Semir形式和与单射偏变换的半环

Maximilien Gadouleau* Marianne Johnson†

2026年3月30日

arXiv:2603.26508v1 [math.RA] 27 Mar 2026

摘要

离散动力系统半环是描述确定性系统模块性的一种简单代数模型。该半环的对象是有限变换（视为有向图并按同构等价），两个变换的和对应于在不同集合上分别应用它们，而乘积对应于并行应用这两个变换。本文将此半环扩展到包含部分变换的情形；和与乘积是自然推广。每个（部分）变换都可以视为由连通（部分）变换组成的一个和（在自然数集上）。我们通过研究任意半环 S 上的形式和半环，将这一思想加以推广。这里我们考虑 S $=\mathrm{F}_2$，为二元域的情形，并聚焦于单射偏变换，即链与圈的和。尽管目前尚无已知的高效算法可以求解原离散动力系统半环中圈的和的除法问题，但我们给出了 F_2 上圈的和的除法问题所有解的简明刻画。随后，我们将这一刻画推广到任意单射偏变换的除法，即 F_2 上链与圈的和。

1 引言

1.1 变换半环

许多大型系统，无论是抽象的还是现实中的，都是模块化的，也就是说，它们由执行各自任务的较小模块组合而成。例子包括布尔网络 [22, 17],脉动阵列 [23], 元胞自动机 [21, 2, 19], 和 Petri网 [7, 8, 27]。类似地，在代数中，结构（代数结构或关系结构）的直积是一种基本运算，可在任何类上定义，例如群、环或半群；而在图论中，不交并是组合两个有向图的一种基本方式。

变换半环最早于2018年由元胞自动机领域的研究人员提出[4] ，作为确定性系统的简单数学模型。[1] 半环的对象是有限变换（从有限集到其自身的函数），并以图同构为准。这些对象配备了两种运算：和对应于两个系统具有互不相交的动力学，而乘积对应于两个动力学的并行组合。

该模型旨在保持简洁的同时具有广泛适用性：被建模的系统具有有限个可能状态，我们并不了解这些状态的语义，而系统则由确定性演化来表示。这两种运算代表组合这些系统的不同方式。完整变换假设每个状态都有一个确定的后继，但某些状态可能导致特征未定义，甚至使整个系统崩溃；这类没有后继的状态则由部分变换来封装。重要的是，这也适用于只能获得有关转移的部分信息的情况。因此，本文将变换半环扩展为部分变换半环；在这种情况下，和与乘积的定义十分自然。

*杜伦大学计算机科学系，英国。m.r.gadouleau@durham.ac.uk

†曼彻斯特大学数学系，英国。marianne.johnson@mathematics.manchester.ac.uk[1]它曾以离散动力系统、有限动力系统或函数有向图的半环之名出现；我们将这些对象称为变换。

两个部分变换的和与乘积示例见图1。半环的对象是无标记图，显示在顶行。底行显示的标记说明了乘积的运作方式：例如，弧 $b \to a$ 位于 A 和 $3 \to 1$ 位于 B 中的弧共同得到弧$b3 \to a1$ 位于 AB中。请注意，乘积是交换的。部分变换可以表示为有向图，其中每个顶点都有唯一的后继。用图论术语来说，和表示有向图的不交并，而乘积表示有向图的直积 [15]。

变换半环最初在 [4] 中被引入，重点关注算法问题。例如，[5, 9, 1, 6]中给出了求解简单方程（与除法方程 $ax = b$相关）的算法， [3]中则给出了一个高效的变换枚举算法。此外， [26]中还为一类称为抽象的约简提供了一个自然框架。具体而言，其思想是聚焦于变换的某个特定方面，从而简化方程的求解。约简的自然例子包括基数、暂态部分、周期部分和同态像。所谓的轮廓由 [10], 引入，它根据状态到周期部分的距离对状态进行计数。展开 [20] 是一个到（可能无限）森林的半环的同态，并且保持暂态部分不变。展开是理解变换半环中暂态部分的关键，因此在 [20] 中被用于刻画可消去变换（a 满足：若$ax = ay$，则 $x = y$），并且更一般地说，还被用于刻画单变量单射多项式 [24]。

求解多元方程 $P(\vec{x}) = c$，其中 P是变换半环上的多元多项式， c 是一个固定变换，被认为是 NP 完全问题，因为对应的轮廓问题确实是 NP 完全的 [10]。然而，揭示代数性质（例如展开同态或单变量单射多项式的分类）往往也会带来算法方面的结果。例如， [20]给出了一个多项式时间算法，用于对两个树状变换（即所有轨迹最终都会到达唯一不动点的变换）进行除法；而[24] 则给出了一个多项式时间算法，用于求解方程 $P(x) = c$ ，其中涉及单变量单射多项式 P 和固定变换 c；后者已在 [25]中进一步推广到所谓的伪单射多项式。

尽管如此，变换半环中许多计算问题的复杂度仍然未知。一个关键问题是除法方程 $ax = b$，即使将范围限定为置换，也就是圈的和。当前最快的算法见 [1], ，可在亚指数时间内求解以下情形： a 和 b 为置换时的 $ax = b$。

1.2 贡献与概要

集合 X 上的部分变换是一个映射 $f\colon Y \to X$，其中 $Y \subseteq X$。由 f 可以定义有向图 D_f，其顶点集为 $V(D_f) = X$，弧集为 $E(D_f) = \{(y, f(y)) : y \in Y\}$。在这个有向图中，每个顶点的出度至多为一；反过来，任何每个顶点的出度至多为一的有向图，都可以用这种方式构造。我们称 X 上的两个部分变换 f 和 f' 等价，当且仅当 D_f 和 $D_{f'}$ 同构。接下来我们考虑部分变换的等价类。两个（等价类）部分变换 $f\colon Y \to X$ 和 $f'\colon Y' \to X'$ 的和，其中 X 和 X' 不交，是它们的不交并： $f + f'\colon Y \cup Y' \to X \cup X'$，其中对所有 $y \in Y$，$(f + f')(y) = f(y)$；并且对所有 $y' \in Y'$，$(f + f')(y') = f'(y')$。它们的乘积由有向图的直积给出： $ff'\colon Y \times Y' \to X \times X'$，其中对所有

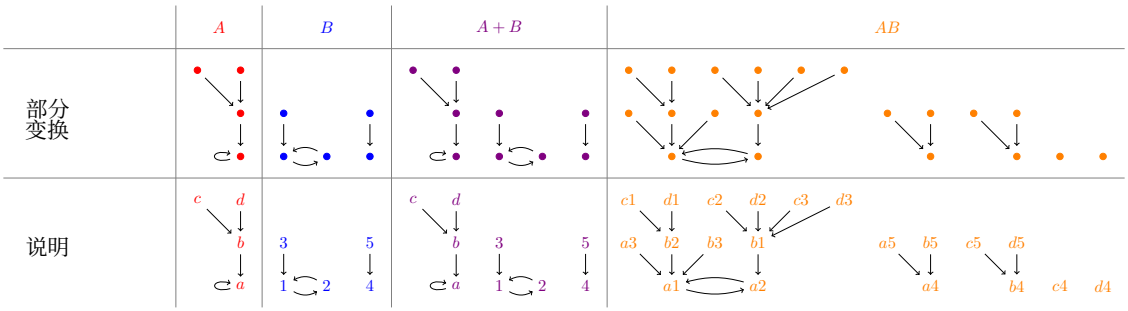


图1：部分变换的和与乘积。

$(y, y') \in Y \times Y'$。显然，这些运算是良定义的，因为和与乘积保持部分变换的等价关系。

本文有两项主要的定性贡献。第一项定性贡献是考虑部分变换。我们从两个方面阐述这种推广的动机。首先，在许多系统中，某些配置会导致状态未定义，或发生某种故障。因此，并非所有状态始终都有后继，系统可由部分变换表示。其次，在系统生物学中，人们通过逐步发现系统中的某些转移来了解该系统，而有些转移在实际中可能难以发现。因此，必须用部分变换描述当前对系统的认知。将变换的和与乘积的定义自然地推广后，部分变换构成一个半环。

第二项主要的定性贡献是通过考虑有限半环 S 上的形式和，将挠引入部分变换半环。这会立即带来加法挠，也可能带来乘法挠。在原始的变换半环中，元素没有挠，因为 a、a^2、a^3.....的顶点集大小各不相同；同样，a、$2a$、$3a$等也都各不相同。例如，圈 C_d 满足 $C_d^2 = dC_d$，因此对所有 $k \geq 1$ 都有 $C_d^k = d^{k-1}C_d$。另一方面，譬如若 $\mathrm{S} = \mathrm{F}_2$ 是二元域，那么我们就对圈的和按“模 2”计数，例如，置换 $C_3 + 4C_4 + 2C_5 + 7C_8$ 变为 $C_3 + C_8$。在这个半环中，若 d 为偶数，则有 $C_d^2 = 0$；若 d 为奇数，则有 $C_d^2 = C_d$；此外，$C_d + C_d = 0$。这些关系不仅大大简化了计算，还带来了丰富的代数结构，可供利用（见第 3 节）。

本文研究某些交换半环中的除法问题（给定 a，$b \in S$ 判断是否存在 $ax = b$ 的解），这等价于研究底层乘法半群中的格林关系（任意一种）。我们特别考察由具有有限支撑的单射偏变换的等价类构成的子半环，其中每个这样的图都可以分解为循环和链。更具体地，对于每个正整数 d，令 $L_d = d \to (d-1) \to \cdots \to 1$ 表示长度为 d 的链，并如前所述，令 $C_d = d \to d-1 \to \cdots \to 1 \to d$ 表示长度为 d的圈。我们将所有有限链的集合记为 L，将所有有限圈的集合记为 C。我们的主要技术贡献集中在圈的和的除法问题上，采用模 2 计数，即在 $\mathrm{S}C$中运算，其中 $\mathrm{S} = \mathrm{F}_2$ 且 $C = \{C_d : d \geq 1\}$ 是所有圈的集合。我们在定理 3.9 中证明，模 2 计数时 $ax = b$ 的解可以用布尔代数中的区间表示；特别是，可以高效地判断 $ax = b$ 是否有解。我们从两个方面扩展这一结果。首先，结合 [24] 关于单射多项式的研究，我们对 F_2C 上的单变量单射多项式进行分类，并在定理 3.21 中证明，求解这类多项式的方程十分直接。其次，我们在定理 4.2 中解决了单射偏变换的除法问题，即 $\mathrm{F}_2(L \cup C)$ 中的除法问题。

本文其余部分安排如下。首先，我们在第 2.1 节介绍形式和半环的一般框架，并在第 2.2 节重点讨论半格元素在 F_2 上的形式和这一重要情形。其次，我们在第 3 节全面研究由模2圈的形式和构成的半环 F_2C：在第 3.1 节给出一些一般性的基本结果；在第3.2节刻画幂等元布尔代数；在第 3.3 节刻画除法方程 $ax = b$ 的解；在第 3.4 节刻画该半群中的（扩展）格林关系；在第 3.5 节对单位元、正则元等进行分类；在第 3.6 节对单变量单射多项式进行分类；并在第 3.7 节研究主理想的交集。最后，我们在第 4 节考虑单射偏变换形式和半环中的除法问题：首先在第 4.1 节讨论幂零单射偏变换（即链的和）这一简单情形，随后在第 4.2 节讨论一般情形。本文最后是第 5 节结论，其中提出了一些未来工作的可能方向。

2 形式和半环

2.1 一般情况

交换半环是一种结构 $(\mathrm{S}, +, \times, 0, 1)$，其中 $(\mathrm{S}, +)$ 在加法下构成单位元为 0 的交换幺半群，在乘法下构成单位元为 1 的交换幺半群，且乘法对加法满足分配律，

也就是说，对于所有 a，b，$c \in \mathsf{S}$，都有 $a \times (b+c) = (a \times b) + (a \times c)$，并且 0 是乘法零元，也就是说，对于所有 $a \in \mathsf{S}$，都有 $0 \times a = a \times 0 = 0$。由于本文讨论的所有半环都是交换的，我们通常只称其为“半环”。如常规做法，在上下文明确时，我们用 ab 代替 $a \times b$。我们用 $\mathbf{N} = \{0, 1, \ldots, \}$ 表示在通常算术运算下的自然数半环。

设 G 是一个集合，S 是一个半环。令 $\mathsf{S}G$ 为由 G 中元素构成、系数取自 S 且具有有限支撑的形式和的集合，即

$$\mathbb{S}G = \left\{ \sum_{j \in G} s_j j : s_j \in \mathbb{S},\ \text{finitely many non-zero } s_j \right\}.$$

对于 $s \in \mathsf{S}G$ 和 $j \in G$，我们用 s_j 表示 s 中 j 的系数。注意，S 在 $\mathsf{S}G$ 上有一个显然的左作用，由 $(as)_j = as_j$ 确定，对所有 $a \in \mathsf{S}$ $s \in \mathsf{S}G$，$j \in G$ 均成立；此外，S 上还定义了逐点加法，由 $(s+t)_j = s_j + t_j$ 确定，对所有 s，$t \in \mathsf{S}G$ 及所有 $j \in G$ 均成立。显然，这一运算满足结合律和交换律。对于 $g \in G$，我们也将（稍微滥用记号）直接写作 g，表示 $\mathsf{S}G$ 中的元素 $1g$。我们还用 0 表示空和，它是加法单位元。为了在 $\mathsf{S}G$ 上指定一个半环结构，只需指定一个形如 $G \times G \to \mathsf{S}G$ 的函数，并使其满足某些自然条件。

定理 2.1. 设$\mathbb{S}$ 是一个交换半环，并假设 G 是一个带有运算的集合 $\cdot :\ G \times G \to \mathbb{S}G$，满足以下三个条件：

1. 对所有 $g, h \in G$, $g \cdot h = h \cdot g$;
2. 存在 $e \in G$，使得对所有 $g \in G$，$e \cdot g = g \cdot e = g \in \mathbb{S}G$；
3. 对所有 $g, h, i, k \in G$
$$\sum_{j \in G} (g \cdot h)_j (j \cdot i)_k = \sum_{j \in G} (h \cdot i)_j (j \cdot g)_k.$$

那么，$\mathbb{S}G$ 关于逐点加法以及由下式给出的乘法构成一个半环：

$$\sum_{g \in G} s_g g \cdot \sum_{h \in G} t_h h = \sum_{g,h \in G} s_g t_h (g \cdot h). \tag{1}$$

