

# Unshuffling Permutations

Samuele Giraudo

Stéphane Vialette

Laboratoire d'Informatique Gaspard-Monge  
Université Paris-Est Marne-la-Vallée  
UMR CNRS 8049

Latin American Theoretical Informatics Symposium  
April 11-15 2016

# Contents

- 1 Background
- 2 Algebraic and combinatorial issues
- 3 Algorithmic issues

# Contents

## 1 Background

# Shuffling words

## Definition (shuffle product of words)

The **shuffle product**  $\sqcup$  on words of  $A^*$  is defined recursively by

$$\begin{aligned}u \sqcup \epsilon &:= \{u\} =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b \cup (u \sqcup vb)a.\end{aligned}$$

To take into account multiplicities, we consider  $\sqcup$  as a linear product

$$\sqcup : \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*]$$

on  $\mathbb{Q}[A^*]$ , the  $\mathbb{Q}$ -linear span of words defined by

$$\begin{aligned}u \sqcup \epsilon &:= u =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b + (u \sqcup vb)a.\end{aligned}$$

## Example

$$\begin{aligned}ab \sqcup ba &= abba + abba + abab + baba + baab + baab \\&= 2abba + abab + baba + 2baab\end{aligned}$$

# Shuffling words

## Definition (shuffle product of words)

The **shuffle product**  $\sqcup$  on words of  $A^*$  is defined recursively by

$$\begin{aligned}u \sqcup \epsilon &:= \{u\} =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b \cup (u \sqcup vb)a.\end{aligned}$$

To take into account multiplicities, we consider  $\sqcup$  as a linear product

$$\sqcup : \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*]$$

on  $\mathbb{Q}[A^*]$ , the  $\mathbb{Q}$ -linear span of words defined by

$$\begin{aligned}u \sqcup \epsilon &:= u =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b + (u \sqcup vb)a.\end{aligned}$$

## Example

$$\begin{aligned}ab \sqcup ba &= abba + abba + abab + baba + baab + baab \\&= 2abba + abab + baba + 2baab\end{aligned}$$

# Shuffling words

## Definition (shuffle product of words)

The **shuffle product**  $\sqcup$  on words of  $A^*$  is defined recursively by

$$\begin{aligned}u \sqcup \epsilon &:= \{u\} =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b \cup (u \sqcup vb)a.\end{aligned}$$

To take into account multiplicities, we consider  $\sqcup$  as a linear product

$$\sqcup : \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*]$$

on  $\mathbb{Q}[A^*]$ , the  $\mathbb{Q}$ -linear span of words defined by

$$\begin{aligned}u \sqcup \epsilon &:= u =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b + (u \sqcup vb)a.\end{aligned}$$

## Example

$$\begin{aligned}ab \sqcup ba &= abba + abba + abab + baba + baab + baab \\&= 2abba + abab + baba + 2baab\end{aligned}$$

# Shuffling words

## Definition (shuffle product of words)

The **shuffle product**  $\sqcup$  on words of  $A^*$  is defined recursively by

$$\begin{aligned}u \sqcup \epsilon &:= \{u\} =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b \cup (u \sqcup vb)a.\end{aligned}$$

To take into account multiplicities, we consider  $\sqcup$  as a linear product

$$\sqcup : \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*]$$

on  $\mathbb{Q}[A^*]$ , the  $\mathbb{Q}$ -linear span of words defined by

$$\begin{aligned}u \sqcup \epsilon &:= u =: \epsilon \sqcup u, \\(ua \sqcup vb) &:= (ua \sqcup v)b + (u \sqcup vb)a.\end{aligned}$$

## Example

$$\begin{aligned}ab \sqcup ba &= abba + abba + abab + baba + baab + baab \\&= 2abba + abab + baba + 2baab\end{aligned}$$

# Key results

Given two words  $v_1$  and  $v_2$ , the set  $v_1 \sqcup v_2$  can be computed in

$$O\left((|v_1| + |v_2|) \binom{|v_1| + |v_2|}{|v_1|}\right)$$

time [Spehner, 1986].

Given three words  $u$ ,  $v_1$ , and  $v_2$ , deciding if  $u$  is in  $v_1 \sqcup v_2$  can be done in

$$O\left(\frac{|u|^2}{\log(|u|)}\right)$$

time [van Leeuwen, Nivat, 1982].

Given a word  $u$ , deciding if there is a word  $v$  such that  $u$  is in  $v \sqcup v$  is NP-complete [Rizzi, Vialette, 2013] [Buss, Soltys, 2014].



## Key results

Given two words  $v_1$  and  $v_2$ , the set  $v_1 \sqcup v_2$  can be computed in

$$O\left((|v_1| + |v_2|) \binom{|v_1| + |v_2|}{|v_1|}\right)$$

time [Spehner, 1986].

Given three words  $u$ ,  $v_1$ , and  $v_2$ , deciding if  $u$  is in  $v_1 \sqcup v_2$  can be done in

$$O\left(\frac{|u|^2}{\log(|u|)}\right)$$

time [van Leeuwen, Nivat, 1982].

Given a word  $u$ , deciding if there is a word  $v$  such that  $u$  is in  $v \sqcup v$  is NP-complete [Rizzi, Vialette, 2013] [Buss, Soltys, 2014].

## Key results

Given two words  $v_1$  and  $v_2$ , the set  $v_1 \sqcup v_2$  can be computed in

$$O\left((|v_1| + |v_2|) \binom{|v_1| + |v_2|}{|v_1|}\right)$$

time [Spehner, 1986].

Given three words  $u$ ,  $v_1$ , and  $v_2$ , deciding if  $u$  is in  $v_1 \sqcup v_2$  can be done in

$$O\left(\frac{|u|^2}{\log(|u|)}\right)$$

time [van Leeuwen, Nivat, 1982].

Given a word  $u$ , deciding if there is a word  $v$  such that  $u$  is in  $v \sqcup v$  is NP-complete [Rizzi, Vialette, 2013] [Buss, Soltys, 2014].

