Counting Toroidal Binary Arrays, II

S. N. Ethier\textsuperscript{1}
Department of Mathematics
University of Utah
155 South 1400 East
Salt Lake City, UT 84112
USA
ethier@math.utah.edu

Jiyeon Lee\textsuperscript{2}
Department of Statistics
Yeungnam University
214-1 Daedong, Kyeongsan
Kyeongbuk 712-749
South Korea
leejy@yu.ac.kr

Abstract

We derive formulas for (i) the number of distinct toroidal $n \times n$ binary arrays, allowing rotation of rows and/or columns as well as matrix transposition, and (ii) the number of distinct toroidal $n \times n$ binary arrays, allowing rotation and/or reflection of rows and/or columns as well as matrix transposition.

\textsuperscript{1}Partially supported by a grant from the Simons Foundation (209632).
\textsuperscript{2}Supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. 2013R1A1A3A04007670).
1 Introduction

A previous paper \[1\] found the number of (distinct) toroidal \(m \times n\) binary arrays, allowing rotation of rows and/or columns, to be

\[
a(m, n) := \frac{1}{mn} \sum_{c \mid m} \sum_{d \mid n} \phi(c)\phi(d) 2^{mn/\text{lcm}(c,d)},
\]

where \(\phi\) is Euler’s phi function and \text{lcm} stands for least common multiple. This is \(A184271\) in the On-Line Encyclopedia of Integer Sequences \[2\]. The main diagonal is \(A179043\). It was also shown that, allowing rotation and/or reflection of rows and/or columns, the number becomes

\[
b(m, n) := b_1(m, n) + b_3(m, n) + b_2(m, n) + b_4(m, n),
\]

where

\[
b_1(m, n) := \frac{1}{4mn} \sum_{c \mid m} \sum_{d \mid n} \phi(c)\phi(d) 2^{mn/\text{lcm}(c,d)},
\]

\[
b_2(m, n) := \frac{1}{4n} \sum_{d \mid n} \phi(d) 2^{mn/d}
\]

\[\begin{cases}
  (4n)^{-1} \sum' \phi(d)(2^{(m+1)n/(2d)} - 2^{mn/d}), & \text{if } m \text{ is odd;}
  (8n)^{-1} \sum' \phi(d)(2^{mn/(2d)} + 2^{(m+2)n/(2d)} - 2 \cdot 2^{mn/d}), & \text{if } m \text{ is even,}
\end{cases}\]

with \(\sum' := \sum_{d \mid n}: d \text{ is odd}\),

\[
b_3(m, n) := b_2(n, m),
\]

and

\[
b_4(m, n) := \begin{cases}
  2^{(mn-3)/2}, & \text{if } m \text{ and } n \text{ are odd;}
  3 \cdot 2^{mn/2-3}, & \text{if } m \text{ and } n \text{ have opposite parity;}
  7 \cdot 2^{mn/2-4}, & \text{if } m \text{ and } n \text{ are even.}
\end{cases}
\]

(The formula for \(b_2(m, n)\) given in \[1\] is simplified here.) This is \(A222188\) in the OEIS \[2\]. The main diagonal is \(A209251\).

Our aim here is to derive the corresponding formulas when \(m = n\) and we allow matrix transposition as well. More precisely, we show that the number of (distinct) toroidal \(n \times n\) binary arrays, allowing rotation of rows and/or columns as well as matrix transposition, is

\[
\alpha(n) = \frac{1}{2} a(n, n) + \frac{1}{2n} \sum_{d \mid n} \phi(d) 2^{n(n+d-2[d/2])/(2d)},
\]

where \(a(n, n)\) is from (1). When we allow rotation and/or reflection of rows and/or columns as well as matrix transposition, the number becomes

\[
\beta(n) = \frac{1}{2} b(n, n) + \frac{1}{4n} \sum_{d \mid n} \phi(d) 2^{n(n+d-2[d/2])/(2d)} + \begin{cases}
  2^{(n^2-5)/4}, & \text{if } n \text{ is odd;}
  5 \cdot 2^{n^2/4-3}, & \text{if } n \text{ is even,}
\end{cases}
\]
where \( b(n,n) \) is from (2). These are the sequences \( \text{A255015} \) and \( \text{A255016} \), respectively, recently added to the OEIS [2].

