ENUMERATION AND CODING METHODS FOR A CLASS OF PERMUTATIONS AND REVERSIBLE LOGICAL GATES

Costas Karanikas¹, Nikolaos Atreas²

¹School of Informatics, Aristotle University of Thessaloniki, Greece
²School of Electrical and Computer Engineering, Faculty of Engineering, Aristotle University of Thessaloniki, Greece

Abstract. We introduce a great variety of coding methods for boolean sparse invertible matrices and we use these methods to create a variety of bijections on the permutation group \( P(m) \) of the set \( \{1,2,\ldots,m\} \). Also, we propose methods for coding, enumerating and shuffling the set \( \{0,\ldots,2^m-1\} \), i.e. the set of all \( m \)-bit binary arrays. Moreover we show that several well known reversible logic gates/circuits (on \( m \)-bit binary arrays) can be coded by sparse matrices.

Key words: Permutations, Reversible Logical Gates.

1 INTRODUCTION

Let \( m \geq 2 \) be a natural number and \( P(m) \) be the group of permutations of the set \( \{1,\ldots,m\} \). In this work we introduce a variety of shuffling methods. More precisely, each shuffling method is a bijective map of a set onto itself, i.e. different inputs yield different outputs and the number of inputs and outputs are equal.

Our main theorem 2 in section 3 or its "binary" version (see theorem 3 in section 4), states that any pair \( (\rho, s) \) of permutations in \( P(m) \) determines a bijective map

\[
T_{\rho,s} : \{0,1,\ldots,2^m-1\} \rightarrow \{0,1,\ldots,2^m-1\}.
\]
Since every non negative integer \(n \in \{0, 1, ..., 2^m - 1\}\) can be expressed either as an \(m\)-bit binary array

\[e_n = (\varepsilon_0(n), \varepsilon_1(n), ..., \varepsilon_{m-1}(n)), \; \varepsilon_j \in \{0, 1\},\]

or by its dyadic expansion

\[n = \sum_{j=1}^{m} \varepsilon_j(n)2^{j-1},\]

the above map \(T_{\rho,s}\) can be considered as a reversible map on the set of all \(m\)-bit binary arrays. In a different terminology, we can say that in theorem 3 we introduce reversible logic gates, i.e. bijective maps on the set of \(m\)-bit binary arrays, (see [1]). An example of a reversible gate is the NOT gate, whereas the AND, OR, XOR gates are irreversible (not reversible), because they map \(4 = 2^2\) input states into \(2 = 2^1\) output states, so information is lost in the merging of paths.

A second target of this work is to enumerate and code permutations in \(P(m)\) of large length (note that the cardinality of the set \(P(m)\) is \(m!\)). Therefore, a reversible map \(T_{\rho,s}\) associated with the pair \((\rho, s)\) can be coded either by the pair \((\rho, s)\) or by an enumeration of \(P(m) \times P(m)\) as in section 2. This coding method is associated with a particular class of sparse boolean invertible matrices introduced in [2] (see also [3–6]). Notice that sparse matrices are very useful for fast processing/transmission of data and they have been effectively used in [6] for detecting specific characteristics on finite data.

The paper is organized in the following sections:

In section 2 we introduce our main tool, the invertible map \(P(m) \rightarrow S(m)\) (see (2) and (3)) and in Proposition 1, we see that this map induces the lexicographical order of the enumeration of \(P(m)\). Moreover we consider the cartesian product \(R(m) = P(1) \times P(2) \times ... \times P(m)\) of permutations to show in theorem 1 that each fixed element of \(R(m)\) provides an enumeration of \(P(m)\).

