A Class of PAs with Efficient Contraction

Avi Levy

11/20/12

Abstract

Optimal permutation arrays (PAs) have a sharply transitive group structure. A contraction operation is defined that constructs new permutation arrays from old ones. We characterize the effect of contraction on all sharply transitive group PAs.

1 Introduction

In section 2, we define $m$-contraction and show that $m \leq 3$ for all PAs. Next in section 3, we restrict our attention to group PAs and prove equivalent conditions for $m = 3$. The main result is in section 4, where we consider sharply transitive group PAs. Theorem 4.1 classifies the contraction of all sharply transitive group PAs.

In this paper, $e$ denotes the identity permutation. PA stands for “permutation array”. When $\sigma, \tau$ are permutations, $d(\sigma, \tau)$ denotes the Hamming distance between $\sigma, \tau$; it is invariant under permutation composition [put citation].

2 $m$-Contraction

Definition 2.1. The contraction [put citation] of $\sigma$ is

$$\sigma' = \left( n \sigma^{-1}(n) \right) \sigma$$

Definition 2.2. The PA$(n,d)$ is said to $m$-contract if the contractions of the elements of the PA$(n,d)$ form a PA$(n,d - m)$. 

1
Let $\sigma, \tau$ be permutations on $\{1, 2, \cdots, n\}$.

**Lemma 2.1.** $d(\sigma', \tau') \geq d(\sigma, \tau) - 3$

When equality holds, $\pi^3(n) = n, \pi(n) \neq n$ where $\pi = \sigma\tau^{-1}$.

**Proof.** Let $s = \sigma^{-1}(n), t = \tau^{-1}(n)$

\[
d(\sigma', \tau') = d((n \ s)\sigma, (n \ t)\tau) = d(\pi, (n \ s \ t)) \geq d(\pi, e) - d(e, (n \ s \ t)) = d(\sigma, \tau) - d(e, (n \ s \ t)) \geq d(\sigma, \tau) - 3
\]

Now, we examine the equality case. Step (**) implies $n, s, t$ are distinct. Step (*) follows from the triangle inequality, which states that $d(a, b) + d(b, c) \geq d(a, c)$.

\[
d(a, b) + d(b, c) = d(a, c) \iff \left(a(i) \neq b(i) \implies b(i) = c(i)\right)
\]

Applied to (*)

\[
d(e, (n \ s \ t)) + d((n \ s \ t), \pi) = d(e, \pi) \iff \pi : (n \ s \ t) \to (s \ t \ n)
\]

Hence $\pi^3(n) = n, \pi(n) \neq n$. \hfill \Box

As a consequence, this shows that $m \leq 3$ in $m$-contraction.

### 3 Conditions for 3-Contraction

In this section, we prove equivalent conditions for 3-contraction of groups.

**Definition 3.1.** A $PA(n, d)$ is called a $G(n, d)$ if it is also a group.

**Theorem 3.1.** A $G(n, d)$ 3-contracts iff $G$ contains a permutation $\pi$ such that
1. $\pi^3(n) = n$
2. $\pi(n) \neq n$
3. $d(e, \pi) = d$

Proof. Suppose $G$ contains such an element $\pi$. Define $s, t$ such that $(n \ s \ t) = (n \ \pi(n) \ \pi^2(n))$ Then the contractions of $\pi, \pi^2$ have distance $d - 3$. Indeed,
\[
d(\pi', (\pi^2)') = d((n \ t)\pi, (n \ s)\pi^2) \\
= d((n \ s \ t), \pi) \\
\quad (\ast) = d(e, \pi) - 3 \\
= d - 3
\]

Step $(\ast)$ requires explanation. In all locations besides $n, s, t$, permutations $e, \pi$ differ iff $(n \ s \ t), \pi$ differ. At locations $n, s, t, e, \pi$ differ but $(n \ s \ t), \pi$ match. Thus the number of mismatches decreases by 3. Since we have found a pair of contracted permutations with Hamming distance $d - 3$, and Lemma 2.1 implies that this is the minimal distance, this implies that $G(n, d)$ 3-contracts.

