arXiv:2302.12446v1 [math.GR] 24 Feb 2023

# 幂零类为 2 的词自动群

ANDR´E NIES 和 FRANK STEPHAN

Abstract. 我们考察幂零类为 2、指数为素数 $p$的群的词自动性。我们证明，这个簇中的无限生成自由群不是词自动的。与之相反，无限超特殊 $p$-群 $E_p$ 是词自动的，具有无限中心的一个中间群 $H_p$ 也同样如此。在最后一节中，我们介绍一种方法，通过余循环证明阿贝尔群的中心扩张具有自动性。

## 1. Introduction

有限签名上的结构称为词自动（或有限自动机可表示），如果其论域是一个可由字母表 $\Sigma$上的有限自动机（有限自动机）识别的字符串集合。原子关系也可由有限自动机识别，具体如下：要检查论域中元素 $a_1$、.....、$a_n$ 之间是否满足某个原子关系，就用一个不属于 $\Sigma$的填充符号$\Diamond$ ，将表示这些元素的字符串扩展为长度相同的字符串 $\sigma_1$、.....、 $\sigma_n$；然后要求存在一个有限自动机，能够识别 $(\Sigma \cup \{\Diamond\})^n$ 上的语言，该语言由将这些字符串 $\sigma_1$、.....、 $\sigma_n$ 逐个堆叠起来所得的字符串构成。

Hodgson 首先研究了字自动结构 [6, 7] ，并用它们为 $(\mathbb{N}, +)$ 的一阶理论是可判定的这一结论给出了新的证明。Khoussainov 和 Nerode 在该领域的奠基性论文中对其进行了深入研究 [9], 。

由于有限自动机的计算能力十分有限，要在某个特定类别中找到非平凡的字自动结构可能颇具挑战；在某些情况下，例如布尔代数这一类别，可以证明只有显而易见的结构才是字自动的 [10]。

字自动群（不要与 Thurston 意义上的自动群混淆）具有良好的封闭性；例如，它在有限直积以及对正则正规子群取商的运算下封闭。在阿贝尔情形下，它对某种类型的有限自动机可识别粘合也封闭 [14]。我们注意到，对于任意有限群 $S$，其直幂 $S^{(\omega)}$ 都是字自动的。

阿贝尔情形。Nies 和 Semukhin [14] 构造了秩为 2 及更高秩的字自动无挠不可分解阿贝尔群。这使它们有别于诸如 $\mathbb{Z} \times \mathbb{Z}$ 这样的例子，后者可以用一种平凡的方式视为字自动群。他们的例子涉及被多个素数整除的问题。目前仍不清楚这类群能否作为 $(\mathbb{Z}[1/p])^n$ 的子群得到，其中 $n \geq 2$ 任意。Braun 和 Str¨ungmann [1], 在 Tsankov [16], 的方法基础上，对无挠阿贝尔群给出了严格限制。特别是，这类群具有有限秩。

字自动群的新例子。本文研究略超出阿贝尔群簇范围的簇中的不可分解字自动群。回顾一下，如果群 $G$ 满足恒等式 $[[x,y],z]$，则称其为二类幂零。在 $G$ 中，这也就是说，$G$ 是一个以阿贝尔群为商群的中心扩张。固定一个奇素数 $p$，令 $\mathcal{N}_{2,\ p}$ 表示由二类幂零且指数为 $p$（即对每个 $x$，$x^p = 1$）的群组成的群簇。注意，对每个$G \in \mathcal{N}_{2,\ p}$，中心 $Z(G)$ 是一个初等阿贝尔 $p$-群，因此可视为域 $R$ 上的向量空间。中心商群 $G/Z(G)$ 也同样如此。

$R = GF(p)$ 表示 $p$ 元素的域。词自动群的新例子是单位三角群的无限生成变体

$$UT_3(R) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in R \right\}.$$

这是 $\mathcal{N}_{2,\ p}$ 中秩为 2 的自由群。它由 $x_0 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ 和 $x_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ 生成。我们有 $[x_0, x_1] = z := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$。$\mathrm{UT}_3(R)$ 的中心是由 $z$ 生成的循环群。

我们通过改变 $\mathrm{UT}_3(R)$ 的定义，引入群 $G \in \mathcal{N}_{2,\ p}$。我们假设 $G$ 有一列由不同生成元组成的无限正合列 $\langle x_n \rangle_{n \in \mathbb{N}}$。如果交换子 $[x_i, x_k]$、$i < k$ 线性无关，那么 $G$ 就是 $\mathcal{N}_{2,\ p}$ 中的无限秩自由群，我们将其记作 $F_\infty$。我们将证明这个群不是字自动的。简言之，对于 $F_\infty$ 的任意 FA-表示，生成元的交换子的线性无关性要求用长度为 $O(n)$ 的 $p(\binom{n}{2})$ 个字符串来表示 $[x_i, x_k]$ 对于 $i < k < n$ 的线性组合；当 $n$ 足够大时，这与之矛盾。

相比之下，如果交换子 $[x_i, x_k] \in Z(G)$ 以某种强依赖方式相关，那么 $G$ 就是字自动的。最简单的例子是我们记作 $E_p$ 的群；如果 $p$ 已被理解，也简称为 $E$：要求存在一个元素 $z \neq e$，使得对于每个 $i < k$ 都有 $[x_i, x_k] = z$。因此，中心是循环的，正如 $\mathrm{UT}_3(R)$ 的情形一样。我们注意到，$E_p$ 是 Higman 和 Hall 意义下的超特殊 $p$-群：中心是阶为 $p$ 的循环群，且等于导出子群；中心商群是初等阿贝尔 $p$-群（即在 $GF(p)$ 上的向量空间）。一个稍微复杂的例子是群 $H_p$：我们要求对于 $i < k$ 有 $[x_i, x_k] = z_k$，其中 $z_k$ 构成中心的一组基。