此外，若$\mathbb{S}$ 是一个环，则$\mathbb{S}G$ 也是一个环。

证明。 首先注意，(1) 中的公式定义了一个良定义的函数 $\mathsf{S}G \times \mathsf{S}G \to \mathsf{S}G$：根据定义，$g \cdot h$ 是一个系数取自 S 且具有有限支撑的形式和；由于 S 在 $\mathsf{S}G$ 的左侧作用，因此对所有 $g, h \in G$ 以及所有 a，$b \in \mathsf{S}$，我们有 $ab(g \cdot h) \in \mathsf{S}G$；继而，由于系数 s_g 和 t_h 中只有有限多个非零，可知上述元素具有有限支撑。容易看出，空和 0 相对于此乘法是左零元和右零元。条件 1 与 S 中的乘法是交换的这一事实，显然意味着此乘积是交换的；而条件 2 中元素 e 的存在则保证 $e \in \mathsf{S}G$是该乘法的单位元。接下来注意，对所有 $g, h, i \in G$，我们有

$$\begin{aligned}
(g \cdot h) \cdot i &= \left(\sum_{j \in G} (g \cdot h)_j j \right) \cdot i = \sum_{j \in G} ((g \cdot h)_j (j \cdot i)) = \sum_{j \in G} \left((g \cdot h)_j \sum_{k \in G} (j \cdot i)_k k \right) = \sum_{k \in G} \sum_{j \in G} (g \cdot h)_j (j \cdot i)_k k \\
g \cdot (h \cdot i) &= g \cdot \left(\sum_{j \in G} (h \cdot i)_j j \right) = \sum_{j \in G} (h \cdot i)_j (g \cdot j) = \sum_{j \in G} \left((h \cdot i)_j \sum_{k \in G} (g \cdot j)_k k \right) = \sum_{k \in G} \sum_{j \in G} (h \cdot i)_j (g \cdot j)_k k,
\end{aligned}$$

因此，当且仅当条件 3 成立时，$(g \cdot h) \cdot i = g \cdot (h \cdot i)$。由此不难验证，在 $\mathsf{S}G$ 上定义的乘法是结合的，而且乘法对加法满足分配律。因此，$\mathsf{S}G$是一个半环。

□

例 2.2。 若 G 是一个交换幺半群，且$\mathbb{S}$ 是一个半环，取 $g \cdot h = gh \in \mathbb{S}G$，容易看出上述各条件都成立。事实上，$G$中幺半群乘法的结合性确保了第三个条件成立，因为对于所有 a、 b、 $c \in G$，都有$(ab)_c = \delta(ab, c)$，因此

$$\sum_j (gh)_j (ji)_k = \delta((gh)i, k) = \delta(g(hi), k) = \sum_j (hi)_j (gj)_k.$$

在这种情况下，$\mathbb{S}G$ 关于给定运算构成了以 G 为基、系数取自 $\mathbb{S}$ 的幺半群代数（通常研究的是 $\mathbb{S}$ 为域的情形）。

注2.3. 假设给定一个运算 $G \times G \to$ 自然数集G，满足定理 *2.1* 的条件。那么，对于任意半环 $\mathbb{S}$，我们都可以利用运算 $\cdot\colon G \times G \to$自然数集$G$在 $\mathbb{S}G$ 上定义乘法。具体而言，若 ϕ 是从自然数集 到$\mathbb{S}$ 的唯一半环同态，我们可以定义 $\cdot_{\mathbb{S}}\colon G \times G \to \mathbb{S}G$为 $g \cdot_{\mathbb{S}} h = \sum_j \phi((g \cdot h)j)j$，不难验证此映射也满足定理 *2.1* 的条件。

例2.4. 取 G 为所有出度最大值不超过一的有限有向图构成的集合，并将同构的图视为相同，则离散动力系统半环就是半环自然数集G，其中两个图的乘积由函数 $G \times G \to$ 自然数集G 确定，如引言中所述。例如，对于图*1*中的 A 和 B，我们得到 $AB = M + 2N + 2P$，其中M 是含有 *12* 个顶点的连通分量， N 是含有三个顶点的连通分量（在同构意义下出现两次），而 P 是由单个顶点组成的连通分量（在同构意义下也出现两次）。对于$\mathbb{S} = \mathbb{F}_2$ ——含有两个元素的域——我们也可以考虑环 $\mathbb{F}_2 G$，这相当于将自然数集 中的所有系数模2计算。例如，在上面的例子中，作为$\mathbb{F}_2 G$中的元素时，我们有 $AB = M$。在接下来的几节中，我们将研究$\mathbb{F}_2 G$的某些子环。

2.2 关于有限半格上的 $\mathbf{F}_2$形式和

现在我们聚焦于一个特殊情形： G 是有限半格，且 $\mathbb{S} = \mathbf{F}_2$，，这对第3节和第4节会有所帮助。在这种情形下，$\mathbb{S}G$的结构是一个布尔代数。

我们回顾一下格的一些基本符号和术语；有关格的权威性综述，请参阅 Gr¨azer [14]所著的书。设 $\mathcal{L} = (L, \vee, \wedge, 0, 1)$ 是一个有界格，其最大元记为 1，最小元记为 0。我们自然地将 $l \leq m$ 记作 $l = l \wedge m$，或等价地记作 $m = l \vee m$。对于任意 $l \in L$，记 $l^{\uparrow} = \{m \in L : m \geq l\}$, $l^{+} = \{m : m > l\}$，以及$l^{\downarrow} = \{m \in L : m \leq l\}$。注意， $l^{\downarrow}$ 也是一个有界格，其最大元为 l，最小元为 0。对于任意 $l \in L$，令 l^c 表示被 l 覆盖的 L 中元素的集合，即 $l^c = \{m \in L : m < l, \nexists n : m < n < l\}$。若 $a^c = \{0\}$，则元素 $a \in L$ 是 $\mathcal{L}$ 的一个原子；我们将 $\mathcal{L}$ 的原子集合记为 $\mathsf{A}(\mathcal{L})$。回顾一下，对于所有 l, $m \in L$，区间 $[l, m]$ 由 $[l, m] = \{x \in L : l \leq x \leq m\}$ 给出；除非$l \leq m$，否则该区间为空。

设 $\mathcal{L} = (L, \vee, \wedge, \mathbf{0}, \mathbf{1})$ 是一个以 n 个元素构成的有限格。那么

$$\mathbb{F}_2 L = \left\{ \sum_{l \in L} a_l l : a_l \in \mathbb{F}_2 \ \forall l \in L \right\},$$

赋予例 2.2 中的加法和乘积，并将 L 视为关于交的幺半群后，它构成一个布尔环。为强调元素 $l \in L$ 与形式和 $1 \cdot l$ 之间的区别，我们将后者称为单位向量 e_l。反过来，$\mathbf{F}_2 L$ 上的布尔环诱导出布尔代数 $V(\mathcal{L}) = (\mathbf{F}_2 L, \vee_{V(\mathcal{L})}, \wedge_{V(\mathcal{L})}, \mathbf{0}_{V(\mathcal{L})}, \mathbf{1}_{V(\mathcal{L})})$，其中:

- 交由 $a \wedge_{V(\mathcal{L})} b = ab$ 给出,
- 并由 $a \vee_{V(\mathcal{L})} b = a + b + ab$ 给出,
- 下界是全零向量（空和）$\mathbf{0}_{V(\mathcal{L})} = 0$,
- 上界是单位向量 $\mathbf{1}_{V(\mathcal{L})} = e_{\mathbf{1}}$,

- 补集由 $\neg_{V(\mathcal{L})} a = a + e_{\mathbf{1}}$ 给出。

当上下文清楚表明我们是在 $V(\mathcal{L})$ 中进行运算时，我们会省略记号中的下标 $V(\mathcal{L})$ 。

所有阶相同的有限格都会得到同构的布尔代数：若 $|L| = n$，则 $V(\mathcal{L})$ 与 $\{1, \ldots, n\}$ 的幂集格同构，而后者显然有 n 个原子 [11]。然而， $V(\mathcal{L})$ 确实包含了 $\mathcal{L}$ 的结构，因为 $e_l \leq e_m$ 属于 $V(\mathcal{L})$ 当且仅当 $l \leq m$ 属于 $\mathcal{L}$。

$\mathrm{F}_2 L$ 的每个元素都可以视为其支撑，也就是 L 中系数非零的元素所构成的子集。因此，若 $a \in \mathrm{F}_2 L$，我们记 $l \in a$，当且仅当 $a_l = 1$，并记 $\bigvee a = \bigvee_{l \in a} l$； $V(\mathcal{L})$ 中的加法 $a + b$ 对应于集合 $a \Delta b$ 的对称差。

在第3.2节中，我们将研究由奇圈自然产生的某类有限格所对应的布尔代数 $\mathrm{F}_2 L$ 。刻画这些代数的原子将非常有用。更一般地，为了在 $\mathrm{F}_2 L$ 中进行计算，确定其原子是一项基本要求。因此，我们在下文的定理 2.6 中构造 $\mathrm{F}_2 L$ 的全部原子。我们先给出一种构造。

引理 2.5。 设 $\mathcal{D} = (D, \vee, \wedge, \mathbf{1}_{\mathcal{D}}, \mathbf{1}_{\mathcal{D}})$ 是一个有限格。那么存在唯一的子集 $a^*(\mathcal{D}) \subseteq D$，使得 $\mathbf{1}_{\mathcal{D}} \in a^*(\mathcal{D})$，并且对于所有满足 $m \neq \mathbf{1}_{\mathcal{D}}$ 的 $m \in D$， $a^*(\mathcal{D})$ 都包含偶数个大于或等于 m的元素。

证明。 将 D 的元素标记为 $d_1, \ldots, d_n$，使得只有当 $i \leq j$ 时才有 $d_i \geq d_j$（特别地， $d_1 = \mathbf{1}_{\mathcal{D}}$ 和 $d_n = \mathbf{0}_{\mathcal{D}}$）。注意，对于所有 $i \geq 2$， $d_i^+ \subseteq \{d_1, \ldots, d_{i-1}\}$。我们递归地构造 $a^*(\mathcal{D})$ 如下。首先， $d_1 = \mathbf{1}_{\mathcal{D}} \in a^*(\mathcal{D})$。然后，对于所有 $2 \leq i \leq n$，当且仅当 $|d_i^+ \cap a^*(\mathcal{D})|$ 为奇数时， $d_i \in a^*(\mathcal{D})$。注意，任何其他选择都会违反引理的某个条件。

□

现在，对于有界格 L 的任意元素 l，记作 $a^l = a^*(l^{\downarrow})$。特别地， $a^{\mathbf{1}} = a^*(\mathcal{L})$。注意，根据构造， $l \in a^l$；此外， a^l 的所有元素都小于或等于 l。回想一下，我们将 L 的子集，尤其是 a^l，视为 $\mathrm{F}_2 L$ 的元素。因此 $\bigvee a^l = l$。

定理 2.6. $V(\mathcal{L})$ 的原子集合为

$$\mathrm{A}(V(\mathcal{L})) = \{a^l : l \in L\}.$$

我们将在证明中看到， $b = a^l$ 是 $V(\mathcal{L})$ 中满足 $\bigvee b = l$ 的唯一元素。证明先从 $V(\mathcal{L})$ 的原子的一个简单而有用的性质开始。

引理 2.7. </style}非零元素 ($\mathcal{L}$) 是原子，当且仅当对所有 $l \in L$，都有 $e_l a \in \{a, 0\}$ 。

证明。 由于 a 非零，当且仅当对所有 $x \in V(\mathcal{L})$ 都有 $xa \in \{a, 0\}$ 时，它是原子。若 a 是原子，那么这对任意单位向量 e_l 尤其成立。反过来，若对所有 $l \in L$ 都有 $e_l a \in \{a, 0\}$，那么对于任意 $x = \sum_l \alpha_l e_l$，我们有 $xa = \sum_l \alpha_l (e_l a) \in \{a, 0\}$。 □

推论 2.8. 若 a 是 $V(\mathcal{L})$的一个原子，则对所有 $l < \bigvee a$， $e_l a = 0$ 。

证明. 若 $l < \bigvee a$，则 l 不可能大于或等于 a的所有元素，也就是说，存在$m \in a \setminus l^{\downarrow}$。回想一下， $e_l a$ 的所有元素都属于 $l^{\downarrow}$，于是我们有 $m \notin e_l a$，从而 $e_l a \neq a$；因此得到 $e_l = 0$。

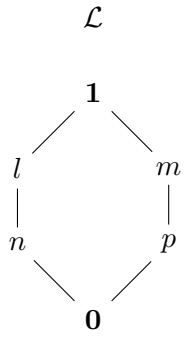
□

定理 *2.6* 的证明. 我们先证明，若 a 和 b 是不同的原子，则 $\bigvee a \neq \bigvee b$。反设结论不成立，设 a 和 b 是原子，且 $a \neq b$，使得 $a \Delta b \neq \emptyset$，但 $s = \bigvee a = \bigvee b$。令 l 为 $a \Delta b$的一个极大元素，即 l 恰好属于 a 或 b 之一，并且对任意 $m \in l^+$，都有 $m \in a \cap b$或 $m \notin a \cup b$。我们得到 $|l^+ \cap a| = |l^+ \cap b|$，从而 $|l^{\uparrow} \cap a| = |l^{\uparrow} \cap b| \pm 1$。因此，若$|l^{\uparrow} \cap a|$ 为奇数，则 $e_l a \neq 0$；若 $|l^{\uparrow} \cap a|$ 为偶数，则 $e_l b \neq 0$。另一方面，由于 $l < s$，根据推论 2.8 有 $e_l a = e_l b = 0$，这正是所需的矛盾。

我们刚刚证明了映射 $\mathrm{A}(V(\mathcal{L})) \to L, a \mapsto \bigvee a$ 是单射。回想一下， $V(\mathcal{L})$ 与 L 的幂集格同构，因此 $|\mathrm{A}(V(\mathcal{L}))| = |L| = n$，该映射也是满射；也就是说，对于每个 $l \in L$， $V(\mathcal{L})$ 中都有一个原子，记作 b，使得 $\bigvee b = l$。注意，（根据假设） b 的所有元素都必须属于 $l^{\downarrow}$。现在我们将证明 $b = a^l$。