# Square words

## Definition (square words)

A word  $u$  is a **square** (w.r.t. the shuffle product  $\sqcup$ ) if there is a word  $v$  such that  $u$  appears in  $v \sqcup v$ .

## Example

The word  $u := \text{cca babb b}$  is a square since  $u$  can be obtained by shuffling  $\text{c a b b}$  with itself.

The first numbers of square binary words of length  $2n$  are

1, 2, 6, 22, 82, 320, 1268, 5102, 20632, 83972.

Open problem [Henshall, Rampersad, Shallit, 2012]

Enumeration of square (binary) words.

# Square words

## Definition (square words)

A word  $u$  is a **square** (w.r.t. the shuffle product  $\sqcup$ ) if there is a word  $v$  such that  $u$  appears in  $v \sqcup v$ .

## Example

The word  $u := \text{c c a b a b b b}$  is a square since  $u$  can be obtained by shuffling  $\text{c a b b}$  with itself.

The first numbers of square binary words of length  $2n$  are

1, 2, 6, 22, 82, 320, 1268, 5102, 20632, 83972.

Open problem [Henshall, Rampersad, Shallit, 2012]

Enumeration of square (binary) words.

# Square words

## Definition (square words)

A word  $u$  is a **square** (w.r.t. the shuffle product  $\sqcup$ ) if there is a word  $v$  such that  $u$  appears in  $v \sqcup v$ .

## Example

The word  $u := \text{c c a b a b b b}$  is a square since  $u$  can be obtained by shuffling  $\text{c a b b}$  with itself.

The first numbers of square binary words of length  $2n$  are

1, 2, 6, 22, 82, 320, 1268, 5102, 20632, 83972.

Open problem [Henshall, Rampersad, Shallit, 2012]

Enumeration of square (binary) words.

# Square words

## Definition (square words)

A word  $u$  is a **square** (w.r.t. the shuffle product  $\sqcup$ ) if there is a word  $v$  such that  $u$  appears in  $v \sqcup v$ .

## Example

The word  $u := \text{c c a b a b b b}$  is a square since  $u$  can be obtained by shuffling  $\text{c a b b}$  with itself.

The first numbers of square binary words of length  $2n$  are

1, 2, 6, 22, 82, 320, 1268, 5102, 20632, 83972.

Open problem [Henshall, Rampersad, Shallit, 2012]

Enumeration of square (binary) words.

# Recognizing square words

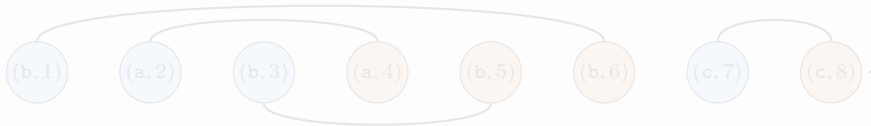
## Definition (perfect matchings for words)

A **perfect matching** of a word  $u$  is a graph  $(V, E)$  such that

- $V := \{(u_i, i) : i \in \{1, \dots, |u|\}\};$
- every vertex of  $V$  belongs to exactly one edge of  $E$ ;
- $(u_i, i) - (u_j, j) \in E$  implies  $u_i = u_j$ .

## Example

The word **b a b a b b c c** admits the perfect matching



## Definition (inclusion-free perfect matchings)

A perfect matching  $(V, E)$  of a word  $u$  is **inclusion-free** if there are no edges  $(u_i, i) - (u_j, j)$  and  $(u_k, k) - (u_\ell, \ell)$  of  $E$  such that  $i < k < \ell < j$ .

# Recognizing square words

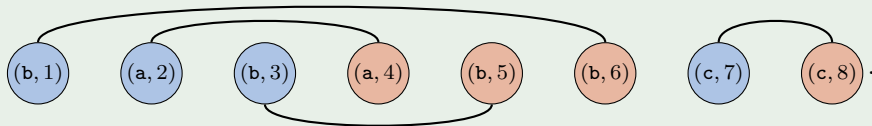
## Definition (perfect matchings for words)

A **perfect matching** of a word  $u$  is a graph  $(V, E)$  such that

- $V := \{(u_i, i) : i \in \{1, \dots, |u|\}\}$ ;
- every vertex of  $V$  belongs to exactly one edge of  $E$ ;
- $(u_i, i) - (u_j, j) \in E$  implies  $u_i = u_j$ .

## Example

The word **b a b a b b c c** admits the perfect matching



## Definition (inclusion-free perfect matchings)

A perfect matching  $(V, E)$  of a word  $u$  is **inclusion-free** if there are no edges  $(u_i, i) - (u_j, j)$  and  $(u_k, k) - (u_\ell, \ell)$  of  $E$  such that  $i < k < \ell < j$ .



# Recognizing square words

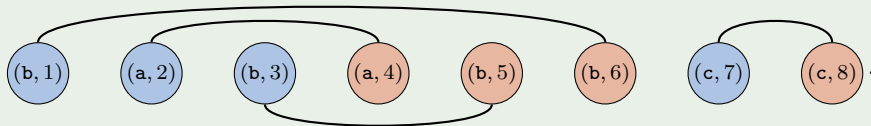
## Definition (perfect matchings for words)

A **perfect matching** of a word  $u$  is a graph  $(V, E)$  such that

- $V := \{(u_i, i) : i \in \{1, \dots, |u|\}\}$ ;
- every vertex of  $V$  belongs to exactly one edge of  $E$ ;
- $(u_i, i) - (u_j, j) \in E$  implies  $u_i = u_j$ .

## Example

The word **b a b a b b c c** admits the perfect matching



## Definition (inclusion-free perfect matchings)

A perfect matching  $(V, E)$  of a word  $u$  is **inclusion-free** if there are no edges  $(u_i, i) - (u_j, j)$  and  $(u_k, k) - (u_\ell, \ell)$  of  $E$  such that  $i < k < \ell < j$ .

# Recognizing square words

## Proposition [Rizzi, Vialette, 2013]

A word  $u$  is a square iff  $u$  admits an inclusion-free perfect matching.