有限指数的阿贝尔子群。Nies 和 Thomas [15] 证明，词自动群的每个有限生成子群都含有一个有限指数的阿贝尔子群。这表明词自动群与阿贝尔群十分接近。每个无挠词自动群是否都含有有限指数的阿贝尔子群，仍是一个未解决的问题 [13, 问题 4.5]。群 $E_p$和 $H_p$ 是没有有限指数阿贝尔子群的词自动挠群。这类群的第一个例子是 [15, 例 12]，我们将在下文的例 6.2 中再次讨论。

同构问题。对于词自动结构这一类结构而言，同构问题的计算复杂性是衡量其复杂性的一个良好指标。该问题询问由有限自动机给出的两个表示是否描述了同构的结构。这是 Khoussainov、Nies、Rubin 和 Stephan [10]研究的一个核心主题。他们证明，词自动图的同构问题是 $\Sigma_1^1$-完全的，而词自动布尔代数的同构问题是可判定的。Kuske、Liu 和 Lohrey [11] 证明，词自动等价关系的同构问题是$\Pi_1^0$-完全的。对于阿贝尔群以及一般的群，其复杂性尚不清楚（[2, 问题 5.1]）。要证明某一类词自动结构的同构问题不可判定，通常需要在该类结构中找到足够复杂结构的构造方法，以便编码某个不可判定问题。相反，要证明其可判定性，则需要对该类结构施加限制。目前尚不清楚 $\mathcal{N}_{2,p}$ 词自动群这一类的同构问题是否可判定。本文同时采用这两种方法，通过给出该类的例子和限制来探讨这一问题。

超特殊 $p$-群的一些模型论。我们注意到，超特殊$p$-群 $E_p$ 已在文献中的许多地方出现。例如，让我们简要回顾这些群的一些模型论性质，关于 $p \neq 2$，这是 Felgner [4]的工作。（他用 $G(p, \leq)$ 表示这些群，其中 $\leq$ 是 $\omega$的通常排序。）在第 423 页，他为 $E_p$的理论提供了一个递归公理系统。该系统表达了群具有指数 $p$，且中心是阶为 $p$ 的循环群，并包含导出子群，而导出子群是非平凡的。此外，它还使用一个无限公理列表表达了中心商群是无限的。这意味着 $E_p$ 是 $\omega$-范畴的，因为根据 Newman [12]的证明，在同构意义下，只有一个指数为 $p$ 的可数无限超特殊群。

如果一个群中成立的每个一阶句子也在某个有限群中成立，则称该群为伪有限群（关于这一概念的背景，见 [8]）。注意，对于每个奇数 $k$，都存在一个指数为 $p$、阶为$p^k$的超特殊群。因此，任意有限组公理都可以在一个有限模型中得到满足。于是$E_p$ 是伪有限的。

## 2. Preliminaries on word automaticity and on groups in $\mathcal{N}_{2,\ p}$

有限自动机表示：事实与示例

定义 2.1. 称有限签名中的一个结构 $A$ 是字自动的（或有限自动机可表示的），如果其论域中的元素可以由正则语言 $D_A$ 中字母表 $\Sigma$上的字符串表示，且这种表示可能是不唯一的，并且满足以下条件。对于每个形如 $Ra_1, \ldots, a_n$，或 $f(a_1, \ldots, a_n) = b$，或 $a = b$ 的原子关系，其中 $R, f$ 分别是 $n$ 元关系符号和函数符号，而 $a_1, \ldots, a_n, b \in A$，都存在一个有限自动机能够按照本文开头所讨论的意义识别它。一个有限自动机表示是由如上所述的有限自动机构成的集合。

例 2.2。结构 $(\mathbb{N}, +)$ 通过自然数的常规二进制展开成为字自动结构。字母表为 $\Sigma = \{0, 1\}$，其定义域

由以 1 结尾的字符串和空字符串组成。用二进制字符串 $\alpha$ 表示数 $n$，其中最低有效位在前。因此$n = n_\alpha = \sum_{i<|\alpha|} \alpha(i)2^i$。空字符串表示 0。字母表 $(\Sigma \cup \{\Diamond\})$ 上的有限自动机[3]通过进位位过程检查和式 $n_\alpha + n_\beta = n_\gamma$ 是否正确，其中进位位向右移动。例如，若 $\alpha = 101$、$\beta = 11001$ 和 $\gamma = 00011$，自动机通过接受字符串来检查这个和是否正确

| | | | | |
|---|---|---|---|---|
| 1 | 0 | 1 | $\Diamond$ | $\Diamond$ |
| 1 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 |

.

