



Unshuffling Permutations

Guillaume Fertin, Samuele Giraudo, Sylvie Hamel, Stéphane Vialette

► To cite this version:

Guillaume Fertin, Samuele Giraudo, Sylvie Hamel, Stéphane Vialette. Unshuffling Permutations: Trivial Bijections and Compositions. TAMC, Apr 2019, Kitakyushu, Japan. pp.242-261, 10.1007/978-3-030-14812-6_15 . hal-02304028

HAL Id: hal-02304028

<https://hal.science/hal-02304028>

Submitted on 14 Feb 2023

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.

Unshuffling permutations: Trivial bijections and compositions^{*}

Guillaume Fertin¹, Samuele Giraudo², Sylvie Hamel³, and Stéphane Vialette²

¹ Université de Nantes, LS2N (UMR 6004), CNRS, Nantes, France
guillaume.fertin@univ-nantes.fr

² Université Paris-Est, LIGM (UMR 8049), CNRS, ENPC, ESIEE Paris, UPEM,
F-77454, Marne-la-Vallée, France {samuele.giraudo,stephane.vialette}@u-pem.fr

³ Université de Montréal, DIRO, Montréal, Québec, Canada
sylvie.hamel@umontreal.ca

Abstract. Given permutations π , σ_1 and σ_2 , the permutation π (viewed as a string) is said to be a *shuffle* of σ_1 and σ_2 , in symbols $\pi \in \sigma_1 \sqcup \sigma_2$, if π can be formed by interleaving the letters of two strings p_1 and p_2 that are order-isomorphic to σ_1 and σ_2 , respectively. Given a permutation $\pi \in S_{2n}$ and a bijective mapping $f : S_n \rightarrow S_n$, the f -UNSHUFFLE-PERMUTATION problem is to decide whether there exists a permutation $\sigma \in S_n$ such that $\pi \in \sigma \sqcup f(\sigma)$. We consider here this problem for the following bijective mappings: inversion, reverse, complementation, and all their possible compositions. In particular, we present combinatorial results about the permutations accepted by this problem. As main results, we obtain that this problem is NP-complete when f is the reverse, the complementation, or the composition of the reverse with the complementation.

Keywords: Permutation · Shuffle product · Computational complexity.

1 Introduction

Given permutations π , σ_1 and σ_2 , π is said to be a *shuffle* of σ_1 and σ_2 , in symbols $\pi \in \sigma_1 \sqcup \sigma_2$, if π is the disjoint union of two patterns p_1 and p_2 (*i.e.*, if, viewed as a string, it can be formed by interleaving the letters of p_1 and p_2) that are order-isomorphic to σ_1 and σ_2 , respectively. This shuffling operation \sqcup was introduced by Vargas [12] in an algebraic context and was called *supershuffle*. In case $\sigma = \sigma_1 = \sigma_2$, the permutation π is said to be a *square w.r.t. the shuffle product* (or simply a *square* when clear from the context), and σ is said to be a *square root of π w.r.t. the shuffle product* (or simply a *square root of π* when clear from the context). Note that a permutation may have several square roots. For example, $\pi = 18346752 \in 1234 \sqcup 4321$ since π is a shuffle of the patterns $p_1 = 1347$ and $p_2 = 8652$ that are order-isomorphic to $\sigma_1 = 1234$ and

^{*} Partially supported by Laboratoire International Franco-Québécois de Recherche en Combinatoire (LIRCO) (G. Fertin and S. Vialette), supported by the Individual Discovery Grant RGPIN-2016-04576 from Natural Sciences and Engineering Research Council of Canada (NSERC) (S. Hamel)

$\sigma_2 = 4321$, respectively (as shown in 18^346^752). However, π is not a square. Besides, $\pi' = 24317856$ is a square as it is a shuffle of the patterns 2175 and 4386 that are both order-isomorphic to 2143 (as shown in 243^178^56). Note that 2143 is not the unique square root of π' since π' is also a shuffle of patterns 2156 and 4378 that are both order-isomorphic to 2134 (as shown in 243^178^56).

The above definitions are of course intended to be natural counterparts to the ordinary shuffle of words and languages. Given words u , v_1 and v_2 , u is said to be a *shuffle* of v_1 and v_2 (denoted $u \in v_1 \sqcup v_2$), if u can be formed by interleaving the letters of v_1 and v_2 in a way that maintains the left-to-right ordering of the letter from each word. For example, $u = abccbabacbb \in abcab \sqcup cbabcb$ (as shown in $ab_ccbab^a_cbb$). Similarly, in case $v = v_1 = v_2$, the word u is said to be a *square w.r.t. the shuffle product*, and v is said to be a *square root of u w.r.t. the shuffle product*. For example, $abaaabaabb$ is a square w.r.t. the shuffle product since it belongs to the shuffle of $abaab$ with itself (as shown in $ab_aaa_baa^b$). Given words u , v_1 and v_2 , deciding whether $u \in v_1 \sqcup v_2$ is $O(|u|^2 / \log(|u|))$ time solvable [6]. To the best of our knowledge, the first $O(|u|^2)$ time algorithm for this problem appeared in [7]. However, deciding whether a given word u is a square w.r.t. the shuffle product is NP-complete [9, 2]. Finally, for a given word u , deciding whether there exists a word v such that u is in the shuffle of v with its reverse v^R (i.e., $u \in v \sqcup v^R$) is NP-complete as well [9]. However, the problem is polynomial-time solvable for words built from a binary alphabet.

Coming back to permutations, by using a pattern avoidance criterion on directed perfect matchings, it is proved in [4] that recognizing permutations that are squares is NP-complete, and a bijection between (213, 231)-avoiding square permutations and square binary words is presented. Given (3142, 2413)-avoiding (a.k.a. *separable*) permutations π , σ_1 and σ_2 , it can be decided in polynomial time whether $\pi \in \sigma_1 \sqcup \sigma_2$ [8].

We finally observe that deciding whether a permutation is a shuffle of two monotone permutations is in P:

(i) *merge permutations* are the union of two increasing subsequences and are characterized by the fact that they contain no decreasing subsequence of length 3 [5], whereas (ii) *skew-merged permutations* are the union of an increasing subsequence with a decreasing subsequence and are characterized by the fact that they contain no subsequence ordered in the same way as 2143 or 3412 [11].

In this paper, we are interested in a generalization of the problem consisting in recognizing square permutations. We call this new problem the f -UNSHUFFLE-PERMUTATION problem, which is defined as follows. Given a permutation $\pi \in S_n$ and a bijective mapping $f : S_n \rightarrow S_n$, the f -UNSHUFFLE-PERMUTATION problem asks whether there exists a permutation $\sigma \in S_n$ such that $\pi \in \sigma \sqcup f(\sigma)$. We say in this case that π is a *generalized square permutation*. In case $f = \text{id}$, the id-UNSHUFFLE-PERMUTATION problem reduces to recognizing square permutations, and hence is NP-complete. This paper is devoted to studying the f -UNSHUFFLE-PERMUTATION problem in case f is either a trivial bijection (identity, complement, reverse or inverse) or obtained by composing trivial bijections. These bijections act on permutations by performing a transformation on their permutation matrices

and can hence be seen as elements of the Dihedral group D_4 , as discussed in the next section. The paper is organized as follows. In Section 2, we provide the needed definitions. Section 3 is devoted to presenting generalized square permutations and some associated enumerative properties. Finally, in Section 4, we show hardness of recognizing some generalized square permutations.

2 Definitions

For any nonnegative integer n , $[n]$ is the set $\{1, \dots, n\}$. We follow the usual terminology on words [3]. Let us recall here the most important ones. Let u be a word. The length of u is denoted by $|u|$. The *empty word*, the only word of null length, is denoted by ϵ . For any $i \in [|u|]$, the i -th letter of u is denoted by $u(i)$. If I is a subset of $[|u|]$, $u|_I$ is the subword of u consisting in the letters of u at the positions specified by the elements of I . A *permutation* of size n is a word π of length n on the alphabet $[n]$ such that each letter admits exactly one occurrence. The set of all permutations of size n is denoted by S_n .

Definition 1 (Reduced form). *If λ is a list of distinct integers, the reduced form of λ , denoted $\text{reduce}(\lambda)$, is the permutation obtained from λ by replacing its i -th smallest entry with i . For instance, $\text{reduce}(31845) = 21534$.*

Definition 2 (Order-isomorphism). *Let λ_1 and λ_2 be two words of distinct integers such that $\text{reduce}(\lambda_1) = \text{reduce}(\lambda_2)$. We say that λ_1 and λ_2 are order-isomorphic and we denote it by $\lambda_1 \simeq \lambda_2$.*

Definition 3 (Pattern containment). *A permutation σ is said to be contained in, or to be a subpermutation of, another permutation π , written $\sigma \preceq \pi$, if π has a (not necessarily contiguous) subsequence whose terms are order-isomorphic to σ . We also say that π admits an occurrence of the pattern σ .*

Thus, $\sigma \preceq \pi$ if there is a set I of positions in π such that $\text{reduce}(\pi|_I) = \sigma$. For example, $1423 \preceq 149362785$ since $\text{reduce}(149362785|_{\{2,3,5,8\}}) = \text{reduce}(4968) = 1423$.

