Decoding twisted permutation codes

Robert F. Bailey[*] Keenan B. Nicholson[†]

November 6, 2023

Abstract

We consider twisted permutation codes, a class of frequency permutation arrays obtained from finite groups with multiple permutation representations of the same degree, introduced by Gillespie, Praeger and Spiga (and later studied by Akbari, Gillespie and Praeger), and develop a decoding algorithm for such codes based on earlier work of the first author for permutation group codes. In particular, we show how to implement this algorithm for an infinite family of groups considered by Akbari, Gillespie and Praeger.

Keywords: permutation code; twisted permutation code; frequency permutation array; uncovering-by-bases.

MSC2020: 94B35 (primary), 20B99, 94B25, 05B40 (secondary)

1 Introduction

A *permutation code* is an error-correcting code where each codeword is a permutation written in list form (i.e. a listing of the symbols from a set of size n, where each symbol appears exactly once). Such a code is also known as a *permutation array*, $\mathrm{PA}(n,d)$, where d denotes the minimum Hamming distance. Permutation codes have a history dating back at least to the 1970s (see [9], for instance), but have more recently been considered because of applications including powerline communications [12], solid-state memory devices [19, 20] and DNA storage of data [8]. We note that for two permutations g, h in the symmetric group S_n, their Hamming distance is $n - \mathrm{fix}(gh^{-1})$ (where $\mathrm{fix}(g)$ denotes the number of fixed points of g). In the case where the set of permutations forms a subgroup G of S_n, the minimum distance is

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

The study of groups of permutations as codes is the subject of several papers of the first author and others [2, 3, 4, 5, 6, 7].

A more general notion is that of a *frequency permutation array*, $\mathrm{FPA}_\lambda(m,d)$, which is a code of alphabet size n and length $m = \lambda n$, where each codeword contains each of the n symbols exactly λ times. Frequency permutation arrays were introduced in the 2006 paper of Huczynska

[*] School of Science and the Environment (Mathematics), Grenfell Campus, Memorial University, Corner Brook, NL A2H 6P9, Canada. E-mail: rbailey@grenfell.mun.ca

[†] Department of Computer Science, Memorial University, St. John's, NL A1C 5S7, Canada. E-mail: keenanbnicholson@gmail.com

and Mullen [18]. A straightforward example of a frequency permutation array can be obtained by taking a permutation code $\mathcal{C}$ of length n and forming the *repetition code*, $\mathrm{Rep}_\lambda(\mathcal{C})$, where each codeword is formed by repeating each codeword of $\mathcal{C}$ λ times. If $\mathcal{C}$ has minimum distance d, then clearly $\mathrm{Rep}_\lambda(\mathcal{C})$ has minimum distance λd.

For reasons of improved decoding performance, it is therefore desirable to obtain FPAs with the same length, alphabet and size as $\mathrm{Rep}_\lambda(\mathcal{C})$, but with a larger minimum distance. An approach to this was introduced in the 2015 paper of Gillespie, Praeger and Spiga [15] and further developed by Akbari, Gillespie and Praeger in 2018 [1], where *twisted permutation codes* were considered. Informally, the idea is that instead of repeating the same permutation λ times over, a codeword can be formed by taking the image of the same element of an abstract group from multiple permutation representations of the same degree; it transpires that this can result in improved minimum distance. Formally, these are defined as follows.

Definition 1.1. Let G be an abstract finite group, and let $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$ be a λ-tuple of (not necessarily distinct) permutation representations of G in the symmetric group S_n. For $g \in G$, let $\rho_i(g)$ be written in list form. The *twisted permutation code*, $\mathrm{Tw}(G, \mathcal{I})$, is defined as

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

That is, each element of $\mathrm{Tw}(G, \mathcal{I})$ is the concatenation of the images of g under each ρ_i (written in list form), so we have a frequency permutation array with alphabet size n and length λn. We call the subwords $\rho_1(g), \rho_2(g), \ldots, \rho_\lambda(g)$ the *components* of a codeword (and similarly, we will refer to the components of a received word).

Unlike [1, 15], we will insist that each permutation representation in $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$ is faithful (although all the examples in [1, 15] are faithful). In the case where $\rho_1, \ldots, \rho_\lambda$ are all the same permutation representation, then we have the λ-fold repetition code $\mathrm{Rep}_\lambda(\rho_i(G))$ once again. For a given G and $\mathcal{I} = (\rho_1, \ldots, \rho_\lambda)$, let δ_{rep} be the minimum of all of the minimum distances of the λ-fold repetition codes $\mathrm{Rep}_\lambda(\rho_i(G))$ (for $1 \leq i \leq \lambda$), and let δ_{tw} be the minimum distance of $\mathrm{Tw}(G, \mathcal{I})$. In [15, Theorem 1.1], it is proved that $\delta_{\mathrm{tw}} \geq \delta_{\mathrm{rep}}$, and a number of examples are given where the inequality is strict, such as the following.

Example 1.2. Let G be the symmetric group S_6, and let ρ_1, ρ_2 be the distinct permutation representations of S_6, interchanged by the outer automorphism. Now, since S_6 has minimum distance 2, we have that $\mathrm{Rep}_2(\rho_1(G))$ and $\mathrm{Rep}_2(\rho_2(G))$ both have minimum distance 4. However, $\mathrm{Tw}(G, (\rho_1, \rho_2))$ has minimum distance 8 (see [15, Section 4.1]).