在上面的有限自动机表示定义中，请注意，对于项 $s,t$，方程 $s = t$ 是一个原子关系。因此，该定义允许等号成为 $D_A$ 上的非平凡等价关系 $E$；这有时在定义有限自动机表示时很有用。不过，由于 $D_A$ 上的长度—字典序排序 $\leq_L$ 可由有限自动机识别，因此可以用正则集 $\{x \in D_A$: $\forall y\,[yEx \to x \leq_L y]\}$ 替换 $D_A$，从而以字符串唯一表示各个元素。

给定一个结构 $\mathcal{A}$ 的有限自动机表示和一个公式 $\phi$（可能带有参数），可以有效地确定一个有限自动机，用以识别由 $\phi$ 定义的 $\mathcal{A}$ 上的关系。证明使用对 $|\phi|$ 的归纳法。为处理存在量词，我们利用这样一个事实：对于每个非确定有限自动机，都存在一个识别相同语言的确定有限自动机。因此，要证明群 $(G, \circ, ^{-1})$ 是字自动的，只需给出一个识别二元群运算 $\circ$ 的有限自动机；一元群运算可以由它定义。

按照 Epstein 和 Thurston 的定义，自动群（见 [3]）按定义都是有限生成的。相比之下，要得到有趣的字自动群，合适的研究范围应在有限生成群之外；因为一个有限生成群是字自动的，当且仅当它含有一个有限指数的阿贝尔子群。请注意，为避免与这两个概念混淆，[13] 中将字自动群称为有限自动机可表示群。

二步幂零群的预备知识。若固定正在讨论的群 $G$ 的一列生成元 $\langle x_i \rangle_{i\in\mathbb{N}}$，对于整数元组 $\alpha$，我们令

$$\underline{\alpha} := \prod_{i<|\alpha|} x_i^{\alpha_i}.$$

对于群元素 $x$、$y$，我们将交换子定义为 $[x, y] = x^{-1}y^{-1}xy$。若 $G$ 是二类幂零的，则交换子诱导出一个交替双线性形式

$$\theta_G \colon (G/Z)^2 \to Z$$

其中 $Z = Z(G)$ 且 $\theta_G(aZ, bZ) = [a, b]$，这是良定义的。因此，对于 $|\alpha| = |\beta| = n$ 以及中心元素 $c$、$d$，

$$\left[\underline{\alpha}c, \underline{\beta}d\right] = \prod_{r<s\leq n} [x_r, x_s]^{\alpha_r\beta_s - \alpha_s\beta_r}$$

下文将不再特别说明地使用这一恒等式。

## 3. The group $F_\infty$ is not word automatic

回想一下，我们用 $F_\infty$ 表示指数为 $p$ 、幂零类 2 的群构成的簇 $\mathcal{N}_{2,p}$ 中的无限秩自由群。设 $\langle x_i\rangle_{i\in\mathbb{N}}$ 是一列自由生成元，并回想我们将 $\underline{\alpha} := \prod_{i<|\alpha|} x_i^{\alpha_i}$ 记作。众所周知（[17], $F_\infty$ 的每个元素都有一个标准形

$$\underline{\alpha}\cdot\prod_{r<s<n}[x_r,x_s]^{v_{r,s}}, \tag{1}$$

其中 $|\alpha|=n$ 和 $0\le v_{r,\ s}<p$。（为使此标准形唯一，可以要求 $\alpha_{n-1}\neq 0\vee\exists r[v_{r,n-1}\neq 0]$；也就是说， $n$ 取最小值。中心元素是指 $\alpha$ 由 0 组成的字符串。）

定理 3.1. $F_\infty$ 不是词自动的。

证明。反设 $F_\infty$ 有一个有限自动机表示。其定义域是某个字母表 $\Sigma$上的正则集 $D\subseteq\Sigma^*$ ，并且有一个有限自动机可识别的运算 $\circ$: $D\times D\to D$ ，用于表示二元群运算。如第 2 节所述，我们可以假设，表示的群中的相等关系就是 $D$ 上的相等关系。因此，我们可以将$F_\infty$ 与定义域为 $D$的结构等同。与之前一样，用 $\le_L$ 表示 $D$上的长度字典序，它同样可由有限自动机识别。

证明的思路是定义 $D$ 中元素的正合列 $\langle u_n\rangle_{n\in\mathbb{N}}$ 和 $\langle z_n\rangle_{n\in\mathbb{N}}$ ，使得中心元素 $[u_i,u_k]$、 $i<k<n$ 在域 $GF(p)$ 上线性无关，并且对于每个 $n$，由 $u_0$、……、 $u_n$ 生成的子群包含于字符串集合 $\{x\in D\colon x\le_L z_{n+1}\}$ 中。此外， $z_{n+1}$ 是通过对 $z_n$ 应用函数 $G$ 得到的，该函数在由 $\le_L$ 扩充的 $D$ 上的结构中一阶可定义。因此，这个函数可由有限自动机识别。现在，泵引理意味着，任意由 $[u_i,u_k]$ 的线性组合（其中 $i<k<n$）构成的字符串，其长度为 $O(n)$。这意味着，当 $n$ 足够大时，允许长度范围内的字符串数量不足以容纳这些 $p^{\binom{n}{2}}$ 个线性组合。

关于细节，我们验证三个断言。注意，中心 $Z=Z(F_\infty)$ 是一个正则集。第一个断言指出，对于每个有限集合 $S\subseteq D$ ，都存在 $u\in D$ ，使得由 $Zr\to[r,u]$ 给出的映射 $ZS/Z\to Z$ 的值域与 $S$ 不相交，且该映射是单射。

断言 3.2。对于每个有限集合 $S\subseteq D$，都存在一个字符串 $u\in D$ ，使得 (i) 若 $r\in S\setminus Z$ ，则 $[r,u]\notin S$；(ii) 对于每个 $v$、 $w\in S$，若 $[v,u]=[w,u]$，则存在 $c\in Z$，使得$c\circ v=w$。