In section 3 we define a class of sparse \(m \times m\) boolean invertible matrices \(Z_m\) identified by a pair \((\rho, s) \in P(m) \times S(m)\) and we use this class of matrices to produce a class of non-linear bijection maps

\[T_{q,\rho,s} : \{0, ..., q^m - 1\} \rightarrow \{0, ..., q^m - 1\},\]

see our main theorem 2.
In section 4 we show that any triple \((\rho, s, \tau)\) of permutations in \(P(m)\) provides a variety of maps from \(\{0, \ldots, 2^m - 1\}\) onto \(\{0, \ldots, 2^m - 1\}\) and we see that several reversible logic gates can be determined by this triple.

Finally, in section 5 we apply theorems 1 and 2, to see with an example that for any pair \((\rho, s) \in P(m) \times S(m)\) and any fixed \(r \in R(2^m)\) we shuffle the elements of the set \(\{0, \ldots, 2^m - 1\}\) and we discuss the random permutation generation problem.

2 Enumeration methods for \(P(m)\)

Let \(m \geq 2\) be a natural number. First we review the lexicographical order of the set

\[
S(m) = \{ s = (s_1, \ldots, s_m) : s_i \in \{1, 2, \ldots, i\} \}. \tag{1}
\]

Obviously, the map

\[
U : S(m) \to \{0, \ldots, m! - 1\} : U(s) = m! \sum_{i=1}^{m} \frac{s_i - 1}{i!} \tag{2}
\]

is a bijection and the elements \(s_i \in \{1, \ldots, i\}\) can be thought of digits of the number \(U(s)\) with respect to the factorial number system. Inversely, for any \(n \in \{0, \ldots, m! - 1\}\), its digits \(s_i(n), i = 1, \ldots, m\) are computed by the formula

\[
s_i(n) = \text{Mod}\left(\left\lfloor \frac{n}{i!} \right\rfloor, i \right) + 1
\]

describing the inverse map \(U^{-1}\). Here, \([x]\) is the floor of \(x\). From now on we say that \(U\) provides the lexicographical order of \(S(m)\). Using the lexicographical order of \(S(m)\) we may obtain an enumeration of the group of permutations \(P(m)\) of the set \(\{1, \ldots, m\}\) as well. In fact, let us define the map

\[
Q : P(m) \to S(m) : Q(\rho) = s = (s_1, \ldots, s_m), \tag{3}
\]

where each element \(s_i \in S(m)\) is defined by using the following iteration scheme:

For the above selection of \(m\) and the initial permutation \(\rho\) in (3), we store the position of the biggest element in \(\rho\), i.e. we define

\[
s_m = \rho^{-1}(m)
\]
and at the same time we delete this element \( \rho(s_m) = m \) from \( \rho \) and so we form a new permutation \( \rho_{(m-1)} \in P(m-1) \) by

\[
\rho_{(m-1)}(j) = \begin{cases} 
\rho(j) & \text{if } j < s_m \\
\rho(j + 1) & \text{if } j \geq s_m
\end{cases}, \quad j = 1, \ldots, m - 1.
\]

Then we follow the previous step for the permutation \( \rho_{(m-1)} \), i.e. we store the position of its biggest element by defining

\[s_{m-1} = \rho_{(m-1)}^{-1}(m - 1)\]

and at the same time we delete the element \( m - 1 \) from \( \rho_{(m-1)} \) and we form a new permutation \( \rho_{(m-2)} \in P(m-2) \) by

\[
\rho_{(m-2)}(j) = \begin{cases} 
\rho_{(m-1)}(j) & \text{if } j < s_{m-1} \\
\rho_{(m-1)}(j + 1) & \text{if } j \geq s_{m-1}
\end{cases}, \quad j = 1, \ldots, m - 2.
\]

We continue in the same spirit until \( S \) is completely determined.

**Example 1** Let \( \rho = (2, 3, 4, 1) \). In order to determine the set \( S = \{s_1, s_2, s_3, s_4\} \) in (3) we are based on the above iteration scheme and so we proceed in the following way:

(i) Define \( s_4 = \rho^{-1}(4) = 3 \) and \( \rho_{(3)} = (2, 3, 1) \).

