arXiv:2601.19271v1 [cs.FL] 27 Jan 2026

保留本原词的态射研究

Francis Wlazinski

2026年1月28日

摘要

本文回顾了一些关于本原词及保留它们的态射的性质，这些内容可见于 [3, 10, 11]。文中也给出了这些证明（我对其做了或多或少的改写）。因此，正如英语所说，本文几乎可以“自成一体”。我也为这项工作添砖加瓦，介绍了一些关于本原词的性质，尤其证明了无幂（≥ 5）的态射是本原的，而无幂（≥ 2）的一致态射也是本原的。

1 预备知识

下文中，A 和 B 是字母表，也就是说，是由符号组成的有限非空集合。

词是由 A 生成的自由 A^* 幺半群的一个 ´元´，其单位元是记作 ε 的空词，其运算“.”通常不记作任何符号，实际上就是符号的并置。我们用 A^+ 表示非空词的集合，也就是 $A^+ = A^* \setminus \{\varepsilon\}$。下文中，我们不会总是明确指出所使用的字母表，因为这通常并不重要。

给定一个非空词 $u = a_1 \dots a_n$，其中 $a_i \in A$，u的长度记作 $|u|$，是整数 n。空词的长度为 $|\varepsilon| = 0$。u的镜像记作 $\tilde{u}$，是词 $a_n \dots a_1$。对于空词这一特殊情况，有 $\tilde{\varepsilon} = \varepsilon$。

如果可以将一个词 w 写成 $pw's$ 的形式，那么就称 p、w' 和 s 是 w的因子，称 p 是 w 的前缀，称 s 是 w的后缀。此外，如果 p 或 s 这两个词中有一个非空，则称 w' 为真。若 p 和 s 这两个词都非空，则称 w' 为内部的。如果 $\varepsilon \neq p = s \neq w$，则称 p 是 w的一个边界。更一般地，词 w 的边界是 w 的一个非空因子，同时也是 w的真前缀和真后缀。

设 w 是一个非空词，i、j 是满足 $0 \leq i-1 \leq j \leq |w|$的两个整数。记 $w_{[i..j]}$ 为 w 的因子，使得 $|w_{[i..j]}| = j-i+1$，且 $w = pw_{[i..j]}s$ 是满足 $|p| = i-1$的两个词 s 和 p。注意，当 $j = i-1$ 时，我们有 $w_{[i..j]} = \varepsilon$。当 $i = j$时，

我们记 $w_{[i]}$ 为因子 $w_{[i..i]}$，也就是说，它是 w 的第 i-`个字母。特别地，$w_{[1]}$ 和 $w_{[|w|]}$ 分别是 $w$ 的第一个和最后一个字母。一般而言，$w_{[i..j]}$ 是 $w$ 的因子，它从 $w$ 的第 $i$-`个字母开始，到第 j-`个字母结束。
在 A 上，无限词（或 ω-词）是由 A中的元素组成的无限序列。 A 上的无限词集合记作 A^{ω}。

如果可以通过循环置换从一个词 u 得到另一个词 v，也就是说，若存在 A^* 中的词 x 和 y，使得 $u = xy$ 且$v = yx$，则称 A^* 中的两个词 u 和 v 共轭。若 x 和 y 均非空，则称 v 是 u 的真共轭词。共轭关系显然是一种等价关系。

本文只考虑整数幂：词 u 的幂递归定义为 $u^0 = \varepsilon$，且对任意整数 $n \geq 1$， $u^n = uu^{n-1}$。对任意整数 $k \geq 2$，情形 ε^k 意义不大。因此，幂 k 是一个词u^k，其中`$u \neq \varepsilon$。如果一个词的某个因子具有 u^k 的形式（其中 $u \neq \varepsilon$），则称该词包含幂 k。若一个词所包含的最大幂严格小于 k，则称该词不含幂 k。

如果一个词非空且不是其他词的幂，则称其为本原词或非周期词；也就是说，若等式 $w = u^k$ 对某个非零整数 k 成立，则 $k = 1$ 是本原词（显然也可写作 ´，和/或 $w = u$）。

对于一个词 $w(\neq \varepsilon)$，满足 $w = t^n$ （其中 $n \geq 1$ 为整数）的最短（唯一）词 t 称为 w 的本原根。记作 $\rho(w)$。
在本文接下来的内容中，我们将多次用到字符串组合学的一些基本性质。首先是不可或缺的 Fine 和 Wilf 定理：

命题 1.1（Fine 和 Wilf）若一个非空词 u 的某个幂与一个非空词 v 的某个幂有一个公共前缀，其长度大于或等于 `(|u|, |v|)，则 u 和 v 是同一个本原词的幂。

换言之， u 和 v 具有相同的本原根。此外，若 $|u| > |v| > 0$，则 u 不是本原的。

此外，界限 $|u| + |v| - pgcd(|u|, |v|)$是最优的。

注释 1.2 由于 $pgcd(|u|, |v|) \leq \min(|u|, |v|)$，特别地有 $|u| + |v| - pgcd(|u|, |v|) \geq \max(|u|, |v|)$。

利用镜像，可直接得到：

推论 1.3 若非空词 u 的一个幂与非空词v 的一个幂具有长度大于或等于 $|u| + |v| - pgcd($ $|u|, |v|)$的公共后缀，则u 和 v 是同一个本原词的幂。

此外，界 $|u| + |v| - pgcd(|u|, |v|)$ 是最优的。

推论 1.4 对任意非零整数 n 和 m，若 $u^n = v^m$，则词 u 和 v是同一个词的幂。

注记 1.5 这意味着，若 $w = u^n$ 且 $n \geq 1$，则 u 是ρ的幂（w是 w的本原根）。

推论 1.6 [4] 设 x 和 y 是两个词。如果 x 的某个幂与 y的某个幂有一个长度大于或等于 $|x| + |y| - gcd(|x|, |y|)$ 的公共因子，那么存在两个词 t_1 和 t_2，使得 x 是 t_1t_2 的某个幂，且 y 是 t_2t_1 的某个幂，其中 t_1t_2 和 t_2t_1 是本原词。此外，如果 $|x| > |y|$，那么 x 不是本原的。

关于词的常见初等方程的解由以下命题给出:

命题 1.7 [7]
设 u、v、w是字母表 A上的三个词。

1. 如果 $vu = uw$ 和 $v \neq \varepsilon$，那么存在两个词 r 和 s，它们属于 A，以及一个整数 n，使得$u = r(sr)^n$、$v = rs$ 和 $w = sr$。2. 如果 $vu = uv$，则称词 u 和 v 可交换，此时存在一个（本原）词 w，它属于 A，以及两个整数 n 和 p，使得 $u = w^n$ 和 $v = w^p$。3. 如果 $uvw = wvu$ 且 $(u, v) \neq (\varepsilon, \varepsilon)$，那么存在两个词 t_1、t_2，它们属于 A，以及三个整数 n、p、q，使得 $u =(t_1t_2)^nt_1$、$v = (t_2t_1)^pt_2$ 和 $w = (t_1t_2)^qt_1$。

注记 1.8 如果两个非空词 x 和 y 可交换，那么 xy 不是本原词。

推论 1.9 本原词 w 有不同的 `共轭词 $|w|$。

注记 1.10 换言之，如果一个词的所有真共轭词都互不相同，那么它就是本原词。

推论 1.11 本原词的所有（真）共轭词都是本原词。

注记 1.12 非本原词包含一个边界。

命题 1.13 一个词是本原词，当且仅当它的某个共轭词是一个没有边界的词。

证明。
如果 w 不是本原的，即 $w = t^n$，其中 $t \neq \varepsilon$ 且 $n \geq 2$，那么 t 是 w的一个边界。
如果 w 是本原的，令 x 为在固定的字典序 ´（记作 $\leq$）下， w 的共轭词 ´中最小的一个。如果 x 有一个边界，那么可以将 $x = uvu$ 写成两个词 $u \neq \varepsilon$ 和v的形式。词 $z = uuv$ 也是 w的一个共轭词。如果 $x = z$，那么 $vu = uv$ 且 x 就不是本原的，这与假设矛盾。因此 $x < z$ 且 $vu < uv$。但此时 $vuu < uvu = x$，其中 vuu 是 w 的一个共轭词：这与选择 x时所依据的假设矛盾 ``。 □

命题 1.14 两个共轭词具有共轭的本原根。

证明。
设 $w = rs \neq \varepsilon$，且 $\underline{w} = sr$ 是它的一个共轭词。设 $t = \rho(w)$ 是 w 的本原根，并设 n 是满足 $w = t^n$ 的整数。存在两个词 t_1 和 t_2 以及一个整数 α，使得 $t = t_1t_2$、 $r = t^{\alpha}t_1$ 和 $s = t_2t^{n-\alpha-1}$。

换言之，$\underline{w} = (t_2t_1)^n$。根据推论 1.11，词 t_2t_1 是本原的。因此， t_2t_1（ t_1t_2 的共轭）是 $\underline{w}$ 的本原根。 □

引理 1.15 [4, 5]
若非空词 v 是 vv 的内部因子，也就是说，若存在两个非空词 x 和 y，使得 $vv = xvy$，那么存在一个非空词 t 和两个整数 i、 $j \geq 1$，使得 $x = t^i$、 $y = t^j$，且 $v = t^{i+j}$。

注记 1.16 换言之，若非空词 v 是 vv 的内部因子，那么 v 不是本原的。

语言 X 是 A^* 的一个子集。
若语言 X 满足其中每个 ´元´素在 X^+ 上都有唯一分解，则称其为一个码。这意味着， X^* 是 A^* 的自由子幺¨半群，且 X 是其一组基。
Un 若码 $X \subset A^*$ 中的所有非空词长度相同，则称其为均匀码。
若一个码是均匀码，且码中没有任何词是两个码中词的连接的内部因子，则称其为无逗号码。

若码 $X \subset A^*$ 中任意词的本原根都属于 X^*，则称其为纯码。 .