### Example

The word  $\text{ccaababb}$  admits the perfect matching



which is inclusion-free and hence is a square.

### Example

The word  $\text{abba}$  is not a square. Its only perfect matching



is not inclusion-free.

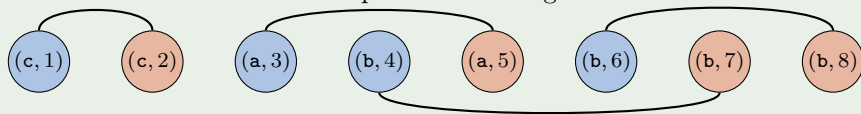
# Recognizing square words

## Proposition [Rizzi, Vialette, 2013]

A word  $u$  is a square iff  $u$  admits an inclusion-free perfect matching.

## Example

The word  $\text{ccababb}$  admits the perfect matching



which is inclusion-free and hence is a square.

## Example

The word  $\text{abba}$  is not a square. Its only perfect matching



is not inclusion-free.

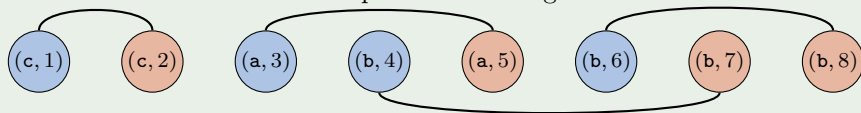
# Recognizing square words

## Proposition [Rizzi, Vialette, 2013]

A word  $u$  is a square iff  $u$  admits an inclusion-free perfect matching.

## Example

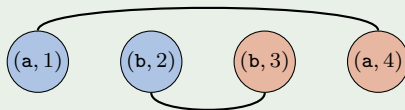
The word  $\text{ccababb}$  admits the perfect matching



which is inclusion-free and hence is a square.

## Example

The word  $\text{abba}$  is not a square. Its only perfect matching



is not inclusion-free.

# Main motivations

Let  $S_n$  be the set of **permutations** of size  $n$  and  $S$  be the set of all permutations.

There are several products on permutations, analogs of the shuffle product of words. Among these, there are

- the shifted shuffle product [Duchamp, Hivert, Thibon, 2002];
- the convolution product [Duchamp, Hivert, Thibon, 2002];
- the supershuffle [Vargas, 2014].

## Main questions

- Combinatorial properties of “square permutations” w.r.t. the supershuffle?
- Complexity of the recognition of “square permutations”?

# Main motivations

Let  $S_n$  be the set of **permutations** of size  $n$  and  $S$  be the set of all permutations.

There are several products on permutations, analogs of the shuffle product of words. Among these, there are

- the shifted shuffle product [**Duchamp, Hivert, Thibon, 2002**];
- the convolution product [**Duchamp, Hivert, Thibon, 2002**];
- the supershuffle [**Vargas, 2014**].

## Main questions

- Combinatorial properties of “square permutations” w.r.t. the supershuffle?
- Complexity of the recognition of “square permutations”?

# Main motivations

Let  $S_n$  be the set of **permutations** of size  $n$  and  $S$  be the set of all permutations.

There are several products on permutations, analogs of the shuffle product of words. Among these, there are

- the shifted shuffle product [[Duchamp, Hivert, Thibon, 2002](#)];
- the convolution product [[Duchamp, Hivert, Thibon, 2002](#)];
- the supershuffle [[Vargas, 2014](#)].

## Main questions

- Combinatorial properties of “square permutations” w.r.t. the supershuffle?
- Complexity of the recognition of “square permutations”?

# Contents

## 2 Algebraic and combinatorial issues



# Combinatorial products and coproducts

Let  $C$  be a set of combinatorial objects and  $\mathbb{Q}[C]$  be the  $\mathbb{Q}$ -linear span of  $C$ .

## Key idea

Knowing how to **break** combinatorial objects explains how to **combine** these.

To define a product  $\cdot : \mathbb{Q}[C] \otimes \mathbb{Q}[C] \rightarrow \mathbb{Q}[C]$ , it is in some cases more convenient to start by defining a **coproduct**  $\Delta : \mathbb{Q}[C] \rightarrow \mathbb{Q}[C] \otimes \mathbb{Q}[C]$ .

Every coproduct fits into the general form

$$\Delta(z) = \sum_{x,y \in C} \lambda_{x,y}^z (x \otimes y)$$

where the  $\lambda_{x,y}^z \in \mathbb{Q}$  are structure coefficients.

Then,  $\Delta$  leads by duality to the definition of  $\cdot$  by

$$x \cdot y := \sum_{z \in C} \lambda_{x,y}^z z.$$

# Combinatorial products and coproducts

Let  $C$  be a set of combinatorial objects and  $\mathbb{Q}[C]$  be the  $\mathbb{Q}$ -linear span of  $C$ .

## Key idea

Knowing how to **break** combinatorial objects explains how to **combine** these.

To define a product  $\cdot : \mathbb{Q}[C] \otimes \mathbb{Q}[C] \rightarrow \mathbb{Q}[C]$ , it is in some cases more convenient to start by defining a **coproduct**  $\Delta : \mathbb{Q}[C] \rightarrow \mathbb{Q}[C] \otimes \mathbb{Q}[C]$ .

Every coproduct fits into the general form

$$\Delta(z) = \sum_{x,y \in C} \lambda_{x,y}^z (x \otimes y)$$

where the  $\lambda_{x,y}^z \in \mathbb{Q}$  are structure coefficients.

Then,  $\Delta$  leads by duality to the definition of  $\cdot$  by

$$x \cdot y := \sum_{z \in C} \lambda_{x,y}^z z.$$

# Combinatorial products and coproducts

Let  $C$  be a set of combinatorial objects and  $\mathbb{Q}[C]$  be the  $\mathbb{Q}$ -linear span of  $C$ .

## Key idea

Knowing how to **break** combinatorial objects explains how to **combine** these.

