arXiv:2304.07126v2 [math.CO] 6 Nov 2023

扭曲置换码的译码

Robert F. Bailey* Keenan B. Nicholson†

2023年11月8日

摘要

我们研究扭曲置换码。这类频率置换阵列由具有多个相同次数置换表示的有限群构造而成，最初由 Gillespie、Praeger 和 Spiga 提出（随后由 Akbari、Gillespie 和 Praeger 研究）。我们基于第一作者此前关于置换群码的研究，为这类码开发了一种译码算法。特别地，我们展示了如何将该算法用于 Akbari、Gillespie 和 Praeger 研究的一族无限群。

关键词： 置换码；扭曲置换码；频率置换阵；基覆盖。

2020年数学主题分类： 94B35（主要），20B99、94B25、05B40（次要）

1 引言

置换码是一种纠错码，其中每个码字都是以列表形式书写的置换（即将大小为 n 的集合中的符号逐一列出，且每个符号恰好出现一次）。这种码也称为置换阵列，PA(n, d)，其中 d 表示最小汉明距离。置换码至少可追溯至 20 世纪 70 年代（例如参见 [9],），但近年来，因其在电力线通信 [12], 、固态存储设备 [19, 20] 和 DNA 数据存储 [8] 等领域的应用而受到关注。注意，对于对称群 S_n 中的两个置换 g、h，它们的汉明距离为 n –fix(gh^{-1})（其中，fix(g) 表示 g 的不动点数）。当这些置换构成 S_n 的一个子群 G 时，最小距离为

$$\min_{\substack{g\in G\\ g\neq 1}}\{n-\mathrm{fix}(g)\} \;=\; n-\max_{\substack{g\in G\\ g\neq 1}}\{\mathrm{fix}(g)\}\,.$$

将置换群作为码来研究，是第一作者及其他作者多篇论文的主题 [2, 3, 4, 5, 6, 7]。

一个更一般的概念是频率置换阵 FPA$_\lambda$(m, d)，它是一种字母表大小为 n 、长度为 $m = \lambda n$的码，其中每个码字都恰好包含 n 个符号各 λ 次。频率置换阵列由 Huczynska 于 2006 年发表的论文中首次提出

*纪念大学格伦费尔校区科学与环境学院（数学），科纳布鲁克，纽芬兰与拉布拉多省 A2H6P9，加拿大。电子邮箱：rbailey@grenfell.mun.ca

†纪念大学计算机科学系，圣约翰斯，纽芬兰与拉布拉多省 A1C 5S7，加拿大。电子邮箱：keenanbnicholson@gmail.com

并由 Mullen [18]合著。一个简单的频率置换阵列示例，可以通过取一个长度为 n 的置换码 $\mathcal{C}$ 并构造重复码 Rep$_\lambda(\mathcal{C})$得到，其中每个码字都是将 $\mathcal{C}$ λ 的每个码字重复若干次构成的。如果 $\mathcal{C}$ 的最小距离为 d，那么显然 Rep$_\lambda(\mathcal{C})$的最小距离为 λd。

因此，为了提高译码性能，我们希望获得长度、字母表和大小均与 Rep$_\lambda(\mathcal{C})$ 相同，但最小距离更大的频率置换阵。Gillespie、Praeger 和 Spiga 在 2015 年的论文 [15] 中提出了一个解决思路，随后 Akbari、Gillespie 和 Praeger 在 2018 [1], 中进一步发展了这一思路，研究了扭曲置换码。非正式地说，这一思路是：码字不再由同一个置换重复 λ 次构成，而是取同一个抽象群元素在多个相同次数的置换表示下的像来构成；事实证明，这样可以改进最小距离。形式化地说，这些码定义如下。

定义 1.1。设 G 是一个有限抽象群，且 $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$ 是 λ元组，由 G 在对称群 S_n中的置换表示组成（这些表示不一定互不相同）。对于 $g \in G$，将$\rho_i(g)$ 写成列表形式。扭曲置换码 Tw$(G, \mathcal{I})$ 定义为

$$\mathrm{Tw}(G, \mathcal{I}) = \{[\, \rho_1(g) \mid \rho_2(g) \mid \cdots \mid \rho_\lambda(g) \,] : g \in G\}.$$

也就是说，Tw$(G, \mathcal{I})$中的每个元素都是 g 在每个 ρ_i 下的像（以列表形式书写）的连接，因此我们得到一个字母表大小为 n 、长度为 λn的频率置换阵。我们将码字的子词 $\rho_1(g)$ $\rho_2(g)$ ... , $\rho_\lambda(g)$ 称为其分量（类似地，我们也将提及接收字的分量）。

不同于 [1, 15], ，我们坚持要求 $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$中的每个置换表示都是忠实的（尽管 [1, 15] 中的所有例子都是忠实的）。当 $\rho_1, \ldots, \rho_\lambda$ 都是同一个置换表示时，我们再次得到 λ重重复码 Rep$_\lambda($ $\rho_i(G))$。对于给定的 G 和 $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$，令 δ_{rep} 为 λ重重复码 Rep$_\lambda(\rho_i(G))$的所有最小距离中的最小值（对于 $1 \le i \le \lambda$），并令 δ_{tw} 为Tw$(G, \mathcal{I})$的最小距离。在 [15, 定理 1.1], 中证明了 $\delta_{\mathrm{tw}} \ge \delta_{\mathrm{rep}}$, 并给出了若干不等式严格成立的例子，例如下例。

例 1.2. 令 G 为对称群 S_6，并令 ρ_1、ρ_2 为 S_6 的两个不同置换表示，它们在外自同构作用下互换。由于 S_6 的最小距离为 2，因此 Rep$_2(\rho_1(G))$ 和 Rep$_2(\rho_2(G))$ 的最小距离均为 4。然而，Tw$(G,$ $(\rho_1, \rho_2))$ 的最小距离为 8 （见 [15, 第 4.1] 节）。

在 [1, 15], 中给出了若干最小距离有所提升（即 $\delta_{\mathrm{tw}} > \delta_{\mathrm{rep}}$）的扭曲置换码示例，但没有给出译码算法。本文旨在将 [3] 中用于把置换群作为码进行译码的方法，推广到扭曲置换码这一新情形。

