Unshuffling Permutations

Samuele Giraudo, Stéphane Vialette

Unshuffling Permutations

Samuele Giraudo and Stéphane Vialette

Université Paris-Est, LIGM (UMR 8049), CNRS, UPEM, ESIEE Paris, ENPC,
F-77454, Marne-la-Vallée, France
samuele.giraudo@univ-mlv.fr
vialette@univ-mlv.fr

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 oriented perfect matchings, we prove that recognizing square permutations is **NP**-complete.

1 Introduction

The *shuffle product*, denoted $\sqcup\!\sqcup$, is a well-known operation on words first defined by Eilenberg and Mac Lane [6]. 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:

1. Given two words v_1 and v_2, compute the set $v_1 \sqcup\!\sqcup v_2$.
2. Given three words u, v_1, and v_2, decide if u is a shuffle of v_1 and v_2.
3. Given words u, v_1, ..., v_k, decide if u is in $v_1 \sqcup\!\sqcup \cdots \sqcup\!\sqcup v_k$.
4. Given a word u, decide if there is a word v such that u is in $v \sqcup\!\sqcup v$.

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 1 can be computed in $O\left((m_1 + m_2)\binom{m_1+m_2}{m_1}\right)$ time [14]. An improvement and a generalization of Problem 1 has been proposed in [1], where it is proved that given words v_1, ..., v_k, the iterated shuffle $v_1 \sqcup\!\sqcup \cdots \sqcup\!\sqcup v_k$ can be computed in

$O\left(\binom{m_1+\cdots+m_k}{m_1,\ldots,m_k}\right)$ time. Problem 2 is in **P**; it is indeed a classical textbook exercise to design an efficient dynamic programming algorithm solving it. It can be tested in $O\left(n^2/\log(n)\right)$ time [15]. To the best of our knowledge, the first $O(n^2)$ time algorithm for this problem appeared in [9]. This algorithm can easily be extended to check in polynomial-time whether or not a word is in the shuffle of any fixed number of given words. Nevertheless, Problem 3 is **NP**-complete [9,17]. This remains true even if the ground alphabet has size 3 [17]. Of particular interest, it is shown in [17] that Problem 3 remains **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 **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 4. It is shown in [3,11] that it is **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 4 is **NP**-complete.

This paper is intended to study a natural generalization of ⧢, denoted by $\bullet$, as a shuffle of permutations. Roughly speaking, given three permutations π, σ_1, and σ_2, π is said to be a *shuffle* of σ_1 and σ_2 if π (viewed as a word) is a shuffle of two words that are order-isomorphic to σ_1 and σ_2. This shuffle product was first introduced by Vargas [16] 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 π being in the shuffle of a permutation σ with itself. Many other shuffle products on permutations appear in the literature. For instance, in [5], the authors define the *convolution product* and the *shifted shuffle product*. For this last product, π is a shuffle of σ_1 and σ_2 if π is in the shuffle, as words, of σ_1 and the word obtained by incrementing all the letters of σ_2 by the size of σ_1. It is a simple exercise to prove that, given three permutations π, σ_1, and σ_2, deciding if π is in the shifted shuffle of σ_1 and σ_2 is in **P**.

This paper is organized as follows. In Section 3 we provide a precise definition of $\bullet$. This definition passes through the preliminary definition of an operator Δ, allowing to *unshuffle* permutations. This operator is in fact a coproduct, endowing the linear span of all permutations with a coalgebra structure (see [8] or [7] for the definition of these algebraic structures). By duality, the unshuffling operator Δ 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 Δ and are more easy to prove on the coproduct side. Second, this way of doing allows to obtain a clear description of the multiplicities of the elements appearing in the shuffle of two permutations, which are worthy of interest from a combinatorial point of view. Section 4 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 1). Next, Section 5 presents some algebraic and combinatorial properties of $\bullet$. We show that $\bullet$ is associative and commutative (Proposition 2), and

that if a permutation is a square, its mirror, complement, and inverse are also squares (Proposition 3). Finally, Section 6 presents the most important result of this paper: the fact that deciding if a permutation is a square is **NP**-complete (Proposition 4). This result is obtained by exhibiting a reduction from the pattern involvement problem [2] which is **NP**-complete.

