arXiv:2302.03579v1 [math.CO] 4 Feb 2023

一副纸牌的反洗牌

Cornelia A. Van Cott 和 Katie Wang

Abstract. 我们研究反洗牌背后的数学原理。反洗牌是一种洗牌方式，与经典的完美洗牌密切相关。进行反洗牌时，将所有纸牌交替发成两堆，然后将其中一堆叠放在另一堆上。有两种叠牌方式（左牌堆叠在上方或右牌堆叠在上方），分别称为左洗牌（L）和右洗牌（R）。我们利用反洗牌，为含有 2^k 张纸牌的一副牌，解决埃尔姆斯利问题（一个经典的数学纸牌戏法）的推广问题。我们还找到了对于所有 n 的取值，含有 $2n$ 张纸牌的一副牌所对应的置换群 $\langle L, R\rangle$ 的结构。我们证明，除非 $n \equiv 3$ （模 4），该群与完美洗牌群相同；在这种情况下，该群 $\langle L, R\rangle$ 等于 B_n，即由 $2n$ 个元素构成的中心对称置换群，而完美洗牌群是 B_n 的指数为 2 的子群。

1. Introduction

魔术师们广为人知的一种纸牌洗牌技巧，便是所谓的完美洗牌（也称为法罗洗牌）。魔术师不仅会用完美洗牌表演纸牌戏法，赌徒自 19 世纪以来也一直利用这种洗牌方式在纸牌游戏中作弊 [1, 3, 9, 11]。和所有纸牌洗牌技巧一样，我们可以从数学角度将完美洗牌视为一组扑克牌的置换。从这个角度出发，我们能更好地理解这类洗牌的特征、局限性和性质。

完美洗牌的方法如下：取一副 $2n$ 扑克牌，将牌正好分成两半。接着，将两叠牌中的扑克牌完美地交错叠在一起。交错叠牌有两种方式。外洗牌会以这样的方式交错叠牌：原牌堆的顶部和底部的扑克牌仍分别留在顶部和底部。内洗牌则会让原牌堆顶部和底部的扑克牌分别变成第二张和倒数第二张。示例见图1 。

尽管如今许多炫目的纸牌戏法都以完美洗牌为基础，但职业魔术师兼数学家 Persi Diaconis 和 Ron Graham 在 2011 年估计，一个人要学会完美洗牌，需要“几百个小时，肯定要重复上千次”。他们还补充道：“我们估计，全世界能在一分钟内完成八次完美洗牌的人不到一百个。”[5]在这种情况下，人们自然会想，是否有一种更简单的洗牌技巧，也能带来表演精彩戏法的机会。出于这一想法，Doug Ensley 在其文章《不完美魔术师的反洗牌》中介绍了所谓的反洗牌 。 [8]

反洗牌并没有那么困难。取一副有 $2n$ 张扑克牌的牌，从牌堆顶端开始，交替将牌发入两个牌堆，先发入左边的牌堆

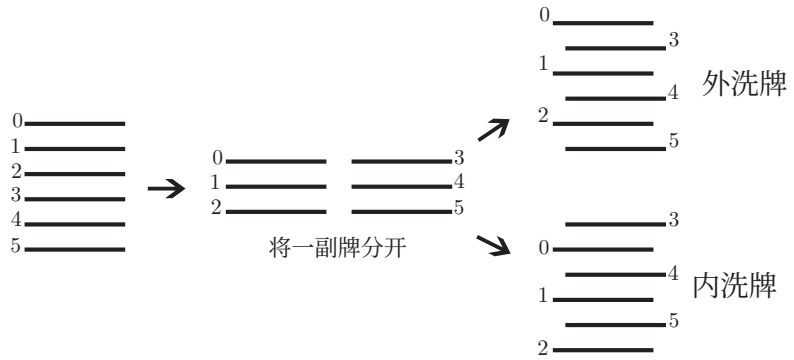

FIGURE 1. 对6张牌的牌组进行完美洗牌。

，然后发入右边的牌堆。将一个牌堆叠在另一个牌堆上，即可重新组成一副牌。有两种叠法。 右洗牌（记作 R）是将右边的牌堆叠在左边的牌堆上。 左洗牌（L）是将左边的牌堆叠在右边的牌堆上。进行右洗牌后，可以看到顶部和底部的扑克牌互换了位置；而进行左洗牌后，原先顶部和底部的扑克牌会成为整副牌中间的两张牌。图2 展示了一个由 6 张牌组成的示例。

Ensley 研究了反洗牌，并介绍了几种可以通过利用反洗牌的数学性质来实现的戏法 [8]。本文旨在继续 Ensley 对反洗牌的研究。

我们有两个主要结果。首先，我们考虑埃尔姆斯利问题，这是一种经典的数学纸牌戏法：将一副牌最上面的一张牌移到任意指定的位置。我们利用一副 2^k 张牌进行反洗牌，解决了埃尔姆斯利问题的一个推广（见定理3.3）。第二个主要结果是，我们确定了由左洗牌和右洗牌 $\langle L, R\rangle$ 在 $2n$ 张牌上生成的置换群的结构。我们证明，当 n 满足 $n \neq 3$ （模 4）时，该群与完美洗牌所生成的群相同。若$n \equiv 3$ （模 4），则由 $\langle L, R\rangle$ 个 $2n$ 张牌生成的群同构于 B_n，即所有中心对称置换构成的群。与此同时，在这种情况下， $\langle I, O\rangle$ 是B_n 的一个指数为 2 的子群。完整结果如下。

定理1.1。 假设一副牌有 $2n$张纸牌。

(a) 若 $2n = 12$，则 $\langle L, R\rangle = \langle I, O\rangle$，它同构于半直积 $\mathbb{Z}_2^6 \rtimes S_5$，其中 S_5 是作用在5 个元素上的对称群。***(b)*** 若 $2n = 24$，则 $\langle L, R\rangle = \langle I, O\rangle$，它同构于半直积 $\mathbb{Z}_2^{11} \rtimes M_{12}$，其中群 M_{12} 是 *12* 次马修群。该群的阶为 $2^{11} \cdot 95040$.。***(c)*** 若 $2n = 2^k$，则 $\langle L, R\rangle = \langle I, O\rangle$，它同构于半直积 $\mathbb{Z}_2^k \rtimes \mathbb{Z}_k$。

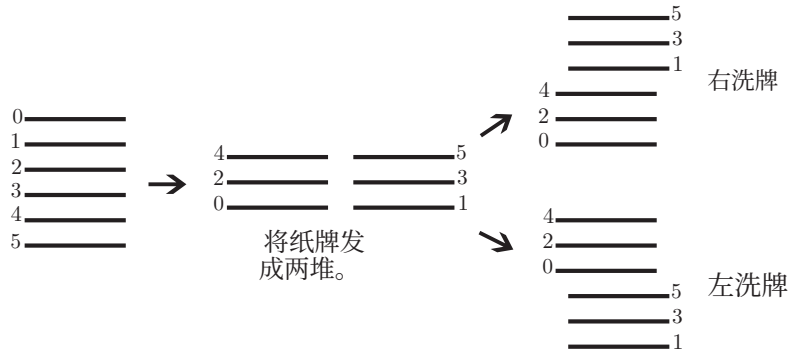

FIGURE 2. 对一副6张牌的牌组进行反洗牌。

(d) 若 $n \equiv 0$（模 *4*），$n > 12$，且 n 不是 *2* 的幂，则 $\langle L, R\rangle = \langle I, O\rangle$是 sgn 和 sgn 的核的交集，其阶为 $n!2^{n-2}$。（我们在第*4*节中定义 sgn和 sgn 。）*(e)* 若 $n \equiv 1$（模 *4*）且 $n > 1$，则 $\langle L, R\rangle = \langle I, O\rangle$ 是核 sgn，其阶为 $n!2^{n-1}$。*(f)* 若 $n \equiv 2$（模 *4*）且 $n > 6$，则 $\langle L, R\rangle = \langle I, O\rangle = B_n$，其中 B_n 是 S_{2n} 中的中心对称置换群，其阶为 $n!2^n$。*(g)* 若 $n \equiv 3$（模 *4*），则 $\langle L, R\rangle = B_n$，其阶为 $n!2^n$。