2 一般结果

以下概念对于 [3], 中的（置换群）译码算法以及下文的内容至关重要。

定义 2.1. 设 G 是一个作用于有限集 Ω 上的置换群。 G 的一个基是 Ω 的一个子集$\{x_1, \ldots, x_k\}$, 其中元素在 G 中的逐点稳定子是平凡群。 G 的基大小记为$b(G)$，是 G 的基的最小大小。

根据定义可直接得出，元素 $g \in G$ 在一个基上的作用能够唯一确定 g：如果 $(x_1^g, \ldots, x_k^g) = (x_1^h, \ldots, x_k^h)$，那么 $g = h$。这对译码很有用：如果传输的是一个置换，而接收字中的错误都位于基所标记的位置之外，那么就能正确识别传输的置换。然而，由于错误可能出现在任何位置，单个基并不足够。因此，我们给出以下定义（同样取自 [3]）。

定义 2.2. 设 G 是作用在有限集 Ω 上的一个置换群，且 $r \geq 0$。对于 G，强度为 r 的基覆盖（r-*UBB*）是指一组基 $\mathcal{U}$，其中每个基都属于 G，并具有如下性质：Ω 的任意r子集都与 $\mathcal{U}$ 中至少一个基不相交。

若 G 的最小距离为 d，则通常假设 $r = \lfloor (d-1)/2 \rfloor$，并称其为 G的纠错能力。

例 2.3. 考虑群 G =PGL(2, 7) 对 $\Omega = \{1, \ldots, 8\}$ 的作用。该作用是锐三重传递的，因此 Ω 中任意 3 元组都是一个基；其最小距离为 5，因此纠错能力为 $\lfloor (5-1)/2 \rfloor = 2$。以下是 G 的一个 2-UBB：

$$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 2 & 3 & 7 \\ 1 & 7 & 8 \end{matrix}$$

通过检查，　　我们可以看出，$\{1, \ldots, 8\}$ 中的任意一对元素都与 UB 中至少一个三元组不相交 B.

我们注意到，若 $\mathcal{U}$ 中的基的大小均为 k，且将每个基视为一个 k-子集，那么 $\mathcal{U}$ 中各基的补集构成一个 $(n, n-k, r)$ 覆盖设计（见 [13, §VI.11]）。Gordon [17] 维护的在线数据库是查找小参数覆盖设计示例的实用资源。我们还指出，对于 $r \leq \lfloor (d-1)/2 \rfloor$，可以保证存在一个 r-UBB（见 [3, 命题 7]）。许多置换群的 UBB 构造可见 [2, 3, 5]。

[3] 中给出的译码算法如下：假设传输一个置换 $g \in G$，且接收字 w 至多包含 r 个错误。对于 $\mathcal{U}$中的每个基，找出 G 中（若存在）在由该基标记的位置上与 w 一致的元素；如果该置换与 w 的距离不超过 r，那么它必定是所传输的置换 g。由于 $\mathcal{U}$中至少有一个基能避开任意一组 r个错误位置，因此我们可以保证译码成功。

当我们谈到“群 G 的基”时，它是 G 的特定置换表示所具有的一种性质。一般而言，如果 G_1 和 G_2 是作用在同一集合 Ω 上的同构群，那么 G_1 的基不一定是 G_2 的基。不过，如果满足以下更强的条件，情况就会简单得多。

定义 2.4. 设 G_1 和 G_2 分别是作用在 Ω_1 和 Ω_2，上的群，并假设存在一个同构 φ： $G_1 \to G_2$。如果存在一个双射$\psi : \Omega_1 \to \Omega_2$，使得对于所有 $x \in \Omega_1$ 以及所有 $g \in G_1$，都有 $\psi(x^g) = (\psi(x))^{(g^\varphi)}$，那么称 G_1 和 G_2 是置换同构。有序对 (ψ, φ) 称为置换同构。

换句话说，如果 G_1 和 G_2 置换同构，那么它们不仅作为抽象群彼此同构，而且在各自的作用域 Ω_1 和 Ω_2上的作用方式也相同。下一个结果是留给读者的一道简单练习。

命题 2.5。 设 G_1 和 G_2 是分别作用于 Ω_1 和 Ω_2, 上的群，并且 (ψ,φ)是一个置换同构。那么，若 $B=\{x_1,\ldots,x_b\}\subseteq\Omega_1$ 是 G_1 在其对 Ω_1, 的作用下的一个基，则$\psi(B)=\{\psi(x_1)\ldots,\psi(x_b)\}\subseteq\Omega_2$ 是 G_2 在其对 Ω_2的作用下的一个基。

因此，如果有两个置换同构的群 G_1 和 G_2，就可以将映射 ψ 应用于 G_1 的基覆盖中的各个基，从而得到 G_2 的基覆盖。

2.1 调整算法

为了将 [3] 中的算法应用于扭曲置换码，我们回顾一下：Tw($G,\mathcal{I}$) 中的码字与抽象群 G 的元素一一对应，因此译码仍然需要识别群元素。对于每个 i，我们用 G_i 表示忠实表示 ρ_i 的像，因此 $\mathcal{G}=(G_1,\ldots,G_\lambda)$ 是由 n 次置换群组成的列表，这些群均与 G 同构。不失一般性，我们选取 G_1 作为“ 指定 ”的副本。暂且假设每个 G_i 都与 G_1 置换同构。

接下来，将 $\alpha_i:\ G_1\to G_i$ 定义为 ρ_1^{-1}（定义在 $G_1=\mathrm{Im}(\rho_1)$ 上）与 ρ_i 的复合。因此，$\mathcal{A}=(\alpha_1,\ldots,\alpha_\lambda)$ 给出了从 G_1 到各个 $(G_1,\ldots,G_\lambda)$ 的同构列表，而 $\mathcal{A}^{-1}=(\alpha_1^{-1},\ldots,\alpha_\lambda^{-1})$ 则给出它们各自的逆映射。我们还令 $\mathcal{F}=(\psi_1,\ldots,\psi_\lambda)$ 为双射，使得 (ψ_i,α_i) 是从 G_1 到 G_i 的置换同构（对于 $1\le i\le\lambda$），而 $\mathcal{F}^{-1}=(\psi_1^{-1},\ldots,\psi_\lambda^{-1})$ 给出相应的逆映射。（注意，对于重复码 Repλ(G_1)，每个 α_i 和每个 ψ_i 都是恒等映射。）