2 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 $\{1, \ldots, n\}$.

We follow the usual terminology on words [4]. 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. We denote by $\widetilde{u}$ 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 $u \sqcup\!\sqcup \epsilon = \{u\} = \epsilon \sqcup\!\sqcup u$ and $ua \sqcup\!\sqcup vb = (u \sqcup\!\sqcup vb)a \cup (ua \sqcup\!\sqcup v)b$, were a and b are letters. A word u is a *square* if there exists a word v such that u belongs to $v \sqcup\!\sqcup v$.

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 occurrence 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 π_i) the i-th letter of any permutation π. For any nonnegative integer n, we write $\nearrow_n$ (resp. $\searrow_n$) for the permutation $12\ldots n$ (resp. $n\,(n-1)\ldots 1$). If π is a permutation of S_n, we denote by $\bar{\pi}$ the *complement* of π, that is the permutation satisfying $\bar{\pi}(i) = n - \pi(i) + 1$ for all $i \in [n]$. The *inverse* of π is denoted by π^{-1}.

If u is a word of integers without multiple occurrences of a same letter, $\mathrm{s}(u)$ is the *standardized* of u, that is 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 $\mathrm{s}(u)(i) < \mathrm{s}(u)(j)$. In particular, the image of the map s is the set S of all permutations. Two words u and v having the same standardized are *order-isomorphic*. If σ is a permutation, there is an *occurrence* of (the *pattern*) σ in π if there is a set P of indexes of letters of π such that σ and $\pi_{|P}$ are order-isomorphic. When π does not admit any occurrence of σ, π *avoids* σ. The set of permutations of size n avoiding σ is denoted by $S_n(\sigma)$.

Let us now provide some definitions about graphs and oriented perfect matchings that are used in the sequel. If G is an oriented graph without loops, two different edges of G are *independent* if they do not share any common vertex. We say that G is an *oriented matching* if all edges of G are pairwise independent. Moreover, G is *perfect* if any vertex of G belongs to at least one arc. For any permutation π of S_n, an *oriented perfect matching on* π is an oriented perfect matching $\mathcal{M}$ on the set of vertices $[n]$. In the sequel, we shall consider a natural

notion of pattern avoidance in oriented perfect matchings on permutations. For instance, an oriented perfect matching $\mathcal{M}$ on a permutation π *admits an occurrence* of the pattern if there are four positions $i < j < k < \ell$ in π such that $(\pi(k), \pi(i))$ and $(\pi(j), \pi(\ell))$ are arcs of $\mathcal{M}$. When $\mathcal{M}$ does not admit any occurrence of a pattern $\mathcal{P}$, we say that $\mathcal{M}$ *avoids* $\mathcal{P}$. The definition naturally extends to sets of patterns: $\mathcal{M}$ *avoids* $P = \{\mathcal{P}_i : 1 \leq i \leq k\}$ if it avoids every pattern $\mathcal{P}_i$.

3 Shuffle product on permutations

The purpose of this section is to define a shuffle product $\bullet$ on permutations. Recall that a first definition of this product was provided by Vargas [16]. To present an alternative definition of this product adapted to our study, we shall first define a coproduct denoted by Δ, enabling to unshuffle permutations. By duality, Δ implies the definition of $\bullet$. The reason why we need to pass by the definition of Δ to define $\bullet$ is justified by the fact that a lot of properties of $\bullet$ depend of properties of Δ, and that this strategy allows to write concise and clear proofs of them. We invite the reader unfamiliar with the concepts of coproduct and duality to consult [8] or [7].