从这个结果可以看出，与使用完美洗牌相比，只进行反洗牌并不会限制能够得到的牌的排列。对于 $n \neq 3 \pmod 4$，对一副 $2n$ 张牌的牌组进行反洗牌，得到的排列集合与完美洗牌完全相同。当 $n \equiv 3 \pmod 4$ 时，反洗牌不仅能得到完美洗牌所能得到的所有排列，还能得到另一组数量相同、但完美洗牌无法得到的排列。

我们将在第 2 节研究反洗牌的数学性质。在第 3节，我们将给出埃尔姆斯利问题在一副由 2^k 张纸牌组成的牌上的推广问题的解法。我们将在第 1.1 节证明定理 4 ，具体如下：定理 4.2 证明定理 1.1的 (a) 和 (b) 部分，定理 4.3 证明 (c)，定理4.6 证明 (d)–(g)。

2. PROPERTIES OF UNSHUFFLES

在整个讨论中，我们考虑包含偶数张纸牌的一副牌，记作 $2n$。我们按照纸牌距牌顶的距离为其编制索引。因此，牌顶的第一张牌索引为 0，第二张牌索引为 1，以此类推。牌底的那张牌索引为 $2n-1$。我们将洗牌视为函数，因此从右向左读取它们的乘积。

已知一次内洗牌或外洗牌后 i^{th} 扑克牌位置的公式（例如，参见 [6, 8]）。这些公式可以用模运算表示

如下：

$$I(i) = 2i + 1 \pmod{2n+1}, \quad \text{and} \quad O(i) = \begin{cases} 2i \pmod{2n-1} & \text{if } i \neq 2n-1 \\ 2n-1 & \text{if } i = 2n-1. \end{cases}$$

同理，我们可以找到公式来表示左洗牌和右洗牌对一副纸牌的作用。注意，这些公式与上文给出的内洗牌和外洗牌公式有相似之处。

引理 2.1. 假设一副牌有 $2n$ 张。左洗牌或右洗牌后，第 i^{th} 张纸牌的索引由以下公式给出：

$$L(i) = ni + n - 1 \pmod{2n+1}, \quad \textit{and} \quad R(i) = \begin{cases} (n-1)i \pmod{2n-1} & \textit{if } i \neq 0 \\ 2n-1 & \textit{if } i = 0. \end{cases}$$

证明。从牌堆顶部开始，将一副纸牌依次交替发入两个牌堆，第一张牌发到左边后，纸牌排列成如下数组：

$$\begin{array}{cc} 2n-2 & 2n-1 \\ 2n-4 & 2n-3 \\ \vdots & \vdots \\ 2 & 3 \\ 0 & 1 \end{array}$$

将两个牌堆叠放在一起进行左洗牌后，纸牌的顺序如下：

$$2n-2, 2n-4, \ldots, 2, 0, 2n-1, 2n-3, \ldots, 3, 1.$$

左洗牌后，第 i^{th} 张纸牌的索引由以下等式给出：

$$L(i) = \begin{cases} -\frac{1}{2}i + n - 1 & \text{if } i \text{ is even} \\ -\frac{1}{2}(i+1) + 2n & \text{if } i \text{ is odd} \end{cases} \tag{1}$$

我们想将 $L(i)$ 写成关于 $\mathbb{Z}_{2n+1}$ 的表达式。注意，在 $\mathbb{Z}^*_{2n+1}$ 中，我们有 $(-2)^{-1} \equiv n$ (模 $2n+1$)，并且还有 $2n \equiv -1$ (模 $2n+1$)。因此，无论 i 是奇数还是偶数，我们都可以将 $L(i)$ 表示如下：$L(i) = ni + (n-1)$ (模 $2n+1$)。

现在让我们来考虑右洗牌。将纸牌叠放，并把右牌堆置于顶部后，纸牌的顺序如下：

$$2n-1, 2n-3, \ldots, 3, 1, 2n-2, 2n-4, \ldots, 2, 0.$$

因此，对于偶数 i，索引 $R(i)$ 只需将 n 加到 $L(i)$ 上即可得到。对于奇数 i，$R(i)$ 则由 $L(i)$ 减去 n 得到。因此：

$$R(i) = \begin{cases} -\frac{1}{2}i + 2n - 1 & \text{if } i \text{ is even} \\ -\frac{1}{2}(i+1) + n & \text{if } i \text{ is odd} \end{cases}$$

我们希望用关于 $\mathbb{Z}_{2n-1}$ 的表达式来表示 $R(i)$。对于$i = 0$，这无法做到，因为 $R(0) = 2n - 1$，所以它是一个特殊情况。但对于 $i > 0$，我们按如下步骤进行。注意，在 $\mathbb{Z}^*_{2n-1}$ 中，我们有 $(-2)^{-1} \equiv n - 1 \pmod{2n+1}$，并且还有$n \equiv 1 - n \pmod{2n-1}$。进行适当的代入后，我们发现，对于所有$i > 0$，上面的 R 公式都可以表示为： $R(i) = (n-1)i \pmod{2n-1}$. □

我们注意到，右洗牌会交换最外侧两张纸牌（纸牌 0 和$2n - 1$）的位置，并对内部的 $2n - 2$ 张纸牌进行左洗牌。示例见图2 。

利用上述公式，现在我们可以确定需要进行多少次左洗牌（或右洗牌），才能使一副牌恢复原来的排列。用数学术语来说，我们要找的是洗牌的阶。

命题 2.2。 设一副牌有 $2n$ 张。左洗牌的阶是 -2 在 $\mathbb{Z}^*_{2n+1}$中的阶。记 -2 在 $\mathbb{Z}^*_{2n-1}$ 中的阶为 r。如果 r 是偶数，那么右洗牌的阶为 r。如果 r 是奇数，那么右洗牌的阶为 $2r$。

证明。 如果重复进行左洗牌 k 次，则有： $L^k(i) = n^k i + n^k - 1$ (模 $2n+1$)。如果 k是 L的阶，那么对于所有 i，都有 $n^k i + n^k - 1 \equiv i$(模 $2n+1$)。这意味着 $n^k \equiv 1$(模 $2n+1$)。换句话说，L 的阶就是 n 在 $\mathbb{Z}^*_{2n+1}$中的阶。等价地， L 的阶就是 n 的逆在 $\mathbb{Z}^*_{2n+1}$中的阶，即 -2。