令 $r_{\mathrm{tw}}=\lfloor(\delta_{\mathrm{tw}}-1)/2\rfloor$ 为 Tw($G,\mathcal{I}$) 的纠错能力，并令 $r'=\lfloor r_{\mathrm{tw}}/\lambda\rfloor$；根据鸽巢原理，如果一个接收字中分布在 λ 个分量上的错误不超过 r_{tw} 个，那么必定存在一个分量，其中的错误不超过 r' 个。最后，假设 $\mathcal{U}$ 是一个强度为 r'的、关于G_1的 UBB（因此 $\psi_i(\mathcal{U})=\{\psi_i(B):\ B\in\mathcal{U}\}$是一个强度为 r'的、关于 G_i的 UBB）。

在算法的实现中，接收方知道群列表 $G_1,\ldots,G_\lambda$，以及映射列表 $\mathcal{A},\mathcal{A}^{-1},\mathcal{F}$和 $\mathcal{F}^{-1}$、纠错能力 r_{tw}，以及基覆盖 $\mathcal{U}$。算法的输入由一个接收字 $\mathsf{w}=[w_1,\ldots,w_\lambda]$组成。

算法 2.6. 假设发送的码字为 $\mathsf{g}=[\rho_1(g)\ldots,\rho_\lambda(g)]$,，且接收字 $\mathsf{w}=[w_1,\ldots,w_\lambda]$ 至多包含 r_{tw} 个错误。选择第一个基 $B_1\in\mathcal{U}$，检查 w_1 中由 B_1所标记位置上的符号；如果没有重复符号，则找出（如果存在）唯一的元素 $h_1\in G_1$，使其在这些位置上与 w_1 一致，然后计算$h_1^{\alpha_2}\in G_2,\ldots,$ $h_1^{\alpha_\lambda}\in G_\lambda$，得到码字 $\mathsf{h}=[h_1,h_1^{\alpha_2},\ldots,h_1^{\alpha_\lambda}]\in$Tw($G,\mathcal{I}$)。如果 h 与 w 的距离不超过 r_{tw}，则必有 $\mathsf{h}=\mathsf{g}$，从而成功解码。

否则，我们转到 w_2，检查 w_2 中由基$\psi_2(B_1)$为 G_2所标记位置上的符号；如果没有重复符号，则找出（如果存在）唯一的元素 $h_2\in G_2$，使其在这些位置上与 w_2一致，然后计算 $h_2^{\alpha_2^{-1}}\in G_1$ 以及 $h_2^{\alpha_2^{-1}\alpha_3}\in G_3,\ldots,h_2^{\alpha_2^{-1}\alpha_\lambda}\in G_\lambda$，得到码字 $\mathsf{h}=[h_2^{\alpha_2^{-1}},h_2,h_2^{\alpha_2^{-1}\alpha_3},\ldots,h_2^{\alpha_2^{-1}\alpha_\lambda}]\in$Tw($G,\mathcal{I}$)。同样，如果 h 与 w 的距离不超过r_{tw}，我们就成功解码。

随后对每个 w_i 继续这一过程，直到成功解码；如果每次都失败，则考虑下一个基 $B_2\in\mathcal{U}$，并对每个 w_1重复这一过程，.....，w_λ，检查每个标记为 $\psi_i(B_2)$ 的 w_i 中的位置，重构出 Tw($G,\mathcal{I}$) 中的一个码字，并将其与 w 比较。如果仍未成功，我们就转到 $\mathcal{U}$ 中的下一个基，再转到下一个，依此类推，直到成功。

由于必定存在一个分量 w_i 至多包含 r' 个错误，并且 $\mathcal{U}$ 是强度为 r'的基覆盖，因此必定存在一个 G_i 的基 $\psi_i(B_j)$，能够避开这些错误。因此，该算法至多经过 $\lambda|\mathcal{U}|$ 次尝试即可保证成功解码。