Definition 4 (Trivial bijections). *Let $\pi = \pi(1)\pi(2) \dots \pi(n)$ be a permutation of size n . The reverse of π is the permutation $r(\pi) = \pi(n)\pi(n-1) \dots \pi(1)$. The complement of π is the permutation $c(\pi) = \pi'(1)\pi'(2) \dots \pi'(n)$, where $\pi'(i) = n - \pi(i) + 1$. The inverse is the regular group theoretical inverse on permutations, that is the $\pi(i)$ -th position of the inverse $i(\pi)$ is occupied by i . The reverse, complement and inverse are called the trivial bijections from S_n to itself.*

Abusing notations, for any $S \subseteq S_n$, we let $c(S)$, $i(S)$ and $r(S)$ stand respectively for $\{c(\pi) : \pi \in S\}$, $\{i(\pi) : \pi \in S\}$ and $\{r(\pi) : \pi \in S\}$.

Definition 5 (Shuffle). *Let $\sigma_1 \in S_{k_1}$ and $\sigma_2 \in S_{k_2}$ be two permutations. A permutation $\pi = \pi(1)\pi(2) \dots \pi(k_1 + k_2)$ is a shuffle of σ_1 and σ_2 if there is a subset I of $[n]$ such that $\pi|_I \simeq \sigma_1$ and $\pi|_{\bar{I}} \simeq \sigma_2$, where $\bar{I} = [n] \setminus I$ and $n = k_1 + k_2$.*

In other terms, π is obtained by interleaving the letters of two words respectively order-isomorphic with σ_1 and σ_2 . We denote by $\sigma_1 \sqcup \sigma_2$ the set of all shuffles of σ_1 and σ_2 .

For example,

$$12 \sqcup 21 = \{1243, 1324, 1342, 1423, 1432, 2134, 2314, 2341, 2413, 2431, \\ 3124, 3142, 3214, 3241, 3421, 4123, 4132, 4213, 4231, 4312\}.$$

We are now ready to define the f -UNSHUFFLE-PERMUTATION problem we focus on in this paper.

Definition 6 (f -Unshuffle-Permutation). *Given a permutation $\pi \in S_{2n}$ and a bijective mapping $f : S_n \rightarrow S_n$, the f -UNSHUFFLE-PERMUTATION problem is to decide whether there exists a permutation $\sigma \in S_n$ such that $\pi \in \sigma \sqcup f(\sigma)$.*

3 Generalized square permutations and enumerative properties

The bijections c , i , and r are involutions and can be seen as particular elements of the dihedral group D_4 encoding all the symmetries of the square. Before explaining why, let us recall a definition for D_4 .

The group D_4 is generated by two elements a and b subjected exactly to the nontrivial relations

$$aa = \epsilon, \quad bbbb = \epsilon, \quad abab = \epsilon, \quad (1)$$

where ϵ is the unit of D_4 . One can think of element a (resp. b) acting on a square by performing a symmetry through the vertical axis (resp. a 90°clockwise rotation). Now, we can regard, for any $n \in \mathbb{N}$, each element of D_4 as a map $\phi : S_n \rightarrow S_n$ such that $\phi(\pi)$, $\pi \in S_n$, is the permutation obtained by performing on its permutation matrix the transformations specified by ϕ . The maps c , i , and r can thus be expressed as

$$c = bba, \quad i = ba, \quad r = a. \quad (2)$$

Figure 1 shows the Cayley graph of this group. The main interest of seeing the three trivial bijections on S_n as elements of D_4 lies in the fact that all the other bijections obtained by composing the trivial ones can be expressed by compositions of the two elements a and b . This will allow us to gain concision in some proofs presented in the sequel.

We now turn to defining *identity squares*, *complement squares*, *reverse squares* and *inverse squares* that are natural generalizations of square permutations to trivial bijections from S_n to itself.

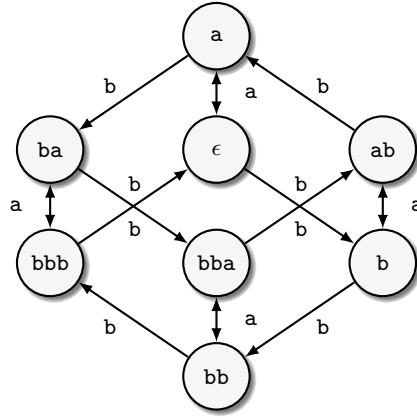


Fig. 1. The Cayley graph of the group D_4 .

Definition 7 (Square permutations for trivial bijections). For $n \in \mathbb{N}$, define

$$\begin{aligned} \mathcal{S}_{2n}^\epsilon &= \{\pi \in S_{2n} : \exists \sigma \in S_n, \text{ such that } \pi \in \sigma \sqcup \sigma\}, \\ \mathcal{S}_{2n}^c &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup c(\sigma)\}, \\ \mathcal{S}_{2n}^r &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup r(\sigma)\}, \\ \mathcal{S}_{2n}^i &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup i(\sigma)\}. \end{aligned}$$

We begin by proving that applying any trivial bijection is in some sense compatible with the shuffle operator.

Lemma 1 (Trivial bijections and shuffle). Let π, σ_1 and σ_2 be permutations such that $\pi \in \sigma_1 \sqcup \sigma_2$. Then

- $c(\pi) \in c(\sigma_1) \sqcup c(\sigma_2)$;
- $r(\pi) \in r(\sigma_1) \sqcup r(\sigma_2)$;
- $i(\pi) \in i(\sigma_1) \sqcup i(\sigma_2)$.

Proof. Let n be the size of π . Since π is a shuffle of σ_1 and σ_2 , there is a subset $I = \{i_1 < \dots < i_k\}$ of $[n]$ such that $\pi|_I \simeq \sigma_1$ and $\pi|_{\bar{I}} \simeq \sigma_2$.

By setting $J = \{n - i_k + 1 < \dots < n - i_1 + 1\}$, we have

$$r(\pi)|_J = (\pi(n) \dots \pi(1))|_J = \pi(i_k) \dots \pi(i_1) \simeq r(\sigma_1). \quad (3)$$

For the same reason, we have also $r(\pi)|_{\bar{J}} \simeq r(\sigma_2)$. Hence, $r(\pi)$ is a shuffle of $r(\sigma_1)$ and $r(\sigma_2)$.

Now, set $J = \{\pi(i) : i \in I\} = \{\pi(\ell_1) < \dots < \pi(\ell_k)\}$ where ℓ_1, \dots, ℓ_k are elements of I . We have

$$i(\pi)|_J = (\pi^{-1}(1) \dots \pi^{-1}(n))|_J = \pi^{-1}(\pi(\ell_1)) \dots \pi^{-1}(\pi(\ell_k)) = \ell_1 \dots \ell_k \simeq i(\sigma_1). \quad (4)$$

For the same reason, we have also $i(\pi)_{|\bar{j}} \simeq i(\sigma_2)$. Hence, $i(\pi)$ is also shuffle of $i(\sigma_1)$ and $i(\sigma_2)$.

Finally, since $b = i \circ r$ in D_4 , the map c can be expressed as compositions involving r and i . Hence, $c(\pi)$ is a shuffle of $c(\pi_1)$ and $c(\pi_2)$. ■

The following lemma is well-known and is a consequence of interpreting c , r , and i as compositions involving a and b according to (2) and the relations (1) between a and b .

Lemma 2 (Compositions of trivial bijections). *For any permutation π ,*

- $(c \circ r)(\pi) = (r \circ c)(\pi)$;
- $(i \circ c)(\pi) = (r \circ i)(\pi)$;
- $(i \circ r)(\pi) = (c \circ i)(\pi)$.

According to Lemma 2 (and the fact that the group D_4 has exactly eight elements), we thus only need to consider the following compositions in the rest of the paper.

Definition 8 (Square permutations for compositions of trivial bijections). *For $n \in \mathbb{N}$, define*

$$\begin{aligned} \mathcal{S}_{2n}^{\text{rc}} &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup (r \circ c)(\sigma)\}, \\ \mathcal{S}_{2n}^{\text{ci}} &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup (c \circ i)(\sigma)\}, \\ \mathcal{S}_{2n}^{\text{ic}} &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup (i \circ c)(\sigma)\}, \\ \mathcal{S}_{2n}^{\text{irc}} &= \{\pi \in S_{2n} : \exists \sigma \in S_n \text{ such that } \pi \in \sigma \sqcup (i \circ r \circ c)(\sigma)\}. \end{aligned}$$

We hence obtain the eight sets $\mathcal{S}_{2n}^{\epsilon}$, \mathcal{S}_{2n}^c , \mathcal{S}_{2n}^r , \mathcal{S}_{2n}^i , $\mathcal{S}_{2n}^{\text{rc}}$, $\mathcal{S}_{2n}^{\text{ci}}$, $\mathcal{S}_{2n}^{\text{ic}}$, and $\mathcal{S}_{2n}^{\text{irc}}$ of square permutations provided by Definitions 7 and 8. Let us now investigate some easy bijective and enumerative properties satisfied by these sets.