To define a product  $\cdot : \mathbb{Q}[C] \otimes \mathbb{Q}[C] \rightarrow \mathbb{Q}[C]$ , it is in some cases more convenient to start by defining a **coproduct**  $\Delta : \mathbb{Q}[C] \rightarrow \mathbb{Q}[C] \otimes \mathbb{Q}[C]$ .

Every coproduct fits into the general form

$$\Delta(z) = \sum_{x,y \in C} \lambda_{x,y}^z (x \otimes y)$$

where the  $\lambda_{x,y}^z \in \mathbb{Q}$  are structure coefficients.

Then,  $\Delta$  leads by duality to the definition of  $\cdot$  by

$$x \cdot y := \sum_{z \in C} \lambda_{x,y}^z z.$$

# Combinatorial products and coproducts

Let  $C$  be a set of combinatorial objects and  $\mathbb{Q}[C]$  be the  $\mathbb{Q}$ -linear span of  $C$ .

## Key idea

Knowing how to **break** combinatorial objects explains how to **combine** these.

To define a product  $\cdot : \mathbb{Q}[C] \otimes \mathbb{Q}[C] \rightarrow \mathbb{Q}[C]$ , it is in some cases more convenient to start by defining a **coproduct**  $\Delta : \mathbb{Q}[C] \rightarrow \mathbb{Q}[C] \otimes \mathbb{Q}[C]$ .

Every coproduct fits into the general form

$$\Delta(z) = \sum_{x,y \in C} \lambda_{x,y}^z (x \otimes y)$$

where the  $\lambda_{x,y}^z \in \mathbb{Q}$  are structure coefficients.

Then,  $\Delta$  leads by duality to the definition of  $\cdot$  by

$$x \cdot y := \sum_{z \in C} \lambda_{x,y}^z z.$$

# Combinatorial products and coproducts

Let  $C$  be a set of combinatorial objects and  $\mathbb{Q}[C]$  be the  $\mathbb{Q}$ -linear span of  $C$ .

## Key idea

Knowing how to **break** combinatorial objects explains how to **combine** these.

To define a product  $\cdot : \mathbb{Q}[C] \otimes \mathbb{Q}[C] \rightarrow \mathbb{Q}[C]$ , it is in some cases more convenient to start by defining a **coproduct**  $\Delta : \mathbb{Q}[C] \rightarrow \mathbb{Q}[C] \otimes \mathbb{Q}[C]$ .

Every coproduct fits into the general form

$$\Delta(z) = \sum_{x,y \in C} \lambda_{x,y}^z (x \otimes y)$$

where the  $\lambda_{x,y}^z \in \mathbb{Q}$  are structure coefficients.

Then,  $\Delta$  leads by duality to the definition of  $\cdot$  by

$$x \cdot y := \sum_{z \in C} \lambda_{x,y}^z z.$$

## Example: unshuffling words

Consider the coproduct

$$\Delta : \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*]$$

on words defined by

$$\Delta(u) := \sum_{P \sqcup Q = \{1, \dots, |u|\}} u|_P \otimes u|_Q.$$

### Example

$$\Delta(\mathbf{baa}) = \epsilon \otimes \mathbf{baa} + \mathbf{b} \otimes \mathbf{aa} + 2(\mathbf{a} \otimes \mathbf{ba}) + 2(\mathbf{ba} \otimes \mathbf{a}) + \mathbf{aa} \otimes \mathbf{b} + \mathbf{baa} \otimes \epsilon$$

### Proposition [Reutenauer, 1993]

The shuffle product of words is the dual product of the unshuffling coproduct of words.

### Example

Since  $\mathbf{a} \otimes \mathbf{ba}$  has multiplicity 2 in  $\Delta(\mathbf{baa})$ , the coeff. of  $\mathbf{baa}$  is 2 in  $\mathbf{a} \sqcup \mathbf{ba}$ :

$$\mathbf{a} \sqcup \mathbf{ba} = \mathbf{aba} + 2\mathbf{baa}.$$

## Example: unshuffling words

Consider the coproduct

$$\Delta : \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*]$$

on words defined by

$$\Delta(u) := \sum_{P \sqcup Q = \{1, \dots, |u|\}} u|_P \otimes u|_Q.$$

### Example

$$\Delta(\text{baa}) = \epsilon \otimes \text{baa} + \text{b} \otimes \text{aa} + 2(\text{a} \otimes \text{ba}) + 2(\text{ba} \otimes \text{a}) + \text{aa} \otimes \text{b} + \text{baa} \otimes \epsilon$$

### Proposition [Reutenauer, 1993]

The shuffle product of words is the dual product of the unshuffling coproduct of words.

### Example

Since  $\text{a} \otimes \text{ba}$  has multiplicity 2 in  $\Delta(\text{baa})$ , the coeff. of  $\text{baa}$  is 2 in  $\text{a} \sqcup \text{ba}$ :

$$\text{a} \sqcup \text{ba} = \text{aba} + 2\text{baa}.$$

## Example: unshuffling words

Consider the coproduct

$$\Delta : \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*]$$

on words defined by

$$\Delta(u) := \sum_{P \sqcup Q = \{1, \dots, |u|\}} u|_P \otimes u|_Q.$$

### Example

$$\Delta(\text{b a a}) = \epsilon \otimes \text{b a a} + \text{b} \otimes \text{a a} + 2(\text{a} \otimes \text{b a}) + 2(\text{b a} \otimes \text{a}) + \text{a a} \otimes \text{b} + \text{b a a} \otimes \epsilon$$

### Proposition [Reutenauer, 1993]

The shuffle product of words is the dual product of the unshuffling coproduct of words.

