RECONSTRUCTION OF FUNCTIONS FROM MINORS

HABILITATIONSSCHRIFT

vorgelegt

der Fakultät Mathematik und Naturwissenschaften

der Technischen Universität Dresden

von

D. Sc. Erkko Lehtonen

geboren am 3. November 1974 in Tampere, Finnland

Eingereicht am 13. September 2017

Wissenschaftlicher Vortrag und Aussprache,

sowie Probevorlesung am 9. Juli 2018

Die Habilitationsschrift wurde in der Zeit von August 2016

bis September 2017 im Institut für Algebra angefertigt.

CONTENTS

ABSTRACT v

ACKNOWLEDGMENTS vii

1 INTRODUCTION AND PRELIMINARIES 1
- 1.1 Overview 1
- 1.2 General notation 3
- 1.3 Binary relations 4
- 1.4 Partitions 4
- 1.5 Functions 6
- 1.6 Permutations and permutation groups 6
- 1.7 Ordered partitions 8
- 1.8 Galois connections 13
- 1.9 Multisets 14

2 MINORS OF FUNCTIONS 15
- 2.1 Functions of several arguments 15
- 2.2 Minors 16
- 2.3 On the structure of the minor order of functions 21
- 2.4 Arity gap 23
- 2.5 Invariance groups 24
- 2.6 Unique identification minors 25
- 2.7 Clones and minor-closed classes of functions 26
  - 2.7.1 Clones 26
  - 2.7.2 Minor-closed classes of functions 29
  - 2.7.3 Reducts of iterative algebra 30
- 2.8 Variants of minors 30

3 RECONSTRUCTION PROBLEMS 33
- 3.1 Definition and examples 33
- 3.2 Reconstruction problem of functions and identification minors 36
- 3.3 Reconstructibility of totally symmetric functions 38
- 3.4 Reconstructibility of affine functions 38
- 3.5 Nonreconstructible functions 42
- 3.6 Reconstructibility of Post classes 44
- 3.7 Remarks 45

4 MINORS OF PERMUTATIONS 47
- 4.1 Minors of permutations 47
- 4.2 Galois connections induced by the minor relation of permutations 52
- 4.3 Compressions and expansions of interval partitions 54

4.4 On groups generated by minors and their differences 61
4.4.1 Special permutations θ_n and λ_k^ℓ 61
4.4.2 Invariant interval partitions 61
4.4.3 Group generated by the minors of a permutation 62
4.4.4 Group generated by the differences of minors of a permutation 64
4.5 Reconstruction problem of permutations and minors 71
4.6 Remarks 72

5 ORDER OF FIRST OCCURRENCE 73
5.1 Formal definition and basic facts 73
5.2 Functions determined by the order of first occurrence 75
5.3 Invariance groups of functions determined by the order of first occurrence 76
5.4 Reconstructibility of functions determined by the order of first occurrence 79
5.4.1 Remarks on the reconstruction problem 79
5.4.2 Weak reconstructibility 80
5.4.3 Reconstructible subclasses 85

A POST CLASSES 89

BIBLIOGRAPHY 93

LIST OF SYMBOLS 101

ABSTRACT

The central notion of this thesis is the minor relation on functions of several arguments. A function $f\colon A^n \to B$ is called a minor of another function $g\colon A^m \to B$ if f can be obtained from g by permutation of arguments, identification of arguments, and introduction of inessential arguments. We first provide some general background and context to this work by presenting a brief survey of basic facts and results concerning different aspects of the minor relation, placing some emphasis on the author's contributions to the field.

The notions of functions of several arguments and minors give immediately rise to the following reconstruction problem: Is a function $f\colon A^n \to B$ uniquely determined, up to permutation of arguments, by its identification minors, i.e., the minors obtained by identifying a pair of arguments? We review known results – both positive and negative – about the reconstructibility of functions from identification minors, and we outline the main ideas of the proofs, which often amount to formulating and solving reconstruction problems for other kinds of mathematical objects.

We then turn our attention to functions determined by the order of first occurrence, and we are interested in the reconstructibility of such functions. One of the main results of this thesis states that the class of functions determined by the order of first occurrence is weakly reconstructible. Some reconstructible subclasses are identified; in particular, pseudo-Boolean functions determined by the order of first occurrence are reconstructible.

As our main tool, we introduce the notion of minor of permutation. This is a quotient-like construction for permutations that parallels minors of functions and has some similarities to permutation patterns. We develop the theory of minors of permutations, focusing on Galois connections induced by the minor relation and on the interplay between permutation groups and minors of permutations. Our results will then find applications in the analysis of the reconstruction problem of functions determined by the order of first occurrence.

ACKNOWLEDGMENTS

The work reported in this thesis was carried out in the ten years following my doctoral graduation from Tampere University of Technology in 2007, during which I have pursued postdoctoral studies at the University of Waterloo, University of Luxembourg, University of Lisbon, and, currently, Dresden University of Technology. The actual writing of this thesis took place in the period from August 2016 to September 2017.

I am thankful to Prof. Dr. Ulrike Baumann, director of the Institute of Algebra, TU Dresden, and to Prof. Dr. Manuel Bodirsky for giving me the opportunity of completing this work.

This work would not have been possible without the help, support, and guidance of many people. I am deeply indebted to my former doctoral advisor and long-time mentor Prof. Dr. Stephan Foldes for introducing me to the wonderful and sometimes frustrating world of mathematical research. I would like to express my thanks to all my coauthors for fruitful collaboration and their precious contributions to this work, as well as to many other colleagues who have offered their advice and assistance. I have learnt a lot from all of them.

I would like to extend my gratitude to my colleagues at the Institute of Algebra, TU Dresden, for the pleasant working environment. Especially discussions with Prof. Dr. Reinhard Pöschel and his "questions of the day" have been most inspiring and enlightening.

My special thanks go to Prof. Dr. Miguel Couceiro, with whom I have had the privilege of collaborating over the course of many years on several occasions in different geographical locations, and who remains a true and steadfast friend. It is always a great pleasure to discuss or debate or just chat with him.

Finally, I am grateful to my parents for their continuous encouragement and support throughout my academic and personal journey.

1

INTRODUCTION AND PRELIMINARIES

This thesis consists of two main parts. The first part (Chapters 1–3) is in the nature of a survey and relies mainly on published studies. Its purpose is to introduce the mathematical notions that are relevant to us, to provide some background and context to the current work, to state some important results, and to present a review of the author's earlier contributions to the field. Almost all proofs are omitted, and references are given to the original publications, which should be consulted for further details. The second part (Chapters 4 and 5) is comprised of new, previously unpublished results with proofs.

1.1 OVERVIEW

Functions of several arguments appear in many fields of mathematics, such as multivariate calculus, predicate logic, and universal algebra, and they are the main objects of study in this thesis. In particular, this thesis revolves around the notion of minors of functions. A function $f\colon A^n \to B$ is called a *minor* of another function $g\colon A^m \to B$, if f can be obtained from g by manipulations of arguments: permutation of arguments, introduction and deletion of inessential arguments, and identification of arguments.

Formation of minors is a way of building new functions from given ones; in fact, minors are particular instances of functional composition in which functions are composed with projections. Minors arise naturally in many contexts. A universal algebraist sees immediately that minors are term functions induced by terms of height 1. For another example, weighted voting systems can be modeled in terms of threshold Boolean functions, and formation of coalitions corresponds to formation of minors of functions.

Minors of functions have been extensively studied by many authors from many different points of view. Chapter 2 comprises a brief survey on various aspects of minors, with a focus on the author's earlier contributions to the topic. We start with structural descriptions of the minor order. Then we discuss the arity gap, which is a measure of the minimum decrease in the number of essential arguments when minors of a function are formed. We give some special attention to functions with a unique identification minor. We explain how minor-closed classes of functions can be defined as the subuniverses of certain algebras and how they can be characterized as the closed classes of a Galois connection between functions and constraints. We also briefly mention some variants of the notion of a minor.

Another central topic of this thesis is reconstruction problems. Speaking in very general terms, a reconstruction problem asks whether a mathematical object can be uniquely recovered from pieces of partial information thereon. An archetypical example of a reconstruction problem is present in a famous unproven conjecture in graph theory, the so-called reconstruction conjecture, due to Kelly [45] and Ulam [84], which concerns whether or not a graph is uniquely determined, up to isomorphism, by the collection of its one-vertex-deleted subgraphs. This is an example of the type of reconstruction problems we discuss in this thesis: given a large class of mathematical objects and a way of deriving "subobjects" of each member of the class, we ask whether or not the objects are uniquely determined by the collection of their derived subobjects.

Our main interest lies in the following reconstruction problem: Is a function $f\colon A^n \to B$ uniquely determined, up to equivalence, by the collection of its identification minors? This problem has been studied by the current author, and in Chapter 3, we survey some known results – both positive and negative – concerning the reconstructibility of functions. On the one hand, certain classes of functions have been shown to be reconstructible, for example, the classes of totally symmetric functions (of sufficiently large arity) and affine functions over finite fields (of sufficiently large arity). On the other hand, infinite families of nonreconstructible functions have been constructed. In Chapter 5, we will present some new results on the reconstruction problem of functions, more specifically, on the reconstructibility of functions determined by the order of first occurrence.

The order of first occurrence is a notion that we consider more carefully in this thesis. The idea of listing objects in the order they first appear in a sequence of data emerges in various everyday situations and it is employed in many fields of science, arts and humanities. For example, in the closing credits of a motion picture or a television show, it is not uncommon that the characters and the cast members who portray them are listed in the order of first appearance. In scientific research articles, the entries in a bibliography are usually arranged either alphabetically by authors' names or in the order of first citation.

In algebra, the idea of arranging objects in the order they first appear is neatly captured by left regular bands, i.e., semigroups satisfying the identities $x^2 \approx x$ and $xyx \approx xy$. These identities convey precisely the meaning that we can delete from a semigroup word any element that has occurred earlier; thus we can reduce every word into one in which each element occurs only once, in the order of first occurrence.

We focus our attention on the function called "ofo" that is defined and valued on the set of all strings over a fixed alphabet and that transforms any string by deleting duplicate letters while keeping only

the first occurrence of each letter. In other words, ofo maps each string to the unique subsequence that lists the different letters occurring in the string in the order of first occurrence – hence the acronym ofo.

A function $f\colon A^n \to B$ is said to be determined by the order of first occurrence, if it is decomposable via ofo as $f = f^* \circ \mathrm{ofo}|_{A^n}$. In other words, the value of f depends only on the order in which elements of A first occur in the input. Functions determined by the order of first occurrence have remarkable properties. For example, they have a unique identification minor. In this thesis, we establish further mathematical properties of functions determined by the order of first occurrence. One of our new results is a characterization of the permutation groups that appear as invariance groups of functions determined by the order of first occurrence (Theorem 5.3.4). We then investigate in detail the reconstruction problem for functions determined by the order of first occurrence in Section 5.4. We establish that the class of functions determined by the order of first occurrence (of sufficiently large arity) is weakly reconstructible (Theorem 5.4.5). Some reconstructible subclasses are identified; in particular, pseudo-Boolean functions determined by the order of first occurrence are reconstructible.

As our main tool, we introduce a new notion of a minor of a permutation in Chapter 4. Minors of permutations can be seen as a quotient-like construction for permutations, and they are in a certain way analogous to minors of functions and have some similarities to permutation patterns. As a first step towards developing a theory of minors of permutations, we investigate the monotone Galois connection $\mathrm{Min}^{(\ell)}$–$\mathrm{Comp}^{(n)}$ induced by the minor relation between ℓ- and n-permutations. We are particularly interested in the interplay between permutation groups and minors of permutations. For the needs of our applications, we establish some results concerning the groups generated by the set of ℓ-minors of an n-permutation τ and the set of differences of ℓ-minors of τ (Propositions 4.4.15 and 4.4.16). We also briefly discuss a reconstruction problem of permutations from minors. With this toolbox, we finally attack the reconstruction problem of functions determined by the order of first occurrence in Chapter 5.

1.2 GENERAL NOTATION

We presuppose that the reader is familiar with fundamental notions in abstract algebra, such as functions, relations, ordered sets, groupoids, semigroups, monoids, groups, rings, fields, lattices, terms, and term operations, which can be found in many textbooks, such as the ones by Cameron [8], Davey and Priestley [24], Denecke and Wismath [26], Foldes [31], and Lang [51]. We will review some of the basic terminology and notions that will be used in this work.

The symbols $\mathbf{N}$ and $\mathbf{N}_+$ stand for the set of all nonnegative integers and the set of all positive integers, respectively. For $a, b \in \mathbf{N}$, the *interval* $\{n \in \mathbf{N} : a \leq n \leq b\}$ is denoted by $[a, b]$. The interval $[1, n] = \{1, \ldots, n\}$ of first n positive integers is denoted simply by $[n]$. Note that if $a > b$ then $[a, b]$ equals the empty set $\emptyset$; in particular $[0] = \emptyset$.

The power set of a set S and the set of all k-element subsets of S are denoted by $\mathcal{P}(S)$ and $\binom{S}{k}$, respectively.

The n-th Cartesian power of a set A is denoted by A^n. We usually designate tuples by bold letters and their components by corresponding italic letters. For example, $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$. We often write a tuple $(a_1, \ldots, a_n)$ as a string (or word) $a_1 \ldots a_n$. We let $A^* := \bigcup_{n \geq 0} A^n$ be the set of all words over A and $A^+ := \bigcup_{n \geq 1} A^n$ be the set of all nonempty words over A. The unique element of A^0 is denoted by ε and is called the empty word.

Let

$$A^n_{\neq} := \{(a_1, \ldots, a_n) \in A^n : a_1, a_2, \ldots, a_n \text{ pairwise distinct}\}, \quad (1.2.1)$$

$$A^\sharp := \bigcup_{n \geq 1} A^n_{\neq}. \quad (1.2.2)$$

Note that $A^n_{\neq} \neq \emptyset$ if and only if $n \leq |A|$.

1.3 BINARY RELATIONS

Recall that a reflexive and transitive relation on a set A is called a *quasiorder* (or *preorder*). An antisymmetric quasiorder is a *partial order,* and a symmetric quasiorder is an *equivalence relation.*

Let $\equiv$ be an equivalence relation on A. We denote the equivalence class of an element $x \in A$ by $x/\equiv$. The set of equivalence classes of $\equiv$ is denoted by $A/\equiv$ and is called the *quotient set* of A by $\equiv$.

It is well known that every quasiorder $\leq$ on A induces an equivalence relation $\equiv$ on A by the rule $x \equiv y$ if and only if $x \leq y$ and $y \leq x$. Moreover, $\leq$ induces a partial order $\preceq$ on the quotient $A/\equiv$ by the rule $x/\equiv \preceq y/\equiv$ if and only if $x \leq y$.

1.4 PARTITIONS

Recall that a *partition* of a set S is a collection of pairwise disjoint nonempty subsets of S whose union is the whole set S. The elements of a partition are called *blocks.* A partition with exactly m blocks is called an *m-partition.* Singleton blocks are *trivial,* and blocks with at least two elements are *nontrivial.* A partition is *trivial* if all its blocks are trivial.

Let Π be a partition of S. The blocks of Π are called Π-*blocks.* For each $x \in S$, we denote by x/Π the unique Π-block that contains x. We write $x \equiv_\Pi y$ if x and y belong to the same Π-block, i.e., $x/\Pi = y/\Pi$.

The relation $\equiv_\Pi$ is an equivalence relation on S. Conversely, the set of equivalence classes of an arbitrary equivalence relation on S is a partition of S. In fact, the partitions of S and the equivalence relations of S are in a one-to-one correspondence given by $\Pi \mapsto \equiv_\Pi$, and we may freely switch between these two notions.

Let Π and Γ be two partitions of S. If every Π-block is a subset of some Γ-block, then Π is a *refinement* of Γ, and Γ is a *coarsening* of Π; in this case we also say that Π is *finer* than Γ and Γ is *coarser* than Π, and we write $\Pi \sqsubseteq \Gamma$. The set of all partitions of S ordered by the refinement relation $\sqsubseteq$ is a semi-modular lattice, and we write $\Pi \wedge \Gamma$ and $\Pi \vee \Gamma$ for the coarsest common refinement and the finest common coarsening of Π and Γ, respectively. In fact, $\Pi \wedge \Gamma = \{B \cap C : B \in \Pi, C \in \Gamma\} \setminus \{\emptyset\}$. The blocks of $\Pi \vee \Gamma$ can be described as follows: for all $x, y \in S$, it holds that $x \equiv_{\Pi\vee\Gamma} y$ if and only if there exists a sequence $z_1, \ldots, z_\ell$ of elements of S such that $x = z_1$, $y = z_\ell$, and $z_i \equiv_\Pi z_{i+1}$ or $z_i \equiv_\Gamma z_{i+1}$ for all $i \in \{1, \ldots, \ell - 1\}$. In other words, $\equiv_{\Pi\vee\Gamma}$ is the transitive closure of $\equiv_\Pi \cup \equiv_\Gamma$.

We will mainly consider partitions of the set $[n]$ for some $n \in \mathbf{N}_+$. We denote the set of all partitions of $[n]$ by $\mathrm{Part}(n)$ and the set of all m-partitions of $[n]$ by $\mathrm{Part}_m(n)$. We denote the trivial partition of $[n]$ by Δ_n.

Remark 1.4.1. We often use a shorthand notation for specifying partitions of $[n]$. Each block is represented by a string of numbers, and different blocks are separated by a vertical line. For example, the partition $\{\{1,3,7,8\},\{2,4,5\},\{6\},\{9\}\}$ of $[9]$ can be written briefly as $1378|245|6|9$.

A partition Π of $[n]$ is called an *interval partition*, if all its blocks are intervals (see Section 1.2). The set of all interval partitions of $[n]$ is denoted by $\mathrm{IntPart}(n)$; we also write $\mathrm{IntPart}_m(n) := \mathrm{IntPart}(n) \cap \mathrm{Part}_m(n)$. The set $\mathrm{IntPart}(n)$ of interval partitions of $[n]$ constitutes a sublattice of the lattice $\mathrm{Part}(n)$ of all partitions of $[n]$ ordered by refinement.

For any $\mathcal{S} \subseteq \mathcal{P}([n])$, the partition of $[n]$ *induced* by $\mathcal{S}$, denoted $\langle \mathcal{S} \rangle_{\mathrm{part}}$, is the finest partition $\Pi \in \mathrm{Part}(n)$ such that every set of the collection $\mathcal{S}$ is a subset of some Π-block. The underlying set $[n]$ will be understood from the context.

The following two facts follow immediately from the definitions.

Fact 1.4.2. For all $\Pi, \Gamma \in \mathrm{Part}(n)$, we have $\Pi \vee \Gamma = \langle \Pi \cup \Gamma \rangle_{\mathrm{part}}$.

Fact 1.4.3. If $\mathcal{S} \subseteq \mathcal{P}([n])$ is a collection of intervals, then $\langle \mathcal{S} \rangle_{\mathrm{part}}$ is an interval partition.

Example 1.4.4. Let $\mathcal{S} = \{\{2,3\},\{3,4\},\{6\},\{7,8\},\{7,8,9\}\} \subseteq \mathcal{P}([10])$. Then $\langle \mathcal{S} \rangle_{\mathrm{part}} = 1\,|\,2\,3\,4\,|\,5\,|\,6\,|\,7\,8\,9\,|\,10$. Note that $\mathcal{S}$ is a collection of intervals, and the partition induced by $\mathcal{S}$ is an interval partition.

Lemma 1.4.5. *Let $\mathcal{S}$ and $\mathcal{T}$ be collections of subsets of $[n]$. Assume that for every $X \in \mathcal{S}$ there exists $Y \in \mathcal{T}$ such that $X \subseteq Y$. Then $\langle \mathcal{S} \rangle_{\text{part}}$ is a refinement of $\langle \mathcal{T} \rangle_{\text{part}}$.*

Proof. Let B be a block of $\langle \mathcal{S} \rangle_{\text{part}}$. Let $x, y \in B$. There exists a sequence $C_1, \ldots, C_p$ of sets in $\mathcal{S}$ such that $x \in C_1$, $y \in C_p$ and $C_i \cap C_{i+1} \neq \emptyset$ for all $i \in \{1, \ldots, p-1\}$. By our assumption, there exist sets $D_1, \ldots, D_p$ in $\mathcal{T}$ such that $C_i \subseteq D_i$ for all $i \in \{1, \ldots, p\}$. We have $x \in D_1$, $y \in D_p$ and $D_i \cap D_{i+1} \supseteq C_i \cap C_{i+1} \neq \emptyset$ for all $i \in \{1, \ldots, p-1\}$. Consequently, x and y belong to the same block of $\langle \mathcal{T} \rangle_{\text{part}}$. We conclude that every block of $\langle \mathcal{S} \rangle_{\text{part}}$ is a subset of some block of $\langle \mathcal{T} \rangle_{\text{part}}$, i.e., $\langle \mathcal{S} \rangle_{\text{part}} \sqsubseteq \langle \mathcal{T} \rangle_{\text{part}}$. □

Remark 1.4.6. In what follows, we will introduce several concepts and notations that involve partitions. We will often abuse notation – for the sake of brevity – and, for any nonempty subset $S \subseteq [n]$, we will write S as a shorthand for the partition of $[n]$ in which S is the only potentially nontrivial block. The intended meaning will be clear from the context.

1.5 FUNCTIONS

Let $f\colon A \to B$ and $g\colon B' \to C$ be functions. If $B \subseteq B'$, then the *composite* function $g \circ f\colon A \to C$ is defined by $(g \circ f)(x) = g(f(x))$ for all $x \in A$. We often denote $g \circ f$ simply by gf.

Any function $\varphi\colon A \to B$ can be lifted to a map between power sets: $\varphi'\colon \mathcal{P}(A) \to \mathcal{P}(B)$, $\varphi'(X) := \{\varphi(x) : x \in A\}$ for any $X \in \mathcal{P}(A)$. We normally use the same symbol for a map and the corresponding lifted map; without risk of confusion, we may write $\varphi(x)$ for any $x \in A$ and $\varphi(X)$ for any $X \subseteq A$. Note also that the lifted map φ' can be lifted further to $\varphi''\colon \mathcal{P}(\mathcal{P}(A)) \to \mathcal{P}(\mathcal{P}(B))$, $\varphi''(\mathcal{X}) := \{\varphi'(X) : X \in \mathcal{X}\}$, and $\varphi''(\mathcal{X})$ will again be written simply as $\varphi(\mathcal{X})$.

Let $f\colon A \to B$ be a function. The *range* (or *image*) of f is $\operatorname{Im} f := \{f(x) : x \in A\} = f'(A)$. The *restriction* of f to a subset $S \subseteq A$ is the function $f|_S\colon S \to f'(S)$, $x \mapsto f(x)$ for all $x \in S$. The *kernel* of f, denoted $\ker f$, is the partition of A where two elements $x_1, x_2 \in A$ belong to the same block if and only if $f(x_1) = f(x_2)$. The following fact is easy to verify.

Fact 1.5.1. Let $f\colon A \to B$ and $g\colon B \to C$. Then $\ker f \sqsubseteq \ker g \circ f$. Moreover, if f is surjective, then $\ker g = f(\ker g \circ f)$.

1.6 PERMUTATIONS AND PERMUTATION GROUPS

A *permutation* of a set S is a bijective map $S \to S$. Equipped with the operation of functional composition, the set of all permutations of S constitutes a group, which is called the *symmetric group* on S.

Subgroups of a symmetric group are called *permutation groups.* For more information on permutation groups, see, e.g., Dixon and Mortimer [27].

It is worth stressing here that we always and consistently compose mappings, in particular, permutations, from right to left. Thus, for permutations σ and τ of S, the composition $\sigma \circ \tau$ is the permutation of S that satisfies $(\sigma \circ \tau)(i) = \sigma(\tau(i))$ for all $i \in S$. This convention may differ from some other treatments of permutations.

We will mainly discuss permutations of the set $[n]$ for some $n \in \mathbf{N}_+$; the number n is called the *degree* of such permutations. We will use both the standard one-line and cycle notations to specify permutations of $[n]$. In *one-line notation,* a word $a_1 \dots a_n \in [n]^n$ with pairwise distinct entries denotes the permutation σ of $[n]$ satisfying $\sigma(i) = a_i$ for all $i \in [n]$. In *cycle notation,* the expression $(a_1 \ \cdots \ a_r)$, where $r \geq 1$ and $a_1, \dots, a_r$ are pairwise distinct elements of $[n]$, denotes the permutation σ satisfying $\sigma(a_i) = a_{i+1}$ whenever $1 \leq i \leq r-1$, $\sigma(a_r) = a_1$, and $\sigma(m) = m$ whenever $m \in [n] \setminus \{a_1, \dots, a_r\}$; such a permutation is called a *cycle*, and the number r is its *length.* Every permutation is a product of disjoint cycles. For example, consider the permutation σ of $\{1, \dots, 7\}$ given by the following table.

i	1	2	3	4	5	6	7
$\sigma(i)$	5	1	7	4	2	6	3

The representation of σ in one-line notation is 5174263 and one possible representation of σ in cycle notation is $(1\ 5\ 2)(3\ 7)$. We denote the identity permutation on any underlying set by id.

The symmetric group and the alternating group on $[n]$ are denoted by S_n and A_n, respectively. For a subset $X \subseteq [n]$, we use the symbol S_X to designate the subgroup of S_n comprising all those permutations which fix all elements of $[n] \setminus X$. Similarly, $A_X := S_X \cap A_n$.

For permutation groups G and G', we write $G \leq G'$ to mean that G is a subgroup of G'. For a set P of permutations on $[n]$, the symbol $\langle P \rangle$ stands for the subgroup of S_n generated by P. If $P_1, \dots, P_t$ are sets of permutations, then we write $\langle P_1, \dots, P_t \rangle$ for $\langle \bigcup_{i=1}^{t} P_i \rangle$.

Definition 1.6.1. If $\Pi = \{X_1, \dots, X_t\}$ is a collection of pairwise disjoint subsets of $[n]$, then $\langle S_{X_1}, \dots, S_{X_t} \rangle = S_{X_1} \cdots S_{X_t}$, i.e., the subgroup of S_n generated by the subgroups $S_{X_1}, \dots, S_{X_t}$ is equal to the product

$$S_{X_1} \cdots S_{X_t} = \{\sigma_1 \circ \cdots \circ \sigma_t : \sigma_1 \in S_{X_1}, \dots, \sigma_t \in S_{X_t}\}.$$

We will denote this subgroup by S_Π. Furthermore, we write $A_\Pi := S_\Pi \cap A_n$. We will be using this notation mostly in cases when Π is a partition of $[n]$.

Fact 1.6.2. Let Π and Γ be partitions of $[n]$. Then $S_\Pi \leq S_\Gamma$ if and only if Π is a refinement of Γ.

We recall here some well-known facts about generators of permutation groups (see, e.g., Dixon and Mortimer [27], Lang [51]), and we will be using these facts in the sequel without explicit mention.

Fact 1.6.3.

(i) If $1 < p < r \leq n$, then
- $(1\ 2\ \cdots\ p)(p\ \ p+1\ \cdots\ r) = (1\ 2\ \cdots\ r)$,
- $(1\ \cdots\ r)(2\ \cdots\ r)^{-1} = (1\ 2)$.

(ii) Examples of generating sets of the symmetric group S_n include
- $\{(1\ 2\ \cdots\ n), (1\ 2)\}$,
- $\{(2\ 3\ \cdots\ n), (1\ 2)\}$,
- $\{(1\ 2\ \cdots\ n), (2\ 3\ \cdots\ n)\}$,
- the set of all adjacent transpositions $(i\ \ i+1)$, $1 \leq i \leq n-1$,
- A_n and any odd permutation.

(iii) Examples of generating sets of the alternating group A_n include
- $\{(1\ 2\ 3), (1\ 2\ \cdots\ n)\}$, if n is odd and $n \geq 3$,
- $\{(1\ 2\ 3), (2\ 3\ \cdots\ n)\}$, if n is even and $n \geq 4$,
- the set of all cycles $(i\ \ \ i+1\ \ \ i+2)$, where i is odd and $1 \leq i \leq n-2$, if n is odd and $n \geq 3$,
- $A_S \cup A_T$, where $S, T \subseteq [n]$ with $|S|, |T| \geq 3$, $S \cup T = [n]$, and $S \cap T \neq \emptyset$.

1.7 ORDERED PARTITIONS

An *ordered partition* is a partition with a linear order of the blocks. For a partition Π of $[n]$, the *standard order* $\leq_\Pi$ is the one in which blocks are ordered by their minima, i.e., for $B, B' \in \Pi$, we have $B \leq_\Pi B'$ if and only if $\min B \leq \min B'$ (where min and $\leq$ refer to the natural order of integers). The blocks of Π can, of course, be ordered in other ways. For example, for any permutation $\sigma \in S_n$, we arrange the blocks in the order in which σ first "encounters" them. More precisely, for $B, B' \in \Pi$, we set $B \leq^\sigma_\Pi B'$ if and only if $\min \sigma^{-1}(B) \leq \min \sigma^{-1}(B')$. (Using this notation, $\leq^{\mathrm{id}}_\Pi$ is just the standard order.) In fact, every ordered partition of $[n]$ arises in this way: for a particular ordering $B_1 \leq' B_2 \leq' \cdots \leq' B_m$ of the blocks of Π, we can define a permutation $\pi = \pi_1\pi_2 \ldots \pi_n \in S_n$ so that the first $|B_1|$ entries are the elements of the block B_1 in some order, which are then followed by the elements of B_2 in some order, and so on. It is obvious that $\leq^\pi_\Pi$ coincides with $\leq'$.

Remark 1.7.1. The shorthand introduced in Remark 1.4.1 can be used for ordered partitions in the obvious way: we just write the blocks

in the desired order. For example, the string 6|245|9|1378 represents the partition $\{\{1,3,7,8\},\{2,4,5\},\{6\},\{9\}\}$ of $[9]$ with the linear order $\{6\} \leq \{2,4,5\} \leq \{9\} \leq \{1,3,7,8\}$ of the blocks.

Definition 1.7.2. Let $\Pi \in \mathrm{Part}_m(n)$. Let $\mathrm{nat}_\Pi \colon [n] \to \Pi$ be the natural surjection that maps each element of $[n]$ to its Π-block. For $\sigma \in S_n$, let $h_\Pi^\sigma \colon [m] \to \Pi$ be the order-isomorphism $([m];\leq) \to (\Pi;\leq_\Pi^\sigma)$. We denote h_Π^{id} simply by h_Π. Define the map $\delta_\Pi \colon [n] \to [m]$ as $\delta_\Pi = (h_\Pi)^{-1} \circ \mathrm{nat}_\Pi$. Note that δ_Π is surjective. Define $\sigma_\Pi \colon [m] \to [m]$ as $\sigma_\Pi := (h_\Pi^{\mathrm{id}})^{-1} \circ h_\Pi^\sigma$. Note that σ_Π is a permutation, because it is a composition of order-isomorphisms.

Remark 1.7.3. Prömel and Voigt [76] called a surjection $\varphi \colon [n] \to [m]$ *rigid* if $\min \varphi^{-1}(i) < \min \varphi^{-1}(j)$ whenever $i < j$. For any partition $\Pi \in \mathrm{Part}_m(n)$, the map δ_Π is the unique rigid surjection $[n] \to [m]$ with kernel Π.

Remark 1.7.4. If $\Pi = \{B_1, \ldots, B_m\}$ with $B_1 \leq_\Pi B_2 \leq_\Pi \cdots \leq_\Pi B_m$, then $\delta_\Pi(i) = j$ if and only if $i/\Pi = B_j$.

Remark 1.7.5. If $I \in \binom{[n]}{2}$ and $\Pi \in \mathrm{Part}_{n-1}(n)$ is the partition whose only nontrivial block is I, then we write δ_I for δ_Π (see Remark 1.4.6). In this case, we can easily write down an explicit formula for δ_I as

$$\delta_I(i) = \begin{cases} i, & \text{if } i < \max I \text{ and } i \notin I, \\ \min I, & \text{if } i \in I, \\ i-1, & \text{if } i > \max I. \end{cases}$$

Let $\Pi \in \mathrm{Part}_m(n)$. The coarsenings of Π are in a one-to-one correspondence with the partitions of the partition Π. Namely, to each coarsening Γ of Π we may associate the partition $\Pi/\Gamma := \{\{B \in \Pi : B \subseteq C\} : C \in \Gamma\}$ of Π, whose blocks are, for each block $C \in \Gamma$, the set of Π-blocks contained in C. Conversely, to each partition Φ of Π we may associate the *flattening* $\Phi^\flat := \{\bigcup \mathcal{B} : \mathcal{B} \in \Phi\}$ of Φ, which is easily seen to be a coarsening of Π. Moreover, it holds that $(\Pi/\Gamma)^\flat = \Gamma$ and $\Pi/\Phi^\flat = \Phi$. Using the mappings of Definition 1.7.2, we can translate partitions of Π into partitions of $[m]$, and in this way every partition of $[m]$ gives rise to a coarsening of Π. This is formalized in the following lemma.

Lemma 1.7.6. *Let $\Pi \in \mathrm{Part}_m(n)$, $\Gamma \in \mathrm{Part}_\ell(n)$ and $\Phi \in \mathrm{Part}_\ell(m)$ with $\ell \leq m \leq n$. Assume that $\Pi \sqsubseteq \Gamma$. Then the following statements hold.*

(i) *Let $\Pi_\Phi := \{\bigcup_{i \in P} h_\Pi(i) : P \in \Phi\}$. Then $\Pi_\Phi \in \mathrm{Part}_\ell(n)$ and $\Pi \sqsubseteq \Pi_\Phi$.*

(ii) $\delta_\Pi(\Gamma) \in \mathrm{Part}_\ell(m)$.

(iii) $\delta_\Pi(\Pi_\Phi) = \Phi$.

(iv) $\Pi_{\delta_\Pi(\Gamma)} = \Gamma$.

Proof. (i) The elements of Π_Φ are unions of Π-blocks, and they are pairwise disjoint. Moreover, their union is $[n]$, because for every $x \in [n]$ we have $x \in \mathrm{nat}_\Pi(x) = h_\Pi(h_\Pi^{-1}(\mathrm{nat}_\Pi(x))) = h_\Pi(\delta_\Pi(x))$, so $x \in \bigcup_{i \in P} h_\Pi(i)$ for $P = \delta_\Pi(x)/\Phi$. Therefore, Π_Φ is a partition of $[n]$ with $|\Phi| = \ell$ blocks.

(ii) The set $\delta_\Pi(\Gamma) = \{\delta_\Pi(C) : C \in \Gamma\} = \{\{\delta_\Pi(i) : i \in C\} : C \in \Gamma\}$ is a set of subsets of $[m]$. The sets $\delta_\Pi(C)$ ($C \in \Gamma$) are pairwise disjoint. For, if $C, C' \in \Gamma$ and $\delta_\Pi(C) \cap \delta_\Pi(C') \neq \emptyset$, then there exist $i \in C$, $j \in C'$ such that $\delta_\Pi(i) = \delta_\Pi(j)$. Then $\mathrm{nat}_\Pi(i) = h_\Pi(\delta_\Pi(i)) = h_\Pi(\delta_\Pi(j)) = \mathrm{nat}_\Pi(j)$, so $i \equiv_\Pi j$. Since $\Pi \sqsubseteq \Gamma$, this implies $i \equiv_\Gamma j$; hence $C = i/\Gamma = j/\Gamma = C'$.

Furthermore, every element of $[m]$ is contained in some $\delta_\Pi(C)$. For, if $x \in [m]$, then let B be the unique Γ-block that contains $h_\Pi(x)$. Then $x \in \{\delta_\Pi(i) : i \in h_\Pi(x)\} \subseteq \{\delta_\Pi(i) : i \in B\} = \delta_\Pi(B)$.

We conclude that $\delta_\Pi(\Gamma)$ is a partition of $[m]$ with $|\Gamma| = \ell$ blocks.

(iii) Observe first that for any $i \in [m]$, it holds that $\mathrm{nat}_\Pi(x) = h_\Pi(i)$ for every $x \in h_\Pi(i)$. Consequently,

$$\delta_\Pi(h_\Pi(i)) = \{\delta_\Pi(x) : x \in h_\Pi(i)\} = \{h_\Pi^{-1}(\mathrm{nat}_\Pi(x)) : x \in h_\Pi(i)\} = \{i\}.$$

It follows that for any $P \in \Phi$,

$$\delta_\Pi(\bigcup_{i \in P} h_\Pi(i)) = \bigcup_{i \in P} \delta_\Pi(h_\Pi(i)) = \bigcup_{i \in P} \{i\} = P.$$

Thus, if $B \in \Phi$, then $B = \delta_\Pi(\bigcup_{i \in B} h_\Pi(i)) \in \delta_\Pi(\Pi_\Phi)$. Conversely, if $B \in \delta_\Pi(\Pi_\Phi)$, then $B = \bigcup_{i \in P} h_\Pi(i)$ for some $P \in \Phi$, and by the above observations we have $B = P \in \Phi$.

(iv) We prove first the claim that $C = \bigcup_{i \in \delta_\Pi(C)} h_\Pi(i)$ for any $C \in \Gamma$. For, if $x \in C$, then $\delta_\Pi(x) \in \delta_\Pi(C)$ and we have

$$x \in \mathrm{nat}_\Pi(x) = h_\Pi(h_\Pi^{-1}(\mathrm{nat}_\Pi(x))) = h_\Pi(\delta_\Pi(x)) \subseteq \bigcup_{i \in \delta_\Pi(C)} h_\Pi(i).$$

If $x \in \bigcup_{i \in \delta_\Pi(C)} h_\Pi(i)$, then there exists $j \in \delta_\Pi(C)$ such that $x \in h_\Pi(j)$, and hence there exists $y \in C$ such that $j = \delta_\Pi(y) = h_\Pi^{-1}(\mathrm{nat}_\Pi(y))$. Then

$$x \in h_\Pi(h_\Pi^{-1}(\mathrm{nat}_\Pi(y))) = \mathrm{nat}_\Pi(y) = y/\Pi \subseteq y/\Gamma = C,$$

where the subset inclusion holds because $\Pi \sqsubseteq \Gamma$.

Using the above claim, we now prove the equality $\Pi_{\delta_\Pi(\Gamma)} = \Gamma$. If $C \in \Gamma$, then $\delta_\Pi(C) \in \delta_\Pi(\Gamma)$, and we have $C = \bigcup_{i \in \delta_\Pi(C)} h_\Pi(i) \in \Pi_{\delta_\Pi(\Gamma)}$. Conversely, if $C \in \Pi_{\delta_\Pi(\Gamma)}$, then $C = \bigcup_{i \in P} h_\Pi(i)$ for some $P \in \delta_\Pi(\Gamma)$. Then $P = \delta_\Pi(B)$ for some $B \in \Gamma$, and we have $C = \bigcup_{i \in \delta_\Pi(B)} h_\Pi(i) = B \in \Gamma$. □

We establish a few technical lemmas and identities involving the maps δ_Π, σ_Π and h^σ_Π that will be used in the later chapters. Statement (ii) of Lemma 1.7.7 makes explicit the fact that the composition of rigid surjections is a rigid surjection (see Prömel and Voigt [76, p. 164]).