For an alternative description, we could define a group action on the set of \( n \times n \) binary arrays, which has \( 2^{n^2} \) elements. If the group is generated by \( \sigma \) (row rotation) and \( \tau \) (column rotation), then the number of orbits is given by \( a(n,n) \); see [1]. If the group is generated by \( \sigma, \tau, \) and \( \zeta \) (matrix transposition), then the number of orbits is given by \( \alpha(n) \); see Theorem 1 below. If the group is generated by \( \sigma, \tau, \rho \) (row reflection), and \( \theta \) (column reflection), then the number of orbits is given by \( b(n,n) \); see [1]. If the group is generated by \( \sigma, \tau, \rho, \theta, \) and \( \zeta \), then the number of orbits is given by \( \beta(n) \); see Theorem 2 below.

Both theorems are proved using Pólya’s enumeration theorem (actually, the simplified unweighted version; see, e.g., van Lint and Wilson [3, Theorem 37.1, p. 524]).

To help clarify the distinction between the various group actions, we consider the case of \( 3 \times 3 \) binary arrays as in [1]. When the group is generated by \( \sigma \) and \( \tau \) (allowing rotation of rows and/or columns), there are 64 orbits, which were listed in [1]. When the group is generated by \( \sigma, \tau, \) and \( \zeta \) (allowing rotation of rows and/or columns as well as matrix transposition), there are 44 orbits, which are listed in Table 1 below. When the group is generated by \( \sigma, \tau, \rho, \) and \( \theta \) (allowing rotation and/or reflection of rows and/or columns), there are 36 orbits, which were listed in [1]. When the group is generated by \( \sigma, \tau, \rho, \theta, \) and \( \zeta \) (allowing rotation and/or reflection of rows and/or columns as well as matrix transposition), there are 26 orbits, which are listed in Table 2 below.

Table 3 provides numerical values for \( \alpha(n) \) and \( \beta(n) \) for small \( n \).

We take this opportunity to correct a small gap in the proof of Theorem 2 in [1]. The proof assumed implicitly that \( m, n \geq 3 \). The theorem is correct as stated for \( m, n \geq 1 \), so the proof is incomplete if \( m \) or \( n \) is 1 or 2. Following the proof of Theorem 2 below, we supply the missing steps.

## 2 Rotation of rows and columns, and matrix transposition

Let \( X_n := \{0,1\}^{(0,1,\ldots,n-1)^2} \) be the set of \( n \times n \) matrices of 0s and 1s, which has \( 2^{n^2} \) elements. Let \( \alpha(n) \) denote the number of orbits of the group action on \( X_n \) by the group of order \( 2n^2 \) generated by \( \sigma \) (row rotation), \( \tau \) (column rotation), and \( \zeta \) (matrix transposition). (Exception: If \( n = 1 \), the group is of order 1.)

Informally, \( \alpha(n) \) is the number of (distinct) toroidal \( n \times n \) binary arrays, allowing rotation of rows and/or columns as well as matrix transposition.

**Theorem 1.** With \( a(n,n) \) defined using (1), \( \alpha(n) \) is given by (3).

**Proof.** Let us assume that \( n \geq 2 \). By Pólya’s enumeration theorem,

\[
\alpha(n) = \frac{1}{2n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (2^{A_{ij}} + 2^{E_{ij}}),
\]  

(5)
Each orbit is represented by its minimal element in 9-bit binary form. Subscripts indicate orbit size. Bars separate different numbers of 1s.

Table 1: A list of the 44 orbits of the group action in which the group generated by $\sigma$, $\tau$, and $\zeta$ acts on the set of $3 \times 3$ binary arrays. (Rows and/or columns can be rotated and matrices can be transposed.) Each orbit is represented by its minimal element in 9-bit binary form. Subscripts indicate orbit size.

where $A_{ij}$ (resp., $E_{ij}$) is the number of cycles in the permutation $\sigma^i\tau^j$ (resp., $\sigma^i\tau^j\zeta$); here $\sigma$ rotates the rows (row 0 becomes row 1, row 1 becomes row 2, ..., row $n - 1$ becomes row 0), $\tau$ rotates the columns, and $\zeta$ transposes the matrix. We know from [1] that

$$a(n, n) = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{A_{ij}},$$

so it remains to find $E_{ij}$. The permutation $\zeta$ has $n$ fixed points and $\binom{n}{2}$ transpositions, so $E_{00} = n(n+1)/2$.