图1给出了算法 2.6 的流程图。

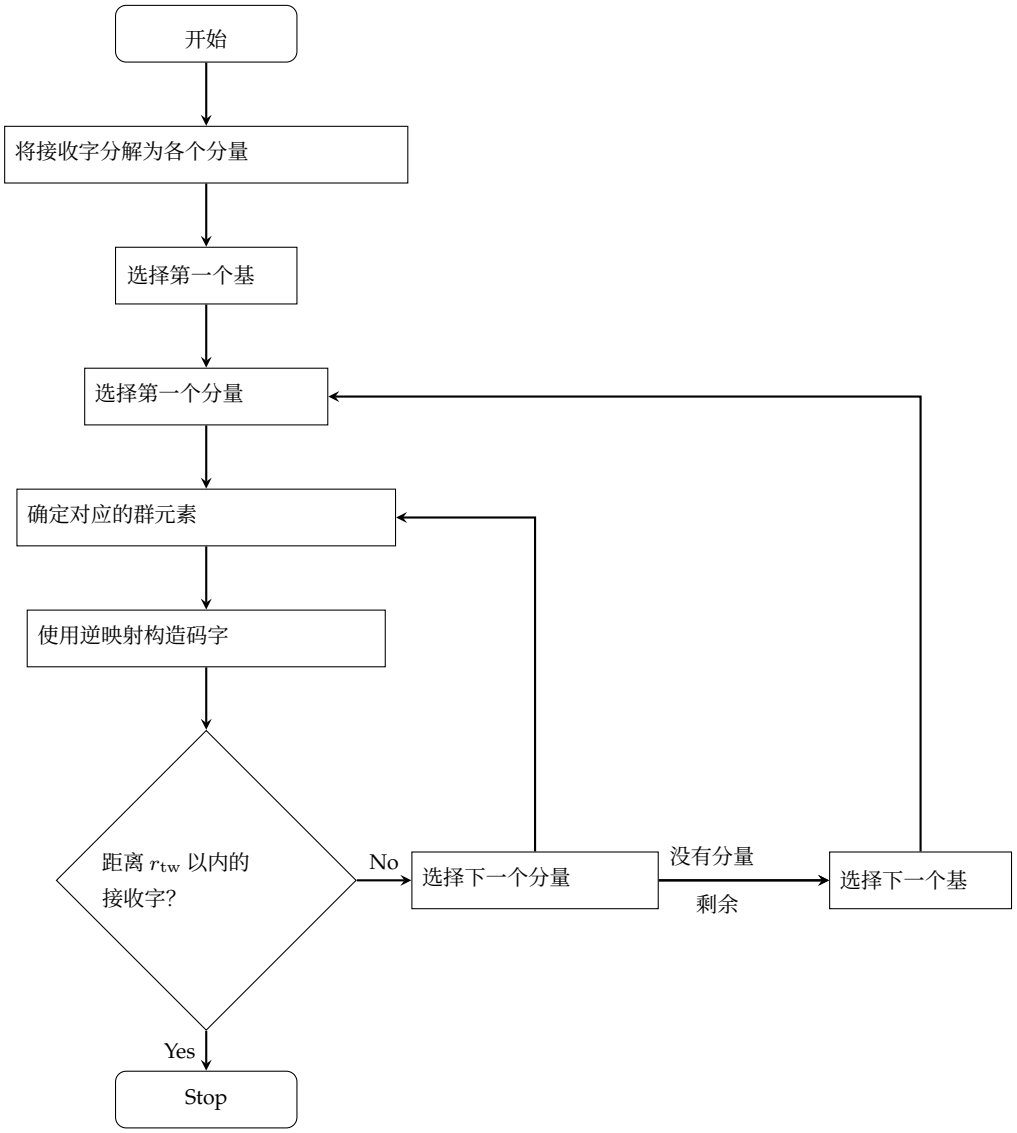


图1：扭曲置换码的译码算法

例2.7. 考虑由 $\mathbb{F}_2^3$上的仿射变换构成的群 $G = \mathrm{ASL}(3,2)$。存在两个不同的置换表示 ρ_1, ρ_2，它们是 S_8的子群，并由一个外自同构互换；使用 GAP [14]，我们发现其中一个表示（以其在 G生成元上的作用来表示）为

$$\begin{aligned}
(2,5)(4,7) &\mapsto (1,3)(2,7)(4,5)(6,8),\\
(2,3,4)(5,6,8) &\mapsto (2,3,4)(5,6,8),\\
(1,2)(3,4)(5,6)(7,8) &\mapsto (1,2)(3,4)(5,6)(7,8),\\
(1,3)(2,4)(5,7)(6,8) &\mapsto (1,3)(2,4)(5,7)(6,8),\\
(1,5)(2,6)(3,7)(4,8) &\mapsto (1,5)(2,6)(3,7)(4,8).
\end{aligned}$$

将此映射记为 α_2，并考虑扭曲置换码 $\mathrm{Tw}(G,\mathcal{I})$，其中 $\mathcal{I} = (\rho_1, \rho_2)$。我们有 $\mathcal{A} = (\mathrm{id}\ \alpha_2)$，且由于 $\mathrm{Im}(\rho_1) = \mathrm{Im}(\rho_2)$，因此有 $\mathcal{F} = (\mathrm{id}, \mathrm{id})$。现在，根据 [15,

第 7.1], 小节中，我们有 $\delta_{\mathrm{tw}} = 12$，这是对 $\delta_{\mathrm{rep}} = 8$ 的改进；这意味着 Tw($G, \mathcal{I}$) 可以纠正 $\lfloor (12-1)/2 \rfloor = 5$ 个错误，而 $r' = \lfloor 5/2 \rfloor = 2$。

G 的基大小为 4，其中最小基对应于$\mathbb{F}_2^3$中的仿射无关 4 元组；下面是一个强度为 $r' = 2$ 的 G基覆盖 $\mathcal{U}$：

$$\begin{array}{cccc} 1 & 2 & 3 & 5 \\ 4 & 5 & 6 & 7 \\ 1 & 4 & 6 & 8 \\ 1 & 5 & 7 & 8 \\ 2 & 3 & 4 & 6 \\ 2 & 3 & 7 & 8 \end{array}$$

我们可以使用 GAP 验证每一行都是 G的一个基。通过观察可知，$\{1, \ldots, 8\}$的任意 2 元子集都与 $\mathcal{U}$中至少一个基不相交。

令 $g = (1,4,6,8,5,3)(2,7) \in G$。现在，$g^{\alpha_2} = (1,7,5,8,2,4)(3,6)$，因此将它们按列表形式连接起来，我们得到码字

$$\mathbf{g} = [g_1 \mid g_2] = [4,7,1,6,3,8,2,5 \mid 7,4,6,1,8,3,5,2]$$

在 Tw($G, \mathcal{I}$) 中。假设发送的是 g，而接收到以下字（含两个错误）：

$$\mathbf{w} = [w_1 \mid w_2] = [4,7,1,6,7,8,2,5 \mid 4,4,6,1,8,3,5,2].$$

第一个基是 $\{1,2,3,5\}$，因此我们先检查 w_1中这些位置上的符号，分别为 4、7、1、7；由于符号 7 重复了，我们无法解码。接着检查 w_2 中的这些位置，得到 4、4、6、8，因此我们再次未能成功。

下一个基是 $\{4,5,6,7\}$；在 w_1 中，我们找到符号 6、7、8、2。它们没有重复，因此得到元素 $h_1 = [4,3,5,6,7,8,2,1] \in G_1$，它在这些位置上与 w_1 一致；应用 α_2得到 $h_1^{\alpha_2} = [1,2,8,7,6,5,3,4]$，于是我们得到码字

$$\mathbf{h} = [4,3,5,6,7,8,2,1 \mid 1,2,8,7,6,5,3,4].$$

然而，由于它与 w 的距离为 $11 > \delta_{\mathrm{tw}}$，因此被拒绝。在 w_2中，我们找到符号 1、8、3、5，并得到 $h_2 = [7,4,6,1,8,3,5,2]$；应用 α_2^{-1}得到 $h_2^{\alpha_2^{-1}} = [4,7,1,6,3,8,2,5]$，于是我们得到码字

$$\mathbf{h} = [4,7,1,6,3,8,2,5 \mid 7,4,6,1,8,3,5,2]$$

它与 w 的距离为 2。因此我们可以得出 $\mathbf{h} = \mathbf{g}$，并且已经成功译码。

在更一般的情形下，群 G_1、……、G_λ 并非置换同构，我们不再拥有映射列表 ψ_1、……、ψ_λ，因此需要为每个不同的像群 G_i 单独构造一个基覆盖。译码算法的步骤类似，但由于需要额外的 UBB，实现起来更加困难。不过，在 [1, 15], 中讨论的每个例子里，像群 G_i 通常不仅是置换同构，而且实际上彼此相等。这意味着每个映射 ψ_i 都是恒等映射，因此我们可以在每个分量中使用相同的 UBB。