For the other direction, suppose that the $G(n, d)$ 3-contracts. Then there exist permutations $\sigma, \tau \in G$ for which the equality case of Lemma 2.1 holds. Thus, $\pi^3(n) = n$ and $\pi(n) \neq n$. Furthermore, $d(\sigma, \tau) - 3 = d - 3 \implies d(e, \pi) = d$. Taking $g = \pi \in G$, we have constructed a $g$ satisfying the conditions of this theorem. \qed

4 Classification

Using Theorem 3.1, we classify contractions of all sharply-transitive $G(n, d)$.

**Theorem 4.1.** Let $G$ be a sharply-transitive $G(n, d)$.

<table>
<thead>
<tr>
<th>Condition</th>
<th>Contracts to</th>
</tr>
</thead>
<tbody>
<tr>
<td>$d \equiv 0 \ mod \ 3$</td>
<td>$PA(n - 1, d - 3)$</td>
</tr>
<tr>
<td>$d \not\equiv 0 \ mod \ 3$</td>
<td>$PA(n - 1, d - 2)$</td>
</tr>
</tbody>
</table>
Proof. Let the $G(n, d)$ undergo $m$-contraction. We’ve shown generally that $m \leq 3$. Now suppose that $m < 2$. If this was the case, after contraction there would be $\frac{n!}{(d-1)!}$ permutations of length $n-1$, with pairwise Hamming distance at most $d-1$. This would imply

$$M(n-1, d-1) \geq \frac{n}{d-1} \frac{(n-1)!}{(d-2)!} > \frac{(n-1)!}{(d-2)!} \geq M(n-1, d-1)$$

This contradiction follows from the maximality of the sharply-transitive group PAs [put citation here]. We conclude $m \in \{2, 3\}$.

The rest of the classification involves the following two cases:

• $d \equiv 0 \mod 3$

  In this case, we will show that 3-contraction occurs by finding an element that satisfies the conditions of Theorem 3.1. Consider the set

  $$S = \{\pi \in G| 1 \leq i \leq n-d \implies \pi(i) = i\}$$

  It is straightforward to verify that $S$ is a subgroup of $G$. Moreover, since $G$ is sharply $n-d+1$-transitive, there is a unique element in $S$ for every value of $\pi(n-d+1)$. Since $\pi(n-d+1)$ takes on each of the $d$ values from $n-d+1$ to $n$ inclusive, there are precisely $d$ elements in $S$.

  By Cauchy’s Theorem, $3|d = |S| \implies S$ has an element of order 3 [put citation here]. Call this element $\pi$. Then $\pi^3(n) = n$. Now consider $d(e, \pi)$. The two permutations match for positions $i \leq n-d$, by construction. By $n-d+1$-transitivity, they can not match anywhere else. Thus $d(e, \pi) = d$. As a consequence, $\pi(n) \neq n$. Thus by Theorem 3.1, the $G(n, d)$ undergoes 3-contraction.

• $d \not\equiv 0 \mod 3$

  We proceed by assuming for contradiction that $G(n, d)$ 3-contracts. By Theorem 3.1, there exists an element $\pi$ with $\pi^3(n) = n$ such that $\pi(n) \neq n$. This implies that $n$ is contained in a 3-cycle. Thus $\pi$ contains a 3-cycle, so its order is a multiple of 3 [put citation here].

  Now we construct a group $S'$ that mimics the construction of $S$ above, such that $\pi \in S'$. Let $I$ be the set of fixed points of $\pi$. By $(n-d+1)$-transitivity, $|I| = n-d$. Then define

  $$S' = \{\sigma \in G|i \in I \implies \sigma(i) = i\}$$
Note that $\pi \in S'$. As before, $S'$ is a group. By sharp transitivity, $|S| = d$. Thus $3|\text{ord}(\pi)|d$, which is a contradiction. Thus $G(n, d)$ undergoes 2-contraction.

\[ \qed \]

5 Conclusions/Results/Citations

Pending. Will report new lower bounds as a consequence of this theorem with data from our table.