Let us denote by $\mathbb{Q}[S]$ the linear span of all permutations. We define a linear coproduct Δ on $\mathbb{Q}[S]$ in the following way. For any permutation π, we set

$$\Delta(\pi) = \sum_{P_1 \sqcup P_2 = [|\pi|]} \mathrm{s}\left(\pi_{|P_1}\right) \otimes \mathrm{s}\left(\pi_{|P_2}\right). \tag{1}$$

We call Δ the *unshuffling coproduct of permutations*. For instance,

$$\Delta(213) = \epsilon \otimes 213 + 2 \cdot 1 \otimes 12 + 1 \otimes 21 + 2 \cdot 12 \otimes 1 + 21 \otimes 1 + 213 \otimes \epsilon, \tag{2}$$

$$\Delta(1234) = \epsilon \otimes 1234 + 4 \cdot 1 \otimes 123 + 6 \cdot 12 \otimes 12 + 4 \cdot 123 \otimes 1 + 1234 \otimes \epsilon, \tag{3}$$

$$\begin{aligned} \Delta(1432) = \epsilon \otimes 1432 + 3 \cdot \mathbf{1} \otimes \mathbf{132} + 1 \otimes 321 + 3 \cdot 12 \otimes 21 \\ + 3 \cdot 21 \otimes 12 + 3 \cdot 132 \otimes 1 + 321 \otimes 1 + 1432 \otimes \epsilon. \end{aligned} \tag{4}$$

Observe that the coefficient of the tensor $1 \otimes 132$ is 3 in (4) because there are exactly three ways to extract from the permutation 1432 two disjoint subwords respectively order-isomorphic to the permutations 1 and 132.

As announced, let us now use Δ to define a shuffle product on permutations. As any coproduct, Δ leads to the definition of a product obtained by duality in the following way. From (1), for any permutation π, we have

$$\Delta(\pi) = \sum_{\sigma,\nu \in S} \lambda^{\pi}_{\sigma,\nu}\, \sigma \otimes \nu, \tag{5}$$

where the $\lambda^{\pi}_{\sigma,\nu}$ are nonnegative integers. Now, by definition of duality, the dual product of Δ, denoted by $\bullet$, is a linear binary product on $\mathbb{Q}[S]$. It satisfies, for any permutations σ and ν,

$$\sigma \bullet \nu = \sum_{\pi \in S} \lambda^{\pi}_{\sigma,\nu}\, \pi, \tag{6}$$

where the coefficients $\lambda^{\pi}_{\sigma,\nu}$ are the ones of (5). We call $\bullet$ the *shuffle product of permutations*. For instance,

$$\begin{aligned} 12 \bullet 21 = {} & 1243 + 1324 + 2 \cdot 1342 + 2 \cdot 1423 + 3 \cdot \mathbf{1432} + 2134 + 2 \cdot 2314 \\ & + 3 \cdot 2341 + 2413 + 2 \cdot 2431 + 2 \cdot 3124 + 3142 + 3 \cdot 3214 + 2 \cdot 3241 \\ & + 3421 + 3 \cdot 4123 + 2 \cdot 4132 + 2 \cdot 4213 + 4231 + 4312. \end{aligned} \tag{7}$$

Observe that the coefficient 3 of the permutation 1432 in (7) comes from the fact that the coefficient of the tensor $12 \otimes 21$ is 3 in (4).

Intuitively, this product shuffles the values and the positions of the letters of the permutations. One can observe that the empty permutation ϵ 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 π *appears* in the shuffle $\sigma \bullet \nu$ of two permutations σ and ν 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 π satisfying $P_1 \sqcup P_2 = [|\pi|]$ such that the subword $\pi_{|P_1}$ is order-isomorphic to σ and the subword $\pi_{|P_2}$ is order-isomorphic to ν.

A permutation π is a *square* if there is a permutation σ such that π appears in $\sigma \bullet \sigma$. In this case, we say that σ is a *square root* of π. Equivalently, π is a square with σ 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 π 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,

$$1, 0, 2, 0, 20, 0, 504, 0, 21032, 0, 1293418. \tag{8}$$

This sequence (and its subsequence obtained by removing the 0's) is for the time being not listed in [13]. The square permutations of sizes 0 to 4 are

Size 0	Size 2	Size 4
ϵ	12, 21	1234, 1243, 1423, 1324, 1342, 4132, 3124, 3142, 3412, 4312, 2134, 2143, 2413, 4213, 2314, 2431, 4231, 3241, 3421, 4321

4 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 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 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,

$$\mathrm{btp}(\mathbf{100101101}000) = \mathbf{C}12\mathbf{B}3\mathbf{A}9\mathbf{48}567, \tag{9}$$

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

Proposition 1. *For any $n \geq 0$, the map* 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 1). The statement of the proposition is a consequence of the following claims implying that ptb is the inverse map of btp over the set of square binary words.