2.2 重复码与“未改进”码的译码

以下观察很有帮助，因为它确保已知的置换码 UBB 可应用于重复码和“未改进”的扭曲置换码（即满足$\delta_{\mathrm{tw}} = \delta_{\mathrm{rep}}$的码）。

命题 2.8. 设 G 是纠错能力为 r的置换群。那么，对于重复码 $\mathrm{Rep}_\lambda(G)$，$\mathrm{Rep}_\lambda(G)$ 所需的 *UBB* 强度 r' 等于 r。

证明。我们知道 $r = \lfloor (d-1)/2 \rfloor$，其中 d 是 G的最小距离。现在，$\mathrm{Rep}_\lambda(G)$的最小距离为 λd，纠错能力为 $\lfloor (\lambda d - 1)/2 \rfloor$，并且有 $r' = \lfloor \lfloor (\lambda d - 1)/2 \rfloor / \lambda \rfloor$。分别考虑 d 和 λ 为奇数或偶数的情况，可得在所有情况下均有 $r' = \lfloor (\lambda d - 1)/2 \rfloor = r$。 □

请注意，同样的结果也适用于“未改进”的扭曲置换码；因此，[2, 3, 5] 中得到的 UBB 不仅可用于相应的重复码，也可用于“未改进”的扭曲置换码。在下表中，我们给出了一些群的更多示例（具有多个置换表示），包括 [15] 中提到的一些群（即 PSL(2,11)、M_{12} 和 A_7），以及它们的参数。对于 $2^4:$ A_6、$2_4:$ S_6 和 M_{22}，我们使用与 [15], 相同的技术，通过 GAP 验证了 $\delta_{\mathrm{tw}} = \delta_{\mathrm{rep}}$。

群 G	$\lvert G\rvert$	n	λ	$\delta_{\mathrm{tw}} = \delta_{\mathrm{rep}}$	r	r'	$b(G)$	$\lvert\mathcal{U}\rvert$
PSL(2, 11)	660	11	2	$2 \cdot 8 = 16$	7	3	3	5
M_{12}	95040	12	2	$2 \cdot 8 = 16$	7	3	5	11
A_7	2520	15	2	$2 \cdot 12 = 24$	11	5	3	9
$2^4 : A_6$	5760	16	4	$4 \cdot 12 = 48$	23	5	4	12
$2^4 : S_6$	11520	16	2	$2 \cdot 8 = 16$	7	3	5	6
M_{22}	443520	22	2	$2 \cdot 16 = 32$	15	7	5	22

表 1：部分“未改进”扭曲置换码的参数和译码

表 1 中提到的 UBB 可在附录 A 中找到。它们均通过取 Gordon 数据库 [17] 中相应的 (n, $n - b(G)$ r')-覆盖设计各区组的补集而获得；在某些情况下，需要重新标记点，以确保每个区组的补集都是群 G 的一个基。

2.3 具有改进的最小距离的扭曲置换码的译码

对于具有改进的最小距离的扭曲置换码 $\mathrm{Tw}(G, \mathcal{I})$，我们所需 UBB 的强度通常高于重复码 $\mathrm{Rep}_\lambda(G)$ 所需的强度。对于群 S_6、A_6 和 ASL(3, 2)，它们均已在 [15] 中被证明能够产生此类“改进的”码，下面我们在表 2 中总结相关细节。

群 G	$\lvert G\rvert$	n	λ	δ_{rep}	δ_{tw}	r_{tw}	r'	$b(G)$	$\lvert\mathcal{U}\rvert$
S_6	720	6	2	4	8	3	1	5	6
A_6	360	6	2	6	8	3	1	4	3
ASL(3, 2)	1344	8	2	8	12	5	2	4	6

表 2：“改进的”扭曲置换码的参数和译码

对于 S_6，相应的 UBB 由 $\{1, \ldots, 6\}$ 的所有 5-子集组成；对于 A_6，我们可以使用 {1234,1256、3456}；对于 ASL(3, 2)，UBB 见例2.7。

由于表 2 中的示例不多，下一节我们将介绍取自 [1] 的一个“改进”码无限族。

3 来自群 $G_k(p)$ 的码

在 [1, 第 3], 节中，Akbari 等人给出了一个扭曲置换码无限族，这些码源自向量空间 $\mathbb{F}_p^k$ 上的仿射群。我们先概述这些群及其对应的码。

令 B_k 为如下的 $k \times k$ 矩阵，其元素取自 $\mathbb{F}_p$:

$$B_k = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 1 \end{bmatrix}.$$

由于 B_k 是下三角幺模矩阵，因此显然可逆。可以证明（见 [1, 引理 4]）， B_k的乘法阶为 p，其幂可表示为

$$B_k^i = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ i & 1 & 0 & \cdots & 0 \\ \binom{i}{2} & i & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \binom{i}{k-1} & \binom{i}{k-2} & \binom{i}{k-3} & \cdots & 1 \end{bmatrix}$$

对于 $0 \le i < p$，其中元素 $\binom{i}{j}$ 均模 p 取值。

定义 3.1. 假设 $V = \mathbb{F}_p^k$ 是行向量空间，并令 $H_k(p)$ 为由 B_k 生成的 $GL(k,p)$ 子群。记 $G_k(p)$ 为 AGL(k,p) 中的子群 $V \rtimes H_k(p)$。

由于 B_k 的乘法阶为 p，因此 $G_k(p)$ 的阶为 p^{k+1}。接下来，我们定义一个 $(k+1) \times (k+1)$ 矩阵

$$A_{\mathbf{v},i} = \begin{bmatrix} 1 & \mathbf{v} \\ \mathbf{0}^T & B_k^i \end{bmatrix},$$