In [1, 15], a number of examples of twisted permutation codes with improved minimum distance (i.e. where $\delta_{\mathrm{tw}} > \delta_{\mathrm{rep}}$) are presented, but no decoding algorithm is given. The purpose of the present paper is to adapt the approach of [3] for decoding permutation groups as codes to the newer situation of twisted permutation codes.

2 General results

The following notion is crucial to the decoding algorithm (for permutation groups) in [3], and in what follows.

Definition 2.1. Let G be a permutation group acting on a finite set Ω. A *base* for G is a subset $\{x_1, \ldots, x_k\}$ of elements of Ω whose pointwise stabilizer in G is trivial. The *base size* of G, denoted $b(G)$, is the smallest size of a base for G.

A direct consequence of the definition is that the action of an element $g \in G$ on a base uniquely identifies g: if $(x_1^g, \ldots, x_k^g) = (x_1^h, \ldots, x_k^h)$ then $g = h$. These are useful for decoding: if a permutation is transmitted and the received word contains errors outside of the positions labelled by a base, then the transmitted permutation can be identified correctly. However, as the errors could be in any possible positions, a single base will not be sufficient. Instead, we have the following definition (also taken from [3]).

Definition 2.2. Let G be a permutation group acting on a finite set Ω, and let $r \geq 0$. An *uncovering-by-bases of strength r* (or *r-UBB*) for G is a collection $\mathcal{U}$ of bases for G with the property that any r-subset of Ω is disjoint from at least one base in $\mathcal{U}$.

If G has minimum distance d, then we usually assume that $r = \lfloor (d-1)/2 \rfloor$, which we call the *correction capability* of G.

Example 2.3. Consider the group $G = \mathrm{PGL}(2,7)$ in its action on $\Omega = \{1, \ldots, 8\}$. This action is sharply 3-transitive, so any 3-tuple from Ω forms a base, and the minimum distance is 5, so the correction capability is $\lfloor (5-1)/2 \rfloor = 2$. The following is a 2-UBB for G:

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

By inspection, we see that any pair from $\{1, \ldots, 8\}$ is disjoint from at least one triple in the UBB.

We observe that, if the bases in $\mathcal{U}$ each have size k and each base for is regarded as a k-subset, then the complements of the bases in $\mathcal{U}$ form an $(n, n-k, r)$ *covering design* (see [13, §VI.11]). The online database maintained by Gordon [17] is a useful resource for examples of covering designs with small parameters. We also remark that for $r \leq \lfloor (d-1)/2 \rfloor$, an r-UBB is guaranteed to exist (see [3, Proposition 7]). Constructions of UBBs for many permutation groups can be found in [2, 3, 5].

The decoding algorithm given in [3] works as follows: suppose a permutation $g \in G$ is transmitted and the received word w contains at most r errors. For each base in $\mathcal{U}$, identify the element (if one exists) of G which agrees with w in the positions labelled by the base; if this permutation is within distance r of w then it must be the transmitted permutation g. Since any combination of r error positions is avoided by at least one base in $\mathcal{U}$, we are guaranteed to succeed.

When we speak of a "base for a group G", it is a property of the specified permutation representation of G. In general, if G_1 and G_2 are isomorphic groups acting on the same set Ω, it is not necessarily true that a base for G_1 is a base for G_2. However, if the following stronger condition holds, the situation is more straightforward.

Definition 2.4. Let G_1 and G_2 be groups acting on Ω_1 and Ω_2, respectively, and suppose there is an isomorphism $\varphi : G_1 \to G_2$. Then G_1 and G_2 are *permutationally isomorphic* if there is a bijection $\psi : \Omega_1 \to \Omega_2$ such that $\psi(x^g) = (\psi(x))^{(g^\varphi)}$ for all $x \in \Omega_1$ and all $g \in G_1$. The pair (ψ, φ) is called a *permutational isomorphism*.

In other words, if G_1 and G_2 are permutationally isomorphic, then not only are they isomorphic as abstract groups, but they act in the same way on their respective domains Ω_1 and Ω_2. The next result is a straightforward exercise for the reader.

Proposition 2.5. *Suppose that G_1 and G_2 are groups acting on Ω_1 and Ω_2, respectively, such that (ψ, φ) is a permutational isomorphism. Then if $B = \{x_1, \ldots, x_b\} \subseteq \Omega_1$ is a base for G_1 in its action on Ω_1, then $\psi(B) = \{\psi(x_1), \ldots, \psi(x_b)\} \subseteq \Omega_2$ is a base for G_2 in its action on Ω_2.*

As a consequence, if we have two permutationally-isomorphic groups G_1 and G_2, we can obtain an uncovering-by-bases for G_2 by applying the map ψ to the bases in a UBB for G_1.

2.1 Adapting the algorithm

To adapt the algorithm from [3] to twisted permutation codes, we recall that the codewords in $\mathrm{Tw}(G, \mathcal{I})$ are in one-to-one correspondence with the elements of the abstract group G, so decoding will still involve identifying group elements. For each i, we let G_i denote the image of the faithful representation ρ_i, so that $\mathcal{G} = (G_1, \ldots, G_\lambda)$ is a list of permutation groups of degree n isomorphic to G. Without loss of generality, we pick G_1 as a "distinguished" copy. For now, assume that each G_i is permutationally isomorphic to G_1.