Proposition 1 (Bijection between \mathcal{S}_{2n}^c and \mathcal{S}_{2n}^r). *For any $n \in \mathbb{N}$, $i(\mathcal{S}_{2n}^c) = \mathcal{S}_{2n}^r$.*

Proof. Let $\pi \in S_{2n}$. We have

$$\begin{aligned} \pi \in \mathcal{S}_{2n}^c &\Leftrightarrow \exists \sigma \in S_n, \pi \in \sigma \sqcup c(\sigma) \\ &\Leftrightarrow \exists \sigma \in S_n, i(\pi) \in i(\sigma) \sqcup (i \circ c)(\sigma) && \text{(Lemma 1)} \\ &\Leftrightarrow \exists \sigma \in S_n, i(\pi) \in i(\sigma) \sqcup (r \circ i)(\sigma) && \text{(Lemma 2)} \\ &\Leftrightarrow \exists \sigma \in S_n, i(\pi) \in \sigma \sqcup r(\sigma) \\ &\Leftrightarrow i(\pi) \in \mathcal{S}_{2n}^r. && \blacksquare \end{aligned}$$

Proposition 2 (Bijection between $\mathcal{S}_{2n}^{\text{ic}}$ and $\mathcal{S}_{2n}^{\text{ci}}$). *For any $n \in \mathbb{N}$, $c(\mathcal{S}_{2n}^{\text{ic}}) = \mathcal{S}_{2n}^{\text{ci}}$, $i(\mathcal{S}_{2n}^{\text{ic}}) = \mathcal{S}_{2n}^{\text{ci}}$, and $r(\mathcal{S}_{2n}^{\text{ic}}) = \mathcal{S}_{2n}^{\text{ci}}$.*

Proof. Let $\pi \in S_{2n}$. We have

$$\begin{aligned}
\pi \in \mathcal{S}_{2n}^{\text{ic}} &\Leftrightarrow \exists \sigma \in S_n, \pi \in \sigma \sqcup (\text{i} \circ \text{c})(\sigma) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{c}(\pi) \in \text{c}(\sigma) \sqcup (\text{c} \circ \text{i} \circ \text{c})(\sigma) & (\text{Lemma 1}) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{c}(\pi) \in \sigma \sqcup (\text{c} \circ \text{i})(\sigma) \\
&\Leftrightarrow \text{c}(\pi) \in \mathcal{S}_{2n}^{\text{ci}}.
\end{aligned}$$

Moreover, we have

$$\begin{aligned}
\pi \in \mathcal{S}_{2n}^{\text{ic}} &\Leftrightarrow \exists \sigma \in S_n, \pi \in \sigma \sqcup (\text{i} \circ \text{c})(\sigma) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{i}(\pi) \in \text{i}(\sigma) \sqcup (\text{i} \circ \text{i} \circ \text{c})(\sigma) & (\text{Lemma 1}) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{i}(\pi) \in \text{i}(\sigma) \sqcup (\text{i} \circ \text{r} \circ \text{i})(\sigma) & (\text{Lemma 2}) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{i}(\pi) \in \sigma \sqcup (\text{i} \circ \text{r})(\sigma) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{i}(\pi) \in \sigma \sqcup (\text{c} \circ \text{i})(\sigma) & (\text{Lemma 2}) \\
&\Leftrightarrow \text{i}(\pi) \in \mathcal{S}_{2n}^{\text{ci}}.
\end{aligned}$$

Finally, the fact that $\text{i} \circ \text{c} \circ \text{i} = \text{r}$ implies that r is also a bijection between $\mathcal{S}_{2n}^{\text{ic}}$ and $\mathcal{S}_{2n}^{\text{ci}}$. \blacksquare

Proposition 3 (Bijection between $\mathcal{S}_{2n}^{\text{i}}$ and $\mathcal{S}_{2n}^{\text{irc}}$). *For any $n \in \mathbb{N}$, $(\text{i} \circ \text{c})(\mathcal{S}_{2n}^{\text{irc}}) = \mathcal{S}_{2n}^{\text{i}}$.*

Proof. Let $\pi \in S_{2n}$. We have

$$\begin{aligned}
\pi \in \mathcal{S}_{2n}^{\text{irc}} &\Leftrightarrow \exists \sigma \in S_n, \pi \in \sigma \sqcup (\text{i} \circ \text{r} \circ \text{c})(\sigma) \\
&\Leftrightarrow \exists \sigma \in S_n, \text{i}(\pi) \in \text{i}(\sigma) \sqcup (\text{r} \circ \text{c})(\sigma) & (\text{Lemma 1}) \\
&\Leftrightarrow \exists \sigma \in S_n, (\text{r} \circ \text{i})(\pi) \in (\text{r} \circ \text{i})(\sigma) \sqcup \text{c}(\sigma) & (\text{Lemma 1}) \\
&\Leftrightarrow \exists \sigma \in S_n, (\text{i} \circ \text{c})(\pi) \in (\text{i} \circ \text{c})(\sigma) \sqcup \text{c}(\sigma) & (\text{Lemma 2}) \\
&\Leftrightarrow \exists \sigma \in S_n, (\text{i} \circ \text{c})(\pi) \in \text{i}(\sigma) \sqcup \sigma \\
&\Leftrightarrow (\text{i} \circ \text{c})(\pi) \in \mathcal{S}_{2n}^{\text{i}}.
\end{aligned}$$

\blacksquare

To simplify notations, we write $s_{2n}^{\epsilon}, s_{2n}^{\text{c}}, s_{2n}^{\text{r}}, s_{2n}^{\text{i}}, s_{2n}^{\text{rc}}, s_{2n}^{\text{ci}}, s_{2n}^{\text{ic}}$, and s_{2n}^{irc} for the cardinalities of the sets $\mathcal{S}_{2n}^{\epsilon}, \mathcal{S}_{2n}^{\text{c}}, \mathcal{S}_{2n}^{\text{r}}, \mathcal{S}_{2n}^{\text{i}}, \mathcal{S}_{2n}^{\text{rc}}, \mathcal{S}_{2n}^{\text{ci}}, \mathcal{S}_{2n}^{\text{ic}}$, and $\mathcal{S}_{2n}^{\text{irc}}$, respectively. Table 1 shows the first cardinalities. We note that, at this time, none of the corresponding integer sequence does appear in OEIS [10].

Lemma 3 (Upper bound for the number of generalized squares). *For any $n \in \mathbb{N}$,*

$$|Q_{2n}| \leq \binom{2n-1}{n-1} \binom{2n}{n} n!, \quad (5)$$

where Q_{2n} is any of the sets $\mathcal{S}_{2n}^{\epsilon}, \mathcal{S}_{2n}^{\text{c}}, \mathcal{S}_{2n}^{\text{r}}, \mathcal{S}_{2n}^{\text{i}}, \mathcal{S}_{2n}^{\text{rc}}, \mathcal{S}_{2n}^{\text{ci}}, \mathcal{S}_{2n}^{\text{ic}}$, or $\mathcal{S}_{2n}^{\text{irc}}$.

n	0	1	2	3	4	5
s_{2n}^{rc}	1	2	20	472	18 988	1 112 688
$s_{2n}^c = s_{2n}^r$	1	2	20	480	19 744	1 185 264
$s_{2n}^i = s_{2n}^{irc}$	1	2	20	488	20 250	1 229 858
s_{2n}^e	1	2	20	504	21 032	1 293 418
$s_{2n}^{ci} = s_{2n}^{ic}$	1	2	20	586	27 990	2 044 596
$(2n)!$	1	2	24	720	40 320	3 628 800

Table 1. Cardinalities of the sets of square permutations of sizes $0 \leq 2n \leq 10$.

Proof. This is a consequence of the fact that to construct a permutation π of Q_{2n} , we can proceed by first choosing a set of n letters among the alphabet $[2n]$ ($\binom{2n}{n}$ choices), then by specifying an order from left to right for these letters ($n!$ choices), and finally by deploying the chosen letters onto a set I of n positions among the set of all possible positions $[2n]$ ($\binom{2n}{n}$ choices). The empty positions are filled by the unique authorized completion such that $\pi|_I \simeq \phi(\pi|_{\bar{I}})$ where ϕ is the considered bijection on S_n . For this reason, there is no more than $\binom{2n}{n}^2 n!$ elements in Q_{2n} . The tighter bound (5) is the consequence of the fact that we can assume that the first position can always be fixed. ■

Let us denote by $\mathcal{S}^{\bullet}_{2n}$ the union of all the sets $\mathcal{S}_{2n}^e, \mathcal{S}_{2n}^c, \mathcal{S}_{2n}^r, \mathcal{S}_{2n}^i, \mathcal{S}_{2n}^{rc}, \mathcal{S}_{2n}^{ci}, \mathcal{S}_{2n}^{ic}$, and \mathcal{S}_{2n}^{irc} . We show that S_{2n} and $\mathcal{S}^{\bullet}_{2n}$ do not coincide.

