and further proposes concepts of  $M$ -paste algebra,  $M$ -cut algebra and  $M$ -recombination. Thus the DNA computing associated with mark set  $M$  can be deduced precisely according to algebraic laws given in proposed algebras. These results will give us much convenience in research on the theory and application of DNA computing.