Lemma 1.7.7. *Let $\sigma, \pi \in S_n$ and $\Pi, \Gamma \in \mathrm{Part}(n)$, and assume that $\Pi \sqsubseteq \Gamma$. Then the following statements hold.*

(i) *For any Γ-blocks C and C', it holds that $C \leq^\pi_\Gamma C'$ if and only if $\delta_\Pi(C) \leq^{\pi_\Pi}_{\delta_\Pi(\Gamma)} \delta_\Pi(C')$. Consequently, the lifted map δ'_Π restricted to Γ is an order-isomorphism $(\Gamma; \leq^\pi_\Gamma) \to (\delta_\Pi(\Gamma); \leq^{\pi_\Pi}_{\delta_\Pi(\Gamma)})$. In other words, $h^{\pi_\Pi}_{\delta_\Pi(\Gamma)} \circ (h^\pi_\Gamma)^{-1} = \delta'_\Pi|_\Gamma$. (Note that the definition of $\delta'_\Pi|_\Gamma$ is independent of π.)*

(ii) $\delta_\Gamma = \delta_{\delta_\Pi(\Gamma)} \delta_\Pi$.

(iii) $\sigma_\Gamma = (\sigma_\Pi)_{\delta_\Pi(\Gamma)}$.

Proof. (i) Assume that $\Pi = \{B_1, \dots, B_m\}$ and $\Gamma = \{C_1, \dots, C_\ell\}$ with

$$B_1 \leq^{\mathrm{id}}_\Pi B_2 \leq^{\mathrm{id}}_\Pi \cdots \leq^{\mathrm{id}}_\Pi B_m, \qquad C_1 \leq^{\mathrm{id}}_\Gamma C_2 \leq^{\mathrm{id}}_\Gamma \cdots \leq^{\mathrm{id}}_\Gamma C_\ell.$$

Since $\Pi \sqsubseteq \Gamma$, every block $C \in \Gamma$ is a union of Π-blocks, namely

$$\begin{aligned} C &= \bigcup_{C \supseteq B \in \Pi} B = \bigcup_{x \in C} \mathrm{nat}_\Pi(x) = \bigcup \mathrm{nat}_\Pi(C) = \bigcup h_\Pi \circ h_\Pi^{-1} \circ \mathrm{nat}_\Pi(C) \\ &= \bigcup h_\Pi \circ \delta_\Pi(C) = \bigcup_{i \in \delta_\Pi(C)} h_\Pi(i) = \bigcup_{i \in \delta_\Pi(C)} B_i. \end{aligned}$$

Now, let $C, C' \in \Gamma$. The condition $C \leq^\pi_\Gamma C'$ is, by definition, equivalent to $\min \pi^{-1}(C) \leq \min \pi^{-1}(C')$, which can be equivalently rewritten as

$$\begin{aligned} \min_{i \in \delta_\Pi(C)} \min \pi^{-1}(B_i) &= \min \pi^{-1}\Big(\bigcup_{i \in \delta_\Pi(C)} B_i \Big) \\ &\leq \min \pi^{-1}\Big(\bigcup_{j \in \delta_\Pi(C')} B_j \Big) = \min_{j \in \delta_\Pi(C')} \min \pi^{-1}(B_j). \end{aligned}$$

This is equivalent to the condition

$$\exists p \in \delta_\Pi(C)\, \forall q \in \delta_\Pi(C') \colon \min \pi^{-1}(B_p) \leq \min \pi^{-1}(B_q). \tag{1.7.1}$$

By the definition of $\leq^\pi_\Pi$, the condition $\min \pi^{-1}(B_p) \leq \min \pi^{-1}(B_q)$ is equivalent to $B_p \leq^\pi_\Pi B_q$, which in turn is equivalent to $(h^\pi_\Pi)^{-1}(B_p) \leq (h^\pi_\Pi)^{-1}(B_q)$. Since $(h^\pi_\Pi)^{-1}(B_p) = (h^\pi_\Pi)^{-1} \circ h^{\mathrm{id}}_\Pi(p) = (\pi_\Pi)^{-1}(p)$ and, similarly, $(h^\pi_\Pi)^{-1}(B_q) = (\pi_\Pi)^{-1}(q)$, condition (1.7.1) is equivalent to

$$\exists p \in \delta_\Pi(C)\, \forall q \in \delta_\Pi(C') \colon (\pi_\Pi)^{-1}(p) \leq (\pi_\Pi)^{-1}(q),$$

that is, $\min(\pi_\Pi)^{-1}(\delta_\Pi(C)) \leq \min(\pi_\Pi)^{-1}(\delta_\Pi(C'))$, which in turn is equivalent to $\delta_\Pi(C) \leq^{\pi_\Pi}_{\delta_\Pi(\Gamma)} \delta_\Pi(C')$.

The last statement holds, because $h^{\pi_\Pi}_{\delta_\Pi(\Gamma)} \circ (h^\pi_\Gamma)^{-1}$ is the unique order-isomorphism $(\Gamma; \leq^\pi_\Gamma) \to (\delta_\Pi(\Gamma); \leq^{\pi_\Pi}_{\delta_\Pi(\Gamma)})$ by the definition of h^π_Γ and $h^{\pi_\Pi}_{\delta_\Pi(\Gamma)}$.

(ii) Since $\Pi \sqsubseteq \Gamma$, we have $i/\Pi \subseteq i/\Gamma$ for any $i \in [n]$, so $\delta_\Pi(i) \in \delta_\Pi(i/\Pi) \subseteq \delta_\Pi(i/\Gamma) \in \delta_\Pi(\Gamma)$. This implies that $\mathrm{nat}_{\delta_\Pi(\Gamma)}(\delta_\Pi(i)) = \delta_\Pi(i)/\delta_\Pi(\Gamma) = \delta_\Pi(i/\Gamma)$. Therefore,

$$(\delta'_\Pi|_\Gamma)^{-1}(\mathrm{nat}_{\delta_\Pi(\Gamma)}(\delta_\Pi(i))) = (\delta'_\Pi|_\Gamma)^{-1}(\delta_\Pi(i/\Gamma)) = i/\Gamma = \mathrm{nat}_\Gamma(i).$$

We conclude that $(\delta'_\Pi|_\Gamma)^{-1} \circ \mathrm{nat}_{\delta_\Pi(\Gamma)} \circ \delta_\Pi = \mathrm{nat}_\Gamma$. Consequently,

$$\begin{aligned}\delta_\Gamma &= (h^{\mathrm{id}}_\Gamma)^{-1} \circ \mathrm{nat}_\Gamma = (h^{\mathrm{id}}_\Gamma)^{-1} \circ (\delta'_\Pi|_\Gamma)^{-1} \circ \mathrm{nat}_{\delta_\Pi(\Gamma)} \circ \delta_\Pi \\ &= (h^{\mathrm{id}}_\Gamma)^{-1} \circ h^{\mathrm{id}}_\Gamma \circ (h^{\mathrm{id}}_{\delta_\Pi(\Gamma)})^{-1} \circ \mathrm{nat}_{\delta_\Pi(\Gamma)} \circ \delta_\Pi \\ &= (h^{\mathrm{id}}_{\delta_\Pi(\Gamma)})^{-1} \circ \mathrm{nat}_{\delta_\Pi(\Gamma)} \circ \delta_\Pi = \delta_{\delta_\Pi(\Gamma)}\delta_\Pi.\end{aligned}$$

(iii) By part (i) we have $h^{\sigma_\Pi}_{\delta_\Pi(\Gamma)} \circ (h^\sigma_\Gamma)^{-1} = \delta'_\Pi|_\Gamma = h^{\mathrm{id}_\Pi}_{\delta_\Pi(\Gamma)} \circ (h^{\mathrm{id}}_\Gamma)^{-1}$. Note that $\mathrm{id}_\Pi = \mathrm{id}$. Therefore,

$$\begin{aligned}(\sigma_\Pi)_{\delta_\Pi(\Gamma)} &= (h^{\mathrm{id}}_{\delta_\Pi(\Gamma)})^{-1} \circ h^{\sigma_\Pi}_{\delta_\Pi(\Gamma)} = (h^{\mathrm{id}}_{\delta_\Pi(\Gamma)})^{-1} \circ h^{\sigma_\Pi}_{\delta_\Pi(\Gamma)} \circ (h^\sigma_\Gamma)^{-1} \circ h^\sigma_\Gamma \\ &= (h^{\mathrm{id}}_{\delta_\Pi(\Gamma)})^{-1} \circ h^{\mathrm{id}}_{\delta_\Pi(\Gamma)} \circ (h^{\mathrm{id}}_\Gamma)^{-1} \circ h^\sigma_\Gamma = (h^{\mathrm{id}}_\Gamma)^{-1} \circ h^\sigma_\Gamma \\ &= \sigma_\Gamma.\end{aligned}$$

□

Lemma 1.7.8. *Let $\Pi \in \mathrm{Part}_m(n)$ and $\Phi \in \mathrm{Part}_\ell(m)$ with $\ell \leq m \leq n$. Let $\sigma \in S_n$. Then $(\sigma_\Pi)_\Phi = \sigma_{\Pi_\Phi}$.*

Proof. We have $\Phi = \delta_\Pi(\Pi_\Phi)$ and $\Pi \sqsubseteq \Pi_\Phi$ by Lemma 1.7.6. Then Lemma 1.7.7(iii) yields $(\sigma_\Pi)_\Phi = (\sigma_\Pi)_{\delta_\Pi(\Pi_\Phi)} = \sigma_{\Pi_\Phi}$. □

Lemma 1.7.9. *Let $\sigma, \pi \in S_n$, and let $\Pi \in \mathrm{Part}_m(n)$.*

(i) *Let B and B' be Π-blocks. Then $B \leq^\sigma_\Pi B'$ if and only if $\pi(B) \leq^{\pi\circ\sigma}_{\pi(\Pi)} \pi(B')$.*

(ii) *The lifted map π' restricted to Π is an order-isomorphism $(\Pi; \leq^\sigma_\Pi) \to (\pi(\Pi); \leq^{\pi\circ\sigma}_{\pi(\Pi)})$. In other words, $h^{\pi\circ\sigma}_{\pi(\Pi)} \circ (h^\sigma_\Pi)^{-1} = \pi'|_\Pi$.*

(iii) $(h^{\mathrm{id}}_\Pi)^{-1} \circ h^\sigma_\Pi = (h^\pi_{\pi(\Pi)})^{-1} \circ h^{\pi\circ\sigma}_{\pi(\Pi)}$.

Proof. (i) Since $\sigma^{-1} = \sigma^{-1} \circ \pi^{-1} \circ \pi = (\pi \circ \sigma)^{-1} \circ \pi$, we have $\sigma^{-1}(B) = (\pi \circ \sigma)^{-1}(\pi(B))$. Therefore

$$\begin{aligned}B \leq^\sigma_\Pi B' &\iff \min \sigma^{-1}(B) \leq \min \sigma^{-1}(B') \\ &\iff \min(\pi \circ \sigma)^{-1}(\pi(B)) \leq \min(\pi \circ \sigma)^{-1}(\pi(B')) \\ &\iff \pi(B) \leq^{\pi\circ\sigma}_{\pi(\Pi)} \pi(B').\end{aligned}$$

(ii) Part (i) shows that $\pi'|_\Pi$ is an order-isomorphism $(\Pi; \leq^\sigma_\Pi) \to (\pi(\Pi); \leq^{\pi\circ\sigma}_{\pi(\Pi)})$. Therefore $h^{\pi\circ\sigma}_{\pi(\Pi)} \circ (h^\sigma_\Pi)^{-1} = \pi'|_\Pi$.

(iii) By part (ii), $h^{\pi\circ\sigma}_{\pi(\Pi)} \circ (h^\sigma_\Pi)^{-1} = \pi'|_\Pi = h^\pi_{\pi(\Pi)} \circ (h^{\mathrm{id}}_\Pi)^{-1}$. The claimed equality follows by composing each side from the left by $(h^\pi_{\pi(\Pi)})^{-1}$ and from the right by h^σ_Π. □

Corollary 1.7.10. *Let* $I, J \in \binom{[n]}{2}$ *with* $I \neq J$. *Let* $\Pi = \langle I, J \rangle_{\text{part}}$. *Then* $\delta_\Pi = \delta_{\delta_I(J)} \circ \delta_I = \delta_{\delta_J(I)} \circ \delta_J$.

Proof. Recall that we use the shorthand I for the partition whose only nontrivial block is I (see Remark 1.4.6). The partitions I and J are refinements of $\langle I, J \rangle_{\text{part}}$, and consequently $\delta_\Pi = \delta_{\delta_I(\Pi)} \circ \delta_I$ by Lemma 1.7.7(ii).

We claim that $\delta_I(\Pi) = \delta_I(J)$. For, if $I \cap J = \emptyset$, then the only nontrivial Π-blocks are I and J. Since $\delta_I(I) = \{\min I\}$ is trivial, we see that $\delta_I(\Pi) = \delta_I(J)$. On the other hand, if $I \cap J \neq \emptyset$, then the only nontrivial Π-block is $I \cup J$. Then $\delta_I(I \cup J) = \delta_I(J)$, and we have $\delta_I(\Pi) = \delta_I(J)$ also in this case.

We conclude that $\delta_\Pi = \delta_{\delta_I(\Pi)} \circ \delta_I = \delta_{\delta_I(J)} \circ \delta_I$. In the same manner we can show that $\delta_\Pi = \delta_{\delta_J(I)} \circ \delta_J$. □

1.8 GALOIS CONNECTIONS

Let $(X; \leq)$ and $(Y; \leq)$ be partially ordered sets. A map $\varphi\colon X \to Y$ is

- *monotone* if $x \leq y$ implies $\varphi(x) \leq \varphi(y)$ for all $x, y \in X$,
- *antitone* if $x \leq y$ implies $\varphi(x) \geq \varphi(y)$ for all $x, y \in X$.

A map $\varphi\colon X \to X$ is

- *extensive* if $x \leq \varphi(x)$ for all $x \in X$,
- *intensive* if $\varphi(x) \leq x$ for all $x \in X$,
- *idempotent* if $\varphi(\varphi(x)) = \varphi(x)$ for all $x \in X$.

A monotone, extensive and idempotent map $\varphi\colon X \to X$ is called a *closure operator* on X. A monotone, intensive and idempotent map $\varphi\colon X \to X$ is called a *kernel operator* on X. If φ is a closure operator (kernel operator, resp.), then $\varphi(x)$ is called the *closure* (*kernel*,[1] resp.) of x, and elements of the form $\varphi(x)$ are called *closed elements* (*kernels*, resp.).

An (*antitone*) *Galois connection* between partially ordered sets X and Y is a pair (φ, ψ) of maps $\varphi\colon X \to Y$, $\psi\colon Y \to X$ with the property that $x \leq \psi(y)$ if and only if $y \leq \varphi(x)$ for all $x \in X$ and $y \in Y$. The maps φ and ψ are called *polarities*. Such maps φ and ψ are antitone, and their compositions $\psi \circ \varphi$ and $\varphi \circ \psi$ are closure operators on X and Y, respectively. The closed elements are said to be *Galois closed* with respect to (φ, ψ).

A *monotone Galois connection* between partially ordered sets X and Y is a pair (φ, ψ) of maps $\varphi\colon X \to Y$, $\psi\colon Y \to X$ with the property that $x \leq \psi(y)$ if and only if $\varphi(x) \leq y$ for all $x \in X$ and $y \in Y$. The map φ is called a *lower adjoint* of ψ, and ψ is called an *upper adjoint* of φ. The maps φ and ψ are monotone, the composition $\psi \circ \varphi$ is a closure operator on X, and the composition $\varphi \circ \psi$ is a kernel operator on Y. A monotone Galois connection between X and Y is just an antitone Galois connection between X and the dual poset of Y; hence

1 This is not to be confused with the kernel defined in Section 1.5.

all statements concerning antitone Galois connections can be easily translated into statements about monotone Galois connections and vice versa.

A Galois connection between power set lattices $(\mathcal{P}(A);\subseteq)$ and $(\mathcal{P}(B);\subseteq)$ is referred to simply as a Galois connection between sets A and B. It is well known that every binary relation $R \subseteq A \times B$ induces an antitone Galois connection between A and B via the maps $\varphi\colon \mathcal{P}(A) \to \mathcal{P}(B)$ and $\psi\colon \mathcal{P}(B) \to \mathcal{P}(A)$ given by

$$\varphi(S) := \{b \in B \mid \forall a \in S\colon (a,b) \in R\},$$
$$\psi(T) := \{a \in A \mid \forall b \in T\colon (a,b) \in R\},$$

for $S \subseteq A$, $T \subseteq B$. Thus, the Galois closed elements are the sets $S \in \mathcal{P}(A)$, $T \in \mathcal{P}(B)$ satisfying $S = \psi(\varphi(S))$ and $T = \varphi(\psi(T))$. Equivalently, $S \in \mathcal{P}(A)$ is closed if $S = \psi(T)$ for some $T \in \mathcal{P}(B)$, and $T \in \mathcal{P}(B)$ is closed if $T = \varphi(S)$ for some $S \in \mathcal{P}(A)$. The sets of closed elements of $\mathcal{P}(A)$ and those of $\mathcal{P}(B)$ form dually isomorphic complete lattices.

For further information on Galois connections, see, e.g., [25].

1.9 MULTISETS

A *multiset* M over a set X is a couple $(X, \mathbf{1}_M)$, where $\mathbf{1}_M\colon X \to \mathbf{N}$ is a map called a *multiplicity function.* The number $\mathbf{1}_M(x)$ is called the *multiplicity* of x in M. If $\mathbf{1}_M(x) \neq 0$, then x is called an *element* of M. We will only consider *finite* multisets, i.e., multisets M for which the set $\{x \in X : \mathbf{1}_M(x) > 0\}$ is finite. In this case the sum $\sum_{x\in X} \mathbf{1}_M(x)$ is a well-defined natural number, and it is called the *cardinality* of M and denoted by $|M|$. The set of all finite multisets over X is denoted by $\mathcal{M}(X)$.

We may specify a finite multiset by listing its elements between angle brackets so that the number of occurrences of each element in the list equals its multiplicity (the order of listing the elements does not matter). For example, $\langle 1,1,1,2,3,3\rangle$ is the multiset $(X, \mathbf{1}_M)$ satisfying $\mathbf{1}_M(1) = 3$, $\mathbf{1}_M(2) = 1$, $\mathbf{1}_M(3) = 2$, and $\mathbf{1}_M(x) = 0$ for all $x \in X \setminus \{1,2,3\}$. We will use the shorthand a^m for m occurrences of a. Thus, we can describe the above multiset equivalently as $\langle 1^3, 2, 3^2\rangle$.

If $(a_i)_{i\in I}$ is an indexed family of elements of X, then we will write $\langle a_i : i \in I\rangle$ to denote the multiset over X in which the multiplicity of each $x \in X$ equals $|\{i \in I : a_i = x\}|$.

Let M and M' be finite multisets over X. The *multiset sum* $M \uplus M'$, the *difference* $M \setminus M'$, and the *intersection* $M \cap M'$ are defined by the multiplicity functions

$$\mathbf{1}_{M\uplus M'}(x) = \mathbf{1}_M(x) + \mathbf{1}_{M'}(x),$$
$$\mathbf{1}_{M\setminus M'}(x) = \max(\mathbf{1}_M(x) - \mathbf{1}_{M'}(x), 0),$$
$$\mathbf{1}_{M\cap M'}(x) = \min(\mathbf{1}_M(x), \mathbf{1}_{M'}(x)).$$

2

MINORS OF FUNCTIONS

New functions can be built from a given function $f\colon A^n \to B$ by manipulating its arguments. We may permute arguments, introduce or delete inessential arguments, or identify arguments. The functions that can be formed in this way are called minors of f. We will make this idea precise below in Definition 2.2.2.

We start by recalling some basic terminology concerning functions of several arguments in Section 2.1. Then we establish several basic properties of the minor relation in Section 2.2. Many of them are folklore or intuitively clear. However, one can hardly find rigorous justifications of these properties in the literature. For this reason, at the risk of sounding pedantic or prolix, we would like to provide detailed proofs here.

In the remainder of this chapter (Sections 2.3–2.8), we will discuss minors of functions from different points of view and we survey the author's past and recent contributions to this field. This sets the general scene for the second main theme of this thesis, namely, reconstruction problems of functions. A reader more interested in reconstruction problems may safely skip these sections and jump to Chapter 3, as there are no important concepts introduced or developed in these sections that the later chapters build upon.

2.1 FUNCTIONS OF SEVERAL ARGUMENTS

Let A and B be nonempty sets. A *function* (*of several arguments*) from A to B is a mapping $f\colon A^n \to B$, where n is a positive integer called the *arity* of f. If $A = B$, then we speak of *operations* on A. Operations on $\{0,1\}$ are called *Boolean functions,* and functions from $\{0,1\}$ to an arbitrary nonempty set B are called *pseudo-Boolean functions.*

We use the symbols $\mathcal{F}_{AB}^{(n)}$ and $\mathcal{O}_A^{(n)}$ to designate the set of all n-ary functions from A to B and the set of all n-ary operations on A, respectively, i.e., $\mathcal{F}_{AB}^{(n)} := B^{A^n}$ and $\mathcal{O}_A^{(n)} := A^{A^n}$, and we set $\mathcal{F}_{AB} := \bigcup_{n\geq 1} B^{A^n}$ and $\mathcal{O}_A := \bigcup_{n\geq 1} A^{A^n}$. For any set $\mathcal{C} \subseteq \mathcal{F}_{AB}$ of functions, the *n-ary part* of $\mathcal{C}$ is $\mathcal{C}^{(n)} := \mathcal{C} \cap \mathcal{F}_{AB}^{(n)}$.

For the development of the theory, it is sometimes easier to work – as Willard [87] did – with tuples $\mathbf{a} \in A^V$ and functions $f\colon A^V \to B$, where A and B are nonempty sets and V is an arbitrary finite nonempty set. In fact, $A^n = A^{[n]}$, and as we will see in Lemma 2.2.10, it does not make any significant difference whether we consider functions $f\colon A^V \to B$ or functions $f\colon A^n \to B$.

Let $f\colon A^n \to B$. For $i \in [n]$, the i-th argument of f is *essential*, or f *depends* on its i-th argument, if there exist tuples $\mathbf{a}, \mathbf{b} \in A^n$ such that $\mathbf{a}$ and $\mathbf{b}$ coincide in all components except the i-th one and $f(\mathbf{a}) \neq f(\mathbf{b})$. In this case, we say that the tuples $\mathbf{a}$ and $\mathbf{b}$ *witness the essentiality* of the i-th argument of f. Arguments that are not essential are *inessential* (or *fictitious*). Denote by $\operatorname{Ess} f$ the set of indices of essential arguments of f, that is,

$$\operatorname{Ess} f := \{i \in [n] \mid \text{the } i\text{-th argument of } f \text{ is essential}\}.$$

The number $|\operatorname{Ess} f|$ of essential arguments of f is called the *essential arity* of f and is denoted by $\operatorname{ess} f$.

We occasionally discuss *partial functions* (*of several arguments*) from A to B, that is, mappings $f\colon C \to B$, where $C \subseteq A^n$ for some $n \in \mathbf{N}_+$. If $C = A^n$, then we are dealing with functions of several arguments as defined above, and as a way of emphasizing this special case, we may speak of *total functions.*

Many of the definitions we formulate for total functions can be used as such or with little obvious modifications in the more general setting of partial functions. For example, in order to define essential arguments of partial functions, we must require that the tuples witnessing the essentiality of an argument of a partial function belong to the domain of that function. Thus, the i-th argument of a partial function $f\colon C \to B$, where $C \subseteq A^n$, is *essential* if there exist tuples $\mathbf{a}, \mathbf{b} \in C$ such that $\mathbf{a}$ and $\mathbf{b}$ coincide in all components except the i-th one and $f(\mathbf{a}) \neq f(\mathbf{b})$.

2.2 MINORS

According to the formal definition, a tuple $\mathbf{a} \in A^V$ is a map $\mathbf{a}\colon V \to A$. Hence we may compose tuples with other maps. In particular, if $\sigma\colon W \to V$, then the composite map $\mathbf{a} \circ \sigma\colon W \to A$ is a tuple in A^W, more precisely, $\mathbf{a} \circ \sigma = (a_{\sigma(i)})_{i \in W}$. In this context, we often simplify the notation and write $\mathbf{a}\sigma$ instead of $\mathbf{a} \circ \sigma$.

Any map $\sigma\colon W \to V$ induces a map $\underline{\sigma}\colon A^V \to A^W$ by the rule $\underline{\sigma}(\mathbf{a}) = \mathbf{a}\sigma$ for all $\mathbf{a} \in A^n$. The following fact will be applied frequently without explicit mention.

Fact 2.2.1. For any $\sigma\colon V \to W$ and $\tau\colon U \to V$, it holds that $\underline{\sigma \circ \tau} = \underline{\tau} \circ \underline{\sigma}$.

Definition 2.2.2. A function $f\colon A^V \to B$ is a *minor* of a function $g\colon A^W \to B$ if there exists a map $\sigma\colon W \to V$ such that $f = g \circ \underline{\sigma}$, i.e., $f(\mathbf{a}) = g(\mathbf{a}\sigma)$ for all $\mathbf{a} \in A^V$. We shall write $f \leq g$ to designate the fact that f is a minor of g.

Remark 2.2.3. Minors of functions have been studied by several authors, and they appear in the literature under different names, such as

- "polymers" (Rosenberg, Szendrei [78]),
- "identification minors" (Ekin, Foldes, Hammer, Hellerstein [28]),
- "$\mathcal{I}$-minors", where $\mathcal{I}$ stands for the set containing just the identity function (Pippenger [72]),
- "subfunctions" (Zverovich [88]),
- "functions obtained by simple variable substitution" (Couceiro, Foldes [11]),
- "$\mathcal{J}$-subfunctions", where $\mathcal{J}$ stands for the clone of projections (the current author [53]),
- "$\mathcal{P}_A$-minors", where $\mathcal{P}_A$ stands for the clone of projections (Szendrei and the current author [64]), and
- "simple minors" (Couceiro and the current author [13]).

We now present with proofs basic properties of the minor relation. It is clearly reflexive and transitive, because $f = f \circ \underline{\mathrm{id}}$ for any function f and the condition $f = g \circ \underline{\sigma}$ and $g = h \circ \underline{\tau}$ implies $f = h \circ \underline{\tau} \circ \underline{\sigma} = h \circ (\underline{\sigma \circ \tau})$. In other words, the minor relation $\leq$ is a quasiorder on $\mathcal{F}_{AB}$, and, as for all quasiorders, it induces an equivalence relation on $\mathcal{F}_{AB}$ by the following rule: $f \equiv g$ if and only if $f \leq g$ and $g \leq f$. We say that f and g are *equivalent* if $f \equiv g$. Furthermore, $\leq$ induces a partial order on the quotient $\mathcal{F}_{AB}/\equiv$ by the rule $f/\equiv \leq g/\equiv$ if and only if $f \leq g$. If $f \leq g$ and $f \not\equiv g$, then we say that f is a *proper minor* of g, and we write $f < g$.

Lemma 2.2.4. *Let $f\colon A^V \to B$, $g\colon A^W \to B$, $\sigma\colon W \to V$, and assume that $f = g \circ \underline{\sigma}$. Then the following statements hold.*

(i) *If $\tau\colon W \to V$ is a map that coincides with σ on $\operatorname{Ess} g$, i.e., $\sigma|_{\operatorname{Ess} g} = \tau|_{\operatorname{Ess} g}$, then $f = g \circ \underline{\tau}$.*

(ii) $\operatorname{Ess} f \subseteq \operatorname{Im} \sigma$.

(iii) *For every $i \in \operatorname{Ess} f$, we have $\sigma^{-1}(i) \cap \operatorname{Ess} g \neq \emptyset$.*

(iv) $\operatorname{ess} f \leq \operatorname{ess} g$.

(v) *If $\operatorname{ess} f = \operatorname{ess} g$, then the restricted map $\sigma|_{\operatorname{Ess} g}\colon \operatorname{Ess} g \to \operatorname{Ess} f$ is a bijection.*

(vi) *$f \equiv g$ if and only if $\operatorname{ess} f = \operatorname{ess} g$.*

(vii) *If σ is injective, then $f \equiv g$.*

Proof. (i) Since the tuples $\mathbf{a}\sigma$ and $\mathbf{a}\tau$ coincide at every position $i \in \operatorname{Ess} g$, for any $\mathbf{a} \in A^V$, for any $\mathbf{a} \in A^V$, we have $g(\mathbf{a}\sigma) = g(\mathbf{a}\tau)$. Consequently, $f(\mathbf{a}) = (g \circ \underline{\sigma})(\mathbf{a}) = g(\mathbf{a}\sigma) = g(\mathbf{a}\tau) = (g \circ \underline{\tau})(\mathbf{a})$.

(ii) We will prove the equivalent reverse inclusion of complements, i.e., $V \setminus \operatorname{Im} \sigma \subseteq V \setminus \operatorname{Ess} f$. Let $i \in V \setminus \operatorname{Im} \sigma$. Then, for any $\mathbf{a}, \mathbf{b} \in A^V$ such that $a_j = b_j$ for all $j \in V \setminus \{i\}$, it holds that $\mathbf{a}\sigma = \mathbf{b}\sigma$, and

so $f(\mathbf{a}) = g(\mathbf{a}\sigma) = g(\mathbf{b}\sigma) = f(\mathbf{b})$. Therefore, the i-th argument is inessential in f, that is, $i \in V \setminus \operatorname{Ess} f$.

(iii) Let $i \in \operatorname{Ess} f$, and assume that $\sigma^{-1}(i) = \{\ell_1, \dots, \ell_r\}$ with the ℓ_j's pairwise distinct. (Note that $\sigma^{-1}(i) \neq \emptyset$ by part (ii).) Let $\mathbf{a}, \mathbf{b} \in A^V$ be tuples that witness the essentiality of the i-th argument in f, and define the sequence $\mathbf{c}^0, \dots, \mathbf{c}^r \in A^W$ as follows: $\mathbf{c}^0 := \mathbf{a}\sigma$, and for $j = 1, \dots, r$, let $\mathbf{c}^j$ be the tuple obtained from $\mathbf{c}^{j-1}$ by changing the ℓ_j-th entry from a_i to b_i. By construction, it holds that $\mathbf{c}^r = \mathbf{b}\sigma$. Since $g(\mathbf{a}\sigma) = f(\mathbf{a}) \neq f(\mathbf{b}) = g(\mathbf{b}\sigma)$, there exists an index $k \in \{1, \dots, r\}$ such that $g(\mathbf{c}^k) \neq g(\mathbf{c}^{k+1})$. But this means that the tuples $\mathbf{c}^k$ and $\mathbf{c}^{k+1}$ witness the essentiality of the ℓ_k-th argument in g. Thus $\ell_k \in \operatorname{Ess} g$, so $\sigma^{-1}(i) \cap \operatorname{Ess} g \neq \emptyset$.

(iv) Parts (ii) and (iii) assert that each element of $\operatorname{Ess} f$ has at least one preimage under σ in the set $\operatorname{Ess} g$. Since preimages of distinct elements are distinct, this implies that $|\operatorname{Ess} f| \leq |\operatorname{Ess} g|$, that is, $\operatorname{ess} f \leq \operatorname{ess} g$.

(v) Continuing the argument of part (iv), in the case when $\operatorname{ess} f = \operatorname{ess} g$, i.e., $|\operatorname{Ess} f| = |\operatorname{Ess} g|$, we see that each element of $\operatorname{Ess} f$ has exactly one preimage under σ in $\operatorname{Ess} g$. We conclude that $\sigma|_{\operatorname{Ess} g} \colon \operatorname{Ess} g \to \operatorname{Ess} f$ is a bijection.

(vi) The fact that $f \equiv g$ implies $\operatorname{ess} f = \operatorname{ess} g$ is an immediate consequence of part (iv). Assume then that $\operatorname{ess} f = \operatorname{ess} g$. Part (v) implies that $\sigma|_{\operatorname{Ess} g} \colon \operatorname{Ess} g \to \operatorname{Ess} f$ is a bijection. Let $\tau \colon V \to W$ be an arbitrary extension of $(\sigma|_{\operatorname{Ess} g})^{-1}$. Then, for all $i \in \operatorname{Ess} g$, we have $(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \sigma^{-1}(\sigma(i)) = i$, so $g \circ (\underline{\tau \circ \sigma}) = g \circ \underline{\mathrm{id}_W} = g$ by Part (i). Consequently, $f \circ \underline{\tau} = g \circ \underline{\sigma} \circ \underline{\tau} = g \circ (\underline{\tau \circ \sigma}) = g$, that is, $g \leq f$. We conclude that $f \equiv g$.

(vii) Since σ in injective, it has a left inverse, i.e., there is a map $\tau \colon V \to W$ such that $\tau \circ \sigma = \mathrm{id}_W$. Then $g = g \circ \underline{\mathrm{id}_W} = g \circ \underline{\sigma} \circ \underline{\tau} = f \circ \underline{\tau}$. Hence $g \leq f$, and we conclude that $f \equiv g$. □

Definition 2.2.5. Let $f, g \colon A^V \to B$. We say that f and g are *similar,* and we write $f \simeq g$, if there exists a bijection $\sigma \colon V \to V$ such that $f = g \circ \underline{\sigma}$.

The similarity relation $\simeq$ is an equivalence relation on B^{A^V}. Reflexivity and transitivity are obvious, because $f = f \circ \underline{\mathrm{id}_V}$ for any f, and $f = g \circ \underline{\sigma}$ and $g = h \circ \underline{\tau}$ with bijective $\sigma, \tau \colon V \to V$ imply $f = h \circ \underline{\tau} \circ \underline{\sigma} = h \circ (\underline{\sigma \circ \tau})$ and $\sigma \circ \tau$ is bijective. As for symmetry, the condition $f = g \circ \underline{\sigma}$ with a bijective $\sigma \colon V \to V$ implies $f \circ \underline{\sigma^{-1}} = g \circ \underline{\sigma} \circ \underline{\sigma^{-1}} = g \circ (\underline{\sigma^{-1} \circ \sigma}) = g \circ \underline{\mathrm{id}_V} = g$ and σ^{-1} is bijective, so $g \simeq f$.

Lemma 2.2.6. *Let $f \colon A^V \to B$ and $g \colon A^W \to B$. Then $f \simeq g$ if and only if $V = W$ and $f \equiv g$.*

Proof. If $f \simeq g$, then $V = W$ and $f = g \circ \underline{\sigma}$ for some bijective $\sigma \colon V \to V$, i.e., $f \leq g$. By the symmetry of $\simeq$, we also obtain $g \leq f$. Hence $f \equiv g$.

If $V = W$ and $f \equiv g$, then there exists $\sigma\colon V \to V$ such that $f = g \circ \underline{\sigma}$. Lemma 2.2.4, parts (v) and (vi), asserts that $\sigma|_{\operatorname{Ess} g}\colon \operatorname{Ess} g \to \operatorname{Ess} f$ is a bijection. Let $\tau\colon V \to V$ be any bijective extension of $\sigma|_{\operatorname{Ess} g}$. We have $f = g \circ \underline{\tau}$ by Lemma 2.2.4(i), and we conclude that $f \simeq g$. □

Lemma 2.2.7. *Let $f\colon A^V \to B$, and assume that $\operatorname{ess} f = m$. Then there exists $h \in \mathcal{F}_{AB}^{(\max(m,1))}$ such that $\operatorname{ess} h = m$ and $f \equiv h$. Moreover, the function h is unique up to similarity.*

Proof. Consider first the case when $m = 0$. This means that f is a constant function, i.e., there exists $c \in A$ such that $f(\mathbf{a}) = c$ for all $\mathbf{a} \in A^V$. Define $h\colon A^1 \to B$, $h(a) = c$ for all $a \in A$. Then clearly $\operatorname{ess} h = 0$. Moreover, it is easy to verify that $f = h \circ \underline{\sigma}$ and $h = f \circ \underline{\tau}$ for arbitrary maps $\sigma\colon [1] \to V$ and $\tau\colon V \to [1]$, so $f \equiv h$.

Assume then that $m \geq 1$. Let $\varphi\colon [m] \to \operatorname{Ess} f$ be an arbitrary bijection, let $\sigma\colon [m] \to V$, $\sigma(i) = \varphi(i)$ for all $i \in [m]$, and let $\tau\colon V \to [m]$ be an arbitrary extension of φ^{-1}. Define $h\colon A^m \to B$, $h = f \circ \underline{\tau}$.

Observe that $\sigma \circ \tau\colon V \to V$ satisfies, for all $i \in \operatorname{Ess} f$,

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \varphi(\varphi^{-1}(i)) = i.$$

Therefore, Lemma 2.2.4(i) implies $f \circ (\underline{\sigma \circ \tau}) = f \circ (\underline{\mathrm{id}_V}) = f$. Consequently, $h \circ \underline{\sigma} = f \circ \underline{\tau} \circ \underline{\sigma} = f \circ (\underline{\sigma \circ \tau}) = f$, so $f \leq h$. We also have $h \leq f$ by definition, so $f \equiv h$.

Concerning the last statement, note that if $h' \in \mathcal{F}_{AB}^{(\max(m,1))}$ is a function with $f \equiv h'$, then $h \equiv h'$ holds by the properties of equivalence relations, and hence $h \simeq h'$ by Lemma 2.2.6. □

Lemma 2.2.8. *Let $f\colon A^V \to B$ and $g\colon A^W \to B$, and assume that $f \leq g$. Then $f \equiv g \circ \underline{\mathrm{nat}_\Pi}$ for some partition Π of W.*

Proof. We have $f = g \circ \underline{\sigma}$ for some $\sigma\colon W \to V$. The map σ can be written as the composition of a surjective and an injective map, namely $\sigma = q_\sigma \circ \mathrm{nat}_\Pi$, where $\Pi := \ker \sigma$, $\mathrm{nat}_\Pi\colon W \to \Pi$ is the natural surjection $i \mapsto i/\Pi$, and $q_\sigma\colon \Pi \to V$ is the injective map given by $i/\Pi \mapsto \sigma(i)$. Thus $f = g \circ \underline{\sigma} = g \circ \underline{\mathrm{nat}_\Pi} \circ \underline{q_\sigma}$. Since q_σ is injective, Lemma 2.2.4(vii) gives that $f \equiv g \circ \underline{\mathrm{nat}_\Pi}$. □

Even though we have developed the theory of minors for functions $f\colon A^V \to B$ with an arbitrary index set V of arguments, it is more customary to state results in terms of functions of the form $f\colon A^n \to B$ where $n \in \mathbf{N}_+$. According to Lemma 2.2.8, every minor of $f\colon A^n \to B$ is equivalent to a function of the form $f \circ \underline{\mathrm{nat}_\Pi}$ for some partition $\Pi \in \operatorname{Part}(n)$. Note, however, that the domain of $f \circ \underline{\mathrm{nat}_\Pi}$ is A^Π and not A^m for some integer m, so this construction brings us out of the realm of "customary" functions. This minor inconvenience can be easily remedied by renaming the blocks of Π via a bijection between Π and $[m]$, where m is the number of blocks of Π. For this purpose, we will use a standard renaming scheme, which we have already seen in Definition 1.7.2: the blocks of Π are linearly ordered by their minima.

Definition 2.2.9. Given numbers $n, m \in \mathbf{N}_+$ with $m \leq n$, a function $f\colon A^n \to B$, and a partition $\Pi \in \mathrm{Part}_m(n)$, define the function $f_\Pi\colon A^m \to B$ as $f_\Pi = f \circ \underline{\delta_\Pi}$. (Recall from Definition 1.7.2 the rigid surjection $\delta_\Pi := (h_\Pi)^{-1} \circ \mathrm{nat}_\Pi$.)