Proposition 4 (Existence of non-square permutations). *For any $n \in \mathbb{N}, n \geq 9, S_{2n} \neq \mathcal{S}^{\bullet}_{2n}$.*

Proof. By Lemma 3 (and using its notations), we have

$$|\mathcal{S}^{\bullet}_{2n}| \leq 8 |Q_{2n}| \leq 8 \binom{2n-1}{n-1} \binom{2n}{n} n!. \quad (6)$$

The proportion of the elements of $\mathcal{S}^{\bullet}_{2n}$ among all the permutations of S_{2n} admits as upper bound, when $n \geq 1$,

$$\frac{|\mathcal{S}^{\bullet}_{2n}|}{|S_{2n}|} \leq \frac{8 \binom{2n-1}{n-1} \binom{2n}{n} n!}{(2n)!} = 4 \binom{2n}{n} \frac{1}{n!}. \quad (7)$$

But $4 \binom{2n}{n} \frac{1}{n!} < 1$ for $n \geq 9$, thereby proving the result. ■

Proposition 5 (Square permutations in some intersections). *Let $n \in \mathbb{N}$ such that $2n \equiv 0 \pmod{4}$. Then,*

the permutation $\pi = 12 \dots (n-1)(n) \ (2n)(2n-1) \dots (n+2)(n+1)$ belongs to $\mathcal{S}_{2n}^e \cap \mathcal{S}_{2n}^r \cap \mathcal{S}_{2n}^c \cap \mathcal{S}_{2n}^i \cap \mathcal{S}_{2n}^{ci} \cap \mathcal{S}_{2n}^{ic}$.

Proof. Let $I = \{1, 3, 5, \dots, 2n-1\}$ and $\bar{I} = [2n] \setminus I$. Then, since

$$\pi|_I \simeq 12 \dots \frac{n}{2} \ n(n-1) \dots \left(\frac{n}{2} + 1\right) \simeq \pi|_{\bar{I}}, \quad (8)$$

we have $\pi|_I \simeq \pi|_{\bar{I}} \simeq i(\pi|_{\bar{I}})$. This shows that π belongs to $\mathcal{S}_{2n}^\epsilon \cap \mathcal{S}_{2n}^i$.

Now, let $J = \{1, 2, \dots, n\}$ and $\bar{J} = [2n] \setminus J$. Then, since

$$\pi|_J \simeq 12 \dots n \quad \text{and} \quad \pi|_{\bar{J}} \simeq n \dots 21, \quad (9)$$

we have $\pi|_J \simeq r(\pi|_{\bar{J}}) \simeq c(\pi|_{\bar{J}}) \simeq (i \circ c)(\pi|_{\bar{J}}) \simeq (c \circ i)(\pi|_{\bar{J}})$. This shows that π belongs to $\mathcal{S}_{2n}^r \cap \mathcal{S}_{2n}^c \cap \mathcal{S}_{2n}^{ic} \cap \mathcal{S}_{2n}^{ci}$. ■

4 Recognizing generalized square permutations

This section is devoted to proving that deciding membership to \mathcal{S}_{2n}^r , \mathcal{S}_{2n}^c and \mathcal{S}_{2n}^{rc} is NP-complete. The approach relies on constraint directed matchings on permutations.

Definition 9 (Directed matching on permutations). Let $\pi \in S_n$. A directed matching on π is a set \mathcal{M} of pairwise disjoint arcs (i, j) , $1 \leq i, j \leq n$ and $i \neq j$, that connect pairs of elements of π . The directed matching \mathcal{M} is perfect if every element of π is the source or the sink of an arc of \mathcal{M} .

Definition 10 (Two-arcs pattern occurrences). A two-arc pattern is a perfect directed matching on the set $[4]$. A perfect directed matching \mathcal{M} on a permutation π of size $2n$ admits an occurrence of a two-arc pattern \mathcal{A} if there is an increasing map $\phi : [4] \rightarrow [2n]$ (i.e., $i < i'$ implies $\phi(i) < \phi(i')$) such that, if (i, i') is an arc of \mathcal{A} , then $(\phi(i), \phi(i'))$ is an arc of \mathcal{M} . We say moreover that \mathcal{M} avoids \mathcal{A} if \mathcal{A} does not admits any occurrence of \mathcal{A} .

We shall draw two-arcs patterns by unlabeled graphs wherein vertices are implicitly indexed from 1 to 4 from left to right. Figure 4 shows an example of a directed perfect matching on a permutation. The directed matching does contain the patterns and does avoid the patterns .

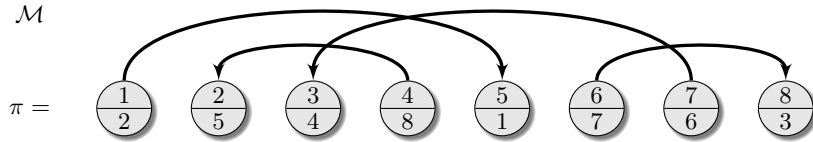


Fig. 2. A directed perfect matching $\mathcal{M} = \{(1, 5), (4, 2), (7, 3), (6, 8)\}$ on the permutation $\pi = 25481763$. Recall that arcs refer to positions in π .

In case π is written as a concatenation of contiguous patterns $\pi = \pi_1 \pi_2 \dots \pi_k$, we write $\mathcal{M}_{\pi_i \rightarrow \pi_j}$ for the subset of arcs of \mathcal{M} with source index in π_i and sink index in π_j . Hence,

$$\mathcal{M} = \bigsqcup_{\substack{i \in [k] \\ j \in [k]}} \mathcal{M}_{\pi_i \rightarrow \pi_j}. \quad (10)$$

The following properties will prove useful for defining equivalences between squares and restricted directed perfect matchings.

Definition 11 (Property \mathbf{P}_1 — Order isomorphism). Let π be a permutation. A directed perfect matching \mathcal{M} on π is said to have property \mathbf{P}_1 if, for any two distinct arcs (i, i') and (j, j') of \mathcal{M} , we have $\pi(i) < \pi(j)$ if and only if $\pi(i') < \pi(j')$.

Definition 12 (Property \mathbf{P}_2 — Order anti-isomorphism). Let π be a permutation. A directed perfect matching \mathcal{M} on π is said to have property \mathbf{P}_2 if, for any two distinct arcs (i, i') and (j, j') of \mathcal{M} , we have $\pi(i) < \pi(j)$ if and only if $\pi(i') > \pi(j')$.

Definition 13 (Property \mathbf{Q}_1 — First start first terminal). Let π be a permutation. A directed perfect matching \mathcal{M} on π is said to have property \mathbf{Q}_1 if it avoids the following set of two-arcs patterns:

$$\mathcal{Q}_1 = \left\{ \begin{array}{c} \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \\ \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \end{array} \right\}.$$

Definition 14 (Property \mathbf{Q}_2 — First start last terminal). Let π be a permutation. A directed perfect matching \mathcal{M} on π is said to have property \mathbf{Q}_2 if it avoids the following set of two-arcs patterns:

$$\mathcal{Q}_2 = \left\{ \begin{array}{c} \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \curvearrowleft \text{---} \\ \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \curvearrowright \text{---} \end{array} \right\}.$$

Observe that $\mathcal{Q}_1 \sqcup \mathcal{Q}_2$ is the set of all two-arcs patterns.

Theorem 1 ([4]). Let $\pi \in S_{2n}$. The two following statements are equivalent.






1. $\pi \in S_{2n}^\epsilon$.
2. There exists a directed perfect matching \mathcal{M} on π that satisfies properties \mathbf{P}_1 and \mathbf{Q}_1 .


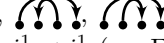
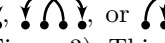
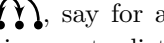
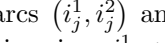
The following two definitions will intervene in the next constructions.

Definition 15 (Lifting). Let $\pi = \pi(1) \pi(2) \dots \pi(n)$ be a permutation of size n and k be a positive integer. We call k -lifting of π , denoted $\pi[k]$, the permutation $(k + \pi(1)) (k + \pi(2)) \dots (k + \pi(n))$ on the alphabet $\{k + 1, \dots, k + n\}$.

Definition 16 (Monotone). For any positive integer k , we let \nearrow_k stand for the increasing permutation $1 2 \dots k$ and \searrow_k stand for the decreasing permutation $k (k - 1) \dots 1$.

Lemma 4 (One shot lemma). Let $\pi \in S_{2n}$ and \mathcal{M} be a perfect directed matching on π that satisfies properties \mathbf{P}_i and \mathbf{Q}_j , $i \in \{1, 2\}$ and $j \in \{1, 2\}$. Then, the perfect directed matching \mathcal{M}' obtained by reversing each arc of \mathcal{M} satisfies properties \mathbf{P}_i and \mathbf{Q}_j .

Lemma 5. Let $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, and $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, be such that $I^1 \cap I^2 = \emptyset$. The directed perfect matching $\mathcal{M} = ([2n], E)$ defined by $E = \{(i_j^1, i_j^2) : j \in [n]\}$ avoids the patterns , , , , and .

