Algorithmic and algebraic aspects of unshuffling permutations
Samuele Giraudo, Stéphane Vialette

To cite this version:
Samuele Giraudo, Stéphane Vialette. Algorithmic and algebraic aspects of unshuffling permutations. Theoretical Computer Science, Elsevier, 2018, 729, pp.20 - 41. 10.1016/j.tcs.2018.02.007. hal-01797134

HAL Id: hal-01797134
https://hal-upec-upem.archives-ouvertes.fr/hal-01797134
Submitted on 23 May 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Algorithmic and algebraic aspects of unshuffling permutations

Samuele Giraudo, Stéphane Vialette

Université Paris-Est, LIGM (UMR 8049), CNRS, ENPC, ESIEE Paris, UPEM, F-77454, Marne-la-Vallée, France

Abstract

A permutation is said to be a square if it can be obtained by shuffling two order-isomorphic patterns. The definition is intended to be the natural counterpart to the ordinary shuffle of words and languages. In this paper, we tackle the problem of recognizing square permutations from both the point of view of algebra and algorithms. On the one hand, we present some algebraic and combinatorial properties of the shuffle product of permutations. We follow an unusual line consisting in defining the shuffle of permutations by means of an unshuffling operator, known as a coproduct. This strategy allows to obtain easy proofs for algebraic and combinatorial properties of our shuffle product. We besides exhibit a bijection between square (213, 231)-avoiding permutations and square binary words. On the other hand, by using a pattern avoidance criterion on directed perfect matchings, we prove that recognizing square permutations is NP-complete.

Contents

1 Notations and basic definitions 3
2 Shuffle product on permutations 7
3 Binary square words and permutations 9
4 Algebraic issues 10
5 Algorithmic issues 14
6 Conclusion and perspectives 31

This paper is an extended version of [GV16].

Email addresses: samuele.giraudo@u-pem.fr (Samuele Giraudo), stephane.vialette@u-pem.fr (Stéphane Vialette)
Introduction

The shuffle product, denoted by $\shuffle$, is a well-known operation on words first defined by Eilenberg and Mac Lane [EML53]. Given three words $u$, $v_1$, and $v_2$, $u$ is said to be a shuffle of $v_1$ and $v_2$ if it can be formed by interleaving the letters from $v_1$ and $v_2$ in a way that maintains the left-to-right ordering of the letters from each word. Besides purely combinatorial questions, the shuffle product of words naturally leads to the following computational problems:

(i) Given two words $v_1$ and $v_2$, compute the set $v_1 \shuffle v_2$.
(ii) Given three words $u$, $v_1$, and $v_2$, decide if $u$ is a shuffle of $v_1$ and $v_2$.
(iii) Given words $u$, $v_1$, …, $v_k$, decide if $u$ is in $v_1 \shuffle \cdots \shuffle v_k$.
(iv) Given a word $u$, decide if there is a word $v$ such that $u$ is in $v \shuffle v$.

Even if these problems seem similar, they radically differ in terms of time complexity. Let us now review some facts about these. In what follows, $n$ denotes the size of $u$ and $m_i$ denotes the size of each $v_i$. A solution to Problem (i) can be computed in $O((m_1 + m_2)(m_1 + m_2))$ time [Spe86]. An improvement and a generalization of Problem (i) has been proposed in [All00], where it is proven that given words $v_1$, …, $v_k$, the iterated shuffle $v_1 \shuffle \cdots \shuffle v_k$ can be computed in $O((m_1 + \cdots + m_k)_{m_1, \ldots, m_k})$ time. Problem (ii) is in $\mathcal{P}$; it is indeed a classical textbook exercise to design an efficient dynamic programming algorithm solving it. It can be tested in $O(n^2/\log(n))$ time [vLN82].

To the best of our knowledge, the first $O(n^2)$ time algorithm for this problem appeared in [Man83]. This algorithm can easily be extended to check in polynomial-time whether a word is in the shuffle of any fixed number of given words. Nevertheless, Problem (iii) is $\mathcal{NP}$-complete [Man83, WH84]. This remains true even if the ground alphabet has size 3 [WH84]. Of particular interest, it is shown in [WH84] that Problem (iii) remains $\mathcal{NP}$-complete even if all the words $v_i$, $i \in [k]$, are identical, thereby proving that, for two words $u$ and $v$, it is $\mathcal{NP}$-complete to decide whether or not $u$ is in the iterated shuffle of $v$. Again, this remains true even if the ground alphabet has size 3. Let us now finally focus on Problem (iv). It is shown in [BS14, RV13] that it is $\mathcal{NP}$-complete to decide if a word $u$ is a square (w.r.t. the shuffle), that is, a word $u$ with the property that there exists a word $v$ such that $u$ is a shuffle of $v$ with itself. Hence, Problem (iv) is $\mathcal{NP}$-complete.

This paper is intended to study a natural generalization of $\shuffle$, denoted by $\bullet$, as a shuffle of permutations. Roughly speaking, given three permutations $\pi$, $\sigma_1$, and $\sigma_2$, $\pi$ is said to be a
shuffle of \( \sigma_1 \) and \( \sigma_2 \) if \( \pi \) (viewed as a word) is a shuffle of two words that are order-isomorphic to \( \sigma_1 \) and \( \sigma_2 \). This shuffle product was first introduced by Vargas [Var14] under the name of supershuffle. Our intention in this paper is to study this shuffle product of permutations \( \bullet \) both from a combinatorial and from a computational point of view by focusing on square permutations, that are permutations \( \pi \) being in the shuffle of a permutation \( \sigma \) with itself. Many other shuffle products on permutations appear in the literature. For instance, in [DHT02], the authors define the convolution product and the shifted shuffle product. For this last product, \( \pi \) is a shuffle of \( \sigma_1 \) and \( \sigma_2 \) if \( \pi \) is in the shuffle, as words, of \( \sigma_1 \) and the word obtained by incrementing all the letters of \( \sigma_2 \) by the size of \( \sigma_1 \). It is a simple exercise to prove that, given three permutations \( \pi, \sigma_1, \) and \( \sigma_2 \), deciding if \( \pi \) is in the shifted shuffle of \( \sigma_1 \) and \( \sigma_2 \) is in \( \mathbb{P} \).

This paper is organized as follows. In Section 2, we provide a precise definition of \( \bullet \). We shall define \( \bullet \) in terms of what we call the unshuffling operator \( \Delta \). The operator \( \Delta \) is in fact a coproduct, endowing the linear span of all permutations with a coalgebra structure (see [JR79] or [GR14] for the definition of these algebraic structures). By duality, the unshuffling operator \( \Delta \) leads to the definition of our shuffle operation on permutations. This approach has many advantages. First, some combinatorial properties of \( \bullet \) depend on properties of \( \Delta \) and those properties are easier to prove on the coproduct side. Second, this approach allows us to obtain a clear description of the multiplicities of the elements appearing in the shuffle of two permutations, which are of interest in their own right from a combinatorial point of view. Section 3 is devoted to showing that the problems related to the shuffle of words has links with the shuffle of permutations. In particular, we show that binary words that are square are in one-to-one correspondence with square permutations avoiding some patterns (Proposition 3.1). Next, Section 4 presents some algebraic and combinatorial properties of \( \bullet \). We show that \( \bullet \) is associative and commutative (Proposition 4.1), and that if a permutation is a square, its mirror, complement, and inverse are also squares (Proposition 4.3). Finally, Section 5 presents the most important result of this paper: the fact that deciding if a permutation is a square is \( \mathsf{NP} \)-complete (Proposition 5.10). This result is obtained by exhibiting a reduction from the \( \mathsf{NP} \)-complete pattern involvement problem [BBL98].

1. Notations and basic definitions

**General notations**

If \( S \) is a finite set, the cardinality of \( S \) is denoted by \(|S|\), and if \( P \) and \( Q \) are two disjoint sets, \( P \sqcup Q \) denotes the disjoint union of \( P \) and \( Q \). For any nonnegative integer \( n \), \([n]\) is the set \( \{1, \ldots, n\} \).

**Words and permutations**

We follow the usual terminology on words [CK97]. Let us recall here the most important ones. Let \( u \) be a word. The length of \( u \) (also called size) is denoted by \(|u|\). The empty word,
the only word of null length, is denoted by $\epsilon$. We denote by $\bar{u}$ the mirror image of $u$, that is the word $u_{|u|}u_{|u|-1} \ldots u_1$. If $P$ is a subset of $[|u|]$, $u_P$ is the subword of $u$ consisting in the letters of $u$ at the positions specified by the elements of $P$. If $u$ is a word of integers and $k$ is an integer, we denote by $u[k]$ the word obtained by incrementing by $k$ all letters of $u$. The shuffle of two words $u$ and $v$ is the set recursively defined by

$$
u \sqcup \epsilon = \{u\} = \epsilon \sqcup u$$

and

$$ua \sqcup vb = (u \sqcup vb) a \cup (ua \sqcup v)b,$$

were $a$ and $b$ are letters. For instance,

$$01 \sqcup 20 = \{0120, 0210, 0201, 2010, 2001\}.$$  

A word $u$ is a square if there exists a word $v$ such that $u$ belongs to $v \sqcup v$. For example, $01202101$ is a square since this word belongs to the set $201 \sqcup 201$.

We denote by $S_n$ the set of permutations of size $n$ and by $S$ the set of all permutations. In this paper, permutations of a size $n$ are specified by words of length $n$ on the alphabet $[n]$ and without multiple occurrences of a letter, so that all above definitions about words remain valid on permutations. The only difference lies on the fact that we shall denote by $\pi(i)$ (instead of $\pi_i$) the $i$-th letter of any permutation $\pi$. For any nonnegative integer $n$, we write $\pi_n$ (resp. $\pi_{\downarrow n}$) for the permutation $12 \ldots n$ (resp. $n(n-1) \ldots 1$). If $\pi$ is a permutation of $S_n$, we denote by $\bar{\pi}$ the complement of $\pi$, that is the permutation satisfying $\bar{\pi}(i) = n - \pi(i) + 1$ for all $i \in [n]$. The inverse of $\pi$ is denoted by $\pi^{-1}$.

If $u$ is a word of integers where no letter occurs more than once, we define the standardization of $u$, $s(u)$, to be the unique permutation of the same size as $u$ such that for all $i, j \in [|u|]$, $u_i < u_j$ if and only if $s(u)(i) < s(u)(j)$. For instance,

$$s(814637) = 613425.$$  

In particular, the image of the map $s$ is the set $S$ of all permutations. Two words $u$ and $v$ having the same standardization are order-isomorphic. If $\sigma$ is a permutation, we say that $\sigma$ occurs in $\pi$ if there is a set of indices $P$ of $[|\pi|]$ such that $\sigma$ and $\pi_P$ are order isomorphic. When $\sigma$ does not occur in $\pi$, $\pi$ is said to avoid $\sigma$. The set of permutations of size $n$ avoiding $\sigma$ is denoted by $S_n(\sigma)$. The pattern involvement problem consists, given two permutations $\pi$ and $\sigma$, in deciding if $\sigma$ occurs in $\pi$. This problem is known to be NP-complete [BBL98].

