AAECC **14**, 97–115 (2003)
Digital Object Identifier (DOI) 10.1007/s00200-003-0125-5

AAECC
Applicable Algebra in Engineering, Communication and Computing

Group Actions on Binary Resilient Functions

Xiang-Dong Hou

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435, USA
(e-mail: xhou@euler.math.wright.edu)

Received: November 20, 2001; revised version: April 18, 2003

Abstract. Let $G_{n,t}$ be the subgroup of $\mathrm{GL}(n, \mathbb{Z}_2)$ that stabilizes $\{x \in \mathbb{Z}_2^n : |x| \le t\}$. We determine $G_{n,t}$ explicitly: For $1 \le t \le n-2$, $G_{n,t} = S_n$ when t is odd and $G_{n,t} = \langle S_n, \Delta \rangle$ when t is even, where $S_n < \mathrm{GL}(n, \mathbb{Z}_2)$ is the symmetric group of degree n and $\Delta \in \mathrm{GL}(n, \mathbb{Z}_2)$ is a particular involution. Let $\mathcal{R}_{n,t}$ be the set of all binary t-resilient functions defined on $\mathbb{Z}_2^n$. We show that the subgroup $\mathbb{Z}_2^n \rtimes (G_{n,t} \cup G_{n,n-1-t}) < \mathrm{AGL}(n, \mathbb{Z}_2)$ acts on $\mathcal{R}_{n,t}/\mathbb{Z}_2$. We determine the representatives and sizes of the conjugacy classes of $\mathbb{Z}_2^n \rtimes S_n$ and $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$. These results allow us to compute the number of orbits of $\mathcal{R}_{n,t}/\mathbb{Z}_2$ under the above group action for $(n, t) = (5, 1)$ and $(6, 2)$.

Keywords: General linear group, Affine linear group, Resilient function.

1 Introduction

The problem considered in this paper originated from binary resilient functions. Let $\mathcal{P}_n$ be the set of all functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$. The Hamming weight of a function $f \in \mathcal{P}_n$, denoted by $|f|$, is the cardinality of $f^{-1}(1)$. The Hamming weight of a binary vector, row or column, is also denoted by $|\cdot|$. We use $\langle \cdot, \cdot \rangle$ to denote the usual dot product in $\mathbb{Z}_2^n$. Thus for $s \in \mathbb{Z}_2^n$, $\langle s, \cdot \rangle \in \mathcal{P}_n$ is the linear function defined by $x \mapsto \langle s, x \rangle$ ($x \in \mathbb{Z}_2^n$). A function $f \in \mathcal{P}_n$ is called t-resilient if

$$|f + \langle s, \cdot \rangle| = 2^{n-1} \text{ for all } s \in \mathbb{Z}_2^n \text{ with } |s| \le t. \tag{1.1}$$

(If (1.1) holds for all $s \in \mathbb{Z}_2^n$ with $1 \le |s| \le t$, f is called tth order correlation-immune.) Resilient functions and correlation-immune functions were introduced by Chor et al [3], Bennett et al [1] and Siegenthaler [6] for applications in several areas of cryptography. The applications include random string generation, fault-tolerant distributed computing and resistance against correlation attack.

This paper is a treatment of binary resilient functions from an algebraic point of view; our attempt is to understand the classification of such functions. Let $\mathcal{R}_{n,t}$ be the set of all t-resilient functions in $\mathcal{P}_n$. Since $f \in \mathcal{R}_{n,t}$ if and only if $f + 1 \in \mathcal{R}_{n,t}$, it suffices to consider $\mathfrak{R}_{n,t} = \mathcal{R}_{n,t}/\mathbb{Z}_2$, i.e., $\mathcal{R}_{n,t}$ modulo the constant functions. It also suffices to assume $1 \le t \le n-4$ since $\mathfrak{R}_{n,0}$ consists of balanced functions and $\mathfrak{R}_{n,t}$ is completely known for $t \ge n-3$ ([2], [4]). The first step towards the classification of $\mathfrak{R}_{n,t}$ is to identify a group action on $\mathfrak{R}_{n,t}$. Obviously, the subgroup $\mathbb{Z}_2^n$ of translations of the affine linear group $\mathrm{AGL}(n, \mathbb{Z}_2)$ acts on $\mathfrak{R}_{n,t}$. The general linear group $\mathrm{GL}(n, \mathbb{Z}_n)$ does not act on $\mathfrak{R}_{n,t}$ unless $t = 0$. However, if we let $G_{n,t}$ be the subgroup of $\mathrm{GL}(n, \mathbb{Z}_2)$ that stabilizes the Hamming sphere $\{x \in \mathbb{Z}_2^n : |x| \le t\} \subset \mathbb{Z}_2^n$, then $G_{n,t}$ acts on $\mathfrak{R}_{n,t}$. We will see that $G_{n,n-1-t}$ also acts on $\mathfrak{R}_{n,t}$ in an indirect way. As it turns out below, either $G_{n,t} \subset G_{n,n-1-t}$ or $G_{n,t} \supset G_{n,n-1-t}$. Hence the semidirect product $\mathbb{Z}_2^n \rtimes (G_{n,t} \cup G_{n,n-1-t}) < \mathrm{AGL}(n, \mathbb{Z}_2)$ acts on $\mathfrak{R}_{n,t}$.

In Section 2, we determine the group $G_{n,t}$ explicitly. For $1 \le t \le n-2$, $G_{n,t} = S_n$ when t is odd and $G_{n,t} = \langle S_n, \Delta \rangle$ when t is even, where $S_n < \mathrm{GL}(n, \mathbb{Z}_2)$ is the symmetric group of degree n and

$$\Delta = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}. \tag{1.2}$$

We describe the action of $\mathbb{Z}_2^n \rtimes (G_{n,t} \cup G_{n,n-1-t})$ on $\mathfrak{R}_{n,t}$ in Section 3.

We are interested in the number of orbits in $\mathfrak{R}_{n,t}$ under the action of $\mathbb{Z}_2^n \rtimes (G_{n,t} \cup G_{n,n-1-t})$, where the group is either $\mathbb{Z}_2^n \rtimes S_n$ or $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$. To compute this number using the Burnside lemma, we need to determine the representatives and sizes of the conjugacy classes of $\mathbb{Z}_2^n \rtimes S_n$ and $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$. We answer these questions in Section 4, which is the technical portion of the paper.

In Section 5, we use the results of Section 4 to compute the number of $\mathbb{Z}_2^n \rtimes (G_{n,t} \cup G_{n-1-t,t})$-orbits in $\mathfrak{R}_{n,t}$ for $(n, t) = (5, 1)$ and $(6, 2)$.

2 The Group $G_{n,t}$

Recall that

$$G_{n,t} = \{A \in \mathrm{GL}(n, \mathbb{Z}_2) : |Ax| \le t \text{ for all } x \in \mathbb{Z}_2^n \text{ with } |x| \le t\}. \tag{2.1}$$

Elements in $G_{n,t}$ are matrices $A \in \mathrm{GL}(n, \mathbb{Z}_2)$ such that any sum of $\le t$ columns of A has weight $\le t$ and any sum of $> t$ columns of A has weight $> t$. Clearly, $G_{n,t} = \mathrm{GL}(n, \mathbb{Z}_2)$ for $t = 0$ or n. When $t = n-1$, $G_{n,n-1} < \mathrm{GL}(n, \mathbb{Z}_2)$ is the stabilizer of $[1, \cdots, 1]^T \in \mathbb{Z}_2^n$. $G_{n,n-1}$ is conjugate to the stabilizer of $[1, 0, \cdots, 0]^T$ and the latter is

$$\left\{ \begin{bmatrix} 1 & * \\ 0 & B \end{bmatrix} : B \in \mathrm{GL}(n-1, \mathbb{Z}_2) \right\} \cong \mathrm{AGL}(n-1, \mathbb{Z}_2). \tag{2.2}$$

Let $S_n < \mathrm{GL}(n, \mathbb{Z}_2)$ be the subgroup of permutation matrices. Then $S_n \subset G_{n,t}$. Let $\Delta \in \mathrm{GL}(n, \mathbb{Z}_2)$ be as in (1.2). It is also easy to see that $\Delta \in G_{n,t}$ when t is even. The main result of this section is the following theorem.

Theorem 2.1. *For* $1 \le t \le n-2$, *we have*

$$G_{n,t} = \begin{cases} S_n, & \text{if } t \text{ is odd}, \\ \langle S_n, \Delta \rangle, & \text{if } t \text{ is even}. \end{cases} \tag{2.3}$$

We first prove a lemma.