Claim 1. The image of btp is the set of all permutations avoiding 213 and 231.

Proof (of Claim 1). Let us first show that the image of btp contains only permutations avoiding 213 and 231. Let u be a binary word, $\pi = \mathrm{btp}(u)$, 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 π admits an occurrence of 213. 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). All these three cases contradict the fact that all letters of w are greater than those of v. A similar argument shows that π avoids 231 as well.

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

Claim 2. If u is a square binary word, $\mathrm{btp}(u)$ is a square permutation.

Proof (of Claim 2). Since u is a square binary word, there is a binary word v such that $u \in v \sqcup\!\sqcup v$. 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 $\mathrm{btp}(u)_{|P}$ and $\mathrm{btp}(u)_{|Q}$ have the same standardized σ. Hence, and by definition of the shuffle product of permutations, $\mathrm{btp}(u)$ appears in $\sigma \bullet \sigma$, showing that $\mathrm{btp}(u)$ is a square permutation. □

Claim 3. If π is a square permutation avoiding 213 and 231, $\mathrm{ptb}(\pi)$ is a square binary word.

Proof (of Claim 3). Let π be a square permutation avoiding 213 and 231. By Claim 1, π is in the image of btp and hence, $u = \mathrm{ptb}(\pi)$ is a well-defined binary word. Since π is a square permutation, there are two disjoint sets P_1 and P_2 of indexes of letters of π 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. □

□

The number of square binary words is Sequence A191755 of [13] beginning by

$$1, 0, 2, 0, 6, 0, 22, 0, 82, 0, 320, 0, 1268, 0, 5102, 0, 020632. \tag{10}$$

According to Proposition 1, this is also the sequence enumerating square permutations avoiding 213 and 231.

5 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 Δ of permutations defined in Section 3 lead to combinatorial properties of $\bullet$.

Proposition 2. *The shuffle product $\bullet$ of permutations is associative and commutative.*

Proof (of Proposition 2). To prove the associativity of $\bullet$, it is convenient to show that its dual coproduct Δ is coassociative, that is

$$(\Delta \otimes I)\Delta = (I \otimes \Delta)\Delta, \tag{11}$$

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 π, we have

$$\begin{aligned}
(\Delta \otimes I)\Delta(\pi) &= (\Delta \otimes I) \sum_{P_1 \sqcup P_2 = [|\pi|]} \mathrm{s}\left(\pi_{|P_1}\right) \otimes \mathrm{s}\left(\pi_{|P_2}\right) \\
&= \sum_{P_1 \sqcup P_2 = [|\pi|]} \Delta\left(\mathrm{s}\left(\pi_{|P_1}\right)\right) \otimes I\left(\mathrm{s}\left(\pi_{|P_2}\right)\right) \\
&= \sum_{P_1 \sqcup P_2 = [|\pi|]} \sum_{Q_1 \sqcup Q_2 = [|P_1|]} \mathrm{s}\left(\mathrm{s}\left(\pi_{|P_1}\right)_{|Q_1}\right) \otimes \mathrm{s}\left(\mathrm{s}\left(\pi_{|P_1}\right)_{|Q_2}\right) \otimes \mathrm{s}\left(\pi_{|P_2}\right) \\
&= \sum_{P_1 \sqcup P_2 \sqcup P_3 = [|\pi|]} \mathrm{s}\left(\pi_{|P_1}\right) \otimes \mathrm{s}\left(\pi_{|P_2}\right) \otimes \mathrm{s}\left(\pi_{|P_3}\right).
\end{aligned} \tag{12}$$

An analogous computation shows that $(I \otimes \Delta)\Delta(\pi)$ is equal to the last member of (12), whence the associativity of $\bullet$.