(ii) Define \( s_3 = \rho_{(3)}^{-1}(3) = 2 \) and \( \rho_{(2)} = (2, 1) \).

(iii) Define \( s_2 = \rho_{(2)}^{-1}(2) = 1 \) and \( \rho_{(1)} = (1) \).

(iv) Define \( s_1 = \rho_{(1)}^{-1}(1) = 1 \) and \( \rho_{(4)} = \emptyset \).

Now we have the following:

**Proposition 1** [2] Let \( U \) and \( Q \) be two maps as in (2) and (3) respectively. Then \( Q \) is a bijection and so the composition map

\[UQ : P(m) \to \{0, \ldots, m! - 1\}\]

provides an enumeration of \( P(m) \).
**Example 2** For \( m = 4 \), we demonstrate the enumeration of the elements of \( P(4) \) derived from Proposition (1) and the lexicographical order of the elements of \( S(4) \) derived from (2).

\[
P(4) = \{(4, 3, 2, 1), (3, 4, 2, 1), (3, 2, 4, 1), (3, 2, 1, 4),
        (4, 2, 3, 1), (2, 4, 3, 1), (2, 3, 4, 1), (2, 3, 1, 4),
        (4, 2, 1, 3), (2, 4, 1, 3), (2, 1, 4, 3), (2, 1, 3, 4),
        (4, 3, 1, 2), (3, 4, 1, 2), (3, 1, 4, 2), (3, 1, 2, 4),
        (4, 1, 3, 2), (1, 4, 3, 2), (1, 3, 4, 2), (1, 3, 2, 4),
        (4, 1, 2, 3), (1, 4, 2, 3), (1, 2, 4, 3), (1, 2, 3, 4)\}.
\]

\[
S(4) = \{(1, 1, 1, 1), (1, 1, 1, 2), (1, 1, 1, 3), (1, 1, 1, 4),
        (1, 1, 2, 1), (1, 1, 2, 2), (1, 1, 2, 3), (1, 1, 2, 4),
        (1, 1, 3, 1), (1, 1, 3, 2), (1, 1, 3, 3), (1, 1, 3, 4),
        (1, 2, 1, 1), (1, 2, 1, 2), (1, 2, 1, 3), (1, 2, 1, 4),
        (1, 2, 2, 1), (1, 2, 2, 2), (1, 2, 2, 3), (1, 2, 2, 4),
        (1, 2, 3, 1), (1, 2, 3, 2), (1, 2, 3, 3), (1, 2, 3, 4)\}.
\]

For instance, the permutation \( \rho = (4, 3, 2, 1) \) is uniquely associated with the set

\[
Q(\rho) = (1, 1, 1, 1)
\]

(apply example 1) and then

\[
UQ(\rho) = 0
\]

by (2). In the same spirit, the permutation \( \rho = (3, 4, 2, 1) \) is uniquely associated with the set

\[
Q(\rho) = (1, 1, 1, 2)
\]

(apply example 1) and then

\[
UQ(\rho) = 1
\]

by (2).

**Remark 1** The set \( S(m) \) in (1) seems to be similar with a Lehmer code [7], but our approach seems to be more efficient for the purpose of obtaining a great variety of enumerating methods for \( P(m) \), see theorem (1) below. We notice that the Lehmer code of a permutation \( \rho = (\rho_1, ..., \rho_m) \) is a sequence of natural numbers \( (L_1, ..., L_m) \) such that \( L_i \) is the number of all elements \( \rho_1, ..., \rho_{i-1} \) which are less than \( \rho_i \), \( i = 1, ..., m \).
We may obtain various enumerations of the elements of \( S(m) \) (and hence \( P(m) \) as well). Indeed, let us fix any element
\[
  r = (r_1, r_2, \ldots, r_m) \in R(m) = P(1) \times P(2) \times \ldots \times P(m),
\]
where
\[
  r_i = (r_{i,1}, \ldots, r_{i,i}) \in P(i), \ i = 1, \ldots, m.
\]
Then we have:

**Theorem 1** Let \( S(m) \) be defined in (1) and \( r \) be a fixed element of \( R(m) \) as in (4). For any \( s \in S(m) \) we define
\[
  W_{r,m}(s) = (r_{1,s_1}, r_{2,s_2}, \ldots, r_{m,s_m})
\]
Then the map \( W_{r,m} \) is onto \( S(m) \).

