可逆数字域和量子域中高层通用顺序计算的考克斯特对称性

H.E. Bez

拉夫堡大学计算机科学系，莱斯特郡 LE11 3TU 电子邮件：
h.e.bez@lboro.ac.uk
helmut.e.bez@gmail.com

arXiv:2302.05171v1 [cs.DM] 10 Feb 2023

摘要

本文研究数字域和量子域中的高层次通用可逆序列处理。具体而言，本文证明：

1. 使用标准的一般求逆过程构造的可逆数字序列过程，以及 2. 序列量子过程，

决定了考克斯特群。在每种情况下，这些群都被证明定义了由序列中给定的基本过程所能构造的所有过程。文中给出了所有情况下考克斯特群表示的显式形式。量子过程被证明在张量积量子比特空间中定义了相应考克斯特群的酉表示。

1 引言与概述

使用众所周知的（例如参见 [2]）一般可逆表示 n

$$\hat{f}(x, y) = (x, y \oplus f(x))，\text{其中} \oplus \text{表示布尔异或运算符}$$

对于布尔函数 f，本文定义了一种逐步求逆的过程，用于处理一般的不可逆布尔函数序列 $f_n \circ f_{n-1} \circ \cdots \circ f_1$。如此构造的可逆序列 $\phi_n \circ \phi_{n-1} \circ \cdots \circ \phi_1$ 中，每个可逆分量函数（一般情况下记为 ϕ_i）都是一个对合，并由 $\{\phi_1, \ldots, \phi_n\}$ 定义一个考克斯特群。对于 2 步序列，即 $n = 2$ 这种情况，证明该群同构于 8 元二面体群 D_8。对于 $n \geq 3$，则生成更一般的考克斯特群，并给出所有情形下的表示。

以量子计算为例，研究表明，对 2 步数字序列 $g(f(x))$ 进行量子化，其中 $f\colon \mathbb{B}^n \to \mathbb{B}^m$ 且 $g\colon \mathbb{B}^m \to \mathbb{B}^k$，会在张量积空间 $\otimes^{n+m+k}\mathbb{C}^2$ 的酉群 $U(\otimes^{n+m+k}\mathbb{C}^2)$ 中导出 D_8 的线性表示。

2 非可逆数字序列处理

数字序列过程的输出取决于初始输入以及一系列先前计算步骤的输出。因此，这类 j 步过程可表示如下：

- 预处理状态：$x \in \mathbb{B}^n$
- po st-process state: $(f_j \circ f_{j-1} \circ \cdots \circ f_2 \circ f_1)(x)$ for some functions $f_1, f_2, \ldots, f$

一般而言，这类计算不可逆；也就是说，无法从后处理状态确定预处理状态。上述内容隐含地假定函数复合 $f_1 \circ f_2 \circ \cdots \circ f_k$ 是定义良好的。上述内容的编码表示可写为：

$x \leftarrow (x_1, \ldots, x_n)$ /* 预处理状态的初始化 */ begin$y_1 \leftarrow f_1(x)$
$y_2 \leftarrow f_2(y_1)$ ...$y_j \leftarrow f_j(y_{j-1})$ end

3 可逆顺序数字处理

3.1 一般求逆过程

对于 f: $\mathbb{B}^n \to \mathbb{B}^m$ 和 g: $\mathbb{B}^m \to \mathbb{B}^k$，函数复合 $g \circ f$ 已定义，但由于 f 和 g 都不可逆，函数 $g \circ f$ 将不可逆。 f 和 g 的一般可逆表示如下:

$$\begin{aligned} \hat{f}(x,y) &= (x, y \oplus f(x)) \\ \hat{g}(y,p) &= (y, p \oplus g(y)) \end{aligned}$$

其中 ˆ f: $\mathbb{B}^{n+m} \to \mathbb{B}^{n+m}$, ˆ$g$: $\mathbb{B}^{m+k} \to \mathbb{B}^{m+k}$, $x \in \mathbb{B}^n$, $y \in \mathbb{B}^m$, $p \in \mathbb{B}^k$。函数 ˆ f 和 ˆgˆ是 f 和 g的可逆表示，但 ˆ$g \circ f$未定义，因此并不代表两步可逆顺序数字处理。