Notice that $\sigma$ and $\tau$ commute, whereas $\sigma \zeta = \zeta \tau$ and $\tau \zeta = \zeta \sigma$. Let $(i, j) \in \{0, 1, \ldots, n - \ldots$
Table 2: A list of the 26 orbits of the group action in which the group generated by $\sigma$, $\tau$, $\rho$, $\theta$, and $\zeta$ acts on the set of $3 \times 3$ binary arrays. (Rows and/or columns can be rotated and/or reflected and matrices can be transposed.) Each orbit is represented by its minimal element in 9-bit binary form. Subscripts indicate orbit size. Bars separate different numbers of 1s.

$$
\begin{array}{cccccccc}
0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 \\
0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 \\
0 & 0 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 \\
1 & 1 & 0 & | & 1 & 1 & 0 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 \\
0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 & | & 0 & 0 & 0 \\
0 & 1 & 1 & | & 0 & 1 & 0 & | & 0 & 1 & 0 & | & 0 & 1 & 0 & | & 0 & 1 & 0 \\
1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 \\
0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 \\
1 & 1 & 1 & | & 1 & 1 & 0 & | & 1 & 1 & 0 & | & 1 & 1 & 0 & | & 1 & 1 & 0 \\
1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 \\
0 & 0 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 & | & 0 & 1 & 1 \\
0 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 \\
0 & 0 & 1 & | & 0 & 0 & 1 & | & 0 & 0 & 1 & | & 0 & 0 & 1 & | & 0 & 0 & 1 \\
0 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 \\
1 & 1 & 1 & | & 1 & 1 & 0 & | & 1 & 1 & 0 & | & 1 & 1 & 0 & | & 1 & 1 & 0 \\
1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 & | & 1 & 1 & 1 \\
\end{array}
$$

Table 3: The values of $\alpha(n)$ and $\beta(n)$ for $n = 1, 2, \ldots, 12$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\alpha(n)$</th>
<th>$\beta(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>44</td>
<td>26</td>
</tr>
<tr>
<td>4</td>
<td>2209</td>
<td>805</td>
</tr>
<tr>
<td>5</td>
<td>674384</td>
<td>172112</td>
</tr>
<tr>
<td>6</td>
<td>954623404</td>
<td>239123150</td>
</tr>
<tr>
<td>7</td>
<td>5744406453840</td>
<td>143612019028</td>
</tr>
<tr>
<td>8</td>
<td>144115192471496836</td>
<td>36028817512382026</td>
</tr>
<tr>
<td>9</td>
<td>14925010120653819583840</td>
<td>373125251904348833632</td>
</tr>
<tr>
<td>10</td>
<td>6338253001142965335834871200</td>
<td>1584563250300891724601506272</td>
</tr>
<tr>
<td>11</td>
<td>109853553706542379117501389992368</td>
<td>2746338834266358751489231123956672</td>
</tr>
<tr>
<td>12</td>
<td>77433143050453552587418968170813573149024</td>
<td>19355825762613388352671214587818634041520</td>
</tr>
</tbody>
</table>

$1)^2 - \{(0, 0)\}$ be arbitrary. Then

$$(\sigma^i \tau^j \zeta)^2 = (\sigma^i \tau^j \zeta)(\zeta \tau^i \sigma^j) = \sigma^{i+j} \tau^{i+j},$$
not a multiple of $n$ fixed point of $(n$). This shows that there are
\[\sigma^i \tau^j \zeta \nexists\]
 facts that, in the cyclic group $\{a, a^2, \ldots, a^{n-1}, a^n = e\}$ of order $n$, $a^k$ is of order $n/\gcd(k, n)$, we find that the permutation $\sigma^i \tau^j \zeta$ is of order $2d$, where $d := n/\gcd(i + j, n)$. Therefore, every cycle of this permutation must have length that divides $2d$.