首先，我们证明 $l \in b$。为导出矛盾，假设 $l \notin b$。由于 $l = \bigvee b$， b 至少有两个不同的极大元素，记作 x 和 y。我们将证明 $e_x b \notin \{b, 0\}$。由于 x， $y \in L$ 是 b 的极大元素，因此我们有 $y \notin x^{\downarrow}$，进而得到 $y \notin e_x b$ 和 $e_x b \neq b$。接下来， $x^{\uparrow} \cap b = \{x\}$，于是 $x \in e_x b$ 和 $e_x b \neq 0$。因此 $e_x b \notin \{b, 0\}$，这与引理 2.7 矛盾。由此矛盾可得 $l \in b$。其次，对于所有 $m < l$，我们有 $l \notin e_m b$，因此由引理 2.7 得到 $e_m b = 0$。于是，对于所有 $m < l$， $|m^{\uparrow} \cap b|$ 甚至成立。最后， b 是 $l^{\downarrow}$ 的子集，使得 $l \in b$，并且对于每个 $m < l$， $|m^{\uparrow} \cap b|$ 都是偶数，因此由引理 2.5 可得 $b = a^l$。 □

例 2.9。 图 2 左侧给出了格 $\mathcal{L}$ 的一个例子，右侧列出了$V(\mathcal{L})$ 的原子。我们注意到 $a^{\mathbf{0}} = e_{\mathbf{0}}$，并且 $a^t = t + \mathbf{0}$ 对每个原子$t \in \mathrm{A}(\mathcal{L})$都成立；这两个事实对任意有限格 $\mathcal{L}$ 均成立。



V（$\mathcal{L}$）的原子:

$$
\begin{aligned}
a^{\mathbf{1}} &= \mathbf{1} + l + m + \mathbf{0}, \\
a^{l} &= l + n, \\
a^{m} &= m + p, \\
a^{n} &= n + \mathbf{0}, \\
a^{p} &= p + \mathbf{0}, \\
a^{\mathbf{0}} &= \mathbf{0} \ (= e_{\mathbf{0}}) 。
\end{aligned}
$$

图 2：六边形格 $\mathcal{L}$ 及 V（$\mathcal{L}$）的原子。

现在我们将讨论推广到 G 是半格而非格的情形。事实上，用于研究这一情形的框架也涵盖了由偶数项之和构成的子格，这在我们研究第 4.2 节中单射偏变换的分解时会派上用场。因此，我们先给出一般性的框架，再聚焦于这两个重要的特殊情形。

现在我们来仔细考察 $V(\mathcal{L})$ 的一种特殊子格。对于任意 $x \in V(\mathcal{L})$ 以及任意 $l \in L$，令 $|x|_l = 1$ （当 $x \geq a^l$ 时），否则令 $|x|_l = 0$。由于 a^l 是原子， $xa^l \in \{a^l, 0\}$；由此可得，当 $xa^l = a^l$ 时 $|x|_l = 1$，而当 $xa^l = 0$ 时 $|x|_l = 0$。接着定义

$$P_l(\mathcal{L}) = \{x \in V(\mathcal{L}) : |x|_l = 0\}.$$

引理 2.10。 对于任意 $l \in L$，有 $P_l(\mathcal{L}) = (a^l + e_{\mathbf{1}})^{\downarrow}$。

证明。 $|x|_l = 0$ 当且仅当 $xa^l = 0$，而这又等价于 $x \leq \neg a^l = a^l + e_{\mathbf{1}}$。 □

这立即给出了区间与 $P_l(\mathcal{L})$的交集的简单刻画，我们将在第 4 节中使用。

推论2.11。 对于所有满足 $\lambda \leq \upsilon$ 的 $\lambda, \upsilon \in V(\mathcal{L})$ 以及所有 $l \in L$，我们有

$$[\lambda, \upsilon] \cap P_l(\mathcal{V}) = [\lambda, \upsilon + \upsilon a^l], \tag{2}$$
$$[\lambda, \upsilon] \setminus P_l(\mathcal{V}) = [\lambda + a^l + \lambda a^l, \upsilon]. \tag{3}$$

证明。 我们有

$$[\lambda, \upsilon] \cap P_l(\mathcal{V}) = [\lambda, \upsilon] \cap [0, a^l + e_{\mathbf{1}}] = [\lambda \vee 0, \upsilon(a^l + e_{\mathbf{1}})] = [\lambda, \upsilon + \upsilon a^l].$$

类似地，$[\lambda, \upsilon] \setminus P_l(\mathcal{V}) = [\lambda, \upsilon] \cap [a^l, e_{\mathbf{1}}] = [\lambda \vee a^l, \upsilon e_{\mathbf{1}}] = [\lambda + a^l + \lambda a^l, \upsilon]$。

□

我们重点关注 $P_{\mathbf{i}}(\mathcal{L})$ 的两个特殊情形。首先，**奇偶校验码**定义为不大于 $a^{\mathbf{0}} = e_{\mathbf{0}}$ 的元素：

$$P_{\mathbf{0}}(\mathcal{L}) = \{x \in V(\mathcal{L}) : |x|_{\mathbf{0}} = 0\}.$$

根据引理 2.10， $P_{\mathbf{0}}(\mathcal{L}) = (e_{\mathbf{1}} + e_{\mathbf{0}})^{\downarrow}$。因此，奇偶校验码是一个布尔代数，其原子为 $\mathsf{A}(V(\mathcal{L})) \setminus \{e_{\mathbf{0}}\}$。奇偶校验码这一术语源于这样一个事实： $|a|_{\mathbf{0}}$ 是 a的基数，将其视为 L的子集，并对 2 取模；因此，奇偶校验码就是所有偶数大小子集构成的族。

其次，从 $\mathcal{L}$ 中去掉上界 $\mathbf{1}$ 会得到一个交半格；反过来，对于任意有限交半格 $\mathcal{S}$，通过添加上界 $\mathbf{1}$ 得到的 $\mathcal{S}^{\mathbf{1}}$ 是一个格。于是，我们可以将$V(\mathcal{L})$构造推广到有限交半格。事实上，设 $\mathcal{L} = \mathcal{S}^{\mathbf{1}}$ 并且

$$V(\mathcal{S}) = P_{\mathbf{1}}(\mathcal{S}^{\mathbf{1}}) = \{x \in V(\mathcal{S}^{\mathbf{1}}) : |x|_{\mathbf{1}} = 0\}.$$

定理 *2.12*。设 $\mathcal{S}$ 是一个有限交半格。设 $a^{\mathbf{1}}$ 是 $V(\mathcal{S}^{\mathbf{1}})$的唯一原子，满足$\bigvee a^{\mathbf{1}} = \mathbf{1}$。那么， $V(\mathcal{S}) = (\mathbf{F}_2\mathcal{S}, \vee, \wedge, \mathbf{1}_{V(\mathcal{S}^{\mathbf{1}})}, \mathbf{0}_{V(\mathcal{S}^{\mathbf{1}})})$，其中 $\mathbf{1}_{V(\mathcal{S}^{\mathbf{1}})} = e_{\mathbf{1}} + a^{\mathbf{1}}$ 且 $\mathbf{0}_{V(\mathcal{S}^{\mathbf{1}})} = 0$ 为空和，是以 $\mathsf{A}(V(\mathcal{S}^{\mathbf{1}})) \setminus \{a^{\mathbf{1}}\}$为原子集的布尔代数。

证明。 我们只需证明 $V(\mathcal{S})$ 的元素集合是 $\mathbf{F}_2\mathcal{S}$。设 $x \in V(\mathcal{S}^{\mathbf{1}})$。若 $\mathbf{1} \notin x$，则根据推论 2.8 有$xa^{\mathbf{1}} = 0$ ；反之，若 $\mathbf{1} \in x$，则 $\mathbf{1} \in xa^{\mathbf{1}}$ ，因而 $xa^{\mathbf{1}} = a^{\mathbf{1}}$。由此可得，$|x|_{\mathbf{1}} = 0$ 当且仅当 $\mathbf{1} \notin x$，即 x 是由 $\mathcal{S}$ 中的项构成的形式和。 □

举例来说，并为下一节作铺垫，半格 $\mathcal{S} = \{C_3, C_5, C_{15}\}$ 的 $V(\mathcal{S}^{\mathbf{1}})$ 如图 3 所示，其中还展示了奇偶校验码 $P_{\mathbf{0}}(\mathcal{L})$ 和布尔代数 $V(\mathcal{S})$。

3 由 C 与$\mathbb{F}_2$生成的半环

本节中，我们考虑“模 2 计算的置换”。一个置换是若干圈之和，其中 $C_d = d \to d-1 \to \cdots \to 1 \to d$ 是长度为 d 的**圈**，对所有 $d \geq 1$ 均如此。因此，设 C 为圈的集合，并考虑 $S = \mathbf{F}_2 C$。

3.1 基本性质

显然， S 是一个环，其乘法单位元为 C_1。在 S 中，我们有 [5, 命题 3]

$$C_m C_n = \gcd(m,n) C_{\mathrm{lcm}(m,n)} = \begin{cases} C_{\mathrm{lcm}(m,n)} & \text{if at least one of } m \text{ and } n \text{ is odd,} \\ 0 & \text{else.} \end{cases}$$

我们先汇集一些关于 S结构的基本事实。记号：对于正整数n ，我们记 $d(n) = \max\{m\colon 2^m \mid n\}$。若 $d(n) = m$，则 $C_n = C_{2^m} C_{n'}$ ，其中 $n = 2^m n'$ ，且 n' 是奇正整数。

Let

$$S_0 = \left\{ \sum_{k \text{ odd}} \alpha_k C_k \in S : \alpha_k \in \{0,1\},\ \text{finite number of nonzero } \alpha_k \right\},$$

表示 S 中所有循环长度均为奇数的元素所构成的集合。

于是，任意元素 $s \in S$ 都可以唯一地写成

$$s = \sum_{i \in \mathbb{N}} s_i C_{2^i},$$

其中，对于所有 i ，均有 $s_i \in S_0$ （且非零的 s_i只有有限多个）。我们还将 S 中仅含偶数长度循环的元素记作

$$S_+ = \left\{ \sum_{i \in \mathbb{N}} s_i C_{2^i} \in S : s_0 = 0 \right\}.$$

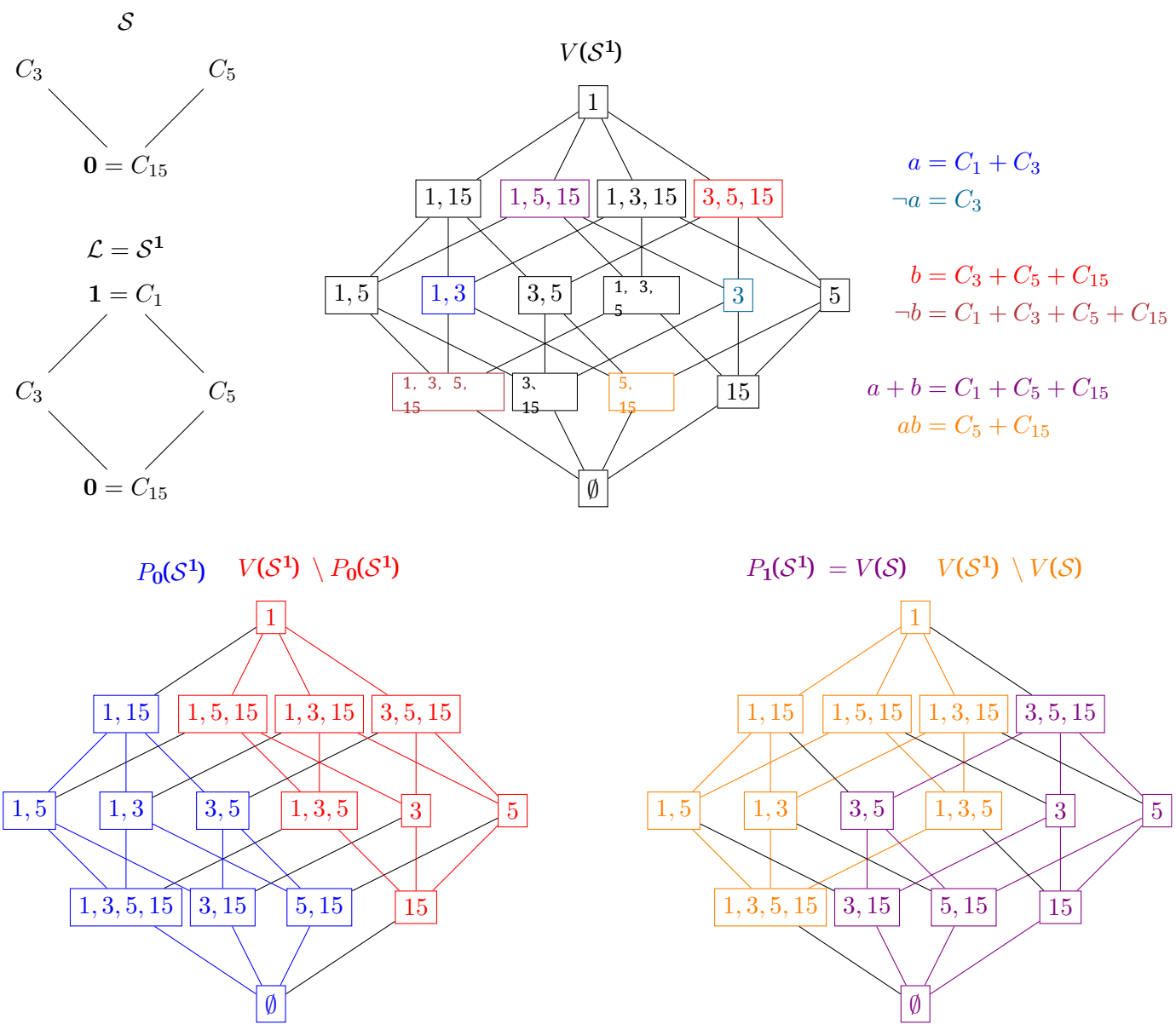


图 3：布尔代数 $V(\mathcal{S}^1)$，其对应的奇偶校验码 $P_0(\mathcal{S}^1)$ 和布尔代数 $V(\mathcal{S})$。

我们注意到， S_+ 是由 C_2、C_4、C_8、.....生成的乘法理想。因此，任意元素 $s \in S$都可以唯一地写成 $s = s_0 + s_+$，其中 $s_0 \in S_0$ 且 $s_+ \in S_+$。容易看出，对于所有 s， $t \in S$

$$s_+ t_+ = 0, \quad s^2 = s_0^2 = s_0, \quad s_+ = s + s^2.$$

下一个引理记录了由这些简单观察得出的若干事实。

引理 3.1. 设 x， $y \in S$。

1. x 是幂等元，当且仅当 x 是奇数长度循环的和。

2. 若 $x \neq 0$，则存在 $k \geq 1$，使得 x 可以唯一地写成 $x = \sum_{i=0}^{k} x_i C_{2^i}$，其中每个 x_i 都是幂等元，且 $x_k \neq 0$。