Finally, to prove the commutativity of $\bullet$, we shall show that Δ is cocommutative, that is for any permutation π, if in the expansion of $\Delta(\pi)$ there is a tensor $\sigma \otimes \nu$ with a coefficient λ, there is in the same expansion the tensor $\nu \otimes \sigma$ with the same coefficient λ. Clearly, a product is commutative if and only if its dual coproduct is cocommutative. Now, from the definition (1) of Δ, one observes that if the pair (P_1, P_2) of subsets of $[|\pi|]$ contributes to the coefficient of $\mathrm{s}\left(\pi_{|P_1}\right) \otimes \mathrm{s}\left(\pi_{|P_2}\right)$, the pair (P_2, P_1) contributes to the coefficient of $\mathrm{s}\left(\pi_{|P_2}\right) \otimes \mathrm{s}\left(\pi_{|P_1}\right)$. This shows that Δ is cocommutative and hence, that $\bullet$ is commutative. □

Proposition 2 implies that $\mathbb{Q}[S]$ endowed with the unshuffling coproduct Δ is a coassociative cocommutative coalgebra, or in an equivalent way, that $\mathbb{Q}[S]$ endowed with the shuffle product $\bullet$ is an associative commutative algebra.

Lemma 1. *The three linear maps*

$$\phi_1, \phi_2, \phi_3 : \mathbb{Q}[S] \to \mathbb{Q}[S] \tag{13}$$

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

We now use the algebraic properties of $\bullet$ exhibited by Lemma 1 to obtain combinatorial properties of square permutations.

Proposition 3. *Let π be a square permutation and σ be a square root of π. Then,*

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

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

$$\phi_j(\sigma \bullet \sigma) = \phi_j(\sigma) \bullet \phi_j(\sigma). \tag{14}$$

Then, since π 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 σ and ν of the same size are *Wilf equivalent* if $\#S_n(\sigma) = \#S_n(\nu)$ for all $n \geq 0$. The well-known [12] fact that there is a single Wilf-equivalence class of permutations of

size 3 together with Proposition 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

$$1, 0, 2, 0, 12, 0, 118, 0, 1218, 0, 14272, \tag{15}$$

while the number of square permutations avoiding 132 begins by

$$1, 0, 2, 0, 11, 0, 84, 0, 743, 0, 7108. \tag{16}$$

Besides, an other consequence of Proposition 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

$$1, 0, 1, 0, 6, 0, 81, 0, 2774, 0, 162945. \tag{17}$$

All Sequences (15), (16), and (17) (and their subsequences obtained by removing the 0s) are for the time being not listed in [13].

6 Algorithmic issues

This section is devoted to proving hardness of recognizing square permutations. In the same way as happens with 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 [3,11]. We have, however, to deal with oriented perfect matchings. The needed properties read as follows (see Fig. 1).

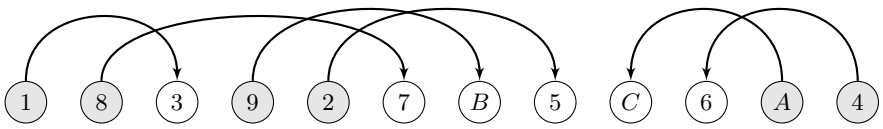
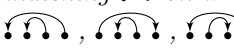
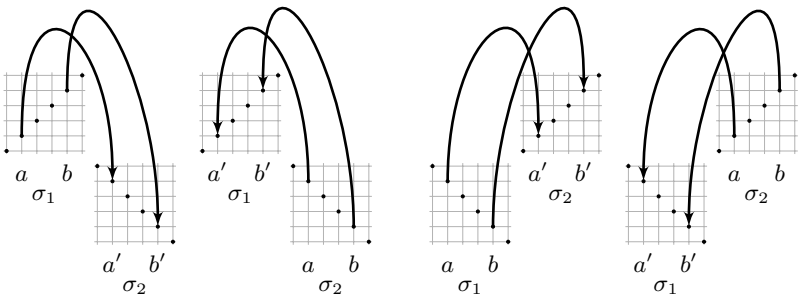


Fig. 1. An oriented perfect matching $\mathcal{M}$ on the permutation $\pi = 183927B5C6A4$ satisfying the properties $\mathbf{P_1}$ and $\mathbf{P_2}$. From $\mathcal{M}$, it follows that π is a square as it appears in the shuffle of $1892A4$ and $37B5C6$, both being order-isomorphic to 145263.