We claim that all cycles have length $d$ or $2d$. Accepting that for now, let us determine how many cycles have length $d$. A cycle that includes entry $(k, l)$ has length $d$ if $(k, l)$ is a fixed point of $(\sigma^i \tau^j \zeta)^d$. For this to hold we must have $d$ odd (otherwise there would be no fixed points because we have excluded the case $i = j = 0$ and $(i + j)d/2 = \text{lcm}(i + j, n)/2$ is not a multiple of $n$). Since

\[(\sigma^i \tau^j \zeta)^d = \sigma^{(i+j)(d-1)/2 + i} \tau^{(i+j)(d-1)/2 + j} \zeta,
\]
we must also have

\[(k, l) = ([l + (i + j)(d - 1)/2 + j], [k + (i + j)(d - 1)/2 + i]),
\]
where $d := n/\gcd(i + j, n)$ and, for simplicity, $[r] := (r \mod n) \in \{0, 1, \ldots, n - 1\}$. For each $k \in \{0, 1, \ldots, n - 1\}$, there is a unique $l$ (namely, $l := [k + (i + j)(d - 1)/2 + i]$) such that (7) holds; indeed,

\[
[l + (i + j)(d - 1)/2 + j] = [k + (i + j)(d - 1)/2 + i] + (i + j)(d - 1)/2 + j
\]

\[
= [k + (i + j)(d - 1)/2 + i + (i + j)(d - 1)/2 + j]
\]

\[
= [k + (i + j)d]
\]

\[
= [k + (i + j)(n/\gcd(i + j, n))]
\]

\[
= [k + \text{lcm}(i + j, n)]
\]

\[
k.
\]

This shows that there are $n$ fixed points of $(\sigma^i \tau^j \zeta)^d$. Each cycle of length $d$ of $\sigma^i \tau^j \zeta$ will account for $d$ such fixed points, hence there are $n/d$ such cycles. All remaining cycles will have length $2d$, and so there are $n(n - 1)/(2d)$ of these. The total number of cycles is therefore $n(n + 1)/(2d)$.

The other possibility is that $d$ is even and all cycles have the same length, $2d$, so there are $n^2/(2d)$ of them. Notice that $d$ is a divisor of $n$, so the contribution to

\[
\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2E_{ij}
\]

6
from odd $d$ is
\[
\sum_{d \mid n: \text{ } d \text{ is odd}} n\varphi(d)2^{n(n+1)/(2d)}
\]
and from even $d$ is
\[
\sum_{d \mid n: \text{ } d \text{ is even}} n\varphi(d)2^{n^2/(2d)}.
\]
The reason for the coefficient $n\varphi(d)$ is that, if $d \mid n$, then the number of elements of the cyclic group $\{e, \sigma, (\sigma\tau)^2, \ldots, (\sigma\tau)^{n-1}\}$ that are of order $d$ is $\varphi(d)$. And for a given $(i, j) \in \{0, 1, \ldots, n-1\}^2$, there are $n$ pairs $(k, l) \in \{0, 1, \ldots, n-1\}^2$ such that $[k + l] = [i + j]$. Putting (8) and (9) together, we obtain
\[
\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2E_{ij} = \sum_{d \mid n} n\varphi(d)2^{n(n+d-2[d/2])/(2d)},
\]
which, together with (5) and (6), yields (3).

It remains to prove our claim that, for $(i, j) \in \{0, 1, \ldots, n-1\}^2-\{(0, 0)\}$, the permutation $\sigma^i\tau^j\varsigma$ cannot have any cycles whose length is a proper divisor of $d := n/\gcd(i+j, n)$. Let $c \mid d$ with $1 \leq c < d$. We must show that $(\sigma^i\tau^j\varsigma)^c$ has no fixed points. We can argue as above with $c$ in place of $d$. For $(k, l)$ to be a fixed point of $(\sigma^i\tau^j\varsigma)^c$ we must have $(i+j)c$ a multiple of $n$. But $d := n/\gcd(i+j, n)$ is the smallest integer $c$ such that $(i+j)c$ is a multiple of $n$ because $(i+j)n/\gcd(i+j, n) = \text{lcm}(i+j, n)$.