### Example

Since  $\text{a} \otimes \text{b a}$  has multiplicity 2 in  $\Delta(\text{b a a})$ , the coeff. of  $\text{b a a}$  is 2 in  $\text{a} \sqcup \text{b a}$ :

$$\text{a} \sqcup \text{b a} = \text{a b a} + 2 \text{b a a}.$$



## Example: unshuffling words

Consider the coproduct

$$\Delta : \mathbb{Q}[A^*] \rightarrow \mathbb{Q}[A^*] \otimes \mathbb{Q}[A^*]$$

on words defined by

$$\Delta(u) := \sum_{P \sqcup Q = \{1, \dots, |u|\}} u|_P \otimes u|_Q.$$

### Example

$$\Delta(\mathbf{b} \mathbf{a} \mathbf{a}) = \epsilon \otimes \mathbf{b} \mathbf{a} \mathbf{a} + \mathbf{b} \otimes \mathbf{a} \mathbf{a} + 2(\mathbf{a} \otimes \mathbf{b} \mathbf{a}) + 2(\mathbf{b} \mathbf{a} \otimes \mathbf{a}) + \mathbf{a} \mathbf{a} \otimes \mathbf{b} + \mathbf{b} \mathbf{a} \mathbf{a} \otimes \epsilon$$

### Proposition [Reutenauer, 1993]

The shuffle product of words is the dual product of the unshuffling coproduct of words.

### Example

Since  $\mathbf{a} \otimes \mathbf{b} \mathbf{a}$  has multiplicity 2 in  $\Delta(\mathbf{b} \mathbf{a} \mathbf{a})$ , the coeff. of  $\mathbf{b} \mathbf{a} \mathbf{a}$  is 2 in  $\mathbf{a} \sqcup \mathbf{b} \mathbf{a}$ :

$$\mathbf{a} \sqcup \mathbf{b} \mathbf{a} = \mathbf{a} \mathbf{b} \mathbf{a} + 2 \mathbf{b} \mathbf{a} \mathbf{a}.$$

# Unshuffling permutations

## Definition (standardization of words)

If  $u$  is a word of integers without multiple occurrence of a same letter, the **standardized**  $\text{std}(u)$  of  $u$  is the unique permutation of  $S_{|u|}$  order-isomorphic to  $u$ .

## Example

$$\text{std}(82194) = 42153$$

## Definition (unshuffling coproduct of permutations)

The **unshuffling coproduct of permutations** is the coproduct on  $\mathbb{Q}[S]$  defined by

$$\Delta(\pi) := \sum_{P \sqcup Q = \{1, \dots, |\pi|\}} \text{std}(\pi|_P) \otimes \text{std}(\pi|_Q).$$

## Example

$$\Delta(213) = \epsilon \otimes 213 + 2(1 \otimes 12) + 1 \otimes 21 + 2(12 \otimes 1) + 21 \otimes 1 + 213 \otimes \epsilon$$

# Unshuffling permutations

## Definition (standardization of words)

If  $u$  is a word of integers without multiple occurrence of a same letter, the **standardized**  $\text{std}(u)$  of  $u$  is the unique permutation of  $S_{|u|}$  order-isomorphic to  $u$ .

## Example

$$\text{std}(82194) = 42153$$

## Definition (unshuffling coproduct of permutations)

The **unshuffling coproduct of permutations** is the coproduct on  $\mathbb{Q}[S]$  defined by

$$\Delta(\pi) := \sum_{P \sqcup Q = \{1, \dots, |\pi|\}} \text{std}(\pi|_P) \otimes \text{std}(\pi|_Q).$$

## Example

$$\Delta(213) = \epsilon \otimes 213 + 1 \otimes 12 + 1 \otimes 21 + 2(12 \otimes 1) + 21 \otimes 1 + 213 \otimes \epsilon$$

# Unshuffling permutations

## Definition (standardization of words)

If  $u$  is a word of integers without multiple occurrence of a same letter, the **standardized**  $\text{std}(u)$  of  $u$  is the unique permutation of  $S_{|u|}$  order-isomorphic to  $u$ .

## Example

$$\text{std}(82194) = 42153$$

## Definition (unshuffling coproduct of permutations)

The **unshuffling coproduct of permutations** is the coproduct on  $\mathbb{Q}[S]$  defined by

$$\Delta(\pi) := \sum_{P \sqcup Q = \{1, \dots, |\pi|\}} \text{std}(\pi|_P) \otimes \text{std}(\pi|_Q).$$

## Example

$$\Delta(213) = \epsilon \otimes 213 + 1 \otimes 12 + 1 \otimes 21 + 2(12 \otimes 1) + 21 \otimes 1 + 213 \otimes \epsilon$$

# Unshuffling permutations

## Definition (standardization of words)

If  $u$  is a word of integers without multiple occurrence of a same letter, the **standardized**  $\text{std}(u)$  of  $u$  is the unique permutation of  $S_{|u|}$  order-isomorphic to  $u$ .

## Example

$$\text{std}(82194) = 42153$$

## Definition (unshuffling coproduct of permutations)

The **unshuffling coproduct of permutations** is the coproduct on  $\mathbb{Q}[S]$  defined by

$$\Delta(\pi) := \sum_{P \sqcup Q = \{1, \dots, |\pi|\}} \text{std}(\pi|_P) \otimes \text{std}(\pi|_Q).$$

## Example

$$\Delta(21\color{red}{3}) = \epsilon \otimes 213 + \color{brown}{2}(1 \otimes \color{red}{12}) + 1 \otimes 21 + 2(12 \otimes 1) + 21 \otimes 1 + 213 \otimes \epsilon$$

# Shuffling permutations

## Definition (shuffling product of permutations)

The **shuffling product of permutations** (supershuffle) is the product  $\bullet$  on  $\mathbb{Q}[S]$  defined as the dual product of the unshuffling product of permutations.

## Proposition

The permutations appearing in  $\sigma \bullet \nu$  are exactly the one obtained by shuffling two words  $u$  and  $v$  respectively order-isomorphic to  $\sigma$  and  $\nu$ .

## Example

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

# Shuffling permutations

## Definition (shuffling product of permutations)

The **shuffling product of permutations** (supershuffle) is the product  $\bullet$  on  $\mathbb{Q}[S]$  defined as the dual product of the unshuffling product of permutations.

## Proposition

The permutations appearing in  $\sigma \bullet \nu$  are exactly the one obtained by shuffling two words  $u$  and  $v$  respectively order-isomorphic to  $\sigma$  and  $\nu$ .