设 A 和 B 是两个字母表。态射 f 从 A^* 到 B^* 是一个从 A^*到 B^* 的映射，满足对 A^* 中的任意词 u和 v， $f(uv) = f(u)f(v)$。如果字母表 B无关紧要，则称 f 定义在 A^*上。注意，定义在 A^* 上的态射完全由 A中字母的像确定。若存在一个整数 L，使得对所有 $a \in A$， $|f(a)| = L$，则称态射 f 是均匀的。

映射 $\epsilon : A^* \to B^*; u \mapsto \varepsilon$ 是一个态射（长度为 0 的均匀态射），对我们来说意义不大。因此，从现在起，我们假设对于所考虑的每个态射 f， $f \neq \epsilon$。

注释 1.17 态射 h 从 A^* 到 B^* 是单射，当且仅当 $h(A)$ 是一个码。

设 $k \geq 2$ 为一个整数。
对于任意整数 $n \geq 1$，如果一个态射将 A^+ 中长度小于或等于 n 的所有无幂 k 词映射为仍然无幂 k 的词，则称该态射为 n-无幂 k，或在 `a n 之前无幂 k。

态射 f 是无幂的 k，如果对于任意整数 $n \geq 1$，它都是 n-无幂的 k。换言之，态射 f 是无幂的 k，如果任意无幂词k 的像也无幂 k。我们也称态射 f 保持´无

幂 k。当 $k=2$（分别为 $k=3$）时，我们称之为无平方态射 ´（分别为无立方态射）。

同样，对于任意整数 $n \geq 1$，如果一个态射将 n 的所有长度小于或等于 ` $n$ 的本原词的像也映射为本原词，则称其为 $A^+$ -本原的，或称其本原性达到 ´ ´ ` n

如果一个态射对于任意整数 n 都是 $n \geq 1$-本原的，则称其为本原态射，即，如果一个态射f到 A^*，且任意本原词的像也是本原词，则称其为本原态射
如果对于 A 中任意不同的字母 a 和 b，词 $f(a)$ 不是 $f(b)$ 的前缀（分别为后缀），则称态射 f 到 A^* 是前缀态射（分别为后缀态射）。如果对于 A 中的任意字母 a， $f(a) \neq \varepsilon$，则称态射 f 到 A^* 是非擦除的。如果一个态射既是前缀态射又是后缀态射，则称其为双定点态射。

注意，前缀态射（分别地，后缀态射）是单射且非消去的。
从 f 到 A^* 的态射 B^* 是 ps-态射，当且仅当等式 ´( ) f、$a(=ps)$ f以及$b(=ps')$ f对c、 $=p's$、 a（可选地b）以及$c \in A$、´、 $c=b$成立，并且 p蕴含 s或 p'。注意，ps-态射是双定点。

给定一个到˜ ˜ ⌢上的态射´， f 的镜像态射定义为 $A(f)$ $f( ) f$，对a中的所有字母 $= f$均成立。特别地，对a上的所有词˜ ⌢，有 $a(A)$ $f(w)$。

例如，若考虑由 $f\colon \{a,b\}^* \to \{x,y,z\}^*$; $a \mapsto xy$ et ~ $b \mapsto yzx$ 定义的态射 f，则其镜像态射 f 定义为 $f(a) = yx$ et $f(b) = xzy$。例如， $f(abb) = xy\,yzx\,yzx$。可以验证， $f(bba) = f(b)f(b)f(a) = xzy\,xzy\,yx$⌢
$= f(\widetilde{abb}) = f(\widetilde{bba})$.
注意，词 w 是本原的，当且仅当 $\tilde{w}$ 是本原的。直接可得，态射 f 是本原的，当且仅当 f 是本原的。
我们自然地将态射的概念推广到无限词。

最后，回顾一下关于无幂态射的两个结果。

命题 **1.18** *[14, 15]*
无幂一致态射对任意整数 $k \geq 3$ 都无幂。

命题 **1.19** *[16]*
无幂态射对任意整数 $k \geq 5$ 都无幂。

2 几个方程

引理 2.1（ [11]中的引理 9）
设 y、 y'、 z 和 z' 是四个词（假设 $|y| = |y'|$ 和 $|z| = |z'|$ 只是等式 ´的推论）。

若 $zy = y'z$ 和 $yz = z'y'$，则 $y = y'$。

证明。
若 $|z| = |z'| = 0$，则等式 ´´显然成立。因此，假设词 z 和 z' 均非空。
若 $|y| \leq |z|$，则 y 和 y' 是 z 的两个后缀，等式 ´´显然成立。
若 $|y| > |z|$，则存在两个词 y_1 和 y'_1，使得 $y' = y_1 z = z y'_1$ 和 $y = y'_1 z = z' y_1$，且 $|y_1| = |y'_1| < |y|$。
我们可以用词 y_1 和 y'_1 代替 y 和 y'，应用相同的推理。同样地，我们得到 $y'_1 = y_1$，或者得到两个新的词 y_2 和 y'_2。如此继续下去。我们得到两个严格递减的词序列（按长度递减）。必然存在一个整数 $p \geq 1$，使得 $|y_p| < |z|$，最终必定有 $y_p = y'_p$。

由 $y'_{p-1} = y_p z$ 和 $y_{p-1} = y'_p z = y_p z$，可得 $y_{p-1} = y'_{p-1}$。然后我们"反推"。 □

注记 2.2 引理 2.1 也可以由命题 1.7 的性质推得。事实上，由 $y'z = zy$，可以得到存在两个词 r 和 s，它们取自A，以及一个整数 n，使得 $z = r(sr)^n$, $y' = rs$ 和 $y = sr$。

于是可得 $yz(= z'y')$ 最终以 $y'(= rs)$ 结尾，并且若 $n \geq 1$，则以 sr 结尾；若$n = 0$，则以 rr 结尾。在第一种情况下，可直接得到 $y = y'$。
在第二种情况下，$yz = s(rr) = (z'r)s = z'y'$。继续利用命题 1.7 的性质 1，存在两个词 R 和 S，它们取自 A，以及一个整数 N，使得 $s = R(SR)^N$,$z'r = RS$ 和 $rr = SR$。此外，有 $|z'| = |r|$。

若 $|R| = |S|$，则 $r = R = S = z'$。
若 $|R| < |S|$，则 $|r| = \frac{1}{2}|SR| < |S|$，且 r 是 S 的后缀，也是 rr 的内部因子。根据引理 1.15，存在一个非空词 t 以及非零整数 α 和 β，使得$r = t^{\alpha+\beta}$、$R = t^{\beta}$ 和 $S = t^{2\alpha+\beta}$。由此可知 $z' = r$。
若 $|R| > |S|$，则 $|r| > |S|$，并且存在两个非空词 r_1 和 r_2，使得 $r = r_1 S = S r_2$。特别地，有 $|r_1| = |r_2|$。由于 R 以 r 和 r_1 结尾，因此可推出 $r_1 = r_2$，且 $z' = r_2 r_1 = r$。

现在，由于 $yz = srr = rrs = z'y'$，根据命题 1.7 的性质 3，存在两个关于 A 的词 t_1、t_2 以及三个整数 i、j、k，使得 $s = (t_1 t_2)^i t_1$、$r = (t_2 t_1)^j t_2$ 和 $r = (t_1 t_2)^k t_1$。于是，要么当 $j = k = 0$ 时有 $r = t_2 = t_1$，要么由于r 以 $t_2 t_1$ 和 $t_1 t_2$ 开头，这两个词必然 ´相等。在这两种情况下，都有 $y = sr = (t_1 t_2)^{i+j+1} = (t_2 t_1)^{i+j+1} = rs = y'$。