Finally, we excluded the case $n = 1$ at the beginning of the proof, but we notice that the formula (3) gives $\alpha(1) = 2$, which is correct.

3 Rotation and reflection of rows and columns, and matrix transposition

Let $X_n := \{0, 1\}^{0,1,\ldots,n-1}^2$ be the set of $n \times n$ matrices of 0s and 1s, which has $2^{n^2}$ elements. Let $\beta(n)$ denote the number of orbits of the group action on $X_n$ by the group of order $8n^2$ generated by $\sigma$ (row rotation), $\tau$ (column rotation), $\rho$ (row reflection), $\theta$ (column reflection), and $\varsigma$ (matrix transposition). (Exceptions: If $n = 2$, the group is of order 8; if $n = 1$, the group is of order 1.)

Informally, $\beta(n)$ is the number of (distinct) toroidal $n \times n$ binary arrays, allowing rotation and/or reflection of rows and/or columns as well as matrix transposition.

Theorem 2. With $b(n, n)$ defined using (2), $\beta(n)$ is given by (4).

Proof. Let us assume that $n \geq 3$. (We will treat the cases $n = 1$ and $n = 2$ later.) By Pólya’s enumeration theorem,
\[
\beta(n) = \frac{1}{8n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (2^{A_{ij}} + 2^{B_{ij}} + 2^{C_{ij}} + 2^{D_{ij}} + 2^{E_{ij}} + 2^{F_{ij}} + 2^{G_{ij}} + 2^{H_{ij}}),
\]
where $A_{ij}$ (resp., $B_{ij}$, $C_{ij}$, $D_{ij}$, $E_{ij}$, $F_{ij}$, $G_{ij}$, $H_{ij}$) is the number of cycles in the permutation $\sigma^i\tau^j$ (resp., $\sigma^i\tau^j\rho$, $\sigma^i\tau^j\theta$, $\sigma^i\tau^j\rho\theta$, $\sigma^i\tau^j\zeta$, $\sigma^i\tau^j\rho\zeta$, $\sigma^i\tau^j\theta\zeta$, $\sigma^i\tau^j\rho\theta\zeta$); here $\sigma$ rotates the rows (row 0 becomes row 1, row 1 becomes row 2, ..., row $n-1$ becomes row 0), $\tau$ rotates the columns, $\rho$ reflects the rows (rows 0 and $n-1$ are interchanged, rows 1 and $n-2$ are interchanged, ..., rows $\lfloor n/2 \rfloor - 1$ and $n - \lfloor n/2 \rfloor$ are interchanged), $\theta$ reflects the columns, and $\zeta$ transposes the matrix. The order of the group generated by $\sigma$, $\tau$, $\rho$, $\theta$, and $\zeta$ is $8n^2$, using the assumption that $n \geq 3$.

We have already evaluated

$$a(n, n) = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2A_{ij},$$

$$\alpha(n) = \frac{1}{2n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (2A_{ij} + 2E_{ij}),$$

and

$$b(n, n) = \frac{1}{4n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (2A_{ij} + 2B_{ij} + 2C_{ij} + 2D_{ij}),$$

so

$$\beta(n) = \frac{1}{2} b(n, n) + \frac{1}{4} \left( \alpha(n) - \frac{1}{2} a(n, n) \right) + \frac{1}{8n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} (2F_{ij} + 2G_{ij} + 2H_{ij}). \tag{11}$$

Let us begin with

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2H_{ij}.$$  

Here we are concerned with the permutations $\sigma^i\tau^j\rho\theta\zeta$ for $(i, j) \in \{0, 1, \ldots, n-1\}^2$. We will need some multiplication rules for the permutations $\sigma$, $\tau$, $\rho$, $\theta$, and $\zeta$, specifically

$$\sigma\tau = \tau\sigma, \quad \sigma\theta = \theta\sigma, \quad \tau\rho = \rho\tau, \quad \rho\theta = \theta\rho, \quad \sigma\rho = \rho\sigma^{-1}, \quad \tau\theta = \theta\tau^{-1},$$

and

$$\sigma\zeta = \zeta\sigma, \quad \tau\zeta = \zeta\tau, \quad \rho\zeta = \zeta\rho, \quad \theta\zeta = \zeta\theta.$$  