Lemma 2.2. *Let* $1 \le t \le n-2$ *and* $A \in G_{n,t}$. *Then all columns of* A *have weight* ≤ 2.

Proof. Assume the contrary and write

$$A = \begin{bmatrix} \mathbf{1}_\mu & b_1 & \cdots & b_{n-1} \\ \mathbf{0}_{n-\mu} & c_1 & \cdots & c_{n-1} \end{bmatrix}, \quad \mu \ge 3, \ b_i \in \mathbb{Z}_2^\mu, \ c_i \in \mathbb{Z}_2^{n-\mu}, \tag{2.4}$$

where $\mathbf{1}_\mu$ is the all 1 column vector of length μ and $\mathbf{0}_{n-\mu}$ is the all 0 column vector of length $n-\mu$. We also assume that μ is the smallest among the column weights of A which are ≥ 3.

First assume that $t - 1 \le n - \mu$. Since $\mathrm{rank}[c_1, \cdots, c_{n-1}] = n - \mu$, there are $s \le t-1$ columns from $[c_1, \cdots, c_{n-1}]$, say, $c_1, \cdots, c_s$, such that $|c_1 + \cdots + c_s| \ge t-1$. It follows that one of

$$\begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \mathbf{1}_\mu \\ \mathbf{0}_{n-\mu} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix}$$

has weight $> t$, which is a contradiction to the fact $A \in G_{n,t}$.

Next assume that $t - 1 > n - \mu$ but $t < n - \frac{\mu}{2}$. Then $[c_1, \cdots, c_{n-1}]$ has $s \le n - \mu$ columns, say, $c_1, \cdots, c_s$, such that $|c_1 + \cdots + c_s| \ge n - \mu$. We have

$$\begin{aligned} &\max\left\{ \left| \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix} \right|, \ \left| \begin{bmatrix} \mathbf{1}_\mu \\ \mathbf{0}_{n-\mu} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix} \right| \right\} \\ &\quad \ge n - \mu + \frac{\mu}{2} = n - \frac{\mu}{2} > t, \end{aligned} \tag{2.5}$$

which is again a contradiction.

Now assume that $t \ge n - \frac{\mu}{2}$. Since $\mu \le t$, we have $t \ge \frac{2}{3}n$. Observe that A stabilizes $\{x \in \mathbb{Z}_2^n : |x| \ge t+1\}$ and that

$$\begin{aligned} |\{x \in \mathbb{Z}_2^n : |x| = t+1\}| &= \binom{n}{t+1} > \binom{n}{t+2} + \cdots + \binom{n}{n} \\ &= |\{x \in \mathbb{Z}_2^n : |x| \ge t+2\}|. \end{aligned} \tag{2.6}$$

(In (2.6), we used the fact that $t \geq \frac{2}{3}n$.) Thus there exists an $x \in \mathbb{Z}_2^n$ such that $|Ax| = |x| = t+1$. Therefore we may assume that the sum of the first $t+1$ columns of A has weight $t+1$. Write

$$A = \begin{bmatrix} d_1 & \cdots & d_n \\ e_1 & \cdots & e_n \end{bmatrix}, \quad d_i \in \mathbb{Z}_2^{t+1},\ e_i \in \mathbb{Z}_2^{n-(t+1)}, \tag{2.7}$$

where

$$d_1 + \cdots + d_{t+1} = \mathbf{1}_{t+1}, \quad e_1 + \cdots + e_{t+1} = 0. \tag{2.8}$$

Since

$$\left| \begin{bmatrix} d_1 \\ e_1 \end{bmatrix} + \cdots + \begin{bmatrix} d_{t+1} \\ e_{t+1} \end{bmatrix} + \begin{bmatrix} d_i \\ e_i \end{bmatrix} \right| \geq t+1 \text{ for all } t+1 < i \leq n, \tag{2.9}$$

we have $|d_i| \leq |e_i|$ and consequently,

$$\left| \begin{bmatrix} d_i \\ e_i \end{bmatrix} \right| \leq 2|e_i| \leq 2\big(n-(t+1)\big) < \mu, \quad t+1 < i \leq n. \tag{2.10}$$

By our assumption on the minimality of μ, we must have

$$\left| \begin{bmatrix} d_i \\ e_i \end{bmatrix} \right| = 1 \text{ or } 2, \quad \text{for } t+1 < i \leq n. \tag{2.11}$$

We claim that $e_{t+2}, \cdots, e_n$ are linearly independent. Otherwise,

$$\alpha_{t+2}e_{t+2} + \cdots + \alpha_n e_n = 0 \tag{2.12}$$

for some $0 \neq (\alpha_{t+2}, \cdots, \alpha_n) \in \mathbb{Z}_2^{n-(t+1)}$. It follows that $\alpha_{t+2}d_{t+2} + \cdots + \alpha_n d_n \neq 0$ and

$$\left| \begin{bmatrix} d_1 \\ e_1 \end{bmatrix} + \cdots + \begin{bmatrix} d_{t+1} \\ e_{t+1} \end{bmatrix} + \alpha_{t+2} \begin{bmatrix} d_{t+2} \\ e_{t+2} \end{bmatrix} + \cdots + \alpha_n \begin{bmatrix} d_n \\ e_n \end{bmatrix} \right| \leq t, \tag{2.13}$$

which is a contradiction.

We further claim that $e_1 = \cdots = e_{t+1} = 0$. Otherwise, say $e_1 \neq 0$. Since $\text{rank}[e_{t+2}, \cdots, e_n] = n-(t+1)$, there is an $i > t+1$ such that $e_i \cdot e_1 \neq 0$, where $e_i \cdot e_1$ is the coordinate wise product of e_i and e_1. Note from (2.11) that $|d_i| \leq 1$ if $|e_i| = 1$ and that $|d_i| = 0$ if $|e_i| = 2$. In either case,

$$\begin{aligned} \left| \begin{bmatrix} d_2 \\ e_2 \end{bmatrix} + \cdots + \begin{bmatrix} d_{t+1} \\ e_{t+1} \end{bmatrix} + \begin{bmatrix} d_i \\ e_i \end{bmatrix} \right| &= \left| \begin{bmatrix} \mathbf{1}_{t+1} \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \begin{bmatrix} d_1 \\ e_1 \end{bmatrix} + \begin{bmatrix} d_i \\ e_i \end{bmatrix} \right| \\ \leq \left| \begin{bmatrix} \mathbf{1}_{t+1} \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \begin{bmatrix} d_1 \\ e_1 \end{bmatrix} \right| &= \left| \begin{bmatrix} d_2 \\ e_2 \end{bmatrix} + \cdots + \begin{bmatrix} d_{t+1} \\ e_{t+1} \end{bmatrix} \right| \leq t, \end{aligned} \tag{2.14}$$

which is a contradiction.

Since A has at least one column with weight ≥ 3 and since the last $n-(t+1)$ columns of A have weight ≤ 2 ((2.11)), one of $d_1, \cdots, d_{t+1}$, say, d_1, has weight ≥ 3. We then have

$$\left\|\begin{bmatrix} d_2 \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \cdots + \begin{bmatrix} d_{t+1} \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \begin{bmatrix} d_{t+2} \\ e_{t+2} \end{bmatrix}\right\| = \left\|\begin{bmatrix} \mathbf{1}_{t+1} \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \begin{bmatrix} d_1 \\ \mathbf{0}_{n-t-1} \end{bmatrix} + \begin{bmatrix} d_{t+2} \\ e_{t+2} \end{bmatrix}\right\| \leq t+1-3+2 = t, \tag{2.15}$$

which is again a contradiction. □

Proof of Theorem 2.1. Let $A \in G_{n,t}$. We want to show that $A \in S_n$ when t is odd and $A \in \langle S_n, \Delta\rangle$ when t is even. By Lemma 2.2, all columns of A have weight ≤ 2. If all columns of A have weight 1, then $A \in S_n$ and we are done. So we assume that A has at least one column with weight 2.