通过镜像，直接得到：

引理 2.3 设 y、y'、z 和 z' 是四个词。
若 $yz = zy'$ 和 $zy = y'z'$，则 $y = y'$。

引理 2.4 设 x、 x_1、 x_2 和 y 是四个词，满足 x、 x_1 和 x_2 均非空，并满足方程 ´、 $x = x_1x_2$ 和 $x_2yx = yxx_1$，那么存在一个词 t 和两个整数 $\alpha \geq 2$ 和 $\beta \geq 0$，使得 $x = t^\alpha$ 和 $y = t^\beta$。

注记 2.5 请注意，引理 2.4 的假设仅意味着 yx 是$(yx)^2$的内部因子。

证明。
根据命题 1.7 的性质 1，存在两个词 u 和 v 以及一个整数 q，使得 $x_2 = uv$, $yx = (uv)^q u$ 和 $x_1 = vu$。由于 $x = x_1x_2 = vuuv$，我们有 $q \geq 1$，且 yx 以 vu结尾。由此可得 $vu = uv$。根据命题 1.7 的性质 2，存在一个词 t 和两个整数 n 和 p，使得 $u = t^n$ 和 $v = t^p$。由此可得 $x = t^{2n+2p}$ 和$y = t^{(q-2)(n+p)+n}$。此外，由于 $x_2 = uv \neq \varepsilon$，由此可得 x 不是本原的。

□

注记 2.6 两个本原词的复合不一定是本原词。例如，若 $u = aba$ 且 $v = bab$，则 $uv = (ab)^3$。

命题 2.7 设 w 是一个本原词， $\underline{w}$ 是它的一个真 $|w| - 1$ 共轭词，且 $i \geq 1$ 和 $j \geq 1$ 是两个整数，那么 $w^i\underline{w}^j$ 是一个本原词。

证明。
设 r 和 s 是满足 $w = rs$ 和 $\underline{w} = sr$ 的词。根据 $\underline{w}$ 的定义，有 $s \neq \varepsilon$ 和 $r \neq \varepsilon$。反证法，假设对于某个整数 $n \geq 2$ 和某个本原词 v，有 $w^i\underline{w}^i = v^n$。我们将证明，大多数情况下会导致词 v 或 w 之一不是本原词：这使得我们在每一种情况下都与假设 `矛盾。

情形 1： $i = j = 1$

• 若 $n = 2$，则 $rs = sr$；根据注记 1.8， w 不是本原的。并且，若 $n \geq 4$ 是偶数，则 $w = v^{n/2}$，也就是说， `再次不是本原的。

• 若 $n = 2k+1$ 是奇数（且 $k \geq 1$），则存在两个长度相同（> 0）的词 v_1 和 v_2，使得 $v = v_1v_2$（特别地， $|v|$ 是偶数）且 $w = rs = v^kv_1$ 和 $\underline{w} = sr = v_2v^k$。
设 $0 \leq \ell \leq k$ 为满足 $|v^\ell| \leq |r| < |v^{\ell+1}|$的整数。存在 v 的一个前缀 v'_1 以及 v 的一个后缀 v''_2，使得 $r = v^\ell v'_1 = v''_2v^\ell$。设 v'_2和 v''_1为满足 $v = v'_1v'_2 = v''_1v''_2$的非空词。
◇ 若 $v'_1 = \varepsilon$，则 s 以 v_1 和 v_2开头。这意味着 $v_1 = v_2$，因此 v不是本原的。

◇ 若 $v'_1 \neq \varepsilon$ 且 $\ell \geq 1$，则由 $v^\ell v'_1 = v''_2v^\ell$可得， v^ℓ 是 $(v^\ell)^2$ 的内部因子。这意味着 v 是 v^2 的内部因子。根据引理 1.15 和注记 1.16， v 不是本原的。

◇ 如果 $v'_1 \neq \varepsilon$ 且 $\ell = 0$，那么 $s = v'_2v^{k-1}v_1 = v_2v^{k-1}v''_1$。

- 如果 $|v_2'| = |v_2|$，那么 $|v_1| = |v_1''|$。这意味着 $v_1 = v_1' = v_1''$且 $v_2 = v_2' = v_2''$。又因为 $r = v_1' = v_2''$，所以可得 $v_1 = v_2$，也就是说 v 非本原。
- 若 $|v_2'| \neq |v_2|$ 且 $k \geq 2$，则 v 是 v^2的内部因子。根据引理 1.15 和注记 1.16，v 不是本原的。
- 若$|v_2'| > |v_2| = \frac{1}{2}|v|$且 $k = 1$（也就是说 $n = 3$），那么我们也有 $|v_1''| > |v_1|$。这意味着 v_2 是 v_2' 的真后缀，而 v_1 是 v_1''的真前缀。由于$rs = v_1v_2v_1$ 与 $|r| = |v_1'| < |v_1|$，且由于 s 以 v_2v_1开头，我们可以推得 v_2v_1是 $(v_2v_1)^2$的内部因子。根据引理 1.15，v_2v_1 不是本原的。而根据推论 1.11，$v = v_1v_2$ 不是本原的。

- 若 $|v_2'| < |v_2| = \frac{1}{2}|v|$ 和 $k = 1$，则 $v = rv_2' = v_1''r$，其中 $|r| = |v_1'| > |v_2'|$。根据命题 1.7 的性质 1，存在两个词 R 和 S，以及一个整数 $q \geq 1$，使得$r = R(SR)^q$，$v_1'' = RS$ 且 $v_2' = SR$。因此 $v = R(SR)^{q+1}$。特别地，若 $R = \varepsilon$ 或若$S = \varepsilon$，则 v 不是本原的。

若 q 是奇数，设 ρ_1 和 ρ_2 为长度相同的词，使得 $R = \rho_1\rho_2$，$v_1 = (RS)^{(q+1)/2}\rho_1$ 且 $v_2 = \rho_2(SR)^{(q+1)/2}$。由于 s 以 $v_2'\rho_1 = SR\rho_1$ 的前缀 ′ 开头，又以 ρ_2SR 的前缀 ′ 开头，因此可得 $SR\rho_1 = \rho_2SR$。根据引理 2.4，R 和 S 是同一个词的幂。这意味着 v 不是本原的。

如果 q 是偶数，设 σ_1 和 σ_2 是长度相同的词，使得 $S = \sigma_1\sigma_2$，$v_1 = (RS)^{q/2}R\sigma_1$ 且 $v_2 = \sigma_2(RS)^{q/2}R$。由于 s 以 $v_1'' = R\sigma_1\sigma_2$ 结尾，且 $\sigma_2R\sigma_1$ 是 v_1 的后缀，由此可推出 ′，并且 $\sigma_1 = \sigma_2$。根据命题 1.7 的性质 2，R 和 σ_1，因而 $S = \sigma_1^2$，是同一个词的幂。这再次意味着 v 不是本原词。

情况 2：$i > j \geq 1$

因此，词 w^i 是 w 的某个幂和 v 的某个幂的公共前缀。

如果 $|w^i| \geq |v| + |w|$，根据命题 1.1，w 和 v 是同一个本原词的幂。因此得到 $w = v$。由于 v^n 以 $\underline{w}^j$ 结尾，由此可知 $w = \underline{w}$：矛盾。

如果 $|w^i| < |v| + |w|$ 那么$|\underline{w}^j| = |w^j| < |v|$ 且 $|w^i| = |v|^n - |\underline{w}^j| > |v|^{n-1} > |v|^{n-2} + |w|$。因此必然有 n´ecessairement $n = 2$。于是存在两个非空的词 w_1 和 w_2，使得$w = w_1w_2$ 且 $v = w^{i-1}w_1 = w_2\underline{w}^j$。这意味着 $i - 1 = j$，并且 $|w_2| = |w_1|$。由此可得 $w_2 = w_1$，且 w 不是本原的。

情况 3：$j > i \geq 1$

这种情况的解决方法与前一种相同。

情况 4：$i = j \geq 2$

如果 n 是偶数，则得到 $rs = sr$，且 w 不是本原的。

因此，$n = 2k + 1$ 为奇数，且 $k \geq 1$。设 v_1 和 v_2 是长度相同的词，满足 $v = v_1v_2$、$w^i = v^kv_1$ 以及 $\underline{w}^i = v_2v^k = v_2(v_1v_2)^k$。

若 $k \geq 2$，则$|\underline{w}^i| = |w^i| = (k + \frac{1}{2})|v|$。因此有 $|w^i| \geq 2|w|$，且 $|w^i| \geq 2|v|$，也就是说 $|\underline{w}^i| = |w^i| \geq |v|+|w| = |v|+|\underline{w}|$。如果 $k = 1$ 且 $i \geq 3$，也能得到不等式 ′，因为