3.2 一般可逆过程的函数扩展

ˆ虽然 f 和 ˆg 表示各自独立的可逆数字计算，但如上所见，它们的函数复合通常未定义。对于序列处理，需要能够通过函数复合算子 $\circ$ 组合的函数。

ˆ 实现 f 和 g 适当函数复合的一种方法，是通过笛卡尔积扩展 f 和 ˆg 函数。此过程扩展其定义域，从而能够定义函数复合，以表示两步可逆数字顺序过程。我们将扩展后的函数记为 ϕ 和 γ，并在下文给出定义。推广到 n步可逆数字序列的情形也就显而易见了。

我们定义 f 和 g，其中 $f: \mathbb{B}^n \to \mathbb{B}^m$ 和 $g: \mathbb{B}^m \to \mathbb{B}^k$ 是可逆函数

$$\begin{aligned} \phi &= \hat{f} \times e^k \\ \gamma &= e^n \times \hat{g} \end{aligned}$$

其中 e^q: $\mathbb{B}^q \to \mathbb{B}^q$, $q = 1, 2, \ldots$, 是恒等函数。我们有 ϕ: $\mathbb{B}^{n+m+k} \to \mathbb{B}^{n+m+k}$,$\gamma$: $\mathbb{B}^{n+m+k} \to \mathbb{B}^{n+m+k}$，满足:

$$\begin{aligned} \phi(x,y,z) &= \hat{f} \times e^k(x,y,z) \\ &= (\hat{f}(x,y), z) \\ &= (x, y \oplus f(x), z) \end{aligned}$$

and

$$\begin{aligned} \gamma(x,y,z) &= e^n \times \hat{g}(x,y,z) \\ &= (x, \hat{g}(y,z)) \\ &= (x, y, z \oplus g(y)) \end{aligned}$$

由此我们得到

$$\begin{aligned} \gamma \circ \phi(x,y,z) &= \gamma(x, y \oplus f(x), z) \\ &= (x, y \oplus f(x), z \oplus g(y \oplus f(x))) \end{aligned}$$

and

$$\gamma \circ \phi(x, 0, 0) = (x,\ f(x),\ g(f(x))).$$

因此，不可逆顺序数字过程 $x \to g(f(x))$ 的结果，可以通过可逆方式从 $\gamma \circ \phi(x, 0, 0)$ 的第 3 个分量获得。

4 由两步可逆数字序列生成的考克斯特群

在全文中，我们用 $G(\mathbb{B}^p)$ 表示从 $\mathbb{B}^p$ 到 $\mathbb{B}^p$的可逆布尔函数在函数复合下构成的群。

4.1 扩展函数 ϕ 和 γ的性质

引理 1. 扩展函数 $\phi = \hat{} f \times e^k$ 和 $\gamma = e^n \times \hat{} g$ 均为自逆函数。

证明。我们有 $\phi(x, y, z) = (x, y \oplus f(x)\ z)$，因此

$$\begin{aligned} \phi \circ \phi(x, y, z) &= \phi(x, y \oplus f(x), z) \\ &= (x, (y \oplus f(x)) \oplus f(x), z) \\ &= (x, y, z) \end{aligned}$$

对 γ也同理。 □

因此，$\phi \in G(\mathbb{B}^{n+m+k})$ 和 $\gamma \in G(\mathbb{B}^{n+m+k})$。由此可知，函数复合 $\phi \circ \gamma$ 和 $\gamma \circ \phi$ 也都是群 $G(\mathbb{B}^{n+m+k})$ 的元素；下面将讨论它们的性质，这些性质是确立本文主要结果所必需的。

4.2 复合函数 $\gamma \circ \phi$ 和 $\phi \circ \gamma$ 的性质

引理 2。其中一个是另一个的逆，即 $(\gamma \circ \phi)^{-1} = \phi \circ \gamma$ 和 $(\phi \circ \gamma)^{-1} = \gamma \circ \phi$。

证明。由 ϕ 和 γ 都是自逆这一事实可直接得出——引理 1。 □

引理 3。 $\gamma \circ \phi(x, y, z) = (x, y \oplus f(x)\ z \oplus g(y \oplus f(x)))$。

证明。参见第 3.2 节 □

引理 4. $\phi \circ \gamma \circ \phi(x, y, z) = (x, y, z \oplus g(y \oplus f(x)))$.