Directed perfect matchings

A directed graph is an ordered pair $G = (V, A)$ where $V$ is a set whose elements are called vertices and $A$ is a set of ordered pairs of vertices, called arcs (from a source vertex to a sink vertex). In this paper, we shall exclusively use $V \subset \mathbb{N}$. Notice that the aforementioned definition does not allow a directed graph to have multiple arcs with same source and target.
nodes. We shall not allow directed loops (that is, arcs that connect vertices with themselves). Two arcs are independent if they do not have a common vertex. An arc \((i, i')\) contains an arc \((j, j')\) if \(\min(i, i') < \min(j, j') < \max(j, j') < \max(i, i')\). If no arc of \(\mathcal{G}\) contains an other arc, we say that \(\mathcal{G}\) is containment-free. Two arcs \((i, i')\) and \((j, j')\) are crossing if \(\min(i, i') < \min(j, j') < \max(i, i') < \max(j, j')\). If no arcs of \(\mathcal{G}\) are crossing, we say that \(\mathcal{G}\) is crossing-free. A directed graph is a directed matching if all its arcs are independent. A directed matching is perfect if every vertex is either a source or a sink.

For any permutation \(\pi\) of an even size \(2n\), a directed perfect matching on \(\pi\) is a pair \(\mathcal{M} = (\mathcal{G}, \pi)\) where \(\mathcal{G}\) is a directed perfect matching on the set \([2n]\) of vertices (see Figure 1). The word of sources (resp. word of sinks) of \(\mathcal{M}\) is the subword \(\pi(i_1)\pi(i_2) \ldots \pi(i_n)\) of \(\pi\) where the indexes \(i_1 < i_2 < \cdots < i_n\) are the sources (resp. sinks) of the arcs of \(\mathcal{M}\). Figure 2 shows an example for these notions.

---

**Figure 1:** A directed perfect matching \(\mathcal{M}\) on the permutation \(\pi = 37268541\), represented on the permutation matrix of \(\pi\). The set of vertices of \(\mathcal{M}\) is \(\{1, \ldots, 8\}\) and the set of arcs of \(\mathcal{M}\) is \(\{(1, 5), (3, 2), (4, 8), (7, 6)\}\).

**Figure 2:** A directed perfect matching \(\mathcal{M}\) on the permutation \(\pi = 41328576\). The word of sources of \(\mathcal{M}\) is \(4327\) and its word of sinks is \(1856\). Unlike in Figure 1, \(\mathcal{M}\) is not drawn on the permutation matrix of \(\pi\).
tions together with the notions of occurrences of patterns accompanying them. Let \( \pi \) be a permutation of size \( 2n \) and \( \mathcal{M} = (\mathcal{G}, \pi) \) be a directed perfect matching on \( \pi \).

1. An unlabeled pattern is a directed perfect matching \( U = ([k], A) \), where \( k \leq n \). We say that \( \mathcal{M} \) contains an unlabeled occurrence of \( U \) if there is an increasing map \( \phi : [k] \to [2n] \) (i.e., \( i < j \in [k] \) implies \( \phi(i) < \phi(j) \)) such that, if \( (i, i') \) is an arc of \( U \) then \( (\phi(i), \phi(i')) \) is an arc of \( \mathcal{G} \). Observe that this first notion of pattern occurrence does not depend on the permutation \( \pi \). In other words, \( \mathcal{M} \) contains an unlabeled occurrence of \( U \) if \( \mathcal{G} \) contains a copy of \( U \) as a subgraph by changing some of its labels if necessary.

2. A labeled pattern is a directed perfect matching \( P = (U, \sigma) \) on a permutation \( \sigma \) of size \( 2k \). We say that \( \mathcal{M} \) contains a labeled occurrence of \( P \) if \( \mathcal{M} \) contains an unlabeled occurrence of the directed perfect matching \( U = ([k], A) \) such that \( s(\pi(\phi(1)))\pi(\phi(2)) \cdots \pi(\phi(2k))) = \sigma \), where \( \phi \) is a map defined as above. In other words, \( \mathcal{M} \) contains a labeled occurrence of \( P \) if \( \mathcal{G} \) contains a copy of \( U \) as a subgraph and the word consisting in the letters of \( \pi \) associated with each vertices of this copy in \( \mathcal{G} \) is order-isomorphic to \( \sigma \).

When \( \mathcal{M} \) does not contain any unlabeled occurrence (resp. labeled occurrence) of an unlabeled pattern \( U \) (resp. labeled pattern \( P \)), we say that \( \mathcal{M} \) avoids \( U \) (resp. \( P \)). This definition naturally extends to sets of patterns by setting that \( \mathcal{M} \) avoids the set of unlabeled patterns (resp. labeled patterns) \( U = \{U_1, \ldots, U_\ell\} \) (resp. \( P = \{P_1, \ldots, P_\ell\} \)) if \( \mathcal{M} \) avoids every \( U_i \) of \( U \) (resp. \( P_i \) of \( P \)).

In this paper, we shall consider only patterns of size 4. The set of all unlabeled patterns of this size is

\[
\mathcal{P} = \mathcal{P}_{\text{pre}} \cup \mathcal{P}_{\text{cont}} \cup \mathcal{P}_{\text{cros}},
\]

where

\[
\mathcal{P}_{\text{pre}} = \{[\text{，，，}],[\text{，，，}],[\text{，，，}],[\text{，，，}]\}, \quad (1.6)
\]

\[
\mathcal{P}_{\text{cont}} = \{[\text{，，，}],[\text{，，，}],[\text{，，，}],[\text{，，，}]\}, \quad (1.7)
\]

\[
\mathcal{P}_{\text{cros}} = \{[\text{，，，}],[\text{，，，}],[\text{，，，}],[\text{，，，}]\}. \quad (1.8)
\]

In these drawings, the vertices of each pattern are implicitly indexed from left to right by 1 to 4. Besides, any labeled pattern \( \mathcal{P} = (U, \sigma) \) is depicted by drawing \( U \) and by labeling all its vertices \( i \) by \( \sigma_i \).

To give some examples of the previous notions, observe that a directed perfect matching \( \mathcal{M} \) on a permutation contains an occurrence of the unlabeled pattern \( \text{，，，} \) if there are four vertices \( i_1 < i_2 < i_3 < i_4 \) of \( \mathcal{M} \) such that \( (i_1, i_4) \) and \( (i_3, i_2) \) are arcs of \( \mathcal{M} \). Moreover, \( \mathcal{M} \) is containment-free (resp. crossing-free) if it avoids all patterns of \( \mathcal{P}_{\text{cont}} \) (resp. \( \mathcal{P}_{\text{cros}} \)). For example, the directed perfect matching on the permutation of Figure 2

- contains exactly two unlabeled occurrences of the pattern \( \text{，，，} \) corresponding to the arcs \((1, 6)\) and \((4, 2)\), or \((3, 8)\) and \((7, 5)\);
contains exactly one unlabeled occurrence of \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs (4, 2) and (3, 8);

- avoids the unlabeled pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \).

The directed perfect matching on the permutation of Figure 1

- contains a labeled occurrence of the pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs (1, 5) and (3, 2);

- contains a labeled occurrence of the pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs (1, 5) and (4, 8);

- contains a labeled occurrence of the pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs arcs (1, 5) and (7, 6);

- contains a labeled occurrence of the pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs (3, 2) and (7, 6);

- contains a labeled occurrence of the pattern \( \begin{array}{c} 2 \\ \hline \\ 1 \end{array} \) corresponding to the arcs (4, 8) and (7, 6);

- avoids all other labeled patterns of size 4.

2. Shuffle product on permutations

The main purpose of this section is to give a formal definition of the shuffle product on permutations. We shall define \( \bullet \) by first defining a co-product called the unshuffling operator \( \Delta \) on permutations. Then \( \bullet \) is defined to be the dual of \( \Delta \). The reason that we define \( \bullet \) in terms of \( \Delta \) is due to the fact that many properties of \( \bullet \) depend on properties of \( \Delta \) and those properties are easier to prove on the co-product side. We invite the reader unfamiliar with the concepts of coproduct and duality to consult [JR79] or [GR14].

Let us denote by \( Q[S] \) the linear span of all permutations. We define a linear coproduct \( \Delta \) on \( Q[S] \) in the following way. For any permutation \( \pi \), we set

\[
\Delta(\pi) = \sum_{P_1 \cup P_2 = |\pi|} s(\pi|_{P_1}) \otimes s(\pi|_{P_2}). \tag{2.1}
\]

We call \( \Delta \) the unshuffling coproduct of permutations. For instance,

\[
\Delta(213) = \epsilon \otimes 213 + 2 \cdot 1 \otimes 12 + 1 \otimes 21 + 2 \cdot 12 \otimes 1 + 21 \otimes 1 + 213 \otimes \epsilon, \tag{2.2}
\]
$$\Delta(1234) = \epsilon \otimes 1234 + 4 \cdot 1 \otimes 123 + 6 \cdot 12 \otimes 12 + 4 \cdot 123 \otimes 1 + 1234 \otimes \epsilon,$$

$$\Delta(1432) = \epsilon \otimes 1432 + 3 \cdot 1 \otimes 132 + 1 \otimes 321 + 3 \cdot 12 \otimes 21 + 3 \cdot 21 \otimes 12 + 3 \cdot 132 \otimes 1 + 321 \otimes 1 + 1432 \otimes \epsilon.$$  \hfill (2.3)

Observe that the coefficient of the tensor $1 \otimes 132$ is 3 in (2.4) because there are exactly three ways to extract from the permutation 1432 two disjoint subwords which are, respectively, order-isomorphic to the permutations 1 and 132.

We can now define our shuffle product $\bullet$ as the product that corresponds to the co-product $\Delta$ under duality. From (2.1), for any permutation $\pi$, we have

$$\Delta(\pi) = \sum_{\sigma, \nu \in S} \lambda^{\pi}_{\sigma, \nu} \sigma \otimes \nu,$$

where the $\lambda^{\pi}_{\sigma, \nu}$ are nonnegative integers. By the definition (2.1) of $\Delta$, the $\lambda^{\pi}_{\sigma, \nu}$ are equal to the number of different ways to extract from $\pi$ two disjoint subwords respectively order-isomorphic to $\sigma$ and $\nu$. Now, by definition of duality, the dual product of $\Delta$, denoted by $\bullet$, is a linear binary product on $\mathbb{Q}[S]$. It satisfies, for any permutations $\sigma$ and $\nu$,

$$\sigma \bullet \nu = \sum_{\pi \in S} \lambda^{\pi}_{\sigma, \nu} \pi,$$

where the coefficients $\lambda^{\pi}_{\sigma, \nu}$ are the ones of (2.5). We call $\bullet$ the shuffle product of permutations. For instance,

$$12 \bullet 21 = 1243 + 1324 + 2 \cdot 1342 + 2 \cdot 1423 + 3 \cdot 1432 + 2134 + 2 \cdot 2314 + 6 \cdot 2341 + 3 \cdot 2431 + 2 \cdot 3124 + 3 \cdot 3142 + 3 \cdot 3214 + 2 \cdot 3241 + 3 \cdot 4123 + 2 \cdot 4132 + 2 \cdot 4213 + 4231 + 4312.$$

Observe that the coefficient 3 of the permutation 1432 in (2.7) comes from the fact that the coefficient of the tensor $1 \otimes 132$ is 3 in (2.4).