Next, define $\alpha_i : G_1 \to G_i$ as the composition of ρ_1^{-1} (defined on $G_1 = \mathrm{Im}(\rho_1)$) with ρ_i. Consequently, $\mathcal{A} = (\alpha_1, \ldots, \alpha_\lambda)$ gives a list of isomorphisms from G_1 to each of $(G_1, \ldots, G_\lambda)$, while $\mathcal{A}^{-1} = (\alpha_1^{-1}, \ldots, \alpha_\lambda^{-1})$ gives their respective inverses. We also let $\mathcal{F} = (\psi_1, \ldots, \psi_\lambda)$ be bijections such that (ψ_i, α_i) is a permutational isomorphism from G_1 to G_i (for $1 \leq i \leq \lambda$), and $\mathcal{F}^{-1} = (\psi_1^{-1}, \ldots, \psi_\lambda^{-1})$ gives the respective inverses. (Note that in the case of the repetition code $\mathrm{Rep}_\lambda(G_1)$, each α_i and each ψ_i is the identity map.)

Let $r_{\mathrm{tw}} = \lfloor (\delta_{\mathrm{tw}} - 1)/2 \rfloor$ be the correction capability of $\mathrm{Tw}(G, \mathcal{I})$, and let $r' = \lfloor r_{\mathrm{tw}}/\lambda \rfloor$; by the pigeonhole principle, if a received word contains at most r_{tw} errors spread across λ components, then there must be a component containing at most r' errors. Finally, suppose that $\mathcal{U}$ is a UBB for G_1 of strength r' (so $\psi_i(\mathcal{U}) = \{\psi_i(B) : B \in \mathcal{U}\}$ is a UBB for G_i of strength r').

In an implementation of the algorithm, the receiver knows the list of groups $G_1, \ldots, G_\lambda$, as well as the lists of mappings $\mathcal{A}$, $\mathcal{A}^{-1}$, $\mathcal{F}$ and $\mathcal{F}^{-1}$, the correction capability r_{tw}, and the uncovering-by-bases $\mathcal{U}$. An input to the algorithm consists of a received word $\mathbf{w} = [w_1, \ldots, w_\lambda]$.

Algorithm 2.6. Suppose that the transmitted codeword is $\mathbf{g} = [\rho_1(g), \ldots, \rho_\lambda(g)]$, and that the received word $\mathbf{w} = [w_1, \ldots, w_\lambda]$ contains at most r_{tw} errors. Choose the first base $B_1 \in \mathcal{U}$ and examine the symbols in w_1 in the positions indexed by B_1; if there are no repeated symbols, find (if it exists) the unique element $h_1 \in G_1$ which agrees with w_1 in those positions, then compute $h_1^{\alpha_2} \in G_2, \ldots, h_1^{\alpha_\lambda} \in G_\lambda$ to obtain a codeword $\mathbf{h} = [h_1, h_1^{\alpha_2}, \ldots, h_1^{\alpha_\lambda}] \in \mathrm{Tw}(G, \mathcal{I})$. If $\mathbf{h}$ is within distance r_{tw} of $\mathbf{w}$, we must have that $\mathbf{h} = \mathbf{g}$, and we have decoded successfully.

Otherwise, we move to w_2 and examine the symbols in the positions of w_2 indexed by the base $\psi_2(B_1)$ for G_2; if there are no repeats, find (if it exists) the unique element $h_2 \in G_2$ which agrees with w_2 in those positions, then compute $h_2^{\alpha_2^{-1}} \in G_1$ as well as $h_2^{\alpha_2^{-1}\alpha_3} \in G_3, \ldots, h_2^{\alpha_2^{-1}\alpha_\lambda} \in G_\lambda$ to obtain a codeword $\mathbf{h} = [h_2^{\alpha_2^{-1}}, h_2, h_2^{\alpha_2^{-1}\alpha_3}, \ldots, h_2^{\alpha_2^{-1}\alpha_\lambda}] \in \mathrm{Tw}(G, \mathcal{I})$. Again, if $\mathbf{h}$ is within distance r_{tw} of $\mathbf{w}$, we have decoded successfully.

This process is then continued for each w_i until we can decode successfully; if we fail each time, we then consider the next base $B_2 \in \mathcal{U}$ and repeat the process for each $w_1, \ldots, w_\lambda$, examining the positions in each w_i labelled by $\psi_i(B_2)$, reconstructing a codeword in $\mathrm{Tw}(G, \mathcal{I})$ and comparing it to $\mathbf{w}$. If there is still no success, we move to the next base in $\mathcal{U}$, and then the next, and so on, until we are successful.

Since there must be a component w_i which contains at most r' errors, and because $\mathcal{U}$ is an uncovering-by-bases of strength r', there must be a base $\psi_i(B_j)$ for G_i avoiding these errors. So the algorithm is guaranteed to decode successfully after at most $\lambda|\mathcal{U}|$ attempts.

Figure 1 gives a flowchart depicting Algorithm 2.6.