证明。由引理 3 可得:

$$\begin{aligned} \phi \circ \gamma \circ \phi(x, y, z) &= \phi(x, y \oplus f(x), z \oplus g(y \oplus f(x))) \\ &= (x, y \oplus f(x) \oplus f(x), z \oplus g(y \oplus f(x))) \\ &= (x, y, z \oplus g(y \oplus f(x))). \end{aligned}$$

□

引理 5. $(\gamma \circ \phi)^2 = (x, y, z \oplus g(y \oplus f(x))\ \oplus g(y))$.

证明。由引理 4 可得:

$$\begin{aligned}(\gamma\circ\phi)^2(x,y,z) &= \gamma(x,y,z\oplus g(y\oplus f(x))\\ &= (x,y,z\oplus g(y\oplus f(x))\oplus g(y))\end{aligned}$$

□

引理 6. $\phi\circ(\gamma\circ\phi)^2=(x,y\oplus f(x)\ [z\oplus g(y\oplus f(x))]\oplus g(y))$.

证明。由引理 5 可得

$$\begin{aligned}\phi\circ(\gamma\circ\phi)^2(x,y,z) &= \phi(x,y,z\oplus g(y\oplus f(x))\oplus g(y))\\ &= (x,y\oplus f(x),z\oplus g(y\oplus f(x))\oplus g(y))\end{aligned}$$

□

引理 7. $(\gamma\circ\phi)^3(x,y,z)\ =(x,y\oplus f(x)\ z\oplus g(y))$.

证明。将 γ 应用于引理 6 的结果，得到:

$$\begin{aligned}\gamma(x,y^+,z^+) &= (x,y^+,z^+\oplus g(y^+))\\ &= (x,y\oplus f(x),([z\oplus g(y\oplus f(x))]\oplus g(y))\oplus g(y\oplus f(x)))\\ &= (x,y\oplus f(x),([z\oplus g(y\oplus f(x))\oplus g(y\oplus f(x)]\oplus g(y))))\\ &= (x,y\oplus f(x),z\oplus g(y)).\end{aligned}$$

□

引理 8. $\phi\circ(\gamma\circ\phi)^3=\gamma$.

证明。将引理 8 的结果左乘 ϕ ，得到:

$$\begin{aligned}\phi\circ(\gamma\circ\phi)^3(x,y,z) &= \phi(x,y\oplus f(x),z\oplus g(y))\\ &= (x,y,z\oplus g(y))\\ &= \gamma(x,y,z).\end{aligned}$$

□

将 $G(\mathbb{B}^{n+m+k})$ 的恒等函数记为 e，则有:

引理 9. $(\gamma\circ\phi)^4=e$,

证明。由引理 8 可得 $(\gamma\circ\phi)^4=\gamma\circ(\phi\circ(\gamma\circ\phi)^3)\ =\gamma\circ\gamma=e$。 □

等价地， $\gamma\circ\phi$ 在群 $G(\mathbb{B}^{n+m+k})$ 中的阶为 4。已知 $\gamma\circ\phi$ 的逆为 $\phi\circ\gamma$，则有:

推论 1。

$$\begin{aligned}\phi\circ\gamma &= (\gamma\circ\phi)^3,\\ (\phi\circ\gamma)^2 &= (\gamma\circ\phi)^2,\\ (\phi\circ\gamma)^3 &= \gamma\circ\phi,\\ (\phi\circ\gamma)^4 &= e.\end{aligned}$$

因此:

命题 n 1. $\gamma \circ \phi$ 和 $\phi \circ \gamma$ 在群 $G(\mathbb{B}^{n+m+k})$ 中的阶为 4 .

推论 2. $(\gamma \circ \phi)^2$ 是自逆的。

证明。由引理 9 可直接得出。 □

推论 3. $C_{\gamma,\ \phi} = \{e, \gamma \circ \phi, (\gamma \circ \phi)^2, (\gamma \circ \phi)^3)\}$ 是一个 4 阶循环群。

证明。由引理 9 可知，$(\gamma \circ \phi)^{-1} = (\gamma \circ \phi)^3$,$(\gamma \circ \phi)^2$ 是自逆的，且 $((\gamma \circ \phi)^3)^{-1} = \gamma \circ \phi$。因此，$C_{\gamma,\ \phi}$ 在求逆下封闭。显然，它在乘法下封闭。

□

推论 4. $C_{\phi,\gamma} = \{e, \phi \circ \gamma, (\phi \circ \gamma)^2, (\phi \circ \gamma)^3)\}$ 是一个 4 阶循环群。