Definition 1 (Property $\mathbf{P_1}$). *Let π be a permutation. An oriented perfect matching $\mathcal{M}$ on π is said to have property $\mathbf{P_1}$ if it avoids all the six patterns*  *and* .



(a) An increasing pattern before and above a decreasing pattern.

(b) A decreasing pattern before and below an increasing pattern.

Fig. 2. Illustration of Lemma 3.

Definition 2 (Property $\mathbf{P_2}$). *Let π be a permutation. An oriented perfect matching $\mathcal{M}$ on π is said to have property $\mathbf{P_2}$ if, for any two distinct arcs $(\pi(a), \pi(a'))$ and $(\pi(b), \pi(b'))$ in $\mathcal{M}$, we have $\pi(a) < \pi(b)$ if and only if $\pi(a') < \pi(b')$.*

The rationale for introducing properties $\mathbf{P_1}$ and $\mathbf{P_2}$ stems from the following lemma.

Lemma 2. *Let π be a permutation. The following statements are equivalent:*

1. *The permutation π is a square.*
2. *There exists an oriented perfect matching $\mathcal{M}$ on π satisfying $\mathbf{P_1}$ and $\mathbf{P_2}$.*

Let π be a permutation. For the sake of clarity, we will say that a bunch of consecutive positions P of π is *above* (resp. *below*) above another bunch of consecutive positions P' in π if $\pi(i) > \pi(j)$ (resp. $\pi(i) < \pi(j)$) for every $i \in P$ and every $j \in P'$. For example, σ_1 is above σ_2 (in an equivalent manner, σ_2 is below σ_1) in Fig. 2(a), whereas σ_1 is below σ_2 (in an equivalent manner, σ_2 is above σ_1) in Fig. 2(b).

Before proving hardness, we give an easy lemma that will prove extremely useful for simplifying the proof of upcoming Proposition 4.

Lemma 3. *Let $\pi = \pi_1\,\sigma_1\,\pi_2\,\sigma_2\,\pi_3$ be a permutation with $|\sigma_1| \geq 2$ and $|\sigma_2| \geq 2$, and $\mathcal{M}$ be an oriented perfect matching on π satisfying $\mathbf{P_1}$ and $\mathbf{P_2}$. The following assertions hold:*

1. *If σ_1 is increasing, σ_2 is decreasing, and σ_1 is above σ_2 (see Fig. 2(a)), then there is at most one arc between σ_1 and σ_2 in $\mathcal{M}$ (this arc can be a (σ_1, σ_2)-arc or a (σ_2, σ_1)-arc).*