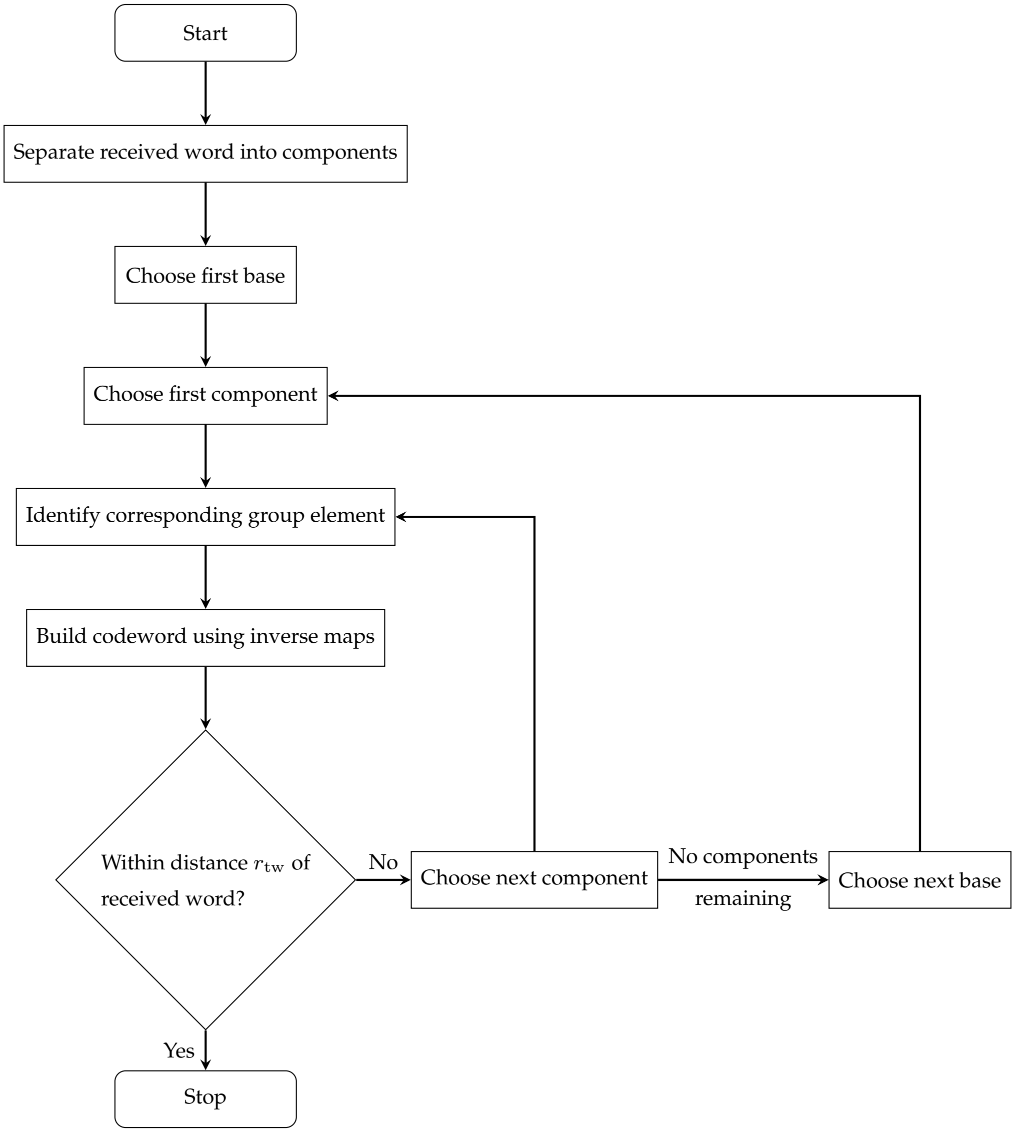
Start
Separate received word into components
Choose first base
Choose first component
Identify corresponding group element
Build codeword using inverse maps
Within distance r_{tw} of received word?
No
Choose next component
No components remaining
Choose next base
Yes
Stop

Figure 1: Decoding algorithm for a twisted permutation code

Example 2.7. Consider the group $G = \mathrm{ASL}(3,2)$ of affine transformations of $\mathbb{F}_2^3$. There are two distinct permutation representations ρ_1, ρ_2 as subgroups of S_8, interchanged by an outer automorphism; using GAP [14], we find one (in terms of its action on generators of G) to be

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

Denote this mapping by α_2, and consider the twisted permutation code $\mathrm{Tw}(G, \mathcal{I})$ where $\mathcal{I} = (\rho_1, \rho_2)$. We have that $\mathcal{A} = (\mathrm{id}, \alpha_2)$, and since $\mathrm{Im}(\rho_1) = \mathrm{Im}(\rho_2)$ we have $\mathcal{F} = (\mathrm{id}, \mathrm{id})$. Now, by [15, subsection 7.1], we have $\delta_{\text{tw}} = 12$, which is an improvement on $\delta_{\text{rep}} = 8$; this means that $\text{Tw}(G, \mathcal{I})$ can correct $\lfloor (12-1)/2 \rfloor = 5$ errors, while $r' = \lfloor 5/2 \rfloor = 2$.

G has base size 4, with the minimum bases corresponding to affine-independent 4-tuples in $\mathbb{F}_2^3$; below is an uncovering-by-bases $\mathcal{U}$ of strength $r' = 2$ for G:

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

We can use GAP to verify that each row is a base for G, and by inspection any 2-subset of $\{1, \ldots, 8\}$ is disjoint from at least one base in $\mathcal{U}$.

Let $g = (1, 4, 6, 8, 5, 3)(2, 7) \in G$. Now, $g^{\alpha_2} = (1, 7, 5, 8, 2, 4)(3, 6)$, so by concatenating these in list form we obtain the codeword

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

in $\text{Tw}(G, \mathcal{I})$. Suppose that $\mathbf{g}$ is transmitted, and the following word (with two errors) is received:

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

The first base is $\{1, 2, 3, 5\}$, so we first examine the symbols in those positions of w_1, which are $4, 7, 1, 7$; since symbol 7 is repeated, we cannot decode. We then examine those positions of w_2 and find $4, 4, 6, 8$, so we are unsuccessful again.