接下来考虑右洗牌。这需要多做一些工作，因为我们必须将一副牌的内部扑克牌与顶部和底部的扑克牌（扑克牌 0 和 $2n-1$）分开考虑。先从索引为 $0 < i < 2n-1$ 的纸牌开始。这些纸牌的右洗牌公式为 $R(i) = (n-1)i$，这等价于 $R(i) = -ni$，因为$n - 1 \equiv -n$ (模 $2n-1$)。将 R 与自身复合 k 次，得到 $R^k(i) = (-n)^k i$，其中 $0 < i < 2n-1$。对于所有 $0 < i < 2n-1$，都有 $R^k(i) \equiv (-n)^k i \equiv i$ (模 $2n-1$)，当且仅当 k 是 $-n$的阶的倍数。换言之， k 是 -2在 $\mathbb{Z}^*_{2n-1}$ 中的阶的倍数（它是 $-n$ 在 $\mathbb{Z}^*_{2n-1}$中的逆）。

现在来看一副牌的顶部和底部的扑克牌（第0张和第 $2n-1$张）。由于经过一次右洗牌后，顶部和底部的扑克牌会互换位置，因此，若要使 $R^k(0) = 0$ 和 $R^k(2n-1) = 2n-1$成立， k 必须是偶数。由此可得，若该值为偶数， R 的阶就是 -2 在$\mathbb{Z}^*_{2n-1}$ 中的阶；否则， R 的阶就是 -2在 $\mathbb{Z}^*_{2n-1}$中的阶的两倍。□

例2.3。 假设我们有*52*张牌。左洗牌的阶就是 -2 在 $\mathbb{Z}^*_{53}$中的阶，即52。 -2 在$\mathbb{Z}^*_{50}$中的阶是*8*，因此右洗牌的阶是*8*。

现在我们介绍第三种洗牌置换，记作 V。这种洗牌置换只是将纸牌的顺序颠倒。示例见图3 。洗牌置换 V 按如下方式改变 i^{th} 扑克牌的索引：

$$V(i) = 2n - 1 - i.$$

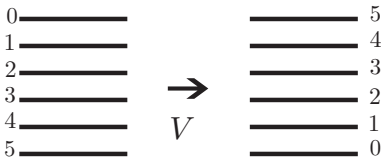

FIGURE 3. 6张牌的牌组上的洗牌置换 V。

注意到 V 的阶为 2。这种新的洗牌置换 V 有助于我们定义左洗牌和右洗牌与完美洗牌之间的联系 I 以及 O。这一联系也在 [8],的命题2中讨论。

命题2.4。 设一副牌有 $2n$ 张牌。左洗牌和右洗牌与内洗牌、外洗牌之间的关系如下： V

$$L = VI^{-1} = I^{-1}V$$
$$R = VO^{-1} = O^{-1}V$$

证明。 我们先证明 $LI = IL$。利用左洗牌和内洗牌的公式，我们计算得 $L(I(i))$ $= n(2i+1) + n - 1 = 2ni + 2n - 1$ (模 $2n+1$)，以及$I(L(i))$ $= 2(ni+n-1)$ $+1 = 2ni + 2n - 1$ (模 $2n+1$)。 LI和IL 的表达式相等，证毕。接下来，注意到：

$L(I(i))$ $= 2ni + 2n - 1 \equiv 2ni + i + 2n - 1 - i \equiv 2n - 1 - i = V(i)$（模 $2n+1$）。因此，我们已经证明了 $LI = IL = V$。等价地， $L = VI^{-1} = I^{-1}V$.

用类似的方法，我们也可以证明 $R = VO^{-1} = O^{-1}V.$ 。这留给读者完成。□

从上面的引理可以看出，左洗牌与内洗牌的逆“很接近”（只差将一副牌的顺序颠倒），而右洗牌同样与外洗牌的逆很接近。

在第 4 节中，我们将关注如何将洗牌 V 表示为完美洗牌的乘积或反洗牌的乘积。下面的引理描述了一个容易处理的特殊情形，这将在定理 4.2 中派上用场。

引理 2.5。 如果 $V = I^y$，其中 y 是偶数，那么 $V = L^y$。

证明。 由命题 2.4， $L = I^{-1}V = VI^{-1}$。利用这一点以及以下事实： $V = I^y$，y 是偶数，且 V^2 是恒等变换，我们计算得： $L^y = (I^{-1}V)^y = (I^y)^{-1}V^y = V.$ □

完美洗牌有一个重要性质，如下所述。取两张距一副牌中心等距离的纸牌。经过一次内洗或外洗牌后，这两张纸牌仍然距一副牌中心等距离。我们将在以下定义中对此作出精确定义。

定义 2.6。 置换 σ 保持 $\{0, 1, \ldots, 2n-1\}$ **中心对称**，如果对于每个 i, $j \in \{0, 1, \ldots, 2n-1\}$，只要 $i+j = 2n-1$，就有 $\sigma(i)+\sigma(j) = 2n-1$。

在魔术师中，这种保持中心对称的原理称为 保持堆叠。完美洗牌能够保持中心对称这一事实，最早由宾夕法尼亚州警员 Russell Duck 于 1957年 指出（见 [6] 第 3 节），这一发现可用于创造各种纸牌戏法。很容易证明，反洗牌也具有这一性质。

命题2.7. 左洗牌和右洗牌保持中心对称。

证明。 完美洗牌 I 和 O 保持中心对称。因此，它们的逆I^{-1} 和 O^{-1}也如此。洗牌 V 会交换每一对中心对称的纸牌，因此 V 也保持中心对称。左洗牌和右洗牌是 V 、 I^{-1}和 O^{-1} （命题 2.4 ）的复合，因此 L 和 R 也必定保持中心对称。 □

3. Elmsley's Problem with unshuffles

20世纪50年代，苏格兰计算机程序员兼魔术师 Alex Elmsley 提出了一个后来广为流传、并以他的名字命名的问题：

> **埃尔姆斯利问题**。 能否通过完美洗牌，将一副牌最上面的那张牌移到任意指定的位置?

Elmsley 本人找到了一个巧妙的解法，并将其发表在扑克牌杂志*Ibidem* （第11期，1957年9月，另见 [5, 6, 14]）上。解法如下。

定理3.1 (埃尔姆斯利问题的解答)。 从一副 $2n$ 张纸牌开始。若要将最上面的一张牌移到第 i个位置，将 i 写成二进制数，然后从左向右读取其二进制表示，令*1*代表一次内洗牌，令*0*代表一次外洗牌。按照从左向右的顺序执行这一串指定的内洗牌和外洗牌，就能将纸牌0移到第 i个位置。

这个巧妙的埃尔姆斯利问题解答引出了不少相关研究。Paul Swinford发现，在一副牌有 2^k 张纸牌这一特殊情况下，上述命题所述的洗牌序列会交换最上面一张牌与第 i^{th} 张牌的位置。更一般地，他指出，若某个洗牌序列能将纸牌 i 移到第 j 个位置，它也能将纸牌 j 移到第 i [19, 20]个位置。后来，Ramnath和Scully描述了一种方法，可以对任意一副有 $2n$ 张纸牌的一副牌 [18]，利用完美洗牌将纸牌 i 移到纸牌 j 的位置。Diaconis和Graham找到了埃尔姆斯利问题逆问题的解法（也就是通过完美洗牌将纸牌 i 移到牌堆顶端） [7]。所谓的广义完美洗牌也有埃尔姆斯利问题的解法 [13]。

用完美洗牌完成这个魔术令人印象深刻。[1] 如果可以使用反洗牌，事情就会容易一些。我们将针对一副牌有 2^k 张牌这一特殊情况，给出埃尔姆斯利问题在反洗牌条件下的解法。首先，我们证明一个引理，根据 i的二进制表示，确定左洗牌或右洗牌后第 i^{th} 张牌的位置。