其中 $\mathbf{v}$ 是 $\mathbb{F}_p^k$ 中的行向量，且 $0 \le i < p$。然后用 $G_k(p)$ 表示所有此类矩阵的集合。在 [1, 引理 5], 中证明了，在矩阵乘法下， $G_k(p)$ 是 $GL(k+1,p)$ 的一个子群，其阶为 p^{k+1}，并且同构于仿射群 $G_k(p)$。他们还证明（见 [1, 引理7]） ， $G_k(p)$ 在 p^k 行向量 $\Omega = \{(1, \mathbf{v}) : \mathbf{v} \in \mathbb{F}_k^p\}$ 的集合上传递且忠实地作用，因此 $G_k(p)$ 可以视为一个作用在 p^k 个点上的置换群。此外，他们给出了一组从 $G_k(p)$ 到 $G_k(p)$ 的同构，并将其记为 $\tau_{\mathbf{w}}$；它们给出了 $G_k(p)$ ~~在~~ Sym(Ω) 中的一组置换表示，因此可用于构造扭曲置换码。特别是，他们证明，作为置换码， $G_k(p)$ 的最小距离为 $p^k - p$，所以 p 重重复码 Rep$^p(G_k(p))$ 的最小距离为 $p^{k+1} - p^2$；然而，利用一组特定的 p 置换表示 $\mathcal{I}$，可以得到一个具有改进的最小距离 $p^{k+1} - p$ 的扭曲置换码 Tw$(G_k(p)\ \mathcal{I})$（见 [1, 命题 9]）。

要将算法 2.6 应用于这些码，我们首先需要获得群 $G_k(p)$ 的基。令 $\mathbf{e}_1$，.....，$\mathbf{e}_k$ 表示 $\mathbb{F}_p^k$ 的标准基向量。

命题 3.2. 对于任意 j，其中 $2 \le j \le k$，我们有 $\{(1, \mathbf{0}), (1, \mathbf{e}j)\}$ 是作用在集合 Ω 上的 $G_k(p)$ 的基。此外， $b(G_k(p)) = 2$。

证明。 假设 $A_{\mathbf{v},\ i}$ 属于 $G_k(p)$ 中 $\{(1,0),(1,\mathrm{e}j)\}$ 的逐点稳定子。首先，我们有

$$\begin{aligned}(1,\mathbf{0})A_{\mathbf{v},i} &= (1,\mathbf{0})\begin{bmatrix}1 & \mathbf{v}\\ \mathbf{0}^T & B_k^i\end{bmatrix}\\ &= (1+0,\mathbf{v}+\mathbf{0})\\ &= (1,\mathbf{v}),\end{aligned}$$

因此，要使 $A_{\mathbf{v},i}$ 固定 (1, 0)，必须有 $\mathbf{v}=\mathbf{0}$。于是我们得到

$$\begin{aligned}(1,\mathbf{e}_j)A_{\mathbf{0},i} &= (1,\mathbf{e}_j)\begin{bmatrix}1 & \mathbf{0}\\ \mathbf{0}^T & B_k^i\end{bmatrix}\\ &= (1+0,\mathbf{0}+\mathbf{e}_jB_k^i).\end{aligned}$$

现在，$\mathbf{e}_jB_k^i$ 恰好是 B_k^i 的第 j 行，即

$$\mathbf{e}_jB_k^i=\left(\binom{i}{j-1},\binom{i}{j-2},\cdots,\binom{i}{1},1,0,\cdots 0\right).$$

因此，要使其等于 ej，我们要求 $j\geq 2$，并且所有二项式系数都等于 0；只有当 $i=0$ 时才会如此。因此，我们有 $A_{\mathbf{0},i}=A_{\mathbf{0},0}=I_{k+1}$，即 $G_k(p)$ 的单位元。因此，$\{(1,0),(1,\mathrm{e}j)\}$ 是 $G_k(p)$ 在 Ω 上作用的一个基。

由于 $G_k(p)$ 在 Ω 上传递地作用，但 $|\Omega|>|G_k(p)|$，可知 $G_k(p)$ 没有大小为 1 的基；因此 $b(G_k(p))=2$。 □

下一步是为 $G_k(p)$ 求一个基覆盖。现在，由于 $b(G_k(p))=2$，我们可以将最小基视为以 Ω 为顶点集的图的边。以下术语和记号由 Burness 和 Giudici 于 2020 年引入 [10]。

定义 3.3. 设 G 是作用于 Ω 上的群，且具有 $b(G)=2$。G的*Saxl* 图记作 $\Sigma(G)$，它是一个顶点集为 Ω 的图，其中当且仅当 $\{u,v\}$ 是 G的一个基时，$\{u,v\}$ 才是图中的一条边。

类似的图（称为“基轨道图”）见于 [5, 第 3], 节，不过其边集由 G 在大小为 2 的基上的单个轨道组成，而非所有此类基。因此，Saxl 图 $\Sigma(G)$ 的边集是 G的各个基轨道图的边集之并。

命题 3.4. 设 G 是一个置换群，作用于大小为 n 的集合 Ω 上，其基大小为 $b(G)=2$。那么，G 的一个最优基覆盖是 *Saxl* 图 $\Sigma(G)$中的一个匹配。

证明。 强度为 r' 的 UBB 的最小可能大小是 $r'+1$，否则就会存在一个由 r' 个点组成的集合，与每个基都有非空交集。一组 $r'+1$ 个两两不相交的基（即 $\Sigma(G)$ 中一组由 $r'+1$ 条两两不相交的边组成的集合）就足够了。但这恰好是 $\Sigma(G)$ 中一个大小为 $r'+1$ 的匹配。由于$r'\leq\left\lfloor\frac{n-2}{2}\right\rfloor$，条件 $2(r+1)\leq n$ 总是成立。 □

回想一下，图 Γ 在 n 个顶点上的完美匹配 是一个匹配（大小为 $\frac{n}{2}$），它包含 Γ 的每个顶点。如果 n 是奇数，则不存在完美匹配；但近完美匹配 是一个包含除一个顶点外所有顶点的匹配。以下结果众所周知（例如，参见 Godsil 和 Royle [16, 第 3.5] 节）。