给定 $S$，我们将用 $u(S)$ 表示满足该断言的 $\le_L$-最小字符串 $u$ 。

为说明这一点，令 $u=x_k$ ，其中 $k$ 足够大，使得任意 $S$ 的元素的标准形中，只会出现满足 $i<k$ 的 $x_i$ 。

对于 (i)，注意到 $r$ 包含某个满足 $i<k$ 的 $x_i$ ，因此 $[r,u]$ 的标准形包含 $[x_i,x_k]$，而 $S$ 中元素的标准形不包含这样的交换子。

对于 (ii)，令 $v=\underline{\alpha}d$ ，其中 $d$ 为中心元。则 $[v,u]$ 的标准形以 $\prod_{i<k}[x_i,x_k]^{\alpha_i}$ 结尾，由此确定 $\alpha$。这就验证了该断言。

现在我们在 $D$ 中递归定义正合列 $\langle u_n\rangle_{n\in\mathbb{N}}$ 和 $\langle z_n\rangle_{n\in\mathbb{N}}$。令 $z_0$ 为表示单位元 1 的字符串。现在假设 $z_n$ 已定义。令

$$u_n = u(V_n) \text{ where } V_n = \{v\colon v \leq_L z_n\},$$

根据断言 3.2。接下来，令 $z_{n+1}$ 为满足以下条件的 $\leq_L$-最小字符串：

(2) for each $v, w \in V_n$ and each $i < p$, one has $w \circ u_n^i \circ [v, u_n] \leq_L z$.

在结构 $(D, \circ, \leq_L)$ 中，可以用一阶方式从 $z_n$ 一致地定义 $u_n$。因此，存在一个函数 $G\colon D \to D$，它在该结构中是一阶可定义的，并且对每个 $n$ 都有 $z_{n+1} = G(z_n)$。正如引言中所述，其可定义性意味着 $G$ 的图可以由有限自动机识别。特别地，我们有 $|z_n| = O(n)$，因为根据泵引理，具有正则图的函数，其输出长度至多比输入长一个常数。

下文中，当 $i \neq k$ 时，我们将用 $u_{i,\ k}$ 表示 $[u_i, u_k]$。

断言 3.3。对每个 $n$，$\langle u_0, \dots, u_n\rangle \subseteq V_{n+1}$。

我们对 $n$ 使用归纳法。对于 $n = 0$，我们有 $\langle u_0\rangle \subseteq V_1$，因为在（2）中可以令 $v$、$w$ 为表示单位元的字符串。对于归纳步骤，注意到根据标准形（以及 $F_\infty$ 的自由性），$\langle u_0, \dots, u_n\rangle$ 中的每个元素都具有以下形式

$$y = \prod_{i\leq n} u_i^{\alpha_i} \prod_{r<s\leq n} [u_{r,s}]^{\gamma_{r,s}}$$

其中 $0 \leq \alpha_i, \gamma_{r,\ s} < p$。这可以改写为 $wu_n^{\alpha_n}[v, u_n]$，其中

$$w = \prod_{i<n} u_i^{\alpha_i} \prod_{r<s<n} [u_{r,s}]^{\gamma_{r,s}} \text{ and } v = \prod_{k<n} u_k^{\gamma_{k,n}}.$$

根据归纳假设 $w$、$v \in V_n$。因此，元素 $y$ 根据（2）属于 $V_{n+1}$。这就证明了该断言。

在下一个断言中，我们将初等阿贝尔 $p$-群视为域 $GF(p)$ 上的向量空间。

断言 3.4。

（a）元素 $Zu_i$ 在 $G/Z$ 中线性无关。（b）元素 $u_{i,\ k}$ 在 $Z$ 中线性无关。

在 (a) 和 (b) 中，我们都对指标的上界 $n$ 使用归纳法。对于 $n = 0$，两个陈述都显然成立。对于 (a)，注意 $u_{n+1}^i \notin V_{n+1}Z$对每个 $i < p$ 都成立：否则存在 $c \in Z$ 使得 $v := u_{n+1}^i c \in V_{n+1}$。我们有 $u_{n+1}^i \notin Z$，因此 $v \notin Z$。由于 $[v, u_{n+1}] = 1$ 且 $1 = z_0 \in V_{n+1}$，这与断言 3.2 中关于 $S = V_{n+1}$ 的条件 (i) 矛盾。因此，根据断言 3.3，$Z\langle u_{n+1}\rangle \cap Z\langle u_0, \dots, u_n\rangle = 0$。

对于 (b)，根据归纳法，$u_{i,\ k}$, $i < k \leq n$ 构成子空间$T_0 \subseteq Z$的一组基。根据断言 3.2 的 (ii)，定义在 $ZV_n/Z$ 上的线性映射 $Zw \to [w, u_{n+1}]$ 是单射。因此，根据 (a)，$i \leq n$ 对应的 $[u_i, u_{n+1}]$ 构成子空间$T_1 \subseteq Z$的一组基。接下来证明 $T_0 \cap T_1 = \{0\}$：若存在系数 $\alpha_i$ 满足 $0 \leq \alpha_i < p$，使得 $\sum_{i\leq n} \alpha_i[u_i, u_{n+1}] = [\sum_{i\leq n} \alpha_i u_i, u_{n+1}] \neq 0$，则 $r := \sum_{i\leq n} \alpha_i u_i \in V_{n+1} \setminus Z$；根据断言 3.3，进而有 $[r, u_{n+1}] \notin V_{n+1}$，而根据断言 3.2 的条件 (i)，可得 $[r, u_{n+1}] \notin V_{n+1}$。再由断言 3.3 可知 $[r, u_{n+1}] \notin T_0$。至此归纳步骤完成，断言得证。