$|w^i| = |w| + \frac{i-1}{i}(k + \frac{1}{2})|v|$。在这两种情况下，根据命题 1.1 和推论 1.3，可知 $\underline{w}$、w 和 v 都是同一个本原词的幂。因此得到$w = v = \underline{w}$。根据推论 1.9 和注记 1.10，w 将是非本原的，这就矛盾了。

如果 $k = 1$ 和 $i = 2$，那么 $w^2 = rsrs = v_1v_2v_1$ 以 $v_1\underline{w} = v_1sr$ 开头，因为 $|v_1| = \frac{1}{2}|v| < |rs|$。如果 $v_1 \neq r$，那么 sr 是$(sr)^2$的内部因子。根据引理 1.15 和注记 1.16，这意味着 $\underline{w}$ 不是本原的：矛盾。如果 $v_1 = r$，那么由于 $\underline{w}^2 = srsr$ 以 v_2 结尾，且 $|v_2| = |v_1|$，可得 $v_2 = r = v_1$，因此 v不是本原的：又一个矛盾。□

推论 2.8 设 r、s 和 z 是非空词，$i \geq 1$、$j \geq 1$ 和 $n \geq 2$ 是三个整数。如果 $(rs)^i(sr)^j = z^n$，那么 r、s 和 z 有相同的本原根。

证明。
根据命题 1.14，词 rs 和 sr 具有共轭的本原根。根据命题 2.7，这些本原根相等。因此，存在一个本原词 t 和一个整数 $\alpha \geq 2$，使得 $rs = sr = t^\alpha$。此外，根据命题 1.7 的性质 1，可得r 和 s 是同一个词的幂，而这个词只能是 t。再根据推论 1.4，z 也是 t 的幂。

□

命题 2.9 [9, 7, 1, 2, 12]
设 x、y 和 z 为非空词，且 m、n 和 q 为大于或等于 2 的整数。如果 $x^my^n = z^q$，那么 x、y 和 z 具有相同的本原根。

命题 2.9 只是下面命题的一个推论：

命题 2.10 设 x、y 和 z 是本原词，且 m、n 和 q 是大于或等于 2 的整数。若 $x^my^n = z^q$，则 $x = y = z$。

证明。
由于 x^m 是 z^q 的前缀，若 $|x^{m-1}| \geq |z|$，则根据命题 1.1，x 和 z 是同一个本原词的幂。因此，y 也如此。于是得到 $x = y = z$。同理，若 $|y^{n-1}| \geq |z|$，根据推论 1.3，x、y和 z 是同一个本原词的幂，再一次有 $x = y = z$。

因此 ($|x| \leq$) $|x^{m-1}| < |z|$ 和 ($|y| \leq$) $|y^{n-1}| < |z|$，也就是说 $|x^{m-1}| + |y^{n-1}| < 2|z|$要么 $|z^q| = |x^m| + |y^n| < 2|z| + |x| + |y| < 4|z|$。这意味着 $q = 2$ 或 3。
我们将证明这两种情形都会导致与 x, y 或 z 的本原性假设相矛盾。

必要时使用镜像，不失一般性，可假设 $|x| \geq |y|$.
情形 1：$q = 3$
因此，存在四个非空词 x_1、x_2、y_1 和 y_2，使得$z = x^{m-1}x_1 = x_2y_1 = y_2y^{n-1}$，其中 $x = x_1x_2$ 且 $y = y_1y_2$。由于 $|z| = |x_2| + |y_1| <$

$|x|+|y| \leq 2|x|$，我们必然有 $m=2$。设 y_1' 为 y_1 的前缀，使得 $x_1x_2 = x_2y_1'$。根据命题 1.7 的性质 1，存在两个词 r 和 s，以及一个整数 ℓ，使得 $x_2 = (rs)^\ell r$、$x_1 = rs$ 且 $y_1' = sr$。

由此可得 $x = (rs)^{\ell+1}r$ 和 $z = xx_1 = (rs)^{\ell+1}rrs = x_2y_1 = (rs)^\ell ry_1$，且 $y_1 = srrs$。若 $r = \varepsilon$ 或 $s = \varepsilon$，则可得 x、y 和 z 不是本原的：这与假设相矛盾。

由于 $|x| \geq |y| > |y_1|$，我们有 $\ell \geq 1$。此外，由于 $|x_2| + |y_1| = |z| = |y_2y^{n-1}| \geq |y_1| + 2|y_2|$，因此可得 $2|y_2| \leq |x_2|$，且 y_2 是 x_2的前缀。因此，存在一个整数 $0 \leq q \leq \ell$和两个词 $t_1 \neq rs$ 与 $t_2 \neq \varepsilon$，使得 $t_1t_2 = rs$ 且 $y_2 = (rs)^qt_1$，也就是说 $x_2 = y_2t_2(rs)^{\ell-q-1}r$。此外，$z$ 以 $y_2y_1 = (rs)^qt_1srrs$ 和 $x = (rs)^{\ell+1}r$开头。

由于 $2|y_2| \leq |x_2|$，因此有 $q < \ell$，且 z 以 $(rs)^qt_1srrs$ 和 $(rs)^qrsrsr$ 开头。这意味着 $t_1sr = rst_1$。根据命题 1.7 的性质 3，存在两个词 u_1、u_2，定义在 A 上，以及三个整数 α、β、γ，使得 $t_1 = (u_1u_2)^\alpha u_1$、$s = (u_2u_1)^\beta u_2$ 和 $r = (u_1u_2)^\gamma u_1$。由于 z 以 rs 结尾，因此也以 u_1u_2 结尾；又由于它以 y_1y_2 结尾，因此也以 u_2u_1 结尾，由此可得 $u_1u_2 = u_2u_1$。根据命题 1.7 的性质 2，词 u_1 和 u_2 是同一个词的幂。因此，r 和 s 也是如此。由此可知，x、y 和 z 都不是本原的，这与假设矛盾。

情况 2：$q = 2$

由于 z是本原的，对于所有整数 $2 \leq m' \leq m$和 $2 \leq n' \leq n$，有 $|x^{m'}| \neq |z|$，$|y^{n'}| \neq |z|$ 。

- 若 $|x^m| < |z|$，则存在两个非空词 y_1 和 y_2，使得 $z = x^my_1 = (y_2y_1)^{n-1}y_2$，其中 $y = y_1y_2$。由于 $|x^m| \geq |x^{m-1}| + |y| \geq |x| + |y_2y_1|$，根据命题 1.1，$x$ 和 y_2y_1 是同一个词的幂。由于 x 和 y 是本原的，且根据推论 1.11，可得 $x = y_2y_1$ 和 $z = (y_2y_1)^my_1 = (y_2y_1)^{n-1}y_2$。这意味着$m = n-1$、$y_1 = y_2$和 y 不是本原的，矛盾。
- 若 $|x^m| > |z|$，则存在两个非空词 x_1 和 x_2，使得 $z = (x_1x_2)^{m-1}x_1 = x_2y^n$，其中 $x = x_1x_2$。

若 $|y^n| \geq |x| + |y|$，那么与前一种情况一样，可得 $y = x_2x_1$，进而得到 $x_1 = x_2$，且 x不是本原的：矛盾。

因此有 $|y^n| < |x| + |y|$。由于 $|z| = |x_2y^n| \leq |x_2| + 2|x|$，可得 $m = 2$或 $m = 3$。设 Y 为 y^n 的前缀，且满足 $x_1x_2 = x_2Y$。根据命题 1.7 的性质 1，存在两个词 r 和 s，以及一个整数 ℓ，使得 $x_2 = (rs)^\ell r$，$x_1 = rs$ 且$Y = sr$。特别地，可得 $x = (rs)^{\ell+1}r$。

有 $r \neq \varepsilon$ 且 $s \neq \varepsilon$，否则 x 将不是本原的。

◇ 若 $m = 2$，那么由于 $z = xx_1 = (rs)^\ell rsrrs = x_2y^n$，可得 $y^n = srrs$。根据推论 2.8，这意味着 x 不是本原的：矛盾。

◇若 $m = 3$，那么由于 $z = x^2x_1 = x_2y^n$，可得 $y^n = sr(rs)^{\ell+1}rrs = sr\,x\,rs$。由于 $|y^n| < |x| + |y|$，因此有 $|y| > 2|r| + 2|s|$。但是 $|(rs)^{\ell+1}r| = |x| = |y^n| + 2|r| + 2|s| \geq |y|$。这意味着 $\ell \geq 1$。