Intuitively, the product $\bullet$ shuffles the values and the positions of the letters of the permutations. One can observe that the empty permutation $\epsilon$ is a unit for $\bullet$ and that this product is graded by the sizes of the permutations (i.e., the product of a permutation of size $n$ with a permutation of size $m$ produces a sum of permutations of size $n + m$).

We say that a permutation $\pi$ appears in the shuffle $\sigma \bullet \nu$ of two permutations $\sigma$ and $\nu$ if the coefficient $\lambda^{\pi}_{\sigma, \nu}$ defined above is different from zero. In a more combinatorial way, this is equivalent to say that there are two sets $P_1$ and $P_2$ of disjoints indexes of letters of $\pi$ satisfying $P_1 \cup P_2 = |\pi|$ such that the subword $\pi|_{P_1}$ is order-isomorphic to $\sigma$ and the subword $\pi|_{P_2}$ is order-isomorphic to $\nu$.

A permutation $\pi$ is a square if there is a permutation $\sigma$ such that $\pi$ appears in $\sigma \bullet \sigma$. In this case, we say that $\sigma$ is a square root of $\pi$. Equivalently, $\pi$ is a square with $\sigma$ as square root if and only if in the expansion of $\Delta(\pi)$, there is a tensor $\sigma \otimes \sigma$ with a nonzero coefficient. In a more combinatorial way, this is equivalent to saying that there are two sets $P_1$ and $P_2$
of disjoints indexes of letters of $\pi$ satisfying $P_1 \sqcup P_2 = [\pi]$ such that the subwords $\pi|_{P_1}$ and $\pi|_{P_2}$ are order-isomorphic. Computer experiments give us the first numbers of square permutations with respects to their size, which are, from size 0 to 10,

$$1, 0, 2, 0, 20, 0, 504, 0, 21032, 0, 1293418.$$  \hfill (2.8)

This sequence (and its subsequence obtained by removing the 0’s) is for the time being not listed in [Slo]. The first square permutations are listed in Table 1.

<table>
<thead>
<tr>
<th>Size 0</th>
<th>Size 2</th>
<th>Size 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\epsilon$</td>
<td>12, 21</td>
<td>1234, 1243, 1423, 1324, 1342, 4132, 3142, 3124, 3412, 3421, 4312, 4321</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2134, 2143, 2413, 4213, 2314, 2431, 4231, 3241, 3421, 4321</td>
</tr>
</tbody>
</table>

Table 1: The square permutations of sizes 0 to 4.

3. Binary square words and permutations

In this section, we shall show that the square binary words are in one-to-one correspondence with square permutations avoiding some patterns. This property establishes a link between the shuffle of binary words and our shuffle of permutations and allows us to obtain a new description of square binary words.

Let $u$ be a binary word of length $n$ with $k$ occurrences of 0. We denote by $\text{btp}$ (Binary word To Permutation) the map sending any such word $u$ to the permutation obtained by replacing from left to right each occurrence of 0 in $u$ by 1, 2, ..., $k$, and from right to left each occurrence of 1 in $u$ by $k + 1$, $k + 2$, ..., $n$. For instance,

$$\text{btp}(1001011000) = \text{C12B3A948567},$$  \hfill (3.1)

where A, B, and C respectively stand for 10, 11, and 12. Observe that for any nonempty permutation $\pi$ in the image of $\text{btp}$, there is exactly one binary word $u$ such that $\text{btp}(u0) = \text{btp}(u1) = \pi$. In support of this observation, when $\pi$ has an even size, we denote by $\text{ptb}(\pi)$ (Permutation To Binary word) the word $ua$ such that $|ua|_0$ and $|ua|_1$ are both even, where $a \in \{0, 1\}$. For instance,

$$\text{ptb}(615423) = 101100 \quad \text{and} \quad \text{ptb}(1423) = 0101.$$  \hfill (3.2)

**Proposition 3.1.** For any $n \geq 0$, the map $\text{btp}$ restricted to the set of square binary words of length $2n$ is a bijection between this last set and the set of square permutations of size $2n$ avoiding the patterns 213 and 231.

**Proof of Proposition 3.1.** The statement of the proposition is a consequence of the following claims implying that $\text{ptb}$ is the inverse map of $\text{btp}$ over the set of square binary words.

**Claim 3.2.** The image of $\text{btp}$ is the set of all permutations avoiding 213 and 231.
Proof of Claim 3.2. Let us first show that the image of btp contains only permutations avoiding 213 and 231. Let $u$ be a binary word, $\pi = \text{btp}(u)$, and $P_0$ (resp. $P_1$) be the set of the positions of the occurrences of 0 (resp. 1) in $u$. By definition of btp, from left to right, the subword $v = \pi|_{P_0}$ is increasing and the subword $w = \pi|_{P_1}$ is decreasing, and all letters of $w$ are greater than those of $v$. Now, assume that 123 occurs in $\pi$. Then, since $v$ is increasing and $w$ is decreasing, there is an occurrence of 3 (resp. 13, 23) in $v$ and a relative occurrence of 21 (resp. 2, 1) in $w$. All these three cases contradict the fact that all letters of $w$ are greater than those of $v$. A similar argument shows that $\pi$ avoids 231 as well.

Finally, observe that any permutation $\pi$ avoiding 213 and 231 necessarily starts by the smallest possible letter or the greatest possible letter. This property is then true for the suffix of $\pi$ obtained by deleting its first letter, and so on for all of its suffixes. Thus, by replacing each letter $a$ of $\pi$ by 0 (resp. 1) if $a$ has the role of a smallest (resp. greatest) letter, one obtains a binary word $u$ such that $\text{btp}(u) = \pi$. Hence, all permutations avoiding 213 and 231 are in the image of btp.

Claim 3.3. If $u$ is a square binary word, $\text{btp}(u)$ is a square permutation.

Proof of Claim 3.3. Since $u$ is a square binary word, there is a binary word $v$ such that $u \in v \cup v$. Then, there are two disjoint sets $P$ and $Q$ of positions of letters of $u$ such that $u|_{P} = v = u|_{Q}$. Now, by definition of btp, the words $\text{btp}(u)|_{P}$ and $\text{btp}(u)|_{Q}$ have the same standardization $\sigma$. Hence, and by definition of the shuffle product of permutations, $\text{btp}(u)$ appears in $\sigma \cdot \sigma$, showing that $\text{btp}(u)$ is a square permutation.

Claim 3.4. If $\pi$ is a square permutation avoiding 213 and 231, $\text{ptb}(\pi)$ is a square binary word.

Proof of Claim 3.4. Let $\pi$ be a square permutation avoiding 213 and 231. By Claim 3.2, $\pi$ is in the image of btp and hence, $u = \text{ptb}(\pi)$ is a well-defined binary word. Since $\pi$ is a square permutation, there are two disjoint sets $P_1$ and $P_2$ of indexes of letters of $\pi$ such that $\pi|_{P_1}$ and $\pi|_{P_2}$ are order-isomorphic. This implies, by the definitions of btp and ptb, that $u|_{P_1} = u|_{P_2}$, showing that $u$ is a square binary word.

This ends the proof of Proposition 3.1.

The number of square binary words is Sequence A191755 of Slo beginning by

$$1, 0, 4, 0, 6, 22, 0, 82, 0, 320, 0, 1268, 0, 5102, 0, 020632. \quad (3.3)$$

According to Proposition 3.1, this is also the sequence enumerating square permutations avoiding 213 and 231. Notice that it is conjectured in [HRS12] that the number of square binary words of length $2n$ is $\left(\binom{2n}{n}\right) \frac{2^n}{n+1} - \left(\binom{2n-1}{n-1}\right) 2^{n-1} + O(2^{n-2})$.

4. Algebraic issues

The aim of this section is to establish some of properties of the shuffle product of permutations $\bullet$. It is worth to note that, as we will see, algebraic properties of the unshuffling coproduct $\Delta$ of permutations defined in Section 2 lead to combinatorial properties of $\bullet$.

Proposition 4.1. The shuffle product $\bullet$ of permutations is associative and commutative.
Proof of Proposition 4.1. To prove the associativity of $\bullet$, it is convenient to show that its dual coproduct $\Delta$ is coassociative, that is

$$(\Delta \otimes I) \Delta = (I \otimes \Delta) \Delta,$$  

(4.1)

where $I$ denotes the identity map. This strategy relies on the fact that a product is associative if and only if its dual coproduct is coassociative. For any permutation $\pi$, we have

$$(\Delta \otimes I) \Delta (\pi) = \sum_{P_1 \cup P_2 = ||\pi||} s (\pi|_{P_1}) \otimes s (\pi|_{P_2})$$

(4.2)

An analogous computation shows that $(I \otimes \Delta) \Delta (\pi)$ is equal to the last member of (4.2), whence the associativity of $\bullet$.

Finally, to prove the commutativity of $\bullet$, we shall show that $\Delta$ is cocommutative, that is, for any permutation $\pi$, if in the expansion of $\Delta (\pi)$ there is a tensor $\sigma \otimes \nu$ with a coefficient $\lambda$, there is in the same expansion the tensor $\nu \otimes \sigma$ with the same coefficient $\lambda$. Clearly, a product is commutative if and only if its dual coproduct is cocommutative. Now, from the definition (2.1) of $\Delta$, one observes that if the pair $(P_1, P_2)$ of subsets of $||\pi||$ contributes to the coefficient of $s (\pi|_{P_1}) \otimes s (\pi|_{P_2})$, the pair $(P_2, P_1)$ contributes to the coefficient of $s (\pi|_{P_2}) \otimes s (\pi|_{P_1})$. This shows that $\Delta$ is cocommutative and hence, that $\bullet$ is commutative. \hfill \Box

Proposition 4.1 shows that $\mathbb{Q}[S]$ under the unshuffling coproduct $\Delta$ is a co-associative co-commutative coalgebra which implies, by duality, that $\mathbb{Q}[S]$ under $\bullet$ is an associative commutative algebra

Lemma 4.2. The three linear maps

$$\phi_1, \phi_2, \phi_3 : \mathbb{Q}[S] \to \mathbb{Q}[S]$$

(4.3)

linearly sending a permutation $\pi$ to, respectively, $\bar{\pi}$, $\bar{\pi}$, and $\pi^{-1}$ are endomorphisms of associative algebras.