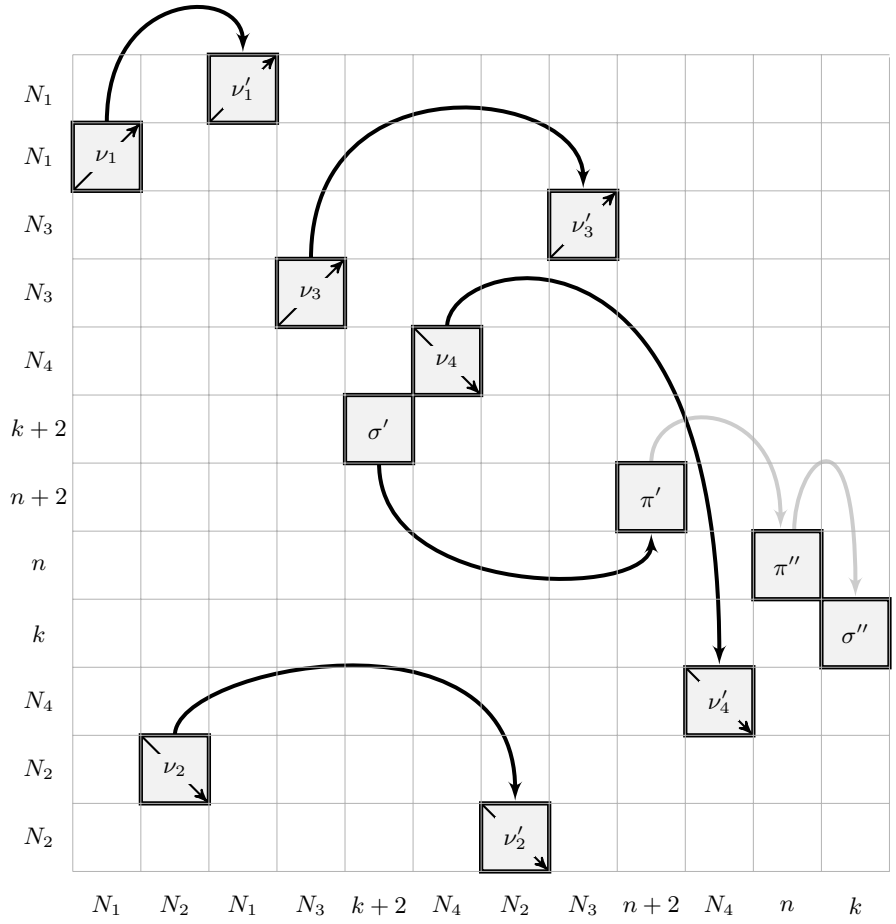


Fig. 3. Schematic representation of the permutation μ used in Proposition 4. Black arcs denote the presence of at least one arc between two bunches of positions in μ. Grey arcs denote edges that are only considered in the forward direction of the proof.

2. *If σ_1 is decreasing, σ_2 is increasing, and σ_1 is below σ_2 (see Fig. 2(b)), then there is at most one arc between σ_1 and σ_2 in $\mathcal{M}$ (this arc can be a (σ_1, σ_2)-arc or a (σ_2, σ_1)-arc).*

Proposition 4. *Deciding whether a permutation is a square is* **NP***-complete.*

Proof (of Proposition 4). The problem is certainly in **NP**. We propose a reduction from the pattern involvement problem which is known to be **NP**-complete [2]: Given two permutations π and σ, decide whether σ occurs in π (as an order-isomorphic pattern).

Let $\pi \in S_n$ and $\sigma \in S_k$ be two arbitrary permutations. Define

$$N_4 = 2(2n + 2k + 4) + 1 = 4n + 4k + 9$$
$$N_3 = 2(2N_4 + 2n + 2k + 4) + 1 = 20n + 20k + 45$$
$$N_2 = 2(2N_3 + 2N_4 + 2n + 2k + 4) + 1 = 100n + 100k + 225$$
$$N_1 = 2(2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4) + 1 = 1000n + 1000k + 1325.$$

Notice that N_1, N_2, N_3 and N_4 are polynomial in n. The crucial properties are that (i) N_1, N_2, N_3 and N_4 are odd integers and (ii) $N_i > \left(\sum_{i<j\leq 4} 2N_j\right) + 2n + 2k + k$ for every $1 \leq i \leq 4$.

We now turn to defining various gadgets (sequences of integers) that act as building blocks in our construction of a new permutation μ:

$$\begin{aligned}
\sigma' &= ((k+1)\ \sigma\ (k+2))\ [2N_2 + N_4 + 2n + k + 2] \\
\pi' &= ((n+1)\ \pi\ (n+2))\ [2N_2 + N_4 + n + k] \\
\sigma'' &= \sigma\ [2N_2 + N_4] \\
\pi'' &= \pi\ [2N_2 + N_4 + k] \\
\nu_1 &= \nearrow_{N_1}\ [2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4] \\
\nu_1' &= \nearrow_{N_1}\ [N_1 + 2N_2 + 2N_3 + 2N_4 + 2n + 2k + 4] \\
\nu_2 &= \nearrow_{N_2}\ [N_2] \\
\nu_2' &= \searrow_{N_2} \\
\nu_3 &= \nearrow_{N_3}\ [2N_2 + 2N_4 + 2n + 2k + 4] \\
\nu_3' &= \nearrow_{N_3}\ [2N_2 + N_3 + 2N_4 + 2n + 2k + 4] \\
\nu_4 &= \searrow_{N_4}\ [2N_2 + N_4 + 2n + 2k + 4] \\
\nu_4' &= \searrow_{N_4}\ [2N_2].
\end{aligned}$$