We first claim that if A has two columns a_1 and a_2 with $|a_1| = |a_2| = 2$, then the coordinate wise product $a_1 \cdot a_2 \neq 0$. Otherwise, write

$$A = \begin{bmatrix} 1\,0 & \\ 1\,0 & \\ 0\,1 & b_1 \cdots b_{n-2} \\ 0\,1 & \\ & \\ 0 & c_1 \cdots c_{n-2} \end{bmatrix}, \quad b_i \in \mathbb{Z}_2^4,\ c_i \in \mathbb{Z}_2^{n-4}. \tag{2.16}$$

Note that $\operatorname{rank}[c_1, \cdots, c_{n-2}] = n-4$. If $t-1 \leq n-4$, there are $s \leq t-1$ columns of $[c_1, \cdots, c_{n-2}]$, say, $c_1, \cdots, c_s$, such that $|c_1 + \cdots + c_s| \geq t-1$. Then one of

$$\begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ \mathbf{0}_{n-4} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ \mathbf{0}_{n-4} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_s \\ c_s \end{bmatrix}$$

has weight $\geq t+1$, which is a contradiction. If $t = n-2$, one of

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ \mathbf{0}_{n-4} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_{n-2} \\ c_{n-2} \end{bmatrix} \text{ and } \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ \mathbf{0}_{n-4} \end{bmatrix} + \begin{bmatrix} b_1 \\ c_1 \end{bmatrix} + \cdots + \begin{bmatrix} b_{n-2} \\ c_{n-2} \end{bmatrix}$$

has weight $\leq 2 + |c_1 + \cdots + c_{n-2}| \leq n-2 = t$, which is also a contradiction.

If A has 3 columns a_1, a_2, a_3 with $|a_1| = |a_2| = |a_3| = 2$, then their coordinate wise product $a_1 \cdot a_2 \cdot a_3 \neq 0$. Otherwise, we would have

$$[a_1\ a_2\ a_3] = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ \vdots & \vdots & \vdots \\ 0 & 0 & 0 \end{bmatrix} \tag{2.17}$$

and a_1, a_2, a_3 would be linearly dependent.

Based on the claim so far, we can write

$$A = \begin{bmatrix} 1 \cdots 1 & \\ 1 & \\ \ddots & B \\ \quad 1 & \\ & \\ 0 & C \end{bmatrix} \tag{2.18}$$

where B is of size $(s+1) \times (n-s)$ and all columns of $\left[\begin{smallmatrix} B \\ C \end{smallmatrix}\right]$ have weight 1. In order for A to be invertible, up to a suitable permutation of the columns, we must have

$$A = \left.\begin{bmatrix} 1 \cdots 1 & & & * \\ 1 & & & * \\ & \ddots & & \vdots \\ & & 1 & * \\ & & 1 & 0 \\ & & \ddots & \vdots \\ & & & 1 \ 0 \end{bmatrix}\right\} {\scriptstyle s+1} = [a_1\ \cdots\ a_n], \quad |a_n| = 1. \tag{2.19}$$

If $s < n-1$, let u be the largest odd integer $\leq \min\{t, s\}$. Observe that $|a_1 + \cdots + a_u| = u + 1$ and that $t - u \leq n - 1 - s$. Thus

$$|a_1 + \cdots + a_u + a_{s+1} + \cdots + a_{s+t-u}| = t + 1, \tag{2.20}$$

which is a contradiction. Therefore we must have $s = n - 1$. Then one can easily see that the fact $A \in G_{n,t}$ forces $a_n = [1, 0, \cdots, 0]^T$. Hence after a permutation of columns, A becomes Δ. When t is even, we have $A \in \langle S_n, \Delta \rangle$; when t is odd, we have a contradiction since $\Delta \notin G_{n,t}$. The proof of the theorem is now complete. □

The group $\langle S_n, \Delta\rangle$ has a familiar structure. For each $1 \le i \le n$, put

$$\Delta_i = \begin{bmatrix} 1 & & & & \\ & \ddots & & & \\ 1 & \cdots & 1 & \cdots & 1 \\ & & & \ddots & \\ & & & & 1 \end{bmatrix} = I + \begin{bmatrix} & & & & & & \\ \overbrace{1 \ \cdots \ 1 \ 0}^{i} & 1 & \cdots & 1 \\ & & & & & & \end{bmatrix}_i \tag{2.21}$$

Then every element in $\langle S_n, \Delta\rangle$ can be uniquely written as P or $\Delta_i P$ for some $P \in S_n$, $1 \le i \le n$. Throughout the paper, elements in S_n are viewed as permutation matrices as well as permutations on $\{1, \cdots, n\}$.

Proposition 2.3. *Let S_{n+1} be the symmetric group on $\{0, 1, \cdots, n\}$. Define*

$$\begin{aligned} \phi : \langle S_n, \Delta\rangle &\longrightarrow S_{n+1} \\ P &\longmapsto P \qquad \text{for } P \in S_n, \\ \Delta_i P &\longmapsto (0, i)P \quad \text{for } P \in S_n \text{ and } 1 \le i \le n. \end{aligned} \tag{2.22}$$

Then ϕ is a group isomorphism.

Proof. Direct computation shows that in $\langle S_n, \Delta\rangle$,

$$P\Delta_i = \Delta_{P(i)} P, \quad 1 \le i \le n, \ P \in S_n, \tag{2.23}$$

and

$$\Delta_i \Delta_j = \Delta_j (i, j), \quad 1 \le i, j \le n, \ i \ne j. \tag{2.24}$$

The same relations hold in S_{n+1} with $(0, i)$ in place of Δ_i. Consequently, the map ϕ in (2.22) is an isomorphism. □

3 Group Actions on $\mathfrak{R}_{n,t}$

The $\mathbb{Z}_2$-algebra $\mathcal{P}_n$ can be written as

$$\mathcal{P}_n = \mathbb{Z}_2[X_1, \cdots, X_n]/(X_1^2 - X_1, \cdots, X_n^2 - X_n) \tag{3.1}$$

and the affine linear group $\mathrm{AGL}(n, \mathbb{Z}_2)$ can be written as

$$\mathrm{AGL}(n, \mathbb{Z}_2) = \left\{ \begin{bmatrix} A & \\ a & 1 \end{bmatrix} : A \in \mathrm{GL}(n, \mathbb{Z}_2), a \in \mathbb{Z}_2^n \right\} < \mathrm{GL}(n+1, \mathbb{Z}_2). \tag{3.2}$$

The group of translations of $\mathrm{AGL}(n, \mathbb{Z}_n)$ is

$$\mathbb{Z}_2^n \cong \left\{ \begin{bmatrix} I & \\ a & 1 \end{bmatrix} : a \in \mathbb{Z}_2^n \right\}. \tag{3.3}$$

For each subgroup $G < \mathrm{GL}(n, \mathbb{Z}_2)$, the semidirect product of $\mathbb{Z}_2^n$ and G is

$$\mathbb{Z}_2^n \rtimes G = \left\{ \begin{bmatrix} A & \\ a & 1 \end{bmatrix} : A \in G, a \in \mathbb{Z}_2^n \right\} < \mathrm{AGL}(n, \mathbb{Z}_2). \tag{3.4}$$

There is a left $\mathrm{AGL}(n, \mathbb{Z}_2)$ action on $\mathcal{P}_n$:

$$\begin{aligned} \mathrm{AGL}(n, \mathbb{Z}_2) \times \mathcal{P}_n &\longrightarrow \mathcal{P}_n \\ (\sigma, f(X)) &\longmapsto \sigma(f(X)) = f(XA + a) \end{aligned} \tag{3.5}$$

where

$$\sigma = \begin{bmatrix} A & \\ a & 1 \end{bmatrix} \in \mathrm{AGL}(n, \mathbb{Z}_2) \text{ and } X = (X_1, \cdots, X_n). \tag{3.6}$$

Consequently, $\mathrm{AGL}(n, \mathbb{Z}_2)$ acts on $\mathcal{P}_n/\mathbb{Z}_2$; the latter contains $\mathfrak{R}_{n,t}$. However, $\mathfrak{R}_{n,t}$ is not $\mathrm{AGL}(n, \mathbb{Z}_2)$-invariant unless $t = 0$. In general, $\mathfrak{R}_{n,t}$ is acted on only by a certain subgroup of $\mathrm{AGL}(n, \mathbb{Z}_2)$.