[1]在此观看并了解这个魔术： https://youtu.be/Y2lXsxmBx7E

引理 3.2。 假设我们有一副包含 2^k 张牌的牌，其中 $k \geq 1$为某个数。用二进制表示法写成 i ，其中$0 \leq i \leq 2n-1$ 为二进制数： $i = x_{k-1}\ x_{k-2} \cdots x_1\ x_0$，并令$x_j = 1 - x_j$。利用二进制展开，左洗牌和右洗牌会将第 i^{th} 张牌移至新位置：

如下：

$$L(x_{k-1}\ x_{k-2} \cdots x_1\ x_0) = x_0\ \overline{x}_{k-1}\ \overline{x}_{k-2} \cdots \overline{x}_2\ \overline{x}_1,$$
$$R(x_{k-1}\ x_{k-2} \cdots x_1\ x_0) = \overline{x}_0\ \overline{x}_{k-1}\ \overline{x}_{k-2} \cdots \overline{x}_2\ \overline{x}_1.$$

证明。 根据左洗牌公式（引理 2.1）以及 $2n = 2^k$这一事实，我们有$L(i) = 2^{k-1}i + (2^{k-1} - 1)$（模 $2^k + 1$）。

代入 $i = x_{k-1} \cdot 2^{k-1} + x_{k-2} \cdot 2^{k-2} + \cdots + x_0 \cdot 2^0$ 的值：

$$L(i) = x_{k-1} \cdot 2^{2k-2} + x_{k-2} \cdot 2^{2k-3} + \cdots + x_0 \cdot 2^{k-1} + 2^{k-1} - 1 \pmod{2^k + 1}.$$

上式可以通过两种方式简化。首先注意，我们可以代入
$2^{k-1} - 1 = 1 \cdot 2^{k-2} + 1 \cdot 2^{k-3} + \cdots + 1 \cdot 2^0$。其次，由于 $2^k \equiv -1$（模 $2^k + 1$），我们可以用 $-x_j \cdot 2^{j-1}$ 替换 $x_j \cdot 2^{j+(k-1)}$。

$$\begin{aligned} L(i) &\equiv -x_{k-1} \cdot 2^{k-2} - x_{k-2} \cdot 2^{k-3} - \cdots - x_1 \cdot 2^0 + x_0 \cdot 2^{k-1} + 2^{k-1} - 1 \\ &\equiv x_0 \cdot 2^{k-1} + (1 - x_{k-1}) \cdot 2^{k-2} + (1 - x_{k-2}) \cdot 2^{k-3} + \cdots + (1 - x_1)2^0 \\ &\equiv x_0 \cdot 2^{k-1} + \overline{x}_{k-1} \cdot 2^{k-2} + \overline{x}_{k-2} \cdot 2^{k-3} + \cdots + \overline{x}_1 2^0 \pmod{2^k + 1} \end{aligned}$$

其中 $\overline{x_j} = 1 - x_j$。我们得到了所需的结论：

$$L(x_{k-1}\ x_{k-2} \cdots x_1\ x_0) = x_0\ \overline{x}_{k-1}\ \overline{x}_{k-2} \cdots \overline{x}_2\ \overline{x}_1.$$

我们对右洗牌使用相同的方法。 $i > 0$ 的右洗牌公式为：$R(i) = (2^{k-1} - 1)i \pmod{2^k - 1}$。由于 $2^{k-1} - 1 \equiv -2^{k-1} \pmod{2^k - 1}$，因此我们有

$$R(i) \equiv -2^{k-1}i \pmod{2^k - 1}$$

对于 $i > 0.$，代入 $i = x_{k-1} \cdot 2^{k-1} + x_{k-2} \cdot 2^{k-2} + \cdots + x_0 \cdot 2^0$ 并利用 $2^k \equiv 1 \pmod{2^k - 1}$这一事实，我们有：

$$\begin{aligned} R(i) &\equiv (-2^{k-1})(x_{k-1} \cdot 2^{k-1} + x_{k-2} \cdot 2^{k-2} + \cdots + x_1 \cdot 2^1 + x_0 \cdot 2^0) \\ &\equiv -x_{k-1} \cdot 2^{2k-2} - x_{k-2} \cdot 2^{2k-3} - \cdots - x_1 \cdot 2^k - x_0 \cdot 2^{k-1} \\ &\equiv -x_{k-1} \cdot 2^{k-2} - x_{k-2} \cdot 2^{k-3} - \cdots - x_1 \cdot 2^0 - x_0 \cdot 2^{k-1} \pmod{2^k - 1} \end{aligned}$$

现在注意到 $1 \cdot 2^{k-1} + 1 \cdot 2^{k-2} + \cdots + 1 \cdot 2^0 = 2^k - 1 \equiv 0 \pmod{2^k - 1}$。因此，我们可以将它加到上面的表达式中，而不改变其值：

$$\begin{aligned} R(i) &\equiv (1 - x_0) \cdot 2^{k-1} + (1 - x_{k-1}) \cdot 2^{k-2} + \cdots + (1 - x_1) \cdot 2^0 \\ &\equiv \overline{x}_0 \cdot 2^{k-1} + \overline{x}_{k-1} \cdot 2^{k-2} + \cdots + \overline{x}_1 \cdot 2^0 \pmod{2^k - 1}, \end{aligned}$$

其中 $\overline{x_j} = 1 - x_j$。这就证明了关于 $i > 0$的结论。

对于特殊情况 $i = 0$，注意我们有如下结果，正如所期望的 d:

$$R(0) = 2^k - 1 = 1 \cdot 2^{k-1} + 1 \cdot 2^{k-2} + \cdots + 1 \cdot 2^0.$$

□

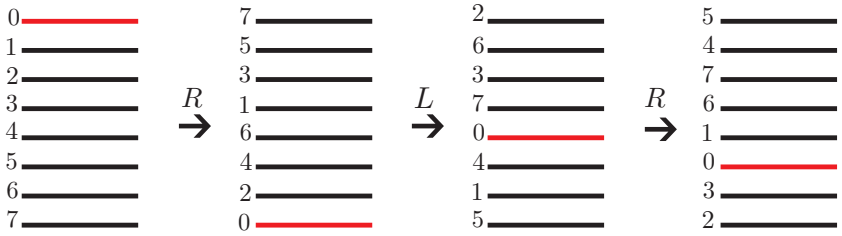

FIGURE 4. 将顶牌移至第 5 个位置的反洗牌。

现在，我们给出并证明使用反洗牌解决埃尔姆斯利问题的方法，适用于有 2^k 张纸牌的情况。事实上，我们解决的是一个更一般的问题。我们描述的过程会在 i 次洗牌置换中交换第 i 张扑克牌和第 j 张扑克牌的位置，其中 k 适用于任意 i，且 j。因此，我们可以将其特化到 $i = 0$ 的情况，从而得到埃尔姆斯利问题的解。

定理3.3。 假设有 2^k 张纸牌，其中 $k \geq 1$。要通过反洗牌交换位置 i 和 j 上的纸牌，请将 i 和 j 写成二进制形式，并计算 $i \oplus j = x_{k-1}\ x_{k-2} \cdots x_1\ x_0$（其中 $\oplus$ 表示异或运算）。用 k次洗牌置换洗牌，依次记为 S_0、S_1、……、S_{k-1}，其中 S_r 定义如下：