Informally speaking, f_Π is the minor of f that is obtained by identifying the arguments belonging to the same block of Π. An important particular case is obtained with partitions with $n-1$ blocks when $n \geq 2$. Namely, for $I \in \binom{[n]}{2}$, define $f_I\colon A^{n-1} \to B$ as $f_I = f \circ \underline{\delta_I}$ (see Remark 1.7.5 for a spelt-out expression for δ_I). In explicit terms, if $I = \{i, j\}$ with $i < j$ and $\mathbf{a} = (a_1, \ldots, a_{n-1}) \in A^{n-1}$, then $\mathbf{a}\delta_I = (a_1, \ldots, a_{j-1}, a_i, a_j, \ldots, a_{n-1})$; hence

$$f_I(a_1, \ldots, a_{n-1}) = f(a_1, \ldots, a_{j-1}, a_i, a_j, \ldots, a_{n-1}),$$

for all $(a_1, \ldots, a_{n-1}) \in A^{n-1}$. Note that a_i occurs twice on the right side of the above equality: both at the i-th and at the j-th position. We will refer to the function f_I as an *identification minor* of f.

Lemma 2.2.10. *Every minor of $f\colon A^n \to B$ is equivalent to a minor of the form f_Π for some partition $\Pi \in \mathrm{Part}(n)$.*

Proof. If g is a minor of $f\colon A^n \to B$, then $g \equiv f \circ \underline{\mathrm{nat}_\Pi}$ for some partition $\Pi \in \mathrm{Part}(n)$ by Lemma 2.2.8. Then $f_\Pi = f \circ \underline{\mathrm{nat}_\Pi} \circ \underline{(h_\Pi)^{-1}} \leq f \circ \underline{\mathrm{nat}_\Pi} \equiv g$. Since $(h_\Pi)^{-1}$ is bijective, Lemma 2.2.4(vii) implies $f_\Pi \equiv g$. □

Lemma 2.2.11. *Let $\Pi, \Gamma \in \mathrm{Part}(n)$, and let $f\colon A^n \to B$. If $\Pi \sqsubseteq \Gamma$, then $f_\Gamma \leq f_\Pi$.*

Proof. We have $\delta_\Gamma = \delta_{\delta_\Pi(\Gamma)}\delta_\Pi$ by Lemma 1.7.7(ii). Thus,

$$f_\Gamma = f \circ \underline{\delta_\Gamma} = f \circ \underline{(\delta_{\delta_\Pi(\Gamma)}\delta_\Pi)} = f \circ \underline{\delta_\Pi} \circ \underline{\delta_{\delta_\Pi(\Gamma)}} = f_\Pi \circ \underline{\delta_{\delta_\Pi(\Gamma)}},$$

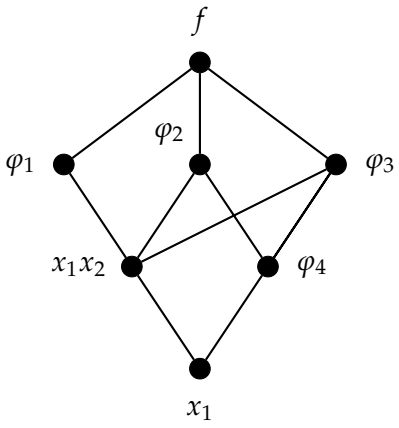
so $f_\Gamma \leq f_\Pi$. □

The "elementary" identification minors f_I ($I \in \binom{[n]}{2}$) are perhaps the most relevant among the minors of f of the form f_Π, because, in view of Lemma 1.7.7(ii), we can obtain f_Π, for any partition Π, by successively identifying just a single pair of arguments at a time. Note also that Corollary 1.7.10 implies the following.

Fact 2.2.12. For any $I, J \in \binom{[n]}{2}$, $(f_I)_{\delta_I(J)} = (f_J)_{\delta_J(I)} = f_\Pi$, where $\Pi = \langle I, J \rangle_{\mathrm{part}}$.

Example 2.2.13. Let $f\colon \{0,1\}^4 \to \{0,1\}$ be the function induced by the polynomial $x_1 + x_1x_2 + x_3x_4$ over the two-element field $\mathrm{GF}(2)$. The minors f_Π of f, for each partition Π of $[4]$ are enumerated in Table 1. The table also displays the Hasse diagram of the principal down-set $\downarrow(f/\equiv)$ in the minor poset $(\mathcal{O}_{\{0,1\}}/\equiv; \leq)$ of Boolean functions. The nodes are labeled with representatives of $\equiv$-classes.

Π	f_Π
$1\|2\|3\|4$	$x_1 + x_1x_2 + x_3x_4$
$12\|3\|4$	x_1x_2
$13\|2\|4$	$x_1 + x_1x_2 + x_1x_3$
$14\|2\|3$	$x_1 + x_1x_2 + x_1x_3$
$1\|23\|4$	$x_1 + x_1x_2 + x_2x_3$
$1\|24\|3$	$x_1 + x_1x_2 + x_2x_3$
$1\|2\|34$	$x_1 + x_1x_2 + x_3$
$123\|4$	x_1x_2
$124\|3$	x_1x_2
$134\|2$	x_1x_2
$1\|234$	$x_1 + x_1x_2 + x_2$
$12\|34$	x_1
$13\|24$	x_1
$14\|23$	x_1
1234	x_1



$$\varphi_1 = x_1 + x_1x_2 + x_1x_3$$
$$\varphi_2 = x_1 + x_1x_2 + x_2x_3$$
$$\varphi_3 = x_1 + x_1x_2 + x_3$$
$$\varphi_4 = x_1 + x_1x_2 + x_2$$

Table 1: Minors of $f = x_1 + x_1x_2 + x_3x_4$.

2.3 ON THE STRUCTURE OF THE MINOR ORDER OF FUNCTIONS

Several studies have aimed at describing the structure of the minor partial order. We highlight some interesting facts in this section.

Lemma 2.2.4 asserts that if $f < g$ then $\operatorname{ess} f < \operatorname{ess} g$. Since essential arities are nonnegative integers, it follows immediately that the minor order $(\mathcal{F}_{AB}/\equiv; \leq)$ has no infinite descending chains. Moreover, the minimal elements of the minor order are exactly the (equivalence classes of) unary functions.

The *diagonal* of $f\colon A^n \to B$ is the map $\operatorname{diag} f\colon A \to B$ given by $\operatorname{diag} f(x) = f(x, \ldots, x)$. It follows immediately from definition that $\operatorname{diag} f \leq f$. In fact, $\operatorname{diag} f$ is the unique unary minor of f. For, let $u \in \mathcal{F}_{AB}^{(1)}$, and assume that $u \leq f$. By the definition of minors, there exists a map $\sigma\colon [n] \to [1]$ such that $u = f \circ \underline{\sigma}$, i.e., $u(a_1) = f(a_{\sigma(1)}, \ldots, a_{\sigma(n)}) = f(a_1, \ldots, a_1) = \operatorname{diag} f(a_1)$; hence $u = \operatorname{diag} f$. Couceiro and Pouzet [23] observed that the poset $(\mathcal{F}_{AB}/\equiv; \leq)$ is disconnected, and two functions belong to the same connected component if and only if they have the same diagonal.

Proposition 2.3.1. *The set $\mathcal{U} := \{\uparrow u : u \in \mathcal{F}_{AB}^{(1)}\}$ of the principal up-sets of unary functions is a partition of $\mathcal{F}_{AB}$. Consequently, any two functions from distinct blocks of $\mathcal{U}$ are incomparable.*

Proof. Since $\operatorname{diag} f \leq f$, we have $f \in \uparrow \operatorname{diag} f$ for any $f \in \mathcal{F}_{AB}$. Hence $\bigcup \mathcal{U} = \mathcal{F}_{AB}$. Now let $u, v \in \mathcal{F}_{AB}^{(1)}$, and assume that $\uparrow u \cap \uparrow v \neq \emptyset$. Then there exists $f \in \uparrow u \cap \uparrow v$, and we have $u \leq f$ and $v \leq f$. Since every

function has a unique unary minor, it follows that $u = v$. Consequently, the up-sets $\uparrow f$ in $\mathcal{U}$ are pairwise disjoint. We conclude that $\mathcal{U}$ is a partition of $\mathcal{F}_{AB}$, as claimed. It follows immediately that if $f \in \uparrow u$, $g \in \uparrow v$ for some $u, v \in \mathcal{F}_{AB}^{(1)}$, and $f \leq g$, then $u = v$. □

It is evident from Example 2.2.13 and from Proposition 2.3.1 that the minor poset is not a lattice. Nevertheless, its connected components are directed posets (posets in which every pair of elements have a lower bound and an upper bound – not necessarily a greatest lower bound and a least upper bound). Namely, by Proposition 2.3.1, two functions have a lower bound if and only if they have the same diagonal, and in this case the diagonal is obviously a lower bound. It was shown by Couceiro and the current author that two functions belonging to the same connected component also have an upper bound.

Proposition 2.3.2 (Couceiro, Lehtonen [16, Proposition 4.2])**.** *Assume that $f\colon A^m \to B$ and $g\colon A^n \to B$ are functions satisfying* $\operatorname{diag} f = \operatorname{diag} g$. *Then there exists a function $h\colon A^{m+n-1} \to B$ such that f and g are minors of h.*

Since every minor of $f\colon A^n \to B$ is equivalent to a minor of the form f_Π, for some partition $\Pi \in \operatorname{Part}(n)$ (see Lemma 2.2.10), the number of minors of f, up to equivalence, is at most the number of partitions of the n-element set (the so-called Bell number B_n). Consequently, the principal down-sets of $(\mathcal{F}_{AB}/{\equiv}; \leq)$ are all finite. In fact, we can say even more about this.

Definition 2.3.3. Let $\mathcal{K}$ be a class of posets. A poset P is *universal* in $\mathcal{K}$ if $P \in \mathcal{K}$ and every poset in $\mathcal{K}$ can be embedded in P.

The following result was first established in the special case of Boolean functions by Couceiro and Pouzet [23, Theorem 3], and it was later generalized to functions with arbitrary finite domains and codomains by Szendrei and the current author [67, Theorem 3.1].

Proposition 2.3.4. *If A and B are finite sets such that $|B| \geq \min(3, |A|)$, then the poset $(\mathcal{F}_{AB}/{\equiv}; \leq)$ is universal in the class of countable posets whose principal down-sets are finite.*

Bouaziz, Couceiro, and Pouzet showed in [7, Theorem 8] that, in the case when $|A| = 2$, all lower covers of $f\colon A^n \to B$ have the same essential arity. This property is very particular to functions defined on a two-element domain, and it is not in general satisfied when $|A| \geq 3$. Examples of functions with lower covers of different essential arities were presented by Couceiro, Waldhauser, and the current author in [22, Example 3.2] and by Couceiro and the current author in [16, Example 5.4].

Concerning the possible essential arities of the upper covers of $f\colon A^n \to B$, we have the following characterization.

Proposition 2.3.5 (Couceiro, Lehtonen [16, Theorem 5.2])**.** *Assume that $f\colon A^n \to B$ is a function that depends on all of its arguments. Let $\ell \in \mathbf{N}_+$.*

(i) *If $\ell \geq \max(|A|, 3)$, then f does not have upper covers of essential arity $n + \ell$.*

(ii) *If $1 \leq \ell < |A|$, then there exists an upper cover of f of essential arity $n + \ell$.*

(iii) *If $|A| = 2$, then f has an upper cover of essential arity $n + 2$ if and only if f is determined by* oddsupp.

In the statement of Proposition 2.3.5, we made use of the following notions, which will be used many times later on.

Definition 2.3.6. Let $\phi\colon A^+ \to X$ be a mapping. A function $f\colon A^n \to B$ is *determined by ϕ* if there exists a map $f^*\colon X \to B$ such that $f = f^* \circ \phi|_{A^n}$.

Definition 2.3.7 (Berman, Kisielewicz [4])**.** Let $\operatorname{supp}\colon \bigcup_{n\geq 1} A^n \to \mathcal{P}(A)$ and $\operatorname{oddsupp}\colon \bigcup_{n\geq 1} A^n \to \mathcal{P}(A)$ be the mappings given by the rules

$$\begin{aligned} \operatorname{supp}(a_1, \ldots, a_n) &:= \{a_1, \ldots, a_n\}, \\ \operatorname{oddsupp}(a_1, \ldots, a_n) &:= \{a \in A : |\{j \in [n] : a_j = a\}| \text{ is odd}\}. \end{aligned}$$

In other words, for any $\mathbf{a} \in A^n$, we have $\operatorname{supp}(\mathbf{a}) = \operatorname{Im} \mathbf{a}$.

2.4 ARITY GAP

Let $f\colon A^n \to B$, and assume that $\operatorname{ess} f \geq 2$. The *arity gap* of f, denoted by $\operatorname{gap} f$, is defined as

$$\operatorname{gap} f = \min_{g<f}(\operatorname{ess} f - \operatorname{ess} g),$$

that is, $\operatorname{gap} f$ is the minimum decrease in the number of essential arguments when proper minors are formed from f.

This notion was first studied by Salomaa [79]. He showed that the arity gap of any Boolean function with at least two essential arguments is at most 2. This result was later generalized by Willard [87].

Theorem 2.4.1 (Willard [87, Lemma 1.2, Corollary 2.3])**.** *Let A and B be arbitrary finite nonempty sets, and let $k := |A|$. Let $f\colon A^n \to B$, and assume that f depends on all of its arguments. If $n > k$, then* $\operatorname{gap} f \leq 2$. *Moreover, if $n > \max(k, 3)$, then* $\operatorname{gap} f = 2$ *if and only if f is determined by* oddsupp.

This result was further refined and the lower bound on the arity of f was removed by Couceiro and the current author in [13]. As pointed out by Couceiro, Waldhauser, and the current author in [20],

also the assumption on finiteness can be removed. In order to state the general result, we need to introduce some terminology.

For $n \geq 2$, let

$$A^n_{=} := \{(a_1, \ldots, a_n) \in A^n : a_i = a_j \text{ for some } i \neq j\}.$$

Let $f\colon A^n \to B$. Any function $g\colon A^n \to B$ satisfying $f|_{A^n_{=}} = g|_{A^n_{=}}$ is called a *support* of f. The *quasi-arity* of f, denoted $\operatorname{qa} f$, is defined as the minimum of the essential arities of all supports of f, i.e., $\operatorname{qa} f := \min_g \operatorname{ess} g$, where g ranges over all supports of f. If $\operatorname{qa} f = m$, then we say that f is *quasi-m-ary*. Note that if A is finite and $n > |A|$, then $A^n_{=} = A^n$ and hence $\operatorname{qa} f = \operatorname{ess} f$. Moreover, $\operatorname{qa} f = \operatorname{ess} f|_{A^n_{=}}$ whenever $n \neq 2$.

Theorem 2.4.2 ([13, Theorem 17], [20, Theorem 3.6])**.** *Let A and B be arbitrary sets with at least two elements. Let $f\colon A^n \to B$, $n \geq 2$, and assume that f depends on all of its arguments. Then the following statements hold.*

(i) *For $3 \leq p \leq n$,* $\operatorname{gap} f = p$ *if and only if* $\operatorname{qa} f = n - p$.

(ii) *For $n \neq 3$,* $\operatorname{gap} f = 2$ *if and only if* $\operatorname{qa} f = n - 2$ *or* $\operatorname{qa} f = n$ *and $f|_{A^n_{=}}$ is determined by* oddsupp.

(iii) *For $n = 3$,* $\operatorname{gap} f = 2$ *if and only if there exists a nonconstant unary function $h\colon A \to B$ and $i_1, i_2, i_3 \in \{0, 1\}$ such that*

$$\begin{aligned} f(x_1, x_0, x_0) &= h(x_{i_1}), \\ f(x_0, x_1, x_0) &= h(x_{i_2}), \\ f(x_0, x_0, x_1) &= h(x_{i_3}). \end{aligned}$$

(iv) *Otherwise* $\operatorname{gap} f = 1$.

Some interesting generalizations of the arity gap and refinements of Theorem 2.4.2 in special instances were discussed in [14, 19, 21, 22].

2.5 INVARIANCE GROUPS

A function $f\colon A^n \to B$ is *invariant under* a permutation $\pi \in S_n$ (or π is an *invariant* of f) if $f = f \circ \underline{\pi}$, that is, $f(\mathbf{a}) = f(\mathbf{a}\pi)$ for all $\mathbf{a} \in A^n$. The set of all permutations under which f is invariant constitutes a subgroup of S_n, and it is called the *invariance group* of f and denoted by $\operatorname{InvGr} f$.

A function $f\colon A^n \to B$ is *totally symmetric* if its invariance group equals the full symmetric group S_n. A function is 2-*set-transitive* if its invariance group is 2-set-transitive. Recall that a permutation group $G \leq S_n$ is 2-*set-transitive* if G is transitive on two-element subsets, that is, for all $p, q, r, s \in [n]$ with $p \neq q$ and $r \neq s$, there exists $\pi \in G$ such that $\{\pi(p), \pi(q)\} = \{r, s\}$ (see Beaumont, Peterson [1]).

Invariance groups of functions have been studied by many researchers, for example Clote and Kranakis [10], Kisielewicz [47], Grech and Kisielewicz [35], Horváth, Makay, Pöschel and Waldhauser [42].

2.6 UNIQUE IDENTIFICATION MINORS

It is a natural question to determine the join-irreducible elements of the minor order, i.e., the functions that have a unique lower cover in the minor poset. While a complete description of such functions is still beyond our knowledge, Bouaziz, Couceiro, and Pouzet [7, Problem 1] obtained some results in the case of Boolean functions. By viewing an arbitrary Boolean function f as a hypergraph, where the hyperedges correspond to the monomials of the unique multilinear polynomial representing f, they characterized the join-irreducible ones among those Boolean functions whose hypergraph representations are Steiner systems or graphs.

We say that a function $f\colon A^n \to B$ has a *unique identification minor* if $f_I \simeq f_J$ for all $I, J \in \binom{[n]}{2}$. This is a stronger property than join-irreducibility, and it already drew the attention of Bouaziz, Couceiro, and Pouzet when they posed the following problem, albeit in somewhat different terminology.

Problem 2.6.1 (Bouaziz, Couceiro, Pouzet [7, Problem 2(ii)])**.** Which functions have a unique identification minor?

It was known to the authors of [7] that the 2-set-transitive functions have a unique identification minor (for a proof, see, e.g., [56, Proposition 4.3]). The current author discovered in [59, 60] further examples of such functions, namely, functions that are determined by ofo or cs (see Definitions 2.3.6 and 2.6.2 and Lemma 5.2.3(i)). These known classes of functions with a unique identification minor do not subsume each other.

Definition 2.6.2. Recall the set $A^\sharp$ defined in (1.2.2). Let $\mathrm{ofo}\colon A^* \to A^\sharp$ be the mapping that sends any tuple $(a_1, \dots, a_n)$ to the tuple obtained from $(a_1, \dots, a_n)$ by removing all duplicates of elements, keeping only the first occurrence of each element occurring in the tuple. In other words, ofo maps each tuple $\mathbf{a}$ to the tuple that lists the different elements occurring in $\mathbf{a}$ in the order of first occurrence. (The name ofo is an initialism of "order of first occurrence".) A more formal definition of ofo will be given in Definition 5.1.4.

Let $\mathrm{ms}\colon A^* \to \mathcal{M}(A)$ be the map that sends each tuple to the multiset of its entries, i.e., $\mathrm{ms}(a_1, \dots, a_n) = \langle a_1, \dots, a_n \rangle$. An element $a \in A$ is called a *singleton* of $\mathbf{a} \in A^*$ if a occurs exactly once in $\mathbf{a}$. Let $\mathrm{sng}\colon A^* \to A^\sharp$ be the map that sends each tuple $\mathbf{a}$ to the tuple that lists the singletons of $\mathbf{a}$ in the order of their occurrence in $\mathbf{a}$. Let $\mathrm{cs}\colon A^* \to \mathcal{M}(A) \times A^\sharp$, $\mathrm{cs}(\mathbf{a}) = (\mathrm{ms}(\mathbf{a}), \mathrm{sng}(\mathbf{a}))$. (The name cs is an initialism of "content and singletons".)

$\mathbf{a}$	$\mathrm{ofo}(\mathbf{a})$	$\mathrm{cs}(\mathbf{a}) = (\mathrm{ms}(\mathbf{a}), \mathrm{sng}(\mathbf{a}))$
mathematician	matheicn	$(\langle \mathsf{a}^3, \mathsf{c}, \mathsf{e}, \mathsf{h}, \mathsf{i}^2, \mathsf{m}^2, \mathsf{n}, \mathsf{t}^2 \rangle, \mathsf{hecn})$
circumference	cirumfen	$(\langle \mathsf{c}^3, \mathsf{e}^2, \mathsf{f}, \mathsf{i}, \mathsf{m}, \mathsf{n}, \mathsf{r}^2, \mathsf{u} \rangle, \mathsf{iumfn})$
ambidextrously	ambidextrously	$(\langle \mathsf{a}, \mathsf{b}, \mathsf{d}, \mathsf{e}, \mathsf{i}, \mathsf{l}, \mathsf{m}, \mathsf{o}, \mathsf{r}, \mathsf{s}, \mathsf{t}, \mathsf{u}, \mathsf{x}, \mathsf{y} \rangle,$ ambidextrously$)$
unprosperousness	unprose	$(\langle \mathsf{e}^2, \mathsf{n}^2, \mathsf{o}^2, \mathsf{p}^2, \mathsf{r}^2, \mathsf{s}^4, \mathsf{u}^2 \rangle, \varepsilon)$

Table 2: Images of some strings under ofo and cs.

Example 2.6.3. In order to illustrate the mappings ofo, ms, sng and cs, let A be the set of lower-case letters of the English alphabet. Table 2 shows the images of some strings under ofo and cs.

Proposition 2.6.4 ([59, Proposition 7])**.** *Assume that $n > |A| + 1$, and let $f\colon A^n \to B$. Then the following conditions are equivalent:*

(i) *f is totally symmetric and determined by* ofo*.*

(ii) *f is 2-set-transitive and determined by* ofo*.*

(iii) *f is determined by* ofo *and for all $I, J \in \binom{[n]}{2}$, there exists a bijection $\beta\colon [n-1] \to [n-1]$ such that $\beta(\min J) = \min I$ and $f(\mathbf{a}\delta_I) = f(\mathbf{a}\beta\delta_J)$ for all $\mathbf{a} \in A^{n-1}$.*

(iv) *f is determined by* supp*.*

It is easy to devise further examples of functions $f\colon A^n \to B$ with a unique identification minor when $n \leq |A|$. In [59, Proposition 9], there was constructed a function of arity $n = |A| + 1$ that has a unique identification minor but is neither 2-set-transitive nor determined by ofo nor determined by cs (see Proposition 5.4.1).

It remains an open problem whether there exist further examples of functions with a unique identification minor when $n \geq |A| + 2$.

2.7 CLONES AND MINOR-CLOSED CLASSES OF FUNCTIONS

2.7.1 *Clones*

Composition is a fundamental operation between functions. One common way of defining composition for functions of several arguments is the following: if $f \in \mathcal{F}_{BC}^{(n)}$ and $g_1, \ldots, g_n \in \mathcal{F}_{AB}^{(m)}$, then the *composition* of f with $g_1, \ldots, g_n$ is the function $f(g_1, \ldots, g_n) \in \mathcal{F}_{AC}^{(m)}$ given by the rule

$$(f(g_1, \ldots, g_n))(\mathbf{a}) = f(g_1(\mathbf{a}), \ldots, g_n(\mathbf{a}))$$

for all $\mathbf{a} \in A^m$.

For $n \in \mathbf{N}_+$ and $i \in [n]$, the *i-th n-ary projection* is the operation $\mathrm{pr}_i^{(n)} \colon A^n \to A$ given by the rule $\mathrm{pr}_i^{(n)}(a_1, \ldots, a_n) = a_i$ for all $(a_1, \ldots, a_n) \in A^n$.

A *clone* on A is a subset $\mathcal{C} \subseteq \mathcal{O}_A$ that contains all projections and is closed under composition (i.e., if $f \in \mathcal{C}^{(n)}$ and $g_1, \ldots, g_n \in \mathcal{C}^{(m)}$ for some $n, m \in \mathbf{N}_+$ then $f(g_1, \ldots, g_n) \in \mathcal{C}$). The clones on A constitute a complete lattice, denoted by $\mathcal{L}_A$, in which the greatest element is the clone $\mathcal{O}_A$ of all operations on A and the least element is the clone of projections, denoted by $\mathcal{I}_A$.

There is a countable infinity of clones on a two-element set, and they were completely described by Emil Post [75]. Named after him, the clones on $\{0, 1\}$ are called *Post classes,* and the lattice of clones on $\{0, 1\}$ is known as *Post's lattice.* We present Post's lattice and introduce notation and nomenclature for Post classes in Appendix A. The situation is considerably different when the underlying set has at least three elements. Janov and Muchnik [44] and, independently, Hulanicki and Świerczkowski [43] showed that there are uncountably many clones on A when $|A| \geq 3$. While a complete description of the lattice of clones on A seems unfeasible when $|A| \geq 3$, clone theory has been an active field of research in the recent decades. For further information and general background on clones, we refer the reader to the books by Lau [52], Pöschel and Kalužnin [74], and Szendrei [82], and to the survey article by Kerkhoff, Pöschel and Schneider [46].

Clones can be defined in an alternative, equivalent way as subuniverses of certain algebras of operations.

Definition 2.7.1 (Mal'cev [68])**.** Define the unary operations ζ, τ, Δ, ∇ and the binary operation $*$ on the set $\mathcal{O}_A$ of all operations on A as follows. For $f \in \mathcal{O}_A^{(n)}$, $g \in \mathcal{O}_A^{(m)}$, let

$$\begin{aligned}(\zeta f)(x_1, x_2, \ldots, x_n) &:= f(x_2, x_3, \ldots, x_n, x_1),\\ (\tau f)(x_1, x_2, \ldots, x_n) &:= f(x_2, x_1, x_3, \ldots, x_n),\\ (\Delta f)(x_1, x_2, \ldots, x_{n-1}) &:= f(x_1, x_1, x_2, \ldots, x_{n-1}),\end{aligned}$$

for $n > 1$, and let $\zeta f = \tau f = \Delta f := f$ for $n = 1$; furthermore, let

$$\begin{aligned}(\nabla f)(x_1, x_2, \ldots, x_{n+1}) &:= f(x_2, \ldots, x_{n+1}),\\ (f * g)(x_1, x_2, \ldots, x_{m+n-1}) &:= f(g(x_1, x_2, \ldots, x_m), x_{m+1}, \ldots, x_{m+n-1}).\end{aligned}$$

The operations ζ and τ are collectively referred to as *permutations of variables,* Δ is called *identification of variables* (or *diagonalization*), ∇ is called *introduction of an inessential variable* (or *cylindrification*), and $*$ is called *composition.* The algebra $(\mathcal{O}_A; \zeta, \tau, \Delta, \nabla, *)$ of type $(1, 1, 1, 1, 2)$ is called the *full iterative algebra* on A, and its subalgebras are called *iterative algebras* on A.

Clones on A are exactly those universes of iterative algebras on A that contain all projections.

Clones can be characterized in terms of a Galois connection between operations and relations, which we will briefly explain here. Recall that an m-ary *relation* on A is a subset of A^m. We denote by $\mathcal{R}_A^{(m)}$ the set of all m-ary relations on A, and we denote by $\mathcal{R}_A$ the set of all finitary relations on A, i.e., $\mathcal{R}_A^{(m)} := \mathcal{P}(A^m)$ and $\mathcal{R}_A := \bigcup_{m\geq 1} \mathcal{R}_A^{(m)}$.

Let $f \in \mathcal{O}_A^{(n)}$, $\rho \in \mathcal{R}_A^{(m)}$, and let $\mathbf{M} = (a_{ij}) \in A^{m\times n}$, an m-by-n matrix over A. We write $\mathbf{M} \prec \rho$ if the columns of $\mathbf{M}$ are m-tuples belonging to the relation ρ, i.e., $(a_{1i}, a_{2i}, \dots, a_{mi}) \in \rho$ for every $i \in [n]$. We designate by $f(\mathbf{M})$ the m-tuple obtained by applying f to the rows of $\mathbf{M}$, i.e.,

$$f(\mathbf{M}) = \begin{pmatrix} f(a_{11}, a_{12}, \dots, a_{1n}) \\ f(a_{21}, a_{22}, \dots, a_{2n}) \\ \vdots \\ f(a_{m1}, a_{m2}, \dots, a_{mn}) \end{pmatrix}.$$

We say that f *preserves* ρ (or that f is a *polymorphism* of ρ, or that ρ is an *invariant* of f), and we write $f \triangleright \rho$, if for all $\mathbf{M} \in A^{m\times n}$ it holds that $\mathbf{M} \prec \rho$ implies $f(\mathbf{M}) \in \rho$.

The preservation relation induces a Galois connection between the sets $\mathcal{O}_A$ and $\mathcal{R}_A$ of operations and relations on A, wherein the polarities are $\mathrm{Pol}\colon \mathcal{P}(\mathcal{R}_A) \to \mathcal{P}(\mathcal{O}_A)$ and $\mathrm{Inv}\colon \mathcal{P}(\mathcal{O}_A) \to \mathcal{P}(\mathcal{R}_A)$ given by

$$\begin{aligned} \mathrm{Pol}\,\mathcal{R} &:= \{f \in \mathcal{O}_A \mid \forall \rho \in \mathcal{R}\colon f \triangleright \rho\}, \\ \mathrm{Inv}\,\mathcal{F} &:= \{\rho \in \mathcal{R}_A \mid \forall f \in \mathcal{F}\colon f \triangleright \rho\}, \end{aligned}$$

for $\mathcal{R} \subseteq \mathcal{R}_A$ and $\mathcal{F} \subseteq \mathcal{O}_A$.

The relevance of the preservation relation for clones is evident from the characterization of closed classes of the Galois connection Pol–Inv. (Relational clones, which are mentioned in the following theorem, are subuniverses of a certain algebra defined on the set $\mathcal{R}_A$ of all relations on A. We omit the details here.)

Theorem 2.7.2 (Geiger [33], Bodnarchuk, Kaluzhnin, Kotov, Romov [5])**.** *Let A be a finite nonempty set.*

(i) *A set $\mathcal{F} \subseteq \mathcal{O}_A$ of operations on A is of the form* $\mathrm{Pol}\,\mathcal{R}$ *for some set $\mathcal{R} \subseteq \mathcal{R}_A$ of relations on A if and only if $\mathcal{F}$ is a clone on A.*

(ii) *A set $\mathcal{R} \subseteq \mathcal{R}_A$ of relations on A is of the form* $\mathrm{Inv}\,\mathcal{F}$ *for some set $\mathcal{F} \subseteq \mathcal{O}_A$ of operations on A if and only if $\mathcal{R}$ is a relational clone on A.*

Later on, Szabó [81] and Pöschel [73] extended Theorem 2.7.2 to operations and relations on arbitrary, possibly infinite sets A. In this case, the Galois closed classes of operations are precisely the locally closed clones; the closure condition for relations is also slightly modified. Recall that a set $\mathcal{C} \subseteq \mathcal{O}_A$ of operations is *locally closed* if for every

$f \in \mathcal{O}_A$, say of arity n, $f \in \mathcal{C}$ whenever for every finite subset $S \subseteq A^n$, there exists $g \in \mathcal{C}$ such that $f|_S = g|_S$.

2.7.2 *Minor-closed classes of functions*

We say that a set $\mathcal{C} \subseteq \mathcal{F}_{AB}$ of functions is *minor-closed* if for all $f, g \in \mathcal{F}_{AB}$, the condition $g \in \mathcal{C}$ and $f \leq g$ implies $f \in \mathcal{C}$, in other words, $\mathcal{C}$ is a down-set of $(\mathcal{F}_{AB}; \leq)$. Examples of minor-closed classes include all clones, order-reversing (antitone) functions, and threshold functions.

Minor-closed classes of functions can be characterized in ways analogous to those we have discussed in Section 2.7.1. Let us consider first a modification of iterative algebras. We can define operations ζ, τ, Δ, ∇ on the set $\mathcal{F}_{AB}$ of all functions from A to B using exactly the same defining rules as in Definition 2.7.1. (We do not even attempt to define a composition operation, analogous to $*$, on $\mathcal{F}_{AB}$.) In this way, we get the algebra $(\mathcal{F}_{AB}; \zeta, \tau, \Delta, \nabla)$. It is easy to see that the minor-closed classes of functions are precisely the subuniverses of this algebra.

Let us discuss next a Galois connection, analogous to Pol–Inv, that captures the minor-closed sets of functions. As expected, the primal objects are functions in $\mathcal{F}_{AB}$, but now the dual objects are something more general than relations. An m-ary *constraint* from A to B is a pair (R, S), where R is an m-ary relation on A and S is an m-ary relation on B, i.e., $R \subseteq A^m$ and $S \subseteq B^m$. Denote by $\mathcal{K}_{AB}^{(m)}$ the set of all m-ary constraints from A to B, and let $\mathcal{K}_{AB} := \bigcup_{m \geq 1} \mathcal{K}_{AB}^{(m)}$. Let $f \in \mathcal{F}_{AB}^{(n)}$ and $(R, S) \in \mathcal{K}_{AB}^{(m)}$. We say that f *preserves* (R, S), and we write $f \triangleright (R, S)$, if for all matrices $\mathbf{M} \in A^{m \times n}$, the condition $\mathbf{M} \prec R$ implies $f(\mathbf{M}) \in S$.

The preservation relation $\triangleright$ induces a Galois connection between functions and constraints. Pippenger [72] showed that if A and B are finite sets, then the Galois closed classes of functions are precisely the minor-closed subsets of $\mathcal{F}_{AB}$. He also defined an algebra on the set $\mathcal{K}_{AB}$ of all constraints and showed that the Galois closed classes of constraints are precisely the subuniverses of this algebra. Later on, Couceiro and Foldes [11] extended Pippenger's results to functions and constraints on arbitrary, possibly infinite sets A and B. In this case, the Galois closed classes of functions are precisely the minor-closed subsets of $\mathcal{F}_{AB}$ that are locally closed; the closure condition for constraints is also slightly modified.

An equivalent characterization was presented by Couceiro and Foldes [12], who showed that minor-closed classes of functions are precisely those which are characterizable by functional equations of a certain prescribed form.

ALGEBRA	REFERENCE
$(\mathcal{O}_A; \zeta, \tau, \Delta, \nabla, *)$	
– subalgebras with projections (clones)	Geiger [33], Bodnarchuk, Kaluzhnin, Kotov, Romov [5] (finite domains), Szabó [81], Pöschel [73] (general)
– all subalgebras	Harnau [38] (finite domains), Behrisch [2] (general)
$(\mathcal{F}_{AB}; \zeta, \tau, \Delta, \nabla)$	Pippenger [72] (finite domains), Couceiro, Foldes [11] (general)
$(\mathcal{F}_{AB}; \zeta, \tau, \nabla)$	Hellerstein [40] (finite domains), Lehtonen [55] (general)
$(\mathcal{O}_A; \zeta, \tau, \nabla, *)$	
– subalgebras with projections	Lehtonen [55]
– all subalgebras	Couceiro, Lehtonen [15]

Table 3: Galois theories for reducts of iterative algebras.

2.7.3 *Reducts of iterative algebra*

The line of research discussed above in Subsections 2.7.1 and 2.7.2 suggests many possible variants of generalizations. Analogous Galois theories that describe the subalgebras of various reducts of the full iterative algebra $(\mathcal{O}_A; \zeta, \tau, \Delta, \nabla, *)$ and of the algebra $(\mathcal{F}_{AB}; \zeta, \tau, \Delta, \nabla)$ have been presented by several authors. It would be too big a digression from the main topic of this thesis to go into further details here, so we only provide references to work along these lines in Table 3.

2.8 VARIANTS OF MINORS

With the notion of functional composition at hand, we can formulate the definition of minors of functions in another, equivalent way as follows. A function $f \in \mathcal{F}_{AB}^{(n)}$ is a *minor* of $g \in \mathcal{F}_{AB}^{(m)}$ if there exist n-ary projections $\mathrm{pr}_{i_1}^{(n)}, \ldots, \mathrm{pr}_{i_m}^{(n)}$ such that $f = g(\mathrm{pr}_{i_1}^{(n)}, \ldots, \mathrm{pr}_{i_m}^{(n)})$. It is easy to see that this definition is equivalent to Definition 2.2.2: if $f = g \circ \underline{\sigma}$ for some $\sigma\colon [m] \to [n]$ then $f = g(\mathrm{pr}_{\sigma(1)}^{(n)}, \ldots, \mathrm{pr}_{\sigma(m)}^{(n)})$, and if $f = g(\mathrm{pr}_{i_1}^{(n)}, \ldots, \mathrm{pr}_{i_m}^{(n)})$ then $f = g \circ \underline{\sigma}$, where $\sigma\colon [m] \to [n]$ is given by $\sigma(j) = i_j$ for all $j \in [m]$.

Thus, f is a minor of g if f is obtained as a composition of g with projections, or, in other words, if f is a substitution instance of g, wherein projections are substituted for arguments. This definition al-

lows an immediate generalization, as we may consider substitution instances of a given function, wherein functions belonging to a certain prescribed collection of functions are substituted for arguments. Indeed, several variants of this idea have been employed in the study of functions of several arguments. For example, Harrison [39] considered two n-ary Boolean functions as equivalent if they are substitution instances of each other with respect to the general linear group $\mathrm{GL}(n, \mathbf{F}_2)$ or the affine general linear group $\mathrm{AGL}(n, \mathbf{F}_2)$. Wang [85] and Wang and Williams [86] defined a Boolean function f to be a minor of another Boolean function g if f is a substitution instance of g wherein projections, negated projections, or constants are substituted for arguments. Other variants of minors were presented in the papers by Feigelson and Hellerstein [30], Pippenger [72], and Zverovich [88].

The idea of classifying functions by their substitution instances occurs also in semigroup theory. The so-called Green's relations, introduced by Green [36], are five fundamental equivalence relations defined on a semigroup. Green's relation $\mathcal{R}$ on a transformation semigroup S relates two transformations $f, g \in S$ if and only if $f = g(h_1(x))$ and $g = f(h_2(x))$ for some $h_1, h_2 \in S \cup \{\mathrm{id}\}$. Henno [41] generalized Green's relations to Menger systems (essentially, abstract clones) and described Green's relations on the clone $\mathcal{O}_A$ of all operations on A, for every set A. In particular, he showed that two operations are $\mathcal{R}$-equivalent if and only if their ranges coincide.

All these notions are unified and generalized by the notions of $\mathcal{C}$-minor and $\mathcal{C}$-equivalence, which can be defined relative to any set $\mathcal{C}$ of operations on A. Namely, for a fixed set $\mathcal{C} \subseteq \mathcal{O}_A$, we say that a function $f \in \mathcal{F}_{AB}^{(n)}$ is a *$\mathcal{C}$-minor* of another function $g \in \mathcal{F}_{AB}^{(m)}$, and we write $f \leq_{\mathcal{C}} g$, if $f = g(h_1, \ldots, h_m)$ for some $h_1, \ldots, h_m \in \mathcal{C}^{(n)}$. If $f \leq_{\mathcal{C}} g$ and $g \leq_{\mathcal{C}} f$, then we say that f and g are *$\mathcal{C}$-equivalent*, and we write $f \equiv_{\mathcal{C}} g$. It can be shown that the $\mathcal{C}$-minor relation $\leq_{\mathcal{C}}$ is a quasiorder on $\mathcal{F}_{AB}$ if and only if $\mathcal{C}$ is a clone on A (see [53]), and in this case the $\mathcal{C}$-equivalence relation is indeed an equivalence relation and we have an induced partial order on the quotient $\mathcal{F}_{AB}/{\equiv_{\mathcal{C}}}$. Thus, for example, Green's relation $\mathcal{R}$ described by Henno is the same notion as $\mathcal{O}_A$-equivalence, and the minor relation of Definition 2.2.2 is the same notion as $\mathcal{I}_A$-minor, where $\mathcal{I}_A$ denotes the clone of projections on A.