It follows that (with $\tau^{-i} := (\tau^{-1})^i$)

$$\sigma^i\tau^j\rho\theta\zeta = \sigma^i\tau^j\zeta\theta\rho = \zeta\tau^i\sigma^j\theta\rho = \zeta\theta\rho\tau^{-i}\sigma^{-j},$$

and hence

$$(\sigma^i\tau^j\rho\theta\zeta)^2 = (\sigma^i\tau^j\rho\theta\zeta)(\zeta\theta\rho\tau^{-i}\sigma^{-j}) = \sigma^{i-j}\tau^{-i+j} = (\sigma\tau^{-1})^{i-j} = (\sigma^{-1}\tau)^{-i+j}. \tag{12}$$
In particular, if $i \in \{0, 1, \ldots, n-1\}$, then the permutation $\sigma^i \tau^j \rho \theta \zeta$ is of order 2. Furthermore, under this permutation, the entry in position $(k, l)$ moves to position $(n-1-[l+i], n-1-[k+i])$, where, as before, $[r] := (r \mod n) \in \{0, 1, \ldots, n-1\}$. Thus, $(k, l)$ is a fixed point if and only if

$$\quad (k, l) = (n-1-[l+i], n-1-[k+i]). \quad (13)$$

For each $k \in \{0, 1, \ldots, n-1\}$ there is a unique $l \in \{0, 1, \ldots, n-1\}$ (namely $l := n-1-[k+i]$) such that (13) holds; indeed,

$$n-1-[l+i] = n-1-[n-1-[k+i]+i] = n-1-[n-1-(k+i)+i] = n-1-[n-1-k] = n-1-(n-1-k) = k.$$

Thus, $\sigma^i \tau^j \rho \theta \zeta$ with $i \in \{0, 1, \ldots, n-1\}$ is of order 2 and has exactly $n$ fixed points, hence $(\frac{n}{2})$ transpositions. This implies that $H_k = n(n+1)/2$ for such $i$.

Now we let $(i, j) \in \{0, 1, \ldots, n-1\}^2$ be arbitrary but with $i \neq j$. Let us generalize (12) to

$$\quad (\sigma^i \tau^j \rho \theta \zeta)^{2d} = \sigma^{(i-j)d} \tau^{(-i+j)d} = ((\sigma \tau^{-1})^{i-j})^d = ((\sigma^{-1} \tau)^{-i+j})^d,$$

$$\quad (\sigma^i \tau^j \rho \theta \zeta)^{2d+1} = \sigma^{(i-j)d+i} \tau^{(-i+j)d+j} \rho \theta \zeta.$$

The proof proceeds much like the proof of Theorem 1. Specifically, $\sigma^i \tau^j \rho \theta \zeta$ is of order $2d$, where $d := n/gcd(|i-j|, n)$. All cycles have length $d$ or $2d$. In fact, if $d$ is odd, there are $n/d$ cycles of length $d$ and $n(n-1)/(2d)$ cycles of length $2d$. If $d$ is even, there are $n^2/(2d)$ cycles, all of length $2d$. And for a given $(i, j) \in \{0, 1, \ldots, n-1\}^2$, there are $n$ pairs $(k, l) \in \{0, 1, \ldots, n-1\}^2$ such that $[k-l] = |i-j|$. We arrive at the conclusion that

$$\frac{1}{8n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{H_{ij}} = \frac{1}{8n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{E_{ij}} = \frac{1}{4} \left( \alpha(n) - \frac{1}{2} a(n, n) \right). \quad (14)$$