(1) 如果 k 是奇数，

$$S_r = \begin{cases} L & if\ x_r = 0 \\ R & if\ x_r = 1 \end{cases}$$

(2) 如果 k 是偶数，

$$S_r = \begin{cases} R & if\ x_r = 0 \\ L & if\ x_r = 1 \end{cases}$$

这一系列洗牌置换将交换位置 i 和 j上的纸牌。

证明。 引理 3.2 告诉我们，左洗牌和右洗牌都会使扑克牌索引的各位向右移动 1 位，并将最后一位移到最前面。由于总共有 k 位，因此，进行 k 次洗牌（左洗牌、右洗牌或两者混合）后，所有各位都会回到原来的位置（其中一些位可能会翻转）。此外，完成这 k 次洗牌后，每一位翻转的次数只能是 k次或 $k-1$次。某一位 x_r 翻转的确切次数，取决于第 r^{th} 次洗牌的类型。如果 x_r是右洗牌，那么该位将翻转 k 次；如果 S_r 是左洗牌，那么该位将翻转 $k-1$ 次。

利用这一点，我们可以设计一系列 k洗牌置换 $S_0, S_1, \ldots, S_{k-1}$，将 j 的二进制展开变为 i 的二进制展开，反之亦然。首先，通过计算 $i \oplus j = x_{k-1}\ x_{k-2} \cdots x_1\ x_0$，找出 j和 i不同的位。

如果 $x_r = 0$，那么我们无需更改 j 的 r^{th} 位，并且可以根据 k 的奇偶性来安排洗牌置换，使得洗牌完成后 r^{th} 位保持不变

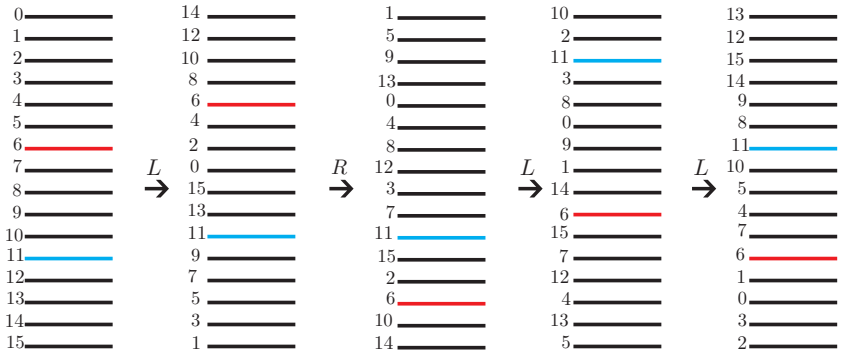

FIGURE 5. 交换第6张牌和第11张牌位置的反洗牌。

。也就是说，如果 k 为奇数，则设置 $S_r = L$，因为这样会使 j 的 r^{th} 位翻转 $k-1$ 次，从而保持不变。如果 k 为偶数，则设置 $S_r = R$，而 j 的 r^{th} 位将翻转 k 次，从而保持不变。

同样，如果 $x_r = 1$，那么 i 和 j 的位不同。我们根据 k 的奇偶性来安排洗牌，使 r^{th} 位翻转。如果 k 是奇数，则设 $S_r = R$，这样 j 的r^{th} 位就会翻转。如果 k 是偶数，则设 $S_r = L$。

这定义了一列 k次洗牌置换： S_0， S_1，……， S_{k-1}。依次执行这些洗牌置换，会使 j 的所有位都与 i 的对应位相同，反之亦然。因此，经过这一列洗牌置换后，位于 i 和 j 的纸牌将交换位置。□

例3.4。 下面通过两个例子说明这个埃尔姆斯利问题的解法：一个例子中 k 为奇数，另一个例子中 k 为偶数。假设有*8*张纸牌，我们希望顶牌与第 5th 张牌交换位置。我们计算 $000_2 \oplus 101_2 = 101_2$。洗牌置换应按以下顺序执行： R， L， R。参见图 *4*。

现在假设有 *16* 张纸牌，我们想交换 6th 号位置和 11th 号位置上的纸牌。用二进制表示，写作 $6 = 0110_2$ 和 $11 = 1011_2$。我们计算$0110_2 \oplus 1011_2 = 1101_2$。定理 *3.3* 告诉我们，按以下阶进行洗牌置换 L， R， L， L 即可交换这两张牌。见图*5*。

4. THE PERMUTATION GROUPS OF UNSHUFFLES

现在我们来考察置换群 $G = \langle L, R\rangle$的结构。通过这一点，我们将准确了解使用反洗牌可以得到哪些牌的排列。在某些（但并非所有）情况下，置换群 $\langle L, R\rangle$ 与 $\langle I, O\rangle$相同。鉴于完美洗牌与反洗牌之间密切的关系（命题2.4），两群经常相同这一事实并不十分令人意外。不过，证明细节需要仔细处理。我们通过一组三个定理（定理1.1 由定理4.2、4.3和4.6）来证明。

首先回顾一下完美洗牌的置换群。令 B_n 为由 $2n$ 个元素构成的所有中心对称置换组成的群。这个群也可以

确定为所有带符号的 $n \times n$ 置换矩阵组成的群。由于 L, R, I和O 本身都是中心对称置换，因此 $\langle L, R\rangle$和 $\langle I, O\rangle$ 都是 B_n的子群。

我们在 B_n 上定义几个同态。首先令

$$sgn : B_n \longrightarrow \{\pm 1\}$$

为满足 $sgn(g)$ 等于置换 g 的符号（或奇偶性）的同态。接下来注意到，虽然每个置换 $g \in B_n$ 都是对 $2n$ 个元素的置换，但 g 会在这 n 个中心对称对上诱导出一个置换。我们定义一个同态

$$\phi : B_n \longrightarrow S_n$$

，令 $\phi(g)$ 等于 g 在这 n 个中心对称对上诱导出的置换。接下来我们定义

$$\overline{sgn} : B_n \longrightarrow \{\pm 1\}$$

，令 $sgn(g)$ 等于置换 $\phi(g) \in S_n$ 的符号。最后，我们可以如下得到一个同态。令 $sgnsgn$: $B_n \longrightarrow \{\pm 1\}$ 为将 g 映射到乘积 $sgn(g)sgn(g)$ 的同态。

现在我们已经准备好陈述 $\langle I, O\rangle$ 的群结构。前面三项分别是在一副牌的大小为 12、24 或 2 的幂时的特殊情形。在此之外，群结构由 n 模 4 的同余类决定。有关证明和完整细节，请参阅 [6]。

定理 4.1. [6] 扑克牌 $2n$ 上的置换群 $\langle I, O\rangle$ 的结构如下：

(1) 如果 $2n = 12$，那么 $\langle I, O\rangle$ 同构于半直积 $\mathbb{Z}_2^6 \rtimes S_5$，其中$S_5$ 是 *5* 个元素上的对称群。*(2)* 如果 $2n = 24$，那么 $\langle I, O\rangle$ 同构于半直积 $\mathbb{Z}_2^{11} \rtimes M_{12}$，其中 M_{12} 是 *12* 次马修群。*(3)* 如果 $2n = 2^k$，$\langle I, O\rangle$ 同构于半直积 $\mathbb{Z}_2^k \rtimes \mathbb{Z}_k$。*(4)* 如果 $n \equiv 0$ *(*模 *4)*，$n > 12$，且 n 不是 *2* 的幂，那么 $\langle I, O\rangle$ 是 sgn和 sgn的核的交集，且其阶为 $n!2^{n-2}$。*(5)* 如果 $n \equiv 1$ *(*模 *4)*且 $n > 1$，那么 $\langle I, O\rangle$ 是核 sgn，且其阶为$n!2^{n-1}$。*(6)* 如果 $n \equiv 2$ *(*模 *4)*且 $n > 6$，那么 $\langle I, O\rangle = B_n$，且其阶为 $n!2^n$。*(7)* 如果 $n \equiv 3$ *(*模 *4)*，那么 $\langle I, O\rangle$ 等于 $sgn \cdot sgn$ 的核，且其阶为$n!2^{n-1}$。