Proposition 3.1. *If $f(X) \in \mathfrak{R}_{n,t}$ and $A \in G_{n,t}$, then $f(XA) \in \mathfrak{R}_{n,t}$.*

Proof. For each $s \in \mathbb{Z}_2^n$ with $|s| \le t$, we have

$$|f(XA) + Xs^T| = |f(X) + XA^{-1}s^T| = 2^{n-1} \tag{3.7}$$

since $|A^{-1}s^T| \le t$. □

Proposition 3.2. *Let $f(X) \in \mathfrak{R}_{n,t}$ and $A \in G_{n,n-t-1}$ and let $\mathbf{1}$ be the all 1 column vector of length n. Then*

$$f(XA) + X(A + I)\mathbf{1} \in \mathfrak{R}_{n,t} \tag{3.8}$$

Proof. For each $s \in \mathbb{Z}_2^n$ with $|s| \le t$, we have

$$\begin{aligned} &\left| f(XA) + X(A + I)\mathbf{1} + Xs^T \right| \\ &= \left| f(X) + XA^{-1}(A + I)\mathbf{1} + XA^{-1}s^T \right| \\ &= \left| f(X) + X\big(\mathbf{1} + A^{-1}(\mathbf{1} + s^T)\big) \right|. \end{aligned} \tag{3.9}$$

Since $|\mathbf{1} + s^T| \ge n - t$ and since $A \in G_{n,n-t-1}$, we have $|A^{-1}(\mathbf{1} + s^T)| \ge n - t$, hence $|\mathbf{1} + A^{-1}(\mathbf{1} + s^T)| \le t$. Consequently,

$$\left| f(X) + X\big(\mathbf{1} + A^{-1}(\mathbf{1} + s^T)\big) \right| = 2^{n-1}, \tag{3.10}$$

and the proof is complete. □

In fact, Proposition 3.2 is the result of the following indirect action of $G_{n,n-t-1}$ on $\mathfrak{R}_{n,t}$:

$$\begin{aligned} \mathfrak{R}_{n,t} \ni f(X) \longmapsto f(X) + X\mathbf{1} \overset{A \in G_{n,n-t-1}}{\longmapsto} f(XA) + XA\mathbf{1} \\ \longmapsto f(XA) + XA\mathbf{1} + X\mathbf{1} \in \mathfrak{R}_{n,t} \end{aligned} \tag{3.11}$$

Assume $1 \le t \le n-2$. If either n is odd or both n and t are even, one can see from Theorem 2.1 that $G_{n,n-t-1} \subset G_{n,t}$ and that the function in (3.8) is simply $f(XA)$. Thus in these cases, the indirect action of $G_{n,n-t-1}$ on $\mathfrak{R}_{n,t}$ is a subgroup action of $G_{n,t}$ on $\mathfrak{R}_{n,t}$. However, when n is even and t is odd, $G_{n,t} = S_n$, $G_{n,n-t-1} = \langle S_n, \Delta \rangle$ and the action of $G_{n,t}$ on $\mathfrak{R}_{n,t}$ is a subgroup action of the indirect action of $G_{n,n-t-1}$ on $\mathfrak{R}_{n,t}$. Of course, all these group actions on $\mathfrak{R}_{n,t}$ can be combined with the action of the translation subgroup $\mathbb{Z}_2^n$ on $\mathfrak{R}_{n,t}$. The following is a summary of the largest group action on $\mathfrak{R}_{n,t}$ we obtained in each case.

(i) When $0 < t \le n-2$ and t is even, $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$ acts on $\mathfrak{R}_{n,t}$:

$$\begin{aligned} \left(\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle\right) \times \mathfrak{R}_{n,t} &\longrightarrow \mathfrak{R}_{n,t} \\ \left(\begin{bmatrix} A & \\ a & 1 \end{bmatrix}, f(X) \right) &\longrightarrow f(XA + a) \end{aligned} \tag{3.12}$$

(ii) When $0 < t \le n-2$ and both n and t are odd, $\mathbb{Z}_2^n \rtimes S_n$ acts on $\mathfrak{R}_{n,t}$:

$$\begin{aligned} (\mathbb{Z}_2^n \rtimes S_n) \times \mathfrak{R}_{n,t} &\longrightarrow \mathfrak{R}_{n,t} \\ \left(\begin{bmatrix} A & \\ a & 1 \end{bmatrix}, f(X) \right) &\longrightarrow f(XA + a) \end{aligned} \tag{3.13}$$

(iii) When $0 < t \le n-2$, n is even but t is odd, $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$ acts on $\mathfrak{R}_{n,t}$:

$$\begin{aligned} \left(\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle\right) \times \mathfrak{R}_{n,t} &\longrightarrow \mathfrak{R}_{n,t} \\ \left(\begin{bmatrix} A & \\ a & 1 \end{bmatrix}, f(X) \right) &\longrightarrow f(XA + a) + X(A + I)\mathbf{1} \end{aligned} \tag{3.14}$$

The classification of $\mathfrak{R}_{n,t}$, whose meaning was not clear until now, can be defined as the classification of $\mathfrak{R}_{n,t}$ under the group actions in (3.12) – (3.14).

4 Conjugacy Classes of $\mathbb{Z}_2^n \rtimes S_n$ and $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$

We are interested in computing the number of orbits in $\mathfrak{R}_{n,t}$ $(1 \le t \le n-3)$ under the group actions in (3.12) – (3.14) using the Burnside lemma. To this end, we need representatives and sizes of the conjugacy classes of each acting group, which is either $\mathbb{Z}_2^n \rtimes S_n$ or $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta \rangle$.

In general, for any subgroup G of $\mathrm{GL}(n, \mathbb{Z}_2)$, representatives of conjugacy classes of $\mathbb{Z}_2^n \rtimes G$ can be found as follows. (We refer the reader to [5] for the details.) Let $\mathcal{A}$ be a system of representatives of conjugacy classes of G. For each $A \in \mathcal{A}$, let $\mathrm{cent}_G(A)$ be the centralizer of A in G and let $\mathrm{Row}(A+I) \subset \mathbb{Z}_2^n$ be the row space of $A+I$. Then $\mathrm{cent}_G(A)$ acts on $\mathbb{Z}_2^n/\mathrm{Row}(A+I)$. Let $\mathcal{C}_A \subset \mathbb{Z}_2^n$ such that the images of elements of $\mathcal{C}_A$ in $\mathbb{Z}_2^n/\mathrm{Row}(A+I)$ form a system of $\mathrm{cent}_G(A)$-orbit representatives. Then

$$\bigcup_{A \in \mathcal{A}} \left\{ \begin{bmatrix} A & \\ a & 1 \end{bmatrix} : a \in \mathcal{C}_A \right\} \tag{4.1}$$

form a system of representatives of conjugacy classes of $\mathbb{Z}_2^n \rtimes G$. Moreover,

$$\begin{aligned} &\left|\mathrm{cent}_{\mathbb{Z}_2^n \rtimes G}\left(\begin{bmatrix} A & \\ a & 1 \end{bmatrix}\right)\right| \\ &\quad = 2^{\mathrm{Null}(A+I)} \cdot \left|\left\{ P \in \mathrm{cent}_G(A) : aP \equiv A \pmod{\mathrm{Row}(A+I)} \right\}\right|. \end{aligned} \tag{4.2}$$

We first introduce some notation. For each partition $\lambda = (\lambda_1, \lambda_2, \cdots) \vdash n$, where $\lambda_i \geq 0$ and $\sum_{i \geq 1} i\lambda_i = n$, let

$$A(\lambda) = \big[(1) \cdots (\lambda_1)\big]\Big[(\lambda_1+1, \lambda_1+2) \cdots (\lambda_1+2\lambda_2-1, \lambda_1+2\lambda_2)\Big] \cdots \in S_n, \tag{4.3}$$

which is a canonical permutation on $\{1, \cdots, n\}$ of cycle type λ. Similarly, for each $\eta = (\eta_1, \eta_2, \cdots) \vdash n+1$, let

$$\begin{aligned} A(\eta) = {} & \big[(0) \cdots (\eta_1 - 1)\big] \\ & \cdot \Big[(\eta_1, \eta_1+1) \cdots \big(\eta_1 + 2(\eta_2-1), \eta_1 + 2(\eta_2-1)+1\big)\Big] \cdots \in S_{n+1}, \end{aligned} \tag{4.4}$$

which is a canonical permutation on $\{0, 1, \cdots, n\}$ of cycle type η. For $\eta = (\eta_1, \eta_2, \cdots) \vdash n+1$ with $\eta_1 > 0$, we define $\eta' = (\eta_1 - 1, \eta_2, \eta_3, \cdots) \vdash n$.