给定 $n$，根据断言 3.3，我们有

$$\prod_{i<k<n}[u_i,u_k]^{\gamma_{i,k}} \in V_n$$

对于指数的每个数组 $\langle\gamma_{i,\ k}\rangle_{i<k<n}$ 其中指数属于 $[0,p)$。根据断言 3.4，所有这些元素都彼此不同。由于 $V_n$ 由长度为 $O(n)$ 的字符串组成，因此我们有 $p^{n(n-1)/2}$ 个长度为 $O(n)$ 的不同字符串；当 $n$足够大时，这就产生了矛盾。□

## 4. Quotients of $F_\infty$ with dependency between the commutators

和之前一样，令 $F_\infty$ 表示簇 $\mathcal{N}_{2,\ p}$ 中由自由生成元$x_i$、 $i\in\mathbb{N}$生成的群。接下来，我们将定义簇 $\mathcal{N}_{2,\ p}$ 中的群 $E$、$H$，它们是 $F_\infty$ 的商群。对于 $E$，我们要求所有交换子 $[x_i,x_\ell]$、 $i<\ell$ 都相等。对于 $H$，我们要求，对于 $i<k$，有 $[x_i,x_k]=z_k$，其中 $z_k$ 在 $\mathbb{Z}/p\mathbb{Z}$ 上线性无关。具体而言，我们通过簇 $\mathcal{N}_{2,\ p}$中的表示来定义这些群：

$$E = \langle\{x_i\}_{i\in\mathbb{N}}, z\colon [x_i,x_k]=z\ (0\le i<k)\rangle \tag{3}$$

$$H = \langle\{x_i\}_{i\in\mathbb{N}}, \{z_k\}_{k\in\mathbb{N}^+}\colon [x_i,x_k]=z_k\ (i<k)\rangle \tag{4}$$

注意，如引言中所述， $E$ 是超特殊的。相比之下， $H$ 的中心维数是无限的。

在幂零群中，每个非平凡正规子群都与中心有非平凡交集。这意味着 $E$ 的每个真商群都是阿贝尔群；特别地， $E$ 不是剩余有限的。另一方面， $H$ 是剩余有限的 $p$群，因此可自然嵌入其 pro-$p$完备化中。为此，取一个元素 $h\neq 1$，它可以用生成元 $x_0$、.....、$x_{n-1}$表示。于是， $h\neq 1$属于有限 $p$群；该群是 $H$ 模由 $x_k$、 $k\ge n$ 生成的正规子群（其中包含所有 $z_k$、$k\ge n$）所得的商群。

我们给出两个代数事实，以支持这样一种说法：我们将在下一节给出的群的有限自动机表示是非平凡的；它们既不能由阿贝尔群的有限自动机表示得到，也不是较简单组成部分的有限自动机表示的组合。

命题 4.1。群 $E, H$ 均没有有限指数的阿贝尔子群。

证明。只需对 $E$证明这一点，因为 $H$ 有 $E$ 作为商群。因此，设 $M$ 是 $E$ 的一个有限指数子群。存在 $k<r<s$使得 $x_rx_k^{-1}\in M$且 $x_sx_k^{-1}\in M$。我们有 $[x_rx_k^{-1},x_sx_k^{-1}]=[x_r,x_s][x_r,x_k^{-1}][x_k^{-1},x_s]=z$，所以 $M$中的这两个元素不交换。□

命题 4.2。群 $E$ 和 $H$ 是不可分解的。

证明。 $E$ 是不可分解的，因为它的每个真商群都是阿贝尔群。设 $H=A\times B$ 对于子群 $A,B$ 成立。记 $Z=Z(H)$，$\widetilde{x_i}=x_iZ$，$\widetilde{A}=AZ/Z$，以及 $\widetilde{B}=BZ/Z$。对于以 $\mathbb{Z}$ 为底的字符串 $\beta$，我们记作 $\widetilde{\beta}=\prod_{i<|\beta|}\widetilde{x_i}^{\beta_i}$。~若 $A\subseteq Z$，则所有 $\widetilde{x_i}$ 都属于 $B$，因此对于每个 $k\ge 1$， $z_k=[x_0,x_k]$ 都属于 $B$，从而 $B=H$。不妨由对称性假设 $A,B\not\subseteq Z$。

首先，对假设一个$x_0^m$m∈，满足 $\widetilde{0}<m<p$。于是存在一个长度至少为 2 的字符串 $\beta$，使得 $\beta\in B$。因此 $[x_0^m,\underline{\beta}]=\prod_{0<i<|\beta|}z_i^{m\beta_i}\neq e$，矛盾。

现在假设情况并非如此。存在字符串 $\alpha$、$\beta$，它们属于 $\{0,\dots,p-1\}$，且满足 $\sim\sim\ \sim\ \sim\widetilde{\alpha}\in A$、$\beta\in B$，使得 $\widetilde{x}_0=\widetilde{\alpha}+\beta$。根据假设，$\alpha_k\neq 0$，其中某个 $k>0$ 取为最小值。于是 $\beta_0=1-\alpha_0$、$\beta_k=-\alpha_k$，并且对 $0<r<k$ 有 $\beta_r=0$。因此，利用交换子的双线性性质，$[\underline{\alpha},\underline{\beta}]$ 含有一个因子 $z_k^{\gamma}$，其中 $\gamma=\alpha_k\beta_0-\alpha_0\beta_k=\alpha_k$。于是 $[\underline{\alpha},\underline{\beta}]\neq e$，矛盾。□