现在我们转而考察群 $G = \langle L, R\rangle$。我们首先证明，在 $2n$ 为 12 或 24 的情形（定理 4.2），以及 $2n$ 为 2 的幂的情形（定理 4.3），$G = \langle L, R\rangle$与完美洗牌群重合。

定理 4.2。 如果 $2n = 12$ 或 $2n = 24$，那么 $\langle L, R\rangle = \langle I, O\rangle$。

证明。 我们首先注意到， I^r 的公式为:

$$I^r(i) \equiv 2^r i + 2^{r-1} + 2^{r-2} + ... + 1 \equiv 2^r i + 2^r - 1 \pmod{2n+1}.$$

现在假设我们有 $2n = 12$ 张纸牌。注意到

$$I^6(i) = 2^6(i) + 2^6 - 1 \equiv 11 - i = V(i) \pmod{13}.$$

因此 $V = I^6$。引理 2.5 现在推出 $V = L^6$。由于我们可以将V表示为 I的形式，命题 2.4 便推出 $\langle L, R\rangle \subseteq \langle I, O\rangle$。此外，由于我们可以将 V表示为 L的形式，因此可推出 $\langle I, O\rangle \subseteq \langle L, R\rangle$。因此 $\langle L, R\rangle = \langle I, O\rangle$。

同理，对于 $2n = 24$ 张纸牌，我们有

$$I^{10}(i) = 2^{10}(i) + 2^{10} - 1 \equiv 23 - i = V(i) \pmod{25}.$$

由于 $V = I^{10}$，引理 2.5 推出 $V = L^{10}$。针对 12 张纸牌的相同论证也适用于 24 张纸牌，因此 $\langle L, R\rangle = \langle I, O\rangle$ 对于 $2n = 24$ 的情形也成立。 □

定理 4.3。 假设 $2n = 2^k$，其中 k 是某个正整数。那么 $\langle L, R\rangle = \langle I, O\rangle$。

证明。 利用证明定理 I^r(i时提到的公式4.2 并令$r = k$，我们得到:

$$I^k(i) \equiv 2^k i + 2^k - 1 \equiv -i + 2^k - 1 = V(i) \pmod{2^k + 1}.$$

因此 $V = I^k$. 这意味着 L 和 R 可以根据命题 I和 O表示为它们的组合2.4。于是 $\langle L, R\rangle \subseteq \langle I, O\rangle$.

现在我们证明 $\langle I, O\rangle \subseteq \langle L, R\rangle$，根据$k$的奇偶性分两种情况讨论。假设 k 是偶数。从命题 $L = VI^{-1}$ 的等式2.4开始。将等式两边分别与自身复合 k 次，得到

$$L^k = (VI^{-1})(VI^{-1}) \cdots (VI^{-1}) = V^k I^{-k} = I^{-k},$$

因为 V和 I^{-1} 可交换，且 k 是偶数。代入 $V = I^k$ 并记住 $V = V^{-1}$，我们得到 $L^k = V.$ 。这意味着 I 和 O 可以用 L和 R表示，其中 k为偶数。因此 $\langle I, O\rangle \subseteq \langle L, R\rangle$，这就如我们所愿，证明了 $\langle I, O\rangle = \langle L, R\rangle$在 k 为偶数时成立

假设 k 是奇数。从 $R = VO^{-1}$ (命题 2.4中的结论)出发，将等式两边各自与自身复合 k 次。记住 O^{-1} 和 V 可交换，并利用 O^{-k} 是恒等变换（因为 $O^k(i) = 2^k i \equiv i$ (模 $2^k - 1$)），我们得到

$$R^k = (VO^{-1})(VO^{-1}) \cdots (VO^{-1}) = V^k O^{-k} = V^k = V.$$

因此，当 k为奇数时， $V = R^k.$。与之前类似，我们得出 $\langle I, O\rangle \subseteq \langle L, R\rangle$，这就如我们所愿，证明了 $\langle I, O\rangle = \langle L, R\rangle$ 在 k为奇数时成立 □

既然上述特殊情形已经解决，接下来更艰巨的任务是考察一般情形。我们必须先给出一些预备定义并证明两个引理。

令 G^* 表示 $G = \langle L, R\rangle$ 的子群，它由 G 中所有使集合 $\{0, 1, \ldots, n-1\}$ 保持不变的洗牌置换构成。由于 G^* 中的所有洗牌置换也必须保持中心对称，因此 G^* 中的元素可以表示为 $\sigma\sigma'$，其中 σ 是 $\{0, 1, \ldots, n-1\}$ 的一个置换，而 σ' 表示元素 $\{0', 1', \ldots,$ 的相应置换（$n-1$）$'\}$，其中 $r' = 2n - 1 - r$。因此， G^*中的元素 $\sigma\sigma'$完全由 σ确定。下面我们将始终使用这一记号，并证明两个引理。

引理 4.4. 设 $n > 1$ 满足： n 不是 *2* 的幂，且 $n \neq 6$,12。群G^* 包含所有形如 $\sigma\sigma'$ 的置换，其中 σ 是$\{0, 1, \ldots, n-1\}$ 上的任意偶置换， σ' 则如上所定义。

证明。在 [6], 中，作者介绍了若干由完美洗牌构造的有用置换，这些置换在我们的情形中也很有用。令 k 和 r 为正整数，并定义：

$$
\begin{aligned}
c &= O(I^{-1}OIO^{-1})^2O^{-1} \\
w &= O^{-1}Ic^{-1}O^{-1}Ic^2I^{-1}Oc^{-1}I^{-1}O \\
b &= (I^kO^{-k}I^{-1}O)^{-2} \\
c' &= ObO^{-1} \\
h(r) &= O^{-r}I^r
\end{aligned}
$$

所有这些置换也都可以通过左洗牌和右洗牌来实现。为此，只需将 $I = VL^{-1}$ 和 $O = VR^{-1}$ 代入上面的表达式。由于V 与 L 和 R 都可交换，且 V^2 是恒等变换，最终得到的是左洗牌和右洗牌的乘积。

在 [6], 的引理 9 中，作者证明了当 n 为奇数时， c 和 w 生成所有形如 $\sigma\sigma'$的置换，其中 σ是 $\{0, 1, \ldots, n-1\}$上的偶置换。因此，我们的结果在 n 为奇数时得证。

现在假设 n 是偶数， n 不是 2 的幂，且 $n \neq 6$,12。令 $2n = 2^kv$，其中 $v > 1$，且 v 为奇数。在 [6], 的引理 15、16、17 和 18 中，作者证明了：在满足关于 n 的上述条件时，洗牌置换 b, c', h(1) h(2) $\ldots, h(k-1)$ 生成所有置换 $\sigma\sigma'$，其中 σ 是 $\{0, 1, \ldots, n-1\}$ 的偶置换。因此，我们关于左洗牌和右洗牌的结果也随之成立。□

我们还必须证明一个预备引理，不过首先要引入一些记号并作些观察。回想一下，同态 ϕ ： $B_n \longrightarrow S_n$ 的定义是将 $\phi(g)$指定为 g 在 n 中心对称对上诱导的置换。在 [6], 中，作者发现置换 I、 O、 $\phi(I)$和 $\phi(O)$的奇偶性取决于 n 模 4 的同余类（见 [6]中的表 3）。还要记住，对于 $0 \leq i \leq n-1$， V会将位置 i 上的扑克牌与位置 i' 上的扑克牌交换，因此 V是 n 个对换的乘积： $V = (0, 0')(1, 1')(2, 2') \cdots (n-1, (n-1)')$。因此， V 的奇偶性为$(-1)^n$。此外， $\phi(V) = (1)$，即恒等置换。