3. 对于 $x = \sum_{i=0}^{k} x_i C_{2^i}$，有 $x^2 = x_0$。因此，对于任意 $x \in S$，有 $x^4 = x^2$。

4. 对于 $x = \sum_i x_i C_{2^i}$ 和 $y = \sum_i y_i C_{2^i}$，我们有 $xy = z = \sum_i z_i C_{2^i}$，其中 $z_0 = x_0 y_0$ 和 $z_i = x_0 y_i + x_i y_0$ 对所有 $i \geq 1$都成立。

5. x 是单位元，当且仅当 $x_0 = C_1$ （此时 $x^2 = C_1$）。

6. $x_0 \leq y_0$ 当且仅当 $x_0 + 1 \geq y_0 + 1$。

证明。 1. 首先，假设 x 仅是奇数长度循环的和，例如 $x = C_{i_1} + \cdots + C_{i_k}$，其中每个 i_j 都是奇数。由于我们处于特征 2 的情形，因此有：

$$x^2 = (C_{i_1} + \cdots + C_{i_k})^2 = C_{i_1}^2 + \cdots + C_{i_k}^2 = C_{i_1} + \cdots + C_{i_k}.$$

接下来，对于任意元素 $x \in S$，我们可以写成 $x = x_0 + x_+$，其中 x_0 仅是奇圈的和，而 x_+ 仅是偶数长度循环的和。由于任意两个偶数长度循环的乘积为 0，因此可得 $(x_+)^2 = 0$，从而 $x^2 = (x_0)^2 + (x_+)^2 = x_0 + 0 = x_0$。因此， x 是幂等元，当且仅当 x 仅是奇数长度循环的和。

2. 根据 S 的定义，我们有 x 可以唯一地写成$x = C_{i_1} + C_{i_2} + \cdots + C_{i_t}$，其中$1 \leq i_1 < i_2 < \cdots < i_t$。令 $M = \{d(i_1) \ldots, d(i_t)\}$，其中对于每个 $1 \leq j \leq t$，回忆一下， $d(i_j)$表示整除 i_j的最大 2 的幂。对于 $m \in M$，令 $I_m = \{s : d(i_s) = m\}$，并注意，对于每个 $s \in I_m$，可写成 $i_s = 2^m i'_s$，其中 i'_s 为奇数。于是，我们可以将这个唯一表达式中的各项重新排列如下：

$$x = \sum_{m \in M} \sum_{s \in I_m} C_{i_s} = \sum_{m \in M} \sum_{s \in I_m} C_{2^m} C_{i'_s} = \sum_{m \in M} C_{2^m} \sum_{s \in I_m} C_{i'_s}.$$

令$x_m = \sum_{s \in I_m} C_{i'_s}$， 显然每个 x_m 都只是奇数长度循环的和，因此根据第 (1) 部分，它是一个幂等元。加入系数为 0 的项，即可得到所需的形式。

3. 正如第 1 部分的证明中所指出的，若 $x = x_0 + x_+$，其中 x_0 只是奇数长度循环的和，而 x_+ 只是偶数长度循环的和，则 $x^2 = x_0$。因此， $x^4 = (x^2)^2 = (x_0)^2 = x_0 = x^2$。

4. 我们有 $z = (x_0 + \sum_{i \geq 1} x_i C_{2^i})(y_0 + \sum_{j \geq 1} y_j C_{2^j})$。由于 $C_{2^i} C_{2^j} = 0$ 当 $i, j > 0$ 时，我们得到 $z = x_0 y_0 + \sum_{i \geq 1} x_i y_0 C_{2^i} + \sum_{j \geq 1} x_0 y_j C_{2^j}$。

5. 假设 x 是一个单位元。那么对于某个 y， $xy = C_1$，并且根据第 (4) 部分， $x_0 y_0 = C_1$。因此，$x_0 = x_0 x_0 y_0 = x_0 y_0 = C_1$。反过来，若 $x_0 = C_1$，则 $x^2 = x_0 = C_1$，这说明 x 是单位元。

6. 对于所有 x_0， $y_0 \in S_0$，我们有 $x_0 + 1 \leq y_0 + 1$ 当且仅当 $(x_0 + 1)(y_0 + 1) = x_0 y_0 + x_0 + y_0 + 1 = x_0 + 1$当且仅当 $x_0 y_0 + y_0 = 0$ 当且仅当 $x_0 y_0 = y_0$ 当且仅当 $x_0 \geq y_0$。

□

3.2 幂等元的布尔代数

W首先注意， S_0 的幂等元构成一个无限布尔代数 ra.

引理 3.2。 $E(S) = S_0$ 中的幂等元构成一个无原子布尔代数，其中对于 $e, f \in E(S)$，有 $e \wedge f = ef$, $e \vee f = e + f + ef$和 $\neg e = C_1 + e$。

证明。 由于 S 是交换的，幂等元的乘积显然也是幂等元。此外，由于 S 的特征为 2，幂等元的和也显然是幂等元。因此，$E(S)$ 是 S的子环，并且显然 $E(S)$ 是一个布尔环。众所周知， [11, 第 2] 章指出，任何布尔环都可以根据给定的运算视为一个布尔代数。

下面证明它是无原子的。设 $s \in E(S)$ 是一个非零元素，记作 $s = \sum_i \alpha_i C_i$ ，并设 p是一个素数，它不整除 s中的任何圈长。则 $t = sC_p = \sum_i \alpha_i C_{ip}$ 满足$t \notin \{0, s\}$ 和 $t \leq s$ （即 $ts = t$），因此 s 不是原子。 □

注 3.3。 可数无限的无原子布尔代数在同构意义下是唯一的，例如有理数集的区间代数 *[11, Chapter 16]*。因此，$(E(S)\ \wedge, \vee, \neg)$ 同构于该区间代数。

在 S_0 中作除法。 利用 S_0的布尔代数结构，我们可以轻松求解方程$ax = b$，其中 $a, b \in S_0$ 只有奇数循环长度。注意，若 $ax = b$ 满足 $a, b \in S_0$，则必然也有$x \in S_0$ （除非 $a = b = 0$，此时任意 $x \in S$ 都是解）。

我们需要任意布尔代数 $\mathcal{V}$ 的一般除法公式（见第 4 节，特别是定理 4.1 和定理 4.2）。我们指出，在任意布尔代数中， $a \geq b$等价于$b \leq a + b + \mathbf{1}_{\mathcal{V}}$；因此，区间 $[b, a + b + \mathbf{1}_{\mathcal{V}}]$ 非空当且仅当 $ab = b$。

命题 3.4。 设 $\mathcal{V}$ 是一个布尔代数，且 $a, b \in \mathcal{V}$。那么， $ax = b$ 的解是 $\mathcal{V}$中的区间 $[b, a + b + \mathbf{1}_{\mathcal{V}}]$。

证明。 存在 x 使得 $ax = b$，当且仅当 $ab = b$ （因为 $ax = b$ 蕴含 $b = ax = aax = ab$）。因此假设 $ab = b$。若 $ax = b$，则通过与上文类似的论证可得 $xb = b$。因此，$x \geq b$且 $x(b + a + \mathbf{1}_{\mathcal{V}}) = b + b + x = x$，故 $x \leq a + b + \mathbf{1}_{\mathcal{V}}$。反过来，若 $b \leq x \leq a + b + \mathbf{1}_{\mathcal{V}}$，则 $(a + b + \mathbf{1}_{\mathcal{V}})x = x$ 且 $bx = b$，于是

$$ax = ax + bx + x + bx + x = (a + b + \mathbf{1}_{\mathcal{V}})x + bx + x = b.$$

□

有限情形。 现在我们关注由整除给定长度的奇圈生成的有限格。设 k 是一个奇正整数，并令 $D(k)$ 表示 k的因子集。因此，我们考虑格 $\mathcal{C}_k = \{C_i : i \mid k\}$，其交运算为 $C_i C_j = C_{\mathrm{lcm}(i,j)}$。例如，格 $\mathcal{C}_{15}$ 如图 3 所示。 S 中循环长度整除 k 的元素构成格 $V(\mathcal{C}_k)$。定理 2.6 给出了其原子的抽象表达；然而，正如下文所示，我们可以给出更明确的表达。

格 $\mathcal{C}_k$与格 $\mathcal{L} = (L = D(k)\ \vee =$最大公因数 $\wedge =$最小公倍数 $\mathbf{0} = k$、$\mathbf{1} = 1)$ 同构。回忆一下，对于元素 $j \in L$， j^c 表示被 j覆盖的 L 的元素集合。在格 $\mathcal{L}$中，对于任意 $j \in D(k)$，我们将 $m(j) = \bigwedge j^c$记作。例如，对于 $k = 45$， $j = 3$ 覆盖 9 和 15，因此 $j^c = \{9, 15\}$和 $m(j) =$最小公倍数(9、15) $= 45$（见下文例 3.7）。我们注意到，区间$[m(j)\ j] = \{l : j \mid l$ 和 $l \mid m(j)\}$ 永远不会为空。现在，对于任意 $j \in D(k)$，令 $T_j \in \mathcal{C}_k$ 定义为

$$T_j = \sum_{l \in [m(j), j]} C_l.$$

定理 3.5. $V(\mathcal{C}_k)$ 的原子集合为 $\{T_j : j \in D(k)\}$。特别地，对于所有 $i \in D(k)$，

$$C_i = \sum_{j \in D(k) : i \mid j} T_j.$$

证明。由于 T_j 均非零，引理 2.7 表明我们只需证明 $C_iT_j \in \{T_j, 0\}$对所有 $i, j \in D(k)$ 成立。我们有 $T_j = \sum_{l\in[m(j)\ j]} C_l$。首先，若 i 整除 j，则 i 整除 $[m(j)\ j]$ 中的任意 l，因此 $C_iC_l = C_l$ 且 $C_iT_j = T_j$。以下我们假设 i 不整除 j。

假设 k 分解为 $k = \prod_{p\in P} p^{k_p}$，其中 P 是 k的素因子集；为方便记号，我们将其视为向量 $k = (k_p : p \in P)$，更一般地，将元素 $t \in D(k)$写作 $t = (t_p : p \in P)$，其中 $0 \le t_p \le k_p$。

于是，设 $j = (j_p : p \in P)$ 和 $i = (j_p : p \in P)$，其中 $0 \le j_p \le k_p$ 且 $0 \le i_p \le k_p$。令 $\Sigma = \{p \in P : i_p > j_p\}$。由于 i 不整除 j，因此有 $|\Sigma| > 0$。令 $\Theta = \{p : j_p = k_p\}$ 且 $\Gamma = P \setminus \Theta$。另请注意，$\Sigma \subseteq \Gamma$。写作 $m(j) = (m_p : p \in P)$，对于每个 $p \in P$，我们都有

$$m_p = \min\{j_p + 1, k_p\} = \begin{cases} j_p & \text{if } p \in \Theta \\ j_p + 1 & \text{if } p \in \Gamma. \end{cases}$$

设 $l \in [m(j)\ j]$，使得对于所有 $p \in \Gamma$，$l_p = j_p + l(\epsilon)_p$，且 $l(\epsilon)_p \in \{0, 1\}$。于是，写作 $q =$最小公倍数$(l,\ i) = (q_p : p \in P)$，我们有

$$q_p = \max\{i_p, l_p\} = \begin{cases} i_p & \text{if } p \in \Sigma \\ l_p = j_p + l(\epsilon)_p & \text{if } p \in \Gamma \setminus \Sigma \\ j_p & \text{if } p \in \Theta. \end{cases}$$

现在令 Q 表示 $D(k)$ 的子集，它由满足以下条件的元素 $(q_p : p \in P)$ 构成：对于所有 $p \in \Sigma$，都有 $q_p = i_p$，并且对于所有 $p \in \Theta$，都有 $q_p = j_p$。那么，对于给定的 $q \in Q$，我们看到

$$A_q := \{l \in [m(j), j] : \operatorname{lcm}(l, i) = q\} = \{l \in [m(j), j] : l(\epsilon)_{\Gamma\setminus\Sigma} = (q - j)_{\Gamma\setminus\Sigma}\}$$

因此 $|A| = 2^{|\Sigma|} \ge 2$。综合以上结果，我们得到

$$C_iT_j = \sum_{l\in[m(j),j]} C_iC_l = \sum_{l\in[m(j),j]} C_{\operatorname{lcm}(l,i)} = \sum_{q\in Q}\sum_{l\in A_q} C_q = 0.$$

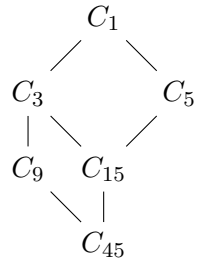
因此，

$$C_i = \sum_{j\in D(k)} C_iT_j = \sum_{j\in D(k):i \mid j} T_j.$$

□

推论 3.6. 对于所有 i，$C_i = \sum_{j:i \mid j} T_j$。

例 3.7. 对于 $k = 45$，格 $\mathcal{C}_{45}$ 以及 V 的原子$(\mathcal{C}_{45})$ 如下所示。



$$\begin{aligned} T_1 &= C_1 + C_3 + C_5 + C_{15} & C_1 &= T_1 + T_3 + T_5 + T_9 + T_{15} + T_{45} \\ T_3 &= C_3 + C_9 + C_{15} + C_{45} & C_3 &= T_3 + T_9 + T_{15} + T_{45} \\ T_5 &= C_5 + C_{15} & C_5 &= T_5 + T_{15} + T_{45} \\ T_9 &= C_9 + C_{45} & C_9 &= T_9 + T_{45} \\ T_{15} &= C_{15} + C_{45} & C_{15} &= T_{15} + T_{45} \\ T_{45} &= C_{45}. & C_{45} &= T_{45}. \end{aligned}$$

3.3 在 S中作除法

现在我们考虑 $ax = b$ 在 S中的除法方程。首先值得注意的是，一般来说，解的数量可能是无限的，例如，对任意 $x \in S_+$，$C_2x = 0$ 都成立。即使只考虑奇数长度，情况也是如此：$(C_3 + C_5)\ x = 0$ 例如对任意 $x \in SC_{15}$都成立。不过，我们可以要求解的大小有界。事实上，我们将在下文证明，如果存在一个解，那么它总是包含一个没有任何“伪影”的解，也就是说，其中的循环长度都是该解自然预期会有的。