Proof. Suppose, aiming at a contradiction, that \mathcal{M} does contain the pattern , , , , or , say for arcs (i_j^1, i_j^2) and (i_k^1, i_k^2) . Wlog, assume $i_j^1 < i_k^1$ (see Figure 3). This is a contradiction since $i_j^1 < i_k^1$ implies $j < k$, and hence, $i_j^2 < i_k^2$. ■

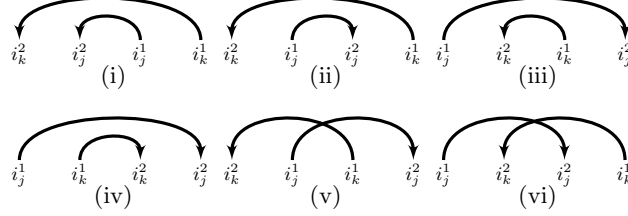

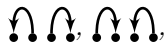




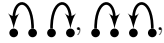
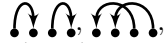



Fig. 3. Arcs (i_j^1, i_j^2) and (i_k^1, i_k^2) with $i_j^1 < i_k^1$.

Lemma 6. Let $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, and $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, be such that $I^1 \cap I^2 = \emptyset$. The directed perfect matching $\mathcal{M} = ([2n], E)$ defined by $E = \{(i_j^1, i_{n-j+1}^2) : j \in [n]\}$ avoids the patterns , , , , and .

Proof. Suppose, aiming at a contradiction, that \mathcal{M} does contain the pattern , , , or , say for arcs (i_j^1, i_{n-j+1}^2) and (i_k^1, i_{n-k+1}^2) . Wlog, assume $i_j^1 < i_k^1$ (see Figure 4). This is a contradiction since $i_j^1 < i_k^1$ implies $j < k$, and hence, $i_{n-j+1}^2 > i_{n-k+1}^2$. ■

Proposition 6. Let $\pi \in S_{2n}$. The two following statements are equivalent.

1. $\pi \in \mathcal{S}_{2n}^r$.
2. There exists a directed perfect matching \mathcal{M} on π that satisfies properties **P₁** and **Q₂**.

Proof. (1 \Rightarrow 2) Let $\pi \in \mathcal{S}_{2n}^r$. Then, there exists $\sigma \in S_n$ such that $\pi \in \sigma \sqcup r(\sigma)$, and hence there exist two disjoint set of indexes $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, and $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, such that

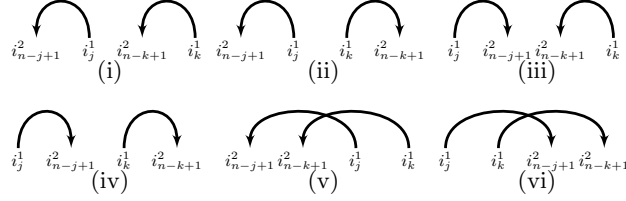


Fig. 4. Arcs (i_j^1, i_{n-j+1}^2) and (i_k^1, i_{n-k+1}^2) with $i_j^1 < i_k^2$.

$\pi(i_1^1)\pi(i_2^1)\cdots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\cdots\pi(i_n^2)$ is order-isomorphic to $r(\sigma)$. Let $\mathcal{M} = (V, E)$ be the directed graph defined by $V = [2n]$ and $E = \{(i_j^1, i_{n-j+1}^2) : j \in [n]\}$. Clearly, \mathcal{M} is a directed perfect matching since $I^1 \cap I^2 = \emptyset$ and $I^1 \cup I^2 = [2n]$. According to Lemma 6, \mathcal{M} does avoid the patterns . Finally, for any two distinct arcs (i_j^1, i_{n-j+1}^2) and (i_k^1, i_{n-k+1}^2) of \mathcal{M} , we have $\pi(i_j^1) < \pi(i_k^1)$ if and only if $\pi(i_{n-j+1}^2) < \pi(i_{n-k+1}^2)$ since $\pi(i_1^1)\pi(i_2^1)\cdots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\cdots\pi(i_n^2)$ is order-isomorphic to $r(\sigma)$. Therefore, \mathcal{M} satisfies properties **P₁** and **Q₂**.

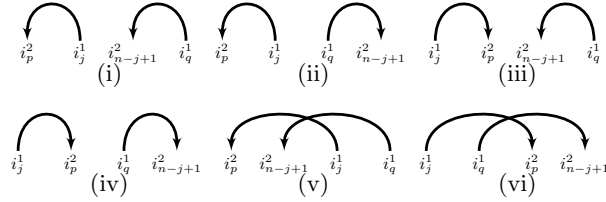





Fig. 5. All possible configurations considered in Proof of Proposition 6 (**2** \Rightarrow **1**).

(2 \Rightarrow 1) Let \mathcal{M} be a directed perfect matching that satisfies properties **P₁** and **Q₂**. Let $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \cdots < i_n^1$, be the set of the sources of the arcs of \mathcal{M} and let $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \cdots < i_n^2$, be the set of the sinks of the arcs of \mathcal{M} . We first show that, for every $j \in [n]$, (i_j^1, i_{n-j+1}^2) is an arc of \mathcal{M} . The proof is by induction on $j = 1, 2, \dots, n$.




- Base. Suppose, aiming at a contradiction that (i_1^1, i_n^2) is not an arc of \mathcal{M} . Then, there exist $1 \leq p < n$ and $1 < q \leq n$ such that (i_1^1, i_p^2) and (i_q^1, i_n^2) are two arcs of \mathcal{M} . But $i_1^1 < i_q^1$ and $i_p^2 < i_n^2$, and hence one of the configurations of Figure 5 (with $j = 1$ and $k = n$) does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property **Q₂**, and hence (i_1^1, i_n^2) is an arc of \mathcal{M} .
- Induction step. Assume that (i_k^1, i_{n-k+1}^2) is an arc of \mathcal{M} for $1 \leq k < j$, and suppose, aiming at a contradiction, that (i_j^1, i_{n-j+1}^2) is not an arc of \mathcal{M} .

Then, there exist $1 \leq p < n - j + 1$ and $j < q \leq n$ such that (i_j^1, i_p^2) and (i_q^1, i_{n-j+1}^2) are two arcs of \mathcal{M} . But $i_j^1 < i_q^1$ and $i_p^2 < i_{n-j+1}^2$, and hence one of the configurations of Figure 5 does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property **Q**₂, and hence (i_j^1, i_{n-j+1}^2) is an arc of \mathcal{M} .

Now, let σ_1 be the pattern of π induced by the sources of \mathcal{M} and σ_2 be the pattern of π induced by the sinks of \mathcal{M} (i.e., $\sigma_1 = \pi(i_1^1) \pi(i_2^1) \dots \pi(i_n^1)$ and $\sigma_2 = \pi(j_1^2) \pi(j_2^2) \dots \pi(i_n^2)$). Clearly σ_1 and σ_2 are disjoint in π (since \mathcal{M} is a matching) and cover π (since \mathcal{M} is perfect). Moreover, the fact that \mathcal{M} satisfies **P**₁ implies immediately that $\text{reduce}(\sigma_1)$ is order-isomorphic to $(\text{reduce} \circ r)(\sigma_2)$, and hence this shows that $\pi \in \mathcal{S}_{2n}^r$. ■

Lemma 7. *Let $\pi \in S_{2n}$ and \mathcal{M} be a perfect directed matching on π that avoids the patterns , , and . Then, for any arc $(i, j) \in \mathcal{M}$, either $1 \leq i \leq n < j \leq 2n$ or $1 \leq j \leq n < i \leq 2n$.*

Proof. We only prove the case $1 \leq i \leq n < j \leq 2n$ since the proof for $1 \leq j \leq n < i \leq 2n$ is similar.


Suppose, aiming at a contradiction, that there exists an arc $(i, j) \in \mathcal{M}$ with $1 \leq i < j \leq n$. Since \mathcal{M} avoids the patterns , , and , there is no arc $(k, \ell) \in \mathcal{M}$ with $j < k \leq 2n$ and $j < \ell \leq 2n$, $k \neq \ell$. Then it follows that there exist $2n - j \geq n$ distinct arcs $(k, \ell) \in \mathcal{M}$ with $1 \leq \min\{k, \ell\} \leq j - 1$ and $j + 1 \leq \max\{k, \ell\} \leq 2n$, $k \neq \ell$. This is a contradiction since $(i, j) \in \mathcal{M}$ with $1 \leq i < j \leq n$. ■

The following technical lemma is needed to simplify the proof of upcoming Proposition 7.

Lemma 8. *Let $k, \ell_1, \ell_2, \ell_3$ and ℓ_4 be positive integers and $\pi \in \mathcal{S}_{2k+\ell_1+\ell_2+\ell_3+\ell_4}^r$ be the permutation defined by $\pi = X_1 \ L \ X_2 \ X_3 \ R \ X_4$, where $X_1 = \mu_1[k + \ell_2]$, $L = \nearrow_k [\ell_2]$, $X_2 = \mu_2$, $X_3 = \mu_3[k + \ell_1 + \ell_2]$, $R = \searrow_k [k + \ell_1 + \ell_2 + \ell_3]$ and $X_4 = \mu_4[2k + \ell_1 + \ell_2 + \ell_3]$ for some permutations $\mu_i \in S_{\ell_i}$, $1 \leq i \leq 4$ (see Figure 6). Let \mathcal{M} be a directed perfect matching on π that satisfies properties **P**₁ and **Q**₂. If $\mathcal{M}_{L \rightarrow R} \neq \emptyset$ or $\mathcal{M}_{R \rightarrow L} \neq \emptyset$, then either $|\mathcal{M}_{L \rightarrow R}| = k$ or $|\mathcal{M}_{R \rightarrow L}| = k$.*

Proof. Suppose first, aiming at a contradiction, that $\mathcal{M}_{L \rightarrow R} \neq \emptyset$ and $\mathcal{M}_{R \rightarrow L} \neq \emptyset$. Let $(i, j) \in \mathcal{M}_{L \rightarrow R}$ and $(i', j') \in \mathcal{M}_{R \rightarrow L}$. By construction, we have $\pi(i) < \pi(i')$ and $\pi(j) > \pi(j')$ thereby contradicting Property **P**₁. Then it follows that either $\mathcal{M}_{L \rightarrow R} \neq \emptyset$ or $\mathcal{M}_{R \rightarrow L} \neq \emptyset$, but not both.