**Proof:** Let us fix an element \( r \in R(m) \). Since \( r_{i,s_i} \leq i \) (due to the fact that \( r_i \in P(i) \)), we deduce that \( W_{r,m}(s) \in S(m) \). Also, the fact that \( r_{i,j} \leq i \) for any \( j = 1, \ldots, i \) implies that \( W_{r,m} \) is onto \( S(m) \), because any element \( s_i \) of \( s = (s_1, \ldots, s_m) \) can be written by \( s_i = r_{i,a(i)} \) for some index \( a(i) \leq i \) and so by defining \( a = \{a(i) : i = 1, \ldots, m\} \) we have \( W_{r,m}(a) = s \).

Let \( U \) be as in (2) and \( W_{r,m} \) be as in theorem 1. It is easy to see that the map
\[
  UW_{r,m}U^{-1} : \{0, \ldots, m! - 1\} \to \{0, \ldots, m! - 1\}
\]
provides a method for shuffling the set \( \{0, \ldots, m! - 1\} \). By altering the selection of \( r \in R(m) \) in (4) we obtain a different shuffling. Finally, it is clear that the class of mappings
\[
\{ QW_{r,m}U^{-1} : r \in R(m) \}
\]
provides a great variety of enumeration/shuffling methods for the set of permutations \( P(m) \).

**Example 3** For \( m = 4 \) and \( r = \{(1, (2,1), (2,1,3), (4,2,1,3)\} \), then by using theorem 1, the lexicographical order of \( S(4) \) (see example 2) is shuffled to:
\[
\{(1,2,2,4), (1,2,2,2), (1,2,2,1), (1,2,2,3),
(1,2,1,4), (1,2,1,2), (1,2,1,1), (1,2,1,3),
(1,2,3,4), (1,2,3,2), (1,2,3,1), (1,2,3,3),
(1,1,2,4), (1,1,2,2), (1,1,2,1), (1,1,2,3),
(1,1,1,4), (1,1,1,2), (1,1,1,1), (1,1,1,3),
(1,1,3,4), (1,1,3,2), (1,1,3,1), (1,1,3,3)\}.
\]
If $Q$ is defined in (3), then by using the composition map

$$Q^{-1}W_{r,4}U^{-1}$$

we obtain the following enumeration of the set $P(4)$:

$$\{(1, 2, 3, 4), (1, 4, 2, 3), (4, 1, 2, 3), (1, 2, 4, 3), (2, 3, 1, 4), (2, 4, 3, 1), (4, 2, 3, 1), (2, 3, 4, 1), (3, 2, 1, 4), (3, 4, 2, 1), (4, 3, 2, 1), (3, 2, 4, 1), (2, 1, 3, 4), (2, 4, 1, 3), (4, 2, 1, 3), (2, 1, 4, 3), (1, 3, 2, 4), (1, 4, 3, 2), (4, 1, 3, 2), (1, 3, 4, 2), (3, 1, 2, 4), (3, 4, 1, 2), (4, 3, 1, 2), (3, 1, 4, 2)\}.$$  

3 A class of boolean matrices coded by permutations and a class of bijection maps

Before we introduce a class of bijection maps on $\{0, 1, \ldots, q^m - 1\}$ for any pair of natural numbers $m, q \geq 2$, we present as in [2] a class of sparse boolean matrices and their properties.