For $\lambda = (\lambda_1, \lambda_2, \cdots) \vdash n$ and $\alpha = (\alpha_1, \alpha_2, \cdots)$ with $0 \leq \alpha_i \leq \lambda_i$, let

$$a_\lambda(\alpha) = (a_{11}, \cdots, a_{1,\lambda_1}, a_{21}, \cdots, a_{2,\lambda_2}, \cdots) \in \mathbb{Z}_2^n \tag{4.5}$$

be any vector such that $a_{ij} \in \mathbb{Z}_2^i$ and

$$|a_{ij}| \equiv \begin{cases} 1 \pmod 2, & \text{for } 1 \leq j \leq \alpha_i, \\ 0 \pmod 2, & \text{for } \alpha_i < j \leq \lambda_i, \end{cases} \tag{4.6}$$

for all i. For $\eta = (\overbrace{0, \cdots, 0}^{m-1}, \eta_m, \eta_{m+1}, \cdots) \vdash n+1$ with $m \geq 2$ and $\eta_m > 0$, and $\beta = (\beta_m, \beta_{m+1}, \cdots)$ with $0 \leq \beta_i \leq \eta_i$, let

$$b_\eta(\beta) = (b_{m,1}, \cdots, b_{m,\eta_m}, b_{m+1,1}, \cdots, b_{m+1,\eta_{m+1}}, \cdots) \in \mathbb{Z}_2^n \tag{4.7}$$

be any vector such that $b_{m,1} \in \mathbb{Z}_2^{m-1}$, $b_{ij} \in \mathbb{Z}_2^i$ for all other (i, j), and

$$|b_{ij}| \equiv \begin{cases} 1 \pmod 2, & \text{for } 1 \leq j \leq \beta_i, \\ 0 \pmod 2, & \text{for } \beta_i < j \leq \eta_i, \end{cases} \tag{4.8}$$

for all i.

We now consider the conjugacy classes of the group $\mathbb{Z}_2^n \rtimes S_n$. Conjugacy classes of S_n are represented by $A(\lambda)$, $\lambda \vdash n$. The centralizer $\mathrm{cent}_{S_n}\big(A(\lambda)\big)$ is generated by two types of elements: a swap between the corresponding elements of two cycles of same length in $A(\lambda)$ and a cyclic shift of elements within a cycle of $A(\lambda)$. Note that for $\lambda = (\lambda_1, \lambda_2, \cdots) \vdash n$,

$$\begin{aligned} \mathrm{Row}\big(A(\lambda) + I\big) = \ & \big\{(x_{11}, \cdots, x_{1,\lambda_1}; x_{21}, \cdots, x_{2,\lambda_2}; \cdots) \\ & \in \mathbb{Z}_2^n : x_{ij} \in \mathbb{Z}_2^i,\ |x_{ij}| \text{even}\big\}. \end{aligned} \tag{4.9}$$

Hence the $\mathrm{cent}_{S_n}\big(A(\lambda)\big)$-orbits in $\mathbb{Z}_2^n/\mathrm{Row}\big(A(\lambda)+I\big)$ are represented by $a_\lambda(\alpha)$ where $\alpha = (\alpha_1, \alpha_2, \cdots)$, $0 \leq \alpha_i \leq \lambda_i$. Moreover,

$$\begin{aligned} & \Big|\big\{P \in \mathrm{cent}_{S_n}\big(A(\lambda)\big) : a_\lambda(\alpha)P \equiv a_\lambda(\alpha) \pmod{\mathrm{Row}(A(\lambda)+I)}\big\}\Big| \\ & = \prod_{i \geq 1} \big[\alpha_i!(\lambda_i - \alpha_i)! i^{\lambda_i}\big]. \end{aligned} \tag{4.10}$$

To summarize, we have the following proposition

Proposition 4.1. *The conjugacy classes of* $\mathbb{Z}_2^n \rtimes S_n$ *are represented by*

$$\left\{\begin{bmatrix} A(\lambda) & \\ a_\lambda(\alpha) & 1 \end{bmatrix} : \lambda = (\lambda_1, \lambda_2, \cdots) \vdash n,\ \alpha = (\alpha_1, \alpha_2, \cdots),\ 0 \leq \alpha_i \leq \lambda_i\right\}. \tag{4.11}$$

Moreover,

$$\left|\mathrm{cent}_{\mathbb{Z}_2^n \rtimes S_n}\left(\begin{bmatrix} A(\lambda) & \\ a_\lambda(\alpha) & 1 \end{bmatrix}\right)\right| = \prod_{i \geq 1}\big[\alpha_i!(\lambda_i - \alpha_i)!(2i)^{\lambda_i}\big]. \tag{4.12}$$

Note that (4.12) follows from (4.2), (4.10) and the fact that $\mathrm{Null}\big(A(\lambda)+I\big) = \lambda_1 + \lambda_2 + \cdots$.

Next, we consider the conjugacy classes of the group $\mathbb{Z}_2^n \rtimes \langle S_n, \Delta\rangle$. We use the isomorphism in Proposition 2.3 to identify $\langle S_n, \Delta\rangle$ with the symmetric group S_{n+1} on $\{0, 1, \cdots, n\}$. Conjugacy classes of S_{n+1} are represented by $A(\eta)$, $\eta \vdash n+1$. However, the action of $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ on $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ is not necessarily permutation of coordinates. In particular, the action of $(0, 1) \in S_{n+1}$ on $x \in \mathbb{Z}_2^n$ gives $x\Delta$. To find the representatives and sizes of $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$-orbits in $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$, we consider different types of η.

Lemma 4.2. *Assume that* $\eta = (1, \eta_2, \eta_3, \cdots) \vdash n+1$. *Then the* $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$-*orbits in* $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ *are represented by* $a_{\eta'}(\alpha)$ *where* $\alpha = (\alpha_2, \alpha_3, \cdots)$, $0 \le \alpha_i \le \eta_i$. *Furthermore,*

$$\begin{aligned}&\Big|\Big\{P \in \text{cent}_{S_{n+1}}\big(A(\eta)\big) : a_{\eta'}(\alpha)P \equiv a_{\eta'}(\alpha) \pmod{\text{Row}(A(\eta)+I)}\Big\}\Big|\\ &= \prod_{i\ge 2}\big[\alpha_i!(\eta_i-\alpha_i)!i^{\eta_i}\big]. \end{aligned} \tag{4.13}$$

Proof. In this case, $A(\eta) = A(\eta') \in S_n$ and $\text{cent}_{S_{n+1}}\big(A(\eta)\big) = \text{cent}_{S_n}\big(A(\eta')\big)$. Thus the results follow from Proposition 4.1. □

Lemma 4.3. *Assume that* $\eta = (\eta_1, \eta_2, \cdots) \vdash n+1$ *with* $\eta_1 \ge 2$. *Then the* $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$-*orbits of* $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ *are represented by* $a_{\eta'}(\alpha)$ *where* $\alpha = (\alpha_1, \alpha_2, \cdots)$, $0 \le \alpha_1 \le \eta_1 - 1$, $0 \le \alpha_i \le \eta_i$ *for* $i \ge 2$ *and the first term in* $(\alpha_i)_{i \text{ odd}}$ *not equal to* $\eta_i/2$ *is* $< \eta_i/2$, *i.e.,* $(\alpha_i)_{i\text{ odd}} \le (\eta_i/2)_{i\text{ odd}}$ *in the lexicographic order. Furthermore,*

$$\begin{aligned}&\Big|\Big\{P \in \text{cent}_{S_{n+1}}\big(A(\eta)\big) : a_{\eta'}(\alpha)P \equiv a_{\eta'}(\alpha) \pmod{\text{Row}(A(\eta)+I)}\Big\}\Big|\\ &= \begin{cases} \prod_{i\ge 1}\big[\alpha_i!(\eta_i-\alpha_i)!i^{\eta_i}\big], & \text{if } (\alpha_i)_{i\text{ odd}} \ne (\eta_i/2)_{i\text{ odd}},\\ 2\prod_{i\ge 1}\big[\alpha_i!(\eta_i-\alpha_i)!i^{\eta_i}\big], & \text{if } (\alpha_i)_{i\text{ odd}} = (\eta_i/2)_{i\text{ odd}}. \end{cases}\end{aligned} \tag{4.14}$$

Proof. In this case $A(\eta) = A(\eta') \in S_n$ but $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ is generated by $\text{cent}_{S_n}\big(A(\eta')\big)$ and $(0, 1) = \Delta$. Since

$$\begin{aligned}\text{Row}\big(A(\eta)+I\big) = \ &\{(x_{12}, \cdots, x_{1,\eta_1}; x_{21}, \cdots, x_{2,\eta_2}; \cdots)\\ &\in \mathbb{Z}_2^n : x_{ij} \in \mathbb{Z}_2^i,\ |x_{ij}| \text{ even}\},\end{aligned} \tag{4.15}$$

we have an isomorphism

$$\begin{aligned}\rho: \quad &\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big) \longrightarrow \mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}\\ &(x_{12}, \cdots, x_{1,\eta_1}; x_{21}, \cdots, x_{2,\eta_2}; \cdots) \longmapsto (|x_{12}|, \cdots, |x_{1,\eta_1}|; |x_{21}|, \cdots, |x_{2,\eta_2}|; \cdots)\end{aligned} \tag{4.16}$$