The $\mathcal{C}$-minor and $\mathcal{C}$-equivalence relations relative to various clones $\mathcal{C}$ were investigated by the current author, partly in collaboration with Szendrei and Nešetřil, in a series of papers [53, 54, 62, 64, 65, 66, 67], and also by Szendrei [83]. Further details would go beyond the scope of this thesis, but let us nevertheless spotlight one particularly interesting theorem that is obtained when the known results are specialized to Boolean functions. In the following, the disjoint union and the lexicographic product of posets are denoted by $\cup$ and $\times_{\mathrm{lex}}$, respectively. The two-element antichain is denoted by $\overline{2}$. Universality is defined

in Definition 2.3.3. For the nomenclature on the clones of Boolean functions, see Appendix A.

Theorem 2.8.1 ([62, Theorem 19], [67, Theorem 6.1])**.** *Let $\mathcal{C}$ be a clone of Boolean functions. Then the $\mathcal{C}$-minor poset $(\mathcal{O}_A/\equiv_{\mathcal{C}}; \leq_{\mathcal{C}})$ is*

- *finite if $S_c \subseteq \mathcal{C}$;*
- *isomorphic to $(\mathbf{N}; \leq) \cup (\mathbf{N}; \leq)$, $(\mathbf{N}; \leq) \cup (\mathbf{N}; \leq) \cup (\mathbf{N}; \leq) \cup (\mathbf{N}; \leq)$ or $(\mathbf{N}; \leq) \times_{\mathrm{lex}} \overline{2}$ if $M_c \subseteq \mathcal{C} \subseteq M$;*
- *universal in the class of countable posets whose principal ideals are finite if $\mathcal{C}$ is a subclone of L, V or Λ; and*
- *universal in the class of all countable posets otherwise.*

3

RECONSTRUCTION PROBLEMS

Reconstruction problems are a very general class of problems that concern whether a mathematical object can be uniquely recovered from pieces of partial information thereon. In this thesis, we direct our attention to a reconstruction problem that involves the minor relation of functions of several arguments that was defined in Section 2.2. Is every function $f\colon A^n \to B$ uniquely determined, up to similarity, by the collection of its identification minors f_I, $I \in \binom{[n]}{2}$?

In Section 3.1, we recall some common terminology of reconstruction problems. We define the reconstruction problem of functions and identification minors in Section 3.2. We shall collect known results about this problem in the remainder of this chapter (Sections 3.3–3.5). We also briefly discuss the tools that were used to analyse different classes of functions. This often amounted to formulating and solving reconstruction problems for other kinds of mathematical objects.

3.1 DEFINITION AND EXAMPLES

The general concept of reconstruction problem was formalized in a beautiful way by Couceiro, Schölzel, and the current author in [17, Section 2.2] as follows. A *reconstruction problem* comprises the following pieces of data:

- a collection $\mathcal{O}$ of *objects*,
- an equivalence relation $\equiv$ on $\mathcal{O}$,
- for each object $O \in \mathcal{O}$, an associated natural number called the *size* of O,
- for each $n \in \mathbf{N}$, an index set I_n,
- for every object O of size n and for every $i \in I_n$, a *derived object* $O_i \in \mathcal{O}$.

Let $O \in \mathcal{O}$ be an object of size n. The equivalence classes $O_i/{\equiv}$ of the derived objects O_i ($i \in I_n$) are referred to as *cards* of O. The *deck* of O, denoted by $\operatorname{deck} O$, is the multiset $\langle O_i/{\equiv} : i \in I_n \rangle$ of the cards of O.

Let O and O' be objects of size n. We say that O' is a *reconstruction* of O, or that O and O' are *hypomorphic*, if $\operatorname{deck} O = \operatorname{deck} O'$, or, equivalently, if there exists a bijection $\varphi\colon I_n \to I_n$ such that $O_i \equiv O'_{\varphi(i)}$ for all $i \in I_n$. If the latter condition holds with φ equal to the identity map on I_n, i.e., $O_i \equiv O'_i$ for all $i \in I_n$, then we say that O and O' are *strongly hypomorphic*. An object is *reconstructible* if it is equivalent to all of its reconstructions.

Let now $\mathcal{C} \subseteq \mathcal{O}$ be a set of objects. The set $\mathcal{C}$ is *reconstructible* if all its members are reconstructible. The set $\mathcal{C}$ is *weakly reconstructible* if for all $O, O' \in \mathcal{C}$, the condition that O and O' are hypomorphic implies $O \equiv O'$. The set $\mathcal{C}$ is *recognizable* if for all $O \in \mathcal{C}$ and $O' \in \mathcal{O}$, the condition that O and O' are hypomorphic implies $O' \in \mathcal{C}$. Note that reconstructibility implies weak reconstructibility, but the converse is not true in general. If $\mathcal{C}$ is a union of $\equiv$-classes, then $\mathcal{C}$ is reconstructible if and only if it is weakly reconstructible and recognizable.

Note that the deck of an object is defined as the *multiset* of its cards. Had we instead defined the deck as the *set* of cards, we would have obtained a variant of the reconstruction problem, the so-called *set-reconstruction problem.* The *set-deck* of an object $O \in \mathcal{O}$, denoted set-deck O, is the set $\{O_i/\equiv : i \in I_n\}$ of the cards of O. An object O' is a *set-reconstruction* of O, if set-deck O = set-deck O'. An object is *set-reconstructible* is it is equivalent to all its set-reconstructions. In an analogous way, we define *set-reconstructible, weakly set-reconstructible,* and *set-recognizable* sets of objects.

Example 3.1.1. In order to illustrate the notions defined above, let us consider the *reconstruction problem of simple graphs and one-vertex-deleted subgraphs* that was mentioned in the introduction (Section 1.1). This reconstruction problem is specified by the following data. The objects are the finite simple graphs, the equivalence relation between objects is the relation of graph isomorphism, the size of a graph is the number of its vertices, and for each $n \in \mathbf{N}$, we have the index set $I_n = [n]$. Without loss of generality, we may assume that we only consider graphs with vertex set $[n]$ for some $n \in \mathbf{N}$. For a graph $G = (V, E)$ with $V = [n]$ and for any $i \in [n]$, the derived object G_i is the induced subgraph of G formed by removing vertex i.

Let us analyse the reconstructibility of small graphs. As can be easily seen, the simple graphs on two vertices, namely the complete graph K_2 and its complement $\overline{K_2}$, have the same deck, comprising two copies of the one-vertex graph, and are consequently not reconstructible and hence also not set-reconstructible. Let us move on to graphs with three vertices. There are, up to isomorphism, four different simple graphs on three vertices, namely, the complete graph K_3, the path P_3, and their complements $\overline{K_3}$ and $\overline{P_3}$ (see Table 4). For each graph G, we form the three subgraphs obtained by deleting a single vertex. The multiset of these three subgraphs is the deck of G, and the set of these subgraphs is the set-deck of G; these are presented in Table 4. As can be seen from the table, the four graphs have pairwise distinct decks. In other words, the simple graphs on three vertices are reconstructible. On the other hand, the graphs P_3 and $\overline{P_3}$ have identical set-decks, so they are not set-reconstructible. Nevertheless, the graphs K_3 and $\overline{K_3}$ are set-reconstructible.

It was conjectured by Kelly [45] and Ulam [84] that every simple graph with at least three vertices is reconstructible. The conjecture

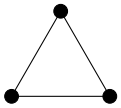
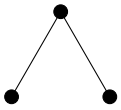
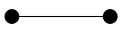
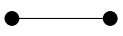
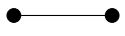
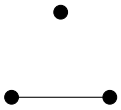
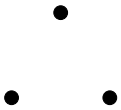
G	deck G	set-deck G
K_3 	K_2 K_2 K_2	K_2
P_3 	K_2  K_2  $\overline{K_2}$	K_2  $\overline{K_2}$
$\overline{P_3}$ 	K_2 $\overline{K_2}$ $\overline{K_2}$	K_2 $\overline{K_2}$
$\overline{K_3}$ 	$\overline{K_2}$ $\overline{K_2}$ $\overline{K_2}$	$\overline{K_2}$

Table 4: The four simple graphs on three vertices and their decks and set-decks.

has been verified by computer for graphs with at most 11 vertices (McKay [70]), and it has been proved for several infinite families of graphs, such as trees (Kelly [45]), regular graphs, disconnected graphs, and so on. Proving or disproving the conjecture in full generality remains one of the most famous open problems in graph theory.

Example 3.1.2. The reconstruction problem of graphs of Example 3.1.1 can be varied in many ways. For example, we may delete edges instead of vertices (see Harary [37] and Ellingham [29]), or we may consider directed graphs or hypergraphs instead of graphs. Directed graphs and hypergraphs are not in general reconstructible from one-vertex-deleted subgraphs: infinite nonreconstructible families of directed graphs have been described by Stockmeyer [80], and infinite nonreconstructible families of hypergraphs have been described by Kocay [49], Kocay and Lui [50], and Couceiro, Schölzel, and the present author [17]. Concerning deletion of edges, it was shown by Berge and Rado [3] that hypergraphs are not in general reconstructible from one-edge-deleted subhypergraphs.

Analogous reconstruction problems have been formulated for various other kinds of mathematical objects, such as posets (see the survey article by Rampon [77]), matrices (see Manvel and Stockmeyer [69]), integer partitions (see Monks [71]), and so on. We will see some further examples later in this chapter, as well as in Section 4.5.

3.2 RECONSTRUCTION PROBLEM OF FUNCTIONS AND IDENTIFICATION MINORS

Definition 3.2.1. The *reconstruction problem of functions of several arguments and identification minors* is specified by the following data. The set of objects is the set $\mathcal{F}_{AB}$ of functions of several arguments from A to B. The equivalence relation is the similarity relation $\simeq$ on $\mathcal{F}_{AB}$. The size of a function $f\colon A^n \to B$ is its arity n. For each $n \in \mathbf{N}_+$, the index set I_n is the set $\binom{[n]}{2}$ of all two-element subsets of $[n]$. For $f\colon A^n \to B$ and $I \in \binom{[n]}{2}$, the derived object f_I is the identification minor f_I of f as in Definition 2.2.9. Hence the cards of f are the similarity classes $f_I/\simeq$ of the identification minors of f, and the deck of f is the multiset $\langle f_I/\simeq : I \in \binom{[n]}{2}\rangle$.

Remark 3.2.2. We would like to draw the reader's attention to an important but easily overlooked detail. For functions $f, g \in \mathcal{F}_{AB}^{(n)}$, the condition $\operatorname{deck} f = \operatorname{deck} g$ does not mean, in general, that $f_I = g_I$ for all $I \in \binom{[n]}{2}$. Even if we know that the two functions have identical decks, we do not know exactly how the identification minors of f are matched with those of g. Moreover, we distinguish between functions only up to similarity (permutation of arguments). Therefore, the condition $\operatorname{deck} f = \operatorname{deck} g$ really means that there exists a bijection $\varphi\colon \binom{[n]}{2} \to \binom{[n]}{2}$ such that $f_{\varphi(I)} \simeq g_I$ for all $I \in \binom{[n]}{2}$. The condition $f_{\varphi(I)} \simeq g_I$ for all $I \in \binom{[n]}{2}$ in turn means that for every $I \in \binom{[n]}{2}$, there exists a permutation $\pi^I \in S_{n-1}$ such that $g_I = f_{\varphi(I)} \circ \underline{\pi^I}$.

For reasons that are explained in the following two remarks, we must assume that functions are of sufficiently large arity in order to have any general positive results. This is of no major concern to us. Inferring from what we have seen about the reconstruction problem of graphs and one-vertex-deleted subgraphs (Example 3.1.1), we might expect that objects of small size are not reconstructible.

Remark 3.2.3. If $n \leq |A|$, then no function $f\colon A^n \to B$ is reconstructible. In particular, functions with an infinite domain are not reconstructible. This is due to the fact that the set $A^n_{\neq}$ (see (1.2.1)) is nonempty whenever $n \leq |A|$, and the values of f at points belonging to the set $A^n_{\neq}$ are completely irrelevant to the identification minors of f. Namely, if $f, g \in \mathcal{F}_{AB}^{(n)}$ are functions that coincide on $A^n \setminus A^n_{\neq}$, i.e., $f|_{A^n \setminus A^n_{\neq}} = g|_{A^n \setminus A^n_{\neq}}$, then $f_I = g_I$ for every $I \in \binom{[n]}{2}$; thus f and g are hypomorphic. However, f and g need not be equivalent. In fact, for any $f \in \mathcal{F}_{AB}^{(n)}$, there exists $g \in \mathcal{F}_{AB}^{(n)}$ such that $f|_{A^n \setminus A^n_{\neq}} = g|_{A^n \setminus A^n_{\neq}}$ but $f \not\equiv g$; for example, let $g|_{A^n_{\neq}}$ be an arbitrary constant function if $f|_{A^n_{\neq}}$ is nonconstant, and let $g|_{A^n_{\neq}}$ be an arbitrary nonconstant function if $f|_{A^n_{\neq}}$ is constant.

Of course, in order to overcome this inconvenience, we might just modify the reconstruction problem and consider partial functions $f\colon A^n \setminus A^n_{\neq} \to B$, but we will not take this approach in this treatise.

Remark 3.2.4. As shown in [56, Example 3.13], there exist nonreconstructible functions of arity $|A|+1$ for any finite A. For example, let $k \in \mathbf{N}_+$ with $k \geq 2$, and assume that A and B are sets such that $|A| = k$ and $A \subseteq B$. Let $n := k+1$, and define $f, f'\colon A^n \to B$ as follows. Fix $\beta \in B$, and for all $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$, let

$$f(\mathbf{a}) = \begin{cases} b, & \text{if } \operatorname{supp}(\mathbf{a}) = A \text{ and } b \text{ occurs twice in } \mathbf{a}, \\ \beta, & \text{otherwise,} \end{cases}$$

$$f'(\mathbf{a}) = \begin{cases} a_1, & \text{if } \operatorname{supp}(\mathbf{a}) = A, \\ \beta, & \text{otherwise.} \end{cases}$$

Note that f is well defined, because if $\operatorname{supp}(\mathbf{a}) = A$, then there is a unique element of A that occurs twice in $\mathbf{a}$. It is clear from the definition that f is totally symmetric but f' is not; hence $f \neq f'$. It is not difficult to verify that for every $I \in \binom{[n]}{2}$, both f_I and f'_I are similar to the function $h\colon A^{n-1} \to B$ given by

$$h(a_1, \ldots, a_{n-1}) = \begin{cases} a_1, & \text{if } \operatorname{supp}(\mathbf{a}) = A, \\ \beta, & \text{otherwise.} \end{cases}$$

Consequently, $\operatorname{deck} f = \operatorname{deck} f'$. We conclude that f and f' are not reconstructible.

Having set forth the reconstruction problem of functions and identification minors and having made a few reasonable restrictions, we may begin to consider whether and to what extent functions are reconstructible. In the remainder of this chapter, we will review known results about this reconstruction problem. On the one hand, several classes of functions have been shown to be reconstructible or weakly reconstructible; the results are summarized in Table 5. On the other hand, infinite families of nonreconstructible functions have been discovered. Not only will we state the results, but we will also briefly discuss our proof techniques, especially when the analysis has led us to formulating other reconstruction problems and finding solutions to them.

In order to illustrate the notions and formalisms we have introduced above, we start with a proof of the simple, almost trivial fact that constant functions of sufficiently large arity are reconstructible.

Proposition 3.2.5 ([56, Example 3.3])**.** *If $f \in \mathcal{F}^{(n)}_{AB}$ is a constant function and $n > |A|$, then f is reconstructible.*

Proof. Since f is constant, there is $\beta \in B$ such that $f(\mathbf{a}) = \beta$ for all $\mathbf{a} \in A^n$. Then for every $I \in \binom{[n]}{2}$, we have $f_I(\mathbf{b}) = f(\mathbf{b}\delta_I) = \beta$ for

all $\mathbf{b} \in A^{n-1}$. Let $g \in \mathcal{F}_{AB}^{(n)}$ be a reconstruction of f. Then there exists a bijection $\varphi\colon \binom{[n]}{2} \to \binom{[n]}{2}$ such that $g_I \simeq f_{\varphi(I)}$ for all $I \in \binom{[n]}{2}$. Therefore, for each $I \in \binom{[n]}{2}$, there exists a permutation $\pi_I \in S_{n-1}$ such that $g_I = f_{\varphi(I)} \circ \underline{\pi_I}$. Let now $\mathbf{a} \in A^n$. Since $n > |A|$, there exist $i, j \in [n]$ such that $i \neq j$ and $a_i = a_j$. Thus $\mathbf{a} = \mathbf{b}\delta_I$ for some $\mathbf{b} \in A^{n-1}$ and $I := \{i, j\}$. Then $g(\mathbf{a}) = g(\mathbf{b}\delta_I) = g_I(\mathbf{b}) = f_{\varphi(I)}(\mathbf{b}\pi_I) = \beta$. Consequently, $g(\mathbf{a}) = \beta$ for all $\mathbf{a} \in A^n$, that is, $f = g$. We conclude that f is reconstructible. □

3.3 RECONSTRUCTIBILITY OF TOTALLY SYMMETRIC FUNCTIONS

Our first nontrivial result on the reconstruction problem is that totally symmetric functions of sufficiently large arity are reconstructible.

Proposition 3.3.1 ([56, Theorem 5.1])**.** *If $f \in \mathcal{F}_{AB}^{(n)}$ is totally symmetric and $n \geq |A| + 2$, then f is reconstructible.*

Proposition 3.3.2 ([56, Proposition 5.2])**.** *Assume that $n > \max(|A|, 3)$ and $f, g \in \mathcal{F}_{AB}^{(n)}$ are totally symmetric. If* $\operatorname{deck} f = \operatorname{deck} g$ *then $f = g$.*

The lower bounds on the arity can be slightly improved in the special case of constant functions (see Proposition 3.2.5) and of functions determined by supp or oddsupp, which are all totally symmetric.

Proposition 3.3.3 ([56, Proposition 3.8])**.** *If $f \in \mathcal{F}_{AB}^{(n)}$ is determined by* supp *and $n > |A|$, then f is reconstructible.*

Proposition 3.3.4 ([56, Proposition 3.9])**.** *If $f \in \mathcal{F}_{AB}^{(n)}$ is determined by* oddsupp *and $n > \max(|A|, 3)$, then f is reconstructible.*

Remark 3.2.4 shows that the bound $n \geq |A| + 2$ in Proposition 3.3.1 is sharp. The following example shows that in Propositions 3.3.2 and 3.3.4, the bound $n \geq 4$ is sharp when $|A| = 2$.

Example 3.3.5 ([56, Example 3.10])**.** Let $A = \{0, 1\}$, let $a, b, c, d \in B$ with $b \neq c$, and let $f, f', g, g'\colon A^3 \to B$ be as defined in Table 6. These functions are pairwise nonsimilar. Functions f and f' are totally symmetric, but h and h' not totally symmetric and not even 2-set-transitive. If $a = c$ and $b = d$ then f is determined by oddsupp. If $a = b$ and $c = d$ then f' is determined by oddsupp. It is not difficult to verify that for all $I \in \binom{[n]}{2}$, each one of f_I, f'_I, g_I and g'_I is similar to the function $(0,0) \mapsto a$, $(0,1) \mapsto b$, $(1,0) \mapsto c$, $(1,1) \mapsto d$. Hence f, f', g and g' are hypomorphic to each other.

3.4 RECONSTRUCTIBILITY OF AFFINE FUNCTIONS

A *nonassociative right semiring* is an algebra $(A; +, \cdot)$ with binary addition and multiplication operations such that

$\mathcal{C}$	arity	$\mathcal{C}^{(n)}$	ref.
constant functions	$n > \lvert A\rvert$	R	3.2.5
functions det. by supp	$n > \lvert A\rvert$	R	3.3.3
functions det. by oddsupp	$n > \max(\lvert A\rvert, 3)$	R	3.3.4
functions det. by ofo	$n \geq \lvert A\rvert + 2$, $\lvert A\rvert \equiv 1, 2 \pmod 4$ or $n \geq \lvert A\rvert + 3$, $\lvert A\rvert \equiv 0, 3 \pmod 4$	W	5.4.5
totally symmetric functions	$n \geq \lvert A\rvert + 2$	R	3.3.1
	$n > \max(\lvert A\rvert, 3)$	W	3.3.2
linear functions over a nonassociative right semiring	$n \geq 4$	W	3.4.2
affine functions over a cancellative nonassociative right semiring	$n \geq 4$	W	3.4.2
affine functions over a finite field	$n > \max(\lvert A\rvert, 3)$	R	3.4.3
clone on $\{0, 1\}$			
– $\mathcal{C} \subseteq \Lambda$, $\mathcal{C} \subseteq V$ or $\mathcal{C} \subseteq L$	$n \geq 4$	S	3.6.1
– $\mathcal{C} \supseteq M_c$	$n \geq 6$	N	3.6.2
– $\mathcal{C} \supseteq M_c U_\infty$ or $\mathcal{C} \supseteq M_c W_\infty$	$n \geq 7$	N	3.6.2
– $\mathcal{C} \supseteq SM$	$3 \leq n \leq 4$ or $n \geq 6$ and $n \equiv 2 \pmod 4$	N	3.6.2
– $\mathcal{C} \subseteq M$	$n = 5$	R	3.6.2
– $\mathcal{C} \subseteq MU_3$ or $\mathcal{C} \subseteq MW_3$	$3 \leq n \leq 4$	W	3.6.2
– $\mathcal{C} \supseteq \Lambda_c$ or $\mathcal{C} \supseteq V_c$	$n = 2$	N	3.6.2

Table 5: Reconstructibility of some function classes. The first column specifies a class $\mathcal{C} \subseteq \mathcal{F}_{AB}$. The third column provides information about the reconstructibility of $\mathcal{C}^{(n)}$ when the arity n satisfies the condition in the second column. The fourth column indicates the number of the Proposition that states the result. Abbreviations: R = reconstructible, W = weakly reconstructible, N = not weakly reconstructible, S = set-reconstructible.

x	y	z	$f(x,y,z)$	$f'(x,y,z)$	$g(x,y,z)$	$g'(x,y,z)$
0	0	0	a	a	a	a
0	0	1	b	c	b	c
0	1	0	b	c	b	c
0	1	1	c	b	b	c
1	0	0	b	c	c	b
1	0	1	c	b	c	b
1	1	0	c	b	c	b
1	1	1	d	d	d	d

Table 6: Nonreconstructible ternary functions.

- $(A;+)$ is a commutative monoid with neutral element 0 ($0+a = a+0 = a$),
- $(A;\cdot)$ is a groupoid with right identity 1 ($a \cdot 1 = a$),
- multiplication is right distributive over addition ($(a+b)\cdot c = a\cdot c + b\cdot c$),
- multiplication on the right by 0 annihilates A ($a \cdot 0 = 0$).

We will denote multiplication simply by concatenation. A nonassociative right semiring $(A;+,\cdot)$ is *cancellative* if the additive monoid $(A;+)$ is cancellative, i.e., $a+b = a+c$ implies $b = c$.

The attribute "nonassociative" refers to the fact that multiplication is not required to be associative, contrary to the usual definition of semirings. The attribute "right" refers to the fact that we only stipulate right multiplicative identity, right distributivity and right annihilation. (A nonassociative left semiring could be defined analogously, but we will not need this notion here.) Examples of nonassociative right semirings include semirings, rings, fields, and bounded distributive lattices. Rings and fields are cancellative.

A function $f\colon A^n \to A$ is *affine* over a nonassociative right semiring $(A;+,\cdot)$ if there exist $a_1,\dots,a_n,c \in A$ such that

$$f(x_1,\dots,x_n) = a_1x_1 + \cdots + a_nx_n + c, \tag{3.4.1}$$

for all $x_1,\dots,x_n \in A$. If $c = 0$ then f is *linear.*

Let $f\colon A^n \to A$ be an affine function over a nonassociative right semiring $(A;+,\cdot)$. It can be shown that if f is linear or if $(A;+,\cdot)$ is cancellative, then f has a unique representation of the form (3.4.1) ([57, Lemma 4.2]). In this case, f is completely described, up to similarity, by the multiset $\langle a_1,\dots,a_n\rangle$ of coefficients and the constant c in the representation (3.4.1). Note also that the identification minors of f are again affine functions, and the multiset of coefficients of f_I, $I = \{i,j\} \in \binom{[n]}{2}$, is $\langle a_1,\dots,a_n\rangle \setminus \langle a_i,a_j\rangle \uplus \langle a_i + a_j\rangle$.

This suggests that we consider another reconstruction problem. Let $(A;+)$ be a commutative groupoid. In the *reconstruction problem of*

multisets over $(A;+)$, the objects are finite multisets over A, and the equivalence relation is the equality relation on $\mathcal{M}(A)$. The size of a multiset is its cardinality. The cards of a multiset $\langle a_1,\dots,a_n\rangle$ are the multisets $\langle a_1,\dots,a_n\rangle \setminus \langle a_i,a_j\rangle \uplus \langle a_i+a_j\rangle$ of cardinality $n-1$, for each $\{i,j\} \in \binom{[n]}{2}$. The reconstructible multisets are completely described as follows.

Proposition 3.4.1 ([57, Theorems 3.7–3.10])**.** *Let* $(A;+)$ *be a commutative groupoid, and let* M *and* M' *be multisets of cardinality* n *over* A*. Then* $\operatorname{deck} M = \operatorname{deck} M'$ *if and only if* $M = M'$ *or one of the following statements holds:*

(i) $n = 2$ *and* $\{M,M'\} = \{\langle r,s\rangle, \langle t,u\rangle\}$ *for some elements* $r,s,t,u \in A$ *satisfying* $r+s = t+u$*;*

(ii) $n = 3$ *and* $\{M,M'\} = \{\langle r,s,t\rangle, \langle r,r+s,r+t\rangle\}$ *for some elements* $r,s,t \in A$ *satisfying*

$$\begin{aligned} r+(r+s) &= s,\\ r+(r+t) &= t,\\ (r+s)+(r+t) &= s+t; \end{aligned}$$

(iii) $n = 3$ *and* $\{M,M'\} = \{\langle r,s,t\rangle, \langle r+s,r+t,s+t\rangle\}$ *for some elements* $r,s,t \in A$ *satisfying*

$$\begin{aligned} (r+s)+(r+t) &= r,\\ (r+s)+(s+t) &= s,\\ (r+t)+(s+t) &= t; \end{aligned}$$

(iv) $n = 4$ *and* $\{M,M'\} = \{\langle r,s,t,u\rangle, \langle r,s,t,v\rangle\}$ *for some elements* $r,s,t,u,v \in A$ *satisfying* $x+u = v$ *and* $x+v = u$ *for all* $x \in \{r,s,t\}$ *and* $r+s = s$*,* $s+t = t$*,* $t+r = r$*.*

Proposition 3.4.1 can then be translated back to the realm of affine functions over a nonassociative right semiring. It should be noted that the nonreconstructible multisets of cardinality 4 are lost in this translation, because addition is associative in a nonassociative right semiring, and any commutative groupoid that contains elements satisfying the conditions of Proposition 3.4.1(iv) is not associative (see [57, Example 3.1]).

Proposition 3.4.2 ([57, Theorem 4.5])**.** *Let* $f,g\colon A^n \to A$ *be affine functions over a nonassociative right semiring* $(A;+,\cdot)$ *with* $n \geq 4$*. If* f *and* g *are linear or if* $(A;+,\cdot)$ *is cancellative, then* $\operatorname{deck} f = \operatorname{deck} g$ *if and only if* $f \simeq g$*.*

This result can be strengthened when $(A;+,\cdot)$ is a finite field. In this case, every non-affine function of arity at least $\max(|A|,3)+1$ has a non-affine identification minor (see [57, Lemma 4.6]), and hence the class of affine functions of arity at least $\max(|A|,3)+1$ is recognizable. Together with Proposition 3.4.2, this implies reconstructibility.

Proposition 3.4.3 ([57, Theorem 4.7]). *Let $f\colon A^n \to A$ be an affine function over a finite field $(A;+,\cdot)$. If $n \geq \max(|A|,3)+1$, then f is reconstructible.*

3.5 NONRECONSTRUCTIBLE FUNCTIONS

Polynomial operations of a bounded distributive lattice can be represented in *disjunctive normal form,* as described by the following classical result.

Theorem 3.5.1 (Goodstein [34]). *Let $\mathbf{A} = (A;\vee,\wedge,0,1)$ be a bounded distributive lattice. A function $f\colon A^n \to A$ is a polynomial operation of $\mathbf{A}$ if and only if*

$$f(x_1,\dots,x_n) = \bigvee_{S\subseteq[n]} (a_S \wedge \bigwedge_{i\in S} x_i), \tag{3.5.1}$$

where the coefficients are given by $a_S = f(e_1,\dots,e_n)$ where $e_i = 1$ if $i \in S$ and $e_i = 0$ if $i \notin S$.

For term operations over a bounded distributive lattice, the coefficients a_S in (3.5.1) are always 0's and 1's. We can discard the monomials with coefficient 0 and take only the disjunction of the monomials with coefficient 1. It follows that a function $f\colon A^n \to A$ is a term operation of a bounded distributive lattice $\mathbf{A} = (A;\vee,\wedge,0,1)$ if and only if

$$f(x_1,\dots,x_n) = \bigvee_{S\in\mathcal{A}} \bigwedge_{i\in S} x_i \tag{3.5.2}$$

for some $\mathcal{A} \subseteq \mathcal{P}([n])$. Moreover, since $\bigwedge_{i\in S} x_i \vee \bigwedge_{i\in S'} x_i = \bigwedge_{i\in S} x_i$ whenever $S \subseteq S'$ by the absorption law, it suffices to take the set $\mathcal{A}_{\min}$ of minimal (with respect to inclusion) elements of $\mathcal{A}$ in place of $\mathcal{A}$ in (3.5.2).

For any set system $\mathcal{A} \subseteq \mathcal{P}(X)$, the set $\mathcal{A}_{\min}$ of minimal elements of $\mathcal{A}$ is an antichain in the power set lattice $(\mathcal{P}(X);\subseteq)$. Antichains in the power set lattice $(\mathcal{P}(X);\subseteq)$ are called *Sperner systems* on X.

The n-ary term operations of a bounded distributive lattice $\mathcal{A} = (A;\vee,\wedge,0,1)$ are in one-to-one correspondence with Sperner systems on $[n]$. Namely, to each Sperner system $\mathcal{A} \subseteq \mathcal{P}([n])$ we can associate the term operation (3.5.2), and every term operation can be represented in the form (3.5.2) for some Sperner system $\mathcal{A}$, as discussed above. Moreover, distinct Sperner systems give rise to distinct term operations.

Let $\mathcal{A}$ be a Sperner system on $[n]$, and let $f\colon A^n \to A$ be as in (3.5.2). Let us consider the identification minors of f. For $I \in \binom{[n]}{2}$, we get

$$\begin{aligned} f_I(x_1,\dots,x_{n-1}) &= (f\circ\underline{\delta_I})(x_1,\dots,x_{n-1}) = f(x_{\delta_I(1)},\dots,x_{\delta_I(n)}) \\ &= \bigvee_{S\in\mathcal{A}} \bigwedge_{i\in S} x_{\delta_I(i)} = \bigvee_{S\in\mathcal{A}} \bigwedge_{i\in\delta_I(S)} x_i = \bigvee_{S\in\delta_I(\mathcal{A})} \bigwedge_{i\in S} x_i = \bigvee_{S\in(\delta_I(\mathcal{A}))_{\min}} \bigwedge_{i\in S} x_i, \end{aligned}$$

and $(\delta_I(\mathcal{A}))_{\min}$ is a Sperner system on $[n-1]$.

This suggests formulating a reconstruction problem for Sperner systems and analysing it in order to determine whether term operations of a bounded distributive lattice are reconstructible. The *reconstruction problem of Sperner systems and identification minors* is specified by the following data. The objects are Sperner systems on $[n]$, for $n \in \mathbf{N}_+$. The equivalence relation is the isomorphism relation: two Sperner systems $\mathcal{A}$ and $\mathcal{B}$ on $[n]$ are isomorphic, denoted $\mathcal{A} \simeq \mathcal{B}$, if there exists a permutation $\pi \in S_n$ such that $\mathcal{A} = \pi(\mathcal{B})$. The objects derived from a Sperner system $\mathcal{A}$ on $[n]$ are the Sperner systems $\mathcal{A}_I := (\delta_I(\mathcal{A}))_{\min}$ on $[n-1]$, for $I \in \binom{[n]}{2}$. Thus, $\operatorname{deck}\mathcal{A} = \langle \mathcal{A}_I/\simeq : I \in \binom{[n]}{2} \rangle$.

The reconstruction problem for Sperner systems and identification minors was studied by Couceiro, Schölzel, and the current author in [17]. We obtained some negative results: we discovered several infinite families of nonreconstructible Sperner systems. The constructions and proofs are quite technical, and we will not go into details here. Just to give an idea of the Sperner systems involved, we present one of our nonreconstructible families in the following example.

Example 3.5.2. For each $m \geq 3$, we define Sperner systems $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ on the set $[2m]$. The systems will be built from a few components that we define first. For $J \subseteq [m]$, let $F_J^m := J \cup \{i+m : i \in [m] \setminus J\}$. Let $\mathcal{F}_1^m := \{F_J^m : J \subseteq [m], |J| \text{ odd}\}$, $\mathcal{F}_2^m := \{F_J^m : J \subseteq [m], |J| \text{ even}\}$. For $p \in [m]$, let $G_p^m := [2m] \setminus \{p, p+m, (p \oplus 1)+m\}$, where $\oplus$ denotes addition modulo m. Let $\mathcal{G}^m := \{G_p^m : p \in [m]\}$. For $i \in \{1,2\}$, define $\mathcal{M}_i^m := \mathcal{F}_i^m \cup \mathcal{G}^m$.

It was shown in [17, Section 3] that for every $m \geq 3$, the Sperner systems $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ are nonisomorphic and hypomorphic. In other words, $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ are not reconstructible. In fact, $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ are strongly hypomorphic, that is, for every $I \in \binom{[n]}{2}$, we have $(\mathcal{M}_1^m)_I \simeq (\mathcal{M}_2^m)_I$. In other words, even with the knowledge of which two-element set $I \in \binom{[n]}{2}$ is associated with each card, it is impossible to reconstruct these Sperner systems.

The nonreconstructible Sperner systems that we discovered, such as the ones in Example 3.5.2, can be translated back to term operations of a bounded distributive lattice, and we arrive to the conclusion that there exist infinite families of nonreconstructible functions, and there even exist infinite families of pairs of nonsimilar, strongly hypomorphic functions. This is true for functions in $\mathcal{F}_{AB}$ for any finite sets A and B with at least two elements, because there exist bounded distributive lattices of every finite cardinality (finite chains, for instance) and because we can easily build new nonreconstructible functions from given ones, for example, by extending the domain or the codomain.

Considering, in particular, Boolean functions, we constructed, for each clone $\mathcal{C}$ among SM, M_cU_∞, M_cW_∞ (see Appendix A), an infinite

family of pairs of nonreconstructible Sperner systems such that its translation into term functions of a two-element lattice results in an infinite family of pairs of nonsimilar, strongly hypomorphic functions that lie within the clone $\mathcal{C}$.

Let us finally mention that our work on Sperner systems had a surprising connection to the reconstruction problem of hypergraphs and one-vertex-deleted subhypergraphs (see Example 3.1.2). Any Sperner system on the set $[n]$, being a subset of $\mathcal{P}([n])$, can be seen as the edge set of a hypergraph with vertex set $[n]$. It turned out that for every $m \geq 3$, the Sperner systems $\mathcal{M}_1^m$ and $\mathcal{M}_2^m$ of Example 3.5.2 are the edge sets of non-isomorphic and strongly hypomorphic hypergraphs (see [17, Corollary 7.3]). Of course, it is well known that hypergraphs are not reconstructible, and infinite families of nonreconstructible hypergraphs have earlier been constructed by Kocay [49] and Kocay and Lui [50]. Nevertheless, our infinite family is quite different from the ones presented earlier in the literature, and it is curious that it arose as a by-product of a completely different reconstruction problem.

3.6 RECONSTRUCTIBILITY OF POST CLASSES

Clones are interesting sets of functions, and it makes sense to ask whether they are reconstructible. It follows from Proposition 3.4.2 that if $\mathcal{C}$ is a clone on $\{0,1\}$ that is contained in L, V or Λ (see Appendix A), then $\mathcal{C}^{(n)}$ is reconstructible for every $n \geq 4$. In fact, $\mathcal{C}^{(n)}$ is also set-reconstructible for every $n \geq 4$. This follows from the following result of Couceiro, Schölzel, and the current author and from the fact that constant functions (of sufficiently large arity) are reconstructible (see Proposition 3.2.5) and hence also set-reconstructible.

Proposition 3.6.1 ([18, Proposition 3.7])**.** *Assume that $(A;\circ)$ is a semilattice or a Boolean group. If $\mathcal{C}$ is a subclone of the clone generated by $\circ$, then $\mathcal{C}^{(n)}$ is set-reconstructible for all $n \geq |A| + 2$.*

As explained in Section 3.5, each one of the clones SM, M_cU_∞, M_cW_∞ (and hence every clone that contains one of them) includes an infinite family of pairs of nonisomorphic, strongly hypomorphic functions; in other words, these clones are not weakly reconstructible and hence also not set-reconstructible.

The infinite families of nonreconstructible functions constructed in [17] do not include functions of every possible arity. Therefore we were not able to determine for every clone $\mathcal{C}$ that is not weakly reconstructible, whether the n-ary part $\mathcal{C}^{(n)}$ is not weakly reconstructible for every n. We were, however, able to conclude the following.

Proposition 3.6.2 ([17, page 282])**.** *Let $\mathcal{C}$ be a clone on $\{0,1\}$.*

(i) *If $\mathcal{C} \supseteq M_c$ and $n \geq 6$, then $\mathcal{C}^{(n)}$ is not weakly reconstructible.*

(ii) *If* $\mathcal{C} \supseteq M_c U_\infty$ *or* $\mathcal{C} \supseteq M_c W_\infty$ *and* $n \geq 7$, *then* $\mathcal{C}^{(n)}$ *is not weakly reconstructible.*

(iii) *If* $\mathcal{C} \supseteq SM$ *and* $3 \leq n \leq 4$ *or* $n \geq 6$ *and* $n \equiv 2 \pmod 4$, *then* $\mathcal{C}^{(n)}$ *is not weakly reconstructible.*

(iv) *If* $\mathcal{C} \subseteq M$, *then* $\mathcal{C}^{(5)}$ *is reconstructible.*

(v) *If* $\mathcal{C} \subseteq MU_3$ *or* $\mathcal{C} \subseteq MW_3$ *and* $3 \leq n \leq 4$, *then* $\mathcal{C}^{(n)}$ *is weakly reconstructible.*

(vi) *If* $\mathcal{C} \supseteq \Lambda_c$ *or* $\mathcal{C} \supseteq V_c$, *then* $\mathcal{C}^{(2)}$ *is not weakly reconstructible.*

3.7 REMARKS

When the current author first looked into the reconstruction problem of functions, he thought that the most obvious starting point would be the functions whose deck is as simple as possible, comprising just a single function with high multiplicity. Such functions are, of course, the ones with a unique identification minor (see Section 2.6). While it was relatively easy to prove that certain classes of functions with a unique identification minor are weakly reconstructible, the author soon realized that it is quite difficult to establish the stronger property of reconstructibility. The lack of a good characterization of functions with a unique identification minor is a significant obstacle in identifying potential candidates for reconstructions of a given function. This explains how the author came across Problem 2.6.1 and motivates his interest in discovering an answer to it.