对于所有 $a \in S$，令 Q_a 表示出现在 a中的循环长度集合，因此 $a = \sum_{q \in Q_a} C_q$。回想一下，对于任意 q，$q = q' 2^{d(q)}$；然后令 $K(a) =$ 最小公倍数$(q' : q \in Q_a)$，并令 $N(a) =$ 最大值$(d(q) : q \in Q_a)$。例如，如果 $a = (C_1 + C_5) + C_7 C_2 + C_5 C_8$，那么我们有 $K(a) =$最小公倍数$(1, 5, 7, 5) = 35$，并且 $N(a) = \log_2 8 = 3$。

现在，对任意 $a = \sum_{q \in Q_a} C_q$ 和 n， $k \in$ 自然数集，令 a_{-n} 表示从 a 中去掉长度可被 2^{q+1} 整除的所有圈 C_q 后得到的元素，并令 $a_{| k}$ 表示从 a 中去掉长度不能被 k整除的所有圈 C_q 后得到的元素。因此

$$a_{-n} = \sum_{q \in Q_a : d(q) \le n} C_q = \sum_{i \le n} a_i C_{2^i},$$
$$a_{| k} = \sum_{q \in Q_a : q \mid k} C_q.$$

注意到 $(a_{-n})_{| k} = (a_{| k})_{-n}$。

命题 3.8。 设 $a, b, x \in S$ 和 $n, k \in$ 自然数集 满足 $\max(N(a)\ N(b)) \le n$ 且 $\mathrm{lcm}(K(a)\ K(b)) \mid k$。那么 $ax = b$ 当且仅当 $a(x_{-n})_{| k} = b$。

证明。 首先注意到，根据假设， $a = (a_{-n})_{| k}$ 和 $b = (b_{-n})_{| k}$。现在，设 x 是 $ax = b$的一个解。映射 $s \mapsto s_{-n}$ 和 $s \mapsto s_{| k}$ 是定义在 S的乘法半群上的半群同态，也就是说：对所有 s， $t \in S$，都有 $((st)_{-n})_{| k} = (s_{-n})_{| k} (t_{-n})_{| k}$。特别地，

$$a(x_{-n})_{| k} = (a_{-n})_{| k} (x_{-n})_{| k} = ((ax)_{-n})_{| k} = (b_{-n})_{| k} = b.$$

□

现在我们给出方程 $ax = b$ in S 的解集的主要刻画。

定理 3.9。 设 $a, b, x \in S$。对所有 $i \in$ 自然数集，令 $l_i = b_i + a_0 b_i + a_i b_0$ *and* $u_i = l_i + a_i + 1$ *and*，并令

$$\lambda_0 = \bigvee_{i \in \mathbb{N}} l_i \in S_0,$$
$$\upsilon_0 = \bigwedge_{i \in \mathbb{N}} u_i \in S_0.$$

对所有 $i \ge 1$，令

$$\lambda_i = a_0 b_i + a_i b_0,$$
$$\upsilon_i = a_0 b_i + a_i b_0 + a_0 + 1.$$

那么，对于所有 $i \in$ 自然数集， $ax = b$ 当且仅当 $x_i \in [\lambda_i, \upsilon_i]$。此外，集合 $\{x \in S : ax = b\}$ 非空当且仅当 $\lambda_0 \le \upsilon_0$。

定理 3.9 的证明基于以下引理。

引理 3.10。 对于任意 $a, b, x \in S$， $ax = b$ 当且仅当以下方程组成立：

$$a_0 x_0 = b_0 \tag{4}$$
$$a_i x_0 = b_i + b_i a_0 + a_i b_0 \ \textit{for all}\ i \ge 1 \tag{5}$$
$$a_0 (x_i + b_i) = a_i b_0 \ \textit{for all}\ i \ge 1. \tag{6}$$

证明。 首先，假设 x 满足方程 (4)、(5) 和 (6)，并令 $c = ax$。由方程 (4) 可得 $c_0 = a_0 x_0 = b_0$，由方程 (5) 和 (6) 可知，对于所有 $i \ge 1$,

$$c_i = a_0 x_i + a_i x_0 = (a_i b_0 + a_0 b_i) + (b_i + b_i a_0 + a_i b_0) = b_i.$$

因此 $c = b$。

反过来，假设 $ax = b$。于是我们有 $b_0 = a_0 x_0$，得到方程 (4)，并且对所有 $i \geq 1$，$b_i = a_i x_0 + a_0 x_i$。由于 $a_0^2 = a_0$ 和 $a_0 x_0 = b_0$，后者意味着 $a_0 x_i = a_0 b_i + a_i b_0$，从而得到 $a_0(x_i + b_i) = a_i b_0$，对所有 $i \geq 1$ 均成立，这就是方程 (6)。因此，

$$a_i x_0 = b_i + a_0 x_i = b_i + a_0 b_i + a_i b_0,$$

这就是方程（5），证毕。 □

定理 *3.9* 的证明。引理 3.10 中的三个（方程）方程组可以利用命题 3.4 求解：我们得到

$$x_0 \in [b_0, a_0 + b_0 + 1] \tag{7}$$
$$x_0 \in [b_i + b_i a_0 + a_i b_0, b_i + b_i a_0 + a_i b_0 + a_i + 1] \text{ for all } i \geq 1 \tag{8}$$
$$x_i + b_i \in [a_i b_0, a_i b_0 + a_0 + 1] \text{ for all } i \geq 1. \tag{9}$$

注意到对于所有 $i \geq 0$，$l_i = b_i + a_0 b_i + a_i b_0$ 和 $u_i = l_i + a_i + 1$，我们得到

$$x_0 \in [l_i, u_i] \ \forall i \geq 0$$
$$x_i + b_i \in [a_i b_0, a_i b_0 + a_0 + 1] \ \forall i \geq 1.$$

第一个方程组等价于 $x_0 \in [\lambda_0, \upsilon_0]$。第二个方程组等价于方程（6），而方程（6）又等价于 $a_0 x_i = a_0 b_i + a_i b_0$；根据命题 3.4，这等价于 $x_i \in [a_0 b_i + a_i b_0, a_0 b_i + a_i b_0 + a_0 + 1] = [\lambda_i, \upsilon_i]$。

最后，如果 $\lambda_0 \not\leq \upsilon_0$，那么解集为空。否则，对于所有 $i \in \in$自然数集，我们有 $l_i \leq u_i$（因此第一个方程组有解）；此外，由于我们有 $l_0 \leq u_0$，故有 $b_0 \leq b_0 + a_0 + 1$，且等价地有 $b_0 \leq a_0$，所以 $a_i b_0 \leq a_0$（因此第二个方程组有解）。 □

我们指出，判断 $ax = b$ 是否有解，可以通过计算 λ_0、υ_0并验证 $\lambda_0 \upsilon_0 = \lambda_0$来完成。这需要 $\Theta(n)$次和与积，其中 $n = \max\{N(a)\ N(b)\}$满足 $n \leq \log \max\{|a|, |b|\}$。

方程 $az = 0$。特别地，方程 $az = 0$ 的解可以简洁地刻画。对每个满足 $x = \sum_{i=0}^{k} x_i C_{2^i}$ 的 $x \in S$，其中每个 x_i 都是幂等元，定义

$$x^+ = \bigvee_{i=0}^{k} x_i \in S_0.$$

由此可见，　　定义显然可知，对所有 $x \in S$ 和所有 $e \in S_0$，$e^+ = e$、$x^+ x = x$以及 $ex^+ = (ex)^+$。

推论 3.11。设 a、$z \in S$。那么 $az = 0$ 当且仅当 $z_0 a^+ = a_0 z^+ = 0$，或者等价地，$z_0 \leq a^+ + 1$且 $a_0 \leq z^+ + 1$。

证明。根据引理 3.10，$az = 0$ 当且仅当以下方程组成立：

$$a_0 z_0 = 0 \tag{10}$$
$$a_i z_0 = 0 \text{ for all } i \geq 1 \tag{11}$$
$$a_0 z_i = 0 \text{ for all } i \geq 1. \tag{12}$$

方程（10）和（11）等价于单个方程 $a^+ z_0 = 0$，换言之，也就是 $z_0 \leq a^+ + 1$。类似地，方程（10）和（12）等价于 $a_0 \leq z^+ + 1$。 □

3.4 扩展的格林关系

接下来我们考察 S 的乘法结构。由于（S，$\cdot$）是一个交换半群，因此所有格林关系 [16] 都重合，即 $\mathcal{R}=\mathcal{L}=\mathcal{H}=\mathcal{D}=\mathcal{J}$。在下文中，我们将这一关系称为 $\mathcal{R}$；回顾一下，对于 a，$b\in S$，当且仅当由 a 生成的主（右）理想等于由 b 生成的主（右）理想时，有 $a\mathcal{R}b$。下一个命题给出了这一关系以及扩展格林关系 $\mathcal{R}^*$ 和 $\mathcal{R}$ 的一个简单刻画。回顾一下，对于幺半群 M 及其元素 a，$b\in M$，若对所有 x，$y\in M$ $xa=ya$，当且仅当 $xb=yb$ 时有 $a\mathcal{R}^*b$；并且若对所有幂等元 e，当且仅当 $eb=b$ 时有 $ea=a$。

P命题 3.12. 设 $a,b\in S$。则在 S 的乘法半群中，我们有：

1. $a\mathcal{R}b$ 当且仅当存在某个单位元 g 使得 $b=ag$；
2. $a\mathcal{R}^*b$ 当且仅当 $a^+=b^+$ 且 $a_0=b_0$;
3. $a\tilde{\mathcal{R}}b$ 当且仅当 $a^+=b^+$。

证明. 1. 令 G 表示 S 的单位群。由引理 3.1 的第 (4) 部分，$G=\{g\in S:\ g_0=C_1\}$。显然，若对某个 a，$b\in S$，有 $a=bg$，则 $g\in G$，且 $a\mathcal{R}b$。现在设 $a\mathcal{R}b$，即对于某个 $x,y\in S$，有 $ax=b$ 且 $by=a$。

于是我们有 $a_0x_0=b_0$ 和 $b_0y_0=a_0$，从而得到 $b_0\le a_0$ 和 $a_0\le b_0$，因此 $a_0=b_0$。特别地，$a_0x_0=a_0y_0=a_0$。此外，由于 $a=by=axy$，按照第 3.1 小节中的记号，我们有

$$a_+=(axy)_+=a_0x_0y_++a_0x_+y_0+a_+x_0y_0=a_0y_++a_0x_++a_+x_0y_0.$$

特别是，

$$a_+x_0=a_0x_0y_++a_0x_0x_++a_+x_0y_0=a_0y_++a_0x_++a_+x_0y_0=a_+,$$

因此 $ax_0=a$。现在考虑 $g=C_1+x_+\in G$。我们有

$$ag=a(x_0+C_1+x)=ax=b,$$

如所需。

2. 由于 S 是一个环，我们有 $a\mathcal{R}^*b$ 属于 S 的乘法半群，当且仅当对所有 $z\in S$，$az=0$ 当且仅当 $bz=0$。若 $a_0=b_0$ 且 $a^+=b^+$，则推论 3.11 立即表明 $a\mathcal{R}^*b$。反过来，若 $a^+\neq b^+$，则存在 $z_0\in(a^++1)^{\downarrow}\Delta(b^++1)^{\downarrow}$，设为 $z_0\le a^++1$，但 $z_0\not\le b^++1$。根据假设，我们有 $(z_0)^+=z_0\le a^++1$，因此（由引理 3.1）也有 $(z_0)^++1\ge a^+\ge a_0$。由此可得推论 3.11 表明 $az_0=0$，而 $bz_0\neq 0$。

3. 容易验证，对于任意幂等元 e，以下条件等价：e 固定 a；对所有 $i\in\mathbb{N}$，$ea_i=a_i$；对所有 i，$e\ge a_i$；$e\ge\bigvee_i a_i=a^+$。因此，当且仅当 $(a^+)^{\uparrow}=(b^+)^{\uparrow}$ 属于布尔代数 S_0 时，$a\tilde{\mathcal{R}}b$ 成立；换言之，$a^+=b^+$。

□

接下来，我们刻画幂等元的 $\{\mathcal{R},\mathcal{R}^*,\tilde{\mathcal{R}}\}$-类。

推论 3.13. 设 G 是 S 的单位群，且 $e\in S_0$ 是幂等元。

1. e 的 $\mathcal{R}$-类是群 eG。2. e 的 $\mathcal{R}^*$-类也是群 eG。
3. e 的 $\tilde{\mathcal{R}}$-类是集合 $\{a\in S:\ a^+=e\}\subseteq eS$。

证明。 1. 这直接由命题 3.12 得出。

2. 假设 $a\mathcal{R}^*e$。根据命题 3.12，我们有 $a^+=e$ 和 $a_0=e$，或者等价地，对所有 $i\ge 1$，有 $a_0=e$ 和$a_ie=a_i$。我们得到 $a=eg$，其中对所有 $i\ge 1$，有 $g_0=C_1$ 和 $g_i=a_i$。

3. 当且仅当 $a^+ = e$时，我们有 $a\tilde{R}e$。由于 $a^+a = a$，这意味着 $a = ea$。注意，对于任意幂等元 $e \in S$，理想 eS 是由 e固定的元素集合。

□

回顾一下，若交换半群 T 满足以下条件，就称其为**限制半群**：(1) 对任意$a \in T$， a 都与某个（唯一的）幂等元 a^+ $\tilde{\mathcal{R}}$-相关；(2) 对任意元素 a 以及 T 中的任意幂等元 e，都有 $ae =$(ae)^+a。关于限制半群的更多内容，读者可参阅论文[13, 18] 以及 Gould 在 [12]中的笔记。

命题 3.14。 S 的乘法半群相对于 a^+、˜构成一个限制半群，其中 $\mathcal{R} \subsetneq \mathcal{R}^* \subsetneq \mathcal{R}$。

证明。 </style}显然， S 满足第一个条件：对于 $x \in S$，与 x相关的唯一幂等元是 x^+。对于第二个条件，我们有$(ae)^+ = ea^+$ （如前所示），并且$(ae)^+a = ea^+a = ea$。