	L	R	$\phi(L)$	$\phi(R)$
$n \equiv 0$ (模 4)	1	1	1	1
$n \equiv 1$ (模 4)	1	-1	1	1
$n \equiv 2$ (模 4)	-1	-1	-1	1
$n \equiv 3$ (模 4)	-1	1	1	-1

TABLE 1. n模 4 的同余类的奇偶性： L、 R、 ϕ（L）、 ϕ（R）。

因此， $\overline{sgn}(V) = 1$。这些奇偶性以及命题 2.4中关于完美洗牌与反洗牌之间关系的结论，有助于我们构造表 1 ，列出L、 R、 $\phi(L)$、和 $\phi(R)$的奇偶性。我们将经常用到该表。

同态 ϕ： $B_n \longrightarrow S_n$ 的核由所有对换（x， x'）生成，其中 $x \in \{0, 1, \ldots, n-1\}$ 和 $x' = 2n-1-x$。这些对换彼此交换。因此， ker（ϕ）是一个阶为 2^n 的群。我们将同态 ϕ 在 G 上的限制记为 $\phi|_G$，并将 $\phi|_G$ 的核记为 K。下面的引理将求出 K 的阶。

引理 4.5。 设 $n > 1$ 满足： n 不是 *2* 的幂，且 $n \neq 6$、12，并令 K 表示同态 $\phi|_G$ 的核。如果 $n \equiv 0$ （模 4），那么 $|K| = 2^{n-1}$。否则， $|K| = 2^n$。

证明。 我们首先按如下方式构造一个置换 $f \in B_n$ ：

$$f(i) = \begin{cases} L(i) & \text{if } i \text{ is even and } 0 \leq i \leq n-1 \\ & \quad \text{or if } i \text{ is odd and } n \leq i \leq 2n-1 \\ L(i)' & \text{if } i \text{ is odd and } 0 \leq i \leq n-1 \\ & \quad \text{or if } i \text{ is even and } n \leq i \leq 2n-1 \end{cases}$$

我们构造这个置换的动机是 f 在中心对称对上诱导的置换与 L 相同，因此 $\phi(f)$ $= \phi(L)$，但与 L不同，置换f保持集合 $\{0, 1, \ldots, n-1\}$ 不变（因此，当然， f也保持集合$\{n, n+1, \ldots, 2n-1\}$ 不变）。验证这一点，请参阅关于 1 的方程 $L(i)$。我们将在全文中使用 f 。

现在假设 $n \equiv 0$， 1，或模 4 余 3。在这种情况下，表 1 告诉我们 $\phi(L)$ 是一个 偶置换。用 $\sigma \in S_n$ 表示这个置换。由此可得 $f = \sigma\sigma'$。根据引理 4.4，由于 σ 是偶置换，我们知道 f 是 G^* 的一个元素。因此， f 可以通过左洗牌和右洗牌来实现。

现在考虑置换： $f^{-1}L$。用轮换表示法写出，我们有： $f^{-1}L$ =$(11')(33') \cdots (kk')$，其中如果 n 为偶数，则 $k = n-1$ ；如果 n 为奇数，则 $k = n-2$ 。

在 $n=3$，4、或 5 这一特殊情况下，我们已经具备了继续所需的全部要素；但对于 $n>5$，我们还需要定义一个额外的要素： $g=(0,\ 1)(3,\ 5)(0',\ 1')(3',\ 5')$。注意，根据引理 4.4，我们知道 $g\in G^*$，因此 g 也可以通过左洗牌和右洗牌实现。准备好这些要素后，我们来构造置换 h:

$$h=\begin{cases} f^{-1}L=(11') & \text{if } n=3 \\ f^{-1}L=(11')(33') & \text{if } n=4,5 \\ (f^{-1}L)g(f^{-1}L)g=(00')(11') & \text{if } n>5 \end{cases}$$

注意到，由于 $f,L,g\in G$，这个置换 h 也是 G 的一个元素。此外， $h\in K$，因为 h 是形如 (xx') 的对换之积。

现在假设 $n=3$。用 G^* 中的元素对 $h=(11')$ 进行共轭，我们生成 $(00')$,$(11')$, 以及 $(22')$，它们都属于 K。这三个元素合起来将生成一个含 8 个元素的集合。因此 $|K|\geq 2^3$. 。但另一方面，我们知道$|K|\leq 2^3$，因为 K 是 ϕ 的核的子群，所以 $|K|=2^3$。至此， $n=3$. 的论证完成。

接下来假设 $n\geq 4$ （并继续假设 $n\equiv 0$,1, 或 3（模 4））。用 G^* 中的元素对 h 进行共轭，可知所有形如 $(yy')(zz')$ 且满足$y,z\in\{0,1,\ldots,n-1\}$ 的元素都属于 K。将这些形如 $(yy')(zz')$ 的元素以所有可能的方式相乘，就能得到由偶数个这类对换组成的任意乘积。这类乘积的总数（它们都属于 K）为:

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots=2^{n-1}.$$

因此 $|K|\geq 2^{n-1}$当 $n\equiv 0$、1、3 (mod 4) 且 $n\geq 4$ 时。

若 $n\equiv 2$ (mod 4)，我们可以用与上述类似的论证证明 $|K|\geq 2^{n-1}$。在这种情况下， $\phi(R)$ 是偶置换，而不是 $\phi(L)$，因此论证只需将 L 改为 R 并作出相应调整即可。我们将这些细节留给读者，并继续假设对于所有 n， $|K|\geq 2^{n-1}$ 。

若 $n\equiv 0$ (mod 4)，则 L 和 R 都是偶置换，因此K 中的所有置换都是偶置换。由于 K 是 ϕ 的核的一个子群，其中包含奇置换且阶为 2^n，我们知道 $|K|<2^n$。另一方面，正如我们上面所展示的，$|K|\geq 2^{n-1}$。因此， $|K|=2^{n-1}$，证毕。

如果 $n\equiv 3$ （模 4），那么 L 是 K 中的一个奇置换，而 $f^{-1}L$ 也是一个奇置换。将 $f^{-1}L$ 与我们上文构造的 K 中偶置换集合里的元素相乘，就会在 K 中生成另一个 2^{n-1} 个互不相同的元素。因此$|K|\geq 2^{n-1}+2^{n-1}=2^n$。另一方面，我们知道 $|K|\leq 2^n$，因为 K 是 ϕ 的核的一个子群，所以结论成立。

最后，假设 $n\equiv 1$或 2（模 4）。在这种情况下， R 是一个奇置换，而 $\phi(R)$ 是偶置换。与之前类似，令 $k\in G^*$，使得 $\phi(k)=\phi(R)$。那么 kR^{-1}是 K中的一个奇置换。与前一种情况一样，可以推出 $|K|=2^n$. □

现在，我们已经准备好确定 $G = \langle L, R\rangle$ 的群结构，其中所有 $n > 1$满足 n 不是 2 的幂且 $n \neq 6$，12。