引理 3.5。 设 Γ 是一个具有 n 个顶点的连通点传递图。那么根据 n 的奇偶性，Γ 要么有完美匹配，要么有近完美匹配。

根据构造，只要 G 是传递的，Saxl 图 $\Sigma(G)$ 就是点传递的；为了将引理 3.5 应用于 $\Sigma(G)$，必须证明它是连通的。（这一条件是必要的：所有分量大小均为奇数的非连通图不可能有（近）完美匹配。）我们希望将此结论应用于 $G_k(p)$ 的 Saxl 图。 ——

引理 3.6. 设 G 是作用在集合 $\Omega = \{(1,\mathbf{v}) : \mathbf{v} \in \mathbb{F}_p^k\}$ 上的群 $G_k(p)$。则 *Saxl* 图 $\Sigma(G)$ 是连通的。

证明。我们将证明，对于每个元素 $(1, \mathbf{v}) \in \Omega$，在 $\Sigma(G)$ 中都存在一条通向 $(1, 0)$ 的路径。

我们在命题 3.2 中看到，$\{(1, 0), (1, \mathbf{e}_j)\}$ 是 G 对于 $2 \le j \le k$ 的一个基。现在考虑 G 在这些基上的轨道；对于 $A_{\mathbf{v},i} \in G$，有

$$(1, \mathbf{0})A_{\mathbf{v},i} = (1, \mathbf{v})$$

and

$$(1, \mathbf{e}_j)A_{\mathbf{v},i} = (1, \mathbf{v} + \mathbf{b}_j^i)$$

其中 $\mathbf{b}_j^i = \mathbf{e}_j B_k^i$ 表示矩阵 B_k^i 的第 j 行。因此，$\{(1, \mathbf{v}), (1, \mathbf{v} + \mathbf{b}_j^i)\}$ 是 G 的一个基。所以，在 $\Sigma(G)$ 中，每个顶点 $(1, \mathbf{v})$ 都与 $(1, \mathbf{v} \pm \mathbf{b}_j^i)$ 相邻；我们可以用 $\mathbf{b}_j^i$ 标记这些边。现在，对于$2 \le j \le k$，有 $\mathbf{b}_j^i = \mathbf{e}_j$，而 $\mathbf{b}_2^1 = \mathbf{e}_1 + \mathbf{e}_2$。

现在假设 $\mathbf{v} = (v_1, v_2, \ldots, v_k)$。那么在 $\Sigma(G)$ 中存在一条从 $(1, v_1, v_2, \ldots, v_k)$ 到 $(1, v_1, v_2, \ldots, v_{k-1}, 0)$ 的路径，其边标记为 $\mathbf{e}_k$；接着存在一条从 $(1, v_1, v_2, \ldots, v_{k-1}, 0)$ 到 $(1, v_1, v_2, \ldots, v_{k-2}, 0, 0)$ 的路径，其边标记为 $\mathbf{e}_{k-1}$；如此继续，直到到达 $(1, v_1, v_2, 0, \ldots, 0)$。从那里出发，存在一条到 $(1, v_1, v_1, 0, \ldots, 0)$ 的路径，其边标记为 $\mathbf{e}_2$,；最后，存在一条到 $(1, 0, \ldots, 0)$ 的路径，其边标记为 $\mathbf{e}_1 + \mathbf{e}_2$。

由于 从任意顶点到 $(1, 0)$ 都存在一条位于 $\Sigma(G)$ 中的路径，因此 $\Sigma(G)$ 是连通的。 □

综合以上结果，我们得到以下结论。

定理 3.7. 扭曲置换码 $\mathrm{Tw}(G_k(p)\ \mathcal{I})$的大小为 p^{k+2}，长度为 p^{k+1}，最小距离为 $p^{k+1} - p$，且可通过一个大小最优的基覆盖来译码，覆盖大小为 $r' + 1 = \left\lfloor \frac{p^k-1}{2} \right\rfloor$。

证明。 $\mathrm{Tw}(G_k(p)\ \mathcal{I})$ 的大小、长度和最小距离均已在 [1] 中确定。由此计算 r' 是一项直接的练习。由于 $\Sigma(G_k(p))$ 是连通的（根据引理 3.6），它存在一个（近）完美匹配（根据引理 3.5），该匹配构成一个最优 UBB（根据命题 3.4）。 □

4 另一个无限族

最后，我们提及另一族群，它们在 [15, 第 6],节中出现，并具有多个置换表示。令 V 为 $\mathbb{F}_{2^m}^2$ 的加法群，令 K 表示特殊线性群 $\mathrm{SL}(2, 2^m)$。由于第一上同调群 $H^1(K, V)$ 的阶为 2^m（参见 [11,表 7.3]），半直积 $G = V \rtimes K$ 有 2^m 个外自同构。因此，G（即仿射特殊线性群 $\mathrm{ASL}(2, 2^m)$）有 2^m 个置换表示，故 $\mathrm{ASL}(2, 2^m)$ 是构造扭曲置换码的候选对象。此外，[2, 定理 5.27] 构造了一族可用于这些群的 UBB。

遗憾的是，如 [15, 定理 6.1], 所示，在这种情况下，扭曲无法产生具有改进的最小距离的码。$G = \mathrm{ASL}(2, 2^m)$ 2^m的非恒等元素可能具有的不动点数为 0、1 或 2^m，因此最小距离为 $2^{2m} - 2^m$。要使扭曲置换码 $\mathrm{Tw}(G, \mathcal{I})$ 的最小距离优于重复码 $\mathrm{Rep}_\lambda(G)$，一个必要条件是：G 中具有

最多不动点的元素的每个共轭类，都必须经由一个外自同构映射到一个不动点较少的元素共轭类；这两个共轭类必须大小相同，且由阶相同的元素组成。然而，在 ASL$(2, 2^m)$ 中，不可能存在这样的共轭类：具有 2^m 个不动点的元素只有一个共轭类，且这些元素的阶为 2；此外，阶为 2 的元素只有另一个共轭类，由初等阿贝尔子群 V 的非零元素构成，其大小与前者不同。

附录 A：一些基覆盖的示例

示例 A.1. 对于群 $G = \mathrm{PSL}(2, 11)$，我们有 $n = 11, b(G) = 3$ 和 $r' = 3$:

$$\begin{array}{ccc} 1 & 2 & 11 \\ 2 & 8 & 10 \\ 3 & 4 & 5 \\ 6 & 7 & 9 \\ 8 & 10 & 11 \end{array}$$