**Definition 1** For any natural number $m \geq 2$ we define by $Z_m$ the class of all $m \times m$ boolean matrices whose row vectors $Z_i$ satisfy

$$Z_i \odot Z_j = c_{ij} Z_{\max\{i,j\}} : c_{ij} \in \{0, 1\}, i, j = 1, \ldots, m,$$

where $\odot$ is the usual Hadamard product operation.

Then the following result is straightforward:

**Lemma 1** [2] Let $A$ be an $m \times m$ boolean matrix and let $1 \leq i < j \leq m$. Then $A \in Z_m$ if and only if $\text{supp}\{A_j\} \subseteq \text{supp}\{A_i\}$ or $\text{supp}\{A_i\} \cap \text{supp}\{A_j\} = \emptyset$. Here, $\text{supp}(A_j)$ denotes the set of all non zero entries of the row $A_j$.

In [2] we proved the following:

**Proposition 2** Let $P(m)$ and $S(m)$ be defined in section 2. Then every matrix in the class $Z_m$ is uniquely identified by a pair $(\rho, s) \in P(m) \times S(m)$.

Using the above observations we may easily construct elements in the above class of $Z_m$ matrices. Indeed, let us fix a pair $(\rho, s) \in P(m) \times S(m)$ which determines a matrix $Z \in Z_m$ in a unique way. From the pair $(\rho, s)$ we may construct $Z$ in the following manner:
(i) First, we use \( \rho \) to permute the rows of the identity matrix \( I_m \) and so we construct an \( m \times m \) permutation matrix, say \( Z_1 \).

(ii) Starting with the above matrix \( Z_1 \), we construct a sequence \( \{Z_i\}_{i=2}^m \) of \( m \times m \) matrices iteratively, by using \( s \in S(m) \). In the \( i^{th} \) step of this iteration, a matrix \( Z_i \) is constructed from the matrix \( Z_{i-1} \) based on the following rule:

(a) If \( s_1 = i \), define \( Z_i = Z_{i-1} \).

(a) If \( s_1 < i \), define \( Z_i \) by replacing only the \( s_1 \)-row of \( Z_{i-1} \) with the sum of the \( i \)-row and \( s_1 \)-row of \( Z_{i-1} \).

(iii) Execute step (ii) for any \( i = 2, \ldots, m \). Then \( Z = Z_m \) is a matrix in the class \( Z_m \).

Example 4 Let \( m = 5 \), \( \rho = (4, 1, 2, 5, 3) \) and \( s = (1, 1, 3, 1, 3) \). Then the element \( Z \in Z_5 \) associated with the above pair \( (\rho, s) \) is the following

\[
Z = \begin{pmatrix}
1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0
\end{pmatrix}.
\]

It is remarkable that any matrix \( Z \) in the class \( Z_m \) (which depends only on a pair \( (\rho, s) \)) is invertible and the entries of inverse matrix \( Z^{-1} \) are immediately computed by the above pair \( (\rho, s) \):

\[
Z_{i,j}^{-1} = \begin{cases} 
1 & i = \rho(j) \\
-1, & i = \rho(s(j)) \text{ and } s(j) < j \\
0 & \text{otherwise}
\end{cases}, \quad i, j = 1, \ldots, m. \tag{5}
\]

Example 5 If \( Z \in Z_5 \) is as in example (4), then the inverse matrix of \( Z \) is calculated directly from (5):

\[
Z^{-1} = \begin{pmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & -1 \\
0 & 0 & 0 & 0 & 1 \\
1 & -1 & 0 & -1 & 0 \\
0 & 0 & 0 & 1 & 0
\end{pmatrix}.
\]
We consider now a matrix $Z^{-1}$ as above corresponding to a pair $\rho = (\rho_1, \ldots, \rho_m) \in P(m)$ and $s = (s_1, \ldots, s_m) \in S(m)$. We shall use $Z^{-1}$ to define a new shuffling method. By elementary calculations, for any real row vector $\mathbf{e} = (e_1, \ldots, e_m)$ we obtain

$$\left(\mathbf{e}Z^{-1}\right)_i = e_{\rho_i} - (1 - \delta_{i,s_i})e_{\rho_{s_i}}, \quad i = 1, \ldots, m. \quad (6)$$