证明。 □

推论 5. $C_{\phi,\gamma} = C_{\gamma,\phi}$。

证明。我们有

$$\begin{aligned} C_{\phi,\gamma} &= \{e, \phi \circ \gamma, (\phi \circ \gamma)^2, (\phi \circ \gamma)^3)\} \\ &= \{e, (\gamma \circ \phi)^3, (\gamma \circ \phi)^2, \gamma \circ \phi\} = C_{\gamma,\phi}. \end{aligned}$$

□

4.3 由函数 ϕ 和 γ生成的群

循环群 $C_{\gamma,\phi}$ 并非由 ϕ 和 γ生成的 $G(\mathbb{B}^{n+m+k})$ 的最大子群。我们有:

ˆ 引理10。函数 $\phi = (f \times e)$ 和 $\gamma = (e \times \hat{}g)$ 生成一个含 8 个元素的子群

$$G_{2s} = \{e, \phi, \gamma, \phi \circ \gamma, (\phi \circ \gamma)^2, (\phi \circ \gamma)^3, \phi \circ (\gamma \circ \phi), \gamma \circ (\phi \circ \gamma)\}$$

$G(\mathbb{B}^{n+m+k})$。

证明。函数 ϕ 和 γ 显然生成了 G_{2s} 的元素。根据上文已确立的 ϕ、γ 及其乘积的性质，可以轻易验证 $G_{\phi,\ \gamma}$ 在求逆和乘积运算下的封闭性。

□

引理11。引理10中定义的子群 $G_{2s} \subset G(\mathbb{B}^{n+m+k})$ 与二面体群 D_8 同构。

证明。举例来说，按照 Ledermann [3]，二面体群 D_8 可定义如下:

$$\{e, A, A^2, A^3, B, AB, A^2B, A^3B\}$$

其中 A 和 B 满足

$$A^4 = B^2 = (AB)^2 = e.$$

借助这些对应关系

$$A = \phi \circ \gamma \text{ and } B = \gamma$$

条件 $A^4 = B^2 = (AB)^2 = e$ 得到满足，因此我们有:

$$\begin{aligned} \{e, A, A^2, A^3, B, AB, A^2B, A^3B\} &= \{e, \phi \circ \gamma, (\phi \circ \gamma)^2, (\phi \circ \gamma)^3, \gamma, \phi, \phi \circ (\gamma \circ \phi), \gamma \circ (\phi \circ \gamma)\} \\ &= G_{2s}. \end{aligned}$$

□

注意，群 G_{2s} 也可以表示为

$$G_{2s} = \{e, \phi, \gamma, \gamma \circ \phi, (\gamma \circ \phi)^2, (\gamma \circ \phi)^3, \phi \circ (\gamma \circ \phi), \gamma \circ (\phi \circ \gamma)\}$$

而且，从数字计算视角来看，元素 ϕ、γ 和 $\gamma \circ \phi$ 足以表示：

1. 由 f 和 g 定义的不可逆计算，以及
2. 由可逆方式实现的两步序列，或函数复合 $g \circ f$

然而，$\{\phi, \gamma, \gamma \circ \phi\}$ 不是 G_{2s} 的子群，而且 $\gamma \circ \phi$ 并非唯一一个可由元素 γ 和 ϕ 构造出来的可逆数字序列。群 G_{2s} 显然代表了由可逆组件 ϕ 和 γ 构造出来的完整可逆数字序列（或可逆“程序”）集合。

4.4 考克斯特群

就群表示而言，群 G_{2s}（因此 D_8 也一样）可定义为：

$$G_{2s} \equiv \langle A, B | A^4 = B^2 = (AB)^2 = e \rangle$$

也就是说，由满足关系 $A^4 = B^2 = (AB)^2 = e$ 的 $\{A, B\}$ 上字符串构成的集合。自 1934 年 H. S. M. Coxeter 于 [1] 引入考克斯特群以来，人们对其进行了广泛研究。它们在数学的许多领域都有应用，并由表示定义。对于 $n > 1 \in \mathbb{N}$ 且 $1 < i, j \leq n$，由元素 $s_1, \ldots, s_n$ 生成的考克斯特群具有如下表示：

$$\langle s_1, \ldots s_n | (s_i s_j)^{m_{ij}} = e \rangle$$

其中，对于所有 $i, j \in \{1, \ldots n\}$，都有 $m_{ij} \in \mathbb{N}$，其中 $m_{ii} = 1$；对于 $i \neq j$，则有 $m_{ij} > 1$ 和 $m_{ij} = m_{ji}$