Proof of Lemma 4.2. To prove, for $j = 1, 2, 3$, that $\phi_j$ is a morphism of associative algebras, we have to prove that for all permutations $\sigma$ and $\nu$,

$$\phi_j (\sigma \bullet \nu) = \phi_j (\sigma) \bullet \phi_j (\nu).$$

(4.4)

By duality, this is equivalent to showing that $\phi_j$ is a morphism of coalgebras, that is,

$$\Delta \phi_j = (\phi_j \otimes \phi_j) \Delta.$$ 

(4.5)

In the sequel, $\pi$ is a permutation.

If $P$ is a set of indexes of letters of $\pi$, we denote by $\bar{P}$ the set $\{||\pi|| - i + 1 : i \in P\}$. Now, since the operation $\bar{\cdot}$ defines a bijection on the set of the subsets of $||\pi||$, and since the
standardization operation commutes with the mirror operation on words without multiple occurrence of a letter, we have
\[
\Delta(\phi_1(\pi)) = \sum_{p_1 \cup p_2 = |\pi|} s(\phi_1(\pi)|p_1) \otimes s(\phi_1(\pi)|p_2)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} s(\bar{\pi}|p_1) \otimes s(\bar{\pi}|p_2)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} s(\bar{\pi}|p_1) \otimes s(\bar{\pi}|p_2)
\]
\[
(4.6)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} \phi_1(s(\pi|p_1)) \otimes s(\pi|p_2)
\]
\[
= (\phi_1 \otimes \phi_1)\Delta(\pi).
\]
This shows that \(\phi_1\) is a morphism of coalgebras and hence, that \(\phi_1\) is a morphism of associative algebras.

Next, since by definition of the complementation operation on permutations, for any permutation \(\tau\) and any indexes \(i\) and \(k\), we have \(\tau(i) < \tau(k)\) if and only if \(\bar{\tau}(i) > \bar{\tau}(k)\), we have
\[
\Delta(\phi_2(\pi)) = \sum_{p_1 \cup p_2 = |\pi|} s(\phi_2(\pi)|p_1) \otimes s(\phi_2(\pi)|p_2)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} s(\bar{\pi}|p_1) \otimes s(\bar{\pi}|p_2)
\]
\[
(4.7)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} \phi_2(s(\pi|p_1)) \otimes s(\pi|p_2)
\]
\[
= (\phi_2 \otimes \phi_2)\Delta(\pi).
\]
This shows that \(\phi_2\) is a morphism of coalgebras and hence, that \(\phi_2\) is a morphism of associative algebras.

Finally, for any permutation \(\tau\), if \(P\) is a set of indexes of letters of \(\tau\), we denote by \(P^{-1}_\tau\) the set \(\{\tau(i) : i \in P\}\). Since the map sending a subset \(P\) of \(|\pi|\) to \(P^{-1}_\tau\) is a bijection, and since \(s(\pi|\mu)^{-1} = s(\pi^{-1}|P^{-1}_\tau)\), we have
\[
\Delta(\phi_3(\pi)) = \sum_{p_1 \cup p_2 = |\pi|} s(\phi_3(\pi)|p_1) \otimes s(\phi_3(\pi)|p_2)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} s(\pi^{-1}|p_1) \otimes s(\pi^{-1}|p_2)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} s(\pi^{-1}|p_1) \otimes s(\pi^{-1}|p_2)
\]
\[
(4.8)
\]
\[
= \sum_{p_1 \cup p_2 = |\pi|} \phi_3(s(\pi|p_1)) \otimes s(\pi|p_2)
\]
\[
= (\phi_3 \otimes \phi_3)\Delta(\pi).
\]
This shows that $\phi_3$ is a morphism of coalgebras and hence, that $\phi_3$ is a morphism of associative algebras.

We now use the algebraic properties of $\bullet$ exhibited by Lemma 4.2 to obtain combinatorial properties of square permutations.

**Proposition 4.3.** Let $\pi$ be a square permutation and $\sigma$ be a square root of $\pi$. Then,

(i) the permutation $\bar{\pi}$ is a square and $\bar{\sigma}$ is one of its square roots;

(ii) the permutation $\bar{\pi}$ is a square and $\bar{\sigma}$ is one of its square roots;

(iii) the permutation $\pi^{-1}$ is a square and $\sigma^{-1}$ is one of its square roots.

**Proof of Proposition 4.3.** All statements (i), (ii), and (iii) are consequences of Lemma 4.2. Indeed, since $\pi$ is a square permutation and $\sigma$ is a square root of $\pi$, by definition, $\pi$ appears in the product $\sigma \bullet \sigma$. Now, by Lemma 4.2, for any $j = 1, 2, 3$, since $\phi_j$ is a morphism of associative algebras from $\mathbb{Q}[S]$ to $\mathbb{Q}[S]$, $\phi_j$ commutes with the shuffle product of permutations $\bullet$. Hence, in particular, one has

$$\phi_j(\sigma \bullet \sigma) = \phi_j(\sigma) \bullet \phi_j(\sigma). \quad (4.9)$$

Then, since $\pi$ appears in $\sigma \bullet \sigma$, $\phi_j(\pi)$ appears in $\phi_j(\sigma \bullet \sigma)$ and appears also in $\phi_j(\sigma) \bullet \phi_j(\sigma)$. This shows that $\phi_j(\sigma)$ is a square root of $\phi_j(\pi)$ and implies (i), (ii), and (iii).

Let us make an observation about Wilf-equivalence classes of permutations restrained on square permutations. Recall that two permutations $\sigma$ and $\nu$ of the same size are Wilf equivalent if $|S_n(\sigma)| = |S_n(\nu)|$ for all $n \geq 0$. The well-known [SS85] fact that there is a single Wilf-equivalence class of permutations of size 3 together with Proposition 4.3 imply that 123 and 321 are in the same Wilf-equivalence class of square permutations, and that 132, 213, 231, and 312 are in the same Wilf-equivalence class of square permutations. Computer experiments show us that there are two Wilf-equivalence classes of square permutations of size 3. Indeed, the number of square permutations avoiding 123 begins by

$$1, 0, 2, 0, 12, 0, 118, 0, 1218, 0, 14272, \quad (4.10)$$

while the number of square permutations avoiding 132 begins by

$$1, 0, 2, 0, 11, 0, 84, 0, 743, 0, 7108. \quad (4.11)$$

Another consequence of Proposition 4.3 is that its makes sense to enumerate the sets of square permutations quotiented by the operations of mirror image, complement, and inverse. The sequence enumerating these sets begins by

$$1, 0, 1, 0, 6, 0, 81, 0, 2774, 0, 162945. \quad (4.12)$$

All Sequences (4.10), (4.11), and (4.12) (and their subsequences obtained by removing the 0s) are for the time being not listed in [Slo].
5. Algorithmic issues

This section is devoted to proving the NP-hardness of recognizing square permutations. As in the case of words, we shall use a linear graph framework where deciding whether a permutation is a square reduces to computing some specific matching in the associated linear graph [RV13, BS14]. We have, however, to deal with directed graphs/perfect matchings satisfying some precise properties. Let us first define two properties.

**Definition 5.1 (Property $P_1$).** Let $\pi$ be a permutation. A directed perfect matching $M$ on $\pi$ is said to have property $P_1$ if it avoids the following set of unlabeled patterns:

$$P_1 = \left\{ \begin{array}{c}
\begin{array}{c}
\text{pattern 1} \\
\text{pattern 2} \\
\text{pattern 3} \\
\text{pattern 4} \\
\text{pattern 5} \\
\text{pattern 6}
\end{array}
\end{array} \right\}. \quad (5.1)$$

Observe that the unlabeled patterns of $P_1$ are the four of $P_{\text{cont}}$ and the two of $P_{\text{cros}}$ that have crossing edges in the opposite directions.

**Definition 5.2 (Property $P_2$).** Let $\pi$ be a permutation. A directed perfect matching $M$ on $\pi$ is said to have property $P_2$ if, for any two distinct arcs $(i, i')$ and $(j, j')$ of $M$, we have $\pi(i) < \pi(j)$ if and only if $\pi(i') < \pi(j')$.

The rationale for introducing properties $P_1$ and $P_2$ stems from the following lemma.

**Lemma 5.3.** Let $\pi$ be a permutation. The following statements are equivalent:

(i) The permutation $\pi$ is a square.

(ii) There exists a directed perfect matching $M$ on $\pi$ satisfying properties $P_1$ and $P_2$.

**Proof of Lemma 5.3.** Assume that (i) holds. Since $\pi$ is a square, $\pi$ has a square root, say $\sigma$. Let $2n = |\pi|$ (and hence $|\sigma| = n$). Then, by definition, there exist two sets

$$I_1 = \{i_1^1 < i_2^1 < \cdots < i_n^1\} \quad \text{and} \quad I_2 = \{i_2^1 < i_2^2 < \cdots < i_n^2\} \quad (5.2)$$

of disjoint indexes of letters of $\pi$ such that $\pi_{I_1}$ and $\pi_{I_2}$ are both order-isomorphic to $\sigma$. Let $G = (V, E)$ be the directed graph such that $V = [2n]$ and $E = \{(i_j^1, i_j^2) : j \in [n]\}$. It is easily seen that $M = (G, \pi)$ is a directed perfect matching since $I_1 \cap I_2 = \emptyset$ and $I_1 \cup I_2 = [2n]$.

We first show that $M$ avoids the unlabeled patterns of $P_{\text{cont}}$. Indeed, suppose, aiming at a contradiction, that such an occurrence appears for, say, arcs $(i_j^1, i_j^2)$ and $(i_k^1, i_k^2)$ of $M$. Assuming without loss of generality $i_j^1 < i_k^1$, we are left with the four configurations

$$\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\text{configuration 1} \\
\text{configuration 2} \\
\text{configuration 3} \\
\text{configuration 4}
\end{array}
\end{array}
\end{array} \quad (5.3)$$

where shadow nodes give the position in the permutation $\pi$. Then it follows that $i_j^2 > i_k^2$. This is a contradiction since $i_j^2 < i_k^2$ implies $j < k$, and hence, $i_j^2 < i_k^2$. We now turn to proving that $M$ also avoids the unlabeled patterns $\begin{array}{c}
\begin{array}{c}
\text{pattern 7} \\
\text{pattern 8}
\end{array}
\end{array}$ and $\begin{array}{c}
\begin{array}{c}
\text{pattern 9} \\
\text{pattern 10}
\end{array}
\end{array}$. Indeed, suppose, aiming at a contradiction, that such an occurrence appears for, say, arcs $(i_j^1, i_j^2)$ and $(i_k^1, i_k^2)$ of $M$. Assuming without loss of generality $i_j^1 < i_k^1$, we are left with the two configurations

$$\begin{array}{c}
\begin{array}{c}
\begin{array}{c}
\text{configuration 5} \\
\text{configuration 6}
\end{array}
\end{array}
\end{array} \quad (5.4)$$

14
Then it follows that $i^2_j > i^2_k$. Again, this is a contradiction since $i^1_j < i^1_k$ implies $j < k$, and hence, $i^2_j < i^2_k$. Finally, for any two distinct arcs $(i^1_j, i^2_j)$ and $(i^1_k, i^2_k)$ of $M$, we have $\pi(i^1_j) < \pi(i^1_k)$ if and only if $\pi(i^2_j) < \pi(i^2_k)$ since we are comparing in both cases two elements (at positions $j$ and $k$) in two patterns that are order-isomorphic to $\sigma$. Therefore, $M$ satisfies properties $P_1$ and $P_2$, so that (ii) holds.