现在我们给出例子来说明这两个真包含。首先，若 $a = C_1$ 且 $b = C_2$，则有 $a^+ = b^+ = C_1$，但 $a_0 \neq b_0$，因此 $a\tilde{\mathcal{R}}b$ 成立而 $a\mathcal{R}^*b$不成立。其次，设 $a = C_3 + C_5C_2$ 且$b = C_3 + C_5C_4$。显然 $a\mathcal{R}^*b$; 下面证明 a 和 b 不 $\mathcal{R}$-相关。为导出矛盾，假设对某个单位元 g有 $a = bg$。我们有

$$C_5 = a_1 = b_1g_0 + b_0g_1 = C_3g_1,$$

因此 $C_5 \leq C_3$，从而 $C_3C_5 = C_5$。然而， $C_3C_5 = C_{15}$，这就得到了所需的矛盾。 □

3.5 S 的特殊元素

我们已经刻画了 S 的幂等元。本小节中，我们将刻画 S 的单位群、正则元（以及所有子群），以及所谓的 S 的余正则元素。

若元素 $a \in S$ 是（乘法意义下）**可消去的**，则 $ax = ay$ 蕴含 $x = y$。

定理 3.15 （ S 的可消去元素分类）。 以下各条件对 $g \in S$ 等价：

1. 方程 $gx = 0$ 有有限多个解 $x \in S$；

2. $x = 0$ 是 $gx = 0$的唯一解；

3. g 是可消去的；

4. g 是单位元；*5.* $g_0 = 1$；*6.* 对某个 $a \in S$， $g = a^2 + a + 1$；

7. $g^2 = 1$。

证明。 第 2 项与第 3 项等价，这是因为 S 是一个环（因为 $ax = ay$ 当且仅当 $a(x - y) = 0$）。对于第 3 项与第 4 项的等价性，注意到 g 是可消去的当且仅当 $g\mathcal{R}^*1$；根据命题 3.12，这当且仅当 g 属于单位群。我们已在引理 3.1 中证明了第 4、5、7 项等价。要证明第 6 项与第 5 项等价，先注意若 $g = a^2 + a + 1$，则 $g_0 = g^2 = a^4 + a^2 + 1 = 1$。反之，若 $g_0 = 1$，则 $g = 0^2 + 0 + 1$。由第 2 项推出第 1 项显然成立。

为完成证明，我们证明 1 蕴含 5。设方程 $gx = 0$ 有有限多个解，并反设 $g = \sum_i = 1^t g_iC_{2^i}$，其中 $g_0 \neq 1$。对于每个 $x^{(k)} =$ (g0 + 1)$C_{2^k} \in S_+$，其中 $k \geq 1$，回忆 $s_+t_+ = 0$ 对所有 s， $t \in S$ 成立，我们有

$$gx^{(k)} = (g_0 + g_+)(g_0 + 1)C_{2^k} = g_0(g_0 + 1)C_{2^k} + 0 = (g_0 + g_0)C_{2^k} = 0,$$

这与 $ax = 0$ 的解只有有限多个相矛盾。

□

由 $G = C_1 + S_+$ 给出的单位群与 $(\mathbf{F}_2^{\mathbb{N}}, +)$ 同构：对于所有 $g, g' \in G$，我们有 $(gg')_0 = C_1$，并且对于所有 $i \geq 1$,

$$(gg')_i = g_0 g'_i + g_i g'_0 = g_i + g'_i = (g + g')_i.$$

因此，$(gg') + C_1 = (g + C_1) + (g' + C_1)$。特别地，任何单位元都是对合：$g^2 = 1$。事实上，每个子群（或等价地，每个正则 $\mathcal{H}$-类）都是半群 eG，其中 $e \in S_0$ 是幂等元。于是 $eG = e + eS_+$ 再次满足 $(egeg') + e = (eg + e) + (eg' + e)$；因此，除非 $e = 0$，否则 eG 同构于 $(\mathbf{F}_2^{\mathbb{N}}, +)$；若 $e = 0$，则它是平凡群。

定理 3.16（正则元的分类）。以下关于 $a \in S$ 的命题彼此等价：

1. $a\mathcal{R}a^2$；*2.* 对某个单位元 $g \in G$，$a = a^2 g$；*3.* $a^3 = a$；*4.* 对某个 $s \in S$，$a = s^3$；*5.* $a^+ = a^2$；*6.* a 是正则的；*7.* a 属于某个子群；*8.* 对某个幂等元 $e \in E(S)$，$a\mathcal{R}e$；*9.* $a\mathcal{R}^* a^2$；*10.* 对某个幂等元 $e \in E(S)$，$a\mathcal{R}^* e$。

证明。首先，第 6、7、8 项等价，这是由 S 是交换的这一事实保证的。其次，第 1 项与第 2 项等价，这由命题 3.12 给出。第三，以下推论可由定义直接得出：第 2 项推出第 8 项（注意到 a^2 是幂等元），第 3 项推出第 4 项，而第 4 项又推出第 6 项；第 1 项推出第 9 项，而第 9 项又推出第 10 项。为完成证明，我们证明：第 5 项当且仅当第 3 项；第 8 项推出第 2 项；第 2 项推出第 3 项；第 4 项推出第 3 项；以及第 10 项推出第 7 项。

证明第 5 项推出第 3 项：若 $a^+ = a^2$，则 $a^3 = aa^+ = a$。

证明第 3 项推出第 5 项：若 $a^3 = a$，则令 $b = a^3$；对所有 $i \in$ 自然数集都有 $a_i = b_i = a_i a_0$，或者等价地，$a_0 \geq a^+$（根据定义，$a_0 \leq a^+$）。

证明 8 推出 2：由命题 3.12，若 $a\mathcal{R}e$ 则 $a = eg$ 对某个单位元 $g \in G$成立，则有 $a^2 = a_0 = (eg)_0 = eg_0 = e$，因此 $a^2 g = eg = a$。

证明 2 推出 3：若 $a = a^2 g$ 对某个单位元 g成立，则 $a^3 = a^2 a^2 g = a^4 g = a^2 g = a$。

证明 4 推出 3：若 $a = s^3$，则利用 $s^4 = s^2$这一事实可得，$a^3 = s^9 = s^3 = a$。

证明 10 推出 7：若 $a\mathcal{R}^* e$，则根据推论 3.13，a 属于群 eG。 □

称元素 $h \in S$ 为**余正则**，如果 $h + C_1$ 是正则的。我们首先给出余正则元素的刻画。

命题 3.17 (余正则元素的分类)。对于 $h \in S$，以下条件等价：

1. h 是余正则的，即 $h + C_1$ 是正则的；

2. $h^3 = h^2$；*3.* 对所有 $i \geq 1$，$h_0 h_i = 0$；

4. 对某个 $a \in S$，$h = a^3 + a^2 + a$；

5. 对某个 $b \in S$，$h = b^3 + 1$。

证明。1 和 5 的等价性直接由定理 3.16 得出。

证明 5 蕴含 2：若 $h = b^3 + 1$，则有 $h^2 = b^6 + 1 = b^2 + 1$，并且

$$h^3 = (b^3 + 1)(b^2 + 1) = b^5 + b^3 + b^2 + 1 = b^3 + b^3 + b^2 + 1 = b^2 + 1 = h^2.$$

证明 2 蕴含 1：若 $h^3 = h^2$，则 $(h+1)^3 = h^3 + h^2 + h + 1 = h + 1$，因此 $h+1$ 是正则的。4 与 5 等价，这是因为 $a^3 + a^2 + a = (a+1)^3 + 1$。

对于 2 与 3 的等价关系，注意到方程 $h^3 = h^2$ 等价于 $h_0 h = h_0$，而后者又等价于对所有 $i \geq 1$ 都有 $h_0 h_i = 0$。 □

推论 3.18. 对于任意 $e \in S$， e 是幂等元，当且仅当 e 是正则且余正则的。

接下来我们证明，余正则元素构成了 $\mathcal{R}$-类的一个横截集。

命题 3.19。 S 的每个 $\mathcal{R}$-等价类都包含唯一的余正则元素。具体而言，设 $H : S \to S$ 由 $H(a) = a + a^2 + a^3$给出。则对所有 $a \in S$， $H(a)$ 是 a的 $\mathcal{R}$-等价类中的唯一余正则元素，因此特别地， H 在 $\mathcal{R}$-等价类上为常数。

证明。 对每个 $a \in S$，都有 $H(a) = a(1+a+a^2) = ag_a$，其中 $g_a = 1+a+a^2$ 是一个单位元（由定理 3.15 可知）。因此，由命题 3.12 可得 $H(a)\mathcal{R}a$。由于（根据命题 3.17） $H(a)$ 是余正则的，这就保证了每个 $\mathcal{R}$-等价类中都存在一个余正则元素。

现在假设 $f \in S$ 是余正则的，且与 a关于 $\mathcal{R}$相关。由命题 3.12 及上一段可知，对某个单位元 g，有 $f = H(a)g$。回想一下， $H(a) = ag_a$，其中 g_a 是一个单位元；并且对于所有单位元 h， $h^2 = 1$ （由定理 3.15 可知）。于是我们得到 $f^2 = H(a)^2 g^2 = a^2 g_a^2 g^2 = a^2$ 以及$f^3 = f^2 f = a^2 H(a)g = (a^3 + a^4 + a^5)g = a^3 g + a^2 g + a^3 g = a^2 g$。由于 f是余正则的，命题 3.17 现在给出 $a^2 g = a^2$。再结合 $g_0 = 1$这一事实，便可推出

$$ag = (a_0 + a_+)g = (a^2 + a_+)g = a^2 g + a_+ g = a^2 + a_+ g = a^2 + a_+(1 + g_+) = a^2 + a_+ + 0 = a_0 + a_+ = a,$$

由此我们推得 $g = 1$，进而得到 $f = H(a)$。这保证了 $H(a)$ 是 a 的 $\mathcal{R}$-类中唯一的余正则元素。注意，对所有满足 $a\mathcal{R}b$ 的 b，我们都有 $H(b) = H(a)$。 □

我们得到对 $\mathcal{R}$的另一种刻画。

推论 3.20. 对于任意 a、 $b \in S$、 $a\mathcal{R}b$，当且仅当 $a_0 = b_0 \geq (a+b)^+$。

证明。 若 $a\mathcal{R}b$，则 $a\mathcal{R}^* b$，因而 $a_0 = b_0$。因此，接下来假设 $a, b \in S$ 且 $a_0 = b_0$，并设法证明，对于这样的 $a, b \in S$，有 $a\mathcal{R}b$ 当且仅当 $a_0 \geq (a+b)^+$。

由命题 3.19 以及对所有 $x \in S$ 都有 $x^2 = x_0$ 这一事实可知， $a\mathcal{R}b$ 当且仅当 $a + a_0 + a_0 a = b + b_0 + b_0 b$；或者等价地（因为 $a_0 = b_0$）， $a + a_0 a = b + a_0 b$。这又等价于（与往常一样，在 F_2 上运算）$(a_0 + 1)(a + b) = 0$。根据推论 3.11，后者等价于$a_0 + 1 \leq (a+b)^+ + 1$ 且 $a_0 + b_0 \leq (a_0 + 1)^+$。第二个不等式显然成立，因为$a_0 = b_0$；而根据引理 3.1， $a_0 + 1 \leq (a+b)^+ + 1$ 等价于 $a_0 \geq (a+b)^+$。

□

3.6 单射多项式

在本小节中，我们对 S 上的单变量单射多项式进行分类，结果表明它们也正是 S 上的满射一元多项式。我们将说明，求解形如 $P(x) = e$ 的多项式方程，其中 P 是双射而 $s \in S$ 固定，十分简单。首先，我们指出，由于对所有 $x \in S$ 都有 $x^4 = x^2$，因此可以假设 $P(x)$ 至多为三次；因此，我们考虑 $P(x) = ax^3 + bx^2 + cx + d$。

定理 3.21 .设 $P(x) = ax^3 + bx^2 + cx + d$ 是 $S[x]$ 中的一个多项式。以下命题等价 $t.$

1. P 是单射；
2. P 是满射；
3. $(a_0, b_0, c_0) = (0, 0, 1)$。

此外，如果 P 是双射，那么对于所有 $s \in S$，

$$P(x) = s \quad \Longleftrightarrow \quad x_0 = d_0 + s_0 \quad and \quad x_+ = d_+ + s_+ + (a+b+c)_+(d_0+s_0).$$

证明。首先，假设 $(a_0, b_0, c_0) = (0,0,1)$。元素 $g = (a+b+c)_+ + 1$ 是一个单位元，并且我们有

$$P(x) = ax^3 + bx^2 + cx + d = a_+x_0 + b_+x_0 + c_+x + x + d = gx_0 + x_+ + d.$$

因此，对于任意 $s \in S$，我们有

$$P(x) = s \iff gx_0 + x_+ = d + s,$$

由此得到 $(gx_0 + x_+)_0 = x_0 = d_0 + s_0$ 以及 $(gx_0 + x_+)_+ = g_+(d_0 + s_0) + x_+ = d_+ + s_+$，因此 $x_+ = d_+ + s_+ + (a+b+c)_+(d_0+s_0)$。（特别地，$P$ 是双射。）

证明的其余部分旨在证明，单射或满射多项式 P 具有 $(a_0, b_0, c_0) = (0,0,1)$。显然，常数项 d 对单射性或满射性没有影响，因此我们从此假设 $d = 0$。

首先，假设 $P = ax^3 + bx^2 + c$ 是单射，目标是证明 $(a_0, b_0, c_0) = (0, 0, 1)$。反设 $(a_0, c_0) \neq (0, 1)$。简单计算可得

$$P(x)_0 = (a+b+c)_0 x_0, \tag{13}$$
$$P(x)_+ = (a_0x_0 + c_0)x_+ + (a+b+c)_+x_0. \tag{14}$$

注意，对于任意 $\alpha_0, \gamma_0 \in S_0$，若且唯若对所有 $x_0 \in S_0$ 都有 $\alpha_0 x_0 + \gamma_0 = 1$，则 $(\alpha_0, \gamma_0) = (0, 1)$。事实上，令 $x_0 = 0$，可得 $\gamma_0 = 1$；再令 $x_0 = 1$，得到 $1 = \alpha_0 + \gamma_0 = \alpha_0 + 1$，从而得到 $\alpha_0 = 0$。由于 $(a_0, c_0) \neq (0, 1)$，我们得出存在 x_0 使得 $\mu_0 = a_0x_0 + c_0 \neq 1$。令

$$x = x_0, \quad y = x_0 + (\mu_0 + 1)C_2.$$

由于 $x_0 = y_0$，根据方程 (13)，我们有 $P(x)_0 = P(y)_0$，并且

$$P(y)_+ = (a_0x_0 + c_0)(\mu_0 + 1)C_2 + (a+b+c)_+x_0 = \mu_0(\mu_0+1)C_2 + P(x)_+ = P(x)_+$$