二面体群 D_{2n} 是考克斯特群的特例，其中 $n = 2$。作为考克斯特群，G_{2s} 的表示为：

$$\begin{aligned} G_{2s} &\equiv \langle s_1, s_2 | s_1 s_1 = e, s_2 s_2 = e, (s_1 s_2)^4 = e \rangle, \\ &= \langle \phi, \gamma | \phi^2 = e,\ \gamma^2 = e,\ (\phi \circ \gamma)^4 = e \rangle, \end{aligned}$$

也就是说，$m_{12} = m_{21} = 4$。

5 一般 n 步可逆数字序列的考克斯特群

5.1 3 个连续步骤的情形

对于三步可逆数字计算，根据一般可逆过程，我们得到 3 个独立对合 ϕ、γ、ρ，定义如下：

$$\begin{aligned} \phi(x, y, z, t) &= (x, y \oplus f(x), z, t) \\ \gamma(x, y, z, t) &= (x, y, z \oplus g(y), t) \\ \rho(x, y, z, t) &= (x, y, z, t \oplus h(z)) \end{aligned}$$

由不可逆数字函数 f、g 和 h（其函数乘积 $h(g(f(x)))$ 有定义），我们得到

$$\begin{aligned}\rho\circ\gamma\circ\phi(x,y,z,t) &= \rho\circ\gamma(x,y\oplus f(x),z,t)\\ &= \rho(x,y\oplus f(x),z\oplus g(y\oplus f(x)),t)\\ &= (x,y\oplus f(x),z\oplus g(y\oplus f(x)),t\oplus h(z\oplus g(y\oplus f(x)))).\end{aligned}$$

并且具有

$$\rho\circ\gamma\circ\phi(x,0,0,0)=(x,\ f(x),\ g(f(x)),\ h(g(f(x))))$$

也就是说，上述部分最后一个分量中可用的数字序列 $h(g(f(x)))$ 的结果，是通过可逆方式计算的。

不难证明，函数 ϕ、γ、ρ 满足以下关系：

$$\phi^2=\gamma^2=\rho^2=e,\ (\phi\circ\gamma)^4=e,\ (\gamma\circ\rho)^4=e,\ (\phi\circ\rho)^2=e$$

由此可知，由 ϕ、γ、ρ 生成的群是具有以下表示的考克斯特群：

$$G_{3s}\equiv\langle\phi,\gamma,\rho|\phi^2=e,\gamma^2=e,\rho^2=e,(\phi\circ\gamma)^4=e,(\gamma\circ\rho)^4=e,(\phi\circ\rho)^2=e\rangle.$$

5.2 n 个连续步骤的情形

对于 n 步不可逆数字序列 $x\to f_n\circ f_{n-1}\circ\cdots\circ f_2\circ f_1(x)$，我们根据一般可逆构造定义可逆函数 f_1、f_2、$\ldots f_n$ 及其扩张

$$\phi_1,\phi_2,\ldots,\phi_n$$

使得乘积

$$\phi_n\circ\phi_{n-1}\circ\cdots\circ\phi_1$$

is a 用于计算不可逆序列的良定义函数乘积 ce

$$f_n\circ f_{n-1}\circ\cdots\circ f_2\circ f_1$$

通过可逆方式。n 步可逆数字序列的群 G_{ns} 是由以下表示定义的考克斯特群：

$$G_{ns}\equiv\langle\phi_1,\ldots,\phi_n|\phi_1^2=\phi_2^2=\cdots=\phi_n^2=e;\ (\phi_k\circ\phi_{k+1})^4=e;\ \text{else}\ (\phi_p\circ\phi_q)^2=e\rangle$$

即，当 $q\neq p+1$ 时，我们有 $(\phi_p\circ\phi_q)^2=e$。等价地，G_{ns} 的表示可写为：

$$\langle\phi_1,\ldots,\phi_n|R_1\cup R_2\cup R_3\rangle$$

其中

$$\begin{aligned}R_1 &= \phi_1^2=\phi_2^2=\cdots=\phi_n^2=e\\ R_2 &= (\phi_k\circ\phi_{k+1})^4=e\\ R_3 &= (\phi_p\circ\phi_q)^2=e\ \text{ when }\ |q-p|\neq 1.\end{aligned}$$