- Si $n \geq 3$ 那么 x 是 rs 的某个幂与 y的某个幂的公共因子

满足 $|x| = |(rs)^{\ell+1}r| \geq 2|rs|$ 并且 $|x| > |y^{n-1}| \geq 2|y|$ 也就是说 $|x| \geq |rs| + |y|$。根据推论 1.6， y 不是本原的，因为 $|y| > |rs|$。
- 若 $n = 2$ 和 ℓ 是奇数，设 ρ_1 和 ρ_2 是长度相同的词，使得 $r = \rho_1\rho_2$和 $y = sr(rs)^{(\ell+1)/2}\rho_1 = \rho_2(sr)^{(\ell+1)/2}rs$。由此可推出 $sr\rho_1 = \rho_2 sr$。根据引理 2.4， r 和 s 是同一个词的幂。这意味着 x 不是本原词：矛盾。

- 若 $n = 2$ 和 ℓ 是偶数，如同前一种情形，设 σ_1 和 σ_2 是长度相同的词，使得 $s = \sigma_1\sigma_2$，同样可得 $y = sr(rs)^{\ell/2}r\sigma_1 = \sigma_2 r(sr)^{\ell/2}rs$。由此可推出 $\sigma_1 = \sigma_2$ 和 $\sigma_1 r = r\sigma_1$。根据命题 1.7 的性质 2， r 和 σ_1，因此 $s = \sigma_1^2$，是同一个词的幂。这意味着 y 不是本原词：又一个矛盾。 □

推论 2.11 若 x 和 y 是两个不同的本原词，则 $x^m y^n$ 对于所有大于 2 的整数 m和 n 都是本原词。

3 本原态射的刻画

命题 3.1（ [11]中的定理 5）
本原态射是单射。

证明。
设 h 是一个从 A^* 到 B^* 的本原态射
首先注意， h 不可能是擦除态射。事实上，若情况如此，我们便可找到 α、$\beta \in A$，使得 $h(\alpha) = \varepsilon$ 且 $h(\beta) \neq \varepsilon$。那么 $\beta\alpha\beta$ 确实是一个本原词，但它在 h 下的像并非如此，因为$h(\beta\alpha\beta) = (h(\beta))^2$。

设 x 和 y 是 A^+ 中的两个词，满足 $h(x) = h(y)$。不失一般性，假设 $|x| \leq |y|$。

由于 h 是本原的，且 $h(xy) = h(x)^2$ 以及 $h(xyy) = h(x)^3$, ，词 xy 和xyy 都不是本原词。

换言之，我们可以将 $xy = u^n$ 和 $xyy = v^m$ 写成非空本原词 u和 v 的形式，并取两个整数 n、$m \geq 2$。
若 $m = 2$，那么，由于 $|x| \leq |y|$，可以找到两个非空词 y_1 和 y_2，使得$y = y_1y_2$ 且 $v = xy_1 = y_2y$。这意味着 x 是 y的真因子（$\neq y$）。由于h 不可擦除，因此得到 $|h（x）| < |h（y）|$。所以这种情况不可能发生。
若 $n = 2$，那么，由于 x 不能是 y的真因子，再次推出 $x = y$，从而证明了单射性。

因此有 $n, m \geq 3$。特别地，我们得到 $|u| \leq \frac{1}{3}(|x| + |y|)$ 和 $|v| \leq \frac{1}{3}(|x| + 2|y|)$。于是 $|u| + |v| \leq \frac{2}{3}|x| + |y| < |x| + |y|$。这意味着 u^n和 v^m有一个公共前缀

其长度大于或等于 `a $|u|+|v|$。根据命题 1.1，由于 u 和 v 是本原的，我们得到 $u=v$。

由此可得 $y=u^{m-n}$ 和 $x=u^{2n-m}$。根据等式 ´，´(h) x($=h$)，可推出 y和 $2n-m=m-n$。

□

注释 3.2 命题 3.1 还有另一种证明，见 ´（命题 5.2）。当 $[3]$(h)x($=h$)，且 y和 x 的本原根不同时，该证明会用到推论 2.11。在这种情况下， y 是一个本原词，但它的像不是本原词。

注释 3.3 2-本原均匀态射是单射。

事实上，若 h 是均匀的，那么有 $h(x)=h(y)$ 且 $x\neq y$，意味着存在一个来自 x_i 的字母 x，以及一个来自 y_i 的字母 y，使得 $x_i\neq y_i$ 且 $h(x_i)=h(y_i)$。因此 x_iy_i 是本原的，而 $h(x_iy_i)$并非如此。

命题 3.4（ [11]中的定理 5）

态射 h从 A^* 到 B^* 是本原的，当且仅当 $h(A)$ 是纯码。

证明。

(⇐) 假设 $h(A)$ 是纯码，并设 x 是 A^+的一个本原词。若 $h(x)=u^k$，其中 u 是 A^+ 的一个本原词，则有 $u^k\in h(A)^*$；又由于 $h(A)$ 是纯的，因此有 $u\in h(A)$。于是存在一个词 $y\in A^+$，使得 $u=h(y)$。这意味着 $h(x)=h(y^k)$。由于 h 是单射（$h(A)$ 是一个码），因此有 $x=y^k$。最后，由于 x ´是本原的，得到 $k=1$ 且 $h(x)$ 是本原的。(⇒) 假设 h 是本原的。设 $w=h(v)$ 是 $h(A)^*$ 中的一个词，且 $r=\rho(v)$ $s=\rho(w)$。设 n、$m\geq 1$ 是满足 $v=r^n$ 和 $w=s^m$的整数。由于 s 和 $h(r)$ 都是本原的，根据推论 1.4，由等式 $s^m=h(r)^n$，可得 $s=h(r)\in h(A)$。

□

引理 3.5 设 f 是从 $\{a,b\}^*$ 到 B^*的一致态射。

α、β、γ和 δ是 $\{a,b\}$中的字母，且满足 $\alpha\neq\beta$。

如果 $f(\alpha)f(\beta)=Xf(a)Y$，或者如果 $f(\alpha)f(\beta)=Xf(b)Y$，其中 X是 $f(\gamma)$的非空后缀，且 Y是 $f(\delta)$的非空前缀，那么 f 不是本原的。

更准确地说，存在一个长度小于或等于二的本原词，其像不是本原的。

证明。

我们将证明，词 $f(a)$、 $f(b)$、 $f(ab)$ 或 $f(ba)$ 中至少有一个不是本原词 .

由对称性，我们只需处理方程 $f(\alpha)f(\beta) = Xf(b)Y$。

注意，若曾有 $\alpha = \beta = b$，那么 $f(b)$ 就会是 $f(b)f(b)$ 的内部因子。根据引理 1.15， $f(b)$ 就不是本原的。

利用镜像对称性，不失一般性，可以假设 $\alpha = a$ 和 $\beta = b$。

若 $\delta = b$，那么 $f(b)$ 是 $f(b)f(b)$ 的内部因子。根据引理 1.15， $f(b)$ 不是本原的。因此我们假设 $\delta = a$。

若 $\gamma = a$，那么 $f(ab)$ 是 $f(ab)f(ab)$ 的内部因子。根据引理 1.15， $f(ab)$ 不是本原的。因此我们假设 $\gamma = b$。

• 如果 $|X| = |Y|$，则有 $2|X| = |XY| = |f(b)|$。由于 $f(b)$ 以 X 和 Y 结尾，因此得到 $X = Y$。又由于 $f(b)Y$ 以 $f(b)$ 结尾，所以 $f(b) = X^2$： $f(b)$ 不是本原的。

• 如果 $|X| > |Y|$，由于 $f(a)$ 以 Y 和 X 开头，存在一个非空词 X'，使得 $X = YX'$。由于 $|XY| = |f(a)| = |f(b)|$，且 $f(b)Y$ 以 $XY = YX'Y$ 和 $f(b)$ 结尾，因而也以 X 结尾，因此得到 $X'Y = YX'$。根据命题 1.7 的性质 2，这意味着 X' 和 Y 是同一个词的幂。这表示 $f(b) = YX'Y$ 不是本原的。

• 若 $|X| < |Y|$，由于 $f(b)$ 以 X 和 Y 结尾，因此存在一个非空词 Y'，使得 $Y = Y'X$。由于 $|XY| = |f(a)| = |f(b)|$，且 $f(b)Y$ 以 XY 和 $f(b)$ 结尾，可得 $f(b) = XY'X$。

由此可知， $f(a) = (XX)Y'$，且 $f(a)$ 以 $Y = Y'X$ 开头。因此存在一个词 Z，使得 $f(a) = Y'(XZ)$，其中 $|Z| = |X|$。

取 $y = XY'$、 $y' = Y'X$、 $z = X$ 和 $z' = Z$，根据引理 2.3，可得 $XY' = Y'X$。根据命题 1.7 的性质 2，这意味着 X 和 Y' 是同一个词的幂。这意味着 $f(a)$ 不是本原的。