## 5. The groups $E$ and $H$ are word automatic

回顾一下，固定一个素数 $p$ 后，群 $E$ 和 $H$ 通过 (3) 和 (4) 定义。我们将基于字母表来描述这些群的有限自动机表示

$$\Sigma=\{0,\dots,p-1\}.$$

变量 $\alpha,\beta,\gamma$ 表示 $\Sigma$ 上的字符串。回顾一下，我们将 $\underline{\alpha}$ 写作 $\prod_i x_i^{\alpha_i}$，其中 $x_i$ 是表示中给出的生成元。利用 (1) 中给出的 $F_\infty$ 中元素的标准形，$E$ 中的每个元素都可以写成 $z^v\cdot\underline{\alpha}$ 的形式，其中 $0\le v<p$。

本节中的所有算术运算均以 $p$ 为模。如果有必要，在诸如 $\alpha+\beta$ 的表达式中，字符串 $\alpha,\beta$ 会被视为在末尾补 0，并按分量相加。

对于群 $E$，注意到当 $n=\max(|\alpha|,|\beta|)$ 时，

$$\underline{\alpha}\cdot\underline{\beta}=z^{-\sum_{k=1}^{n-1}\alpha_k(\sum_{i=0}^{k-1}\beta_i)}\cdot\overline{\alpha+\beta}. \tag{5}$$

这是因为，可以通过对递减的正数 $k$ 进行计算：将项 $x_k^{\alpha_k}$ 向右移动，使其越过 $i=0$ 的项 $x_i^{\beta_i}$，.....，$k-1$，然后将其与 $x_k^{\beta_k}$ 合并，得到 $x_k^{\alpha_k+\beta_k}$。每次这样的移动都会在 $E$ 的中心产生一个因子 $z^{-\alpha_k\beta_i}$。

命题 5.1。群 $E$ 是字自动的。

证明。元素 $z^v\cdot\underline{\alpha}$ 由字符串 $v\alpha$ 表示。定义域由满足以下条件的字符串 $v\alpha$ 构成：$\alpha$ 为空，或者其最后一项不为 0。

我们描述一个有限自动机，用来检查 (5)，从而正确验证二进制群运算。它处理由三个字符串 $v\alpha$、$w\beta$、$r\gamma$ 组成的输入，这些字符串分别叠放在三条轨道上。如有必要，我们在字符串末尾补上 0，使其长度均为 $1+n$，其中 $n=$ 为 $\max(|\alpha|,|\beta|,|\gamma|)$。因此，有限自动机处理的是按以下格式排列、取自字母表 $\Sigma^3$ 的输入：

$$s_{-1}s_0\dots s_{n-1}=\begin{array}{|c|c|c|c|c|}\hline v&\alpha_0&\alpha_1&\cdots&\alpha_{n-1}\\\hline w&\beta_0&\beta_1&\cdots&\beta n-1\\\hline r&\gamma_0&\gamma_1&\cdots&\gamma_{n-1}\\\hline\end{array}$$

当有限自动机扫描第一个栈符号 $s_{-1}$ 时，会将其存储在由状态提供的定长存储器中。扫描 $s_k$ for $k=0$，.....，$n-1$ 时，它会检查 $\alpha_k+\beta_k=\gamma_k$（如果检查失败，则进入拒绝状态，并一直保持在该状态，直到扫描完整个输入）。有限自动机将当前值 $\sum_{i<k}\beta_i$ 存储在其定长内部存储器中。它将 $\alpha_k$ $(\sum_{i<k}\beta_i)$ 加到一个取值范围为 $\Sigma$ 的变量 $x$ 上，该变量的初始值为 0，也可视为存储在内部存储器中。扫描完最后一个符号后，它会检查 $v+w-x=r\bmod p$，并据此决定是否接受。□

$H$ 中的每个元素都可以写成如下形式

$$\prod_{s<|\alpha|} z_s^{v_s} \cdot \underline{\alpha}$$

其中 $0 \le v_s < p$。中心元素是满足 $\alpha$ 仅由 0 组成的元素。如果 $n = \max(|\alpha|, |\beta|)$，类似于 (5)，我们在 $H$ 中有

$$\underline{\alpha} \cdot \underline{\beta} = \prod_{k=1^{n-1}} z_k^{-\alpha_k(\sum_{i<k}\beta_i)} \cdot \underline{\alpha+\beta}. \tag{6}$$

命题 5.2。群 $H$ 是字自动的。

证明。群 $h$ 中的元素将由字母表 $\Sigma$上的一对等长字符串$\alpha$、$v$ 表示，它们的长度均为 $n$，满足若 $n>0$ 则 $v_0 = 0$，且二者不能都以 0 结尾，并且 $h = \prod_{k=1}^{n} z_k^{v_k} \cdot \underline{\alpha}$。这些字符串写在两条轨道上，其中 $\alpha$ 位于 $v$上方。

我们描述一个用于检查（6）的有限自动机，从而正确验证群运算。它处理字母表 $\Sigma^6$ 上的、具有以下格式的字符串

$$s_0 \dots s_{n-1} = \begin{array}{|c|c|c|c|} \hline \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \hline v_0 & v_1 & \cdots & v_{n-1} \\ \hline \beta_0 & \beta_1 & \cdots & \beta n-1 \\ \hline w_0 & w_1 & \cdots & w_{n-1} \\ \hline \gamma_0 & \gamma_1 & \cdots & \gamma_{n-1} \\ \hline r_0 & r_1 & \cdots & r_{n-1} \\ \hline \end{array}.$$