示例 A.2. 对于群 M_{12}，我们有 $n = 12, b(M_{12}) = 5$ 和 $r' = 3$。由于 M_{12} 是尖锐 5-传递的，任意一个 5 元子集都构成一个基。此示例取自 [2, 表 1]。

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 6 & 11 & 12 \\ 1 & 3 & 7 & 8 & 9 \\ 1 & 4 & 6 & 7 & 10 \\ 1 & 5 & 8 & 9 & 11 \\ 2 & 4 & 8 & 9 & 12 \\ 2 & 5 & 7 & 10 & 11 \\ 3 & 4 & 7 & 11 & 12 \\ 3 & 5 & 6 & 10 & 12 \\ 3 & 6 & 8 & 9 & 11 \\ 6 & 7 & 8 & 9 & 10 \end{array}$$

例 A.3. 对于群 A_7，我们有 $n = 15, b(A_7) = 4$ 和 $r' = 5$。此例在 [2] 中有所提及，但未在那里明确给出。

$$\begin{array}{ccc} 1 & 2 & 8 \\ 2 & 6 & 7 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \\ 9 & 12 & 15 \\ 9 & 13 & 14 \\ 10 & 11 & 12 \\ 10 & 11 & 15 \\ 13 & 14 & 15 \end{array}$$

例 A.4. 对于群 $G = 2^4 : A_6$, 我们有 $n = 16, b(G) = 4$ 和 $r' = 5$:

1	2	9	16
1	3	9	10
1	4	9	11
2	3	10	16
2	4	11	16
3	4	10	11
5	6	12	13
5	7	13	14
5	8	13	15
6	7	12	14
6	8	12	15
7	8	14	15

示例 A.5. 对于群 $G = 2^4 : S_6$, 我们有 $n = 16, b(G) = 5$ 和 $r' = 3$:

1	3	4	6	13
2	3	6	11	16
2	4	11	13	16
5	7	9	14	15
7	8	10	12	14
8	9	10	12	15

例 A.6. 对于群 M_{22}, 我们有 $n = 22, b(M_{22}) = 5$ 和 $r' = 7$:

1	2	4	14	19
1	2	7	13	17
1	3	4	15	17
1	3	5	7	19
1	5	13	14	15
2	3	5	14	17
2	3	13	15	19
2	4	5	7	15
3	4	7	13	14
4	5	13	17	19
6	8	9	11	18
6	8	10	20	21
6	9	12	16	21
6	10	12	18	22
6	11	16	20	22
7	14	15	17	19
8	9	10	16	22
8	11	12	21	22
8	12	16	18	20
9	10	11	12	20
9	18	20	21	22
10	11	16	18	21

致谢

第一作者感谢 NSERC Discovery Grant 提供的经费支持。第二作者曾获 NSERC Undergraduate Student Research Award。本研究的部分内容取自第二作者在纪念大学格伦费尔校区完成的理学学士高年级项目论文。两位作者均感谢匿名审稿人提出的建议，以及 Peter Cameron 和 Robert Guralnick 富有启发性的讨论。

参考文献

[1] M. Akbari、N. I. Gillespie 和 C. E. Praeger，通过扭曲提高码的最小距离，*Electron. J. Combin.* **25(3)**（2018），#P3.36，19 页。[2] R. F. Bailey，关于基传递置换群的基覆盖，*Des. Codes Cryp-togr.* **41**（2006），153–176。[3] R. F. Bailey，来自置换群的纠错码，*Discrete Math.* **309**（2009），4253–4265。[4] R. F. Bailey 和 J. N. Bray，Mathieu 群 M_{12} 的译码，*Adv. Math. Commun.* **1**（2007），477–487。[5] R. F. Bailey 和 P. J. Cameron，关于基覆盖的单轨道猜想，*J.GroupTheory* **11**（2008），845–850。[6] R. F. Bailey 和 J. P. Dixon，置换群的距离计数器，*Comm. Algebra* **35**（2007），3045–3051。[7] R. F. Bailey 和 T. Prellberg，广义超八面体群的译码及可纠正错误模式的渐近分析，*Contrib. Discrete Math.* **7**（2012），1–14。[8] N. Beeri 和 M. Schwartz，采用霰弹枪测序技术进行 DNA 存储的改进秩调制码，*IEEE Trans. Inform. Theory* **68**（2022），3719–3730。[9] I. F. Blake、G. Cohen 和 M. Deza，使用置换进行编码，*Inform. and Control* **43**（1979），1–19。[10] T. C. Burness 和 M. Giudici，关于置换群的 Saxl 图，*Math. Proc. Cam-bridge Philos.Soc.* **168**（2020），219–248。[11] P. J. Cameron，置换群，伦敦数学学会学生教材（45），剑桥大学出版社，剑桥，1999。[12] W. Chu、C. J. Colbourn 和 P. Dukes，电力线通信中置换码的构造，*Des. Codes Cryptogr.* **32**（2004），51–64。[13] C. J. Colbourn 和 J. H. Dinitz（编辑），组合设计手册（第二版），CRC Press，博卡拉顿，2007。[14]GAP 群，*GAP – 群、算法与程序，第 4.11.1 版*；2021，www.gap-system.org。

[15] N. I. Gillespie、C. E. Praeger 和 P. Spiga，扭曲置换码，*J. Group Theory* **18**（2015），407–433。[16] C. D. Godsil 和 G. F. Royle，代数图论，数学研究生教材（207），Springer-Verlag，纽约，2001。[17] D. M. Gordon，覆盖设计，www.dmgordon.org/cover/；最后访问日期：2023 年 10 月 22 日。[18] S. Huczynska 和 G. L. Mullen，频率置换阵列，*J. Combin. Des.* **14** （2006），463–478。[19] T. Kløve、T. T. Lin、S.-C. Tsai 和 W.-G. Tzeng，切比雪夫距离下的置换阵列，*IEEETrans. Inform. Theory* **56** （2010），2611–2617。[20] I. Tamo 和 M. Schwartz，秩调制方案中有限幅度错误的纠正，*IEEETrans. Inform. Theory* **56** （2010），2551–2560。