The action of $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ on $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ induces an action of $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ through the isomorphism ρ. To describe the first action, it suffices to describe the second. The induced action of an element $P \in \text{cent}_{S_{n+1}}\big(A(\eta)\big)$ on an element $\epsilon \in \mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ will be denoted by ϵ^P. The induced action of $\text{cent}_{S_n}\big(A(\eta')\big)$ on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ is easy to describe: If $\sigma \in \text{cent}_{S_n}\big(A(\eta')\big)$ is a cyclic shift within a cycle of $A(\eta')$, it acts trivially on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$; if $\sigma \in \text{cent}_{S_n}\big(A(\eta')\big)$ is a swap between two cycles of $A(\eta')$, its induced action on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ is a transposition of the two coordinates of $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ corresponding to the two cycles of $A(\eta')$. To see the action of Δ on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$, observe that for $(x_{12},\cdots,x_{1,\eta_1};x_{21},\cdots,x_{2,\eta_2};\cdots) \in \mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ $(x_{ij}\in\mathbb{Z}_2^i)$,

$$\begin{aligned}(x_{12},&\cdots,x_{1,\eta_1};x_{21},\cdots,x_{2,\eta_2};\cdots)\Delta\\ &=(x_{12},\cdots,x_{1,\eta_1};x_{21},\cdots,x_{2,\eta_2};\cdots)+|x_{12}|(0,1,\cdots,1)\\ &=(y_{12},\cdots,y_{1,\eta_1};y_{21},\cdots,y_{2,\eta_2};\cdots),\end{aligned}\tag{4.17}$$

where

$$|y_{ij}| \equiv \begin{cases}|x_{12}| \pmod 2, & \text{if } (i,j)=(1,2),\\ |x_{ij}|+i|x_{12}| \pmod 2, & \text{if } (i,j)\neq(1,2).\end{cases}\tag{4.18}$$

Hence the induced action of Δ on $(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots) \in \mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ gives

$$\begin{aligned}(\epsilon_{12},&\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)^\Delta\\ &=(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)\\ &\quad+\epsilon_{12}(0,\overbrace{1,\cdots,1}^{\eta_1-2};\overbrace{0,\cdots,0}^{\eta_2};\overbrace{1,\cdots,1}^{\eta_3};\cdots).\end{aligned}\tag{4.19}$$

From the induced action of $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ on $\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$ described above, it is clear that the $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$-orbits of $\mathbb{Z}_2^n/\text{Row}\big(A(\eta)+I\big)$ are represented by $a_{\eta'}(\alpha)$ where $\alpha=(\alpha_1,\alpha_2,\cdots)$, $0\le\alpha_1\le\eta_1-1$, $0\le\alpha_i\le\eta_i$ for $i\ge 2$ and $(\alpha_i)_{i\text{ odd}} \le (\eta_i/2)_{i\text{ odd}}$ in the lexicographic order.

To prove (4.14), observe that each element in $\text{cent}_{S_{n+1}}\big(A(\eta)\big)$ can be uniquely written in the form σ or $\Delta_k\sigma$ where $\sigma\in\text{cent}_{S_n}\big(A(\eta')\big)$, $\Delta_k=(0,k)\in S_{n+1}$ and $1\le k\le\eta_1-1$. Write $\rho\big(a_{\eta'}(\alpha)\big)=(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)\in\mathbb{Z}_2^{-1+\eta_1+\eta_2+\cdots}$. The number of $\sigma\in\text{cent}_{S_n}\big(A(\eta')\big)$ such that

$$(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)^\sigma=(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)\tag{4.20}$$

is

$$\alpha_1!(\eta_1-1-\alpha_1)!\prod_{i\ge 2}\big[\alpha_i!(\eta_i-\alpha_i)!i^{\eta_i}\big]. \tag{4.21}$$

Meanwhile, $\rho\big(a_{\eta'}(\alpha)\big)^{\Delta_k\sigma}=\rho\big(a_{\eta'}(\alpha)\big)$ if and only if

$$\begin{aligned}&(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)^{\sigma^{-1}}\\ &\quad=(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)^{\Delta_k}\\ &\quad=(\epsilon_{12},\cdots,\epsilon_{1,\eta_1};\epsilon_{21},\cdots,\epsilon_{2,\eta_2};\cdots)\\ &\qquad+\epsilon_{1,k+1}(\overbrace{\underbrace{1,\cdots,1,0}_{k},1,\cdots,1}^{\eta_1-1};\overbrace{0,\cdots,0}^{\eta_2};\overbrace{1,\cdots,1}^{\eta_3};\cdots).\end{aligned} \tag{4.22}$$

(The last equality in (4.22) follows from the proof of (4.19).) When $(\alpha_1,\alpha_3,\alpha_5,\cdots)\ne(\eta_1/2,\eta_3/2,\eta_5/2,\cdots)$, (4.22) holds only if $\epsilon_{1,k+1}=0$, i.e., $\alpha_1+1\le k\le\eta_1-1$. For each such k, the number of $\sigma\in\mathrm{cent}_{S_n}\big(A(\eta')\big)$ satisfying (4.22) is given by (4.21). When $(\alpha_1,\alpha_3,\alpha_5,\cdots)=(\eta_1/2,\eta_3/2,\eta_5/2,\cdots)$, for each $1\le k\le\eta_1-1$, the number of $\sigma\in\mathrm{cent}_{S_n}\big(A(\eta')\big)$ satisfying (4.22) is given by (4.21). From these observations, we have the total number of $P\in\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$ such that $\rho\big(a_{\eta'}(\alpha)\big)^P=\rho\big(a_{\eta'}(\alpha)\big)$, i.e., $a_{\eta'}(\alpha)P\equiv a_{\eta'}(\alpha)$ (mod $\mathrm{Row}(A(\eta)+I)$). □

Lemma 4.4. *Assume that* $\eta=(\overbrace{0,\cdots,0}^{m-1},\eta_m,\eta_{m+1},\cdots)\vdash n+1$ *with* $m\ge 2$ *and* $\eta_m>0$. *Then the* $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$*-orbits of* $\mathbb{Z}_2^n/\mathrm{Row}\big(A(\eta)+I\big)$ *are represented by* $b_\eta(\beta)$*, defined in (4.7), where* $\beta=(\beta_m,\beta_{m+1},\cdots)$, $0\le\beta_i\le\eta_i$ *and* $(\beta_i)_{i\,\mathrm{odd}}\le(\eta_i/2)_{i\,\mathrm{odd}}$ *in the lexicographic order. Furthermore,*

$$\begin{aligned}&\Big|\Big\{P\in\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big):b_\eta(\beta)P\equiv b_\eta(\beta)\pmod{\mathrm{Row}(A(\eta)+I)}\Big\}\Big|\\ &\quad=\begin{cases}\displaystyle\prod_{i\ge m}\big[\beta_i!(\eta_i-\beta_i)!i^{\eta_i}\big], & \text{if } \sum_{i\,\mathrm{odd}}\eta_i=0 \text{ or } (\beta_i)_{i\,\mathrm{odd}}\ne(\eta_i/2)_{i\,\mathrm{odd}},\\ \displaystyle 2\prod_{i\ge m}\big[\beta_i!(\eta_i-\beta_i)!i^{\eta_i}\big], & \text{if } \sum_{i\,\mathrm{odd}}\eta_i>0 \text{ and } (\beta_i)_{i\,\mathrm{odd}}=(\eta_i/2)_{i\,\mathrm{odd}}.\end{cases}\end{aligned} \tag{4.23}$$

Proof. Since $A(\eta)=(0,1,\cdots,m-1)(m,\cdots)\cdots=(0,1)(1,\cdots,m-1)(m,\cdots,)\cdots=\Delta(1,\cdots,m-1)(m,\cdots)\cdots$, we see that

$$\begin{aligned}&\mathrm{Row}\big(A(\eta)+I\big)\\ &\quad=\Big\{(x_{m,1},\cdots,x_{m,\eta_m};x_{m+1,1},\cdots,x_{m+1,\eta_{m+1}};\cdots)\in\mathbb{Z}_2^n:\\ &\quad\quad x_{m,1}\in\mathbb{Z}_2^{m-1},\ x_{ij}\in\mathbb{Z}_2^i\text{ for all other }(i,j),\ |x_{ij}|\text{ even for all }(i,j)\Big\}\\ &\quad\quad+\langle(0,1,\cdots,1)\rangle.\end{aligned} \tag{4.24}$$