开始时，有限自动机扫描 $s_0$ 并检查 $v_0 = w_0 = r_0 = 0$。与 $E$的情形一样，当有限自动机为 $k \ge 0$扫描 $s_k$ 时，它检查 $\alpha_k + \beta_k = \gamma_k$，并将当前值 $\sum_{i<k}\beta_i$ 存储在其固定大小的内部存储器中。不过，现在它还会检查

$$v_k + w_k - \alpha_k(\textstyle\sum_{i<k}\beta_i) = r_k \mod p$$

（若 $k=0$，则显然成立。）如果这些检查中有任何一项未通过，自动机便进入拒绝状态。否则，在扫描完整个输入后，它就接受该输入。□

B¨uchi 自动机是处理无限词的（非确定性）有限自动机。如果某个处理该词的计算过程无限次处于接受状态，那么该词就被接受。Hodgson 最早研究了 B¨uchi 自动结构 [7], ，并称之为宏自动结构。背景介绍见 [13, 第 2 节1]。下面我们简要举例说明一个以非平凡方式成为 B¨uchi 自动结构的非阿贝尔不可数群。

ˆ 事实 5.3。pro-$p$ 完备化 $H_p$ 是 $H_p$ B¨uchi 自动的。

ˆ 证明。对每一对取自 $\{0,\dots,p-1\}$ 的无限词 $\alpha$、$v$，在 $H_p$ 中都可以构造极限 $\prod_i x_i^{\alpha_i}$: $= \lim_n \prod_{i<n} x_i^{\alpha_i}$ 和 $\prod_{k>0} z_k^{v_k}$。群 $H_p$ 中的一个元素 $h$ˆ 由一对满足$h = \prod_{k>0} z_k^{v_{k-1}} \cdot \prod_i x_i^{\alpha_i}$的无限词 $\alpha$、$v$ 表示。我们可以使用上文中的同一个自动机，现在令其处理无限词，以验证 $H_p$ 上的二元群运算。□

## 6. Constructing word automatic groups via cocycles

我们回顾关于阿贝尔群的中心扩张的一些众所周知的事实。给定两个阿贝尔群 $A$ and $Q$, $Q$ 被 $A$ 中心扩张是一个正合

列 $0 \to A \to L \to Q \to 0$，满足 $A \subseteq Z(L)$。余循环用于描述这类扩张。余循环是一个函数 $f\colon\ Q \times Q \to A$，满足

$$f(u,v) + f(u+v,w) = f(v,w) + f(u,v+w).$$

在 $Q \times A$ 上，运算

$$(u,a) \cdot (v,b) := (u+v, a+b+f(u,v))$$

定义了一个群 $L_f$；当且仅当 $f$ 对称时，它是阿贝尔群。容易验证，利用映射 $a \to (0,a)$ 和 $(u,a) \to u$，可以得到一个正合列 $0 \to A \to L_f \to Q \to 0$。$(u,a)$ 的逆元是 $(-u.-a-f(u,-u))$。对于结合律，如果我们计算 $[(u,a)+(v.b)]+(w,c)$，则右侧第二个分量中的“修正项”为 $f(u,v)+f(u+v,w)$。如果我们计算 $(u,a)+[(v.b)+(w,c)],$，修正项则为 $f(v,w)+f(u,v+w)$。

反过来，给定一个正合列 $0 \to A \to L \to Q \to 0$，其中 $A \leq Z(L)$，为了确定一个 2-余循环 $c\colon\ Q \times Q \to A$，使其产生一个等价扩张，可以选取一组 $T$，作为 $A$ 在 $L$ 中的陪集代表元。固定一个双射 $Q \to T$，并将 $q$ 的像记为 $\overline{q}$，则该余循环为

$$f(q_0,q_1)\colon = \overline{q_0} \cdot \overline{q_1} \cdot (\overline{q_0+q_1})^{-1} \in A.$$

详细背景可参见例如 Fuchs [5, 第 9] 章（他将这些对象称为“$A$ 对 $Q$的扩张”，但在记号中采用相同的顺序，即先写 $Q$，再写 $A$）。

命题 6.1. 设 $A$ 和 $Q$ 是词自动阿贝尔群。设 $L$ 是 $Q$ 对 $A$的中心扩张，由正合列 $0 \to A \to L \to Q \to 0$ 给出，其中 $A \leq Z(L)$。假设有一个描述此扩张的余循环 $f\colon\ Q \times Q \to A$ 是有限自动机可识别的。那么 $L$是字自动的。

证明。 $L$ 可以构造为集合 $Q \times A$，其运算如上所述。因此， $L$可以用一阶方式在词自动双类型结构（$Q \sqcup A, +_Q, +_A, f$）中解释。这表明 $L$ 是字自动的。□

因此，若我们能选取 $T$，使相应的余循环 $f$ 可以由有限自动机计算，就能得到 $L$的 FA-表示。作为命题 6.1 的应用示例，我们重新考察一个在 [15,例 12], 中引入的群，它没有有限指数的阿贝尔子群。我们给出一个基于余循环的简短证明，说明这个群是字自动的。