## Example

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

# Shuffling permutations

## Definition (shuffling product of permutations)

The **shuffling product of permutations** (supershuffle) is the product  $\bullet$  on  $\mathbb{Q}[S]$  defined as the dual product of the unshuffling product of permutations.

## Proposition

The permutations appearing in  $\sigma \bullet \nu$  are exactly the one obtained by shuffling two words  $u$  and  $v$  respectively order-isomorphic to  $\sigma$  and  $\nu$ .

## Example

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



# Square permutations

## Definition (square permutations)

A permutation  $\pi$  is a **square** (w.r.t. the shuffle product  $\bullet$ ) if there is  $\sigma \in S$  such that  $\pi$  appears in  $\sigma \bullet \sigma$ . We say that  $\sigma$  is a **square root** of  $\pi$ .

By duality,  $\pi$  is a square if there is  $\sigma \in S$  such that  $\sigma \otimes \sigma$  appears in  $\Delta(\pi)$ .

## Proposition

A permutation  $\pi$  is a square iff  $\pi$  can be obtained by shuffling two order-isomorphic words.

## Example

The permutation  $\pi := 25167834$  is square since  $\pi$  can be obtained by shuffling  $1683$  and  $2574$  and  $\text{std}(1683) = \text{std}(2574) = 1342$ .

# Square permutations

## Definition (square permutations)

A permutation  $\pi$  is a **square** (w.r.t. the shuffle product  $\bullet$ ) if there is  $\sigma \in S$  such that  $\pi$  appears in  $\sigma \bullet \sigma$ . We say that  $\sigma$  is a **square root** of  $\pi$ .

By duality,  $\pi$  is a square if there is  $\sigma \in S$  such that  $\sigma \otimes \sigma$  appears in  $\Delta(\pi)$ .

## Proposition

A permutation  $\pi$  is a square iff  $\pi$  can be obtained by shuffling two order-isomorphic words.

## Example

The permutation  $\pi := 25167834$  is square since  $\pi$  can be obtained by shuffling  $1683$  and  $2574$  and  $\text{std}(1683) = \text{std}(2574) = 1342$ .

# Square permutations

## Definition (square permutations)

A permutation  $\pi$  is a **square** (w.r.t. the shuffle product  $\bullet$ ) if there is  $\sigma \in S$  such that  $\pi$  appears in  $\sigma \bullet \sigma$ . We say that  $\sigma$  is a **square root** of  $\pi$ .

By duality,  $\pi$  is a square if there is  $\sigma \in S$  such that  $\sigma \otimes \sigma$  appears in  $\Delta(\pi)$ .

## Proposition

A permutation  $\pi$  is a square iff  $\pi$  can be obtained by shuffling two order-isomorphic words.

## Example

The permutation  $\pi := 25167834$  is square since  $\pi$  can be obtained by shuffling **1683** and **2574** and  $\text{std}(\mathbf{1683}) = \text{std}(\mathbf{2574}) = 1342$ .

# Some properties of square permutations

The first numbers of square permutations of size  $2n$  are

1, 2, 20, 504, 21032, 1293418.

Square permutations are compatible with some involutions on permutations:

## Proposition

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

- ①  $\tilde{\pi}$  is a square and  $\tilde{\sigma}$  is one of its square roots;
- ②  $\bar{\pi}$  is a square and  $\bar{\sigma}$  is one of its square roots;
- ③  $\pi^{-1}$  is a square and  $\sigma^{-1}$  is one of its square roots.

There is a link with square binary words:

## Proposition

The set of binary words of length  $n$  that are square w.r.t.  $\sqcup$  is in one-to-one correspondence with the set of square permutations of length  $n$  avoiding the patterns 213 and 231.

# Some properties of square permutations

The first numbers of square permutations of size  $2n$  are

$$1, 2, 20, 504, 21032, 1293418.$$

Square permutations are compatible with some involutions on permutations:

## Proposition

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

- ①  $\tilde{\pi}$  is a square and  $\tilde{\sigma}$  is one of its square roots;
- ②  $\bar{\pi}$  is a square and  $\bar{\sigma}$  is one of its square roots;
- ③  $\pi^{-1}$  is a square and  $\sigma^{-1}$  is one of its square roots.

There is a link with square binary words:

## Proposition

The set of binary words of length  $n$  that are square w.r.t.  $\sqcup$  is in one-to-one correspondence with the set of square permutations of length  $n$  avoiding the patterns 213 and 231.

# Some properties of square permutations

The first numbers of square permutations of size  $2n$  are

$$1, 2, 20, 504, 21032, 1293418.$$

Square permutations are compatible with some involutions on permutations:

## Proposition

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

- ①  $\tilde{\pi}$  is a square and  $\tilde{\sigma}$  is one of its square roots;
- ②  $\bar{\pi}$  is a square and  $\bar{\sigma}$  is one of its square roots;
- ③  $\pi^{-1}$  is a square and  $\sigma^{-1}$  is one of its square roots.

There is a link with square binary words:

## Proposition

The set of binary words of length  $n$  that are square w.r.t.  $\sqcup$  is in one-to-one correspondence with the set of square permutations of length  $n$  avoiding the patterns 213 and 231.

# Contents

## 3 Algorithmic issues

# Pattern involvement problem

## Definition (permutation patterns)

A permutation  $\pi$  **contains** a permutation  $\sigma$  if there exists a subsequence of (not necessarily consecutive) letters of  $\pi$  that has the same relative order as  $\sigma$ , and in this case  $\sigma$  is said to be a **pattern** of  $\pi$ , written  $\sigma \leq \pi$ .

Otherwise,  $\pi$  **avoids**  $\sigma$ .

## Example

The permutation  $\pi = 391867452$  contains the pattern  $\sigma := 51342$  since  $\text{std}(91674) = 51342$ .

## Definition (pattern involvement problem)

The **pattern involvement problem** is the decision problem consisting in, given  $\pi, \sigma \in S$ , decide whether  $\sigma \leq \pi$ .

## Proposition [Bose, Buss, Lubiw, 1998]

The pattern involvement problem is NP-complete.