Thus there is an isomorphism

$$\begin{aligned}\rho :&\mathbb{Z}_2^n/\mathrm{Row}\big(A(\eta)+I\big) \longrightarrow \mathbb{Z}_2^{\eta_m+\eta_{m+1}+\cdots}/\langle(\overbrace{m,\cdots,m}^{\eta_m};\overbrace{m+1,\cdots,m+1}^{\eta_{m+1}};\cdots)\rangle\\ &(x_{m1},\cdots,x_{m,\eta_m};x_{m+1,1},\cdots,x_{m+1,\eta_{m+1}};\cdots)\\ &\longmapsto (|x_{m1}|,\cdots,|x_{m,\eta_m}|;|x_{m+1,1}|,\cdots,|x_{m+1,\eta_{m+1}}|;\cdots)\end{aligned} \tag{4.25}$$

We use $H(\eta)$ to denote the target space of ρ. The $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$-action on $\mathbb{Z}_2^n/\mathrm{Row}\big(A(\eta)+I\big)$ induces a $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$-action on $H(\eta)$ through the isomorphism ρ. The induced action can be described as follows: If $P \in \mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$ is a cyclic shift within a cycle of $A(\eta)$, P acts trivially on $H(\eta)$; if $P \in \mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$ is a swap between two cycles of the same length in $A(\eta)$, the action of P on $H(\eta)$ is a transposition of the two coordinates of $H(\eta)$ corresponding to the two cycles of $A(\eta)$. We omit the proofs of these claims since they are routine computations. Using the induced action of $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$ on $H(\eta)$, it is clear that the $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$-orbits of $\mathbb{Z}_2^n/\mathrm{Row}\big(A(\eta)+I\big)$ are represented by $b_\eta(\beta)$ where $\beta=(\beta_m,\beta_{m+1},\cdots)$, $0\le\beta_i\le\eta_i$ and $(\beta_i)_{i\text{ odd}}\le(\eta_i/2)_{i\text{ odd}}$ in the lexicographic order. Equation (4.23) also follows easily from the induced $\mathrm{cent}_{S_{n+1}}\big(A(\eta)\big)$-action on $H(\eta)$. □

Combining Lemmas 4.2 – 4.4 and using (4.2), we have the following proposition.

Proposition 4.5. *The representatives of the conjugacy classes of* $\mathbb{Z}_2^n \rtimes \langle S_n,\Delta\rangle$ *and the sizes of the centralizers of the representatives are as follows:*

(i) $$\begin{bmatrix} A(\eta) & \\ a_{\eta'}(\alpha) & 1\end{bmatrix},\ \eta=(1,\eta_2,\eta_3,\cdots)\vdash n+1,\ \alpha=(\alpha_2,\alpha_3,\cdots),\quad 0\le\alpha_i\le\eta_i, \tag{4.26}$$

$$\left|\mathrm{cent}_{\mathbb{Z}_2^n\rtimes\langle S_n,\Delta\rangle}\left(\begin{bmatrix} A(\eta) & \\ a_{\eta'}(\alpha) & 1\end{bmatrix}\right)\right| = \prod_{i\ge 2}\big[\alpha_i!(\eta_i-\alpha_i)!(2i)^{\eta_i}\big]. \tag{4.27}$$

(ii) $$\begin{bmatrix} A(\eta) & \\ a_{\eta'}(\alpha) & 1\end{bmatrix},\ \eta=(\eta_1,\eta_2,\cdots)\vdash n+1,\ \eta_1\ge 2,$$
$$\alpha=(\alpha_1,\alpha_2,\cdots),\ 0\le\alpha_1\le\eta_1-1,\ 0\le\alpha_i\le\eta_i \textit{ for } i\ge 2,$$
$$(\alpha_i)_{i\text{ odd}}\le(\eta_i/2)_{i\text{ odd}} \textit{ in the lexicographic order,} \tag{4.28}$$

$$\left|\mathrm{cent}_{\mathbb{Z}_2^n \rtimes \langle S_n, \Delta\rangle}\left(\begin{bmatrix} A(\eta) & \\ a_{\eta'}(\alpha) & 1 \end{bmatrix}\right)\right| = \begin{cases} \frac{1}{2}\prod_{i\ge 1}\big[\alpha_i!(\eta_i-\alpha_i)!(2i)^{\eta_i}\big], & \textit{if } (\alpha_i)_{i \text{ odd}} \ne (\eta_i/2)_{i \text{ odd}}, \\ \prod_{i\ge 1}\big[\alpha_i!(\eta_i-\alpha_i)!(2i)^{\eta_i}\big], & \textit{if } (\alpha_i)_{i \text{ odd}} = (\eta_i/2)_{i \text{ odd}}. \end{cases} \tag{4.29}$$

(iii) $\begin{bmatrix} A(\eta) & \\ b_\eta(\beta) & 1 \end{bmatrix}$, $\eta = (\overbrace{0,\cdots,0}^{m-1}, \eta_m, \eta_{m+1}, \cdots) \vdash n+1,\ m \ge 2,\ \eta_m > 0,$

$$\beta = (\beta_m, \beta_{m+1}, \cdots),\ 0 \le \beta_i \le \eta_i, \\ (\beta_i)_{i \text{ odd}} \le (\eta_i/2)_{i \text{ odd}} \textit{ in the lexicographic order,} \tag{4.30}$$

$$\left|\mathrm{cent}_{\mathbb{Z}_2^n \rtimes \langle S_n, \Delta\rangle}\left(\begin{bmatrix} A(\eta) & \\ b_\eta(\beta) & 1 \end{bmatrix}\right)\right| = \begin{cases} \frac{1}{2}\prod_{i\ge m}\big[\beta_i!(\eta_i-\beta_i)!(2i)^{\eta_i}\big], & \textit{if } (\beta_i)_{i \text{ odd}} \ne (\eta_i/2)_{i \text{ odd}}, \\ \prod_{i\ge m}\big[\beta_i!(\eta_i-\beta_i)!(2i)^{\eta_i}\big], & \textit{if } (\beta_i)_{i \text{ odd}} = (\eta_i/2)_{i \text{ odd}}. \end{cases} \tag{4.31}$$

In order to obtain (4.31) in Case (iii) in Proposition 4.5, we used the fact that

$$\mathrm{Null}\big(A(\eta)+I\big) = \begin{cases} -1+\eta_m+\eta_{m+1}+\cdots, & \text{if } \sum_{i \text{ odd}} \eta_i > 0, \\ \eta_m+\eta_{m+1}+\cdots, & \text{if } \sum_{i \text{ odd}} \eta_i = 0. \end{cases} \tag{4.32}$$

5 Numbers of Orbits in $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$

Using Propositions 4.1 and 4.5, we are able to compute the numbers of $\mathbb{Z}_2^5 \rtimes S_5$-orbits in $\mathfrak{R}_{5,1}$ and the $\mathbb{Z}_2^6 \rtimes \langle S_6, \Delta\rangle$-orbits in $\mathfrak{R}_{6,2}$ with a computer. The results are given in the following tables. When searching through elements in $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$, we used an obvious reductive property of resilient functions to reduce the amount of computation: If $F(X_1,\cdots,X_n) = f(X_1,\cdots,X_{n-1}) + X_n g(X_1,\cdots,X_{n-1}) \in \mathfrak{R}_{n,t}$, then $f(X_1,\cdots,X_{n-1}) \in \mathfrak{R}_{n-1,t-1}$.

Now that the numbers of orbits in $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$ are known to be 256 and 131, the problem of classifying $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$ becomes finding the right number of elements in $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$ that are pairwise nonequivalent under the group actions. Using a reasonable amount of computer time, we have found the orbit representatives in $\mathfrak{R}_{5,1}$ and $\mathfrak{R}_{6,2}$, but the results are too lengthy to be included in the paper.