6 量子序列处理

6.1 $\mathbb{B}^{n+m+k}$ 作为 G_{2s}空间

由第 3 节和第 4 节可知， G_{2s}（等价地， D_8）在 $\mathbb{B}^{n+m+k}$ 上的作用定义如下：

$$\begin{aligned}
\phi(x,y,z) &= (x, y\oplus f(x), z)\\
\gamma(x,y,z) &= (x, y, z\oplus g(y))\\
\gamma\circ\phi(x,y,z) &= (x, y\oplus f(x), z\oplus g(y\oplus f(x)))\\
(\gamma\circ\phi)^2(x,y,z) &= (x, y, z\oplus g(y\oplus f(x))\oplus g(y))\\
(\gamma\circ\phi)^3(x,y,z) &= (x, y\oplus f(x), z\oplus g(y))\\
\phi\circ(\gamma\circ\phi)(x,y,z) &= (x, y, z\oplus g(y\oplus f(x)))\\
\gamma\circ(\phi\circ\gamma)(x,y,z) &= (x, y\oplus f(x), (z\oplus g(y))\oplus g(y\oplus f(x))).
\end{aligned}$$

由此，我们定义基元素上的相应作用：

$$B_{\otimes^{n+m+k}\mathbb{C}^2} = \{|x\rangle|y\rangle|z\rangle : x\in\mathbb{B}^n, y\in\mathbb{B}^m, z\in\mathbb{B}^k\}$$

$\otimes^{n+m+k}\mathbb{C}^2$ 的作用为

$$\begin{aligned}
U_\phi|x\rangle|y\rangle|z\rangle &= |x\rangle|y\oplus f(x)\rangle|z\rangle\\
U_\gamma|x\rangle|y\rangle|z\rangle &= |x\rangle|y\rangle|z\oplus g(y)\rangle\\
U_{\gamma\circ\phi}|x\rangle|y\rangle|z\rangle &= |x\rangle|y\oplus f(x)\rangle|z\oplus g(y\oplus f(x))\rangle\\
&\vdots\\
U_{\gamma\circ(\phi\circ\gamma)}|x\rangle|y\rangle|z\rangle &= |x\rangle|y\oplus f(x)\rangle|(z\oplus g(y))\oplus g(y\oplus f(x))\rangle
\end{aligned}$$

其从 $B_{\otimes^{n+m+k}\mathbb{C}^2}$ 扩展到整个 $\otimes^{n+m+k}\mathbb{C}^2$的线性扩张确定了酉算子。

注意：

$$U_{\gamma\circ\phi}|x\rangle|0\rangle|0\rangle = |x\rangle|f(x)\rangle|g(f(x))\rangle$$

这是数字序列 $g(f(x))$ 的一种量子实现。通过测量 $U_{\gamma\circ\phi}|x\rangle|0\rangle|0\rangle$ 的 k 个量子比特 $|g(f(x))\rangle$，可以得到 $g(f(x))$ 的值。

由上述内容还可得

$$U_{\gamma\circ\phi} = U_\gamma U_\phi$$

and

命题 2. 对于 $\psi\in G_{2s}$，映射 $\psi\to U_\psi$ 是群 G_{2s} 在张量积空间 $\otimes^{n+m+k}\mathbb{C}^2$ 的酉群中的酉表示。

n 步数字序列的量子化会导出类似的结论。

7 结论

考克斯特群已被证明既出现在高层级的 n 步可逆数字序列处理中，也出现在序列处理的量子表示中。在这两种情况下，这些群

均已被证明能够代表由给定处理步骤构造出的所有可逆过程。

此外，已有研究表明，在量子情形下会出现考克斯特群的某些特定酉表示；作者尚不了解这些表示的一般性质及其特征。

参考文献

[1] H.S.M. Coxeter，由反射生成的有限群及其由反射生成的子群，《剑桥哲学学会会刊》，30，466-282（1934年）。[2] M.A. Nielson 和 I.L. Chuang，《量子计算与量子信息》，十周年纪念版，剑桥大学出版社（2010年）。[3] W. Ledermann，《有限群论导论》，大学数学教材丛书，Oliver and Boyd，（1963年）。