Here, $\delta_{i,j}$ denotes the usual Kronecker’s delta symbol. Inspired from (6) we have:

**Theorem 2** Let $m, q \geq 2$ be natural numbers, $\rho = (\rho_1, \ldots, \rho_m) \in P(m)$ and $s = (s_1, \ldots, s_m) \in S(m)$. We define the set

$$E^{(q)}_m = \{\mathbf{e}_n = (e_{n,1}, \ldots, e_{n,m}) : n = 0, \ldots, q^m - 1\},$$

where $\mathbf{e}_n$ is the sequence of digits of $n \in \{0, \ldots, q^m - 1\}$ with respect to its $q$-adic expansion

$$n = \sum_{i=1}^{m} e_{n,i}q^{i-1}.$$

Then the map

$$T_{q,\rho,s}: E^{(q)}_m \rightarrow E^{(q)}_m$$

such that for any $i = 1, \ldots, m$

$$T_{q,\rho,s}(\mathbf{e}_n)_i = \text{Mod}\left(e_{n,\rho_i} - (1 - \delta_{i,s_i})e_{n,\rho_{s_i}}, q\right)$$

is a bijection.

**Proof:** For any natural numbers $m, q \geq 2$ we fix a pair $(\rho, s) \in P(m) \times S(m)$ and we consider the above operator $T_{q,\rho,s}$. From now on we write

$$T = T_{q,\rho,s}$$

for simplicity. Let $T(\mathbf{e}_k)$ and $T(\mathbf{e}_n)$ be two sequences for some pair $(k, n) \in \{0, \ldots, q^m - 1\}^2$. Notice that the elements of $\mathbf{e}_k$ and $\mathbf{e}_n$ belong in $\{0, \ldots, q - 1\}$ by definition. Assume that

$$T(\mathbf{e}_k) = T(\mathbf{e}_n) \Rightarrow T(\mathbf{e}_k)_i = T(\mathbf{e}_n)_i, \quad \forall i = 1, \ldots, m. \quad (7)$$

If $i = 1$ in (7), then by recalling the definition of $S(m)$ in (1) we have $s_1 = 1$, so

$$T(\mathbf{e}_k)_1 = T(\mathbf{e}_n)_1 \Rightarrow \text{Mod}(e_{k,\rho_1}, q) = \text{Mod}(e_{n,\rho_1}, q).$$
Hence $e_{k,\rho_1} = e_{n,\rho_1}$. 

If $i = 2$, then $s_2 \in \{0, 1\}$. For $s_2 = 2$ we immediately obtain 

$$e_{k,\rho_2} = e_{n,\rho_2}.$$ 

For $s_2 = 1$ we have 

$$T(e_k)_2 = T(e_n)_2$$ 

$$\Rightarrow Mod\left( e_{k,\rho_2} - e_{k,\rho_2}, q \right) = Mod\left( e_{n,\rho_2} - e_{n,\rho_2}, q \right)$$ 

$$\Rightarrow Mod\left( e_{k,\rho_2} - e_{n,\rho_1}, q \right) = Mod\left( e_{n,\rho_2} - e_{n,\rho_1}, q \right),$$ 

where the last equality was derived from the fact that $e_{k,\rho_1} = e_{n,\rho_1}$ as we showed above. Hence, either 

$$e_{k,\rho_2} - e_{n,\rho_1} = e_{n,\rho_2} - e_{n,\rho_1} \Rightarrow e_{k,\rho_2} = e_{n,\rho_2}$$ 

or 

$$q - (e_{k,\rho_2} - e_{n,\rho_1}) = q - (e_{n,\rho_2} - e_{n,\rho_1}) \Rightarrow e_{k,\rho_2} = e_{n,\rho_2}.$$ 

Therefore, in any case we obtain 

$$e_{k,\rho_2} = e_{n,\rho_2}.$$ 

We proceed in the same manner for the remaining values $i = 3, ..., m$ obtaining 

$$e_{k,\rho_i} = e_{n,\rho_i}, \forall i = 1, ..., m.$$ 

Since $\rho$ is a permutation, necessarily 

$$e_{k,\rho_i} = e_{n,\rho_i}, \forall i = 1, ..., m$$ 

and the proof is complete.