The next base is $\{4, 5, 6, 7\}$; in w_1 we find symbols $6, 7, 8, 2$. There are no repeats, so we obtain the element $h_1 = [4, 3, 5, 6, 7, 8, 2, 1] \in G_1$ which agrees with w_1 in those positions; applying α_2 yields $h_1^{\alpha_2} = [1, 2, 8, 7, 6, 5, 3, 4]$, and we obtain the codeword

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

However, since this is at distance $11 > \delta_{\text{tw}}$ from $\mathbf{w}$, it is rejected. In w_2, we find symbols $1, 8, 3, 5$, and obtain $h_2 = [7, 4, 6, 1, 8, 3, 5, 2]$; applying α_2^{-1} yields $h_2^{\alpha_2^{-1}} = [4, 7, 1, 6, 3, 8, 2, 5]$, and we obtain the codeword

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

which is distance 2 from $\mathbf{w}$. So we can conclude that $\mathbf{h} = \mathbf{g}$, and we have decoded successfully.

In the more general case where the groups $G_1, \ldots, G_\lambda$ are not permutationally isomorphic, we no longer have the list of mappings $\psi_1, \ldots, \psi_\lambda$, and will require a separate uncovering-by-bases for each distinct image group G_i. The decoding algorithm proceeds similarly, but the need for additional UBBs makes it more difficult to implement. However, in each of the examples considered in [1, 15], the image groups G_i are typically not just permutationally isomorphic, but are in fact equal. This means that each map ψ_i is the identity map, and we can use the same UBB in each component.

2.2 Decoding repetition codes and "unimproved" codes

The following observation is helpful, as it ensures that known UBBs for permutation codes can be applied to repetition codes and "unimproved" twisted permutation codes (i.e. those for which $\delta_{\text{tw}} = \delta_{\text{rep}}$).

Proposition 2.8. *Suppose that G is a permutation group with correction capability r. Then, for the repetition code $\mathrm{Rep}_\lambda(G)$, the strength r' of the UBB required for $\mathrm{Rep}_\lambda(G)$ is equal to r.*

Proof. We know that $r = \lfloor (d-1)/2 \rfloor$, where d is the minimum distance of G. Now, $\mathrm{Rep}_\lambda(G)$ has minimum distance λd, correction capability $\lfloor (\lambda d - 1)/2 \rfloor$, and we have $r' = \lfloor \lfloor (\lambda d - 1)/2 \rfloor / \lambda \rfloor$. A case analysis to consider when d and λ are each odd or even then shows that, in all cases, $r' = \lfloor (\lambda d - 1)/2 \rfloor = r$. □

Note that the same result holds for "unimproved" twisted permutation codes; consequently, the UBBs obtained in [2, 3, 5] may be used not just for the corresponding repetition codes, but also the "unimproved" twisted permutation codes. In the table below, we give some further examples of groups (with multiple permutation representations), including some mentioned in [15] (namely $\mathrm{PSL}(2,11)$, M_{12} and A_7), and their parameters. For $2^4 : A_6$, $2^4 : S_6$ and M_{22}, we verified that $\delta_{\mathrm{tw}} = \delta_{\mathrm{rep}}$ with the same techniques as [15], using GAP.

Group G	$\lvert G\rvert$	n	λ	$\delta_{\mathrm{tw}} = \delta_{\mathrm{rep}}$	r	r'	$b(G)$	$\lvert\mathcal{U}\rvert$
$\mathrm{PSL}(2,11)$	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

Table 1: Parameters and decoding for some "unimproved" twisted permutation codes

The UBBs mentioned in Table 1 can be found in Appendix A. Each was obtained by taking the complements of blocks of the corresponding $(n, n - b(G), r')$-covering designs given in Gordon's database [17]; in some cases, the points needed to be relabelled to ensure that the complement of each block was a base for the group G.

2.3 Decoding twisted permutation codes with improved minimum distance

In the case of a twisted permutation code $\mathrm{Tw}(G, \mathcal{I})$ with improved minimum distance, the strength of the UBB we need is typically larger than that needed for the repetition code $\mathrm{Rep}_\lambda(G)$. For the groups S_6, A_6 and $\mathrm{ASL}(3,2)$, each of which were shown in [15] to yield such "improved" codes, we summarize the details in Table 2 below.

Group 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
$\mathrm{ASL}(3,2)$	1344	8	2	8	12	5	2	4	6

Table 2: Parameters and decoding for some "improved" twisted permutation codes

For S_6, the corresponding UBB consists of all 5-subsets of $\{1, \ldots, 6\}$; for A_6, we can use $\{1234, 1256, 3456\}$; for $\mathrm{ASL}(3,2)$, the UBB is given in Example 2.7.

As Table 2 does not give very many examples, in the next section we consider an infinite family of "improved" codes, taken from [1].

3 Codes from the groups $G_k(p)$

In [1, Section 3], Akbari *et al.* give an infinite family of twisted permutation codes, which arise from affine groups over the vector space $\mathbb{F}_p^k$. We begin by giving a summary of these groups and the corresponding codes.