# Pattern involvement problem

## Definition (permutation patterns)

A permutation  $\pi$  **contains** a permutation  $\sigma$  if there exists a subsequence of (not necessarily consecutive) letters of  $\pi$  that has the same relative order as  $\sigma$ , and in this case  $\sigma$  is said to be a **pattern** of  $\pi$ , written  $\sigma \leq \pi$ .

Otherwise,  $\pi$  **avoids**  $\sigma$ .

## Example

The permutation  $\pi = 391867452$  contains the pattern  $\sigma := 51342$  since  $\text{std}(91674) = 51342$ .

## Definition (pattern involvement problem)

The **pattern involvement problem** is the decision problem consisting in, given  $\pi, \sigma \in S$ , decide whether  $\sigma \leq \pi$ .

## Proposition [Bose, Buss, Lubiw, 1998]

The pattern involvement problem is **NP**-complete.

# Pattern involvement problem

## Definition (permutation patterns)

A permutation  $\pi$  **contains** a permutation  $\sigma$  if there exists a subsequence of (not necessarily consecutive) letters of  $\pi$  that has the same relative order as  $\sigma$ , and in this case  $\sigma$  is said to be a **pattern** of  $\pi$ , written  $\sigma \leq \pi$ .

Otherwise,  $\pi$  **avoids**  $\sigma$ .

## Example

The permutation  $\pi = 391867452$  contains the pattern  $\sigma := 51342$  since  $\text{std}(91674) = 51342$ .

## Definition (pattern involvement problem)

The **pattern involvement problem** is the decision problem consisting in, given  $\pi, \sigma \in S$ , decide whether  $\sigma \leq \pi$ .

## Proposition [Bose, Buss, Lubiw, 1998]

The pattern involvement problem is **NP**-complete.

# Pattern involvement problem

## Definition (permutation patterns)

A permutation  $\pi$  **contains** a permutation  $\sigma$  if there exists a subsequence of (not necessarily consecutive) letters of  $\pi$  that has the same relative order as  $\sigma$ , and in this case  $\sigma$  is said to be a **pattern** of  $\pi$ , written  $\sigma \leq \pi$ .

Otherwise,  $\pi$  **avoids**  $\sigma$ .

## Example

The permutation  $\pi = 391867452$  contains the pattern  $\sigma := 51342$  since  $\text{std}(91674) = 51342$ .

## Definition (pattern involvement problem)

The **pattern involvement problem** is the decision problem consisting in, given  $\pi, \sigma \in S$ , decide whether  $\sigma \leq \pi$ .

## Proposition [Bose, Buss, Lubiw, 1998]

The pattern involvement problem is **NP**-complete.

# Recognizing square permutations

## Definition (perfect matchings for permutations)

A **perfect matching** of a permutation  $\pi \in S_n$  is a directed graph  $(V, A)$  such that

- $V := \{(\pi_i, i) : i \in \{1, \dots, n\}\}$ ;
- every vertex of  $V$  belongs to exactly one arc of  $A$ .

## Definition (property $P_1$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $P_1$  if it avoids all the six patterns .

## Definition (property $P_2$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $P_2$  if, for all arcs  $(\pi_i, i) \rightarrow (\pi_j, j)$  and  $(\pi_k, k) \rightarrow (\pi_\ell, \ell)$  of  $A$ ,  $\pi_i < \pi_k$  iff  $\pi_j < \pi_\ell$ .







# Recognizing square permutations

## Definition (perfect matchings for permutations)

A **perfect matching** of a permutation  $\pi \in S_n$  is a directed graph  $(V, A)$  such that

- $V := \{(\pi_i, i) : i \in \{1, \dots, n\}\}$ ;
- every vertex of  $V$  belongs to exactly one arc of  $A$ .

## Definition (property $\mathbf{P}_1$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $\mathbf{P}_1$  if it avoids all the six patterns , , , , , and .

## Definition (property $\mathbf{P}_2$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $\mathbf{P}_2$  if, for all arcs  $(\pi_i, i) \rightarrow (\pi_j, j)$  and  $(\pi_k, k) \rightarrow (\pi_\ell, \ell)$  of  $A$ ,  $\pi_i < \pi_k$  iff  $\pi_j < \pi_\ell$ .







# Recognizing square permutations

## Definition (perfect matchings for permutations)

A **perfect matching** of a permutation  $\pi \in S_n$  is a directed graph  $(V, A)$  such that

- $V := \{(\pi_i, i) : i \in \{1, \dots, n\}\}$ ;
- every vertex of  $V$  belongs to exactly one arc of  $A$ .

## Definition (property $\mathbf{P}_1$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $\mathbf{P}_1$  if it avoids all the six patterns , , , , , and .

## Definition (property $\mathbf{P}_2$ )

Let  $\pi \in S$ . A perfect matching  $(V, A)$  of  $\pi$  has property  $\mathbf{P}_2$  if, for all arcs  $(\pi_i, i) \rightarrow (\pi_j, j)$  and  $(\pi_k, k) \rightarrow (\pi_\ell, \ell)$  of  $A$ ,  $\pi_i < \pi_k$  iff  $\pi_j < \pi_\ell$ .

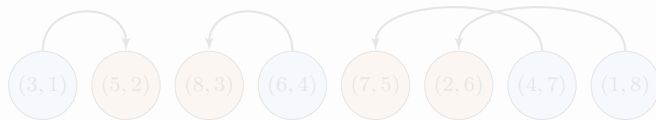
# Recognizing square permutations

## Proposition

A permutation  $\pi$  is a square (w.r.t. the shuffle product  $\bullet$ ) iff  $\pi$  admits a perfect matching satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

## Example

The permutation  $\pi := 35867241$  is a square since it admits the perfect matching



satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

Moreover, this shows that  $\pi$  appears in the shuffle of the words  $3641$  and  $5872$ , both order-isomorphic to  $2431$ .