Assume now that (ii) holds. Let $$I^1 = \{i^1_1 < i^1_2 < \cdots < i^1_n\} \quad \text{and} \quad I^2 = \{i^2_1 < i^2_2 < \cdots < i^2_n\} \quad (5.5)$$ such that $I^1$ is the set the sources of the arcs of $M$ and $I^2$ is the set of the sinks of the arcs of $M$. Let us first show that, for every $j \in [n]$, $(i^1_j, i^2_j)$ is an arc of $M$. For that, we show that $(i^1_n, i^2_n)$ is an arc of $M$. Suppose, aiming at a contradiction that this is false. Then, there exist two vertices $i^2_q$ and $i^2_j$ of $M$ such that $(i^1_n, i^2_q)$ and $(i^1_j, i^2_n)$ are arcs of $M$. Since $p < n$ and $q < n$, there is in $M$ one of the four configurations

\[
\begin{array}{cccccc}
1 & 2 & 3 & 4 & 5 & 6 \\
\end{array}
\]

This is a contradiction since $M$ satisfies property $P_1$ and hence avoids the unlabeled patterns $\equiv, \equiv, \equiv, \equiv$. Therefore, $(i^1_n, i^2_n)$ is an arc of $M$. By iteratively applying the same reasoning, this also shows that all $(i^1_j, i^2_j)$, $j \in [n-1]$, are arcs of $M$. Now, let $p^1$ be the word of sources and $p^2$ be the word of sinks of $M$. Clearly $p^1$ and $p^2$ are disjoint in $\pi$ (since $M$ is a matching) and cover $\pi$ (since $M$ is perfect). Moreover, the fact that $M$ satisfies $P_2$ implies immediately that $p^1$ and $p^2$ are order-isomorphic. Hence, this shows that $\pi$ is a square, so that (i) holds.

Observe that, given a square permutation $\pi \in S_{2n}$ and a directed perfect matching $M$ on $\pi$ satisfying properties $P_1$ and $P_2$, one can recover a square root of $\pi$ by considering the standardization permutation of the word of sources (or, equivalently, the word of sinks) of $M$. Figure 3 provides an illustration of Lemma 5.3 and of this observation.

![Figure 3](image-url)

Figure 3: A directed perfect matching $M$ on the permutation $\pi = 183927B5C6A4$ satisfying the properties $P_1$ and $P_2$. From $M$, it follows that $\pi$ is a square as it appears in the shuffle of 1892A4 and 37B5C6, both being order-isomorphic to 145263, a square root of $\pi$.

Let $\pi$ be a permutation. For the sake of clarity, we will say that a bunch of consecutive positions $P$ of $\pi$ is above (resp. below) another bunch of consecutive positions $P'$ in $\pi$ if $\pi(i) > \pi(j)$ (resp. $\pi(i) < \pi(j)$) for every $i \in P$ and every $j \in P'$. For example, $\sigma_1$ is above
\(\sigma_2\) (in an equivalent manner, \(\sigma_2\) is below \(\sigma_1\)) in Figure 6(a), whereas \(\sigma_1\) is below \(\sigma_2\) (in an equivalent manner, \(\sigma_2\) is above \(\sigma_1\)) in Figure 6(b).

Moreover, if \(\pi\) is a permutation satisfying \(\pi = \pi_1\pi_2\pi_3\pi_2\pi_1\) and \(\mathcal{M}\) is a directed perfect matching on \(\pi\), a \((\sigma_1, \sigma_2)\)-arc (resp. \((\sigma_2, \sigma_1)\)-arc) of \(\mathcal{M}\) is any arc \((i, j)\) (resp. \((j, i)\)) of \(\mathcal{M}\) such that the \(i\)-th letter of \(\pi\) belongs to \(\sigma_1\) and the \(j\)-th letter of \(\pi\) belongs to \(\sigma_2\).

Let us now state and prove some lemmas that will prove extremely useful for simplifying the proof of upcoming Proposition 5.10. First, whereas Lemma 5.3 states that a directed perfect matching on a permutation with Property \(P_1\) avoids some unlabeled patterns of length 4 (more specifically, it avoids the unlabeled patterns of \(P_1\)), the following two lemmas state that a directed perfect matching on a permutation with Property \(P_2\) also avoids some additional labeled patterns. These two lemmas are easily proved by requiring Property \(P_2\).

For example, an occurrence of the labeled pattern \(\overline{3 \ 4 \ 2 \ 1}\) induces the existence of two arcs \((i_1, i_3)\) and \((i_2, i_4)\) with \(i_1 < i_2 < i_3 < i_4\) and \(\pi(i_4) < \pi(i_3) < \pi(i_2) < \pi(i_1)\).

\[\begin{array}{cccc}
1243 & 1342 & 1432 & 2134 \\
2341 & 2431 & 3124 & 3214 \\
3421 & 4123 & 4213 & 4312 \\
\end{array}\]

Figure 4: The labeled patterns with crossing edges avoided by any directed perfect matching on a permutation satisfying Property \(P_2\).

**Lemma 5.4** (Forbidden crossing patterns). *Let \(\pi\) be a permutation and \(\mathcal{M}\) be a directed...*
perfect matching on $\pi$ satisfying Property $P_2$. Then $M$ avoids the following labeled patterns

(5.7)

see Figure 4.

Figure 5: The labeled patterns with consecutive edges avoided by any directed perfect matching on a permutation satisfying Property $P_2$.

Lemma 5.5 (Forbidden precedence patterns). Let $\pi$ be a permutation and $M$ be a directed perfect matching on $\pi$ satisfying Property $P_2$. Then $M$ avoids the following labeled patterns

(5.8)
see Figure 5.

Figure 6: Illustration of Corollary 5.6.

A useful corollary of Lemma 5.4 reads as follows.

**Corollary 5.6.** Let $\pi = \pi_1 \sigma_1 \pi_2 \sigma_2 \pi_3$ be a permutation and $M$ be a directed perfect matching on $\pi$ satisfying Properties $P_1$ and $P_2$. The following assertions hold.

(i) If $\sigma_1$ is increasing, $\sigma_2$ is decreasing, and $\sigma_1$ is above $\sigma_2$ (see Figure 6(a)), then there is at most one arc between $\sigma_1$ and $\sigma_2$ in $M$ (this arc can be a $(\sigma_1, \sigma_2)$-arc or a $(\sigma_2, \sigma_1)$-arc).

(ii) If $\sigma_1$ is decreasing, $\sigma_2$ is increasing, and $\sigma_1$ is below $\sigma_2$ (see Figure 6(b)), then there is at most one arc between $\sigma_1$ and $\sigma_2$ in $M$ (this arc can be a $(\sigma_1, \sigma_2)$-arc or a $(\sigma_2, \sigma_1)$-arc).

**Proof of Corollary 5.6.** Suppose, aiming at a contradiction, that (i) does not hold. Since $M$ has Property $P_1$, it avoids the unlabelled patterns of $P_1$. Then it follows that $M$ contains (see Figure 6(a)) either two crossing $(\sigma_1, \sigma_2)$-arcs (a $\begin{array}{c} 3 \ 4 \ 2 \ 1 \end{array}$ labeled pattern) or two crossing $(\sigma_2, \sigma_1)$-arcs (a $\begin{array}{c} 3 \ 4 \ 2 \ 1 \end{array}$ labeled pattern). Hence, according to Lemma 5.4, $M$ cannot have Property $P_2$. This is the sought-after contradiction.

The proof for (ii) is similar (see Figure 6(b)) replacing the labeled patterns $\begin{array}{c} 3 \ 4 \ 2 \ 1 \end{array}$ and $\begin{array}{c} 3 \ 4 \ 2 \ 1 \end{array}$ by $\begin{array}{c} 2 \ 1 \ 3 \ 4 \end{array}$ and $\begin{array}{c} 2 \ 1 \ 3 \ 4 \end{array}$.

**Lemma 5.7.** Let $\pi = \pi_1 \sigma_1 \pi_2 \sigma_2 \pi_3$ be a permutation where $\sigma_1$ is an increasing pattern and $\sigma_2$ is (right) below $\sigma_1$, and $M$ be a directed perfect matching on $\pi$ that has Properties $P_1$ and $P_2$. If $M$ contains a $(\sigma_1, \sigma_2)$-arc or a $(\sigma_2, \sigma_1)$-arc, then it does not contain a $(\sigma_1, \sigma_1)$-arc.
**Proof of Lemma 5.7.** Suppose, aiming at a contradiction, that $M$ contains a $(\sigma_1, \sigma_2)$-arc or a $(\sigma_2, \sigma_1)$-arc $(i, i')$, and a $(\sigma_1, \sigma_1)$-arc $(j, j')$. Since $M$ has Property $P_1$, it avoids the unlabeled patterns of $P_1$. Therefore, $M$ contains one of the following labeled patterns: \(2\ 3\ 4\ 1\) and \(2\ 3\ 4\ 1\) (see Figure 7). Hence, according to Lemmas 5.4 and 5.5, $M$ cannot have Property $P_2$. This is the sought-after contradiction.

**Lemma 5.8.** Let $\pi$ be a permutation and $M$ be a directed perfect matching on $\pi$. If $M$ has properties $P_1$ and $P_2$, then so does the directed perfect matching $M'$ obtained from $M$ by reversing each of its arcs.

**Proof of Lemma 5.8.** It is immediate that $M'$ satisfies Property $P_2$, since, for any two arcs $(i, i')$ and $(j, j')$ of $M$, we have $\pi(i) < \pi(j)$ if and only if $\pi(i') < \pi(j')$. As for Property $P_1$, it is enough to observe that the set of unlabeled patterns $P_1$ is closed by arc reversals.

A direct interpretation of Lemma 5.8 is that, if a permutation $\pi$ is a square, one can exchange the roles of the two order-isomorphic patterns that cover $\pi$. This can also be seen
as a consequence of Proposition 4.1 about the commutativity of $\bullet$. Besides, an immediate but useful consequence of Lemma 5.8 reads as follows.