Suppose now that $\mathcal{M}_{L \rightarrow R} \neq \emptyset$ and $\mathcal{M}_{R \rightarrow L} = \emptyset$ (the case $\mathcal{M}_{L \rightarrow R} = \emptyset$ and $\mathcal{M}_{R \rightarrow L} \neq \emptyset$ can be proved with the same arguments). Suppose, aiming at a contradiction, that $|\mathcal{M}_{L \rightarrow R}| \neq k$ and let $(i, j) \in \mathcal{M}_{L \rightarrow R}$. According to Lemma 7, we are left with considering the four following cases.

- There exists $(i', j') \in \mathcal{M}_{L \rightarrow \mu_3}$. Since \mathcal{M} avoids , we have $i < i'$, and hence $\pi(i) < \pi(i')$ and $\pi(j) > \pi(j')$. This is a contradiction since \mathcal{M} satisfies Property **P**₁.

- There exists $(i', j') \in \mathcal{M}_{\mu_3 \rightarrow L}$ and hence $\pi(i) < \pi(i')$ and $\pi(j) > \pi(j')$. This is a contradiction since \mathcal{M} satisfies Property \mathbf{P}_1 .
- There exists $(i', j') \in \mathcal{M}_{L \rightarrow \mu_4}$. Since \mathcal{M} avoids $\begin{array}{c} \curvearrowright \\ \curvearrowright \end{array}$, we have $i' < i$, and hence $\pi(i) > \pi(i')$ and $\pi(j) < \pi(j')$. This is a contradiction since \mathcal{M} satisfies Property \mathbf{P}_1 .
- There exists $(i', j') \in \mathcal{M}_{\mu_4 \rightarrow L}$ and hence $\pi(i) < \pi(i')$ and $\pi(j) > \pi(j')$. This is a contradiction since \mathcal{M} satisfies Property \mathbf{P}_1 .

Therefore, $|\mathcal{M}_{L \rightarrow R}| = k$. ■

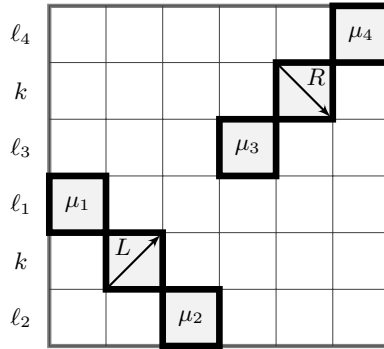


Fig. 6. Illustration of Lemma 8, where $\pi = X_1 \ L \ X_2 \ X_3 \ R \ X_4$.

Proposition 7. \mathbf{r} -UNSHUFFLE-PERMUTATION is NP-complete.

Proof. We reduce from PERMUTATION PATTERN which, given two permutations $\pi \in S_n$ and $\sigma \in S_k$ with $k \leq n$, asks whether σ is a pattern of π . PERMUTATION PATTERN is known to be NP-complete [1]. Let $\pi \in S_n$ and $k \in S_k$ be an instance of PERMUTATION PATTERN. Set $N_2 = n + k + 1$ and $N_1 = 2N_2$. Define a target permutation $\mu \in S_{2n+2k+2N_1+2N_2}$ by $\mu = \mu_\pi \ \mu_2 \ \mu_1 \ \mu_\sigma \ \mu'_2 \ \mu'_\pi \ \mu'_1 \ \mu'_\sigma$, where

$$\begin{aligned}
 \mu_\sigma &= \sigma, & \mu_\pi &= \pi[k + N_1 + N_2], \\
 \mu'_\pi &= \mathbf{r}(\pi)[2n + k + 2N_1 + 2N_2] & \mu'_\sigma &= \mathbf{r}(\sigma)[n + k + N_1 + 2N_2], \\
 \mu_1 &= \nearrow_{N_1} [k], & \mu'_1 &= \searrow_{N_1} [2n + k + N_1 + 2N_2], \\
 \mu_2 &= \nearrow_{N_2} [k + N_1], & \mu'_2 &= \searrow_{N_2} [n + k + N_1 + N_2].
 \end{aligned}$$

Clearly, the construction can be carried out in polynomial time. We claim that σ is a pattern of π if and only if $\mu \in \mathcal{S}_{2n+2k+2N_1+2N_2}^{\mathbf{r}}$.

(\Rightarrow) Suppose that σ is a pattern of π . Then there exist indices $P = \{p_1, p_2, \dots, p_k\}$, $1 \leq p_1 < p_2 < \dots < p_k \leq n$, such that σ and $\pi(p_1)\pi(p_2)\dots\pi(p_k)$ are order-isomorphic. For the sake of simplification, let $Q = [n] \setminus P$ and write

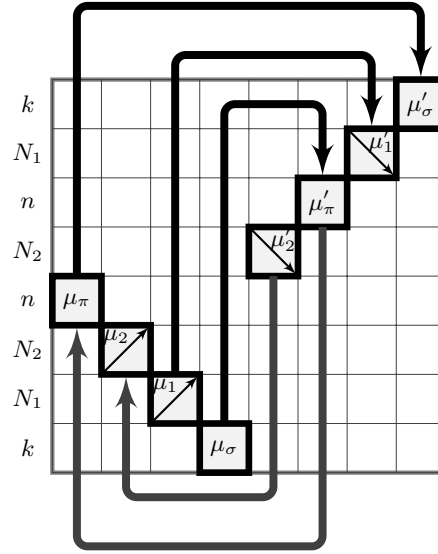


Fig. 7. Schematic representation of the construction used in Proposition 7.

$Q = \{q_1, q_2, \dots, q_{n-k}\}$, $1 \leq q_1 < q_2 < \dots < q_{n-k} \leq n$. Define a directed matching

$$\mathcal{M} = \mathcal{M}_{\mu_\sigma \rightarrow \mu'_\pi} \uplus \mathcal{M}_{\mu'_\pi \rightarrow \mu_\pi} \uplus \mathcal{M}_{\mu_\pi \rightarrow \mu'_\sigma} \uplus \mathcal{M}_{\mu_1 \rightarrow \mu'_1} \uplus \mathcal{M}_{\mu'_2 \rightarrow \mu_2}$$

on μ as follows.

$$\begin{aligned} \mathcal{M}_{\mu_\sigma \rightarrow \mu'_\pi} &= \{(n + N_1 + N_2 + i, n + k + N_1 + 2N_2 + p_i) : 1 \leq i \leq k\} \\ \mathcal{M}_{\mu'_\pi \rightarrow \mu_\pi} &= \{(2n + k + N_1 + 2N_2 - q_i + 1, q_i) : 1 \leq i \leq n - k\} \\ \mathcal{M}_{\mu_\pi \rightarrow \mu'_\sigma} &= \{(p_i, 2n + 2k + 2N_1 + 2N_2 - i) : 1 \leq i \leq k\} \\ \mathcal{M}_{\mu_1 \rightarrow \mu'_1} &= \{(n + N_2 + i, 2n + k + 2N_1 + 2N_2 - i + 1) : 1 \leq i \leq N_1\} \\ \mathcal{M}_{\mu'_2 \rightarrow \mu_2} &= \{(n + k + N_1 + 2N_2 - i + 1, n + i) : 1 \leq i \leq N_2\}. \end{aligned}$$

Informally,

- $\mathcal{M}_{\mu_\sigma \rightarrow \mu'_\pi}$ is the directed (left-to-right) matching describing the (reversed) occurrence of σ in $r(\pi)$,
- $\mathcal{M}_{\mu'_\pi \rightarrow \mu_\pi}$ is the directed (right-to-left) matching connecting the elements of $r(\pi)$ and π that are not part of the occurrence of σ in π ,
- $\mathcal{M}_{\mu_\pi \rightarrow \mu'_\sigma}$ is the directed (left-to-right) matching describing the (reversed) occurrence of $r(\sigma)$ in π ,
- $\mathcal{M}_{\mu_1 \rightarrow \mu'_1}$ is a directed (left-to-right) matching that fully connects μ_1 to μ'_1 and
- $\mathcal{M}_{\mu'_2 \rightarrow \mu_2}$ is a directed (right-to-left) matching that fully connects μ'_2 to μ_2 .

It is now a simple matter to check that \mathcal{M} is a directed matching on μ that satisfies properties \mathbf{P}_1 and \mathbf{Q}_2 . Therefore, according to Proposition 6, $\mu \in \mathcal{S}_{2n+2k+2N_1+2N_2}^r$.