□

命题 3.6（ [11]中的定理 12）

设 $n \geq 2$ 是一个整数。存在一些二元态射，它们直到 n 都是本原的，但本身并非本原。

证明。

考虑从 $\{a, b\}^*$ 到 $\{a, b\}^*$ 的态射 f，其定义为 $f(a) = aba$ 和 $f(b) = (baa)^{n-1}b$。

有 $f(a^n b) = (aba)^{n-1}aba\,(baa)^{n-1}b = (aba)^{n-1}ab \mid (aba)^{n-1}ab$。

首先注意到， $f(a)$ 以 a 开头并以其结尾，而 $f(b)$ 以 b 开头并以其结尾。这意味着 f 是单射。

事实 1：如果 $f(b) = sf(a)p$ 与词的像的一个后缀以及词的像的 p 前缀，那么，由于 $f(b) = ba(aba)^{n-2}ab$，必然有 $s = ba(aba)^{\alpha}$ 和 $p = (aba)^{\beta}ab$，其中 $\alpha + \beta = n - 3$。这意味着， s 是 $f(a^{\alpha+1})$ 的一个后缀，而 p 是 $f(a^{\beta+1})$ 的一个前缀。

事实 2：不可能有 $sf(b) = f(b)p$，使其同时与词的像的一个真后缀（$\neq f(b)$）以及词的像的真 ′缀相对应。事实上，方程 $sf(b) = sb(aab)^{n-2}aab = b(aab)^{n-2}aabp$ 意味着，方程中每个词的至少两个因子必须对齐。这意味着 p 会以 $(aab)^{\ell}aab$ 开头，其中 ℓ 为整数；这是不可能的。

若 $f(w) = u^k$ 对于某个整数 $k \geq 2$，且 w 是本原的，则 w 至少包含一次字母 b。如果两个出现位置之一 u^{k-1} 包含 $f(b)$，根据事实 1 和 2，则$|w| \geq 1 + n$。否则，这意味着 $|f(b)| > |u^{k-1}|$。但 u 中确实存在一个因子 $f(a)$。同样根据事实 1，可再次得到 ` $|w| \geq 1 + n$。 □

命题 3.7（ [11]中的定理 10）
二元均匀态射是本原的，当且仅当它是 2-本原的。

证明。
由于蕴含关系 ′显然成立，我们只需考察逆命题 `，并通过反证法 ′证明。

设 $L \geq 1$ 为一个整数，并设 f 是从 $\{a, b\}^*$ 到 B^*的一个 L-一致态射。
设 w 是一个长度为 n 的本原词。假设 $f(w)$ 不是本原词，也就是说，存在一个非空词 u 和一个整数 $k \geq 2$，使得 $f(w) = u^k$。不妨考虑其本原根，因此可以不失一般性地假设 u 是本原词。还假设 w 的长度（因而 $f(w)$ 的长度）最小。若 $n \leq 2$，证明即告完成。因此，我们将对 $n \geq 3$ 使用反证法。

根据注释 3.3，若 f 不是单射，则 f 不是 2-本原。这也就完成了证明。

有 $|f(w)| = |w| \times L = k \times |u|$。由于 f 是单射， $|u|$ 不可能是 L 的倍数（也就是说， k 是 $|w|$的一个因数），否则 w 就不是本原词。
情形 1： $|u| < L$
设 $i \geq 2$ 为满足 $w_{[i]} = w_{[1]}$的最小索引。若不存在这样的索引，只需考虑 $f(w)$的镜像 ′。

由于 $f(w_{[i]})$ 是 u^k的因子，因此存在 u的一个后缀 u_1 、 u 的一个前缀 u_2 以及一个整数 $j \geq 0$，使得 $f(w_{[i]}) = u_1u^ju_2$。
若 $u_1 = \varepsilon$，则 $f(w_{[1..i-1]})$ 是 u 的幂：这与关于 w最小长度的假设 `相矛盾。

若 $u_1 \neq \varepsilon$，则 $f(w_{[1]})$ 的前缀 u ′是 uu的内部因子。这意味着 u 不是本原的：这与关于 u 的假设 ``相矛盾。
情况 2： $|u| > L$
情况 2.1： $k = 2$
这意味着 $n = 2p + 1$ 是奇数。
Il e存在两个非空词 x和 y，使得 $u = f(w_{[1..p]})x = yf(w_{[p+2..n]})$， $f(w_{p+1}) = xy$

且 $|x| = |y|$。
由此可得， $f(w_{[1]})$ 以 y 开头，而 $f(w_{[n]})$ 以 x 结尾。
如果 $x = y$ （当 $w_{[1]} = w_{[p+1]}$ 或 $w_{[n]} = w_{[p+1]}$ 时即为此情况），那么 $f(w_{[p+1]})$ 不是本原的：证明完毕。因此， $x \neq y$、 $w_{[1]} = w_{[n]} \neq w_{[p+1]}$ ，并且 $f(w_{[1]}) = f(w_{[n]}) = yx$。

因此，要么 $w_{[1]} = w_{[n]} = a$ 且 $w_{[p+1]} = b$ ，要么 $w_{[1]} = w_{[n]} = b$ 且 $w_{[p+1]} = a$。这两种情况是对称的，因此只讨论第一种。
设 ℓ_1 是满足 $w_{[1+\ell_1]} = b$ 的最小整数，并设 ℓ_2 是满足 $w_{[p+1+\ell_2]} = a$ 的最小整数。这样的整数确实存在，并且有 $\ell_1 \leq p$ 和 $\ell_2 \leq p$。
词 uy 以 $f(a^{\ell_1})f(b) = (yx)^{\ell_1}xy$ 开头，并以 $y\,f(b)^{\ell_2-1}f(a) = (yx)^{\ell_2}yyx$ 开头。
若 $\ell_1 = \ell_2$，则 $x = y$ （且 $f(b)$ 不是本原的）：这与当前情况相矛盾。
若 $\ell_1 \neq \ell_2$，则 $xy = yx$ 且 $f(b)$ 不是本原的：这与假设矛盾。

情况 2.1： $k \geq 3$

设 i_2 是满足 u 为 $f(w_{[1..i_2]})$ 的前缀的最小索引，并设 i_3 是满足 uu 为 $f(w_{[1..i_3]})$ 的前缀的最小索引。
存在词 p_2、 s_2、 p_3和 s_3，使得 $f(w_{i_2}) = p_2 s_2$且 $f(w_{i_3}) = p_3 s_3$。根据 i_2 和 i_3的定义，不可能有 $p_2 = \varepsilon$ 或 $p_3 = \varepsilon$。根据 w 的本原性或 w长度的最小性，也可排除 $s_2 = \varepsilon$ 或 $s_3 = \varepsilon$的情况。

还要注意， $|p_2| = |p_3|$ （或 $|s_2| = |s_3|$）将意味着 $|u|$ 是 L 的倍数，从而意味着 $p_2 = \varepsilon$；这是我们刚刚排除的情形。
设 X 为满足 Xp_2 是 u 的长度为 L 的后缀的词，并设 Y 为满足 s_2Y 是 u 的长度为 L 的前缀的词。因此有 $Xf(w_{[i_2]})Y = f(w_{[1]})f(w_{[n]})$。
若 $w_{[1]} \neq w_{[n]}$，根据引理 3.5，存在一个长度小于或等于二的本原词，其像不是本原的：证明结束。
若 $w_{[1]} = w_{[n]} = w_{[i_2]}$，则 $f(w_{[i_2]})$ 是 $f(w_{[i_2]})f(w_{[i_2]})$ 的内部因子： $f(w_{[i_2]})$ 不是本原的。

同样，若 $w_{[1]} = w_{[n]} = w_{[i_3]}$，则可得 $f(w_{[i_3]})$ 是 $f(w_{[i_3]})f(w_{[i_3]})$ 的内部因子，因此它不是本原的。
因此，我们还需考虑 $w_{[1]} = w_{[n]} \neq w_{[i_2]} = w_{[i_3]}$的情形。不失一般性，可以假设前两个 $'$相等于 a ，后两个 $'$相等于 b。
设 ℓ_1 是满足 $w_{[\ell_1]} = a$的最大整数。这样的整数存在，且有 $1 \leq \ell_1 \leq i_2 - 1$。于是考虑第一个词中的因子 $f(w_{[\ell_1]})f(w_{[\ell_1+1]}) = f(a)f(b)$ 及其在第二个词中的出现。根据引理 3.5，存在一个长度小于或等于二的本原词，其像不是本原的。
□