Let B_k be the following $k \times k$ matrix over $\mathbb{F}_p$:

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

Since B_k is lower unitriangular, it is clearly invertible. It can be shown (see [1, Lemma 4]) that B_k has multiplicative order p, and that its powers are given by

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

for $0 \leq i < p$, and where the entries $\binom{i}{j}$ are taken modulo p.

Definition 3.1. Suppose that $V = \mathbb{F}_p^k$ is the space of row vectors, and let $H_k(p)$ be the subgroup of $GL(k, p)$ generated by B_k. Denote by $G_k(p)$ the subgroup $V \rtimes H_k(p)$ of $\mathrm{AGL}(k, p)$.

Since B_k has multiplicative order p, it follows that $G_k(p)$ has order p^{k+1}. Next, we define a $(k+1) \times (k+1)$ matrix

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

where $\mathbf{v}$ is a row vector in $\mathbb{F}_p^k$, and $0 \leq i < p$. Then denote the collection of all such matrices by $\overline{G_k(p)}$. In [1, Lemma 5], it is shown that $\overline{G_k(p)}$ is a subgroup of $GL(k+1, p)$ under matrix multiplication, has order p^{k+1}, and is isomorphic to the affine group $G_k(p)$. They also show (in [1, Lemma 7]) that $\overline{G_k(p)}$ acts faithfully and transitively on the set of p^k row vectors $\Omega = \{(1, \mathbf{v}) : \mathbf{v} \in \mathbb{F}_k^p\}$, so $\overline{G_k(p)}$ can be viewed as a permutation group on p^k points. Furthermore, they give a collection of isomorphisms, which they denote by $\tau_{\mathbf{w}}$, from $G_k(p)$ to $\overline{G_k(p)}$; these give a collection of permutation representations of $G_k(p)$ in $\mathrm{Sym}(\Omega)$, and thus can be used to construct twisted permutation codes. In particular, they show that as a permutation code $\overline{G_k(p)}$ has minimum distance $p^k - p$, so the p-fold repetition code $\mathrm{Rep}_p(\overline{G_k(p)})$ has minimum distance $p^{k+1} - p^2$; however, using a particular collection $\mathcal{I}$ of p permutation representations, there is a twisted permutation code $\mathrm{Tw}(G_k(p), \mathcal{I})$ with improved minimum distance $p^{k+1} - p$ (see [1, Proposition 9]).

To apply Algorithm 2.6 to these codes, we first need to obtain bases for the group $\overline{G_k(p)}$. Let $\mathbf{e}_1, \ldots, \mathbf{e}_k$ denote the standard basis vectors of $\mathbb{F}_p^k$.

Proposition 3.2. *For any j where $2 \leq j \leq k$, we have that $\{(1, \mathbf{0}),\ (1, \mathbf{e}_j)\}$ is a base for $\overline{G_k(p)}$ acting on the set Ω. Furthermore, $b(\overline{G_k(p)}) = 2$.*

Proof. Suppose that $A_{\mathbf{v},i}$ lies in the pointwise stabilizer of $\{(1,\mathbf{0}),\ (1,\mathbf{e}_j)\}$ in $\overline{G_k(p)}$. First, we have

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

so for $A_{\mathbf{v},i}$ to fix $(1,\mathbf{0})$ we must have $\mathbf{v}=\mathbf{0}$. Then we have

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

Now, $\mathbf{e}_jB_k^i$ is precisely row j of B_k^i, i.e.

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

So for this to be equal to $\mathbf{e}_j$, we require that $j \geq 2$ and that all the binomial coefficients are equal to 0; this will happen only when $i=0$. Consequently, we have that $A_{\mathbf{0},i}=A_{\mathbf{0},0}=I_{k+1}$, i.e. the identity element of $\overline{G_k(p)}$. Hence $\{(1,\mathbf{0}),\ (1,\mathbf{e}_j)\}$ is a base for $\overline{G_k(p)}$ acting on Ω.

Since $\overline{G_k(p)}$ acts transitively on Ω but $|\Omega| > |\overline{G_k(p)}|$, it follows that $\overline{G_k(p)}$ has no base of size 1; therefore $b(\overline{G_k(p)})=2$. □

The next step is to obtain an uncovering-by-bases for $\overline{G_k(p)}$. Now, since $b(\overline{G_k(p)})=2$, we can regard the minimum bases as the edges of a graph with vertex set Ω. The following terminology and notation was introduced by in 2020 by Burness and Giudici [10].

Definition 3.3. Let G be a group acting on Ω with $b(G)=2$. The *Saxl graph* of G, denoted $\Sigma(G)$, is the graph with vertex set Ω, and where $\{u,v\}$ is an edge if and only if it is a base for G.

Similar graphs (named "base-orbital graphs") appear in [5, Section 3], but where the edge set consists of a single orbit of G on its bases of size 2, rather than all such bases. Thus the edge set of the Saxl graph $\Sigma(G)$ is the union of the edge sets of each of the base-orbital graphs of G.