We are now in position to define our target permutation μ (see Fig. 3 for an illustration):

$$\mu = \nu_1\ \nu_2\ \nu_1'\ \nu_3\ \sigma'\ \nu_4\ \nu_2'\ \nu_3'\ \pi'\ \nu_4'\ \pi''\ \sigma''.$$

It is immediate that μ can be constructed in polynomial-time in n and k. It can be shown that σ occurs in π if and only if there exists an oriented perfect matching $\mathcal{M}$ on μ satisfying $\mathbf{P_1}$ and $\mathbf{P_2}$. □

7 Conclusion

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 1, how many binary strings of length $2n$ are squares; see also Problem 4 in

[10])? How hard is the problem of deciding whether a $(213, 231)$-avoiding permutation is a square (Problem 4 in [10], see also [3,11])? Given two permutations π and σ, how hard is the problem of deciding whether σ is a square root of π? As for algebra, one can ask for a complete algebraic study of $\mathbb{Q}[S]$ as a graded associative algebra for the shuffle product $\bullet$. 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

1. C. Allauzen. Calcul efficace du shuffle de k mots. Technical report, Institut Gaspard Monge, Université Marne-la-Vallée, 2000.
2. P. Bose, J.F.Buss, and A. Lubiw. Pattern matching for permutations. *Information Processing Letters*, 65(5):277–283, 1998.
3. S. Buss and M. Soltys. Unshuffling a square is NP-hard. *Journal of Computer and System Sciences*, 80(4):766–776, 2014.
4. C. Choffrut and J. Karhumäki. *Combinatorics of Words, in G. Rozenberg and A. Salomaa (eds), Handbook of Formal Languages.* Springer-Verlag, 1997.
5. G. Duchamp, F. Hivert, and J.-Y. Thibon. Noncommutative symmetric functions. VI. Free quasi-symmetric functions and related algebras. *Int. J. Algebr. Comput.*, 12(5):671–717, 2002.
6. S. Eilenberg and S. Mac Lane. On the groups of $H(\Pi, n)$. I. *Ann. of Math. (2)*, 58:55–106, 1953.
7. D. Grinberg and V. Reiner. Hopf Algebras in Combinatorics. 2014. arXiv:1409.8356.
8. S. A. Joni and G.-C. Rota. Coalgebras and bialgebras in combinatorics. *Stud. Appl. Math.*, 61(2):93–139, 1979.
9. A. Mansfield. On the computational complexity of a merge recognition problem. *Discrete Applied Mathematics*, 5:119–122, 1983.
10. D. Henshall N. Rampersad and J. Shallit. Shuffling and unshuffling. http://arxiv.org/abs/1106.5767, 2011.
11. R. Rizzi and S. Vialette. On recognizing words that are squares for the shuffle product. In A.A. Bulatov and A.M. Shur, editors, *8th International Computer Science Symposium in Russia, CSR 2013, Ekaterinburg, Russia*, pages 235–245, 2013.
12. R. Simion and F.W.Schmidt. Restricted permutations. *European Journal of Combinatorics*, 6(4):383–406, 1985.
13. N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. https://oeis.org/.
14. J.-C. Spehner. Le calcul rapide des melanges de deux mots. *Theoretical Computer Science*, 47:181–203, 1986.
15. J. van Leeuwen and M. Nivat. Efficient recognition of rational relations. *Information Processing Letters*, 14(1):34–38, 1982.
16. Y. Vargas. Hopf algebra of permutation pattern functions. *26th International Conference on Formal Power Series and Algebraic Combinatorics*, pages 839–850, 2014.
17. M.K. Warmuth and D. Haussler. On the complexity of iterated shuffle. *Journal of Computer and System Sciences*, 28(3):345–358, 1984.