定理 4.6。 假设一副牌有 $2n$ 张扑克牌，并令 $G = \langle L, R\rangle$。

(a) 若 $n \equiv 0$ （模 4），则 $n > 12$；且若 n 不是 *2* 的幂，则 $G = \langle I, O\rangle$。

(b) 若 $n \equiv 1$ （模 4）且 $n > 1$，则 $G = \langle I, O\rangle$。*(c)* 若 $n \equiv 2$ （模 4）且 $n > 6$，则 $G = \langle I, O\rangle = B_n$。*(d)* 若 $n \equiv 3$ （模 4），则 $G = B_n$。

证明。 在所有情况下，我们都知道 $A_n \subseteq \phi\left(G^*\right) \subseteq \phi\left(G\right)$ 由引理 4.4得出，并且我们将经常使用这一事实。

我们先证明 (a)。注意，对于 $\phi(L)$ 和 $\phi(R)$，它们都是偶置换，其中 $n \equiv 0$(模 4)（表 1）。因此，我们得出 $\phi(G) = A_n$，因为 $A_n \subseteq \phi(G^*) \subseteq \phi(G)$。根据第一同构定理和引理 4.5，可得 $|G| = |A_n||K| = n! \cdot 2^{n-2}$。

接下来我们证明，当 $n \equiv 0$ (模 4) 时，$G = \langle L, R\rangle \subseteq \langle I, O\rangle$。由于 $L = VI^{-1}$和 $R = VO^{-1}$，只需证明 $V \in \langle I, O\rangle$。根据定理 4.1，$\langle I, O\rangle$ 是 sgn 和sgn的核的交集。我们已经讨论过，V 的奇偶性是 $(-1)^n$，并且由于 n 是偶的，$sgn\left(V\right) = 1$。我们还知道 $sgn\left(V\right) = 1$。因此可得 $V \in \langle I, O\rangle$，从而 $\langle L, R\rangle \subseteq \langle I, O\rangle$。由于这两个群的阶相同，我们得出 $G = \langle L, R\rangle = \langle I, O\rangle$。

对于 (b)，我们可以用与 (a) 类似的论证来证明 $|G| = |A_n||K|$。根据引理 4.5，$|G| = n! \cdot 2^{n-1}$。现在，定理 4.1 告诉我们，对于 $n \equiv 1$ （模 4），群 $\langle I, O\rangle$ 等于sgn的核。由于 $sgn(V) = 1$，我们知道 $V \in \langle I, O\rangle$。因此，$G = \langle L, R\rangle \subseteq \langle I, O\rangle$。由于两个群的阶相同，因此必有 $G = \langle L, R\rangle = \langle I, O\rangle$。

现在我们证明 (c)。注意，$\phi(L)$ 在 $n \equiv 2$ （模 4）时为奇数。因此，我们可以得出 $\phi(G) = S_n$，因为 A_n 与 $\phi(L)$ 一起将生成 S_n的所有置换。根据第一同构定理和引理 4.5，我们有 $|G| = |S_n||K| = n! \cdot 2^n$。现在 $\langle L, R\rangle$ 是 B_n的一个子群，但由于两个群的阶相同，我们得出 $G = \langle L, R\rangle = \langle I, O\rangle = B_n$。

我们对 (d) 的证明与 (c) 的证明类似。在这种情况下，奇数的是 $\phi(R)$，而不是 $\phi(L)$ （表 1 ）；但同样地，我们可以得出结论：$\phi(G) = S_n$。第一同构定理和引理 4.5 告诉我们 $|G| = |S_n||K| = n! \cdot 2^n$。我们知道 $G = \langle L, R\rangle \subseteq B_n$，但由于这两个群的阶相等，我们便得到所需结论 $G = B_n$。 □

例 4.7。 完美洗牌群与反洗牌群最早出现差异的最小情形是 n，即 $n = 3$ （一副有 *6* 张牌的牌组）。一副有 *6* 张牌的牌组共有 $6! = 720$ 种可能的排列。完美洗牌和反洗牌分别只能实现 *24* 种和 *48* 种牌的排列。

特别是，定理 *4.1* 告诉我们，群 $\langle I, O\rangle$ 等于$sgnsgn$ 的核。该核是一个 *24* 阶群，同构于 S_4，即作用在 *4* 个元素上的对称群。另一方面，定理 *4.6* 告诉我们，群 $\langle L, R\rangle$ 是 B_3，也就是由

所有 *6* 个元素的中心对称置换构成的群。该群的阶为 *48*，同构于直积 $S_4 \times \mathbb{Z}_2$。

这里我们将重点限于完美洗牌和反洗牌，不过还有许多不同的洗牌技术，能带来数学上的乐趣 [2,4, 10, 12, 13, 16]。有三本精彩的科普书籍深入探讨了这些想法，并介绍了有趣的数学纸牌戏法，可用来给亲友留下深刻印象： [5, 15, 17]。

References

[1] 匿名。《赌博科学大揭秘》。纽约：F. A. Brady，1860 年。[2] Dave Bayer 和 Persi Diaconis。《追踪燕尾洗牌，直至其巢穴》。Ann. Appl. Probab.，2(2)：294–313，1992 年。[3] Frederick Braue 和 Jean Hugard。《专业纸牌技术》。Martino Publishing，1940 年。[4] Steve Butler、Persi Diaconis 和 Ron Graham。《翻转洗牌与马蹄洗牌的数学》。Amer. Math. Monthly，123(6)：542–556，2016 年。[5] P. Diaconis 和 R. Graham。《魔法数学：赋予精彩魔术戏法生命的数学思想》。普林斯顿大学出版社，2011 年。[6] Persi Diaconis、R. L. Graham 和 William M. Kantor。《完美洗牌的数学》。Adv. in Appl. Math.，4(2)：175–196，1983 年。[7] Persi Diaconis 和 Ron Graham。《埃尔姆斯利问题的解答》。Math Horizons，14(3)：22–27，2007 年。[8] Doug Ensley。《不完美魔术师的反洗牌》。Math Horizons，11(3)：13–16，2004 年。[9] J. H. Green。《赌博的技艺与苦难揭秘》。宾夕法尼亚州费城：G. B. Zieber，1847 年。[10] Samuel Johnson、Lakshman Manny、Cornelia A. Van Cott 和 Qiyu Zhang。《广义完美洗牌一瞥》。Involve，14(5)：813–828，2021 年。[11] Charles T. Jordan。《三十个纸牌谜题》。加利福尼亚州彭格罗夫，1919 年。[12] Arne Ledet。《二次幂张数牌组的蒙日洗牌》。Math. Scand.，98(1)：5–11，2006 年。[13] Steve Medvedoff 和 Kent Morrison。《完美洗牌群》。Math. Mag.，60(1)：3–14，1987 年。[14] S. Brent Morris。《法罗洗牌的基础数学》。Pi Mu Epsilon J.，6：85–92，1975 年。[15] S. Brent Morris。《魔术戏法、洗牌与动态计算机存储器》。MAA Spectrum。美国数学协会，华盛顿特区，1998 年。Martin Gardner 作序。[16] S. Brent Morris 和 Robert E. Hartwig。《广义法罗洗牌》。Discrete Math.，15(4)：333–346，1976 年。[17] C. Mulcahy。《数学纸牌魔术：五十二种全新效果》。Taylor & Francis，2013 年。[18] Sarnath Ramnath 和 Daniel Scully。《用完美洗牌将扑克牌 i 移至位置 j 》。Math. Mag.，69(5)：361–365，1996 年。[19] Paul Swinford。《法罗幻想》。The Haley Press，印第安纳州康纳斯维尔，1968 年。[20] Paul Swinford。《更多法罗幻想》。自费出版，1971 年。