Next we evaluate

$$\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{E_{ij}} = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2^{G_{ij}}, \quad (15)$$

where the equality holds by symmetry. We consider the permutations $\sigma^i \tau^j \rho \zeta$ for $(i, j) \in \{0, 1, \ldots, n-1\}^2$. From the multiplication rules, it follows that

$$\quad \sigma^i \tau^j \rho \zeta = \zeta \theta \tau^{-i} \sigma^j \quad$$

and hence

$$\quad (\sigma^i \tau^j \rho \zeta)^2 = (\sigma^i \tau^j \rho \zeta)(\zeta \theta \tau^{-i} \sigma^j) = \sigma^i \tau^j \rho \theta \tau^{-i} \sigma^j = \sigma^{i-j} \tau^{-i-j} \rho \theta = \theta \rho \sigma^{-i+j} \tau^{-i-j}, \quad (16)$$

which implies

$$\quad (\sigma^i \tau^j \rho \zeta)^4 = (\sigma^{i-j} \tau^{-i+j} \rho \theta)(\theta \rho \sigma^{-i+j} \tau^{-i-j}) = e.$$
So the permutation $\sigma^i\tau^j\rho\zeta$ is of order 4. The entry in position $(k, l)$ moves to position $([l + j], n - 1 - [k + i])$ under this permutation. Thus, $(k, l) \in \{0, 1, \ldots, n - 1\}^2$ is a fixed point of $\sigma^i\tau^j\rho\zeta$ if and only if

$$(k, l) = ([l + j], n - 1 - [k + i]).$$

There is a solution $(k, l)$ if and only if there exists $l \in \{0, 1, \ldots, n - 1\}$ such that, with $k := [l + j]$, we have $n - 1 - [k + i] = l$ or, equivalently,

$$[l + i + j] = n - 1 - l. \quad (17)$$

When $i + j \leq n - 1$, $(17)$ is equivalent to

$$l + i + j = n - 1 - l \quad \text{or} \quad l + i + j - n = n - 1 - l$$

or to

$$l = (n - 1 - i - j)/2 \quad \text{or} \quad l = (2n - 1 - i - j)/2.$$

If $n$ is odd and $i + j$ is odd, then there is one fixed point, $(k, l) = ([2(n - 1 - i + j)/2], [2(n - 1 - i - j)/2])$. If $n$ is odd and $i + j$ is even, then there is one fixed point, $(k, l) = ([n - 1 - i + j]/2, [(n - 1 - i - j)/2])$. If $n$ is even and $i + j$ is odd, then there are two fixed points, namely

$$(k, l) = ([n - 1 - i + j]/2, [(n - 1 - i - j)/2]),$$

$$(k, l) = ([2n - 1 - i + j]/2, [(2n - 1 - i - j)/2]).$$

Finally, if $n$ is even and $i + j$ is even, then there is no fixed point.

When $i + j \geq n$, $(17)$ is equivalent to

$$l + i + j - n = n - 1 - l \quad \text{or} \quad l + i + j - 2n = n - 1 - l$$

or to

$$l = (2n - 1 - i - j)/2 \quad \text{or} \quad l = (3n - 1 - i - j)/2.$$

If $n$ is odd and $i + j$ is odd, then there is one fixed point, $(k, l) = ([2(n - 1 - i + j)/2], [2(n - 1 - i - j)/2])$. If $n$ is odd and $i + j$ is even, then there is one fixed point, $(k, l) = ([3n - 1 - i + j]/2, [3n - 1 - i - j]/2) = ([n - 1 - i + j]/2, [(n - 1 - i - j)/2])$. If $n$ is even and $i + j$ is odd, then there are two fixed points, namely

$$(k, l) = ([2n - 1 - i + j]/2, [(2n - 1 - i - j)/2]),$$

$$(k, l) = ([n - 1 - i + j]/2, [(n - 1 - i - j)/2]).$$

Finally, if $n$ is even and $i + j$ is even, then there is no fixed point. Notice that the results are the same for $i + j \geq n$ as for $i + j \leq n - 1$. 