Totally symmetric functions have a unique identification minor, and in Section 3.3 we saw that they are reconstructible. In Section 5.4, we will analyse the reconstructibility of another class of functions with a unique identification minor, namely, functions determined by ofo.

4

MINORS OF PERMUTATIONS

We are now going to develop theory of minors of permutations. This notion is somewhat analogous to minors of functions, which were considered in earlier chapters. In fact, we have already seen minors of permutations when we discussed ordered partitions in Section 1.7, but we have just not been calling them that way yet.

First, in Section 4.1, we introduce minors of permutations and establish some basic facts about the poset of minors. Then, in Section 4.2, we discuss Galois connections induced by the minor relation. As a tool for analysing minors, we introduce in Section 4.3 two transformations of interval partitions: compression and expansion. Next, in Section 4.4, we investigate the permutation groups generated by the ℓ-minors of a given n-permutation τ and by the differences of the ℓ-minors of τ. These theoretical results will find applications in the analysis of functions determined by the order of first occurrence in Chapter 5. Finally, we briefly discuss a reconstruction problem of permutations and minors in Section 4.5 and an open group-theoretical problem in Section 4.6.

A reader familiar with the theory of permutation patterns (see, e.g., Kitayev [48]) will recognize many similarities and differences between minors of permutations and permutation patterns. Much of the theory developed in Sections 4.1 and 4.2 parallels the work of Pöschel and the current author [63] on permutation patterns.

4.1 MINORS OF PERMUTATIONS

Let $\mathbf{P} := \bigcup_{n\geq 1} S_n$ be the set of all finite permutations. We refer to S_n as the n-th *level* of $\mathbf{P}$.

Definition 4.1.1. Let $\sigma \in S_n$ and let $\Pi \in \mathrm{Part}_m(n)$. Recall from Definition 1.7.2 the permutation $\sigma_\Pi \in S_m$ defined as $\sigma_\Pi := (h_\Pi^{\mathrm{id}})^{-1} \circ h_\Pi^\sigma$. We say that a permutation τ is a *minor* of σ, and we write $\tau \leq \sigma$, if $\tau = \sigma_\Pi$ for some partition $\Pi \in \mathrm{Part}(n)$. In order to emphasize the fact that τ is an m-permutation, we may also say that τ is an *m-minor* of σ.

Fact 4.1.2. Given a permutation $\sigma = \sigma_1 \dots \sigma_n \in S_n$ in one-line notation and an m-partition Π of $[n]$, we can construct σ_Π by the following procedure.

1. Replace each σ_i by the minimum of its Π-block, i.e., for each $i \in [n]$, let $\sigma'_i := \min \sigma_i/\Pi$.

2. Delete any repetitions of letters from $\sigma' = \sigma'_1 \dots \sigma'_n$, i.e., let $\sigma'' := \mathrm{ofo}(\sigma')$. (Note that $|\sigma''| = m$, because Π has m blocks, so there are m distinct minima.)

3. For each $i \in [m]$, replace the i-th smallest entry of σ'' by i. The resulting string is the one-line notation of σ_Π.

Fact 4.1.3. In line with the notational convention explained in Remark 1.4.6, for any $\sigma \in S_n$ and $\emptyset \neq I \subseteq [n]$, we write σ_I to designate the minor σ_Π, where $\Pi \in \mathrm{Part}(n)$ is the partition whose only potentially nontrivial block is I. If $I \in \binom{[n]}{2}$, then the permutation σ_I can be written explicitly in terms of σ as follows:

$$\sigma_I(i) = \begin{cases} \min I, & \text{if } i = \min \sigma^{-1}(I), \\ \sigma(i), & \text{if } i \neq \min \sigma^{-1}(I),\ i < \max \sigma^{-1}(I), \\ & \quad \text{and } \sigma(i) < \max I, \\ \sigma(i) - 1, & \text{if } i \neq \min \sigma^{-1}(I),\ i < \max \sigma^{-1}(I), \\ & \quad \text{and } \sigma(i) > \max I, \\ \sigma(i+1), & \text{if } i \geq \max \sigma^{-1}(I) \text{ and } \sigma(i+1) < \max I, \\ \sigma(i+1) - 1, & \text{if } i \geq \max \sigma^{-1}(I) \text{ and } \sigma(i+1) > \max I. \end{cases}$$

Example 4.1.4. The minors of the permutation $\sigma = 42531 \in S_5$ are presented in Table 7. For each $m \in \{1, \dots, 5\}$, we enumerate all m-partitions Π of $[5]$, and for each partition Π, we indicate the order $\leq^\sigma_\Pi$ and the minor σ_Π. We use the shorthand introduced in Remarks 1.4.1 and 1.7.1 to specify (ordered) partitions.

Lemma 4.1.5. *The minor relation is a partial order on the set* $\mathbf{P}$ *of all finite permutations.*

Proof. The minor relation is clearly reflexive, because for every $\sigma \in S_n$ we have $\sigma = \sigma_{\Delta_n}$ where Δ_n is the trivial partition of $[n]$. The minor relation is antisymmetric, because if $\sigma \in S_n$ and $\tau \in S_m$ and $\sigma \leq \tau$ and $\tau \leq \sigma$, then $n \leq m \leq n$, so $m = n$. Since the only n-partition of $[n]$ is the trivial partition Δ_n, it follows that $\sigma = \tau_{\Delta_n} = \tau$. For transitivity, observe that if $\pi \in S_\ell$, $\tau \in S_m$, $\sigma \in S_n$ and $\pi \leq \tau$ and $\tau \leq \sigma$, then there exist $\Phi \in \mathrm{Part}_\ell(m)$ and $\Pi \in \mathrm{Part}_m(n)$ such that $\pi = \tau_\Phi$ and $\tau = \sigma_\Pi$. It follows from Lemmas 1.7.6 and 1.7.8 that $\Pi_\Phi \in \mathrm{Part}_\ell(n)$ and $\pi = (\sigma_\Pi)_\Phi = (\sigma_\Pi)_{\delta_\Pi(\Pi_\Phi)} = \sigma_{\Pi_\Phi}$, that is, $\pi \leq \sigma$. □

Recall that a poset $(P; \leq)$ is *graded,* if there exists a *rank function* $r\colon P \to \mathbf{N}$ satisfying the following conditions: $r(x) < r(y)$ whenever $x < y$ in P, and whenever x is a lower cover of y in P, the equality $r(y) = r(x) + 1$ holds.

Lemma 4.1.6. *The minor poset* $(\mathbf{P}; \leq)$ *is a graded poset with rank function* $r\colon \mathbf{P} \to \mathbf{N}$, $r(\sigma) = n$ *for all* $\sigma \in S_n$, $n \in \mathbf{N}$.

$m = 5$

Π	$\leq_\Pi^\sigma$	σ_Π
1|2|3|4|5	4|2|5|3|1	42531

$m = 4$

Π	$\leq_\Pi^\sigma$	σ_Π	Π	$\leq_\Pi^\sigma$	σ_Π
12|3|4|5	4|12|5|3	3142	1|24|3|5	24|5|3|1	2431
13|2|4|5	4|2|5|13	3241	1|25|3|4	4|25|3|1	4231
14|2|3|5	14|2|5|3	1243	1|2|34|5	34|2|5|1	3241
15|2|3|4	4|2|15|3	4213	1|2|35|4	4|2|35|1	4231
1|23|4|5	4|23|5|1	3241	1|2|3|45	45|2|3|1	4231

$m = 3$

Π	$\leq_\Pi^\sigma$	σ_Π	Π	$\leq_\Pi^\sigma$	σ_Π
123|4|5	4|123|5	213	13|24|5	24|5|13	231
124|3|5	124|5|3	132	13|25|4	4|25|13	321
125|3|4	4|125|3	312	13|2|45	45|2|13	321
134|2|5	134|2|5	123	14|23|5	14|23|5	123
135|2|4	4|2|135	321	14|25|3	14|25|3	123
145|2|3	145|2|3	123	14|2|35	14|2|35	123
1|234|5	234|5|1	231	15|23|4	4|23|15	321
1|235|4	4|235|1	321	15|24|3	24|15|3	213
1|245|3	245|3|1	231	15|2|34	34|2|15	321
1|2|345	345|2|1	321	1|23|45	45|23|1	321
12|34|5	34|12|5	213	1|24|35	24|35|1	231
12|35|4	4|12|35	312	1|25|34	34|25|1	321
12|3|45	45|12|3	312			

$m = 2$

Π	$\leq_\Pi^\sigma$	σ_Π	Π	$\leq_\Pi^\sigma$	σ_Π
1234|5	1234|5	12	134|25	134|25	12
1235|4	4|1235	21	135|24	24|135	21
1245|3	1245|3	12	145|23	145|23	12
1345|2	1345|2	12	15|234	234|15	21
1|2345	2345|1	21	14|235	14|235	12
123|45	45|123	21	13|245	245|13	21
124|35	124|35	12	12|345	345|12	21
125|34	34|125	21			

$m = 1$

Π	$\leq_\Pi^\sigma$	σ_Π
12345	12345	1

Table 7: Minors of $\sigma = 42531$.

Proof. We show that the function r prescribed in the statement of the lemma is a rank function for $(\mathbf{P}; \leq)$. Let $\sigma \in S_n$, $\pi \in S_m$. If $\pi < \sigma$ then $\pi = \sigma_\Pi$ for some partition $\Pi \in \mathrm{Part}(n)$ with fewer than n blocks. Then clearly $r(\pi) = |\Pi| < n = r(\sigma)$.

Assume then that π is a lower cover of σ, and let $\Pi \in \mathrm{Part}(n)$ be such that $\pi = \sigma_\Pi$. Suppose, to the contrary, that $|\Pi| = m < n - 1$. It is well known that the poset of partitions of a finite set ordered by refinement is a semimodular lattice and hence a graded poset. Therefore, there exists a partition $\Phi \in \mathrm{Part}_{n-1}(n)$ such that $\Phi \sqsubseteq \Pi$. By Lemma 1.7.7(iii), we have $\sigma_\Pi < \sigma_\Phi < \sigma$, which contradicts the assumption that $\pi = \sigma_\Pi$ is a lower cover of σ. □

The *direct sum* of permutations $\sigma \in S_m$ and $\tau \in S_n$ is the permutation $\sigma \oplus \tau$ of degree $m + n$ that consists of σ followed by a shifted copy of τ, formally

$$(\sigma \oplus \tau)(i) = \begin{cases} \sigma(i), & \text{if } 1 \leq i \leq m, \\ m + \tau(i - m), & \text{if } m + 1 \leq i \leq m + n. \end{cases}$$

An *interval* in a permutation σ is an interval $[a, b]$ (as defined in Section 1.2) such that the set of values $\{\sigma(i) : i \in [a, b]\}$ is also an interval.[1] For permutations $\sigma \in S_n$ and $\tau_i \in S_{m_i}$ for $i \in [n]$, the *inflation* of σ by $\tau_1, \ldots, \tau_n$ is the permutation $\sigma[\tau_1, \ldots, \tau_n]$ of degree $\sum_{i=1}^{n} m_i$ obtained by replacing each entry $\sigma(i)$ of σ with an interval that is order-isomorphic to τ_i. For example, $2413[123, 21, 1, 231] = 234981675$.

Lemma 4.1.7.

(i) *The minor poset* $(\mathbf{P}; \leq)$ *has a least element, namely* $1 \in S_1$.

(ii) *The minor poset* $(\mathbf{P}; \leq)$ *has no maximal elements.*

(iii) *Any two permutations* $\pi \in S_m$ *and* $\tau \in S_n$ *have an upper bound of degree* $m + n - 1$.

Proof. (i) Clear.

(ii) For any $\sigma \in S_n$, we have $\sigma \leq \sigma \oplus 1$, because $(\sigma \oplus 1)_\Pi = \sigma$ for $\Pi = \langle \{n, n + 1\} \rangle_{\mathrm{part}}$.

(iii) Given $\pi \in S_m$ and $\tau \in S_n$, let $\sigma := \pi[\tau, 1, 1, \ldots, 1]$. Then $\pi = \sigma_\Pi$ and $\tau = \sigma_\Gamma$ for $\Pi := \langle [\pi(1), \pi(1) + m - 1] \rangle_{\mathrm{part}}$ and $\Gamma := \langle [1, \pi(1)], [\pi(1) + m - 1, m + n - 1] \rangle_{\mathrm{part}}$. □

Let us derive a few useful identities involving minors of permutations.

Lemma 4.1.8. *Let* $\pi, \tau \in S_n$, *and let* $\Pi \in \mathrm{Part}_m(n)$.

1 This overloaded use of the term "interval" should not cause any confusion, because the concept of an interval in a permutation will only be used in the definition of inflation of permutation that comes next.

(i) $(\pi^{-1})_\Pi = (\pi_{\pi(\Pi)})^{-1}$.

(ii) $(\pi \circ \tau)_\Pi = \pi_\Pi \circ \tau_{\pi^{-1}(\Pi)}$.

(iii) $(\pi^{-1} \circ \tau)_\Pi = (\pi_{\pi(\Pi)})^{-1} \circ \tau_{\pi(\Pi)}$.

Proof. (i) By the definition of π_Π, we have

$$\begin{aligned}(\pi^{-1})_\Pi = (h^{\mathrm{id}}_\Pi)^{-1} \circ h^{\pi^{-1}}_\Pi &= (h^{\pi}_{\pi(\Pi)})^{-1} \circ h^{\mathrm{id}}_{\pi(\Pi)} \\ &= ((h^{\mathrm{id}}_{\pi(\Pi)})^{-1} \circ h^{\pi}_{\pi(\Pi)})^{-1} = (\pi_{\pi(\Pi)})^{-1},\end{aligned}$$

where the second equality holds by Lemma 1.7.9(iii).

(ii) By the definition of σ_Π and Lemma 1.7.9(iii), we have

$$\begin{aligned}(\pi \circ \tau)_\Pi = (h^{\mathrm{id}}_\Pi)^{-1} \circ h^{\pi\circ\tau}_\Pi &= (h^{\pi^{-1}}_{\pi^{-1}(\Pi)})^{-1} \circ h^{\tau}_{\pi^{-1}(\Pi)} \\ &= (h^{\pi^{-1}}_{\pi^{-1}(\Pi)})^{-1} \circ h^{\mathrm{id}}_{\pi^{-1}(\Pi)} \circ (h^{\mathrm{id}}_{\pi^{-1}(\Pi)})^{-1} \circ h^{\tau}_{\pi^{-1}(\Pi)} \\ &= (h^{\mathrm{id}}_\Pi)^{-1} \circ h^{\pi}_\Pi \circ (h^{\mathrm{id}}_{\pi^{-1}(\Pi)})^{-1} \circ h^{\tau}_{\pi^{-1}(\Pi)} = \pi_\Pi \circ \tau_{\pi^{-1}(\Pi)}.\end{aligned}$$

(iii) By parts (i) and (ii), we have

$$(\pi^{-1} \circ \tau)_\Pi = (\pi^{-1})_\Pi \circ \tau_{\pi(\Pi)} = (\pi_{\pi(\Pi)})^{-1} \circ \tau_{\pi(\Pi)}. \qquad \square$$

The following lemma is a generalized and sharpened version of [56, Lemma 4.1].

Lemma 4.1.9. *Let $\sigma \in S_n$, and let $\Pi \in \mathrm{Part}(n)$.*

(i) $\mathrm{nat}_\Pi \circ \sigma = h^{\sigma}_\Pi \circ (h^{\mathrm{id}}_{\sigma^{-1}(\Pi)})^{-1} \circ \mathrm{nat}_{\sigma^{-1}(\Pi)}$.

(ii) $\delta_\Pi \circ \sigma = \sigma_\Pi \circ \delta_{\sigma^{-1}(\Pi)}$.

Proof. (i) By Lemma 1.7.9(ii), the mapping $h^{\mathrm{id}}_{\sigma^{-1}(\Pi)} \circ (h^{\sigma}_\Pi)^{-1}$ is an order-isomorphism $(\Pi; \leq^{\sigma}_\Pi) \to (\sigma^{-1}(\Pi); \leq^{\mathrm{id}}_{\sigma^{-1}(\Pi)})$ and it is given by the rule $B \mapsto \sigma^{-1}(B)$ for every $B \in \Pi$. Therefore its inverse $h^{\sigma}_\Pi \circ (h^{\mathrm{id}}_{\sigma^{-1}(\Pi)})^{-1}$ is the mapping $\sigma^{-1}(B) \mapsto B$.

Now let $x \in [n]$, and let $B := x/\Pi$. Then $\sigma^{-1}(x) \in \sigma^{-1}(B)$, so $\mathrm{nat}_{\sigma^{-1}(\Pi)}(\sigma^{-1}(x)) = \sigma^{-1}(B)$, and we have

$$h^{\sigma}_\Pi((h^{\mathrm{id}}_{\sigma^{-1}(\Pi)})^{-1}(\mathrm{nat}_{\sigma^{-1}(\Pi)}(\sigma^{-1}(x)))) = B = \mathrm{nat}_\Pi(x).$$

Consequently, $h^{\sigma}_\Pi \circ (h^{\mathrm{id}}_{\sigma^{-1}(\Pi)})^{-1} \circ \mathrm{nat}_{\sigma^{-1}(\Pi)} \circ \sigma^{-1} = \mathrm{nat}_\Pi$. We obtain the claimed identity by composing both sides from the right by σ.

(ii) The definitions and part (i) yield

$$\begin{aligned}\sigma_\Pi \circ \delta_{\sigma^{-1}(\Pi)} &= (h^{\mathrm{id}}_\Pi)^{-1} \circ h^{\sigma}_\Pi \circ (h^{\mathrm{id}}_{\sigma^{-1}(\Pi)})^{-1} \circ \mathrm{nat}_{\sigma^{-1}(\Pi)} \\ &= (h^{\mathrm{id}}_\Pi)^{-1} \circ \mathrm{nat}_\Pi \circ \sigma = \delta_\Pi \circ \sigma. \qquad \square\end{aligned}$$

4.2 GALOIS CONNECTIONS INDUCED BY THE MINOR RELATION OF PERMUTATIONS

For $\tau \in S_n$ and $\ell \leq n$, we denote by $\operatorname{Min}^{(\ell)} \tau$ the set of all ℓ-minors of τ, i.e., $\operatorname{Min}^{(\ell)} \tau := \{\sigma \in S_\ell : \sigma \leq \tau\}$. For any set $S \subseteq S_\ell$, we say that a permutation $\tau \in S_n$ is *compatible* with S if $\operatorname{Min}^{(\ell)} \tau \subseteq S$. For $S \subseteq S_\ell$ and $T \subseteq S_n$, we write

$$\operatorname{Comp}^{(n)} S := \{\tau \in S_n \mid \operatorname{Min}^{(\ell)} \tau \subseteq S\},$$
$$\operatorname{Min}^{(\ell)} T := \bigcup_{\tau \in T} \operatorname{Min}^{(\ell)} \tau.$$

Thus, $\operatorname{Comp}^{(n)} S$ is the set of all n-permutations compatible with S, and $\operatorname{Min}^{(\ell)} T$ is the set of all ℓ-minors of the permutations in T. It is not difficult to verify that

$$\operatorname{Comp}^{(n)} S = \{\tau \in S_n \mid \forall \sigma \in S_\ell \setminus S \colon \sigma \not\leq \tau\},$$
$$\operatorname{Min}^{(\ell)} T = S_\ell \setminus \{\sigma \in S_\ell \mid \forall \sigma \in T \colon \sigma \not\leq \tau\}.$$

Consequently, $\operatorname{Min}^{(\ell)}$ and $\operatorname{Comp}^{(n)}$ are precisely the lower and upper adjoints of the monotone Galois connection between $\mathcal{P}(S_\ell)$ and $\mathcal{P}(S_n)$ induced by the complement $\not\leq$ of the minor relation (see Section 1.8). This means that for all $S \subseteq S_\ell$ and $T \subseteq S_n$,

$$\operatorname{Min}^{(\ell)} T \subseteq S \iff T \subseteq \operatorname{Comp}^{(n)} S. \tag{4.2.1}$$

Moreover, $\operatorname{Min}^{(\ell)} \operatorname{Comp}^{(n)}$ and $\operatorname{Comp}^{(n)} \operatorname{Min}^{(\ell)}$ are kernel and closure operators on S_ℓ and S_n, respectively.

The upper adjoint $\operatorname{Comp}^{(n)}$ is particularly well behaved when it comes to permutation groups.

Proposition 4.2.1. *If G is a subgroup of S_ℓ, then $\operatorname{Comp}^{(n)} G$ is a subgroup of S_n.*

Proof. Assume that $G \leq S_\ell$, and let $\pi, \tau \in \operatorname{Comp}^{(n)} G$. Thus $\operatorname{Min}^{(\ell)} \pi$ and $\operatorname{Min}^{(\ell)} \tau$ are subsets of G. By Lemma 4.1.8(iii) we have

$$\begin{aligned}
\operatorname{Min}^{(\ell)}(\pi^{-1} \circ \tau) &= \{(\pi^{-1} \circ \tau)_\Pi : \Pi \in \operatorname{Part}_\ell(n)\} \\
&= \{(\pi_{\pi(\Pi)})^{-1} \circ \tau_{\pi(\Pi)} : \Pi \in \operatorname{Part}_\ell(n)\} \\
&\subseteq \{\rho^{-1} \circ \gamma : \rho \in \operatorname{Min}^{(\ell)} \pi,\ \gamma \in \operatorname{Min}^{(\ell)} \tau\} \\
&= (\operatorname{Min}^{(\ell)} \pi)^{-1} (\operatorname{Min}^{(\ell)} \tau) \subseteq G^{-1} G \subseteq G.
\end{aligned}$$

Consequently, $\pi^{-1} \circ \tau \in \operatorname{Comp}^{(n)} G$, which implies that $\operatorname{Comp}^{(n)} G$ is a subgroup of S_n. □

Remark 4.2.2. There is no counterpart of Proposition 4.2.1 for the lower adjoint $\operatorname{Min}^{(\ell)}$, because the set $\operatorname{Min}^{(\ell)} H$ is not necessarily a group even if H is a subgroup of S_n. The group $H = \langle (1\,4) \rangle = \{1234, 4231\} \leq S_4$ serves as a counterexample. It is easy to verify that $\operatorname{Min}^{(3)} H = \{123, 231, 312, 321\}$, which is not a subgroup of S_3.

In view of Proposition 4.2.1 and Remark 4.2.2, it would make sense to modify the monotone Galois connection Min–Comp into one between the subgroup lattices $\mathrm{Sub}(S_\ell)$ and $\mathrm{Sub}(S_n)$. To this end, define, for arbitrary subgroups $G \leq S_\ell$ and $H \leq S_n$,

$$\begin{aligned} \mathrm{gComp}^{(n)}\, G &:= \langle \mathrm{Comp}^{(n)}\, G \rangle = \mathrm{Comp}^{(n)}\, G, \\ \mathrm{gMin}^{(\ell)}\, H &:= \langle \mathrm{Min}^{(\ell)}\, H \rangle. \end{aligned}$$

Let us verify that $(\mathrm{gMin}^{(\ell)}, \mathrm{gComp}^{(n)})$ is indeed a monotone Galois connection.

Lemma 4.2.3. *For all subgroups $G \leq S_\ell$ and $H \leq S_n$, it holds that $\mathrm{gMin}^{(\ell)}\, H \subseteq G$ if and only if $H \subseteq \mathrm{gComp}^{(n)}\, G$.*

Proof. Assume first that $\mathrm{gMin}^{(\ell)}\, H \subseteq G$. Then $\mathrm{Min}^{(\ell)}\, H \subseteq G$, which implies $H \subseteq \mathrm{Comp}^{(n)}\, G$ by the defining property (4.2.1) of monotone Galois connection. Since $\mathrm{Comp}^{(n)}\, G = \mathrm{gComp}^{(n)}\, G$ by Lemma 4.2.1, we have $H \subseteq \mathrm{gComp}^{(n)}\, G$. For the converse implication, assume that $H \subseteq \mathrm{gComp}^{(n)}\, G$. Since $\mathrm{gComp}^{(n)}\, G = \mathrm{Comp}^{(n)}\, G$, this means $\mathrm{Min}^{(\ell)}\, H \subseteq G$. Hence $\mathrm{gMin}^{(\ell)}\, H = \langle \mathrm{Min}^{(\ell)}\, H \rangle \subseteq \langle G \rangle = G$. □

The adjoints $\mathrm{Min}^{(\ell)}$ and $\mathrm{Comp}^{(n)}$, as well as $\mathrm{gMin}^{(\ell)}$ and $\mathrm{gComp}^{(n)}$ have a "transitive" property that allows of going up or down the levels of **P** one by one.

Proposition 4.2.4. *Assume $\ell \leq m \leq n$. For all $S \subseteq S_\ell$ and all $T \subseteq S_n$, we have*

$$\mathrm{Comp}^{(n)}\, \mathrm{Comp}^{(m)}\, S = \mathrm{Comp}^{(n)}\, S, \tag{4.2.2}$$

$$\mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, T = \mathrm{Min}^{(\ell)}\, T. \tag{4.2.3}$$

For all $G \leq S_\ell$ and all $H \leq S_n$, we have

$$\mathrm{gComp}^{(n)}\, \mathrm{gComp}^{(m)}\, G = \mathrm{gComp}^{(n)}\, G, \tag{4.2.4}$$

$$\mathrm{gMin}^{(\ell)}\, \mathrm{gMin}^{(m)}\, H = \mathrm{gMin}^{(\ell)}\, H. \tag{4.2.5}$$

Proof. We prove equality (4.2.3) first. Let $\pi \in \mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, T$. Then $\pi = \tau_\Phi$ for some $\tau \in \mathrm{Min}^{(m)}\, T$ and $\Phi \in \mathrm{Part}_\ell(m)$. Similarly, $\tau = \sigma_\Pi$ for some $\sigma \in T$ and $\Pi \in \mathrm{Part}_m(n)$. Lemma 1.7.8 yields $\pi = (\sigma_\Pi)_\Phi = \sigma_{\Pi_\Phi}$, where $\Pi_\Phi \in \mathrm{Part}_\ell(n)$ is as defined in Lemma 1.7.6, that is, $\pi \in \mathrm{Min}^{(\ell)}\, \sigma \subseteq \mathrm{Min}^{(\ell)}\, T$. Thus $\mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, S \subseteq \mathrm{Min}^{(\ell)}\, T$.

Let now $\pi \in \mathrm{Min}^{(\ell)}\, T$. Then $\pi = \sigma_\Gamma$ for some $\sigma \in T$ and $\Gamma \in \mathrm{Part}_\ell(n)$. Let $\Pi \in \mathrm{Part}_m(n)$ be a refinement of Γ. By Lemma 1.7.6, $\delta_\Pi(\Gamma) \in \mathrm{Part}_\ell(m)$ and $\Gamma = \Pi_{\delta_\Pi(\Gamma)}$. Lemma 1.7.8 yields $\sigma_\Gamma = \sigma_{\Pi_{\delta_\Pi(\Gamma)}} = (\sigma_\Pi)_{\delta_\Pi(\Gamma)}$. Then $\sigma_\Pi \in \mathrm{Min}^{(m)}\, \sigma$; hence $(\sigma_\Pi)_{\delta_\Pi(\Gamma)} \in \mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, \sigma \subseteq \mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, T$. Thus $\mathrm{Min}^{(\ell)}\, T \subseteq \mathrm{Min}^{(\ell)}\, \mathrm{Min}^{(m)}\, T$. We have shown that (4.2.3) holds.

We now prove (4.2.2). By the definition of Comp, the condition $\sigma \in \mathrm{Comp}^{(n)}\, \mathrm{Comp}^{(m)}\, S$ is equivalent to $\mathrm{Min}^{(m)}\, \sigma \subseteq \mathrm{Comp}^{(m)}\, S$. This

in turn is equivalent to $\mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,\sigma \subseteq S$. Since $\mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,\sigma = \mathrm{Min}^{(\ell)}\,\sigma$ by (4.2.3), we can rewrite the last condition as $\mathrm{Min}^{(\ell)}\,\sigma \subseteq S$, which is equivalent to $\sigma \in \mathrm{Comp}^{(n)}\,S$. Thus $\mathrm{Comp}^{(n)}\,\mathrm{Comp}^{(m)}\,S = \mathrm{Comp}^{(n)}\,S$.

Equality (4.2.4) follows from Proposition 4.2.1 and equality (4.2.2):

$$\begin{aligned}\mathrm{gComp}^{(n)}\,\mathrm{gComp}^{(m)}\,G &= \langle \mathrm{Comp}^{(n)} \langle \mathrm{Comp}^{(m)}\,G\rangle\rangle \\ &= \mathrm{Comp}^{(n)}\,\mathrm{Comp}^{(m)}\,G = \mathrm{Comp}^{(n)}\,G = \langle \mathrm{Comp}^{(n)}\,G\rangle \\ &= \mathrm{gComp}^{(n)}\,G.\end{aligned}$$

As for (4.2.5), the inclusion $\mathrm{gMin}^{(\ell)}\,H \subseteq \mathrm{gMin}^{(\ell)}\,\mathrm{gMin}^{(m)}\,H$ can be proved by making use of the monotonicity of $\mathrm{Min}^{(\ell)}$ and equality (4.2.3) as follows:

$$\begin{aligned}\mathrm{gMin}^{(\ell)}\,H = \langle \mathrm{Min}^{(\ell)}\,H\rangle &= \langle \mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,H\rangle \\ &\subseteq \langle \mathrm{Min}^{(\ell)} \langle \mathrm{Min}^{(m)}\,H\rangle\rangle = \mathrm{gMin}^{(\ell)}\,\mathrm{gMin}^{(m)}\,H.\end{aligned}$$

For the converse inclusion, let $\sigma \in \mathrm{gMin}^{(\ell)}\,\mathrm{gMin}^{(m)}\,H$. Then there exist permutations $\sigma^1, \sigma^2, \ldots, \sigma^p \in \mathrm{Min}^{(\ell)}\,\mathrm{gMin}^{(m)}\,H$ such that $\sigma = \sigma^1 \circ \sigma^2 \circ \cdots \circ \sigma^p$. This in turn means that, for each $i \in [p]$, there exists $\tau^i \in \mathrm{gMin}^{(m)}\,H$ such that $\sigma^i \leq \tau^i$. Consequently, for each $i \in [p]$, there exist $\tau^{i1}, \tau^{i2}, \ldots, \tau^{ij_i} \in \mathrm{Min}^{(m)}\,H$ such that $\tau^i = \tau^{i1} \circ \tau^{i2} \circ \cdots \circ \tau^{ij_i}$. Now, by applying Lemma 4.1.8(ii) and the monotonicity of $\mathrm{Min}^{(\ell)}$, we obtain, for every $i \in [p]$, that

$$\begin{aligned}\sigma^i \in \mathrm{Min}^{(\ell)}\,\tau^i &= \mathrm{Min}^{(\ell)}\,\tau^{i1}\tau^{i2}\cdots\tau^{ij_i} \\ &\subseteq (\mathrm{Min}^{(\ell)}\,\tau^{i1})(\mathrm{Min}^{(\ell)}\,\tau^{i2})\cdots(\mathrm{Min}^{(\ell)}\,\tau^{ij_i}) \\ &\subseteq (\mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,H)(\mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,H)\cdots(\mathrm{Min}^{(\ell)}\,\mathrm{Min}^{(m)}\,H) \\ &= (\mathrm{Min}^{(\ell)}\,H)(\mathrm{Min}^{(\ell)}\,H)\cdots(\mathrm{Min}^{(\ell)}\,H) \\ &\subseteq \langle \mathrm{Min}^{(\ell)}\,H\rangle = \mathrm{gMin}^{(\ell)}\,H.\end{aligned}$$

Since $\mathrm{gMin}^{(\ell)}\,H$ is a group, we have $\sigma = \sigma^1 \circ \cdots \circ \sigma^p \in \mathrm{gMin}^{(\ell)}\,H$. □

According to Proposition 4.2.4, it would be sufficient to describe $\mathrm{Min}^{(m-1)}\,S$ and $\mathrm{Comp}^{(m+1)}\,S$ for arbitrary m and $S \subseteq S_m$. Recursive application of such relations between consecutive levels of **P** would yield descriptions of $\mathrm{Min}^{(\ell)}\,S$ and $\mathrm{Comp}^{(n)}\,S$ for arbitrary ℓ, m, n with $\ell \leq m \leq n$ and $S \subseteq S_m$.

4.3 COMPRESSIONS AND EXPANSIONS OF INTERVAL PARTITIONS

We are going to define two simple transformations of interval partitions: compression and expansion. These transformations change the size of the underlying set of an interval partition while retaining

some essential information about its block structure. We will state and prove several lemmas that will be used later in the analysis of minors of permutations.

Definition 4.3.1. The *distance* between nonempty subsets B and C of $\mathbf{N}$, denoted $d(B, C)$ is the quantity $\min\{|b - c| : b \in B, c \in C\}$. Note that $d(B, C) = 0$ if and only if $B \cap C \neq \emptyset$. If $d(B, C) = 1$, then we say that B and C are *adjacent*.

Definition 4.3.2. Let $\Pi \in \mathrm{IntPart}(n)$ be an interval partition of $[n]$. For $n \geq 2$, the *compression* of Π is the partition $\Pi^{\downarrow} \in \mathrm{Part}(n-1)$ defined as $\Pi^{\downarrow} := \langle \mathcal{C}_\Pi \rangle_{\mathrm{part}}$ where

$$\mathcal{C}_\Pi := \{B \cap [n-1] : B \in \Pi\} \cup \{B - 1 : B \in \Pi,\, B \cap \{1, 2\} = \emptyset\}. \tag{4.3.1}$$

The *expansion* of Π is the partition $\Pi^{\uparrow} \in \mathrm{Part}(n+1)$ defined as follows:

$$1^{\uparrow} := 12, \quad 1|2^{\uparrow} := 1|23, \quad 12^{\uparrow} := 123,$$

and for $n \geq 3$, $\Pi^{\uparrow} := \langle \mathcal{E}_\Pi \rangle_{\mathrm{part}}$, where

$$\mathcal{E}_\Pi := \{2/\Pi, (n/\Pi) + 1\} \cup \{B \setminus \{\min B\} : B \in \Pi\}. \tag{4.3.2}$$

Note that since the elements of $\mathcal{C}_\Pi$ and $\mathcal{E}_\Pi$ are intervals, $\Pi^{\downarrow}$ and $\Pi^{\uparrow}$ are interval partitions by Fact 1.4.3.

For iterated compressions and expansions, we write, for $\ell \geq 1$,

$$\Pi^{\downarrow^1} := \Pi^{\downarrow}, \qquad \Pi^{\uparrow^1} := \Pi^{\uparrow},$$
$$\Pi^{\downarrow^{\ell+1}} := (\Pi^{\downarrow^\ell})^{\downarrow}, \qquad \Pi^{\uparrow^{\ell+1}} := (\Pi^{\uparrow^\ell})^{\uparrow},$$

whenever the right sides of the above expressions are defined.

Informally speaking, compression merges each nontrivial block of Π with the block that is adjacent to it to the left. Exceptionally, the block $2/\Pi$ is not merged with $1/\Pi$. Furthermore, after merging blocks, we must remove the element n from the block that contains it in order to obtain a partition of the set $[n-1]$. In expansion, nontrivial blocks get split into two blocks, one containing only the least element and the other containing all the remaining elements. Exceptionally, the block $1/\Pi$ is not split into two. Furthermore, we must adjoin the element $n+1$ to the block $(n/\Pi) \setminus \{\min(n/\Pi)\}$ in order to obtain a partition of the set $[n+1]$.

Example 4.3.3. In Table 8 we present two interval partitions of the set $\{1, \ldots, 12\}$ and a few iterated expansions and compressions thereof.

Lemma 4.3.4. *Let Π be an interval partition of $[n]$, and assume that $\Pi = \{B_1, \ldots, B_r\}$ with $B_1 <_\Pi B_2 <_\Pi \cdots <_\Pi B_r$. Then the following statements hold.*

$\Pi^{\uparrow^3}$	$= 1\,2\,3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10 \mid 11 \mid 12 \mid 13\,14\,15$
$\Pi^{\uparrow^2}$	$= 1\,2\,3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10 \mid 11 \mid 12\,13\,14$
$\Pi^{\uparrow}$	$= 1\,2\,3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8\,9 \mid 10 \mid 11\,12\,13$
Π	$= 1\,2\,3 \mid 4\,5 \mid 6 \mid 7\,8\,9 \mid 10\,11\,12$
$\Pi^{\downarrow}$	$= 1\,2\,3\,4\,5 \mid 6\,7\,8\,9\,10\,11$
$\Pi^{\downarrow^2}$	$= 1\,2\,3\,4\,5\,6\,7\,8\,9\,10$
$\Pi^{\downarrow^3}$	$= 1\,2\,3\,4\,5\,6\,7\,8\,9$
$\Pi^{\uparrow^3}$	$= 1 \mid 2\,3\,4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10 \mid 11 \mid 12 \mid 13 \mid 14 \mid 15$
$\Pi^{\uparrow^2}$	$= 1 \mid 2\,3\,4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9 \mid 10\,11 \mid 12 \mid 13 \mid 14$
$\Pi^{\uparrow}$	$= 1 \mid 2\,3\,4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9\,10\,11 \mid 12 \mid 13$
Π	$= 1 \mid 2\,3\,4 \mid 5 \mid 6 \mid 7 \mid 8\,9\,10\,11 \mid 12$
$\Pi^{\downarrow}$	$= 1 \mid 2\,3\,4 \mid 5 \mid 6 \mid 7\,8\,9\,10\,11$
$\Pi^{\downarrow^2}$	$= 1 \mid 2\,3\,4 \mid 5 \mid 6\,7\,8\,9\,10$
$\Pi^{\downarrow^3}$	$= 1 \mid 2\,3\,4 \mid 5\,6\,7\,8\,9$

Table 8: Compressions and expansions of interval partitions

(i) *A set* $C \subseteq [n+1]$ *with* $|C| \geq 2$ *is a block of* $\Pi^{\uparrow}$ *if and only if one of the following conditions is satisfied:*
   (a) $C = B \setminus \{\min B\}$ *for some* $B \in \Pi$ *satisfying* $|B| \geq 3$ *and* $\{2, n\} \cap B = \emptyset$.
   (b) $C = 2/\Pi$, $|2/\Pi| > 1$ *and* $n \notin 2/\Pi$.
   (c) $C = (n/\Pi) + 1$, $|n/\Pi| > 1$ *and* $2 \notin n/\Pi$.
   (d) $C = [n+1]$ *and* $[n] \in \Pi$.
   (e) $C = [2, n+1]$ *and* $[2, n] \in \Pi$.

(ii) *There are no adjacent nontrivial blocks in* $\Pi^{\uparrow}$.

(iii) *If a nontrivial block of* $\Pi^{\uparrow}$ *contains* n*, then it also contains* $n+1$.

(iv) *If a nontrivial block of* $\Pi^{\uparrow}$ *contains* 3*, then it also contains* 2.

(v) *A set* $C \subseteq [n-1]$ *with* $|C| \geq 2$ *is a block of* $\Pi^{\downarrow}$ *if and only if one of the following conditions is satisfied:*
   (a) $n \geq 3$, $C = B_r \cap [n-1]$ *and* $B_r = [1, n]$.
   (b) $n \geq 4$, $C = B_r \cap [n-1]$ *and* $B_r = [2, n]$.
   (c) $C = \bigcup_{i=p}^{q} (B_i \cup (B_{i+1} - 1))$ *for some* $p, q \in [r-1]$ *with* $p \leq q$ *and* $r > 1$ *such that*
      - $B_p = 2/\Pi$ *or* $|B_p| = 1$ *and* $B_p \neq \{1\}$.
      - $|B_i| > 1$ *for all* $i \in [p+1, q]$*, and*
      - *if* $|B_{q+1}| > 1$ *then* $B_{q+1} = n/\Pi$.