根据方程 (14)。因此，P 不是单射。接下来，假设 $(a_0, c_0) = (0, 1)$，但 $b_0 \neq 0$。同样，我们得到

$$P(x)_0 = (b_0 + 1)x_0,$$
$$P(x)_+ = x_+ + (a+b+c)_+x_0.$$

因此，如果 $x = 0$ 且 $y = b_0 + (a+b+c)_+b_0$，我们得到 $P(x) = P(y) = 0$。因此，P 再次不是单射。

最后，我们证明，如果 P 是满射，则 $(a_0, b_0, c_0) = (0, 0, 1)$。我们考虑 $x, y \in S$，使得

$$P(x) = C_1 + C_2 + (a+b+c)_+$$
$$P(y) = C_2.$$

首先，$P(x)_0 = (a+b+c)_0x_0 = 1$，这意味着 $x_0 = 1$ 且 $(a+b+c)_0 = 1$。其次，$P(y)_0 = (a+b+c)_0y_0 = y_0 = 0$，因此 $P(y)_+ = c_0y_+ = C_2$，这意味着 $c_0 = 1$。第三，$P(x)_+ = (a_0+1)x_+ + (a+b+c)_+ = C_2 + (a+b+c)_+$，因此 $(a_0+1)x_+ = C_2$，这意味着 $a_0 = 0$。我们得到 $(a_0, b_0, c_0) = (0, 0, 1)$。 □

3.7 主理想的交集

在本小节中，我们关注两个主理想的交集 $xS \cap yS$。主要问题是这个交集是否仍为主理想。我们无法完全回答这个问题，但证明了在自然约束下，$xS \cap yS$ 确实是一个主理想。另一方面，我们至今还没有找到任何满足 $x, y \in S$ 且 $xS \cap yS$ 不是主理想的例子。

我们首先证明，可以将注意力集中在 x 的情形。 $\tilde{\mathcal{R}}y.$

引理 3.22。 设 $x, y \in S$。记 $\alpha = xy^+$ 和 $\beta = yx^+$，则有 $xS \cap yS = \alpha S \cap \beta S$ 和 $\alpha \tilde{\mathcal{R}} \beta$。

证明。 设 $\alpha = xy^+$ 和 $\beta = yx^+$。显然， $\alpha S = xy^+S \subseteq xS$ 和 $\beta S = yx^+S \subseteq yS$，因此 $\alpha S \cap \beta S \subseteq xS \cap yS$。此外， $\alpha^+ = x^+y^+ = \beta^+$。现在假设 $m = xa = yb \in xS \cap yS$。那么 $m = xa = x^+xa = x^+m = x^+yb = \alpha b$，由对称性可得 $m = \beta a$，从而得到 $m \in \alpha S \cap \beta S$。 □

命题 3.23。 设 $x, y \in S$，且 x 是正则的。那么 $xS \cap yS = xyS$。

证明。 若 x 是正则的，则（由定理 3.16） $xS = x^2S$，其中 x^2 是幂等元，因此不失一般性，设 x 是幂等元，从而得到 $x^+ = x$。使用引理 3.22 中的记号，我们有

$$\beta = yx^+ = yx = yy^+x = \alpha y,$$

因此 $\beta \in \alpha S$ 和 $xS \cap yS = \alpha S \cap \beta S = \beta S = xyS$。 □

很容易构造出满足 $xS \cap yS \neq xyS$的例子；例如，若 $x = y = C_2$，则 $C_2 \in C_2S = xS \cap yS \neq \{0\}$，而 $xyS = \{0\}$，因为 $xy = 0$。这是以下结果的一个特殊情形。

命题 3.24. 若 $xy = 0$，则 $xS \cap yS = \gamma_{x,y}S$，其中 $\gamma_{x,y} = (1 + (x + y)^+)x = (1 + (x + y)^+)y$.

证明。 现在假设 $xy = 0$，于是

$$x_0y_0 = 0, \text{ and } x_0y_i + y_0x_i = 0 \text{ for all } i > 0, \tag{15}$$

并考虑 $xS \cap yS$。根据引理 3.22 和命题 3.12，不失一般性，我们可以假设 $x^+ = y^+$。由以下事实可知：$(x+y)^+(x+y) = x+y$ that $(1+(x+y)^+)x = (1+(x+y)^+)y$。将这个元素称为 $\gamma_{x,y}$ 显然 $\gamma_{x,y}S \subseteq xS \cap yS$。我们要证明其逆命题。于是，假设 $m = xa = yb \in xS \cap yS$，从而

$$m_0 = x_0a_0 = y_0b_0, \text{ and } m_i = y_0b_i + b_0y_i = x_0a_i + a_0x_i \text{ for all } i > 0. \tag{16}$$

x_0 的幂等性与方程 (15) 和 (16) 共同推出

$$\begin{aligned} m_0 &= x_0a_0 = x_0^2a_0 = x_0y_0b_0 = 0, \\ x_0m_i &= x_0^2a_i + x_0a_0x_i = x_0a_i, \text{ and} \\ x_0m_i &= x_0y_0b_i + x_0b_0y_i = 0 + y_0b_0x_i = 0. \end{aligned}$$

因此，对所有 i，都有 $x_0m_i = x_0a_i = 0$；对偶地论证（这次利用 y_0 的幂等性）还可得，对所有 i，都有 $y_0m_i = y_0b_i = 0$。但根据方程 (16)，我们有 $m_0 = a_0x_0 = b_0y_0$、$m_i = x_0a_i + a_0x_i = a_0x_i$，且对所有 $i > 0$，都有 $m_i = y_0b_i + b_0y_i = b_0y_i$，综合起来可得

$$m = a_0x = b_0y.$$

现在，回想起 $x^+ = y^+$，我们有

$$a_0x^+ = (a_0x)^+ = m^+ = (b_0y)^+ = b_0y^+,$$

因此

$$a_0(x + y) = a_0x + a_0y = a_0x + a_0x^+y = a_0x + b_0y = m + m = 0.$$

由推论 3.11，我们得到 $a_0(x + y)^+ = 0$，因此

$$m = a_0x = a_0x + a_0(x + y)^+x = \gamma_{x,y}a_0 \in \gamma_{x,y}S.$$

□

4 单射偏部分变换的半环

在本节中，我们现在考虑所有单射偏变换，即由链 L_d 和循环C_e构成的和。容易验证（系数取自自然数集）对于任意 e，$d \geq 1$，我们有

$$\begin{aligned} L_e L_d &= (|d-e|+1)L_{\min(d,e)} + \sum_{i=1}^{\min(d,e)-1} 2L_i, \\ C_e C_d &= \gcd(d,e) C_{\mathrm{lcm}(d,e)}, \\ L_e C_d &= dL_e. \end{aligned}$$

回顾一下，所有链的集合记作 L，循环的集合记作 C。在 $\mathrm{F}_2(L \cup C)$ 中进行运算时，我们得到

$$L_e L_d = \begin{cases} L_{\min(d,e)} & \text{if } e \equiv d \mod 2 \\ 0 & \text{otherwise.} \end{cases}$$

4.1 由 L 与 $\mathbb{F}_2$ 生成的格

我们首先考虑模 2 的链和的情形，即 $\mathrm{F}_2 L$。首先注意，偶数长度与奇数长度互不影响，因为当 e 和 d 的奇偶性不同时，$L_d L_e = 0$。于是，我们可以将问题分解为偶数长度链的问题和奇数长度链的问题。更准确地说，对于$\epsilon \in \{0,1\}$，令

$$L^{(\epsilon)} = \left\{ a \in \mathbb{F}_2 L : a = \sum_{j \geq 1} \alpha_{2j-\epsilon} L_{2j-\epsilon} \right\},$$

即 $L^{(0)}$ 仅涉及偶数长度链，而 $L^{(1)}$ 则涉及奇数长度链。于是，任意 $a \in \mathrm{F}_2 L$都可以唯一地分解为 $a = a^{(0)} + a^{(1)}$，其中 $a^{(0)} = \sum_{j \equiv 0 \bmod 2} \alpha_j L_j \in L^{(0)}$，且 $a^{(1)} = \sum_{j \equiv 1 \bmod 2} \alpha_j L_j \in L^{(1)}$。因此，

$$ax = b \quad \Longleftrightarrow \quad b^{(0)} = a^{(0)} x^{(0)} \text{ and } b^{(1)} = a^{(1)} x^{(1)}.$$

因此，我们只考虑 $L^{(1)}$ 中的除法问题；$L^{(0)}$ 的情形与之等价。

在 $\mathrm{F}_2 L$ 中，$L_d^2 = L_d$，因此乘积构成一个半格。事实上，它与自然数集 $\mathbb{N}$ 的有限子集格同构。具体而言，令 $Z_1 = L_1$，并令所有奇数 $i \geq 3$ 对应 $Z_i = L_i + L_{i-2}$。现在，对于所有奇数 i，j，我们有：

$$Z_i Z_j = \delta_{ij} Z_i,$$

因此，如果 $a = \sum_i a_i Z_i$ 且 $b = \sum_j b_j Z_j$，我们就有 $ab = \sum_k a_k b_k Z_k$。换句话说，若将 a 与其支撑（$S(a) = \{i : a_i = 1\}$）对应起来，则 $S(ab) = S(a) \cap S(b)$。我们注意到，由于缺少乘法单位元 C_1，格 $\mathrm{F}_2 L$ 不是布尔代数。然而，由 $\mathcal{L}_k = \{Z_1, Z_3, \ldots, Z_k\}$ 生成的子格确实是一个布尔代数 $V(\mathcal{L}_k)$，其原子为 Z_1，……，Z_k，上界为 $Z_1 + Z_3 + \cdots + Z_k = L_k$。例如，由 Z_1，Z_3，Z_5 生成的布尔代数如图 4 所示。

对于任意 $a = \sum_j \alpha_j L_j$，我们将 a 的**高度**定义为

$$\mathrm{h}(a) = \max\{j : \alpha_j = 1\},$$

约定 $\mathrm{h}(0) = 0$。如果 a，x，$b \in L^{(1)}$ 满足 $ax = b$，则 $\mathrm{h}(b) = \min\{\mathrm{h}(a), \mathrm{h}(x)\}$。对于任意 $x \in L^{(1)}$ 以及任意奇数 $h \in \mathbb{N}$，令

$$\begin{aligned} x_{-h} &= \sum_{i \leq h} x_i Z_i, \\ x_{+h} &= \sum_{j \geq h+2} x_j Z_j, \end{aligned}$$

使得 $x = x_{-h} + x_{+h}$。

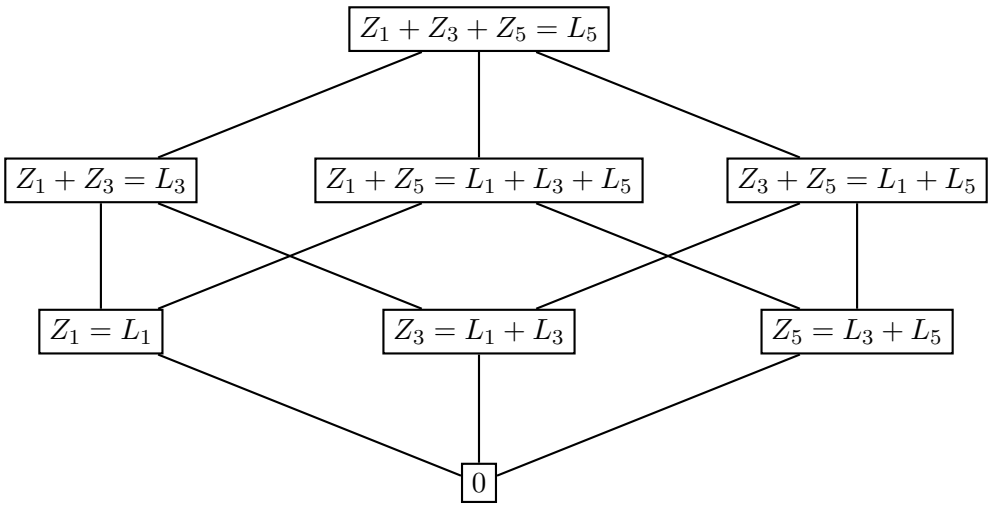


图 4：由高度为 1、3 和 5 的链生成的布尔代数 $V(\mathcal{L}_5)$。

定理 4.1。设 $a, b \in L^{(1)}$ 满足 $\mathrm{h}(a) = h$。那么 $x \in L^{(1)}$ 满足 $ax = b$，当且仅当 $x_{-h} \in [b, b + a + L_h]$ 属于布尔代数 $V(\mathcal{L}_h)$。

证明。对于任意 $k \geq h = \mathrm{h}(a)$，我们有 $aL_k = a$，因此 $aZ_{k+2} = a(L_{k+2} + L_k) = a + a = 0$，由此可得，对于任意 $x \in L^{(1)}$，都有 $ax_{+h} = 0$。我们得到

$$ax = b \iff ax_{-h} = b,$$

而根据命题 3.4，后者等价于布尔代数 $V(\mathcal{L}_h)$ 中的 $x_{-h} \in [b, b + a + L_h]$。

□

4.2 在由 L、C 和 $\mathbb{F}_2$ 生成的半环中进行除法

任意 $d \in \mathrm{F}_2(L \cup C)$ 都可以唯一地分解为 $d = d^{(0)} + d^{(1)} + d^{(C)}$，其中对于 $\epsilon \in \{0, 1\}$ 和 $d^{(C)} \in \mathrm{F}_2 C = S$，有 $d^{(\epsilon)} \in L^{(\epsilon)}$。为使记号简洁，我们记 $d^{(C)} = \sum_i d_i C_{2^i}$，其中对所有 i，都有 $d_i \in S_0$。

现在，我们给出方程 $ax = b$ in $\mathrm{F}_2(L \cup C)$ 的解集的刻画。首先，引入一些有用的记号。对于所有 $i \in \mathbb{N}$，令 λ_i, υ_i 如定理 3.9 中关于除法$a^{(C)}x^{(C)} = b^{(C)}$的定义。对于所有 $t \in \{0, 1\}$，令 X_t 表示 $a^{(C)}x^{(C)} = b^{(C)}$ 的解集，其中$|x^{(C)}| \equiv t \bmod 2$。根据定理 3.9，该集合为

$$X_t = \left\{ x^{(C)} \in S : x_i \in [\lambda_i, \upsilon_i] \ \forall i \in \mathbb{N}, |x^{(C)}| \equiv t \mod 2 \right\}.$$