It is clear that the above operator $T_{q,\rho,s}$ provides a code for shuffling the elements of the set $\{0, ..., q^m - 1\}$.

**Example 6** Let $q = 3$, $\rho = (2, 1)$, $s = (1, 2)$ and 

$$E^{(3)}_2 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2), (2, 0), (2, 1), (2, 2)\}.$$ 

Then by the above definition of $T_{q,\rho,s}$ we obtain 

$$(0, 0) \rightarrow (0, 0), (0, 1) \rightarrow (1, 0), (0, 2) \rightarrow (2, 0),$$ 

$$(1, 0) \rightarrow (0, 1), (1, 1) \rightarrow (1, 1), (1, 2) \rightarrow (2, 1),$$ 

$$(2, 0) \rightarrow (0, 2), (2, 1) \rightarrow (1, 2) \text{ and } (2, 2) \rightarrow (2, 2)$$ 

or 

$$T_{q,\rho,s} : \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \rightarrow \{0, 3, 6, 1, 4, 7, 2, 5, 8\}.$$
4 On reversible gates

In this section we see that several of the well known reversible gates can be obtained by the bijection maps of theorem 2. First, we modify theorem 2 as follows:

**Theorem 3** For any natural number \( m \), let \(( \rho, s) \in P(m) \times S(m)\) be as in theorem 2 and

\[
E_m = \{ e_n := (e_{n,1}, ..., e_{n,m}) : n = \{0, ..., 2^m - 1\}\}
\]

be the set of all \( m \)-bit arrays. Then:

(i) The map

\[
T_{\rho, \sigma} : E_m \rightarrow E_m
\]

such that for any \( j = 1, ..., m \) we have

\[
T_{\rho, \sigma}(e_n)_j = |e_{n, \rho_j} - (1 - \delta_j, s(j))e_{n, \rho_s(j)}|
\]

is a bijection.

(ii) For any permutation \( \tau \in P(m) \) we denote by

\[
L_\tau(e_n) = (e_{n, \tau(1)}, ..., e_{n, \tau(m)})
\]

the element of \( E_m \) obtained from shuffling \( e_n \) by the permutation \( \tau \).

Then

\[
L_\tau T_{\rho, \sigma} : E_m \rightarrow E_m
\]

is a bijection too.

**Proof:** (i). It is a direct consequence of theorem 2 for \( q = 2 \).

(ii) It is immediate.

**Example 7 The Feynman Gate.** It is a 2-bit reversible map such that

\[
(0, 0) \rightarrow (0, 0), \ (0, 1) \rightarrow (0, 1), \ (1, 0) \rightarrow (1, 1) \text{ and } (1, 1) \rightarrow (1, 0).
\]

According to theorem 3, this gate corresponds to the map \( T_{\rho, \sigma} \), where

\[
\rho = (1, 2) \text{ and } \sigma = (1, 1).
\]
In a different notation this gate can be uniquely described by a matrix in the class $\mathbb{Z}_2$ associated with the above pair $(\rho, s) \in P(2) \times S(2)$ (see definition 1 or example 4)

\[ Z_{\rho,s} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}. \]

Also, in a different notation this gate can be described by the following $4 \times 4$ matrix (by concatenating the corresponding inputs and outputs)

\[
\begin{bmatrix}
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 1 & 0
\end{bmatrix}.
\]

**Example 8 The Double Feynman Gate.** It is a reversible map on the 3 bit binary arrays so that

- $(0,0,0) \rightarrow (0,0,0)$, $(1,0,0) \rightarrow (1,1,1)$, $(0,1,0) \rightarrow (0,1,0)$,

- $(1,1,0) \rightarrow (1,0,1)$, $(0,0,1) \rightarrow (0,0,1)$, $(1,0,1) \rightarrow (1,1,0)$,

- $(0,1,1) \rightarrow (0,1,1)$ and $(1,1,1) \rightarrow (1,0,0)$.