(vi) *Assume that* Π *has no adjacent nontrivial blocks. Then a set* $C \subseteq [n-1]$ *with* $|C| \geq 2$ *is a block of* $\Pi^{\downarrow}$ *if and only if one of the following conditions is satisfied:*

(a) $C = (2/\Pi) \cap [n-1]$ *and* $|2/\Pi| > 1$.
(b) $C = (B \cap [n-1]) \cup (B-1)$ *for some nontrivial block* $B \in \Pi$ *with* $2 \notin B$.

Proof. Straightforward verification. □

Lemma 4.3.5. *Let* Π *and* Γ *be interval partitions of* $[n]$. *If* Π *is a refinement of* Γ, *then* $\Pi^{\downarrow}$ *is a refinement of* $\Gamma^{\downarrow}$.

Proof. We are going to show that every set in $\mathcal{C}_\Pi$, as defined in (4.3.1), is a subset of some set in $\mathcal{C}_\Gamma$. Lemma 1.4.5 then implies that $\Pi^{\downarrow} = \langle \mathcal{C}_\Pi \rangle_{\mathrm{part}} \sqsubseteq \langle \mathcal{C}_\Gamma \rangle_{\mathrm{part}} = \Gamma^{\downarrow}$.

Let $S \in \mathcal{C}_\Pi$. Then there exists a block $B \in \Pi$ such that $S = B \cap [n-1]$ or $S = B - 1$ and $B \cap \{1,2\} = \emptyset$. Since $\Pi \sqsubseteq \Gamma$, there exists a block $C \in \Gamma$ such that $B \subseteq C$. Then $B \cap [n-1] \subseteq C \cap [n-1] \in \mathcal{C}_\Gamma$ and $B - 1 \subseteq C - 1$. If $C \cap \{1,2\} = \emptyset$, then $C - 1 \in \mathcal{C}_\Gamma$. If $C \cap \{1,2\} \neq \emptyset$ and $B \cap \{1,2\} = \emptyset$, then, since the blocks of Π and Γ are intervals, $B - 1 \subseteq C \cap [n-1] \in \mathcal{C}_\Gamma$. □

Lemma 4.3.6. *Let* Π *and* Γ *be interval partitions of* $[n]$. *If* Π *is a refinement of* Γ, *then* $\Pi^{\uparrow}$ *is a refinement of* $\Gamma^{\uparrow}$.

Proof. We are going to show that every set in $\mathcal{E}_\Pi$, as defined in (4.3.2), is a subset of some set in $\mathcal{E}_\Gamma$. Lemma 1.4.5 then implies that $\Pi^{\uparrow} = \langle \mathcal{E}_\Pi \rangle_{\mathrm{part}} \sqsubseteq \langle \mathcal{E}_\Gamma \rangle_{\mathrm{part}} = \Gamma^{\uparrow}$.

Let $S \in \mathcal{E}_\Pi$. The claim clearly holds for $S \in \{2/\Pi, (n/\Pi)+1\}$, because $2/\Pi \subseteq 2/\Gamma \in \mathcal{E}_\Gamma$ and $(n/\Pi)+1 \subseteq (n/\Gamma)+1 \in \mathcal{E}_\Gamma$. If $S = B \setminus \{\min B\}$ for some $B \in \Pi$, then there is $C \in \Gamma$ such that $B \subseteq C$, and we have $B \setminus \{\min B\} \subseteq C \setminus \{\min C\} \in \mathcal{E}_\Gamma$. □

Lemma 4.3.7. *Let* $n \geq 2$, *and let* Π *be an interval partition of* $[n]$. *Then the following statements hold.*

(i) Π *is a refinement of* $\Pi^{\downarrow\uparrow}$.

(ii) *Assume that* Π *is not a trivial partition,* Π *has no adjacent nontrivial blocks, for every nontrivial block* $B \in \Pi$ *we have* $B \subseteq [n-2]$ *or* $n \in B$, *and if* $3/\Pi$ *is nontrivial then* $2 \in 3/\Pi$. *Then* $\Pi = \Pi^{\downarrow\uparrow}$.

Proof. Statements (i) and (ii) are easily verified when $2 \leq n \leq 3$. If $n = 2$, then $\Pi = 1|2$ or $\Pi = 12$, and in either case, $\Pi^{\downarrow} = 1$ and $\Pi^{\downarrow\uparrow} = 12$. Consider then the case when $n = 3$. If $\Pi = 1|2|3$ or $\Pi = 1|23$, then $\Pi^{\downarrow} = 1|2$ and $\Pi^{\downarrow\uparrow} = 1|23$. If $\Pi = 12|3$ or $\Pi = 123$, then $\Pi^{\downarrow} = 12$ and $\Pi^{\downarrow\uparrow} = 123$. For the remainder of the proof, assume that $n \geq 4$.

(i) Let B be a Π-block. We need to show that B is included in some block of $\Pi^{\downarrow\uparrow}$. This is obviously the case when $|B| = 1$, so we may assume that B is nontrivial. We will consider different possibilities according to whether or not 2 and n are elements of B.

Assume first that $2 \in B$ and $n \in B$. Then $B \cap [n-1] \in \mathcal{C}_\Pi$, so there is $C \in \Pi^\downarrow$ such that $B \cap [n-1] \subseteq C$. Since B is an interval, the elements 2 and $n-1$ are contained in B and hence in C. Consequently, $\mathcal{E}_{\Pi^\downarrow}$ contains sets $2/\Pi^\downarrow = C$ and $((n-1)/\Pi^\downarrow)+1 = C+1$. Since $n \geq 4$, we have $|C| \geq 2$, so $C \cap (C+1) \neq \emptyset$. Therefore there is $D \in \Pi^{\downarrow\uparrow}$ such that $C \cup (C+1) \subseteq D$, and we have $B = (B \cap [n-1]) \cup \{n\} \subseteq C \cup (C+1) \subseteq D \in \Pi^{\downarrow\uparrow}$.

Assume then that $2 \in B$ and $n \notin B$. Then $B = B \cap [n-1] \in \mathcal{C}_\Pi$, so there is $C \in \Pi^\downarrow$ such that $B \subseteq C$. Hence $C = 2/\Pi^\downarrow \in \mathcal{E}_{\Pi^\downarrow}$. Therefore there is $D \in \Pi^{\downarrow\uparrow}$ such that $C \subseteq D$, and we have $B \subseteq C \subseteq D \in \Pi^{\downarrow\uparrow}$.

Assume then that $2 \notin B$ and $n \in B$. Then $B-1 \in \mathcal{C}_\Pi$, so there is $C \in \Pi^\downarrow$ such that $B-1 \subseteq C$. Since $n-1 \in B-1 \subseteq C$, we have $C+1 = ((n-1)/\Pi^\downarrow)+1 \in \mathcal{E}_{\Pi^\downarrow}$. Therefore there is $D \in \Pi^{\downarrow\uparrow}$ such that $C+1 \subseteq D$, and we have $B \subseteq C+1 \subseteq D \in \Pi^{\downarrow\uparrow}$.

Assume finally that $2 \notin B$ and $n \notin B$. Then $B \cap [n-1] = B$ and $B-1$ are elements of $\mathcal{C}_\Pi$, so there is $C \in \Pi^\downarrow$ such that $B \cup (B-1) \subseteq C$. Then $\mathcal{E}_{\Pi^\downarrow}$ contains $C \setminus \{\min C\}$. Therefore there is $D \in \Pi^{\downarrow\uparrow}$ such that $C \setminus \{\min C\} \subseteq D$. Since $\min C < \min B$, we have $B \subseteq C \setminus \{\min C\} \subseteq D \in \Pi^{\downarrow\uparrow}$.

(ii) We have $\Pi \sqsubseteq \Pi^{\downarrow\uparrow}$ by part (i), so it suffices to show $\Pi^{\downarrow\uparrow} \sqsubseteq \Pi$. Let $D \in \Pi^{\downarrow\uparrow}$. We need to show that D is included in some block of Π. This is obviously the case when $|D| = 1$, so we may assume that D is nontrivial.

Since $\Pi^{\downarrow\uparrow}$ is an interval partition, it follows from Lemma 4.3.4(iii) that either $D \subseteq [n-2]$ or $n \in D$. Consider first the case when $D \subseteq [n-2]$. Then Lemma 4.3.4(i) gives rise to two subcases.

Case 1: $D = 2/\Pi^\downarrow$ and $n-1 \notin 2/\Pi^\downarrow$. By Lemma 4.3.4(vi), either $2/\Pi^\downarrow = (2/\Pi) \cap [n-1] = 2/\Pi$ or $2/\Pi^\downarrow = (B \cap [n-1]) \cup (B-1)$ for some nontrivial block $B \in \Pi$ with $2 \notin B$. The latter is not possible, because $2 \notin B$ implies $3 \notin B$ by our hypotheses, and hence $2 \notin (B \cap [n-1]) \cup (B-1)$ yet $2 \in 2/\Pi^\downarrow$. Consequently, $D = 2/\Pi^\downarrow = 2/\Pi \in \Pi$.

Case 2: $D = C \setminus \{\min C\}$ for some $C \in \Pi^\downarrow$ with $\{2, n-1\} \cap C = \emptyset$. By Lemma 4.3.4(vi), either $C = (B \cap [n-1]) \cup (B-1)$ for some nontrivial block $B \in \Pi$ or $C = (2/\Pi) \cap [n-1] = 2/\Pi$. The latter is clearly not possible because $2 \notin C$. Since $n-1 \notin C$, we also have $n-1 \notin B$, so $(B \cap [n-1]) \cup (B-1) = B \cup \{\min B - 1\}$. Consequently, $D = C \setminus \{\min C\} = (B \cup \{\min B - 1\}) \setminus \{\min B - 1\} = B \in \Pi$.

Consider then the case when $n \in D$. Lemma 4.3.4(i) gives rise to two subcases.

Case 1: $D = ((n-1)/\Pi^\downarrow)+1$ and $2 \notin (n-1)/\Pi^\downarrow$. According to Lemma 4.3.4(vi) we have $(n-1)/\Pi^\downarrow = (B \cap [n-1]) \cup (B-1)$ for some nontrivial block $B \in \Pi$. Then $B \not\subseteq [n-2]$ because $n-1 \in B$, so our hypotheses imply that $n \in B$. Consequently,

$$\begin{aligned} D &= ((n-1)/\Pi^\downarrow)+1 = ((B \cap [n-1]) \cup (B-1))+1 \\ &= (B-1)+1 = B \in \Pi. \end{aligned}$$

Case 2: $D = \{1, \dots, n\}$ or $D = \{2, \dots, n\}$. Then we must have $C := D \cap [n-1] \in \Pi^{\downarrow}$. Lemma 4.3.4(vi) implies that $C = (2/\Pi) \cap [n-1]$; C cannot be of the form $(B \cap [n-1]) \cup (B-1)$ for some nontrivial $B \in \Pi$ with $2 \notin \Pi$, because our hypotheses would force $3 \notin B$, whence $2 \notin (B \cap [n-1]) \cup (B-1)$. Since $n-1 \in C \subseteq 2/\Pi$, we have $2/\Pi \nsubseteq [n-2]$, so our hypotheses imply that $n \in 2/\Pi$. Consequently, $D = 2/\Pi \in \Pi$. □

Lemma 4.3.8. *Let Π be an interval partition of $[n]$. Then the following statements hold.*

(i) *Every nontrivial block of $\Pi^{\uparrow\downarrow}$ is a block of Π. Consequently, $\Pi^{\uparrow\downarrow}$ is a refinement of Π.*

(ii) *If every two-element Π-block has a nonempty intersection with $\{2, n\}$, then $\Pi^{\uparrow\downarrow} = \Pi$.*

Proof. (i) Let D be a nontrivial block of $\Pi^{\uparrow\downarrow}$. By Lemma 4.3.4(ii), $\Pi^{\uparrow}$ has no adjacent nontrivial blocks. Therefore Lemma 4.3.4(vi) implies that $D = (2/\Pi^{\uparrow}) \cap [n]$ or $D = (C \cap [n]) \cup (C-1)$ for some nontrivial block $C \in \Pi^{\uparrow}$ with $2 \notin C$.

Consider first the case when $D = (2/\Pi^{\uparrow}) \cap [n]$. Lemma 4.3.4(i) gives rise to three subcases.

Case 1: $2/\Pi^{\uparrow} = 2/\Pi$ and $n \notin 2/\Pi$. Then $D = (2/\Pi^{\uparrow}) \cap [n] = 2/\Pi \in \Pi$.

Case 2: $2/\Pi^{\uparrow} = [n+1]$ and $[n] \in \Pi$. Then $D = [n] \in \Pi$.

Case 3: $2/\Pi^{\uparrow} = [2, n+1]$ and $[2, n] \in \Pi$. Then $D = [2, n] \in \Pi$.

Consider then the case when $D = (C \cap [n]) \cup (C-1)$ for some nontrivial block $C \in \Pi^{\uparrow}$ with $2 \notin C$. Lemma 4.3.4(i) gives rise to two subcases.

Case 1: $C = B \setminus \{\min B\}$ for some $B \in \Pi$ with $\{2, n\} \cap B = \emptyset$. Then $D = (B \setminus \{\min B\}) \cup \{\min B\} = B \in \Pi$.

Case 2: $C = (n/\Pi) + 1$ and $2 \notin n/\Pi$. Then

$$D = (((n/\Pi) + 1) \cap [n]) \cup (((n/\Pi) + 1) - 1) = n/\Pi \in \Pi.$$

We conclude that every nontrivial block of $\Pi^{\uparrow\downarrow}$ is a block of Π. Consequently, every block of $\Pi^{\uparrow\downarrow}$ is included in a block of Π, that is, $\Pi^{\uparrow\downarrow} \sqsubseteq \Pi$.

(ii) Under the assumption about the two-element blocks of Π, Lemma 4.3.4(i) provides a one-to-one correspondence between the nontrivial blocks of Π and those of $\Pi^{\uparrow}$. By Lemma 4.3.4(ii), $\Pi^{\uparrow}$ has no adjacent nontrivial blocks, so Lemma 4.3.4(vi) provides a one-to-one correspondence between the nontrivial blocks of $\Pi^{\uparrow}$ and those of $\Pi^{\uparrow\downarrow}$. It follows from part (i) that $\Pi^{\uparrow\downarrow}$ and Π have the same nontrivial blocks; hence $\Pi^{\uparrow\downarrow} = \Pi$. □

Definition 4.3.9. Let Π be an interval partition of $[n]$. If Π has at least two nontrivial blocks, then the *minimum distance between nontrivial* Π*-blocks,* denoted $\mu(\Pi)$, is

$$\min\{d(B,C) : B,C \in \Pi,\ B \neq C,\ |B| \geq 2,\ |C| \geq 2\};$$

otherwise $\mu(\Pi) := \infty$.

Lemma 4.3.10. *Let Π be an interval partition of $[n]$. Then the following statements hold.*

(i) $\mu(\Pi^{\uparrow}) \geq \mu(\Pi) + 1$.

(ii) *If $\mu(\Pi) \geq 2$, then $\mu(\Pi^{\downarrow}) = \mu(\Pi) - 1$.*

Proof. (i) Assume that B and C are nontrivial blocks of $\Pi^{\uparrow}$ such that $B <_{\Pi} C$. Then there exist Π-blocks B' and C' such that $B = B'$ or $B = B' \setminus \{\min B'\}$ and $C = C' \setminus \{\min C'\}$ or $C = C' + 1$. Then $\max B = \max B'$ and $\min C = \min C' + 1$. Therefore, $d(B,C) = d(B',C') + 1$. Consequently, the inequality $\mu(\Pi^{\uparrow}) \geq \mu(\Pi) + 1$ holds.[2]

(ii) Since Π has no adjacent nontrivial blocks, Lemma 4.3.4(vi) provides a one-to-one correspondence between the nontrivial blocks of Π and those of $\Pi^{\downarrow}$. Assume that B and C are nontrivial blocks of $\Pi^{\downarrow}$ such that $B <_{\Pi} C$. Then there exist nontrivial blocks $B', C' \in \Pi$ such that $B = B'$ or $B = B' \cup (B' - 1)$, and $C = C' \cup (C' - 1)$ or $C = C' - 1$. Then $\max B' = \max B$ and $\min C' = \min C - 1$, so $d(B,C) = d(B',C') - 1$. Consequently, $\mu(\Pi^{\downarrow}) = \mu(\Pi) - 1$. □

Lemma 4.3.11. *Let $k, \ell \in \mathbf{N}_+$. Let Π be an interval partition of $[k+\ell]$. Then $\Pi = \Gamma^{\uparrow^{\ell}}$ for some interval partition Γ of $[k]$ if and only if*

- $\mu(\Pi) \geq \ell + 1$,
- *for every nontrivial $B \in \Pi$, either $B \subseteq [k-1]$ or $k + \ell \in B$, and*
- *for every nontrivial $B \in \Pi$, either $\min B \geq \ell + 3$ or $2 \in B$.*

Proof. For necessity, assume that $\Pi = \Gamma^{\uparrow^{\ell}}$ for some $\Gamma \in \mathrm{IntPart}(k)$. It follows from Lemma 4.3.10 that $\mu(\Pi) = \mu(\Gamma^{\uparrow^{\ell}}) \geq \mu(\Gamma) + \ell \geq \ell + 1$. An easy inductive proof based on Lemma 4.3.4(i) shows that if B is a nontrivial block of $\Gamma^{\uparrow^{\ell}}$ then either $B \subseteq [k-1]$ or $k + \ell \in B$ and either $\min B \geq \ell + 3$ or $2 \in B$.

For sufficiency, we claim that if $\Pi \in \mathrm{IntPart}(k+\ell)$ satisfies the conditions of the lemma, then $\Pi = \Pi^{\downarrow^{\ell}\uparrow^{\ell}}$. Thus the theorem holds if we choose $\Gamma := \Pi^{\downarrow^{\ell}}$. We prove the claim by induction on ℓ. If $\ell = 1$, then the conditions of Lemma 4.3.7(ii) are satisfied with $n = k + 1$, so we have $\Pi = \Pi^{\downarrow\uparrow}$. Assume then that the claim holds for

2 Note that the inequality may hold as a strict inequality, because it is possible that there exists a nontrivial block $D' \in \Pi$ such that $B' < D' < C'$ but there is no nontrivial block $D \in \Pi^{\uparrow}$ such that $B < D < C$. This happens when $|D'| = 2$; in this case the block D' is split into singletons when we expand Π.

$\ell = m$ ($m \geq 1$). Let Π be an interval partition of $[k+m+1]$ such that $\mu(\Pi) \geq m+2$ and every nontrivial $B \in \Pi$ satisfies either $B \subseteq [k-1]$ or $k+m+1 \in B$, and either $\min B \geq m+4$ or $2 \in B$. The conditions of Lemma 4.3.7(ii) are satisfied with $n = k+m+1$, so we have $\Pi = \Pi^{\downarrow\uparrow}$. By Lemma 4.3.10, $\mu(\Pi^{\downarrow}) = \mu(\Pi) - 1 \geq m+1$. It is clear that every nontrivial $B \in \Pi^{\downarrow}$ satisfies either $B \subseteq [k-1]$ or $k+m \in B$, and either $\min B \geq m+3$ or $2 \in B$. By the inductive hypothesis, $\Pi^{\downarrow} = (\Pi^{\downarrow})^{\downarrow^m\uparrow^m}$. Thus, $\Pi = \Pi^{\downarrow\uparrow} = ((\Pi^{\downarrow})^{\downarrow^m\uparrow^m})^{\uparrow} = \Pi^{\downarrow^{m+1}\uparrow^{m+1}}$. □

4.4 ON GROUPS GENERATED BY MINORS AND THEIR DIFFERENCES

We develop some results concerning the groups generated by the set of ℓ-minors of an n-permutation τ and by the set of differences of ℓ-minors of τ. Due to the transitive property of the operator $\mathrm{gMin}^{(\ell)}$ (see Proposition 4.2.4), the special case $\ell = n-1$ is of particular importance.

4.4.1 *Special permutations θ_n and λ_k^ℓ*

In what follows, the permutations θ_n and λ_k^ℓ defined below play a very special role.

Definition 4.4.1. For $n \geq 2$, the permutation $\theta_n \in S_n$ is the following product of $\lfloor n/2 \rfloor$ disjoint adjacent transpositions:

$$\theta_n := \begin{cases} (1\ 2)(3\ 4)\cdots(n-1\ \ n), & \text{if } n \text{ is even,} \\ (2\ 3)(4\ 5)\cdots(n-1\ \ n), & \text{if } n \text{ is odd.} \end{cases}$$

If $1 \leq \ell \leq k$ and $\ell \equiv k \pmod 2$, then the permutation $\lambda_k^\ell \in S_k$ is defined as follows:

$$\lambda_k^\ell := \begin{cases} (1\ 2)(3\ 4)\cdots(\ell-2\ \ \ell-1)(\ell+1\ \ \ell+2)\cdots(k-1\ \ k), \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k \text{ is odd,} \\ (2\ 3)(4\ 5)\cdots(\ell-2\ \ \ell-1)(\ell+1\ \ \ell+2)\cdots(k-1\ \ k), \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } k \text{ is even.} \end{cases}$$

Remark 4.4.2. Note that θ_n is an even permutation if and only if $n \equiv 0, 1 \pmod 4$. Note also that λ_{n-1}^ℓ has parity opposite to that of θ_n.

Fact 4.4.3. Let $I = \{i, j\} \in \binom{[n]}{2}$ with $i < j$. Then $(\theta_n)_I = \lambda_{n-1}^\ell$, where ℓ is the unique element of $\{j-1, j\}$ that is congruent to $n-1$ modulo 2.

4.4.2 *Invariant interval partitions*

Recall the notions of invariant relation and polymorphism from Section 2.7. Since a partition of $[n]$ is a collection of subsets of $[n]$ and

subsets of $[n]$ are unary relations on $[n]$, it makes perfect sense to speak of polymorphisms of a partition. A unary polymorphism is usually called an *endomorphism,* and a bijective endomorphism is an *automorphism.* In particular, a permutation $\sigma \in S_n$ preserves a subset $S \subseteq [n]$ if and only if $\sigma(i) \in S$ for all $i \in S$, and σ is an automorphism of a partition $\Pi \in \mathrm{Part}(n)$ if and only if σ preserves every block of Π. We denote the set of all automorphisms of a relation ρ by $\operatorname{Aut}\rho$.

Remark 4.4.4. Note that the automorphisms of a partition Π and the automorphisms of its associated equivalence relation $\equiv_\Pi$ are not in general the same. Namely, a permutation $\sigma \in S_n$ preserves $\Pi \in \mathrm{Part}(n)$ if and only if $\sigma(B) = B$ for every $B \in \Pi$, and σ preserves $\equiv_\Pi$ if and only if $\sigma(B) \in \Pi$ for every $B \in \Pi$. It thus holds that $\operatorname{Aut}\Pi \subseteq \operatorname{Aut}\equiv_\Pi$, and the inclusion holds as an equality if and only if the blocks of Π are of pairwise distinct sizes.

The *finest invariant interval partition* of a permutation $\sigma \in S_n$, denoted $\mathrm{fiip}(\sigma)$, is the finest interval partition of $[n]$ that is preserved by σ. (The fact that $\mathrm{fiip}(\sigma)$ is uniquely defined is an easy consequence of the fact that $\mathrm{IntPart}(n)$ is a closure system.)

Example 4.4.5. The finest invariant interval partitions of some permutations of the set $\{1, \ldots, 7\}$ are shown below.

σ	$\mathrm{fiip}(\sigma)$
1234567	1|2|3|4|5|6|7
1235647	1|2|3|456|7
1325476	1|23|45|67
2134765	12|3|4|567
4317625	1234567
7234561	1234567

Fact 4.4.6. Let $\sigma \in S_n$.

(i) All blocks of $\mathrm{fiip}(\sigma)$ have cardinality 2 if and only if n is even and $\sigma = \theta_n$.

(ii) The singleton $\{1\}$ is a block of $\mathrm{fiip}(\sigma)$ and all remaining blocks of $\mathrm{fiip}(\sigma)$ have cardinality 2 if and only if n is odd and $\sigma = \theta_n$.

4.4.3 *Group generated by the minors of a permutation*

Lemma 4.4.7. *Let $\sigma \in S_n$, and let $\Pi := \mathrm{fiip}(\sigma)$. Then σ_I preserves $\Pi^\downarrow$ for every $I \in \binom{[n]}{2}$. In other words,* $\mathrm{Min}^{(n-1)}\,\sigma \subseteq S_{\Pi^\downarrow}$. *Consequently,* $\langle \mathrm{Min}^{(n-1)}\,\sigma \rangle \subseteq S_{\Pi^\downarrow}$.

Proof. Let $\Pi = \{B_1, \ldots, B_r\}$ with $B_p <_\Pi B_q$ whenever $p < q$. Assume that $I = \{i, j\}$, with $i < j$, and assume that $i \in B_\alpha$ and $j \in B_\beta$. It

is clear that $\alpha \leq \beta$. It is easy to see that $\mathrm{fiip}(\sigma_I)$ comprises the following blocks: B_ℓ for every $\ell < \beta$, $B_\ell - 1$ for every $\ell > \beta$, and some blocks obtained by partitioning $B_\beta \setminus \{\max B_\beta\}$ (provided this set is nonempty). The partition $\Pi^\downarrow$ is a coarsening of $\mathrm{fiip}(\sigma_I)$, and hence σ_I preserves $\Pi^\downarrow$. It thus follows from the definition of $\mathrm{Min}^{(n-1)}\,\sigma$ that $\mathrm{Min}^{(n-1)}\,\sigma \subseteq S_{\Pi^\downarrow}$. The last claim follows from the fact that $S_{\Pi^\downarrow}$ is a permutation group. □

Lemma 4.4.8. *Let Π be an interval partition of $[n]$. For every $\sigma \in S_\Pi$ and for every $I \in \binom{[n]}{2}$, it holds that $\sigma_I \in S_{\Pi^\downarrow}$, and hence $\mathrm{Min}^{(n-1)}\,S_\Pi \subseteq S_{\Pi^\downarrow}$.*

Proof. Let $\Gamma := \mathrm{fiip}(\sigma)$. Since $\sigma \triangleright \Pi$, we have, by the definition of the finest invariant interval partition, that $\Gamma \sqsubseteq \Pi$. For every $I \in \binom{[n]}{2}$, $\sigma_I \triangleright \Gamma^\downarrow$ by Lemma 4.4.7, and since $\Gamma^\downarrow \sqsubseteq \Pi^\downarrow$ by Lemma 4.3.5, it holds that $\sigma_I \triangleright \Pi^\downarrow$, i.e., $\sigma_I \in S_{\Pi^\downarrow}$. Thus $\mathrm{Min}^{(n-1)}\,S_\Pi \subseteq S_{\Pi^\downarrow}$. □

Lemma 4.4.9. *Let Π be an interval partition of $[n]$. Then $\mathrm{Comp}^{(n+1)}\,S_\Pi = S_{\Pi^\uparrow}$.*

Proof. The claim clearly holds if $\Pi = \{[n]\}$ and hence $\Pi^\uparrow = \{[n+1]\}$, or if $\Pi = \{\{1\},[2,n]\}$ and hence $\Pi^\uparrow = \{\{1\},[2,n+1]\}$ so we may assume that $2 \not\equiv_\Pi n$. Consequently $1/\Pi = 1/\Pi^\uparrow$ and $2/\Pi = 2/\Pi^\uparrow$.

If $\sigma \in S_{\Pi^\uparrow}$, then $\mathrm{Min}^{(n)}\,\sigma \subseteq S_{\Pi^{\uparrow\downarrow}}$ by Lemma 4.4.8, because $\Pi^\uparrow$ is an interval partition. Since $\Pi^{\uparrow\downarrow} \sqsubseteq \Pi$ by Lemma 4.3.8, we have $S_{\Pi^{\uparrow\downarrow}} \subseteq S_\Pi$ (see Definition 1.6.1). Therefore $\sigma \in \mathrm{Comp}^{(n+1)}\,S_\Pi$. We have shown $S_{\Pi^\uparrow} \subseteq \mathrm{Comp}^{(n+1)}\,S_\Pi$.

In order to show that the converse inclusion $\mathrm{Comp}^{(n+1)}\,S_\Pi \subseteq S_{\Pi^\uparrow}$ holds, we prove that $\sigma \notin S_{\Pi^\uparrow}$ implies $\sigma \notin \mathrm{Comp}^{(n+1)}\,S_\Pi$. Thus, assume that $\sigma \notin S_{\Pi^\uparrow}$. Then there is an element $i \in [n+1]$ such that $\sigma(i) \notin i/\Pi^\uparrow$; let α be the smallest i with this property. Then necessarily $\sigma(\alpha) > \alpha$. This means that $n+1 \notin \alpha/\Pi^\uparrow$, so $\alpha/\Pi^\uparrow \subseteq [n-1]$ by Lemma 4.3.4(iii). We will split the analysis in three different cases, depending on whether α is contained in the $\Pi^\uparrow$-block of 1 or 2, or in neither.

Assume first that $\alpha \in 1/\Pi^\uparrow$. Since $\alpha/\Pi^\uparrow \subseteq [n-1]$, there are at least two elements in $[n+1] \setminus 1/\Pi^\uparrow$. Let $\gamma \in [n+1] \setminus (1/\Pi^\uparrow \cup \{\sigma(\alpha)\})$. Then for $I := \{\sigma(\alpha), \gamma\}$ we have $\sigma_I(\alpha) = \min(\sigma(\alpha),\gamma) \notin 1/\Pi^\uparrow = 1/\Pi = \alpha/\Pi$.

Assume then that $\alpha \notin 1/\Pi^\uparrow$ and $\alpha \in 2/\Pi^\uparrow$. Then it clearly holds that $1/\Pi = 1/\Pi^\uparrow = \{1\}$ and $\sigma(1) = 1$. Since $\alpha/\Pi^\uparrow \subseteq [n-1]$, the set $[n+1] \setminus (\{1\} \cup 2/\Pi^\uparrow)$ contains at least two elements. Let $\gamma \in [n+1] \setminus (\{1\} \cup 2/\Pi^\uparrow \cup \{\sigma(\alpha)\})$. Then for $I := \{\sigma(\alpha), \gamma\}$ we have $\sigma_I(\alpha) = \min(\sigma(\alpha),\gamma) \notin 2/\Pi^\uparrow = 2/\Pi = \alpha/\Pi$.

Finally, assume that $\alpha \notin 1/\Pi^\uparrow$ and $\alpha \notin 2/\Pi^\uparrow$. Then $\alpha \geq 3$ and the permutation σ maps each one of the blocks $1/\Pi^\uparrow$ and $2/\Pi^\uparrow$ onto itself. If $\alpha - 1 \not\equiv_\Pi \sigma(\alpha) - 1$, then for $I := \{1,2\}$ we have $\sigma_I(\alpha-1) = \sigma(\alpha) - 1 \notin (\alpha-1)/\Pi$. Assume that $\alpha - 1 \equiv_\Pi \sigma(\alpha) - 1$. Since $\alpha < \sigma(\alpha)$, this implies that α/Π is an interval that contains $\alpha - 1$ and $\sigma(\alpha) - 1$.

At the same time, we must have $\sigma(\alpha) \notin \alpha/\Pi$, because otherwise Lemma 4.3.4(i), together with the fact that $\alpha/\Pi^{\uparrow} \subseteq [n-1]$, would yield $\sigma(\alpha) \in (\alpha/\Pi) \setminus \{\min \alpha/\Pi\} = \alpha/\Pi^{\uparrow}$, contradicting the choice of α. It follows that $\sigma(\alpha) \leq n$. Consequently, $\sigma(\alpha)+1 = \sigma(\beta)$ for some $\beta > \alpha$. Then for $I = \{\sigma(\alpha), \sigma(\alpha)+1\}$ we have $\sigma_I(\alpha) = \sigma(\alpha) \notin \alpha/\Pi$.

In each case we have found a minor σ_I of σ such that $\sigma_I \notin S_\Pi$. Therefore $\sigma \notin \mathrm{Comp}^{(n+1)} S_\Pi$. □

Lemma 4.4.10. *Let Π be an interval partition of $[n]$, and let $\sigma \in S_{n+1}$. Then $\mathrm{Min}^{(n)} \sigma \subseteq S_\Pi$ if and only if $\sigma \in S_{\Pi^{\uparrow}}$.*

Proof. By definition, the condition $\mathrm{Min}^{(n)} \sigma \subseteq S_\Pi$ is equivalent to $\sigma \in \mathrm{Comp}^{(n+1)} S_\Pi$, and we have $\mathrm{Comp}^{(n+1)} S_\Pi = S_{\Pi^{\uparrow}}$ by Lemma 4.4.9. □

4.4.4 *Group generated by the differences of minors of a permutation*

For any set $S \subseteq S_n$ of n-permutations, let $\Delta S := \{\pi^{-1} \circ \tau : \pi, \tau \in S\}$ be the set of differences (or quotients) between elements of S. We are going to determine the permutations $\sigma \in S_n$ for which the sets $\mathrm{Min}^{(\ell)} \sigma$ and $\langle \Delta \mathrm{Min}^{(\ell)} \rangle$ have a nonempty intersection. To this end, we first determine $\langle \mathrm{Min}^{(n-1)} \sigma \rangle$ and $\langle \Delta \mathrm{Min}^{(n-1)} \rangle$. The general case then follows from the "transitive property" (Proposition 4.2.4). We start with several auxiliary lemmas.

Lemma 4.4.11. *Let $\sigma \in S_n$ and $p, q, r, s \in [n]$.*

(i) *If $p < q < r$ and $\sigma(p) > \sigma(x)$ for $x \in \{q, r\}$, then $(p\ q\ \cdots\ r-1) \in \Delta \mathrm{Min}^{(n-1)} \sigma$.*

(ii) *If $p < q < r-1$ and $\sigma(p) > \sigma(x)$ for $x \in \{q, q+1, r\}$, then $S_{\{p,q,\ldots,r-1\}} \subseteq \langle \Delta \mathrm{Min}^{(n-1)} \sigma \rangle$.*

(iii) *If $p < q < r$ and $\sigma(q) > \sigma(x)$ for $x \in \{p, r\}$, then $(q\ \cdots\ r-1) \in \Delta \mathrm{Min}^{(n-1)} \sigma$.*

(iv) *If $p < q < r$ and $\sigma(p) > \sigma(r)$ and $\sigma(q) = \sigma(p)+1$, then $S_{\{p,q,\ldots,r-1\}} \subseteq \langle \Delta \mathrm{Min}^{(n-1)} \sigma \rangle$.*

(v) *If $p < q < r$ and $\sigma(p) > \sigma(q)$ and $\sigma(r) = \sigma(p)+1$, then $(p\ q\ \cdots\ r-1) \in \Delta \mathrm{Min}^{(n-1)} \sigma$.*

(vi) *If $p < q < r < s$ and $\sigma(p) > \sigma(x)$ for $x \in \{q, s\}$ and $\sigma(r) = \sigma(p)+1$, then $S_{\{p,q,\ldots,s-1\}} \subseteq \langle \Delta \mathrm{Min}^{(n-1)} \sigma \rangle$.*

(vii) *If $p < q$ and $\sigma(p) < \sigma(q)$ and $\sigma(q+1) = \sigma(q)+2$ and $\sigma(q+2) = \sigma(q)+1$, then $(q\ q+1) \in \Delta \mathrm{Min}^{(n-1)} \sigma$.*

(viii) *If $p < q < r$ and $\sigma(p) < \sigma(q) = \sigma(r)-1$, then $(q\ \cdots\ r-1) \in \Delta \mathrm{Min}^{(n-1)} \sigma$.*

Proof. In this proof, we are going to designate the values of σ at certain points by the Greek letters α, β, γ. These are always chosen in such a way that α is the largest number among α, β, γ.

For strings $\mathbf{a}, \mathbf{b} \in \mathbf{N}^\sharp$ of numbers without repetitions, we write $\mathbf{a} \approx \mathbf{b}$ if $\mathbf{a}$ and $\mathbf{b}$ are order-isomorphic, i.e., the entries of $\mathbf{a}$ and $\mathbf{b}$ appear in the same relative order of magnitude.

(i) Write $\alpha := \sigma(p)$, $\beta := \sigma(q)$, $\gamma := \sigma(r)$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1} \alpha \sigma_{p+1} \dots \sigma_{q-1} \beta \sigma_{q+1} \dots \sigma_{r-1} \gamma \sigma_{r+1} \dots \sigma_n.$$

Since $\alpha > \beta$ and $\alpha > \gamma$, we have

$$\begin{array}{rl} \sigma_{\alpha\beta} \approx & \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} \sigma_{q+1} \sigma_{q+2} \dots \sigma_{r-1} \;\; \gamma \;\; \sigma_{r+1} \dots \sigma_n, \\ \sigma_{\alpha\gamma} \approx & \sigma_1 \dots \sigma_{p-1} \gamma \sigma_{p+1} \dots \sigma_{q-1} \;\; \beta \;\; \sigma_{q+1} \dots \sigma_{r-2} \sigma_{r-1} \sigma_{r+1} \dots \sigma_n. \\ & \quad\;\; \uparrow \qquad\qquad\;\; \uparrow \qquad\qquad\qquad\;\; \uparrow \\ & \quad\;\; p \qquad\qquad\;\; q \qquad\qquad\qquad\;\; r-1 \end{array}$$

Thus $\sigma_{\alpha\gamma}^{-1} \circ \sigma_{\alpha\beta} = (p \; q \; q+1 \; \cdots \; r-1)$.

(ii) It follows from part (i) that $\Delta\,\mathrm{Min}^{(n-1)}\,\sigma$ contains the permutations $(p \;\; q \;\; \cdots \;\; r-1)$ and $(p \;\; q+1 \;\; \cdots \;\; r-1)$, which constitute a generating set of $S_{\{p,q,\dots,r-1\}}$.

(iii) Write $\beta := \sigma(p)$, $\alpha := \sigma(q)$, $\gamma := \sigma(r)$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} \alpha \sigma_{q+1} \dots \sigma_{r-1} \gamma \sigma_{r+1} \dots \sigma_n.$$

Since $\alpha > \beta$ and $\alpha > \gamma$, we have

$$\begin{array}{rl} \sigma_{\alpha\beta} \approx & \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} \sigma_{q+1} \sigma_{q+2} \dots \sigma_{r-1} \;\; \gamma \;\; \sigma_{r+1} \dots \sigma_n, \\ \sigma_{\alpha\gamma} \approx & \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} \;\; \gamma \;\; \sigma_{q+1} \dots \sigma_{r-2} \sigma_{r-1} \sigma_{r+1} \dots \sigma_n. \\ & \quad\;\; \uparrow \qquad\qquad\;\; \uparrow \qquad\qquad\qquad\;\; \uparrow \\ & \quad\;\; p \qquad\qquad\;\; q \qquad\qquad\qquad\;\; r-1 \end{array}$$

Thus $\sigma_{\alpha\gamma}^{-1} \circ \sigma_{\alpha\beta} = (q \; q+1 \; \cdots \; r-1)$.