10
Using (16), under the permutation \((\sigma^i \tau^j \rho \zeta)^2\), the entry in position \((k, l)\) moves to position 
\((n-1 - [k+i-j], n-1 - [l+i+j])\). Thus, \((k, l) \in \{0, 1, \ldots, n-1\}^2\) is a fixed point of 
\((\sigma^i \tau^j \rho \zeta)^2\) if and only if 
\[
(k, l) = (n-1 - [k+i-j], n-1 - [l+i+j]).
\]
A necessary and sufficient condition on \((k, l)\) is (17) together with 
\([k+i-j] = n-1-k\). Solutions have \(l\) as before. On the other hand, \(k\) must satisfy 
\[
k+i-j-n = n-1-k, \quad k+i-j = n-1-k, \quad \text{or} \quad k+i-j+n = n-1-k,
\]
or equivalently, 
\[
k = [(n-1-i+j)/2] \quad \text{or} \quad k = [(2n-1-i+j)/2].
\]
If \(n\) is odd, the only fixed points of \((\sigma^i \tau^j \rho \zeta)^2\) are those already shown to be fixed points 
of \(\sigma^i \tau^j \rho \zeta\). If \(n\) is even and \(i+j\) is odd, there are two fixed points of \((\sigma^i \tau^j \rho \zeta)^2\) that are not 
fixed points of \(\sigma^i \tau^j \rho \zeta\), namely 
\[
(k, l) = ([(n-1-i+j)/2], [(2n-1-i-j)/2]),
\]
\[
(k, l) = ([(2n-1-i+j)/2], [(n-1-i-j)/2]).
\]
Finally, there are no fixed points when \(n\) is even and \(i+j\) is even.
Consequently, if \(n\) is odd, then the permutation \(\sigma^i \tau^j \rho \zeta\), which is of order 4, has only one 
fixed point. Therefore, it has one cycle of length 1 and \((n^2-1)/4\) cycles of length 4. Thus, 
\[
\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2F_{ij} = n^2 2^{(n^2+3)/4}.
\]
For even \(n\), if \(i+j\) is odd, then the permutation \(\sigma^i \tau^j \rho \zeta\) has two cycles of length 1 and one 
cycle of length 2, and the remaining cycles are of length 4. If \(i+j\) is even, then all cycles of 
the permutation \(\sigma^i \tau^j \rho \zeta\) are of length 4, hence there are \(n^2/4\) of them. Thus, 
\[
\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} 2F_{ij} = \frac{1}{2} n^2 2^{(n^2-4)/4+3} + \frac{1}{2} n^2 2^{n^2/4} = 5n^2 2^{n^2/4-1}.
\]
These results, together with (3), (10), (11), (14), and (15), yield (4).
Finally, recall that we have assumed that \(n \geq 3\). We notice that the formula (4) gives 
\(\beta(1) = 2\) and \(\beta(2) = 6\), which are correct, as we can see by direct enumeration. \(\Box\)
In the derivation of (2) in [1], the proof requires \(m, n \geq 3\) because the group \(D_m \times D_n\) 
used in the application of Pólya’s enumeration theorem (\(D_m\) being the dihedral group of 
order \(2m\)), is incorrect if \(m\) or \(n\) is 1 or 2. If \(m = 2\), row rotation and row reflection are 
the same, so the latter is redundant. Thus, \(D_2\) should be replaced by \(C_2\), the cyclic group
of order 2. The reason (2) is still valid is that $b_1(2,n) = b_2(2,n)$ and $b_3(2,n) = b_4(2,n)$, as is easily verified. If $m = 1$, again row reflection is redundant, so $D_1$ should be replaced by $C_1$. Here (2) remains valid because $b_1(1,n) = b_2(1,n)$ and $b_3(1,n) = b_4(1,n)$. A similar remark applies to $n = 2$ and $n = 1$, except that here $b_1(m,2) = b_3(m,2)$, $b_2(m,2) = b_4(m,2)$, $b_1(m,1) = b_3(m,1)$, and $b_2(m,1) = b_4(m,1).

References


2010 *Mathematics Subject Classification*: Primary 05A05.

*Keywords*: toroidal array, Euler’s phi function, group action, orbit, Pólya’s enumeration theorem.

(Concerned with sequences A040076, A179043, A184271, A209251, A222188, A255015, and A255016.)

Received February 19 2015; revised version received June 3 2015. Published in *Journal of Integer Sequences*, July 16 2015.

Return to *Journal of Integer Sequences* home page.