According to theorem 3, this gate corresponds to the map $T_{\rho,\sigma}$, where

\[ \rho = (1,2,3) \text{ and } \sigma = (1,1,1). \]

In a different notation, this gate can be uniquely described by a matrix in the class $\mathbb{Z}_3$ associated with the above pair $(\rho, s) \in P(3) \times S(3)$ (see the above definition 1 or example 4)

\[ Z_{\rho,s} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \]

Also, in a different notation this gate can be described by the following $8 \times 6$ matrix (by concatenating the corresponding inputs and outputs)

\[
\begin{bmatrix}
0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0
\end{bmatrix}.
\]
According to theorem 3, this gate corresponds to the map $Z$ in a different notation, this gate can be uniquely described by a matrix in the $Z$ class. In a different notation, this gate can be described by the following matrix (by concatenating the corresponding inputs and outputs). Example 8 The Double Feynman Gate. Also, in a different notation this gate can be described by the following matrix (by concatenating the corresponding inputs and outputs).

We mention here that the 2-bit Swap gate can be also implemented by the map $T_{\rho,s}$ by selecting $\rho = (2,1)$ and $s = (1,2)$. However, the 3-bit Toffoli and Fredkin gates cannot be implemented via $T_{\rho,s}$.

5 CODING PSEUDORANDOM PERMUTATIONS

We apply theorem 2 to give by an example a method to code a pseudo-random permutation in $P(2^m)$. For any $(\rho,s) \in P(m) \times S(m)$ and a fixed random permutation $r \in R(2^m)$ we shuffle the image of $T_{2,\rho,s}$ by the composition map $W_{r,2}T_{2,\rho,s}$ for some particular selection of $r \in R(2^8)$ (see theorem 1) and we obtain a pseudo-random permutation coded by a triple $(\rho,s,r)$.

Example 9 Let $\rho = (5,7,6,3,4,8,1,2)$ and $s = (1,1,1,4,5,2,7,3)$. Figure 1 shows how the bijective map $T_{2,\rho,s}$ of theorem 2 shuffles the elements of the set $I_8 = \{0, ..., 2^8-1\}$. In figure 2 we use a fixed element $r \in R(2^8)$ (see theorem 1) and we shuffle the set $I_8$ by means of the composition operator $W_{r,2}T_{2,\rho,s}$. In this case, the graph appears to be more "randomly" distributed than the graph of figure 1.

In conclusion, we demonstrated a variety of new enumeration/shuffling methods for the group of permutations. We also proposed a class of bijections for sets of natural numbers based on efficient coding methods for
sparse boolean matrices. We also discussed possible connections of the shuffling problem with the random permutation generation problem. According to [8,9], any permutation in $P(m)$ can be almost uniformly randomly distributed using $m \log_2(m)/2$. This observation may be important for establishing a connection between our shuffling method and the random permutation generation problem in future. We believe that this direction is very promising.

REFERENCES


Fig. 2: The set of points \{ (n, W_r, T_n^2, \rho, s_n) : n \in I_8 \} for some \( r \in \mathbb{R} (2_8) \) and \((\rho, s)\) as in example 9.

We also discussed possible connections of the shuffling problem with the random permutation generation problem. According to [8,9], any permutation in \( P(m) \) can be almost uniformly randomly distributed using \( m \log_2(m)/2 \). This observation may be important for establishing a connection between our shuffling method and the random permutation generation problem in future. We believe that this direction is very promising.

References