(iv) Write $\alpha := \sigma(p)$, $\beta := \sigma(r)$; then $\sigma(q) = \alpha + 1$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1} \alpha \sigma_{p+1} \dots \sigma_{q-1} (\alpha+1) \sigma_{q+1} \dots \sigma_{r-1} \beta \sigma_{r+1} \dots \sigma_n.$$

Since $\alpha > \beta$ we have

$$\begin{array}{rl} \sigma_{\alpha(\alpha+1)} \approx & \sigma_1 \dots \sigma_{p-1} \alpha \sigma_{p+1} \dots \sigma_{q-1} \;\; \sigma_{q+1} \;\; \sigma_{q+2} \dots \sigma_{r-1} \;\; \beta \;\; \sigma_{r+1} \dots \sigma_n, \\ \sigma_{\alpha\beta} \approx & \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} (\alpha+1) \sigma_{q+1} \dots \sigma_{r-2} \sigma_{r-1} \sigma_{r+1} \dots \sigma_n \\ \approx & \sigma_1 \dots \sigma_{p-1} \beta \sigma_{p+1} \dots \sigma_{q-1} \;\; \alpha \;\; \sigma_{q+1} \dots \sigma_{r-2} \sigma_{r-1} \sigma_{r+1} \dots \sigma_n. \\ & \quad\;\; \uparrow \qquad\qquad\;\; \uparrow \qquad\qquad\qquad\;\; \uparrow \\ & \quad\;\; p \qquad\qquad\;\; q \qquad\qquad\qquad\;\; r-1 \end{array}$$

Thus $\sigma_{\alpha\beta}^{-1} \circ \sigma_{\alpha(\alpha+1)} = (p \; q \; q+1 \; \cdots \; r-1) \in \Delta\,\mathrm{Min}^{(n-1)}\,\sigma$. By part (iii), $\Delta\,\mathrm{Min}^{(n-1)}$ also contains $(q \;\; \cdots \;\; r-1)$. These permutations constitute a generating set of $S_{\{p,q,\dots,r-1\}}$.

(v) Write $\alpha := \sigma(p)$, $\beta := \sigma(q)$; then $\sigma(r) = \alpha + 1$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1} \alpha \sigma_{p+1} \dots \sigma_{q-1} \beta \sigma_{q+1} \dots \sigma_{r-1} (\alpha+1) \sigma_{r+1} \dots \sigma_n.$$

Since $\alpha > \beta$, we have

$$\begin{aligned}
\sigma_{\alpha\beta} &\approx \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}\sigma_{q+1}\sigma_{q+2}\dots\sigma_{r-1}(\alpha+1)\sigma_{r+1}\dots\sigma_n \\
&\approx \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}\sigma_{q+1}\sigma_{q+2}\dots\sigma_{r-1}\ \ \alpha\ \ \sigma_{r+1}\dots\sigma_n, \\
\sigma_{\alpha(\alpha+1)} &\approx \sigma_1 \dots \sigma_{p-1}\alpha\sigma_{p+1}\dots\sigma_{q-1}\ \ \beta\ \ \sigma_{q+1}\dots\sigma_{r-2}\ \ \sigma_{r-1}\ \ \sigma_{r+1}\dots\sigma_n. \\
&\qquad\qquad\ \uparrow_{p} \qquad\qquad\ \uparrow_{q} \qquad\qquad\ \uparrow_{r-1}
\end{aligned}$$

Thus $\sigma_{\alpha(\alpha+1)}^{-1} \circ \sigma_{\alpha\beta} = (p\ q\ q+1\ \cdots\ r-1)$.

(vi) By part (iv), $S_{\{p,r,\dots,s-1\}} \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$; in particular $(p\ r) \in \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$. By part (v), $(p\ q\ \cdots\ r-1) \in \Delta\,\mathrm{Min}^{(n-1)}\,\sigma$. The claim then follows, because $\langle (p\ r), (p\ q\ \cdots\ r-1)\rangle = S_{\{p,q,\dots,r\}}$, and $S_{\{p,r,\dots,s-1\}}$ and $S_{\{p,q,\dots,r\}}$ generate $S_{\{p,q,\dots,s-1\}}$.

(vii) Write $\beta := \sigma(p)$, $\alpha := \sigma(q)$; then we have $\sigma(q+1) = \alpha+2$ and $\sigma(q+2) = \alpha+1$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}\alpha(\alpha+2)(\alpha+1)\sigma_{q+3}\dots\sigma_n.$$

Since $\alpha > \beta$, we have

$$\begin{aligned}
\sigma_{\alpha\beta} &\approx \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}(\alpha+2)(\alpha+1)\sigma_{q+3}\dots\sigma_n \\
&\approx \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}(\alpha+2)\ \ \alpha\ \ \sigma_{q+3}\dots\sigma_n, \\
\sigma_{\beta(\alpha+1)} &\approx \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}\ \ \alpha\ \ (\alpha+2)\sigma_{q+3}\dots\sigma_n. \\
&\qquad\qquad\ \uparrow_{p} \qquad\qquad\ \uparrow_{q} \quad\ \uparrow_{q+1}
\end{aligned}$$

Thus $\sigma_{\beta(\alpha+1)}^{-1} \circ \sigma_{\alpha\beta} = (q\ q+1)$.

(viii) Write $\beta := \sigma(p)$, $\alpha := \sigma(q)$; then $\sigma(r) = \alpha+1$. Then

$$\sigma = \sigma_1 \dots \sigma_{p-1}\beta\sigma_{p+1}\dots\sigma_{q-1}\alpha\sigma_{q+1}\dots\sigma_{r-1}(\alpha+1)\sigma_{r+1}\dots\sigma_n,$$

and we have

$$\begin{aligned}
\sigma_{\alpha\beta} &\approx \sigma_1 \dots \sigma_{q-1}\sigma_{q+1}\sigma_{q+2}\dots\sigma_{r-1}(\alpha+1)\sigma_{r+1}\dots\sigma_n \\
&\approx \sigma_1 \dots \sigma_{q-1}\sigma_{q+1}\sigma_{q+2}\dots\sigma_{r-1}\ \ \alpha\ \ \sigma_{r+1}\dots\sigma_n, \\
\sigma_{\alpha(\alpha+1)} &\approx \sigma_1 \dots \sigma_{q-1}\ \ \alpha\ \ \sigma_{q+1}\dots\sigma_{r-2}\ \ \sigma_{r-1}\ \ \sigma_{r+1}\dots\sigma_n. \\
&\qquad\qquad\ \uparrow_{q} \qquad\qquad\ \uparrow_{r-1}
\end{aligned}$$

Thus $\sigma_{\alpha(\alpha+1)}^{-1} \circ \sigma_{\alpha\beta} = (q\ \cdots\ r-1)$. □

Let $\sigma \in S_n$. If $\sigma(i) > \sigma(j)$ for all $j \in [i-1]$, then we say that $\sigma(i)$ is a *left-to-right maximum* and i is its *position.*

Lemma 4.4.12. *Let $\sigma \in S_n$. Then for every $B \in \mathrm{fiip}(\sigma)$, we have $S_{B\setminus\{\max B\}} \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$.*

Proof. Let $B \in \mathrm{fiip}(\sigma)$, say $B = [a,b]$. The claim is trivial if $|B| \le 2$, so we assume that $|B| \ge 3$.

Let $m_1, \dots, m_s$ be the positions of the left-to-right maxima in B, with $m_1 < m_2 < \cdots < m_s$. (Hence $\sigma(m_1) < \sigma(m_2) < \cdots < \sigma(m_s)$.) Let us make three observations.

Observation 1: For every $i \in [n]$, $\sigma(m_i) > m_i$. (For, otherwise $a \le \sigma(j) \le \sigma(m_i) \le m_i$ for all $j \in [a, m_i]$, from which it follows that $\sigma(m_i) = m_i$ and $\sigma \triangleright [a, m_i - 1]$ and hence also $\sigma \triangleright [m_i + 1, b]$. Therefore σ preserves the partition obtained from $\mathrm{fiip}(\sigma)$ by splitting B into intervals $[a, m_i - 1]$, $\{m_i\}$, $[m_i + 1, b]$, contradicting the fact that $\mathrm{fiip}(\sigma)$ is the finest interval partition preserved by σ.)

Observation 2: For $i \in [s-1]$, we have $\sigma(m_i) > \sigma(j)$ for all $j \in [m_i + 1, m_{i+1} - 1]$. (This is clear from the definition of a left-to-right maximum and from the fact that there is no left-to-right maximum at a position between m_i and m_{i+1}.)

Observation 3: For $i \in [s-1]$, there exists $j \in [m_{i+1} + 1, b]$ such that $\sigma(m_i) > \sigma(j)$. (For, suppose to the contrary that this is not the case. Then σ maps the interval $[m_{i+1}, b]$ into $[\sigma(m_i) + 1, b]$. If there exists $\gamma \in [\sigma(m_i) + 1, b] \setminus \sigma([m_{i+1}, b])$, then $\sigma(x) = \gamma$ for some $x \in [a, m_{i+1} - 1]$. By Observation 2, we must have $\sigma(m_i) \ge \gamma$. This contradicts the fact that $\gamma \ge \sigma(m_i) + 1$.)

We are going to prove that $S_{[m_i, b-1]} \subseteq \langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$ for every $i \in S_s$. Our lemma will then follow immediately from this, because $m_1 = a$.

We prove the claim by reverse induction, starting at $i = s$. By Observation 1, we have $b = \sigma(m_s) > m_s$. If $m_s = b - 1$, then $S_{[m_s, b-1]}$ is the trivial group, so the claim obviously holds. If $m_s \le b - 2$, then $\sigma(x) < b$ for all $x \in [m_s, b]$, so Lemma 4.4.11(i) implies that $(m_s\ m_s + 1), (m_s\ m_s + 1\ \cdots\ b - 1) \in \Delta \operatorname{Min}^{(n-1)} \sigma$. Thus $\Delta \operatorname{Min}^{(n-1)} \sigma$ includes a generating set of $S_{[m_s, b-1]}$, so the claim holds for $i = s$.

Assume then that $S_{[m_{i+1}, b-1]} \subseteq \langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$ for some $i < s$. If $m_i < m_{i+1} - 1$, then $\sigma(m_i) > \sigma(\ell)$ for all $\ell \in [m_i + 1, m_{i+1} - 1]$ by Observation 2 and there is $j \in [m_{i+1} + 1, b]$ such that $\sigma(m_i) > \sigma(j)$ by Observation 3. Then $(m_i\ m_i + 1\ \cdots\ j - 1) \in \Delta \operatorname{Min}^{(n-1)} \sigma$ by Lemma 4.4.11(i). If $m_i = m_{i+1} - 1$, then there is $j \in [m_{i+1} + 1, b]$ such that $\sigma(m_i) > \sigma(j)$ by Observation 3. Furthermore, there is $\ell \in [m_{i+1}, b]$ such that $\sigma(\ell) = \sigma(m_i) + 1$. Then, depending on whether $\ell < j$ or $j < \ell$, either $S_{\{m_i, \ell, \ldots, j-1\}} \subseteq \langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$ or $(m_i\ j\ \cdots\ \ell - 1) \in \Delta \operatorname{Min}^{(n-1)} \sigma$ holds by parts (iv) and (v) of Lemma 4.4.11. In all cases, $\langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$ includes a generating set of $S_{[m_i, b-1]}$. This concludes the inductive proof. □

Lemma 4.4.13. *Let $\sigma \in S_n$, let $\Pi := \mathrm{fiip}(\sigma)$ and assume that $\Pi = \{B_1, \ldots, B_t\}$ with $B_1 <_\Pi B_2 <_\Pi \cdots <_\Pi B_t$. For $i \in [t-1]$, write $C_i := B_i \cup (B_{i+1} - 1)$.*

(i) *For any $i \in [t-1]$, if $B_i \neq \{1\}$ and $|B_i| \neq |B_{i+1}|$ or $|B_i| = |B_{i+1}| \neq 2$, then $S_{C_i} \subseteq \langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$.*

(ii) *For any $i \in [t-1]$, if $|B_i| = |B_{i+1}| = 2$, then $A_{C_i} \subseteq \langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$.*

Proof. Recall from Lemma 4.4.12 that the group $\langle \Delta \operatorname{Min}^{(n-1)} \sigma \rangle$ includes $S_{B \setminus \{maxB\}}$ for every $B \in \Pi$.

The claim clearly holds if $|B_i| = |B_{i+1}| = 1$, so we will assume that this is not the case. Assume first that $|B_i| = 1$, say $B_i = \{q\}$ for some $q \neq 1$, and $|B_{i+1}| > 1$. Then $\sigma(q) = q$ and there is $p \in B_{i-1}$ such that $\sigma(p) = q - 1$ and $r \in B_{i+1} \setminus \{q+1\}$ such that $\sigma(r) = q + 1$. Since $p < q < r$, Lemma 4.4.11(viii) implies $(q \ \cdots \ r-1) \in \Delta\operatorname{Min}^{(n-1)}\sigma$. Consequently, the group $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$ includes

$$\langle (q \ \cdots \ r-1), S_{B_{i+1}\setminus\{\max B_{i+1}\}} \rangle = S_Q,$$

where

$$Q := \{q\} \cup B_{i+1} \setminus \{\max B_{i+1}\} = B_i \cup (B_{i+1} - 1).$$

Assume then that $|B_i| \geq 2$, say $B_i = [a, b]$ with $a < b$. Then $\sigma(b) < b$ and there is $p \in B_i \setminus \{b\}$ such that $\sigma(p) = b$, and there is $r \in B_{i+1}$ such that $\sigma(r) = b + 1$. It follows from Lemma 4.4.11(v) that $\tau := (p \ b \ \cdots \ r-1) \in \Delta\operatorname{Min}^{(n-1)}\sigma$. If $|B_{i+1}| = 1$, then $q = b + 1$ holds, so $\tau = (p \ b)$. Consequently, $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$ includes $\langle \tau, S_{B_i\setminus\{\max B_i\}} \rangle = S_Q$, where $Q := B_i = B_i \cup (B_{i+1} - 1)$. If $|B_{i+1}| \geq 2$, then $q > b + 1$ holds. Unless $|B_i| = |B_{i+1}| = 2$, we have that $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$ includes $\langle \tau, S_{B_i\setminus\{\max B_i\}}, S_{B_{i+1}\setminus\{\max B_{i+1}\}} \rangle = S_Q$, where

$$\begin{aligned} Q &:= (B_i \setminus \{\max B_i\}) \cup (B_{i+1} \setminus \{\max B_{i+1}\}) \cup \{p, b, \ldots, r-1\} \\ &= B_i \cup (B_{i+1} - 1). \end{aligned}$$

If $|B_i| = |B_{i+1}| = 2$, then $\tau = (a \ b \ b+1)$ and $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$ includes $\langle \tau \rangle = A_Q$, where $Q := \{a, b, b+1\} = B_i \cup (B_{i+1} - 1)$. □

Lemma 4.4.14. *Let $n \in \mathbf{N}_+$ and $\sigma \in S_n$, and let $\Pi := \operatorname{fiip}(\sigma)$. Assume that $\Pi = \{B_1, \ldots, B_r\}$ with $B_1 <_\Pi B_2 <_\Pi \cdots <_\Pi B_r$.*

(i) *If $|B_i| = 2$ for all $i \in [r]$, then $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle = A_{n-1}$. If $n \equiv 0 \pmod 4$, then $\langle \operatorname{Min}^{(n-1)}\sigma \rangle = S_{n-1}$. If $n \equiv 2 \pmod 4$, then $\langle \operatorname{Min}^{(n-1)}\sigma \rangle = A_{n-1}$.*

(ii) *If $|B_1| = 1$ and $|B_i| = 2$ for all $i \in [2, r]$, then $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle = A_{[2,n-1]}$. If $n \equiv 1 \pmod 4$, then $\langle \operatorname{Min}^{(n-1)}\sigma \rangle = S_{[2,n-1]}$. If $n \equiv 3 \pmod 4$, then $\langle \operatorname{Min}^{(n-1)}\sigma \rangle = A_{[2,n-1]}$.*

(iii) *Otherwise, $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle = \langle \operatorname{Min}^{(n-1)}\sigma \rangle = S_{\Pi^\downarrow}$.*

Proof. (i) Note that n is even and $\sigma = \theta_n$ by Fact 4.4.6. By Remark 4.4.2 and Fact 4.4.3, all permutations in $\operatorname{Min}^{(n-1)}\sigma$ have the same parity, so all permutations in $\Delta\operatorname{Min}^{(n-1)}\sigma$ are even. Consequently, the inclusion $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle \subseteq A_{n-1}$ holds. We also have $A_{n-1} \subseteq \langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$, because the group $\langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle$ contains $A_{B_i \cup (B_{i+1}-1)}$ for all $i \in [r-1]$ by Lemma 4.4.13(ii), and these constitute a generating set of A_{n-1}.

If $n \equiv 0 \pmod 4$, then by Remark 4.4.2, $\operatorname{Min}^{(n-1)}\sigma$ is a set of odd permutations. As we have shown above, $A_{n-1} = \langle \Delta\operatorname{Min}^{(n-1)}\sigma \rangle \subseteq$

$\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle$. Hence the set $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle$ includes a generating set of S_{n-1}, and we conclude that $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = S_{n-1}$.

If $n \equiv 2 \pmod 4$, then by Remark 4.4.2, $\mathrm{Min}^{(n-1)}\,\sigma$ is a set of even permutations, i.e., $\mathrm{Min}^{(n-1)}\,\sigma \subseteq A_{n-1}$. Then $A_{n-1} = \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle \subseteq \langle \mathrm{Min}^{(n-1)}\,\sigma\rangle \subseteq \langle A_{n-1}\rangle = A_{n-1}$, so $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = A_{n-1}$.

(ii) The proof is similar to part (i). In this case, n is odd and $\sigma = \theta_n$, so all permutations in $\mathrm{Min}^{(n-1)}\,\sigma$ have the same parity and fix 1. Thus $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle \subseteq A_{[2,n-1]}$. We also have $A_{[2,n-1]} \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$, because $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$ contains $A_{B_i\cup(B_{i+1}-1)}$ for all $i \in [2, r-1]$, and these constitute a generating set of $A_{[2,n-1]}$.

In a similar way as in part (i), we deduce that if $n \equiv 1 \pmod 4$, then $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = S_{[2,n-1]}$; and if $n \equiv 3 \pmod 4$, then $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = A_{[2,n-1]}$.

(iii) Let C be a block of $\Pi^{\downarrow}$. We will show that $S_C \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$. If $|C| = 1$, then this is trivial, so we may assume that $|C| \geq 2$. Then one of the conditions in Lemma 4.3.4(v) holds. If $C = B_r \cap [n-1]$, where $B_r = 2/\Pi$, then $S_C \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$ by Lemma 4.4.12.

Assume then that $C = \bigcup_{i=p}^{q}(B_i \cup (B_{i+1}-1))$ for some $p, q \in [r-1]$ with $p \leq q$ such that

- $B_p = 2/\Pi$ or $|B_p| = 1$ and $B_p \neq \{1\}$,
- $|B_i| > 1$ for all $i \in [p+1, q]$, and
- if $|B_{q+1}| > 1$ then $B_{q+1} = n/\Pi$.

Now it follows from Lemma 4.4.13 that for every $i \in [p, q]$, the set $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$ includes A_{C_i}, where $C_i = B_i \cup (B_{i+1}-1)$; these generate A_C. Not all blocks $B_p, \ldots, B_{q+1}$ are of size 2 (otherwise C would be as in part (i) or (ii)). Therefore, there exists $j \in [p, q]$ such that S_{C_j} is included in $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$. Consequently, $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$ includes a generating set of S_C; hence $S_C \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$.

Thus, we have shown that $S_{\Pi^{\downarrow}} \subseteq \langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle$. It also holds that $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle \subseteq \langle \mathrm{Min}^{(n-1)}\,\sigma\rangle$, and we have $\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle \subseteq S_{\Pi^{\downarrow}}$ by Lemma 4.4.7. Therefore $\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle = \langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = S_{\Pi^{\downarrow}}$, as claimed. □

Proposition 4.4.15. *Let $n \in \mathbf{N}_+$ and $\sigma \in S_n$, and let $\Pi := \mathrm{fiip}(\sigma)$. Then*

$$\langle \mathrm{Min}^{(n-1)}\,\sigma\rangle = \begin{cases} A_{\Pi^{\downarrow}}, & \text{if } n \equiv 2,3 \pmod 4 \text{ and } \sigma = \theta_n, \\ S_{\Pi^{\downarrow}}, & \text{otherwise,} \end{cases}$$

and

$$\langle \Delta\,\mathrm{Min}^{(n-1)}\,\sigma\rangle = \begin{cases} A_{\Pi^{\downarrow}}, & \text{if } \sigma = \theta_n, \\ S_{\Pi^{\downarrow}}, & \text{otherwise.} \end{cases}$$

Proof. In view of the description of $\mathrm{fiip}(\theta_n)$ provided in Fact 4.4.6, this is simply a reformulation of Lemma 4.4.14. □

Let $k, n \in \mathbf{N}_+$, $k \leq n$, and let $\sigma = \sigma_1 \ldots \sigma_n \in S_n$. Define $\sigma^{(\leq k)} \in S_k$ to be the permutation whose presentation in one-line notation is the substring of $\sigma_1 \ldots \sigma_n$ consisting of the entries that are less than or equal

to k. In fact, $\sigma^{(\leq k)}$ is a minor of σ, because, as is easy to verify, it holds that $\sigma^{(\leq k)} = \sigma_\Pi$, where Π is the partition of $[n]$ whose only potentially nontrivial block is $[k+1, n] \cup \{c\}$, where $c := \sigma(\min \sigma^{-1}([k]))$. It is clear that $\sigma^{(\leq n)} = \sigma$ and $\sigma^{(\leq k)} \leq \sigma^{(\leq k')} \leq \sigma$ for all $k, k' \in \mathbf{N}_+$ with $k \leq k' \leq n$.

Proposition 4.4.16. *Let $n, k \in \mathbf{N}_+$ with $2 \leq k < n$, and let $\sigma \in S_n$. Then $\operatorname{Min}^{(k)} \sigma \cap \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle = \emptyset$ if and only if $n = k+1 \equiv 0, 1 \pmod 4$ and $\sigma = \theta_n$.*

Proof. Assume first that $n = k+1 \equiv 0, 1 \pmod 4$ and $\sigma = \theta_n$. In this case, θ_n is an even permutation and every permutation in $\operatorname{Min}^{(k)} \sigma$ is odd by Remark 4.4.2 and Fact 4.4.3. On the other hand, $\langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$ is an alternating group by Proposition 4.4.15. Consequently, $\operatorname{Min}^{(k)} \sigma \cap \langle \Delta \operatorname{Min}^{(k)} \rangle = \emptyset$.

For the converse implication, we will prove the contrapositive. We assume that $n > k+1$ or $k+1 \equiv 2, 3 \pmod 4$ or $\sigma \neq \theta_n$, and we want to show that $\operatorname{Min}^{(k)} \sigma \cap \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle \neq \emptyset$. Since $\sigma^{(\leq k)} \in \operatorname{Min}^{(k)} \sigma$, it suffices to show that $\sigma^{(\leq k)} \in \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$.

Observe first that $\operatorname{Min}^{(k)} \sigma^{(\leq k+1)} \subseteq \operatorname{Min}^{(k)} \operatorname{Min}^{(k+1)} \sigma = \operatorname{Min}^{(k)} \sigma$ by the monotonicity of $\operatorname{Min}^{(k)}$ and Proposition 4.2.4. Hence

$$\Delta \operatorname{Min}^{(k)} \sigma^{(\leq k+1)} \subseteq \Delta \operatorname{Min}^{(k)} \sigma. \tag{4.4.1}$$

If $\sigma^{(\leq k+1)} \neq \theta_{k+1}$, then, since $\sigma^{(\leq k)} \leq \sigma^{(\leq k+1)}$, we have

$$\begin{aligned} \sigma^{(\leq k)} \in \operatorname{Min}^{(k)} \sigma^{(\leq k+1)} &\subseteq \langle \operatorname{Min}^{(k)} \sigma^{(\leq k+1)} \rangle \\ &= \langle \Delta \operatorname{Min}^{(k)} \sigma^{(\leq k+1)} \rangle \subseteq \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle, \end{aligned}$$

where the equality holds by Proposition 4.4.15 and the last inclusion holds by (4.4.1).

From now on, we assume that $\sigma^{(\leq k+1)} = \theta_{k+1}$. Proposition 4.4.15 and (4.4.1) yield $A_{\Pi^\downarrow} = \langle \Delta \operatorname{Min}^{(k)} \sigma^{(\leq k+1)} \rangle \subseteq \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$, where $\Pi = \operatorname{fiip}(\theta_{k+1})$. If $k+1 \equiv 2 \pmod 4$, then the permutation $\sigma^{(\leq k)} = (1\ 2)(3\ 4) \cdots (k-2\ k-1)$ is even, so $\sigma^{(\leq k)} \in A_k = A_{\Pi^\downarrow} \subseteq \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$. If $k+1 \equiv 3 \pmod 4$, then $\sigma^{(\leq k)} = (2\ 3)(4\ 5) \cdots (k-2\ k-1)$ is an even permutation fixing 1, so $\sigma^{(\leq k)} \in A_{\{2,\ldots,k\}} = A_{\Pi^\downarrow} \subseteq \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$.

If $k+1 \equiv 0 \pmod 4$, then we must have $n > k+1$ by our assumptions. Recall that since $\sigma^{(\leq k+1)} = \theta_{k+1}$, the one-line representation of $\theta_{k+1} = 2143 \ldots (k+1)k$ is a subsequence of $\sigma_1 \ldots \sigma_n$. Depending on the position of the first occurrence of an element of $\{k+2, \ldots, n\}$ in $\sigma_1 \ldots \sigma_n$, we have one of the following four cases.

Case 1: If $\sigma = 214\sigma_4 \ldots \sigma_n$, then for the k-partitions

$$\begin{aligned} \Gamma_1 &:= \langle \{1,2\}, \{3,4\}, [k+2, n] \rangle_{\text{part}}, \\ \Gamma_2 &:= \langle \{1\}, \{2,3,4\}, [k+2, n] \rangle_{\text{part}}, \end{aligned}$$

we have $\sigma_{\Gamma_1} = 12a_3 \ldots a_k$ and $\sigma_{\Gamma_2} = 21a_3 \ldots a_k$ for some $a_3 \ldots a_k \in [k]^{k-2}$, and $(\sigma_{\Gamma_1})^{-1} \circ \sigma_{\Gamma_2} = (1\ 2)$.

Case 2: If $\sigma = 2\alpha 1\beta 4\sigma_{p+q+4}\dots\sigma_n$, where $\alpha \in [k+2,n]^p$, $p \geq 1$, $\beta \in [k+2,n]^q$, $q \geq 0$, then, for the partitions Γ_1 and Γ_2 given above, we have $\sigma_{\Gamma_1} = 1k2b_3\dots b_k$ and $\sigma_{\Gamma_2} = 2k1b_4\dots b_k$ for some $b_4\dots a_k \in [k]^{k-3}$, and $(\sigma_{\Gamma_1})^{-1} \circ \sigma_{\Gamma_2} = (1\ 3)$.

Case 3: If $\sigma = \alpha 2\beta 1\gamma 4\sigma_{p+q+r+4}\dots\sigma_n$, where $\alpha \in [k+2,n]^p$, $p \geq 1$, $\beta \in [k+2,n]^q$, $q \geq 0$, $\gamma \in [k+2,n]^r$, $r \geq 0$, then, for the partitions Γ_1 and Γ_2 given above, we have $\sigma_{\Gamma_1} = k12c_3\dots c_k$ and $\sigma_{\Gamma_2} = k21c_4\dots c_k$ for some $c_4\dots c_k \in [k]^{k-4}$, and $(\sigma_{\Gamma_1})^{-1} \circ \sigma_{\Gamma_2} = (2\ 3)$.

Case 4: If $\sigma = 21\alpha 4\sigma_{p+4}\dots\sigma_n$, where $\alpha = \alpha_1\dots\alpha_p \in [k+2,n]^p$, $p \geq 1$, then for the k-partitions

$$\Gamma_3 := \langle \{1\}, \{2,3\}, \{4,\alpha_1,\dots,\alpha_p\}, [k+2,n] \setminus \{\alpha_1,\dots,\alpha_p\} \rangle_{\text{part}},$$
$$\Gamma_4 := \langle \{1,2\}, \{3,\alpha_1,\dots,\alpha_p\}, \{4\}, [k+2,n] \setminus \{\alpha_1,\dots,\alpha_p\} \rangle_{\text{part}},$$

we have $\sigma_{\Gamma_3} = 213d_4\dots d_k$ and $\sigma_{\Gamma_4} = 123d_4\dots d_k$ for some $d_4\dots d_k \in [k]^{k-3}$, and $(\sigma_{\Gamma_3})^{-1} \circ \sigma_{\Gamma_4} = (1\ 2)$.

Consequently, $\Delta \operatorname{Min}^{(k)} \sigma$ contains one of the transpositions $(1\ 2)$, $(1\ 3)$ and $(2\ 3)$. As noted above, $\Delta \operatorname{Min}^{(k)} \sigma$ also contains generators of A_k. Since the alternating group A_k and a transposition generate the full symmetric group S_k, we conclude that $\langle \Delta \operatorname{Min}^{(k)} \sigma \rangle = S_k$. Then it obviously holds that $\sigma^{(\leq k)} \in \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$.

If $k+1 \equiv 1 \pmod 4$, then a similar argument as above shows that $\Delta \operatorname{Min}^{(k)} \sigma$ contains one of the transpositions $(2\ 3)$, $(2\ 4)$ and $(3\ 4)$. Since $\Delta \operatorname{Min}^{(k)} \sigma$ also contains generators of $A_{\{2,\dots,k\}}$, we conclude that $S_{\{2,\dots,k\}} \subseteq \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$. Hence, clearly, $\sigma^{(\leq k)} \in \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$. □

4.5 RECONSTRUCTION PROBLEM OF PERMUTATIONS AND MINORS

Minors of permutations give rise to a reconstruction problem. Given a permutation $\sigma \in S_n$ and a fixed parameter $k \in \mathbf{N}$ with $k \leq n$, we define the deck of σ as the multiset of all $(n-k)$-minors of σ, i.e., $\operatorname{deck} \sigma := \langle \sigma_\Pi \mid \Pi \in \operatorname{Part}_{n-k}(n) \rangle$. This reconstruction problem was studied by the current author [58], and the reconstructibility of permutations is completely understood in the case when $k = 1$, namely:

- No n-permutation is reconstructible from $(n-1)$-minors when $n \leq 3$.
- The permutations 1342 and 1423 have the same deck. All other 4-permutations are reconstructible.
- All n-permutations are reconstructible when $n \geq 5$.

It was also shown that for every $n \geq 2$, the set S_n of all n-permutations is not set-reconstructible. Investigation of this reconstruction problem for $k > 1$ remains a topic of future research.

4.6 REMARKS

Proposition 4.4.15 addresses a special instance of the following group-theoretical problem.

Problem 4.6.1. Let G be a group, let $S \subseteq G$ be an arbitrary subset of G, and let $\Delta S := \{g^{-1}h \mid g, h \in S\}$ be the set of differences between elements of S. Then clearly $\langle \Delta S \rangle \leq \langle S \rangle$. Under which conditions on S do the groups $\langle \Delta S \rangle$ and $\langle S \rangle$ coincide?

The current author is not aware of any general nontrivial results concerning this problem.

5

ORDER OF FIRST OCCURRENCE

We shall now delve more deeply into the idea of listing objects appearing in a sequence of data in the order of first occurrence. We start with a formal definition of the map ofo, and we establish some of its elementary properties. Having the formalism set up, we will then focus on functions determined by ofo, which are noteworthy as examples of functions with a unique identification minor. We determine which permutation groups arise as invariance groups of functions determined by ofo. Finally we investigate the reconstructibility of functions determined by ofo. Theorems developed in the previous chapters will find applications here.

5.1 FORMAL DEFINITION AND BASIC FACTS

We have already described the map ofo informally in Definition 2.6.2. In order to facilitate easy and precise development of the theory, we provide a formal definition.

Recall from Definition 1.7.2 the natural surjection $\mathrm{nat}_\Pi\colon [n] \to \Pi$, the order-isomorphism $h_\Pi\colon ([m];\leq) \to (\Pi;\leq_\Pi)$, and the rigid surjection $\delta_\Pi\colon [n] \to [m]$, $\delta_\Pi = (h_\Pi)^{-1} \circ \mathrm{nat}_\Pi$ that are associated with a partition $\Pi \in \mathrm{Part}_m(n)$. Recall also that a tuple $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$ is formally a map $\mathbf{a}\colon [n] \to A$.

Definition 5.1.1. For a partition $\Pi \in \mathrm{Part}_m(n)$, define the mapping $\eta_\Pi\colon [m] \to [n]$ by the rule $\eta_\Pi(i) = \min(h_\Pi(i))$ for all $i \in [m]$, that is, $\eta_\Pi = \min \circ h_\Pi$, where we view min as the map $\min\colon \Pi \to [n]$ that chooses the smallest element from each Π-block. In particular, for the trivial partition $\Delta_n \in \mathrm{Part}_n(n)$, the equality $\eta_{\Delta_n} = \mathrm{id}_{[n]}$ holds.

Lemma 5.1.2. *For any partition* $\Pi \in \mathrm{Part}_m(n)$, $\delta_\Pi \circ \eta_\Pi = \mathrm{id}_{[m]}$.

Proof. For any $i \in [m]$, we have $h_\Pi(i) \in \Pi$ and $\min(h_\Pi(i)) \in h_\Pi(i)$, so clearly $\mathrm{nat}_\Pi(\min(h_\Pi(i))) = h_\Pi(i)$. Therefore,

$$\delta_\Pi \circ \eta_\Pi = (h_\Pi)^{-1} \circ \mathrm{nat}_\Pi \circ \min \circ h_\Pi = (h_\Pi)^{-1} \circ h_\Pi = \mathrm{id}_{[m]}\,. \qquad \square$$

Lemma 5.1.3. *Let* $\mathbf{a} \in A^n$, *and let* $\mathbf{u} := \mathbf{a}\eta_{\ker \mathbf{a}}$. *Then* $\mathbf{u} \in A^{|\ker \mathbf{a}|}_{\neq}$ *and* $\mathbf{a} = \mathbf{u}\delta_{\ker \mathbf{a}}$.

Proof. Write $\Pi := \ker \mathbf{a}$, and let m be the number of blocks in Π. By the definition of kernel, we have $a_i = a_j$ if and only if $i \equiv_\Pi j$, for all $i, j \in [n]$. In particular, $\min(i/\Pi) \equiv_\Pi i$ for any $i \in [n]$. Since $\mathbf{u}(p) = \mathbf{a}(\eta_\Pi(p)) = \mathbf{a}(\min(h_\Pi(p)))$ for any $p \in [m]$ and $h_\Pi\colon [m] \to \Pi$

is a bijection, it follows that $u_p = u_q$ if and only if $p = q$, for all $p, q \in [m]$. In other words, $\mathbf{u}$ is injective, that is, $\mathbf{u} \in A^m_{\neq}$. Furthermore,

$$\mathbf{u}\delta_\Pi = \mathbf{a}\eta_\Pi\delta_\Pi = \mathbf{a}\min h_\Pi (h_\Pi)^{-1}\operatorname{nat}_\Pi = \mathbf{a}\min\operatorname{nat}_\Pi = \mathbf{a},$$

where the last equality holds, because, by the above observations, $\mathbf{a}(\min(\operatorname{nat}_\Pi(i))) = \mathbf{a}(\min(i/\Pi)) = \mathbf{a}(i)$. □

We can now define the map ofo in terms of η_Π.

Definition 5.1.4. Recall the set $A^\sharp$ from (1.2.2). The map $\operatorname{ofo}\colon A^* \to A^\sharp$ is defined by the following rule: for any $n \in \mathbf{N}$ and $\mathbf{a} \in A^n$, set $\operatorname{ofo}(\mathbf{a}) := \mathbf{a}\eta_{\ker \mathbf{a}}$.

It is quite easy to see that the above formal definition of ofo captures the informal one given in Definition 2.6.2. First, note that $\mathbf{a}\eta_{\ker \mathbf{a}} \in A^\sharp$ by Lemma 5.1.3. For any $i \in [n]$, the first occurrence of the element a_i in $\mathbf{a}$ is at position $\min(i/\ker \mathbf{a})$. Let $\mathbf{u} := \mathbf{a}\eta_{\ker \mathbf{a}}$ and $m := |\ker \mathbf{a}|$. Then for any $p, q \in [m]$, $p \leq q$ is equivalent to $h_{\ker \mathbf{a}}(p) \leq_{\ker \mathbf{a}} h_{\ker \mathbf{a}}(q)$, which is equivalent to $\min(h_{\ker \mathbf{a}}(p)) \leq \min(h_{\ker \mathbf{a}}(q))$, i.e., $\eta_{\ker \mathbf{a}}(p) \leq \eta_{\ker \mathbf{a}}(q)$. This means that for all $p, q \in [m]$, the first occurrence of u_p in $\mathbf{a}$ lies to the left of or at the same position as the first occurrence of u_q in $\mathbf{a}$ if and only if $p \leq q$. In other words, $\operatorname{ofo}(\mathbf{a}) = \mathbf{a}\eta_{\ker \mathbf{a}} = \mathbf{u}$ lists the elements of A occurring in $\mathbf{a}$ in the order of first occurrence.

Note, in particular, that when $\mathbf{a} \in A^n_{\neq}$, then $\ker \mathbf{a} = \Delta_n$, and we have $\operatorname{ofo}(\mathbf{a}) = \mathbf{a}$.

The first equality in the next lemma formalizes the rather obvious statement that if we insert in a string repetitions of some letters such that each inserted letter has already occurred to the left of the point of insertion, then the value of the string under ofo remains unchanged. The second equality is noteworthy as it provides a link between ofo and minors of permutations.

Lemma 5.1.5. *For any $\mathbf{a} \in A^m$, for any partition $\Pi \in \operatorname{Part}_m(n)$, and for any permutation $\sigma \in S_n$, the following equalities hold:*

(i) $\operatorname{ofo}(\mathbf{a}\delta_\Pi) = \operatorname{ofo}(\mathbf{a})$,

(ii) $\operatorname{ofo}(\mathbf{a}\delta_\Pi\sigma) = \operatorname{ofo}(\mathbf{a}\sigma_\Pi)$.

Proof. (i) Let $\mathbf{a} \in A^m$. Let $\Phi := \ker \mathbf{a}$, and assume that $\Phi \in \operatorname{Part}_\ell(m)$. Let $\Gamma := \ker \mathbf{a}\delta_\Pi$. Since $\ker \delta_\Pi \sqsubseteq \ker \mathbf{a}\delta_\Pi$ and $\ker \delta_\Pi = \Pi$, we have $\Pi \sqsubseteq \Gamma$ (see Fact 1.5.1). Since δ_Π is surjective onto $[m]$, we have $\delta_\Pi(\Gamma) = \Phi$. By Lemma 1.7.7, $\delta_\Gamma = \delta_{\delta_\Pi(\Gamma)}\delta_\Pi = \delta_\Phi\delta_\Pi$.

Let $\mathbf{u} := \mathbf{a}\eta_\Phi$; then $\mathbf{a} = \mathbf{u}\delta_\Phi$ by Lemma 5.1.3. Then $\mathbf{a}\delta_\Pi = \mathbf{u}\delta_\Phi\delta_\Pi = \mathbf{u}\delta_\Gamma$. Consequently,

$$\operatorname{ofo}(\mathbf{a}\delta_\Pi) = \mathbf{a}\delta_\Pi\eta_\Gamma = \mathbf{u}\delta_\Gamma\eta_\Gamma = \mathbf{u} = \mathbf{a}\eta_\Phi = \operatorname{ofo}(\mathbf{a}),$$

where the third equality holds by Lemma 5.1.2.