**Corollary 5.9.** Let $\pi$ be a permutation and $i$ and $i'$ be two distinct indexes of $\pi$. There exists a directed perfect matching on $\pi$ with Properties $P_1$ and $P_2$ that contains the arc $(i, i')$ if and only if there exists a directed perfect matching on $\pi$ with Properties $P_1$ and $P_2$ that contains the arc $(i', i)$.

Having disposed of these preliminary observations, we now turn to stating and proving the NP-hardness of the targeted problem.

**Proposition 5.10.** Deciding whether a permutation is a square is NP-complete.

**Proof of Proposition 5.10.** This decision problem is certainly in NP. To prove that it is NP-complete, we propose a reduction from the pattern involvement problem which is known to be NP-complete [BBL98].

Let $\pi \in S_n$ and $\sigma \in S_k$ be two permutations. Let us set

$$N_4 = 2(2N_4 + 2n + 2k + 4) + 3,$$
$$N_3 = 2(2N_3 + 2N_4 + 2n + 2k + 4) + 3,$$
$$N_2 = 2(2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4) + 3,$$
$$N_1 = 2(2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4) + 3.$$  \hfill (5.9)

Notice that $N_1, N_2, N_3$ and $N_4$ are polynomials in $n$. The crucial properties are that

(i) the integers $N_1, N_2, N_3$ and $N_4$ are odd;

(ii) the relation

$$N_i > \left( \sum_{i<j \leq 4} 2N_j \right) + 2n + 2k + 4$$  \hfill (5.10)

holds for every $i \in [k]$.

To construct a new permutation $\mu$ from $\pi$ and $\sigma$, we now turn to defining various gadgets (sequences of integers) that will act as building blocks. Recall that, for any permutation $p = p_1 p_2 \cdots p_x$ of $[x]$ and any non-negative integer $y$, $p[y]$ stand for the sequence $(p_1 + y, p_2 + y, \cdots, p_x + y)$. Define

$$\sigma' = ((k+1) \sigma (k+2)) [2N_2 + N_4 + 2n + k + 2],$$
$$\pi' = ((n+1) \pi (n+2)) [2N_2 + N_4 + n + k + 2],$$
$$\sigma'' = \sigma [2N_2 + N_4],$$
$$\pi'' = \pi [2N_2 + N_4 + k],$$
$$\nu_1 = \gamma_{N_1} [2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4],$$
$$\nu_1' = \gamma_{N_1} [N_1 + 2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4],$$
$$\nu_2 = \gamma_{N_2} [N_2],$$
$$\nu_2' = \gamma_{N_2} [2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4],$$
$$\nu_3 = \gamma_{N_3} [2N_2 + N_4 + 2n + 2k + 4],$$
$$\nu_3' = \gamma_{N_3} [2N_2 + N_3 + 2N_4 + 2n + 2k + 4],$$
$$\nu_4 = \gamma_{N_4} [2N_2 + N_4 + 2n + 2k + 4],$$
$$\nu_4' = \gamma_{N_4} [2N_2].$$  \hfill (5.11)
We are now in position to define our target permutation $\mu$ (see Figure 8 for an illustration) as

$$\mu = \nu_1 \nu_2' \nu_3' \nu_4' \nu_2' \nu_3' \pi' \nu_4' \pi'' \sigma''.$$  \hspace{1cm} (5.12)

It is immediate that $\mu$ can be constructed in polynomial-time in $n$ and $k$. We claim that $\sigma$ occurs in $\pi$ if and only if there exists a directed perfect matching $\mathcal{M}$ on $\mu$ that has Properties $P_1$ and $P_2$ (that is, by Lemma 5.3, $\mu$ is a square).

Suppose first that $\sigma$ occurs in $\pi$ and fix any occurrence. Construct a directed matching $\mathcal{M}$ on $\mu$ as follows (all arcs are oriented to the right):

![Figure 8: Schematic representation of the permutation $\mu$ used in the proof of Proposition 5.10. Black arcs denote the presence of at least one arc between two bunches of positions in $\mu$. Grey arcs denote arcs that are only considered in the forward direction of the proof.](image-url)
(1) $\mathcal{M}$ contains $N_1$ pairwise crossing $(\nu_1, \nu'_1)$-arcs.
(2) $\mathcal{M}$ contains $N_2$ pairwise crossing $(\nu_2, \nu'_2)$-arcs.
(3) $\mathcal{M}$ contains $N_3$ pairwise crossing $(\nu_3, \nu'_3)$-arcs.
(4) $\mathcal{M}$ contains $N_4$ pairwise crossing $(\nu_4, \nu'_4)$-arcs.
(5) $\mathcal{M}$ contains $k + 2$ pairwise crossing $(\sigma', \pi')$-arcs as depicted in Figure 9. More precisely,

\[ ((k + 1) \sigma (k + 2)) \{2N_2 + N_4 + 2n + k + 2 \} \]

\[ (n + 1) \pi (n + 2) \{2N_2 + 2N_3 + N_4 + k + 2 + 1 \} \]

(i) the first position of $\sigma'$ (i.e., $(2N_1 + N_2 + N_3) + 1$) is linked to the first position of $\pi'$ (i.e., $(2N_1 + 2N_2 + 2N_3 + N_4 + k + 2) + 1$),

(ii) the last position of $\sigma'$ (i.e., $(2N_1 + N_2 + N_3) + k + 2$) is linked to the last position of $\pi'$ (i.e., $(2N_1 + 2N_2 + 2N_3 + N_4 + k + 2) + n + 2$), and all other positions in $\sigma'$ are linked by means of $k$ pairwise crossing arcs to the positions in $\pi'$ that correspond to the fixed occurrence of $\sigma$ in $\pi$. (Notice that we use here the fact that $\sigma$ occurs in $\pi$).

Figure 9: Illustration of the directed perfect matching $\mathcal{M}$ between gadgets $\sigma'$, $\pi'$, $\pi''$ and $\sigma''$ assuming two input permutation $\sigma = 312$ and $\pi = 452136$ (where a specific occurrence of $\sigma$ in $\pi$ is depicted in bold).
(6) $\mathcal{M}$ contains $n - k$ pairwise crossing $(\pi', \pi'')$-arcs as depicted in Figure 9. More precisely, all positions in $\pi'$ that do not correspond to the fixed occurrence of $\sigma$ in $\pi$ are linked by means of $n - k$ pairwise crossing arcs to the positions in $\pi''$ that do not correspond to the fixed occurrence of $\sigma$ in $\pi$.

(7) $\mathcal{M}$ contains $k$ pairwise crossing $(\pi'', \sigma'')$-arcs as depicted in Figure 9. More precisely, the positions in $\pi''$ that correspond to the fixed occurrence of $\sigma$ in $\pi$ are linked by means of $k$ pairwise crossing arcs to all positions in $\sigma''$. (Notice that, again, we use here the fact that $\sigma$ occurs in $\pi$).

It can be easily checked (probably referring to Figure 8) that $\mathcal{M}$ is perfect and has Properties $P_1$ and $P_2$.

Conversely, suppose that there exists an directed perfect matching $\mathcal{M}$ on $\mu$ that has Properties $P_1$ and $P_2$. We show that $\sigma$ occurs as a pattern in $\pi$. Whereas the directed perfect matching $\mathcal{M}$ may not be as regular as in the forward direction, the main idea is to prove that $\mathcal{M}$ contains enough structure (more precisely, $k + 2 (\sigma', \pi')$-arcs) so that we can conclude that $\sigma$ occurs in $\pi$. We have divided the reverse direction into a set of basic claims that progressively defines and refines the overall structure of $\mathcal{M}$.

Claim 5.11. We may assume that there is no $(\nu_1', \nu_1)$-arc in $\mathcal{M}$.

Proof of Claim 5.11. We first observe that, according to Property $P_1$, since $\mathcal{M}$ avoids the unlabeled patterns of $\mathcal{P}_1$, $\mathcal{M}$ cannot contain both a $(\nu_1, \nu_1')$-arc and a $(\nu_1', \nu_1)$-arc. Now, if $\mathcal{M}$ does not contain a $(\nu_1', \nu_1)$-arc we are done. Otherwise, $\mathcal{M}$ does contain some $(\nu_1', \nu_1)$-arcs and no $(\nu_1, \nu_1')$-arc, and the result follows from Lemma 5.8.

Claim 5.12. There is neither a $(\nu_1, \nu_2)$-arc nor a $(\nu_2, \nu_1)$-arc in $\mathcal{M}$.

Proof of Claim 5.12. First, according to Corollary 5.6, there exists at most one arc between $\nu_1$ and $\nu_2$ in $\mathcal{M}$ (this arc can be a $(\nu_1, \nu_2)$-arc or a $(\nu_2, \nu_1)$-arc). Suppose now, aiming at a contradiction, that there exists either one $(\nu_1, \nu_2)$-arc or one $(\nu_2, \nu_1)$-arc, say $a = (i, i')$, in $\mathcal{M}$. In this case, according to Lemma 5.7, $\mathcal{M}$ does not contain any $(\nu_1, \nu_1')$-arc. We now claim that $\mathcal{M}$ contains $N_1 - 1$ pairwise crossing $(\nu_1, \nu_1')$-arcs (and $i = 1$) if $a$ is a $(\nu_1, \nu_2)$-arc, or $N_1 - 1$ pairwise crossing $(\nu_1', \nu_1)$-arcs (and $i' = 1$) if $a$ is a $(\nu_2, \nu_1)$-arc (recall here that $\overline{\mathcal{A}}$ and $\overline{\mathcal{B}}$ are forbidden patterns in $\mathcal{M}$). Indeed, observe first that $N_1 - 1 > |\nu_1| + |\sigma'| + |\nu_2| + |\nu_1'| + |\pi'| + |\nu_1'| + |\pi''| + |\sigma_1|$. Therefore, there exists at least one $(\nu_1, \nu_2)$-arc if $a$ is a $(\nu_1, \nu_2)$-arc or at least one $(\nu_1', \nu_1)$-arc if $a$ is a $(\nu_2, \nu_1)$-arc. Hence, if $\mathcal{M}$ does not contain $N_1 - 1$ pairwise crossing $(\nu_1, \nu_1')$-arcs or $N_1 - 1$ pairwise crossing $(\nu_1', \nu_1)$-arcs, then it contains one of the following labeled patterns: $\overline{\mathcal{A}} \overline{\mathcal{A}}$, $\overline{\mathcal{B}}$, $\overline{\mathcal{A}} \overline{\mathcal{B}}$, $\overline{\mathcal{B}} \overline{\mathcal{A}}$, and $\overline{\mathcal{B}} \overline{\mathcal{B}}$. Applying Lemma 5.4 and Lemma 5.5 yields a contradiction. Then it follows that $\mathcal{M}$ contains $N_1 - 1$ pairwise crossing $(\nu_1, \nu_1')$-arcs (and $i = 1$) if $a$ is a $(\nu_1, \nu_2)$-arc, or $N_1 - 1$ pairwise crossing $(\nu_1', \nu_1)$-arcs (and $i' = 1$) if $a$ is a $(\nu_2, \nu_1)$-arc. But it follows from Claim 5.11 that $\mathcal{M}$ does not contain any $(\nu_1', \nu_1)$-arc, and hence $\mathcal{M}$ contains $N_1 - 1$ pairwise crossing $(\nu_1, \nu_1')$-arcs and $a$ is a $(\nu_1, \nu_2)$-arc (since $\overline{\mathcal{B}} \overline{\mathcal{B}}$ is forbidden).