Table 1. $\mathbb{Z}_2^5 \rtimes S_5$ acting on $\mathfrak{R}_{5,1}$

$\sigma = \begin{bmatrix} A(\lambda) & \\ a & 1 \end{bmatrix}$: representatives of conj. classes of $\mathbb{Z}_2^5 \rtimes S_5$		$\lvert \mathrm{cent}_{\mathbb{Z}_2^5 \rtimes S_5}(\sigma) \rvert$	$\lvert \{f \in \mathfrak{R}_{5,1} : \sigma(f) = f\} \rvert$
λ	a		
(5)	(0 0 0 0 0)	$5!2^5$	403,990
	(1 0 0 0 0)	$4!2^5$	6,546
	(1 1 0 0 0)	$2!3!2^5$	2,774
	(1 1 1 0 0)	$2!3!2^5$	1,810
	(1 1 1 1 0)	$4!2^5$	2,774
	(1 1 1 1 1)	$5!2^5$	6,546
(3,1)	(0 0 0 0 0)	$3!2^5$	3,436
	(0 0 0 1 0)	$3!2^5$	132
	(1 0 0 0 0)	$2!2^5$	1,932
	(1 0 0 1 0)	$2!2^5$	44
	(1 1 0 0 0)	$2!2^5$	1,260
	(1 1 0 1 0)	$2!2^5$	36
	(1 1 1 0 0)	$3!2^5$	1,932
	(1 1 1 1 0)	$3!2^5$	44
(2,0,1)	(0 0 0 0 0)	$2!2^3 \cdot 3$	49
	(0 0 1 0 0)	$2!2^3 \cdot 3$	37
	(1 0 0 0 0)	$2^3 \cdot 3$	21
	(1 0 1 0 0)	$2^3 \cdot 3$	17
	(1 1 0 0 0)	$2!2^3 \cdot 3$	17
	(1 1 1 0 0)	$2!2^3 \cdot 3$	21
(1,2)	(0 0 0 0 0)	$2!2^5$	978
	(0 1 0 0 0)	2^5	54
	(0 1 0 1 0)	$2!2^5$	146
	(1 0 0 0 0)	$2!2^5$	870
	(1 1 0 0 0)	2^5	26
	(1 1 0 1 0)	$2!2^5$	70
(1,0,0,1)	(0 0 0 0 0)	2^4	6
	(0 1 0 0 0)	2^4	10
	(1 0 0 0 0)	2^4	42
	(1 1 0 0 0)	2^4	6
(0,1,1)	(0 0 0 0 0)	$2^3 \cdot 3$	13
	(0 0 1 0 0)	$2^3 \cdot 3$	9
	(1 0 0 0 0)	$2^3 \cdot 3$	9
	(1 0 1 0 0)	$2^3 \cdot 3$	5
(0,0,0,0,1)	(0 0 0 0 0)	$2 \cdot 5$	5
	(1 0 0 0 0)	$2 \cdot 5$	1

Number of $\mathbb{Z}_2^5 \rtimes S_5$-orbits in $\mathfrak{R}_{5,1} = 256$

Table 2. $\mathbb{Z}_2^6 \rtimes \langle S_6, \Delta \rangle$ acting on $\mathfrak{R}_{6,2}$

$\sigma = \left[\begin{smallmatrix} A(\eta) & \\ a & 1 \end{smallmatrix}\right]$: representatives of conj. classes of $\mathbb{Z}_2^6 \rtimes \langle S_6, \Delta \rangle$		$\lvert \mathrm{cent}_{\mathbb{Z}_2^5 \rtimes \langle S_6, \Delta \rangle}(\sigma) \rvert$	$\lvert \{ f \in \mathfrak{R}_{6,2} : \sigma(f) = f \} \rvert$
η	a		
(7)	(0 0 0 0 0 0)	$7!2^6$	8,375,430
	(1 0 0 0 0 0)	$6!2^6$	404,266
	(1 1 0 0 0 0)	$2!5!2^6$	32,482
	(1 1 1 0 0 0)	$3!4!2^6$	30,446
(5,1)	(0 0 0 0 0 0)	$5!2^6$	31,030
	(0 0 0 0 1 0)	$5!2^6$	6,440
	(1 0 0 0 0 0)	$4!2^6$	17,726
	(1 0 0 0 1 0)	$4!2^6$	240
	(1 1 0 0 0 0)	$2!3!2^6$	9,410
	(1 1 0 0 1 0)	$2!3!2^6$	276
(4,0,1)	(0 0 0 0 0 0)	$4!2^4 \cdot 3$	342
	(0 0 0 1 0 0)	$4!2^4 \cdot 3$	326
	(1 0 0 0 0 0)	$3!2^4 \cdot 3$	58
	(1 0 0 1 0 0)	$3!2^4 \cdot 3$	50
	(1 1 0 0 0 0)	$2!2!2^4 \cdot 3$	46
(3,2)	(0 0 0 0 0 0)	$3!2!2^6$	4,862
	(0 0 1 0 0 0)	$3!2^6$	412
	(0 0 1 0 1 0)	$3!2!2^6$	722
	(1 0 0 0 0 0)	$2!2!2^6$	7,130
	(1 0 1 0 0 0)	$2!2^6$	200
	(1 0 1 0 1 0)	$2!2!2^6$	398
(3,0,0,1)	(0 0 0 0 0 0)	$3!2^5$	14
	(0 0 1 0 0 0)	$3!2^5$	38
	(1 0 0 0 0 0)	$2!2^5$	106
	(1 0 1 0 0 0)	$2!2^5$	18
(2,1,1)	(0 0 0 0 0 0)	$2!2^4 \cdot 3$	64
	(0 0 0 1 0 0)	$2!2^4 \cdot 3$	56
	(0 1 0 0 0 0)	$2!2^4 \cdot 3$	20
	(0 1 0 1 0 0)	$2!2^4 \cdot 3$	12
	(1 0 0 0 0 0)	$2^4 \cdot 3$	32
	(1 1 0 0 0 0)	$2^4 \cdot 3$	12
(2,0,0,0,1)	(0 0 0 0 0 0)	$2!2^2 \cdot 5$	10
	(0 1 0 0 0 0)	$2!2^2 \cdot 5$	2
	(1 0 0 0 0 0)	$2^2 \cdot 5$	6
(1,3)	(0 0 0 0 0 0)	$3!2^6$	1,054
	(1 0 0 0 0 0)	$2!2^6$	136
	(1 0 1 0 0 0)	$2!2^6$	306
	(1 0 1 0 1 0)	$3!2^6$	28
(1,1,0,1)	(0 0 0 0 0 0)	2^5	6
	(0 0 1 0 0 0)	2^5	18
	(1 0 0 0 0 0)	2^5	48
	(1 0 1 0 0 0)	2^5	36

Table 2 (Continued)

$\sigma = \left[\begin{smallmatrix} A(\eta) & \\ a & 1 \end{smallmatrix}\right]$: representatives of conj. classes of $\mathbb{Z}_2^6 \rtimes \langle S_6, \Delta\rangle$		$\lvert \mathrm{cent}_{\mathbb{Z}_2^5 \rtimes \langle S_6, \Delta\rangle}(\sigma)\rvert$	$\lvert\{f \in \mathfrak{R}_{6,2} : \sigma(f) = f\}\rvert$
η	a		
(1,0,2)	(0 0 0 0 0 0)	$2!2^2 3^2$	249
	(1 0 0 0 0 0)	$2^2 3^2$	35
	(1 0 0 1 0 0)	$2!2^2 3^2$	85
(1,0,0,0,0,1)	(0 0 0 0 0 0)	$2^2 \cdot 3$	1
	(1 0 0 0 0 0)	$2^2 \cdot 3$	1
(0,2,1)	(0 0 0 0 0 0)	$2!2^4 \cdot 3$	2
	(1 0 0 0 0 0)	$2^4 \cdot 3$	10
	(1 1 0 0 0 0)	$2!2^4 \cdot 3$	2
(0,1,0,0,1)	(0 0 0 0 0 0)	$2^2 \cdot 5$	0
	(1 0 0 0 0 0)	$2^2 \cdot 5$	0
(0,0,1,1)	(0 0 0 0 0 0)	$2^3 \cdot 3$	2
	(0 0 1 0 0 0)	$2^3 \cdot 3$	2
(0,0,0,0,0,0,1)	(0 0 0 0 0 0)	7	0
Number of $\mathbb{Z}_2^6 \rtimes \langle S_6, \Delta\rangle$-orbits in $\mathfrak{R}_{6,2} = 131$			

References

1. Bennett, C.H., Brassard, G., Robert, J.-M.: Privacy amplification by public discussion. SIAM J. Computing **17**, 210–229 (1988)
2. Camion, P., Carlet, C., Charpin, P., Sendrier, N.: *On correlation-immune functions*. Lecture Notes in Comput. Sci. **576**, New York: Springer-Verlag, 1992, pp. 86–100
3. Chor, B., Goldreich, O., Hastad, J., Freidmann, J., Rudich, S., Smolensky, R.: The bit extraction problem or t-resilient functions. Proc. 26th IEEE Symposium on Fundations of Computer Science 396–407 (1985)
4. Hou, X.: On binary resilient functions. Des. Codes Cryptogr. **28**, 93–112 (2003)
5. Hou, X.: $AGL(m, 2)$ acting on $R(r, m)/R(s, m)$. J. Algebra **171**, 921–938 (1995)
6. Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory **30**, 776–780 (1984)