对于 $\epsilon \in \{0, 1\}$，令

$$h = h^{(\epsilon)} = \begin{cases} \mathrm{h}(a^{(\epsilon)}) & \text{if } |a^{(C)}| \equiv 0 \mod 2, \\ \max(\mathrm{h}(a^{(\epsilon)}), \mathrm{h}(b^{(\epsilon)})) & \text{if } |a^{(C)}| \equiv 1 \mod 2. \end{cases}$$

然后令

$$Y_t^{(\epsilon)} = \begin{cases} \{x^{(\epsilon)} \in L^{(\epsilon)} : x_{-h}^{(\epsilon)} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)} + L_h] \subseteq V(\mathcal{L}_h)\} & \text{if } |a^{(C)}| \equiv 0 \mod 2, \\ \{x^{(\epsilon)} \in L^{(\epsilon)} : x^{(\epsilon)} = x_{-h}^{(\epsilon)} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)}] \subseteq V(\mathcal{L}_h)\} & \text{if } |a^{(C)}| \equiv 1 \mod 2. \end{cases}$$

定理 4.2. 设 $a, b, x \in \mathbb{F}_2(L \cup C)$。那么，按照上述记号，$ax = b$ 当且仅当$x^{(C)} \in X_t$ 对于某个 $t \in \{0, 1\}$ 且 $x^{(\epsilon)} \in Y_{(\epsilon)\,t}$ 对所有 $\epsilon \in \{0, 1\}$ 均成立。

证明。</style}我们有 $ax = b$ 当且仅当

$$b^{(C)} = a^{(C)}x^{(C)}, \tag{17}$$

$$b^{(\epsilon)} = a^{(\epsilon)}x^{(\epsilon)} + a^{(\epsilon)}x^{(C)} + a^{(C)}x^{(\epsilon)}, \forall \epsilon \in \{0, 1\}. \tag{18}$$

首先，借助定理 3.9，我们可以求解方程 (17)。如上所述，对于每个 $t \in \{0,1\}$，满足模 2 条件 $|x^{(C)}| \equiv t$ 的方程 (17) 的 $x^{(C)}$解集为 X_t。

其次，对于 $|x^{(C)}| \equiv t \bmod 2$，方程 (18) 等价于

$$b^{(\epsilon)} = a^{(\epsilon)}x^{(\epsilon)} + ta^{(\epsilon)} + a^{(C)}x^{(\epsilon)}. \tag{19}$$

断言 1. 设 $|a^{(C)}| \equiv 0 \bmod 2$。记 $h = \mathsf{h}(a^{(\epsilon)})$，则 $x^{(\epsilon)}$ 是方程 (19) 的解，当且仅当

$$x^{(\epsilon)}_{-h} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)} + L_h]$$

在 $V(\mathcal{L}_h)$ 中。

证明。 若 $|a^{(C)}| \equiv 0 \bmod 2$，则方程 (19) 化为

$$a^{(\epsilon)}x^{(\epsilon)} = b^{(\epsilon)} + ta^{(\epsilon)},$$

由定理 4.1 可得 $x^{(\epsilon)}_{-h} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)} + L_h]$。 □

断言 2. 设 $|a^{(C)}| \equiv 1 \bmod 2$。记 $h = \max(\mathsf{h}(a^{(\epsilon)}), \mathsf{h}(b^{(\epsilon)}))$，则 $x^{(\epsilon)}$ 是方程 (19) 的解，当且仅当

$$x^{(\epsilon)} = x^{(\epsilon)}_{-h} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)}]$$

在 $V(\mathcal{L}_h)$ 中。

证明。 如果 $|a^{(C)}| \equiv 1$ 模 2，则方程 (19) 化简为

$$x^{(\epsilon)} = a^{(\epsilon)}x^{(\epsilon)} + b^{(\epsilon)} + ta^{(\epsilon)}.$$

请注意，这并不等价于 $(a^{(\epsilon)} + 1)x^{(\epsilon)} = b^{(\epsilon)} + ta^{(\epsilon)}$，因为乘法单位元$1 = C_1$ 不属于 L。然而，由于右侧的高度至多为 $h = \max(\mathsf{h}(a^{(\epsilon)}), \mathsf{h}(b^{(\epsilon)}))$，我们有 $\mathsf{h}(x^{(\epsilon)}) \le h$，因此 $x^{(\epsilon)} = x^{(\epsilon)}_{-h}$。上面的方程于是等价于

$$(a^{(\epsilon)} + L_h)x^{(\epsilon)} = b^{(\epsilon)} + ta^{(\epsilon)},$$

根据定理 4.1，得到 $x^{(\epsilon)} = x^{(\epsilon)}_{-h} \in [b^{(\epsilon)} + ta^{(\epsilon)}, b^{(\epsilon)} + (t+1)a^{(\epsilon)}]$。 □

□

遗憾的是，刻画集合 X_t 并不简单，原因如下。设$\mathcal{P} = \{e \in S_0 : |e| \equiv 0 \text{ 模 } 2\}$ 表示“奇偶校验码”。那么，对于任意满足$\lambda < \upsilon$的区间 $[\lambda, \upsilon]$，交集 $[\lambda, \upsilon] \cap \mathcal{P}$都包含无限上升链：若 $e \in [\lambda, \upsilon] \cap \mathcal{P}$且 $k = \mathrm{lcm}(K(\lambda)\ K(\upsilon)\ K(x))$，则 $f = e + C_k + C_{3k}$满足 $f \in [\lambda, \upsilon] \cap \mathcal{P}$和 $f > e$。类似地，集合$[\lambda, \upsilon] \setminus \mathcal{P}$则包含无限下降链。

尽管如此，如果我们将求解 F_2 上的方程视为对求解自然数集 N 上方程的简化——后者对解的可能规模有严格界限——那么我们就可以对 x 作出一些限制，使得 $ax = b$ 属于 $\mathrm{F}_2(C \cup L)$。设 k 为奇整数，满足最小公倍数$(K(a^{(C)})\ K(b^{(C)}))$ $\mid k$，即 $a^{(C)} = a^{(C)}_{\mid k}$ 且 $b^{(C)} = b^{(C)}_{\mid k}$；换言之，$a$ 和 b 中的所有圈长度都整除某个 m 的 $k2^m$。这样一来，就能更精确地确定满足 $x^{(C)} = x^{(C)}_{\mid k}$ 的解，因为现在我们可以始终在有限布尔代数中进行运算。

对于所有 $i \in$ 自然数集，令 λ_i, υ_i 如定理 3.9 中关于除法 $a^{(C)}x^{(C)} = b^{(C)}$ 所述，并定义 $V(\mathcal{C}_k)$ 的区间$J(i,0) = [\lambda_i + C_k + \lambda_i C_k, \upsilon_i]$和 $J(i,1) = [\lambda_i, \upsilon_i + \upsilon_i C_k]$。那么，对于所有 $t \in \{0,1\}$，令

$$W_t = \left\{ \omega \in \{0,1\}^* : \sum_i \omega_i \equiv t \mod 2 \right\}$$

$$(X_t)_{\mid k} = \bigcup_{\omega \in W_t} \left\{ x^{(C)}_{\mid k} \in S : x_i \in J(i, \omega_i)\ \forall i \ge 0 \right\}.$$

命题 4.3。 令 $a, b, x \in \mathbb{F}_2(C \cup L)$ 满足 最小公倍数$(K(a^{(C)})\ K(b^{(C)})\ K(x^{(C)}))\mid k$。那么，沿用上述记号，$ax = b$ 当且仅当 $x^{(C)} \in (X_t)\mid^{k}$ 对某个 $t \in \{0,1\}$ 成立，且 $x^{(\epsilon)} \in Y_{(\epsilon)\,t}$ 对所有$\epsilon \in \{0,1\}$成立。

证明。 推论2.11表明，使得.....且.....的 $x^{(C)}$ 为 $J\ (i,\ \omega_i)$，其中$J\ (i,\ \mathbf{0}) = [\lambda_i + a^{\mathbf{0}} + \lambda_i a^{\mathbf{0}}, \upsilon_i]$ 且 $J\ (i,\ \mathbf{1}) = [\lambda_i, \upsilon_i + \upsilon_i a^{\mathbf{0}}]$，其中 $a^{\mathbf{0}} = \mathbf{0}$由 $V\ (\mathcal{C}_k)$ 中的 C_k给出。因此，对于 $t = |x^{(C)}| \in \{0,1\}$，$x^{(C)} \in\ (X_t)\mid^{k}$。证明的其余部分沿用定理 4.2。 □

5 结论与未来工作

本文提出了一个关于形式和半环的通用框架。随后，我们将这一框架应用于研究 $S =\mathrm{F}_2 C$，其中 C 是圈的集合。我们刻画了 S的许多代数性质，并高效地解决了该环中的除法问题。这与原始的圈的和除法问题形成鲜明对比，因为目前尚无已知的多项式时间算法。随后，我们将研究扩展到$\mathrm{F}_2\ (L \cup C)$，即考虑圈和链的和，它们是单射偏变换。

对部分变换及其形式和半群的研究，具有许多自由度。

- 部分变换的选择。本文采用的方法可以扩展到更一般的部分变换类。一个自然的候选对象是有界高度变换类（高度指从一个状态到某个周期状态的路径的最大长度，也称为前周期），它们构成一个子半环。

- 半环 S 的选择。选择半环 S $=\mathrm{F}_2$ 带来了一些强大的代数性质，并大幅简化了某些问题（尤其是圈的和的除法问题）。选择其他 S 可能会从不同角度揭示部分变换半环的整体结构。自然的例子包括布尔半环（就乘积而言，它等价于在所谓的幂单群上进行运算）以及其他素域 F_p。

- 不同的问题。即使将研究范围限定在本文关注的 $S =\mathrm{F}_2 C$ 上，仍有许多有趣的问题尚未解决，包括：主理想的交集、多项式恒等式、更一般的一元多项式方程的求解、多元方程的求解等。

致谢

我们感谢 Sara Riva 就使用部分变换的动机进行了富有成效的讨论。

参考文献

[1] Florian Bridoux、Christophe Crespelle、Thi Ha Duong Phan 和 Adrien Richard。《函数有向图半环中的置换分解》。载于第*30*届元胞自动机与离散复杂系统国际研讨会，*AUTOMATA 2024*，第95–107页，2024年7月。[2] William Chin、Barbara Cortzen 和 Jerry Goldman。《带边界条件的线性细胞自动机》。《线性代数及其应用》，322：193–206，2001年。[3] Oscar Defrain、Antonio E. Porreca 和 Ekaterina Timofeeva。《函数有向图的同构类多项式延迟生成》。《离散应用数学》，357：24–33，2024年。[4] Alberto Dennunzio、Valentina Dorigatti、Enrico Formenti、Luca Manzoni 和 Antonio E. Porreca。《有限离散时间动力系统上的多项式方程》。载于第*13*届面向研究与工业的元胞自动机国际会议，*ACRI 2018*，第298–306页，2018年9月。

[5] Alberto Dennunzio、Enrico Formenti、Luciano Margara、Valentin Montmirail 和 Sara Riva。《求解离散动力系统上的方程》。载于《生物信息学与生物统计学计算智能方法——第16届国际会议，CIBB 2019》，第119–132页，2019年9月。[6] Alberto Dennunzio、Enrico Formenti、Luciano Margara 和 Sara Riva。《关于函数有向图半环上基本方程求解的札记》。《离散数学与理论计算机科学》，27，2025年。[7] Raymond Devillers。《迁移系统的乘积与Petri网的加法》。载于《第16届并发在系统设计中应用国际会议论文集》，第65–73页，2016年。[8] Raymond Devillers。《迁移系统的关节与乘积及其在Petri网综合中的应用》。《Fundamenta Informaticae》，183：1–31，2021年。[9] Enrico Formenti、Jean-Charles R´egin 和 Sara Riva。《多值决策图助力求解离散动力系统上的方程》。载于《约束规划、人工智能与运筹学集成国际会议》，第196–213页，2021年。[10] Caroline Gaze-Maillot。《有限动力系统的代数分析》。硕士论文，Aix-Marseille Universit´e，2020年。[11] Steven Givant 和 Paul Halmos。《布尔代数导论》。施普林格，2009年。[12] Victoria Gould。《关于限制半群及相关结构的札记》。网址：https: //www-users.york.ac.uk/~varg1/restriction.pdf。[13] Victoria Gould 和 Christopher Hollings。《限制半群与归纳星座》。《Communications in Algebra》，38：261–287，2010年。[14] George Gr¨atzer。《一般格论》。Birkh¨auser，2003年。[15] Richard Hammack、Wilfried Imrich 和 Sandi Klavˇzar。《积图手册》。CRC出版社，2011年。[16] John M. Howie。《半群理论基础》。牛津大学出版社，1995年。[17] Claus Kadelka、Matthew Wheeler、Alan Veliz-Cuba、David Murrugarra 和 Reinhard Laubenbacher。《生物系统的模块化：结构与功能之间的联系》。《J. R. Soc. Interface》，20(20230505)，2023年。[18] Ganna Kudryavtseva。《离散限制半群及其代数的拓扑方法》。arXiv，2025年。[19] Harold V. McIntosh。《一维元胞自动机》。Luniver出版社，2009年。[20] ´Emile Naquin 和 Maximilien Gadouleau。《有限动力系统半环中的因式分解》。《Theoretical Computer Science》，998(114509)，2024年6月。[21] John Pedersen。《作为代数系统的元胞自动机》。《Complex Systems》，6：237–250，1992年。[22]K´evin Perrot、Pacˆome Perrotin 和 Sylvain Sen´e。《布尔自动机网络的（分解）组合》。《Fundamenta Informaticae》，181(2-3)：163–188，2021年。[23] N. Petkov。《脉动并行处理》。北荷兰出版社，1992年。[24] Alberto E. Porreca 和 Marius Rolland。《有限离散动力系统上多项式的单射性》。载于《欧洲可计算性会议2025（CiE 2025）论文集》，2025年。[25] Alberto E. Porreca 和 Marius Rolland。《求解有限动力系统上的“伪单射”多项式方程》。载于《第31届元胞自动机与离散复杂系统国际研讨会（AUTOMATA 2025）论文集》，2025年。

[26] Sara Riva。离散动力系统的因子分解。博士论文，索菲亚安提波利斯信号与计算机科学实验室（I3S），尼斯大学，法国，2022年。

[27] Viktor Teren、Jordi Cortadella 和 Tiziano Villa。将迁移系统分解为若干同步自由选择佩特里网集合。载于第*25*届*Euromicro*数字系统设计会议论文集，第165–173页，2022年。