Proposition 3.4. *Let G be a permutation group, acting on a set Ω of size n, with base size $b(G)=2$. Then an optimal uncovering-by-bases for G is a matching in the Saxl graph $\Sigma(G)$.*

Proof. The smallest possible size of a UBB of strength r' is $r'+1$, as otherwise there will be a set of r' points which intersects each base non-trivially. A set of $r'+1$ disjoint bases (i.e. a set of $r'+1$ disjoint edges in $\Sigma(G)$) will be sufficient. But this is exactly a matching of size $r'+1$ in $\Sigma(G)$. Since $r' \leq \left\lfloor \frac{n-2}{2} \right\rfloor$, the requirement that $2(r+1) \leq n$ will always hold. □

Recall that a *perfect matching* in a graph Γ on n vertices is a matching (of size $\frac{n}{2}$) which includes every vertex of Γ. If n is odd, no perfect matching can exist, but a *near-perfect matching* is a matching which includes every vertex except one. The following result is well-known (see, for example, Godsil and Royle [16, Section 3.5]).

Lemma 3.5. *Let Γ be a connected, vertex-transitive graph with n vertices. Then Γ has either a perfect matching or a near-perfect matching, depending on the parity of n.*

By construction, the Saxl graph $\Sigma(G)$ will be vertex-transitive whenever G is transitive; in order to apply Lemma 3.5 to $\Sigma(G)$, one must show that it is connected. (The condition is necessary: a disconnected graph where all components have odd size can never have a (near-) perfect matching.) We would like to apply this to the Saxl graph of $\overline{G_k(p)}$.

Lemma 3.6. *Let G be the group $\overline{G_k(p)}$ acting on the set $\Omega = \{(1, \mathbf{v}) \, : \, \mathbf{v} \in \mathbb{F}_p^k\}$. Then the Saxl graph $\Sigma(G)$ is connected.*

Proof. We will show that for each element $(1, \mathbf{v}) \in \Omega$, there exists a path in $\Sigma(G)$ to $(1, \mathbf{0})$.

We saw in Proposition 3.2 that $\{(1, \mathbf{0}), (1, \mathbf{e}_j)\}$ is a base for G for $2 \leq j \leq k$. Now consider the orbit of G on such bases; for $A_{\mathbf{v},i} \in G$, we have that

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

and

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

where $\mathbf{b}_j^i = \mathbf{e}_j B_k^i$ denotes row j of the matrix B_k^i. So $\{(1, \mathbf{v}), (1, \mathbf{v} + \mathbf{b}_j^i)\}$ is a base for G. Therefore, in $\Sigma(G)$ each vertex $(1, \mathbf{v})$ is adjacent to $(1, \mathbf{v} \pm \mathbf{b}_j^i)$; we can label these edges by $\mathbf{b}_j^i$. Now, for $2 \leq j \leq k$, we have that $\mathbf{b}_j^i = \mathbf{e}_j$, while $\mathbf{b}_2^1 = \mathbf{e}_1 + \mathbf{e}_2$.

Now suppose that $\mathbf{v} = (v_1, v_2, \ldots, v_k)$. Then there is a path in $\Sigma(G)$ from $(1, v_1, v_2, \ldots, v_k)$ to $(1, v_1, v_2, \ldots, v_{k-1}, 0)$ using edges labelled by $\mathbf{e}_k$, then a path from $(1, v_1, v_2, \ldots, v_{k-1}, 0)$ to $(1, v_1, v_2, \ldots, v_{k-2}, 0, 0)$ using edges labelled by $\mathbf{e}_{k-1}$, and so on, until we reach $(1, v_1, v_2, 0, \ldots, 0)$. From there, there is a path to $(1, v_1, v_1, 0, \ldots, 0)$ using edges labelled by $\mathbf{e}_2$, and then finally a path to $(1, 0, \ldots, 0)$ using edges labelled by $\mathbf{e}_1 + \mathbf{e}_2$.

Since there is a path in $\Sigma(G)$ from any vertex to $(1, \mathbf{0})$, it follows that $\Sigma(G)$ is connected. □

Putting all of this together, we have the following result.

Theorem 3.7. *The twisted permutation code $\mathrm{Tw}(G_k(p), \mathcal{I})$, which has size p^{k+2}, length p^{k+1} and minimum distance $p^{k+1} - p$, can be decoded using an uncovering-by bases of optimal size $r' + 1 = \left\lfloor \frac{p^k - 1}{2} \right\rfloor$.*

Proof. The size, length and minimum distance of $\mathrm{Tw}(G_k(p), \mathcal{I})$ were all determined in [1]. Calculating r' is a straightforward exercise from this. Since $\Sigma(\overline{G_k(p)})$ is connected (by Lemma 3.6), it has a (near-) perfect matching (by Lemma 3.5), which forms an optimal UBB (by Proposition 3.4). □

4 Another infinite family

We conclude the paper by mentioning another family of groups, mentioned in [15, Section 6], with multiple permutation representations. Let V be the additive group of $\mathbb{F}_{2^m}^2$ and K denote the special linear group $\mathrm{SL}(2, 2^m)$. Since the first cohomology group $H^1(K, V)$ has order 2^m (cf. [11, Table 7.3]), we have 2^m outer automorphisms of the semidirect product $G = V \rtimes K$. It follows that there are 2^m permutation representations of G, the affine special linear group $\mathrm{ASL}(2, 2^m)$, and thus $\mathrm{ASL}(2, 2^m)$ is a candidate for constructing a twisted permutation code. Furthermore, a family of UBBs which can be used for these groups is constructed in [2, Theorem 5.27].