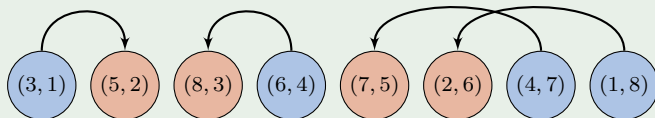
# Recognizing square permutations

## Proposition

A permutation  $\pi$  is a square (w.r.t. the shuffle product  $\bullet$ ) iff  $\pi$  admits a perfect matching satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

## Example

The permutation  $\pi := 35867241$  is a square since it admits the perfect matching



satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

Moreover, this shows that  $\pi$  appears in the shuffle of the words **3641** and **5872**, both order-isomorphic to 2431.



# Hardness of recognizing square permutations

## Proposition

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

## Main ideas of the proof

- We show that the pattern involvement problem is reducible in polynomial time to the problem of deciding if a permutation is a square.

- For this, given two permutations  $\sigma$  and  $\pi$ , we show that  $\sigma \leq \pi$  iff  $\mu_{\sigma,\pi}$  is a square, where  $\mu_{\sigma,\pi}$  is a permutation constructed in polynomial time from  $\sigma$  and  $\pi$ .

We use the fact that  $\mu_{\sigma,\pi}$  is a square iff  $\mu_{\sigma,\pi}$  admits a perfect matching satisfying  $P_1$  and  $P_2$ .

# Hardness of recognizing square permutations

## Proposition

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

## Main ideas of the proof

- We show that the pattern involvement problem is reducible in polynomial time to the problem of deciding if a permutation is a square.
- For this, given two permutations  $\sigma$  and  $\pi$ , we show that  $\sigma \leq \pi$  iff  $\mu_{\sigma,\pi}$  is a square, where  $\mu_{\sigma,\pi}$  is a permutation constructed in polynomial time from  $\sigma$  and  $\pi$ .
- We use the fact that  $\mu_{\sigma,\pi}$  is a square iff  $\mu_{\sigma,\pi}$  admits a perfect matching satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

# Hardness of recognizing square permutations

## Proposition

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

## Main ideas of the proof

- We show that the pattern involvement problem is reducible in polynomial time to the problem of deciding if a permutation is a square.
- For this, given two permutations  $\sigma$  and  $\pi$ , we show that  $\sigma \leq \pi$  iff  $\mu_{\sigma,\pi}$  is a square, where  $\mu_{\sigma,\pi}$  is a permutation constructed in polynomial time from  $\sigma$  and  $\pi$ .
- We use the fact that  $\mu_{\sigma,\pi}$  is a square iff  $\mu_{\sigma,\pi}$  admits a perfect matching satisfying  $\mathbf{P}_1$  and  $\mathbf{P}_2$ .

# Hardness of recognizing square permutations

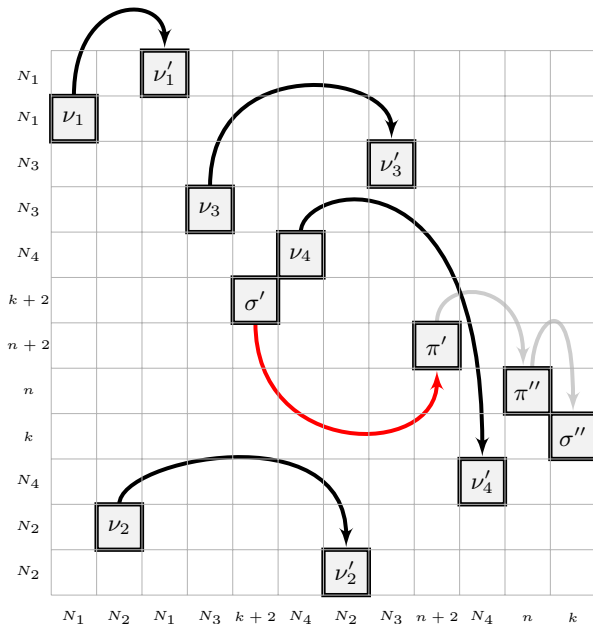
## Proposition

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

## Main ideas of the proof

- We show that the pattern involvement problem is reducible in polynomial time to the problem of deciding if a permutation is a square.
- For this, given two permutations  $\sigma$  and  $\pi$ , we show that  $\sigma \leq \pi$  iff  $\mu_{\sigma,\pi}$  is a square, where  $\mu_{\sigma,\pi}$  is a permutation constructed in polynomial time from  $\sigma$  and  $\pi$ .
- We use the fact that  $\mu_{\sigma,\pi}$  is a square iff  $\mu_{\sigma,\pi}$  admits a perfect matching satisfying **P**<sub>1</sub> and **P**<sub>2</sub>.

# Hardness of recognizing square permutations



# Open problems

## Combinatorics

Enumeration of square permutations?

## Algorithms

Given two permutations  $\pi$  and  $\sigma$ , how hard is the problem of deciding whether  $\sigma$  is a square root of  $\pi$ ?

## Algebra

How algebraic properties of the associative algebra  $(\mathbb{Q}[S], \bullet)$  or of the coalgebra  $(\mathbb{Q}[S], \Delta)$  are connected to combinatorial and algorithmic properties of square permutations?

# Open problems

## Combinatorics

Enumeration of square permutations?

## Algorithms

Given two permutations  $\pi$  and  $\sigma$ , how hard is the problem of deciding whether  $\sigma$  is a square root of  $\pi$ ?

## Algebra

How algebraic properties of the associative algebra  $(\mathbb{Q}[S], \bullet)$  or of the coalgebra  $(\mathbb{Q}[S], \Delta)$  are connected to combinatorial and algorithmic properties of square permutations?

# Open problems

## Combinatorics

Enumeration of square permutations?

## Algorithms

Given two permutations  $\pi$  and  $\sigma$ , how hard is the problem of deciding whether  $\sigma$  is a square root of  $\pi$ ?

## Algebra

How algebraic properties of the associative algebra  $(\mathbb{Q}[S], \bullet)$  or of the coalgebra  $(\mathbb{Q}[S], \Delta)$  are connected to combinatorial and algorithmic properties of square permutations?