4 本原态射与幂 $k \geq 2$

引理 4.1（ [3]中的命题 5.4）
设 f 是从 A^* 到 B^* 的单射态射，且 w 是 A^+ 中的一个本原词。假设 $f(w) = u^m$，其中 $u \neq \varepsilon$ 是本原的，且 $m \geq 1$ 是一个整数。对于任意词 $v \in A^+$，有 $f(v) = u^\ell$，其中 $\ell \geq 1$ 是一个整数，当且仅当 v 是 w 的幂。

证明。
由于 $f(v^m) = u^{\ell m} = f(w^\ell)$，且 f 是单射，我们可由此推出 $v^m = w^\ell$。根据推论 1.4，可得 v 和 w 是同一个词的幂。这个词只能是 w 本身，因为它是本原的。
□

下面的性质针对 [10] 中不含平方的态射进行表述。但它对任意整数 $k \geq 2$ 都成立。

引理 4.2 设 f 是从 A^* 到 B^* 的态射，并设 $k \geq 2$ 是一个整数。
若 f 是无幂 k，则 f 是双定点。因此它是一个单射态射。

证明。
例如，若 f 不是前缀态射，则存在两个不同的字母 x 和 y，使得 $f(x)$ 是 $f(y)$ 的前缀。在这种情况下，不含幂 k 的词 $x^{k-1}y$ 的像会包含 $f(x)^k$。

同样，若 f 不是后缀态射。
□

推论 4.3 无幂 $k \geq 2$ 的二元均匀态射是本原的。

证明。
根据逆否命题，假设定义在 $\{a, b\}$ 上的 f 一致态射 d´ 不是本原的。根据命题 3.7，有 $f(x) = u^m$，其中 $x \in \{a, b, ab, ba\}$、u 是一个非空词，且 $m \geq 2$ 是一个整数。

因此有 $f(x^{k-1}) = u^{m(k-1)}$。但是 $x^{k-1} \in \{a^{k-1}, b^{k-1}, (ab)、(ba)^{k-1}\}$ 是一个不含幂 k 的词，而 $m(k-1) \geq k$： f 不不含幂 k。
□

以下引理针对 [11] 中不含平方的态射表述（推论 7）。但它对任意整数 $k \geq 2$ 都成立（证明基本相同）。

引理 4.4 存在一些本原态射，它们并非对任意整数 $k \geq 2$ 都无幂的 k。

证明。
设 $k \geq 2$ 为一个整数。考虑从 $\{a, b, c\}^*$ 到 $\{a, b, c\}^*$ 的态射 f，其定义为 $f(a) = ac^k$, $f(b) = bc^k$ 和 $f(c) = abc^k$。

假设存在一个词 w，使得 $f(w)$ 不是本原的。我们可以将 $f(w) = u^p$写成一个非空词 u 和一个整数 $p \geq 2$的形式。
根据长度准则，词 u 必然以 c^k 结尾（否则 u 只会包含 c，这是荒谬的）。

这意味着存在一些整数 $0 \leq i_q \leq |w|$，使得 $i_0 = 0$ 且 $u = f(w_{[i_{q-1}+1..i_q]})$ 对所有 $1 \leq q \leq p$ 都成立。由于 f 是一个前缀态射，因此 f 是单射。这意味着所有 $w_{[i_{q-1}+1..i_q]}$ 都相等，从而 $w = (w_{[1..i_1]})^p$： w 不是本原的。 □

定义整数 $(t_k)_{k\geq 2}$，令 $t_2 = 3$、$t_3 = 4$；若 $k \geq 4$ 为偶数，则 $t_k = \frac{k^2}{2}$；若 $k \geq 5$ 为偶数，则 $t_k = k \times (k-1)/2 + 2$。特别地，这意味着当 $k \geq 4$ 时，有 $t_k = k\lfloor \frac{k}{2} \rfloor + 2$（模 2 的 k）。

命题 4.5 *[13]* 设 $k \geq 2$ 为一个整数。如果一个二元态射不含幂k 直到 t_k，那么它是本原的。

注记 4.6 界 t_k 是最优的，并且改进了 Leconte 在其论文中给出的界，该界为 $k \times (k+1)/2$。

推论 4.7 不含幂 k 的二元态射是本原的。

命题 4.5 的证明基于 Lentin 和 Schützenberger 的一个结果:

引理 4.8 [6] 定义在 $\{a, b\}$ 上的态射 f是本原的，当且仅当对所有词 $w \in a^*b \cup ab^*$， $f(w)$ 都是本原的。

引理 4.9 设 w 为一个本原词，并设 $j \geq 1$ 为一个整数。
设 k_j 为使得 w^j 包含一个 k_j 幂的最大整数。则有 $k_j \leq \max\{j, k_1, k_2, k_3\}$。特别地，存在一个整数 $j_0 \geq 1$，使得当 $j \geq j_0$ 时， $k_j = j$。

注记 4.10 换言之，存在一个整数 $j_0 \geq 1$，使得当 $j \geq j_0$ 时， w^j 不含有 $j+1$ 幂。

证明。
当 $j = 1$、$j = 2$ 或 $j = 3$ 时，结果是显然的。
我们将对 $q \geq 4$ 通过归纳法证明该性质。
假设对于某个整数 $q \geq 4$， $k_{q-1} \leq \max\{q-1, k_1, k_2, k_3\}$。
若 $k_q = k_{q-1}$，则可立即得到 $k_q \leq \max\{q-1, k_1, k_2, k_3\} \leq \max\{q, k_1, k_2, k_3\}$。
若 $k_q > k_{q-1}$，则令 v 为满足 $w^q = pv^{k_q}s$的非空词。根据 k_q的定义，词 v 是本原的。我们有 $|p| < |w|$，否则 v^{k_q} 将成为 w^{q-1}的因子；这与假设 $k_q > k_{q-1}$相矛盾。同样，我们必然有 $|s| < |w|$。

这意味着 $|v^{k_q}| > |w^{q-2}| \geq 2|w|$。此外，我们有 $|v^{k_q}| \geq |v^{k_q-1}| + |v| \geq 2|v|$。因此，词 v^{k_q} 是 v 的某个幂和 w 的某个幂的公共因子，其长度大于或等于 ´ ´ ` $|v| + |w|$。

根据推论 1.6，存在两个词 t_1 和 t_2，使得 v 是 t_1t_2的幂，且 w 是 t_2t_1的幂。由于 v 和 w 是本原的，因此可 deduire 得到 $v = t_1t_2$和 $w = t_2t_1$。如果 $t_1 \neq \varepsilon$，则得到 $k_q = q - 1$；如果 $t_1 = \varepsilon$，则得到 $k_q = q$。也就是说$k_q \leq \max\{q, k_1, k_2, k_3\}$ □

注 4.11 k_2 不能被 $\{2, k_1\}$ 控制这一事实，可以通过使用例如 $w = ca(bc)^n b$ 以及 $n \geq 2$来证明。类似地， k_3 不能被$\{3, k_1, k_2\}$ 控制这一事实，可以通过使用例如 $w = bcab(abcab)^n abca$ 以及 $n \geq 2$ 来证明。

命题 4.12 一个不含幂 k 且满足 $k \geq 5$ 的态射是本原的。

证明。
用逆否命题，假设态射 $f\colon A^* \to B^*$ 不是本原的。
设 w 是一个本原词，使得 $f(w) = u^n$ 且满足 $n \geq 2$。
根据性质 4.9，存在一个整数 j_0，使得对于任意 $k \geq j_0$， w^k 中的最大幂都小于或等于 k。换言之，词 w^k 因此不含幂 $k + 1$

但是 $f(w^k) = u^{n\times k}$ 且满足 $n \times k \geq k + 1$。这意味着，对于任意 $k \geq \max\{5; j_0\}$， f并非不含幂 $k + 1$。根据性质 1.19，对于任意整数 $5 \leq k \leq \max\{5; j_0\}$， f 因此并非不含幂 k。
□

命题 4.13 无幂 k 且满足 $k \geq 3$ 的一致态射是本原的。

证明。证明与命题 4.12 的证明相同，但使用性质 1.18。
□

5 无平方态射

引理 5.1（ [3]中的引理 4.3）
设 f 是从 A^* 到 B^* 的态射，且 a 和 b 是 A中的两个字母。假设存在 B^*中两个不同时为空的词 X和 Y，使得 $f(a) = Xf(b)Y$。
如果 X是 $f(a)$的非空后缀，或者如果 Y是 $f(a)$的非空前缀，那么 f不是 3-无平方的。

证明。
如果 $b = a$那么 $f(a)$ 是 $(f(a))^2$ 的内部因子。根据引理 1.15 和注记 1.16，$f(a)$ 不是本原的，也就是说 $f(a)$ 含有一个平方。

如果 $b \neq a$并且 X是 $f(a)$的非空后缀，那么 $f(aba)$含有 $Xf(b)Xf(b)$。如果 $b \neq a$并且 Y是 $f(a)$的非空前缀，那么 $f(aba)$含有 $f(b)Yf(b)Y$。 □