例 6.2. 设群 $L$ 的生成元为 $x$、$y_i$、$z_k$（$i$、$k \in \mathbb{N}$），并满足关系

$$y_i^2 = z_k^2 = 1 \qquad [y_i, z_k] = [y_i, x] = 1 \qquad z_i^{-1} x z_i = x y_i$$

我们有一个正合列 $0 \to A \to L \to Q \to 0$，其中 $A = Z(L) = \langle x^2, \{y_i\}_{i\in\mathbb{N}} \rangle$，且 $Q := L/A$ 是群 $Ax$ 和 $Az_i$ 的直和。记作 $v = Ax$ 和 $w_i = Az_i$，使得 $v^2 = w_i^2 = 1$ 属于 $Q$。$Q$ 中的元素具有标准形 $q_{s,\,\alpha} = v^s \cdot \prod_i w_i^{\alpha_i}$其中 $s = 0$，1，且 $\alpha$ 是一个比特串（必要时视为在末尾补 0）。

截面 $T$ 由元素 $q_{s,\,\alpha} = x^s \prod_i z_i^{\alpha_i} \in L$ 组成。利用 $z_i x = x z_i y_i$，可验证相应的 2-余循环为

$$c(q_{s,\alpha}, q_{t,\beta}) = \overline{q_{s,\alpha}} \cdot \overline{q_{t,\beta}} \cdot (\overline{q_{s,\alpha} + q_{t,\beta}})^{-1} = x^{2s+t} \prod_i y_i^{\gamma_i}$$

其中 $\gamma_i = (s+2t)\alpha_i + (s+t)\beta_i$ 模 2。显然，这个余循环可以由有限自动机计算。

注 6.3。Nies 和 Semukhin [14, 定理 4.2] 证明，具有有限指数词自动正规子群的阿贝尔群本身也是字自动的。根据命题 6.1，这一结论实际上不局限于阿贝尔群。

注 6.4. 在第5节中，我们证明了群 $E_p$ 和 $H_p$ 是词自动的。利用余循环，证明中的自动机也可以在一定程度上简化。形如$\underline{\alpha}$ 的元素构成该扩张的一个截面。相应的余循环分别由式 (5) 和 (6) 给出。以 $H$为例，$\widetilde{\ }$余循环将 $Q = H/Z(H)$中元素 $\widetilde{\alpha}$、$\beta$ 组成的有序对映射到 $\prod_{k=1}^{n-1} z_k^{r_k} \in Z(H)$中的元素，其中 $|\alpha| = |\beta| = n$。因此，验证该余循环的自动机处理如下格式的字符串

$$t_0 \dots t_{n-1} = \begin{array}{|c|c|c|c|} \hline \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \hline \beta_0 & \beta_1 & \cdots & \beta n-1 \\ \hline 0 & r_1 & \cdots & r_{n-1} \\ \hline \end{array}.$$

在扫描符号 $t_0$、.....、$t_k$、.....时，它在大小固定的内部存储器中存储当前值 $\sum_{i<k} \beta_i$。它检查 $-\alpha_k(\sum_{i<k} \beta_i) = r_k$是否模 $p$成立；否则就进入拒绝状态。如果输入已全部扫描完毕，则接受。

## References


[1] G. Braun 和 L. Str¨ungmann. 有限自动机可表示的无挠阿贝尔群的分解. *International Journal of Algebra and Computation* 21 08 1463 1472, , ( ): – . 2011

[2] A. Nies（编者）. Logic Blog 2021. 预印本见 https://arxiv.org/pdf/2202.13643.pdf，2021.

[3] D. Epstein. *Word processing in groups*. AK Peters/CRC Press，1992. [4] U. Felgner. 关于 $\aleph_0$-范畴超特殊 $p$-群. *Logique et Analyse*，第 407–428 页，1975. [5] L. Fuchs. *Abelian groups*. Springer，2015. [6] B. R. Hodgson. *Théories décidables par automate fini*. 博士论文，蒙特利尔大学，1976. [7] B. R. Hodgson. 由有限自动机判定的理论. , : – .[8] A. O. Houcine 和 F. Point. 伪有限群的几种可能情形. *Journal of Group Theory* 16 4 461 495, 2013 , ( ): – .[9] B. Khoussainov 和 A. Nerode. 结构的自动表示. 见 *International Workshop on Logic and Computational Complexity* 367 392 ，第 – 页. Springer，1994.[10] B. Khoussainov 、 A. Nies 、 S. Rubin 和 F. Stephan. 自动结构：丰富性与局限性. *Log. Methods Comput. Sci.*, 3(2):2:2, 18，2007. [11] D. Kuske、J. Liu 和 M. Lohrey. 具有传递关系的自动结构类上的同构问题. *Transactions of the American Mathematical Society* 365 10 5103 5151, 2013 , ( ): – .

[12] M. Newman. 关于一类幂零群. *Proceedings of the London Mathematical Society* 3 1 365 375, 1960 , ( ): – .

[13] A. Nies. 描述群. *Bull. Symbolic Logic*, 13(3):305–339，2007. [14] A. Nies 和 P. Semukhin. 有限自动机可表示的阿贝尔群. *Annals of Pure and Applied Logic* 161 3 458 467, 2009 , ( ): – .

[15] A. Nies 和 R. Thomas. 有限自动机可表示的群与环. *Journal of Algebra*, 320 2 569 585, 2008 ( ): – .[16] T. Tsankov. 有理数加法群不存在自动表示. *The Journal of Symbolic Logic*, 76(4):1341–1351，2011.

[17] R. Warfield. *Nilpotent groups*，第 513 卷。Springer，2006。