Unfortunately, as shown in [15, Theorem 6.1], twisting does not yield codes with improved minimum distance in this instance. The possible numbers of fixed points of a non-identity element of $G = \mathrm{ASL}(2, 2^m)$ are 0, 1 or 2^m, and thus the minimum distance is $2^{2m} - 2^m$. For the minimum distance of a twisted permutation code $\mathrm{Tw}(G, \mathcal{I})$ to be improved from that of the repetition code $\mathrm{Rep}_\lambda(G)$, a necessary condition is that each conjugacy class of elements of G with the maximum number of fixed points must be mapped by an outer automorphism to a conjugacy class of elements with fewer fixed points; these two conjugacy classes must have the same size and consist of elements of the same order. However, in $\mathrm{ASL}(2,2^m)$ no such conjugacy classes can exist: there is a unique conjugacy class of elements with 2^m fixed points, and these elements have order 2; there is only one other conjugacy class of elements of order 2, formed of the non-zero elements of the elementary abelian subgroup V, and this has a different size.

A Appendix: Some examples of uncoverings-by-bases

Example A.1. For the group $G = \mathrm{PSL}(2,11)$, we have $n = 11$, $b(G) = 3$ and $r' = 3$:

1	2	11
2	8	10
3	4	5
6	7	9
8	10	11

Example A.2. For the group M_{12}, we have $n = 12$, $b(M_{12}) = 5$ and $r' = 3$. Since M_{12} is sharply 5-transitive, any 5-subset forms a base. This example is taken from [2, Table 1].

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

Example A.3. For the group A_7, we have $n = 15$, $b(A_7) = 4$ and $r' = 5$. This example is referred to in [2], but is not given there explicitly.

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

Example A.4. For the group $G = 2^4 : A_6$, we have $n = 16$, $b(G) = 4$ and $r' = 5$:

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

Example A.5. For the group $G = 2^4 : S_6$, we have $n = 16$, $b(G) = 5$ and $r' = 3$:

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

Example A.6. For the group M_{22}, we have $n = 22$, $b(M_{22}) = 5$ and $r' = 7$:

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

Acknowledgements

The first author acknowledges financial support from an NSERC Discovery Grant. The second author was the recipient of an NSERC Undergraduate Student Research Award. Part of this work is taken from the second author's B.Sc. Senior Project thesis at Grenfell Campus, Memorial University. Both authors would like to thank the anonymous referees for their suggestions, and Peter Cameron and Robert Guralnick for useful discussions.

References

[1] M. Akbari, N. I. Gillespie and C. E. Praeger, Increasing the minimum distance of codes by twisting, *Electron. J. Combin.* **25(3)** (2018), #P3.36, 19 pp.

[2] R. F. Bailey, Uncoverings-by-bases for base-transitive permutation groups, *Des. Codes Cryptogr.* **41** (2006), 153–176.

[3] R. F. Bailey, Error-correcting codes from permutation groups, *Discrete Math.* **309** (2009), 4253–4265.

[4] R. F. Bailey and J. N. Bray, Decoding the Mathieu group M_{12}, *Adv. Math. Commun.* **1** (2007), 477–487.

[5] R. F. Bailey and P. J. Cameron, On the single-orbit conjecture for uncoverings-by-bases, *J. Group Theory* **11** (2008), 845–850.

[6] R. F. Bailey and J. P. Dixon, Distance enumerators for permutation groups, *Comm. Algebra* **35** (2007), 3045–3051.

[7] R. F. Bailey and T. Prellberg, Decoding generalised hyperoctahahedral groups and asymptotic analysis of correctible error patterns, *Contrib. Discrete Math.* **7** (2012), 1–14.

[8] N. Beeri and M. Schwartz, Improved rank-modulation codes for DNA storage with shotgun sequencing, *IEEE Trans. Inform. Theory* **68** (2022), 3719–3730.

[9] I. F. Blake, G. Cohen and M. Deza, Coding with permutations, *Inform. and Control* **43** (1979), 1–19.

[10] T. C. Burness and M. Giudici, On the Saxl graph of a permutation group, *Math. Proc. Cambridge Philos. Soc.* **168** (2020), 219–248.

[11] P. J. Cameron, *Permutation Groups*, London Math. Soc. Student Texts (45), Cambridge University Press, Cambridge, 1999.

[12] W. Chu, C. J. Colbourn and P. Dukes, Constructions for permutation codes in powerline communications, *Des. Codes Cryptogr.* **32** (2004), 51–64.

[13] C. J. Colbourn and J. H. Dinitz (editors), *Handbook of Combinatorial Designs* (second edition), CRC Press, Boca Raton, 2007.

[14] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1*; 2021, `www.gap-system.org`.

[15] N. I. Gillespie, C. E. Praeger and P. Spiga, Twisted permutation codes, *J. Group Theory* **18** (2015), 407–433.

[16] C. D. Godsil and G. F. Royle, *Algebraic Graph Theory*, Graduate Texts in Mathematics (207), Springer-Verlag, New York, 2001.

[17] D. M. Gordon, *Covering Designs*, `www.dmgordon.org/cover/`; last accessed 22 October 2023.

[18] S. Huczynska and G. L. Mullen, Frequency permutation arrays, *J. Combin. Des.* **14** (2006), 463–478.

[19] T. Kløve, T. T. Lin, S.-C. Tsai and W.-G. Tzeng, Permutation arrays under the Chebyshev distance, *IEEE Trans. Inform. Theory* **56** (2010), 2611–2617.

[20] I. Tamo and M. Schwartz, Correcting limited-magnitude errors in the rank-modulation scheme, *IEEE Trans. Inform. Theory* **56** (2010), 2551–2560.