引理 5.2（ [3]中的命题 5.3）
设 f是从 A^*到 B^*的单射态射，且 w是 A^+中的一个词，长度为 $n \geq 2$。假设 $f(w) = u^m$，其中 $u \neq \varepsilon$是本原的，且 $m \geq 2$。
如果存在两个整数 $1 \leq i_1 < i_2 \leq n$和一个词 $v \in B^*$，使得 $f(w_{[1..i_1]}) = u^{\ell_1}v$且$f(w_{[1..i_2]}) = u^{\ell_2}v$，其中 $0 \leq \ell_1 < \ell_2 \leq m$是整数，那么 w不是本原的。

证明。
设 $w_r = w_{[1..i_1]}w_{[i_2+1..n]} \neq \varepsilon$。有 $f(w_r) = u^{m-(\ell_2-\ell_1)}$，其中 $|w_r| < |w|$。此外，$f((w_r)^m) = f(w^{m-(\ell_2-\ell_1)})$。由于 f是单射，由此可得$(w_r)^m = w^{m-(\ell_2-\ell_1)}$。
根据推论 1.4，可知 w_r和 w是同一个词的幂。由于 $|w_r| < |w|$，因此可以推得 w不是本原的。 □

命题 5.3 [3, 10, 11]
没有平方的态射是本原的。

证明。
设 f是一个从 A^*到 B^*的不含平方的态射。根据引理 4.2，可知 f是单射。设 w是一个长度为 n的词，使得 $f(w) = u^m$，其中 u是本原词，$m \geq 2$是一个整数。用反证法，假设 w是本原的。此外，假设其长度最小。根据引理 5.2，例如，这意味着不存在整数 $i \leq j$使得 $|f(w_{[i..j]})|$是 $|u|$的倍数。

还需注意，由于 f不含平方，对于 w中的每个字母 $w_{[i]}$，都有 $|f(w_{[i]})| < 2|u|$，否则，$f(w_{[i]})$就会包含 u的某个共轭的平方。
情形 1：$|u^j| < |f(w_{[1]})|$，其中 $j \geq 1$为一个整数。
在这种情况下，正如刚才所指出的，u^j是 $f(w_{[1]})$的一个前缀；又由于后者不含平方，因此有 $j = 1$。
存在一个 B^+中的词 V_1，使得 $f(w_{[1]}) = uV_1$且 $V_1f(w_{[2..n]}) = u^{m-1}$。
由于 V_1是 u^{m-1}的一个前缀，且 $|f(w_{[1]})| < 2|u|$，因此有 $|V_1| < |u|$，也就是说，V_1是 u的一个前缀。这意味着 V_1是 $f(w_{[1]})$的一个边界。
如果 $|f(w_{[n]})| < |u|$，则存在一个词 V'，使得 $f(w_{[1]}) = uV_1 = V'f(w_{[n]})V_1$，其中 V_1是 $f(w_{[1]})$的固定前缀。根据引理 5.1，f不可能是无平方的：这与假设矛盾。因此 $|f(w_{[n]})| > |u|$。此外，由于 $f(w_{[n]}w_{[1]})$包含 uu，且 f是无平方的，我们可以推出 $w_{[n]} = w_{[1]}$。

设 V_2为满足 $u = V_1V_2$的词。我们得到 $f(w_{[1]}) = uV_1 = V_1V_2V_1$（因此特别地，$V_2$非空）。但 $f(w_{[1]}) = f(w_{[n]})$以 $u = V_1V_2$结尾。根据注记 1.8，这意味着 u不是本原的：这与假设相矛盾。

情况 2: $|u^j| < |f(w_{[n]})|$，其中 $j \geq 1$ 是一个整数。

这一情形可按与情形 1 完全相同的方式处理。

情况 3: $|u| > |f(w_{[1]})|$ 且 $|u| > |f(w_{[n]})|$。

设 i 是使得 $|f(w_{[1..i]})| > |u|$ 成立的最小整数。存在 u 的一个非空后缀 V_1，以及 u^{m-1} 的一个非空前缀 V_2，使得 $u = f(w_{[1..i]})V_1$，$f(w_{[i]}) = V_1V_2$，且 $u^{m-1} = V_2f(w_{[i+1..n]})$。

情况 3.1: $|V_2| > |f(w_{[1]})|$。

设 ℓ 是使得 $|f(w_{[1..\ell]})| > |V_2|$ 成立的最小整数。存在 f 的一个前缀 V_2'，使得 $f(w_{[\ell]})$ 是 V_2 的后缀。由于 $f(w_{[i]})f(w_{[\ell]})$ 包含 $(V_2')^2$,，且 f 不含平方子串，因此必有 $w_{[\ell]} = w_{[i]}$。于是，$f(w_{[i]}) = V_1V_2 = V_1f(w_{[1..\ell-2]})f(w_{[\ell-1]})V_2'$，其中 V_2' 是 $f(w_{[i]})$ 的前缀。根据引理 5.1，f 将含有平方子串，这与假设矛盾。

情况 3.2: $|V_2| \leq |f(w_{[1]})|$。

由于 $f(w_{[i]})f(w_{[1]})$ 包含 $(V_2)^2$，这意味着 $w_{[1]} = w_{[i]}$，因此 V_2 是 $f(w_{[i]})$ 的后缀。

若 $|V_1| > |f(w_{[n]})|$，则存在一个非空词 V_1'，使得 $V_1 = V_1'f(w_{[n]})$。于是得到$f(w_{[i]}) = V_1'f(w_{[n]})V_2$。根据引理 5.1，$f$ 将不是无平方的：这与假设矛盾。

若 $|V_1| \leq |f(w_{[n]})|$，由于 $f(w_{[n]})f(w_{[i]})$ 包含 $(V_1)^2$,，且 f 是无平方的，我们必然有 $w_{[n]} = w_{[i]}$。这意味着 $V_2V_1 = f(w_{[i]}) = V_1V_2$，并且 $f(w_{[i]})$ 含有一个平方：这与假设矛盾。

□

推论 5.4 不含幂 $k(\geq 2)$ 的一致态射是本原的。

参考文献

[1] Tero Harju 和 Dirk Nowotka。《自由半群中的方程》$x^i = y^jz^k$。Semigroup Forum，68(3):488–490，2004。[2] P´al D¨om¨osi 和 G´eza Horv´ath。《Lyndon–Sch¨utzenberger 定理的另一种证明》。Theor. Comput. Sci.，366(3):194–198，2006。[3] HK Hsiao、YT Yeh 和 SS Yu。《保持平方无因子性和本原性的同态》。Acta Mathematica Hungarica，101(1):113–130，2003。[4] V. Ker¨anen。《自由幺半群上态射的 k-自由性》。Annales Academiae Scientarium Fennicae 61，A辑，1986。[5] M. Leconte。《无重复码》。博士论文，LITP 巴黎第六大学，1985年10月。[6] A. Lentin 和 M.P. Sch¨utzenberger。《自由幺半群理论中的一个组合问题》。北卡罗来纳大学论文集，1967年1月。

[7] M. Lothaire。《词上的组合学》，数学百科全书第17卷。Addison-Wesley，1983年。1997年由剑桥大学出版社在剑桥数学丛书中重印，英国剑桥，1997年。[8] M. Lothaire。《词上的代数组合学》，数学百科全书第90卷。剑桥大学出版社，英国剑桥，2002年。[9] R. C. Lyndon 和 M. P. Sch¨utzenberger。《自由群中的方程》$a^M = b^N c^P$。《密歇根数学杂志》，9(4):289–298，1962年。[10] Victor Mitrana。《保持本原词的态射》。技术报告第69号，图尔库计算机科学中心，布加勒斯特大学数学学院，1996年。[11] Victor Mitrana。《本原态射》。《信息处理快报》，64(6):277–281，1997年。[12] Jeffrey Shallit。《形式语言与自动机理论进阶》。2008年1月。[13] Francis Wlazinski。《用于 k-幂自由二进制态射的测试集》。TIA，35:437–452，2001年。[14] Francis Wlazinski。《非（$k+1$）-幂自由态射的约化》。RAIRO 理论信息学与应用，第50卷，第1期，2016年1月至3月，献给第15届“Journ´ees montoises d’informatique th´eorique”的专刊：3–20，2016年。[15] Francis Wlazinski。《一致无立方幂态射对所有整数 $k \geq 4$ 都是 k-幂自由的》。RAIRO-Theor. Inf. Appl.，51(4):205–216，2017年。[16] Francis Wlazinski。《k-幂自由态射对于任意整数 $k \geq 5$ 都是（$k+1$）-幂自由态射》。工作论文，2023年9月。