We now observe that $|\nu_1| = |\nu_1'| = N_1$. Hence, since $\mathcal{M}$ is perfect, there exists a position in $\nu_1'$ that is not involved in a $(\nu_1, \nu_1')$-arc in $\mathcal{M}$. We rule out this configuration by considering two cases:
• There exists a \((\nu_2, \nu_1')\)-arc \((j, j')\) in \(\mathcal{M}\) (we cannot have a \((\nu_1', \nu_2)\)-arc since the unlabeled pattern \(\overbrace{1\ 2\ 3\ 4\ 1}^2\) is forbidden), see Figure 10(a) and Figure 10(b). Then it follows that \(\mathcal{M}\) contains the labeled pattern \(\overbrace{2\ 1\ 3\ 4\ 1}^3\) (with arc \((j, j')\) and any \((\nu, \nu_1')\)-arc). Applying Lemma 5.4 yields the sought-after contradiction.
• There exists an arc \((j,j')\) \(j = 2N_1 + N_2\) and \(j' > 2N_1 + N_2\), or \(j' = 2N_1 + N_2\) and \(j > 2N_1 + N_2\), see Figure 10(c) and Figure 10(d). Then it follows that \(\mathcal{M}\) contains one of the two following labeled patterns: \(\begin{array}{c} \mathcal{M}_1 \end{array}\) (with arc \((i,i')\) and arc \((j,j')\)). Applying Lemma 5.5 yields the sought-after contradiction.

\[\square\]

**Claim 5.13.** There is at least one \((\nu_1, \nu'_1)\)-arc in \(\mathcal{M}\).

**Proof of Claim 5.13.** Suppose, aiming at a contradiction, that there is no \((\nu_1, \nu'_1)\)-arc in \(\mathcal{M}\). Then it follows that there exists an arc \((i,i')\) in \(\mathcal{M}\) that is neither a \((\nu_1, \nu_1)\)-arc (since \(N_1\) is odd) nor a \((\nu_1, \nu_2)\)-arc (Claim 5.12) nor a \((\nu_1, \nu'_1)\) (by our contradiction hypothesis). (In other words, \(i \leq N_1\) and \(i' > 2N_1 + N_2\).) Therefore, since \(\mathcal{M}\) is containment-free (i.e., it avoids the unlabeled patterns of \(P_{\text{cont}}\)), there is neither a \((\nu_2, \nu_2)\)-arc nor a \((\nu'_1, \nu'_1)\)-arc in \(\mathcal{M}\). Then it follows that \(\mathcal{M}\) contains either \(N_1\) arcs \((j,j')\) with \(N_1 + N_2 < j \leq 2N_1 + N_2\) and \(j' > 2N_1 + N_2\) (if \(i \leq N_1\) and \(i' > 2N_1 + N_2\)), or \(N_1\) arcs \((i,i')\) with \(N_1 + N_2 < j' \leq 2N_1 + N_2\) and \(j > 2N_1 + N_2\) (if \(i' \leq N_1\) and \(i > 2N_1 + N_2\)), otherwise \(\mathcal{M}\) would not be containment-free. But \(|\nu'_2| = N_1 > |\nu_3| + |\sigma'| + |\nu'_4| + |\pi'| + |\nu'_3| + |\sigma''| + |\pi''|\). This is a contradiction. \[\square\]

The above claim will be complemented in upcoming Claim 5.24.

**Claim 5.14.** There is no \((\nu_2, \nu_2)\)-arc in \(\mathcal{M}\).

**Proof of Claim 5.14.** Combine Claim 5.13 together with the fact that \(\mathcal{M}\) is containment-free (i.e., it avoids the unlabeled patterns of \(P_{\text{cont}}\)). \[\square\]

**Claim 5.15.** There is neither a \((\nu_2, \nu'_1)\)-arc nor a \((\nu'_1, \nu_2)\)-arc in \(\mathcal{M}\).

---

**Figure 11:** Illustration of Claim 5.15.
Proof of Claim 5.15. First, according to Corollary 5.6–(ii), there exists either at most one \((v_2, v'_2)\)-arc and no \((v_1, v'_2)\)-arc, or at most one \((v'_2, v_2)\)-arc and no \((v_2, v'_1)\)-arc \((i, i')\) in \(M\) (see Figure 11). Now from Claim 5.13, there exists at least one \((v_1, v'_1)\)-arc, say \((j, j')\), in \(M\). Hence, since \(M\) is containment-free \(i.e.,\) it avoids the unlabeled patterns of \(P_{cont}\), \(M\) contains one of the following labeled patterns: \(\begin{array}{c} 2 \end{array} \begin{array}{ccc} 1 & 3 & 4 \end{array}\) and \(\begin{array}{cc} 1 \end{array} \begin{array}{ccc} 2 & 4 \end{array}\). Applying Lemma 5.4 yields the sought-after contradiction. □

Claim 5.16. There is at least one \((v_2, v'_2)\)-arc in \(M\).

Proof of Claim 5.16. First, according to Claim 5.13, there exists at least one \((v_1, v'_1)\)-arc in \(M\) and hence, since \(M\) avoids the unlabeled pattern \(\begin{array}{c} 2 \end{array} \begin{array}{ccc} 1 & 3 & 4 \end{array}\) (Property \(P_1\)) there is no \((v_2, v'_2)\)-arc in \(M\). Now, suppose, aiming at a contradiction, that there is no \((v_2, v'_2)\)-arc in \(M\). Notice that there is neither a \((v_1, v_2)\)-arc \(\text{Claim 5.12}\) nor a \((v_2, v_1)\)-arc \(\text{Claim 5.12}\) nor a \((v_2, v'_2)\)-arc \(\text{Claim 5.14}\) nor a \((v_2, v'_1)\)-arc \(\text{Claim 5.15}\) nor a \((v'_2, v_2)\)-arc \(\text{Claim 5.15}\) in \(M\). But \(|v_2| = N_2 > |v_3| + |\sigma'| + |v_1| + |v'_1| + |\sigma'| + |v_{\sigma''}| + |\sigma''|\). Hence \(M\) cannot be a directed perfect matching, thereby contradicting our hypothesis about \(M\). □

Claim 5.17. There is neither a \((v'_1, v'_1)\)-arc, nor a \((v'_4, v'_3)\)-arc, nor a \((v_3, v'_1)\)-arc, nor a \((v'_1, v'_4)\)-arc, nor a \((v'_4, v'_4)\)-arc, nor a \((v_1, v'_3)\)-arc nor a \((v_4, v'_4)\)-arc nor a \((v_3, v'_4)\)-arc nor a \((v'_3, v'_3)\)-arc nor a \((v_3, v'_1)\)-arc, nor a \((v_4, v'_3)\)-arc nor a \((v_4, v'_4)\)-arc in \(M\).

Proof of Claim 5.17. Combine Claim 5.16 with the fact that \(M\) is containment-free \(i.e.,\) it avoids the unlabeled patterns of \(P_{cont}\). □

Claim 5.18. There is neither a \((v_2, v'_3)\)-arc, nor a \((v'_3, v'_3)\)-arc, nor a \((v_2, \pi')\)-arc, nor a \((\pi', v'_2)\)-arc, nor a \((v_2, v'_4)\)-arc, nor a \((v'_4, v'_2)\)-arc, nor a \((v_2, \pi'')\)-arc, nor a \((\pi'', v'_2)\)-arc nor a \((v'_2, \sigma'')\)-arc, nor a \((\sigma'', v'_2)\)-arc in \(M\).

Proof of Claim 5.18. Suppose aiming at a contradiction that \(M\) contains a \((v_2, v'_3)\)-arc, a \((v'_3, v'_3)\)-arc, a \((v'_2, \pi')\)-arc, a \((\pi', v'_2)\)-arc, a \((v'_2, v'_4)\)-arc, a \((v'_4, v'_2)\)-arc, a \((v_2, \pi'')\)-arc, a \((\pi'', v'_2)\)-arc or a \((v'_2, \sigma'')\)-arc or a \((\sigma'', v'_2)\)-arc, say \((i, i')\). We now observe that \(v_3, \pi', v'_4, \pi''\) and \(\sigma''\) are all right above of both \(v_2\) and \(v'_2\). Furthermore, according to Claim 5.16, there exists a \((v_2, v'_2)\)-arc, say \((j, j')\). Then, it follow that \(M\) contains one of the following labeled patterns: \(\begin{array}{c} 1 \end{array} \begin{array}{ccc} 2 & 4 \end{array}\) and \(\begin{array}{c} 1 \end{array} \begin{array}{ccc} 2 & 4 \end{array}\) (see Figure 12). Applying Lemma 5.5 and Lemma 5.4 yields the sought-after contradiction. □

Claim 5.19. There is neither a \((v_3, v'_2)\)-arc nor a \((v'_2, v'_3)\)-arc in \(M\).

Proof of Claim 5.19. Suppose, aiming at a contradiction, that there exists \((v_3, v'_2)\)-arc or a \((v'_2, v'_3)\)-arc \((j, j')\) in \(M\). According to Claim 5.16, there exists at least one \((v_2, v'_2)\)-arc \((i, i')\) in \(M\). Since \(M\) avoids the unlabeled pattern \(\begin{array}{c} 2 \end{array} \begin{array}{ccc} 1 & 3 & 4 \end{array}\) (Property \(P_1\)), there is no \((v'_3, v_2)\)-arc in \(M\) (see Figure 13), and hence \((j, j')\) is a \((v_3, v'_2)\)-arc. Then it follows that \(M\) contains the labeled pattern \(\begin{array}{c} 3 \end{array} \begin{array}{ccc} 4 \end{array}\) (see Figure 13). Applying Lemma 5.4 yields the sought-after contradiction. □

Claim 5.20. There is at most one \((v_2, v_3)\)-arc or at most one \((v_3, v_2)\)-arc in \(M\).

Proof of Claim 5.20. Apply Corollary 5.6. □
We will see soon (upcoming Claim 5.25) that there exists actually no \((\nu_2, \nu_3)\)-arc in \(\mathcal{M}\).

Claim 5.21. There is neither a \((\nu_1, \nu_3)\)-arc, nor a \((\nu_3, \nu_1)\)-arc in \(\mathcal{M}\).