(\Leftarrow) Suppose that $\mu \in \mathcal{S}_{2n}^r$. Therefore, according to Proposition 6, there exists a directed perfect matching \mathcal{M} on μ that satisfies properties \mathbf{P}_1 and \mathbf{Q}_2 . We begin with a sequence of claims that help defining the general structure of \mathcal{M} .

Claim. We may assume that $|\mathcal{M}_{\mu_1 \rightarrow \mu'_1}| = N_1$.

Proof. Combining Lemma 7 and $N_1 = 2N_2 > n + k + N_2$, we conclude that $\mathcal{M}_{\mu_1 \rightarrow \mu'_1} \neq \emptyset$ or $\mathcal{M}_{\mu'_1 \rightarrow \mu_1} \neq \emptyset$. Thus, applying Lemma 8, we obtain $|\mathcal{M}_{\mu_1 \rightarrow \mu'_1}| = N_1$ or $|\mathcal{M}_{\mu'_1 \rightarrow \mu_1}| = N_1$. Therefore, by Lemma 4 (One shot lemma), we may assume that $\mathcal{M}_{\mu_1 \rightarrow \mu'_1} \neq \emptyset$. ■

Claim. Assuming $|\mathcal{M}_{\mu_1 \rightarrow \mu'_1}| = N_1$, we have $|\mathcal{M}_{\mu'_2 \rightarrow \mu_2}| = N_2$.

Proof. Combining Claim 4, Lemma 7 and $N_2 > n + k$, we conclude that $\mathcal{M}_{\mu_2 \rightarrow \mu'_2} \neq \emptyset$ or $\mathcal{M}_{\mu'_2 \rightarrow \mu_2} \neq \emptyset$. Applying Lemma 8, we obtain $|\mathcal{M}_{\mu_2 \rightarrow \mu'_2}| = N_2$ or $|\mathcal{M}_{\mu'_2 \rightarrow \mu_2}| = N_2$. The claim now follows from $\mathcal{M}_{\mu_1 \rightarrow \mu'_1} \neq \emptyset$ (Claim 4) and the fact that \mathcal{M} avoids \curvearrowright (Property \mathbf{Q}_2). ■

From the above two claims and the fact that \mathcal{M} avoids \curvearrowright (Property \mathbf{Q}_2), we conclude that $|\mathcal{M}_{\mu_\sigma \rightarrow \mu'_\pi}| = k$. But \mathcal{M} satisfies Property \mathbf{P}_1 and hence there exists an occurrence of $r(\sigma)$ in $r(\pi)$. It follows that σ is a pattern of π . ■

Proposition 8. *Let $\pi \in S_{2n}$. The two following statements are equivalent.*

1. $\pi \in \mathcal{S}_{2n}^c$.
2. *There exists a directed perfect matching \mathcal{M} that satisfies properties \mathbf{P}_2 and \mathbf{Q}_1 .*

Proof. (**1** \Rightarrow **2**) Let $\pi \in \mathcal{S}_{2n}^c$. Then, there exists $\sigma \in S_n$ such that $\pi \in \sigma \sqcup c(\sigma)$, and hence there exist two disjoint set of indices $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, and $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, such that $\pi(i_1^1)\pi(i_2^1)\dots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\dots\pi(i_n^2)$ is order-isomorphic to $c(\sigma)$. Let $\mathcal{M} = (V, E)$ be the directed graph defined by $V = [2n]$ and $E = \{(i_j^1, i_j^2) : j \in [n]\}$. Clearly, \mathcal{M} is a directed perfect matching since $I^1 \cap I^2 = \emptyset$ and $I^1 \cup I^2 = [2n]$. According to Lemma 5, the directed perfect matching \mathcal{M} does avoid the patterns $\curvearrowright, \curvearrowright, \curvearrowright, \curvearrowright, \curvearrowright, \curvearrowright$. Finally, for any two distinct arcs (i_j^1, i_j^2) and (i_k^1, i_k^2) of \mathcal{M} , we have $\pi(i_j^1) < \pi(i_k^1)$ if and only if $\pi(i_j^2) > \pi(i_k^2)$ since $\pi(i_1^1)\pi(i_2^1)\dots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\dots\pi(i_n^2)$ is order-isomorphic to $c(\sigma)$ (and hence $\pi(i_j^2) = n - \pi(i_j^1)$ and $\pi(i_k^2) = n - \pi(i_k^1)$). Therefore, \mathcal{M} satisfies properties \mathbf{P}_2 and \mathbf{Q}_1 .

(**2** \Rightarrow **1**) Let \mathcal{M} be a directed perfect matching that satisfies properties \mathbf{P}_2 and \mathbf{Q}_1 . Let $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, be the set the sources of the arcs of \mathcal{M} and let $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, be the set of the sinks of the arcs of \mathcal{M} . We first show that, for every $j \in [n]$, (i_j^1, i_j^2) is an arc of \mathcal{M} . The proof is by induction on $j = 1, 2, \dots, n$.

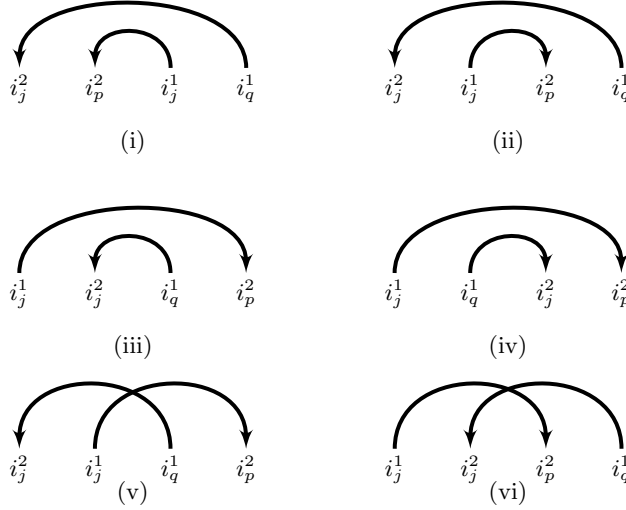


Fig. 8. All possible configurations considered in Proof of Proposition 8 ($\mathbf{2} \Rightarrow \mathbf{1}$).

- Base. Suppose, aiming at a contradiction that (i_1^1, i_1^2) is not an arc of \mathcal{M} . Then, there exist $1 < p \leq n$ and $1 < q \leq n$ such that (i_1^1, i_p^2) and (i_q^1, i_1^2) are two arcs of \mathcal{M} . But $i_1^1 < i_q^1$ and $i_1^2 < i_p^2$, and hence one of the configurations of Figure 8 (with $j = 1$) does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property \mathbf{Q}_1 , and hence (i_1^1, i_1^2) is an arc of \mathcal{M} .
- Induction step. Assume that (i_k^1, i_{n-k+1}^2) is an arc of \mathcal{M} for $1 \leq k < j$, and suppose, aiming at a contradiction, that (i_j^1, i_j^2) is not an arc of \mathcal{M} . Then, there exist $j < p \leq n$ and $j < q \leq n$ such that (i_j^1, i_p^2) and (i_q^1, i_{n-j+1}^2) are two arcs of \mathcal{M} . But $i_j^1 < i_q^1$ and $i_j^2 < i_p^2$, and hence one of the configurations of Figure 8 does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property \mathbf{Q}_1 , and hence (i_j^1, i_j^2) is an arc of \mathcal{M} .

Now, let σ_1 be the pattern of π induced by the sources of \mathcal{M} and σ_2 be the pattern of π induced by the sinks of \mathcal{M} (i.e., $\sigma_1 = \pi(i_1^1) \pi(i_2^1) \dots \pi(i_n^1)$ and $\sigma_2 = \pi(j_1^2) \pi(j_2^2) \dots \pi(i_n^2)$). Clearly σ_1 and σ_2 are disjoint in π (since \mathcal{M} is a matching) and cover π (since \mathcal{M} is perfect). Moreover, the fact that \mathcal{M} satisfies \mathbf{P}_2 implies immediately that $\text{reduce}(\sigma_1)$ is order-isomorphic to $(\text{reduce} \circ c)(\sigma_2)$, and hence this shows that $\pi \in \mathcal{S}_{2n}^c$. \blacksquare

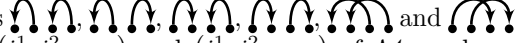
Corollary 1. c -UNSHUFFLE-PERMUTATION is NP-complete.

Proof. Combine Proposition 7 with Proposition 1. \blacksquare

Proposition 9. Let $\pi \in S_{2n}$. The two following statements are equivalent.

1. $\pi \in \mathcal{S}_{2n}^{\text{rc}}$.