Proof of Claim 5.21. Suppose, aiming at a contradiction, that there exists a \((\nu_1, \nu_3)\)-arc or a \((\nu_3, \nu_1)\)-arc, say \((j, j')\), in \(\mathcal{M}\). According to Claim 5.13, there exists at least one \((\nu_1, \nu'_1)\)-arc, say \((i, i')\), in \(\mathcal{M}\). Since \(\mathcal{M}\) avoids the unlabeled pattern \(\text{CrossingRL}\) (Property \(P_1\)), there is no \((\nu_3, \nu_1)\)-arc in \(\mathcal{M}\) (see Figure 14), and hence \((j, j')\) is a \((\nu_1, \nu_3)\)-arc. Then it follows that \(\mathcal{M}\) contains the labeled pattern \(2\ 3\ 4\ 1\) (see Figure 14). Applying Lemma 5.4 yields the sought-after contradiction. 

Claim 5.22. There exists a \((\nu_3, \nu'_3)\)-arc in \(\mathcal{M}\).

Proof of Claim 5.22. First, according to Claim 5.16, there exists at least one \((\nu_2, \nu'_2)\)-arc in \(\mathcal{M}\). Since \(\mathcal{M}\) avoids the unlabeled pattern \(\text{CrossingRL}\) (Property \(P_1\)) there is no \((\nu'_3, \nu_3)\)-arc in \(\mathcal{M}\). Now, suppose, aiming at a contradiction, that there is no \((\nu_3, \nu'_3)\)-arc in \(\mathcal{M}\). Combining Claim 5.17, Claim 5.19, Claim 5.20 Claim 5.21 together with our hypothesis,
we conclude that $N_3 - 1$ positions in $\nu_3$ are involved in arcs of $\mathcal{M}$ that are neither $(\nu_1, \nu_3)$-arcs, nor $(\nu_3, \nu_1)$-arcs, nor $(\nu_2, \nu_3)$-arcs, nor $(\nu_3, \nu_2)$-arcs, nor $(\nu_1', \nu_3)$-arcs, nor $(\nu_3, \nu_1')$-arcs, nor $(\nu_2, \nu_3)$-arcs, nor $(\nu_3, \nu_2)$-arcs, nor $(\nu_3, \nu_1')$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs, nor $(\nu_3, \nu_3)$-arcs. But $N_3 - 1 > |\pi'| + |\nu'_3| + |\nu''_4| + |\sigma''| = N_4 + 2n + 2k + 4$, and hence $\mathcal{M}$ is not a perfect matching. This is the sought-after contradiction.

Claim 5.23. There is neither a $(\sigma', \sigma')$-arc, nor a $(\sigma', \nu_4)$-arc, nor a $(\nu_4, \sigma')$-arc, nor a
Proof of Claim 5.24. First, according to Claim 5.16, $M$ contains at least one $(\nu_1, \nu'_1)$-arc. Now, suppose, aiming at a contradiction, that $M$ does not contain $N_1$ $(\nu_1, \nu'_1)$-arcs. Combining Claim 5.12, Claim 5.15, Claim 5.15 and Claim 5.17, we conclude that $M$ contains one of the two following labeled patterns: $\nu_3, \nu_4, \nu'_2, \nu'_3, \pi', \nu'_4, \sigma'$ or $\nu_3, \nu_4, \nu'_2, \nu'_3, \pi', \nu'_4, \sigma''$ (see Figure 15). Applying Lemma 5.4 or Lemma 5.5 yields the sought-after contradiction.

Proof of Claim 5.26. According to Claim 5.25, all positions in $\nu_2$ and $\nu'_2$ are involved in $(\nu_2, \nu'_2)$-arcs in $M$.

Claim 5.27. There is neither a $(\nu_4, \nu'_3)$-arc nor a $(\nu'_3, \nu_4)$-arc in $M$. 

Figure 15: Illustration of Claim 5.24.
Proof of Claim 5.27. First, according to Corollary 5.6–(ii), there exists either at most one \((\nu_4, \nu'_3)\)-arc and no \((\nu'_3, \nu_4)\)-arc, or at most one \((\nu'_3, \nu_4)\)-arc and no \((\nu_4, \nu'_3)\)-arc \((i, i')\) in \(\mathcal{M}\) (see Figure 16). Now from Claim 5.22, there exists at least one \((\nu_3, \nu'_3)\)-arc, say \((j, j')\), in \(\mathcal{M}\). Hence, since \(\mathcal{M}\) is containment-free \(\text{i.e.}, it avoids the unlabeled patterns of } P_{\text{cont}}, \mathcal{M}
contains one of the two following labeled patterns: \(\begin{array}{cccc}
2 & 1 & 3 & 4 \\
\end{array}\) and \(\begin{array}{cccc}
2 & 1 & 3 & 4 \\
\end{array}\). Applying Lemma 5.4 yields the sought-after contradiction.

Claim 5.28. There is at least one \((\nu_4, \nu'_4)\)-arc in \(\mathcal{M}\).

Proof of Claim 5.28. First, according to Claim 5.22, there is at least one \((\nu_3, \nu'_3)\)-arc in \(\mathcal{M}\). Therefore, since \(\mathcal{M}\) avoids the unlabeled pattern \(\begin{array}{cccc}
2 & 1 & 3 & 4 \\
\end{array}\) (Property \(P_1\)), there is no \((\nu'_4, \nu_4)\)-arc in \(\mathcal{M}\). Now, suppose, aiming at a contradiction, that there is no \((\nu_4, \nu'_4)\)-arc in \(\mathcal{M}\). First, according to Claim 5.24 and Claim 5.25, there is neither a \((\nu_3, \nu'_4)\)-arc nor a \((\nu'_3, \nu_4)\)-arc nor a \((\nu'_4, \nu_3)\)-arc nor a \((\nu_4, \nu'_2)\)-arc nor a \((\nu'_4, \nu_2)\)-arc nor a \((\nu_4, \nu'_2)\)-abstract nor a \((\nu'_2, \nu_4)\)-arc in \(\mathcal{M}\). Furthermore, according to Claim 5.27, there is neither a \((\nu_4, \nu'_4)\)-arc nor a \((\nu_3, \nu'_4)\)-arc in \(\mathcal{M}\). But \(N_4 > |\pi'| + |\pi''| + |\sigma'|\), and hence \(\mathcal{M}\) is not a direct perfect matching, which contradicts our hypothesis about \(\mathcal{M}\).

Claim 5.29. There is neither a \((\pi', \pi')\)-arc nor a \((\sigma', \pi'')\)-arc nor a \((\pi'', \sigma')\)-arc nor a \((\sigma', \sigma'')\)-arc nor a \((\sigma'', \sigma')\)-arc in \(\mathcal{M}\).

Proof of Claim 5.29. Combine Claim 5.28 together with the fact that \(\mathcal{M}\) has Property \(P_1\) and hence is containment-free \(\text{i.e.}, it avoids the unlabeled patterns of } P_{\text{cont}}\).

Claim 5.30. There is neither a \((\sigma', \nu'_3)\)-arc nor a \((\nu'_3, \nu')\)-arc in \(\mathcal{M}\).

Figure 16: Illustration of Claim 5.27.
Proof of Claim 5.30. First, according to Claim 5.22, there is at least one \((\nu_3, \nu'_3)\)-arc in \(\mathcal{M}\). Therefore, since \(\mathcal{M}\) avoids the unlabeled pattern \(\square\) (Property \(P_1\)), there is no \((\nu'_3, \sigma')\)-arc in \(\mathcal{M}\). Now, suppose, aiming at a contradiction, that there is a \((\sigma', \nu'_3)\)-arc in \(\mathcal{M}\). Hence, since \(\mathcal{M}\) is containment-free (i.e., it avoids the unlabeled patterns of \(P_{\text{cont}}\)), \(\mathcal{M}\) contains the labeled pattern \(\square\). Applying Lemma 5.4 yields the sought-after contradiction.

Claim 5.31. There is neither a \((\sigma', \nu'_4)\)-arc nor a \((\nu'_4, \sigma')\)-arc in \(\mathcal{M}\).

Proof of Claim 5.31. First, according to Claim 5.28, there is at least one \((\nu_4, \nu'_4)\)-arc in \(\mathcal{M}\). Therefore, since \(\mathcal{M}\) is containment-free (i.e., it avoids the unlabeled patterns of \(P_{\text{cont}}\)), and avoids \(\square\) (Property \(P_1\)), there is no \((\nu'_4, \sigma')\)-arc in \(\mathcal{M}\). Now, suppose, aiming at a contradiction, that there is a \((\sigma', \nu'_4)\)-arc in \(\mathcal{M}\). Hence, \(\mathcal{M}\) contains the labeled pattern \(\square\). Applying Lemma 5.4 yields the sought-after contradiction.

Claim 5.32. There is no \((\pi', \sigma')\)-arc in \(\mathcal{M}\).

Proof of Claim 5.32. Combine Claim 5.28 together with the fact that \(\mathcal{M}\) avoids the unlabeled pattern \(\square\) (Property \(P_1\)).

Combining the above claims, we conclude that there are \(k + 2\) \((\sigma', \pi')\)-arcs in \(\mathcal{M}\). Recall that
\[
\sigma' = ((k + 1) \sigma (k + 2)) [2N_2 + N_4 + 2n + k + 2]
\]
and that
\[
\pi' = ((n + 1) \pi (n + 2)) [2N_2 + N_4 + n + k + 2].
\]
Then it follows we have at least \(k\) (possibly \(k + 1\) or \(k + 2\)) independent \((\sigma', \pi')\)-arcs \((a, a')\) in \(\mathcal{M}\) with
\[
2N_1 + N_2 + N_3 + 1 < a < 2N_1 + N_2 + N_3 + k + 2
\]
and
\[
2N_1 + N_2 + N_3 + (k + 2) + 1 < a' < 2N_1 + N_2 + N_3 + (k + 2) + n + 2.
\]
Therefore, by our hypothesis about \(\mathcal{M}\), \(\sigma\) occurs as a pattern in \(\pi\).

6. Conclusion and perspectives

There are a number of further directions of investigation in this general subject. They cover several areas: algorithmic, combinatorics, and algebra. Let us mention several — not necessarily new — open problems that are, in our opinion, the most interesting. How many permutations of \(S_{2n}\) are squares? How many \((213, 231)\)-avoiding permutations of \(S_{2n}\) are squares? (Equivalently, by Proposition 3.1, how many binary strings of length \(2n\) are squares; see also Problem 4 in [HRS12])? How hard is the problem of deciding whether a \((213, 231)\)-avoiding permutation is a square (Problem 4 in [HRS12], see also [BS14, RV13])? Given two permutations \(\pi\) and \(\sigma\), how hard is the problem of deciding whether \(\sigma\) is a square root of \(\pi\)? As for algebra, one can ask for a complete algebraic study of \(\mathbb{Q}[S]\) as a graded associative algebra for the shuffle product \(\circ\). Describing a generating family for \(\mathbb{Q}[S]\),
defining multiplicative bases of $\mathbb{Q}[S]$, and determining whether $\mathbb{Q}[S]$ is free as an associative algebra are worthwhile questions.

References