2. *There exists a directed perfect matching \mathcal{M} that satisfies properties \mathbf{P}_2 and \mathbf{Q}_2 .*

Proof. (**1** \Rightarrow **2**) Let $\pi \in S_{2n}^{\text{rc}}$. Then, there exists $\sigma \in S_n$ such that $\pi \in \sigma \sqcup (\text{r} \circ \text{c})(\sigma)$, and hence there exist two disjoint set of indices $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, and $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, such that $\pi(i_1^1)\pi(i_2^1)\dots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\dots\pi(i_n^2)$ is order-isomorphic to $(\text{r} \circ \text{c})(\sigma)$. Let $\mathcal{M} = (V, E)$ be the directed graph defined by $V = [2n]$ and $E = \{(i_j^1, i_{n-j+1}^2) : j \in [n]\}$. Clearly, \mathcal{M} is a directed perfect matching since $I^1 \cap I^2 = \emptyset$ and $I^1 \cup I^2 = [2n]$. According to Lemma 6, the directed perfect matching \mathcal{M} does avoid the patterns . Finally, for any two distinct arcs (i_j^1, i_{n-j+1}^2) and (i_k^1, i_{n-k+1}^2) of \mathcal{M} , we have $\pi(i_j^1) < \pi(i_k^1)$ if and only if $\pi(i_{n-j+1}^2) > \pi(i_{n-k+1}^2)$ since $\pi(i_1^1)\pi(i_2^1)\dots\pi(i_n^1)$ is order-isomorphic to σ and $\pi(i_1^2)\pi(i_2^2)\dots\pi(i_n^2)$ is order-isomorphic to $(\text{r} \circ \text{c})(\sigma)$. Therefore, \mathcal{M} satisfies properties \mathbf{P}_1 and \mathbf{Q}_2 .

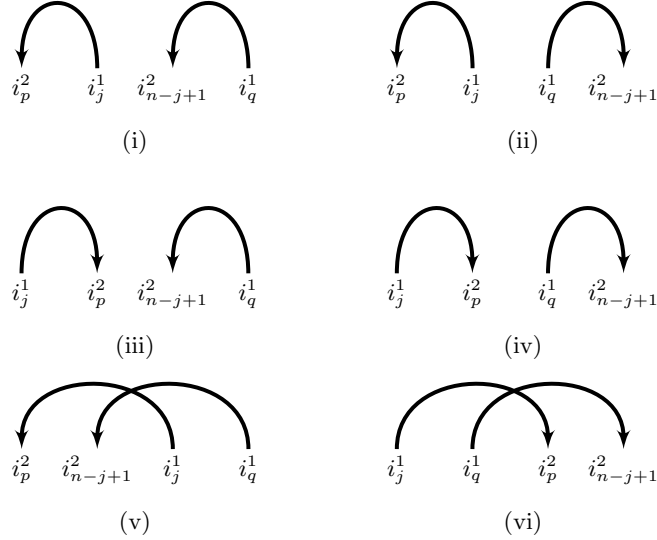


Fig. 9. All possible configurations considered in Proof of Proposition 9 (**2** \Rightarrow **1**).

(**2** \Rightarrow **1**) Let \mathcal{M} be a directed perfect matching that satisfies properties \mathbf{P}_1 and \mathbf{Q}_2 . Let $I^1 = \{i_j^1 : j \in [n]\}$, $i_1^1 < i_2^1 < \dots < i_n^1$, be the set the sources of the arcs of \mathcal{M} and let $I^2 = \{i_j^2 : j \in [n]\}$, $i_1^2 < i_2^2 < \dots < i_n^2$, be the set of the sinks of the arcs of \mathcal{M} . We first show that, for every $j \in [n]$, (i_j^1, i_{n-j+1}^2) is an arc of \mathcal{M} . The proof is by induction on $j = 1, 2, \dots, n$.

- Base. Suppose, aiming at a contradiction that (i_1^1, i_n^2) is not an arc of \mathcal{M} . Then, there exist $1 \leq p < n$ and $1 < q \leq n$ such that (i_1^1, i_p^2) and (i_q^1, i_n^2) are two arcs of \mathcal{M} . But $i_1^1 < i_q^1$ and $i_p^2 < i_n^2$, and hence one of the configurations of Figure 9 (with $j = 1$ and $k = n$) does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property **Q₂**, and hence (i_1^1, i_n^2) is an arc of \mathcal{M} .
- Induction step. Assume that (i_k^1, i_{n-k+1}^2) is an arc of \mathcal{M} for $1 \leq k < j$, and suppose, aiming at a contradiction, that (i_j^1, i_{n-j+1}^2) is not an arc of \mathcal{M} . Then, there exist $1 \leq p < n - j + 1$ and $j < q \leq n$ such that (i_j^1, i_p^2) and (i_q^1, i_{n-j+1}^2) are two arcs of \mathcal{M} . But $i_j^1 < i_q^1$ and $i_p^2 < i_{n-j+1}^2$, and hence one of the configurations of Figure 9 does occur in \mathcal{M} . This is a contradiction since \mathcal{M} satisfies Property **Q₂**, and hence (i_j^1, i_{n-j+1}^2) is an arc of \mathcal{M} .

Now, let σ_1 be the pattern of π induced by the sources of \mathcal{M} and σ_2 be the pattern of π induced by the sinks of \mathcal{M} (i.e., $\sigma_1 = \pi(i_1^1) \pi(i_2^1) \dots \pi(i_n^1)$ and $\sigma_2 = \pi(j_1^2) \pi(j_2^2) \dots \pi(j_n^2)$). Clearly σ_1 and σ_2 are disjoint in π (since \mathcal{M} is a matching) and cover π (since \mathcal{M} is perfect). Moreover, the fact that \mathcal{M} satisfies **P₂** implies immediately that $\text{reduce}(\sigma_1)$ is order-isomorphic to $(\text{reduce} \circ r \circ c)(\sigma_2)$, and hence this shows that $\pi \in \mathcal{S}_{2n}^{\text{rc}}$. ■

Proposition 10. $(r \circ c)$ -UNSHUFFLE-PERMUTATION is NP-complete.

Proof (sketch). The proof is similar to Proposition 7, replacing μ'_1 by \nearrow_{N_1} $[2n+k+N_1+2N_2]$, μ'_2 by \nearrow_{N_2} $[n+k+N_1+N_2]$, μ'_π by $(r \circ c)(\pi)[2n+k+2N_1+2N_2]$ and μ'_σ by $(r \circ c)(\sigma)[n+k+N_1+2N_2]$. ■

5 Conclusion and perspectives

In this paper we have proposed to investigate the problem of recognizing those permutations π for which there exists a permutation σ such that $\pi \in \sigma \sqcup f(\sigma)$ for some bijection $f : S_n \rightarrow S_n$. Quite a number of problems are left open by the results presented here. For instance, can we efficiently decide membership to \mathcal{S}_{2n}^i (i.e., the permutations π for which there exists a permutation σ such that $\pi \in \sigma \sqcup i(\sigma)$)? To conclude, we wish to mention two conjectures.

Conjecture 1 (Enumeration). For any $n \in \mathbb{N}$, $s_{2n}^{\text{rc}} \leq s_{2n}^c = s_{2n}^r \leq s_{2n}^{\text{irc}} = s_{2n}^i \leq s_{2n}^e \leq s_{2n}^{\text{ci}} = s_{2n}^{\text{ic}}$.

Conjecture 2 (Ubiquitous generalized squares). For any $n \in \mathbb{N}$, $\mathcal{S}_{2n}^e \cap \mathcal{S}_{2n}^r \cap \mathcal{S}_{2n}^c \cap \mathcal{S}_{2n}^i \cap \mathcal{S}_{2n}^{\text{ci}} \cap \mathcal{S}_{2n}^{\text{ic}} \cap \mathcal{S}_{2n}^{\text{rc}} \cap \mathcal{S}_{2n}^{\text{irc}} \neq \emptyset$.

References

1. Bose, P., Buss, J.F., Lubiw, A.: Pattern matching for permutations. Inf. Process. Lett. **65**(5), 277–283 (1998)
2. Buss, S., Soltys, M.: Unshuffling a square is NP-hard. J. Comput. Syst. Sci. **80**(4), 766–776 (2014)

3. Choffrut, C., Karhumäki, J.: Combinatorics of Words, in G. Rozenberg and A. Salomaa (eds), Handbook of Formal Languages. Springer-Verlag (1997)
4. Giraudo, S., Vialette, S.: Algorithmic and algebraic aspects of unshuffling permutations. *Theor. Comput. Sci.* **729**, 20–41 (2018)
5. Knuth, D.E.: The Art of Computer Programming, Volume III: Sorting and Searching. Addison-Wesley (1973)
6. van Leeuwen, J., Nivat, M.: Efficient recognition of rational relations. *Inf. Process. Lett.* **14**(1), 34–38 (1982)
7. Mansfield, A.: On the computational complexity of a merge recognition problem. *Discrete Applied Mathematics* **5**(1), 119–122 (1983)
8. Neou, B.E., Rizzi, R., Vialette, S.: Pattern matching for separable permutations. In: Proceedings of 23rd International Symposium on String Processing and Information Retrieval. pp. 260–272 (2016)
9. Rizzi, R., Vialette, S.: On recognizing words that are squares for the shuffle product. In: Proceedings of the 8th International Symposium in Computer Science - Theory and Applications. pp. 235–245 (2013)
10. Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences, <https://oeis.org/>
11. Stankova, Z.: Forbidden subsequences. *Discrete Mathematics* **132**(1-3), 291–316 (1994)
12. Vargas, Y.: Hopf algebra of permutation pattern functions. 26th International Conference on Formal Power Series and Algebraic Combinatorics pp. 839–850 (2014)