(ii) By Lemma 4.1.9(ii) and part (i), we have

$$\operatorname{ofo}(\mathbf{a}\delta_\Pi\sigma) = \operatorname{ofo}(\mathbf{a}\sigma_\Pi\delta_{\sigma^{-1}(\Pi)}) = \operatorname{ofo}(\mathbf{a}\sigma_\Pi).$$ □

5.2 FUNCTIONS DETERMINED BY THE ORDER OF FIRST OCCURRENCE

Recall from Definition 2.3.6 that a function $f\colon A^n \to B$ is determined by ofo, if there exists a map $f^*\colon A^\sharp \to B$ such that $f = f^* \circ \mathrm{ofo}|_{A^n}$. In this case we also say that f is *determined by the order of first occurrence.* We denote by $\mathsf{OFO}^{(n)}$ the set of all n-ary functions that are, up to similarity (permutation of arguments, cf. Definition 2.2.5), determined by ofo, i.e., functions $f\colon A^n \to B$ satisfying $f \simeq f^* \circ \mathrm{ofo}|_{A^n}$ for some $f^*\colon A^\sharp \to B$. We write $\mathsf{OFO} := \bigcup_{n\geq 1} \mathsf{OFO}^{(n)}$.

Remark 5.2.1. The range of $\mathrm{ofo}|_{A^n}$ equals the set

$$A_n^\sharp := A^\sharp \cap \bigcup_{i=1}^{n} A^i.$$

Therefore, only the restriction of f^* to $A_n^\sharp$ is relevant in the composition $f^* \circ \mathrm{ofo}|_{A^n}$. Consequently, $f^* \circ \mathrm{ofo}|_{A^n} = g^* \circ \mathrm{ofo}|_{A^n}$ if and only if $f^*|_{A_n^\sharp} = g^*|_{A_n^\sharp}$. If $|A| \leq n$, then obviously $A_n^\sharp = A^\sharp \setminus \{\varepsilon\}$, where ε denotes the empty word.

Example 5.2.2. If $A = \{0,1\}$, then $\operatorname{Im} \mathrm{ofo}|_{A^1} = \{0,1\}$ and for $n \geq 2$, $\operatorname{Im} \mathrm{ofo}|_{A^n} = \{0,1,01,10\}$. From this fact it is easy to see that a function $f\colon \{0,1\}^n \to B$ is determined by ofo if and only if there exist maps $\varphi, \gamma\colon \{0,1\} \to B$ such that

$$f(a_1,\dots,a_n) = \begin{cases} \varphi(a_1), & \text{if } a_1 = \cdots = a_n, \\ \gamma(a_1), & \text{otherwise.} \end{cases}$$

Let us record here a few useful facts about functions determined by ofo. Note that statement (i) in the following asserts in particular that every function determined by ofo has a unique identification minor (see Section 2.6).

Lemma 5.2.3. *Let $f^*\colon A^\sharp \to B$, and let $f\colon A^n \to B$.*

(i) *If $f = f^* \circ \mathrm{ofo}|_{A^n}$ and $\Pi \in \mathrm{Part}_m(n)$, then $f_\Pi = f^* \circ \mathrm{ofo}|_{A^m}$.*

(ii) *If $f_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$, then there exists a map $h^*\colon A^\sharp \to B$ such that $f = h^* \circ \mathrm{ofo}|_{A^n}$ and $f^*(\mathbf{a}) = h^*(\mathbf{a})$ for all $\mathbf{a} \in A^\sharp$ with $|\mathrm{supp}(\mathbf{a})| < n$.*

(iii) *If $n > |A|$ and $f_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$, then $f = f^* \circ \mathrm{ofo}|_{A^n}$.*

Proof. (i) For any $\Pi \in \mathrm{Part}_m(n)$ and $\mathbf{a} \in A^m$, we have

$$f_\Pi(\mathbf{a}) = f(\mathbf{a}\delta_\Pi) = f^* \circ \mathrm{ofo}(\mathbf{a}\delta_\Pi) = f^* \circ \mathrm{ofo}(\mathbf{a}),$$

where the last equality holds by Lemma 5.1.5.

(ii) Assume that $f_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$. Define the map $h^* \colon A^\sharp \to B$ as follows:

$$h^*(\mathbf{a}) = \begin{cases} f^*(\mathbf{a}), & \text{if } |\mathrm{supp}(\mathbf{a})| < n, \\ f(\mathbf{a}), & \text{if } |\mathrm{supp}(\mathbf{a})| = n. \end{cases}$$

Let $\mathbf{b} \in A^n$. If $\mathbf{b} = \mathbf{a}\delta_I$ for some $\mathbf{a} \in A^{n-1}$ and $I \in \binom{[n]}{2}$, then $|\mathrm{supp}(\mathbf{a})| < n$ and we have

$$\begin{aligned} f(\mathbf{b}) = f(\mathbf{a}\delta_I) = f_I(\mathbf{a}) &= f^*(\mathrm{ofo}(\mathbf{a})) \\ &= h^*(\mathrm{ofo}(\mathbf{a}) = h^*(\mathrm{ofo}(\mathbf{a}\delta_I)) = h^*(\mathrm{ofo}(\mathbf{b})). \end{aligned}$$

Otherwise $\mathbf{b} \in A^n_{\neq}$, and we have $\mathrm{ofo}(\mathbf{b}) = \mathbf{b}$, $\mathrm{supp}(\mathbf{b}) = n$, and $f(\mathbf{b}) = h^*(\mathbf{b}) = h^*(\mathrm{ofo}(\mathbf{b}))$. Therefore, $f = h^* \circ \mathrm{ofo}|_{A^n}$. By the definition of h^*, the equality $f^*(\mathbf{a}) = h^*(\mathbf{a})$ holds whenever $|\mathrm{supp}(\mathbf{a})| < n$.

(iii) If $n > |A|$, then the function h^* constructed in part (ii) equals f^*, and the claim follows. □

5.3 INVARIANCE GROUPS OF FUNCTIONS DETERMINED BY THE ORDER OF FIRST OCCURRENCE

In this section, our goal is to determine which permutation groups may arise as invariance groups of functions $f \colon A^n \to B$ determined by the order of first occurrence. It turns out that if $n \leq |A|$, then every subgroup of the symmetric group S_n is the invariance group of some n-ary function determined by ofo, but if $n > |A|$, then only subgroups of a special form are possible. We are going to make good use of compressions and expansions of interval partitions that were defined in Section 4.3.

Proposition 5.3.1. *Let $k, n \in \mathbf{N}_+$ such that $k \geq 2$ and $n \leq k$, and let A and B be sets such that $|A| = k$ and $|B| \geq 2$. Then, for every subgroup G of S_n, there exists a function $f \colon A^n \to B$ determined by* ofo *such that* $\mathrm{InvGr}\, f = G$.

Proof. Let $G \leq S_n$, and assume, without loss of generality, that $A = [k]$. Let α and β be distinct elements of B. Denote $\mathbf{n} := (1, \ldots, n)$. Define $f^* \colon A^\sharp \to B$ by the rule

$$f^*(\mathbf{a}) = \begin{cases} \alpha, & \text{if } \mathbf{a} = \mathbf{n}\sigma \text{ for some } \sigma \in G, \\ \beta, & \text{otherwise.} \end{cases}$$

Let $f = f^* \circ \mathrm{ofo}|_{A^n}$. We claim that $\mathrm{InvGr}\, f = G$.

Let $\pi \in S_n$. Assume first that $\pi \in G$, and let $\mathbf{a} \in A^n$. If $\mathbf{a} = \mathbf{n}\sigma$ for some $\sigma \in G$, then also $\sigma\pi \in G$, and we have $f(\mathbf{a}) = f(\mathbf{n}\sigma) = \alpha = f(\mathbf{n}\sigma\pi) = f(\mathbf{a}\pi)$. If $\mathbf{a} = \mathbf{n}\tau$ for some $\tau \in S_n \setminus G$, then τ is a member of the coset τG of G which is disjoint from G. In this case

also $\tau\pi \in \tau G$, so $f(\mathbf{a}) = f(\mathbf{n}\tau) = \beta = f(\mathbf{n}\tau\pi) = f(\mathbf{a}\pi)$. If $\mathbf{a}$ is not of the form $\mathbf{n}\tau$ for any permutation $\tau \in S_n$, then neither is $\mathbf{a}\pi$, and we have $f(\mathbf{a}) = \beta = f(\mathbf{a}\pi)$. We conclude that $\pi \in \operatorname{InvGr} f$.

Assume then that $\pi \notin G$. Then $f(\mathbf{n}) = \alpha \neq \beta = f(\mathbf{n}\pi)$, so $\pi \notin \operatorname{InvGr} f$. □

Lemma 5.3.2. *Let $n \in \mathbf{N}_+$, $\sigma \in S_n$, assume that $n \geq |A|$, and let $f^*\colon A^\sharp \to B$. The following conditions are equivalent.*

(i) $\sigma \in \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^n})$.

(ii) *For every $m \in [n]$, the inclusion $\operatorname{Min}^{(m)} \sigma \subseteq \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$ holds.*

(iii) *There exists $m \in [n]$ with $m \geq |A|$ such that the inclusion $\operatorname{Min}^{(m)} \sigma \subseteq \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$ holds.*

Proof. (i) $\implies$ (ii) Assume that $\sigma \in \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^n})$. Let $m \in [n]$, and let $\Pi \in \operatorname{Part}_m(n)$. Then for all $\mathbf{a} \in A^m$,

$$\begin{aligned} f^* \circ \operatorname{ofo}|_{A^m}(\mathbf{a}) &= f^* \circ \operatorname{ofo}|_{A^n}(\mathbf{a}\delta_\Pi) \\ &= f^* \circ \operatorname{ofo}|_{A^n}(\mathbf{a}\delta_\Pi\sigma) = f^* \circ \operatorname{ofo}|_{A^m}(\mathbf{a}\sigma_\Pi), \end{aligned}$$

where the first equality holds by Lemma 5.1.5(i), the second equality holds because $\sigma \in \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^n})$, and the third equality holds by Lemma 5.1.5(ii). Thus $\sigma_\Pi \in \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$. We conclude that $\operatorname{Min}^{(n)} \sigma \subseteq \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$.

(ii) $\implies$ (iii) Trivial.

(iii) $\implies$ (i) Assume that $m \in [n]$ satisfies $m \geq |A|$ and $\operatorname{Min}^{(m)} \sigma \subseteq \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$. Then for any $\Pi \in \operatorname{Part}_m(n)$ and for any $\mathbf{a} \in A^m$, we have

$$\begin{aligned} f^* \circ \operatorname{ofo}|_{A^n}(\mathbf{a}\delta_\Pi) &= f^* \circ \operatorname{ofo}|_{A^m}(\mathbf{a}) \\ &= f^* \circ \operatorname{ofo}|_{A^m}(\mathbf{a}\sigma_\Pi) = f^* \circ \operatorname{ofo}|_{A^n}(\mathbf{a}\delta_\Pi\sigma), \quad (5.3.1) \end{aligned}$$

where the first equality holds by Lemma 5.1.5(i), the second equality holds because $\sigma_\Pi \in \operatorname{Min}^{(m)} \sigma \subseteq \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^m})$, and the third equality holds by Lemma 5.1.5(ii).

Now let $\mathbf{b} \in A^n$. Note that $\ker \mathbf{b} \in \operatorname{Part}_\ell(n)$ for some $\ell \leq |A|$. Let $\Pi \in \operatorname{Part}_m(n)$ be an arbitrary refinement of $\ker \mathbf{b}$. Lemmas 1.7.7(ii) and 5.1.3 yield $\mathbf{b} = \mathbf{b}\eta_{\ker \mathbf{b}}\delta_{\ker \mathbf{b}} = \mathbf{b}\eta_{\ker \mathbf{b}}\delta_{\delta_\Pi(\ker \mathbf{b})}\delta_\Pi$. Therefore, taking $\mathbf{a} := \mathbf{b}\eta_{\ker \mathbf{b}}\delta_{\delta_\Pi(\ker \mathbf{b})}$, we get $\mathbf{b} = \mathbf{a}\delta_\Pi$. We conclude from (5.3.1) that $f^* \circ \operatorname{ofo}_{A^n}(\mathbf{b}) = f^* \circ \operatorname{ofo}|_{A^n}(\mathbf{b}\sigma)$; hence $\sigma \in \operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^n})$. □

Proposition 5.3.3. *Let $k \geq 2$, and let A and B be sets such that $|A| = k$ and $|B| \geq 2$. Let $f^*\colon A^\sharp \to B$.*

(i) *Assume that one of the following conditions holds:*

(C1) $k \equiv 1 \pmod 4$ *and* $\operatorname{InvGr}(f^* \circ \operatorname{ofo}|_{A^k}) = A_k$,

(C2) $k \equiv 2 \pmod 4$ *and* $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k}) \in \{A_k, A_{[2,k]}\}$.
Then $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{k+1}}) = \{\mathrm{id}, \theta_{k+1}\}$.

(ii) *Let* $\ell \in \mathbf{N}_+$. *If* $\ell \geq 2$ *or conditions* (C1) *and* (C2) *do not hold, then* $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{k+\ell}}) = S_{\Pi^{\uparrow \ell}}$, *where* Π *denotes the coarsest interval partition* $\Theta \in \mathrm{IntPart}(k)$ *such that* S_Θ *is a subgroup of* $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k})$.

Proof. (i) By Proposition 4.4.15, we have $\langle \mathrm{Min}^{(k)}\, \theta_{k+1} \rangle = A_k$ when $k \equiv 1 \pmod 4$, and $\langle \mathrm{Min}^{(k)}\, \theta_{k+1} \rangle = A_{[2,k]} \subseteq A_k$ when $k \equiv 2 \pmod 4$. Moreover $\mathrm{Min}^{(k)}\, \mathrm{id} = \{\mathrm{id}\} \subseteq A_{[2,k]} \subseteq A_k$. Lemma 5.3.2 now yields $\{\mathrm{id}, \theta_{k+1}\} \subseteq \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{k+1}})$

If $\sigma \in S_{k+1} \setminus \{\mathrm{id}, \theta_{k+1}\}$, then by Proposition 4.4.15, $\langle \mathrm{Min}^{(k)}\, \sigma \rangle = S_{\Gamma^\downarrow}$, where $\Gamma := \mathrm{fiip}(\sigma)$. In this case, the partition Γ contains a nontrivial block and it is not of the form described in Fact 4.4.6. Consequently, $\Gamma^\downarrow$ must contain a nontrivial block. Hence $S_{\Gamma^\downarrow}$ contains odd permutations and so does $\mathrm{Min}^{(k)}\, \sigma$. But then $\mathrm{Min}^{(k)}\, \sigma$ is not included in A_k nor in $A_{[2,k]}$. Therefore Lemma 5.3.2 gives $\sigma \notin \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{k+1}})$. We conclude that $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{k+1}}) \subseteq \{\mathrm{id}, \theta_{k+1}\}$.

(ii) The result will follow by a simple inductive argument from the claim that is stated below, taking $n = k$ as the basis of induction. Observe that for any interval partition $\Pi \in \mathrm{IntPart}(n)$, Π itself is the coarsest interval partition $\Theta \in \mathrm{IntPart}(n)$ such that S_Θ is a subgroup of S_Π. Observe also that if $G = A_n$ or $G = A_{[2,n]}$, or $n \geq 4$ and $G = \{\mathrm{id}, \theta_n\}$, then the coarsest interval partition $\Theta \in \mathrm{IntPart}(n)$ such that S_Θ is a subgroup of G is the trivial partition. Note also that for $n = 3$, $\{\mathrm{id}, \theta_n\} = S_\Pi$, where $\Pi = \{\{1\}, \{2,3\}\}$.

Claim. Let $n \geq k$, and assume that it is neither the case that $n \equiv 1 \pmod 4$ and $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^n}) = A_n$ nor is it the case that $n \equiv 2 \pmod 4$ and $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^n}) \in \{A_n, A_{[2,n]}\}$. If Π is the coarsest interval partition $\Theta \in \mathrm{IntPart}(n)$ such that S_Θ is a subgroup of $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^n})$, then $\mathrm{InvGr}(f^* \circ \mathrm{ofo}_{A^{n+1}}) = S_{\Pi^\uparrow}$.

In order to prove the claim, write $G := \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^n})$. Observe first that Π is well defined. Namely, if $\Theta = \Delta_n$, then $S_\Theta = \{\mathrm{id}\}$ is a subgroup of G. Furthermore, if $\Theta_1, \Theta_2 \in \mathrm{IntPart}(n)$ are interval partitions such that S_{Θ_1} and S_{Θ_2} are subgroups of G, then $\langle S_{\Theta_1}, S_{\Theta_2} \rangle = S_{\Theta_1 \vee \Theta_2}$ is also a subgroup of G.

In order to prove the inclusion $S_{\Pi^\uparrow} \subseteq \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{n+1}})$, let $\sigma \in S_{\Pi^\uparrow}$. By Lemma 4.4.10, $\mathrm{Min}^{(n)}\, \sigma \subseteq S_\Pi \subseteq G$, and Lemma 5.3.2 gives $\sigma \in \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{n+1}})$.

For the converse inclusion, let $\sigma \in \mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^{n+1}})$, and let $\Gamma := \mathrm{fiip}(\sigma)$. Then $\langle \mathrm{Min}^{(n)}\, \sigma \rangle \subseteq G$ by Lemma 5.3.2. We need to consider different possibilities.

If $n \equiv 1 \pmod 4$ and $\sigma = \theta_{n+1}$, then $\langle \mathrm{Min}^{(n)}\, \sigma \rangle = A_n$ by Proposition 4.4.15. By our assumptions $G \neq A_n$, so we must have $G = S_n$. Then $\Pi = \{[n]\}$, whence $\Pi^\uparrow = \{[n+1]\}$, and then clearly $\sigma \in S_{n+1} = S_{\Pi^\uparrow}$.

If $n \equiv 2 \pmod 4$ and $\sigma = \theta_{n+1}$, then $\langle \mathrm{Min}^{(n)} \sigma \rangle = A_{[2,n]}$ by Proposition 4.4.15. Since the overgroups of $A_{[2,n]}$ are $A_{[2,n]}$, A_n, $S_{[2,n]}$ and S_n, and since we are assuming that $G \notin \{A_n, A_{[2,n]}\}$, it follows that $G = S_{[2,n]}$ or $G = S_n$. If $G = S_{[2,n]}$, then $\Pi = \{\{1\}, [2,n]\}$, whence $\Pi^\uparrow = \{\{1\}, [2,n+1]\}$ and $S_{\Pi^\uparrow} = S_{[2,n+1]}$. If $G = S_n$, then $\Pi = \{[n]\}$, whence $\Pi^\uparrow = \{[n+1]\}$ and $S_{\Pi^\uparrow} = S_{n+1}$. We clearly have $\sigma = \theta_{n+1} \in S_{[2,n+1]} \subseteq S_{n+1}$, so it holds that $\sigma \in S_{\Pi^\uparrow}$.

Otherwise (i.e., in the case that $\sigma \neq \theta_{n+1}$ or $n \equiv 0, 3 \pmod 4$), $\langle \mathrm{Min}^{(n)} \sigma \rangle = S_{\Gamma^\downarrow}$ by Proposition 4.4.15. Since $\Gamma^\downarrow$ is an interval partition and $S_{\Gamma^\downarrow} \leq G$, we must have $\Gamma^\downarrow \sqsubseteq \Pi$. Then $\Gamma^{\downarrow\uparrow} \sqsubseteq \Pi^\uparrow$ by Lemma 4.3.6. Since $\Gamma \sqsubseteq \Gamma^{\downarrow\uparrow}$ by Lemma 4.3.7, we have $\Gamma \sqsubseteq \Pi^\uparrow$ by the transitivity of the refinement relation. Hence $\sigma \in S_\Gamma \subseteq S_{\Pi^\uparrow}$. This completes the proof. □

We are now ready to characterize the permutation groups that arise as invariance groups of functions determined by ofo of large arity. The description refers to partitions of the form $\Pi^{\uparrow^\ell}$, where Π is an interval partition; these are explicitly characterized in Lemma 4.3.11.

Theorem 5.3.4. *Let $n, k \in \mathbf{N}$ with $2 \leq k < n$, and let A and B be sets such that $|A| = k$ and $|B| \geq 2$. Let G be a subgroup of S_n. Then there exists a function $f\colon A^n \to B$ determined by* ofo *such that* $\mathrm{InvGr}(f) = G$ *if and only if $G = S_{\Pi^{\uparrow^{n-k}}}$ for some interval partition $\Pi \in \mathrm{IntPart}(k)$ or $n = k+1$ and $G = \{\mathrm{id}, \theta_n\}$.*

Proof. If $f\colon A^n \to B$ is determined by ofo, then $f = f^* \circ \mathrm{ofo}|_{A^n}$ for some $f^*\colon A^\sharp \to B$. Let $\Pi \in \mathrm{IntPart}(k)$ be the coarsest interval partition Θ such that S_Θ is a subgroup of $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k})$. By Proposition 5.3.3, $\mathrm{InvGr}(f) = S_{\Pi^{\uparrow^{n-k}}}$ or $n = k+1$ and $\mathrm{InvGr}(f) = \{\mathrm{id}, \theta_n\}$.

For the converse implication, note first that Proposition 5.3.1 guarantees that for every subgroup G of S_k, there exists $f^*\colon A^\sharp \to B$ such that $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k}) = G$. If $n = k+1$ and $G = \{\mathrm{id}, \theta_n\}$, then choose $f^*\colon A^\sharp \to B$ so that $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k}) = A_k$. If $G = S_{\Pi^{\uparrow^{n-k}}}$ for some $\Pi \in \mathrm{IntPart}(k)$, then choose f^* so that $\mathrm{InvGr}(f^* \circ \mathrm{ofo}|_{A^k}) = S_\Pi$. Now, let $f\colon A^n \to B$, $f := f^* \circ \mathrm{ofo}|_{A^n}$. Then $\mathrm{InvGr}(f) = G$ by Proposition 5.3.3. □

5.4 RECONSTRUCTIBILITY OF FUNCTIONS DETERMINED BY THE ORDER OF FIRST OCCURRENCE

5.4.1 *Remarks on the reconstruction problem*

We now return to the topic of reconstruction problem of functions of several arguments and identification minors (see Definition 3.2.1). We shall investigate the reconstructibility of functions determined by the order of first occurrence.

In view of Lemma 5.2.3, the reconstruction problem may at first sight seem entirely trivial for functions determined by ofo. Namely, if $f\colon A^n \to B$ is of the form $f = f^* \circ \mathrm{ofo}|_{A^n}$ for some $f^*\colon A^\sharp \to B$, then its identification minors are all equal to $f^* \circ \mathrm{ofo}|_{A^{n-1}}$. At the same time, if $f\colon A^n \to B$ is a function such that $f_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$, then $f = f^* \circ \mathrm{ofo}|_{A^n}$. This does not, however, mean that f would be reconstructible. Recall that in the context of the reconstruction problem, functions are distinguished only up to similarity. If $g\colon A^n \to B$ is a reconstruction of f, then the deck of g comprises $\binom{n}{2}$ copies of $f^* \circ \mathrm{ofo}|_{A^{n-1}}$, which means that $g_I \simeq f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$; this does not mean that $g_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$.

When studying the reconstructibility of functions $f\colon A^n \to B$, we must assume that the arity n is sufficiently large. As explained in Remark 3.2.3, the assumption $n > |A|$ is indispensable. The following result shows that there also exist nonreconstructible n-ary functions determined by ofo when $n = |A| + 1$.

Proposition 5.4.1 ([59, Proposition 9])**.** *Assume that $n = k + 1$ and A and B are sets such that $|A| = k \geq 2$ and $|B| \geq 2$. Then there exist functions $f\colon A^n \to B$ and $f^*\colon A^\sharp \to B$ such that $f_I \simeq f^* \circ \mathrm{ofo}|_{A^{n-1}}$ for every $I \in \binom{[n]}{2}$ but f is not similar to any function determined by* ofo*. Furthermore, if $k > 2$, then $\mathrm{InvGr}\, f = \{\mathrm{id}\}$, and hence f is not 2-set-transitive.*

5.4.2 *Weak reconstructibility*

A first step towards establishing that a set of functions is reconstructible is to show that it is weakly reconstructible. In this subsection, we prove that the class $\mathsf{OFO}^{(n)}$ is weakly reconstructible for sufficiently large n. First we note that it is, at least in principle, possible that distinct maps $f^*, g^*\colon A^\sharp \to B$ give rise to functions $f^* \circ \mathrm{ofo}|_{A^n}$ and $g^* \circ \mathrm{ofo}|_{A^n}$ that, although distinct, are similar, i.e., $f^* \circ \mathrm{ofo}|_{A^n} \simeq g^* \circ \mathrm{ofo}|_{A^n}$. We need to investigate the conditions under which this happens.

Definition 5.4.2. Let $k, n \in \mathbf{N}_+$ with $k \leq n$. A permutation $\sigma \in S_n$ is *k-equalizing* if for all sets A and B such that $|A| = k$ and $|B| \geq 2$ and for every $f^+, g^+\colon A^k_{\neq} \to B$, the condition that $f^+ = g^+ \circ \underline{\sigma_\Pi}|_{A^k_{\neq}}$ for all $\Pi \in \mathrm{Part}_k(n)$ implies $f^+ = g^+$.

Lemma 5.4.3. *Let $n, k \in \mathbf{N}_+$ with $2 \leq k < n$, and let $\sigma \in S_n$. Then σ is k-equalizing precisely unless $n = k + 1 \equiv 0, 1 \pmod 4$ and $\sigma = \theta_n$.*

Proof. Assume first that $n = k + 1 \equiv 0, 1 \pmod 4$ and $\sigma = \theta_n$. Let $\alpha, \beta, \gamma \in B$ such that $\alpha \neq \beta$ and $\alpha \neq \gamma$. Define the functions

$f^+, g^+ \colon A^k_{\neq} \to B$ as follows. Let $\mathbf{k} := (1, 2, \dots, k) \in A^k$. If k is odd, then let

$$f^+(\mathbf{a}) = \begin{cases} \alpha, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some even } \tau \in S_k, \\ \beta, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some odd } \tau \in S_k, \end{cases} \tag{5.4.1}$$

$$g^+(\mathbf{a}) = \begin{cases} \alpha, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some odd } \tau \in S_k, \\ \beta, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some even } \tau \in S_k. \end{cases} \tag{5.4.2}$$

If k is even, then let

$$f^+(\mathbf{a}) = \begin{cases} \alpha, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some even } \tau \in S_k \text{ with } \tau(1) = 1, \\ \beta, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some odd } \tau \in S_k \text{ with } \tau(1) = 1, \\ \gamma, & \text{otherwise,} \end{cases} \tag{5.4.3}$$

$$g^+(\mathbf{a}) = \begin{cases} \alpha, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some odd } \tau \in S_k \text{ with } \tau(1) = 1, \\ \beta, & \text{if } \mathbf{a} = \mathbf{k}\tau \text{ for some even } \tau \in S_k \text{ with } \tau(1) = 1, \\ \gamma, & \text{otherwise.} \end{cases} \tag{5.4.4}$$

Let $\Pi \in \mathrm{Part}_k(n)$. By Remark 4.4.2 and Fact 4.4.3, $(\theta_n)_\Pi$ is an odd permutation. Moreover, if $n \equiv 1 \pmod 4$, then $(\theta_n)_\Pi$ fixes 1. It is thus clear that $f^+ = g^+ \circ \underline{(\theta_n)_\Pi}|_{A^k_{\neq}}$. Since this holds for every partition Π but $f^+ \neq g^+$, we conclude that θ_n is not k-equalizing.

Assume then that it is not the case that $n = k + 1 \equiv 0, 1 \pmod 4$ and $\sigma = \theta_n$. Let $f^+, g^+ \colon A^k_{\neq} \to B$ and assume that $f^+ = g^+ \circ \underline{\sigma_\Pi}|_{A^k_{\neq}}$ for all partitions $\Pi \in \mathrm{Part}_k(n)$. If $\Pi_1, \Pi_2 \in \mathrm{Part}_k(n)$, $g^+ \circ \underline{\sigma_{\Pi_1}}|_{A^k_{\neq}} = f^+ = g^+ \circ \underline{\sigma_{\Pi_2}}|_{A^k_{\neq}}$, which implies $g^+ = g^+ \circ \underline{(\sigma_{\Pi_1})^{-1}\sigma_{\Pi_2}}|_{A^k_{\neq}}$. Thus g^+ is invariant under every permutation in $\Delta \operatorname{Min}^{(k)} \sigma$ and hence under every permutation in $\langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$.

By Proposition 4.4.16, we have $\operatorname{Min}^{(k)} \sigma \cap \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle \neq \emptyset$. Take any $\pi \in \operatorname{Min}^{(k)} \sigma \cap \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle$. Since $\pi \in \operatorname{Min}^{(k)} \sigma$, we have $f^+ = g^+ \circ \underline{\pi}|_{A^k_{\neq}}$ by our assumption. Since $\pi \in \langle \Delta \operatorname{Min}^{(k)} \sigma \rangle \subseteq \operatorname{InvGr} g^+$, we have $g^+ \circ \underline{\pi}|_{A^k_{\neq}} = g^+$. Therefore $f^+ = g^+$, and we conclude that σ is k-equalizing. □

Lemma 5.4.4. *Let $n, k \in \mathbf{N}_+$ with $k < n$, and assume that it is not the case that $n = k + 1 \equiv 0, 1 \pmod 4$. Assume that A and B are sets such that $|A| = k$, $|B| \geq 2$. Then for all $f, g \colon A^n \to B$ it holds that if $f = f^* \circ \mathrm{ofo}|_{A^n}$ and $g = g^* \circ \mathrm{ofo}|_{A^n}$ for some $f^*, g^* \colon A^\sharp \to B$ and $f \simeq g$, then $f = g$.*

Proof. Since $f \simeq g$, there exists $\sigma \in S_n$ such that $f = g \circ \underline{\sigma}$, i.e., $f^*(\mathrm{ofo}(\mathbf{a})) = g^*(\mathrm{ofo}(\mathbf{a}\sigma))$ for all $\mathbf{a} \in A^n$. It follows from Lemma 5.1.5 that for every $\Pi \in \mathrm{Part}_m(n)$ $(1 \leq m \leq k)$ and for every $\mathbf{a} \in A^m_{\neq}$,

$$f^*(\mathbf{a}) = f^*(\mathrm{ofo}(\mathbf{a}\delta_\Pi)) = g^*(\mathrm{ofo}(\mathbf{a}\delta_\Pi\sigma)) = g^*(\mathbf{a}\sigma_\Pi).$$

We conclude that $f^*|_{A^m_{\neq}} = g^*|_{A^m_{\neq}} \circ \underline{\sigma_\Pi}|_{A^m_{\neq}}$. It follows from our assumptions and from Lemma 5.4.3 that σ is m-equalizing. Therefore $f^*|_{A^m_{\neq}} = g^*|_{A^m_{\neq}}$. Since this holds for every $m \in [k]$, we have $f^* = g^*$. Consequently $f = g$. □

The next result shows that the class $\mathsf{OFO}^{(n)}$ is weakly reconstructible for sufficiently large n.

Theorem 5.4.5. *Let $n, k \in \mathbf{N}_+$ such that $k \equiv 1, 2 \pmod 4$ and $n \geq k+2$, or $k \equiv 0, 3 \pmod 4$ and $n \geq k+3$. Assume that A and B are sets such that $|A| = k$ and $|B| \geq 2$. Let $f, g\colon A^n \to B$ be functions determined by* ofo. *If* $\operatorname{deck} f = \operatorname{deck} g$, *then $f \simeq g$.*

Proof. Let $f^*, g^*\colon A^\sharp$ be such that $f = f^* \circ \mathrm{ofo}|_{A^n}$ and $g = g^* \circ \mathrm{ofo}|_{A^n}$. By Lemma 5.2.3, $f_I = f^* \circ \mathrm{ofo}|_{A^{n-1}}$ and $g_I = g^* \circ \mathrm{ofo}|_{A^{n-1}}$ for all $I \in \binom{[n]}{2}$. Since $\operatorname{deck} f = \operatorname{deck} g$, we have $f^* \circ \mathrm{ofo}|_{A^{n-1}} \simeq g^* \circ \mathrm{ofo}|_{A^{n-1}}$. Lemma 5.4.4 now yields $f^* \circ \mathrm{ofo}|_{A^{n-1}} = g^* \circ \mathrm{ofo}|_{A^{n-1}}$. We conclude from Remark 5.2.1 that $f^* = g^*$, hence that $f = g$, and finally that $f \simeq g$. □

The permutation θ_n is not k-equalizing when $n = k+1 \equiv 0, 1 \pmod 4$. In the following proposition, we use this fact to provide an example of a pair of functions determined by ofo that are nonequivalent but have the same deck. This shows that in Theorem 5.4.5, the lower bound on the arity n is sharp when $k \equiv 0, 3 \pmod 4$.

Proposition 5.4.6. *Let $n, k \in \mathbf{N}_+$ be such that $k \equiv 0, 3 \pmod 4$ and $n = k+2$. Assume that A and B are sets such that $|A| = k$ and $|B| \geq 2$. Then there exist functions $f, g\colon A^n \to B$ that are determined by* ofo *such that $f \not\simeq g$ and $f_I \simeq g_J$ for all $I, J \in \binom{[n]}{2}$.*

Proof. Assume, without loss of generality, that $A = [k]$. Let $\alpha, \beta, \gamma \in B$ with $\alpha \neq \beta$ and $\alpha \neq \gamma$, let $\mathbf{k} := (1, \ldots, k) \in A^k$, and let the mappings $f^+, g^+\colon A^k_{\neq} \to B$ be as in (5.4.1) and (5.4.2) if k is odd, or as in (5.4.3) and (5.4.4) if k is even. Extend f^+ and g^+ into functions $f^*, g^*\colon A^\sharp \to B$ as follows:

$$f^*(\mathbf{u}) = \begin{cases} f^+(\mathbf{u}), & \text{if } \mathbf{u} \in A^k_{\neq}, \\ \gamma, & \text{otherwise,} \end{cases} \qquad g^*(\mathbf{u}) = \begin{cases} g^+(\mathbf{u}), & \text{if } \mathbf{u} \in A^k_{\neq}, \\ \gamma, & \text{otherwise.} \end{cases}$$

Let $f := f^* \circ \mathrm{ofo}|_{A^{k+2}}$ and $g := g^* \circ \mathrm{ofo}|_{A^{k+2}}$. By Lemma 5.2.3(i), we have $f_I = f^* \circ \mathrm{ofo}|_{A^{k+1}}$ and $g_J = g^* \circ \mathrm{ofo}|_{A^{k+1}}$ for all $I, J \in \binom{[n]}{2}$. Let $\mathbf{a} \in A^{k+1}$, and let $\mathbf{u} := \mathrm{ofo}(\mathbf{a}) = \mathbf{a}\eta_{\ker \mathbf{a}}$. If $\mathbf{u} \notin A^k_{\neq}$, then $A \neq \operatorname{supp}(\mathbf{a}) = \operatorname{supp}(\mathbf{a}\theta_{k+1})$; hence $\mathrm{ofo}(\mathbf{a}\theta_{k+1}) \notin A^k_{\neq}$ and we have

$$f_I(\mathbf{a}) = f^*(\mathrm{ofo}(\mathbf{a})) = \gamma = g^*(\mathrm{ofo}(\mathbf{a}\theta_{k+1}) = g_J(\mathbf{a}\theta_{k+1}).$$

On the other hand, if $\mathbf{u} \in A^k_{\neq}$, then

$$\mathrm{ofo}(\mathbf{a}\theta_{k+1}) = \mathrm{ofo}(\mathbf{u}\delta_{\ker \mathbf{a}}\theta_{k+1}) = \mathrm{ofo}(\mathbf{u}(\theta_{k+1})_{\ker \mathbf{a}}) = \mathrm{ofo}(\mathbf{u}\lambda^\ell_k) = \mathbf{u}\lambda^\ell_k,$$

for some $\ell \in [k]$. Since $k \equiv 0,3 \pmod 4$, Remark 4.4.2 implies that λ_k^ℓ is an odd permutation; moreover λ_k^ℓ fixes 1 if k is even. It follows that $f^+(\mathbf{u}) = g^+(\mathbf{u}\lambda_k^\ell)$. Consequently, $f_I(\mathbf{a}) = f^+(\mathbf{u}) = g^+(\mathbf{u}\lambda_k^\ell) = g_J(\mathbf{a}\theta_{k+1})$. We conclude that $f_I = g_J \circ \underline{\theta_{k+1}}$. Hence $f_I \simeq g_J$ for all $I, J \in \binom{[n]}{2}$.

In order to verify that $f \not\simeq g$, we will find for each permutation $\sigma \in S_{k+2}$, a $(k+2)$-tuple $\mathbf{a}$ such that $f(\mathbf{a}) \neq g(\mathbf{a}\sigma)$. Let $\Pi \in \mathrm{Part}_k(k+2)$ be the partition whose only nontrivial block is $\{k, k+1, k+2\}$. Let $\mathbf{u} := \mathbf{k}\delta_\Pi = (1, 2, \ldots, k, k, k) \in A^{k+2}$. Note that $\mathrm{ofo}(\mathbf{u}) = \mathbf{k}$, and by Lemma 5.1.5, we have $\mathrm{ofo}(\mathbf{u}\sigma) = \mathrm{ofo}(\mathbf{k}\delta_\Pi\sigma) = \mathrm{ofo}(\mathbf{k}\sigma_\Pi) = \mathbf{k}\sigma_\Pi$, for any $\sigma \in S_{k+2}$.

Let $\sigma \in S_{k+2}$. If $\sigma(1) \neq 1$, then $\mathbf{u}\sigma$ is a tuple the first component of which is distinct from 1, and the same is true for $\mathrm{ofo}(\mathbf{u}\sigma)$. Therefore, if $k \equiv 0 \pmod 4$ and $\sigma(1) \neq 1$, then $f(\mathbf{u}) = \alpha \neq \gamma = g(\mathbf{u}\sigma)$, and we are done. We assume from now on that if $k \equiv 0 \pmod 4$, then $\sigma(1) = 1$.

If σ_Π is an even permutation, then $f(\mathbf{u}) = f^* \circ \mathrm{ofo}(\mathbf{u}) = f^+(\mathbf{k}) = \alpha \neq \beta = g^+(\mathbf{k}\sigma_\Pi) = g^* \circ \mathrm{ofo}(\mathbf{u}\sigma) = g(\mathbf{u}\sigma)$ and we are done. We assume from now on that σ_Π is odd; hence $\sigma_\Pi \neq \mathrm{id}$. We split the analysis into three cases.

Case 1: $\sigma(k+1) = k+1$ and $\sigma(k+2) = k+2$. Then σ_Π equals the restriction of σ to the set $[k]$. Let p be the largest $i \in [k]$ such that $\sigma(i) \neq i$; such an element exists because $\sigma_\Pi \neq \mathrm{id}$. We have $1 < p \leq k$ and $\sigma(p) < p$. Write $q := \sigma^{-1}(p)$; we also have $q < p$. Let $\mathbf{a} = (a_1, \ldots, a_{k+2}) \in A^{k+2}$ be the tuple satisfying

$$a_i = \begin{cases} i, & 1 \leq i \leq p-1, \\ \sigma(p), & i = p, \\ i-1, & p+1 \leq i \leq k, \\ k, & k+1 \leq i \leq k+2. \end{cases}$$

Note that the element $\sigma(p)$ occurs twice in $\mathbf{a}$, namely $a_{\sigma(p)} = a_p = \sigma(p)$. It is clear that $\mathrm{ofo}(\mathbf{a}) = \mathbf{k}$. We have $\mathbf{a}\sigma = (b_1, \ldots, b_{k+2})$, where

$$b_i = \begin{cases} \sigma(i), & 1 \leq i \leq q-1, \\ \sigma(p), & i = q, \\ \sigma(i), & q+1 \leq i \leq p, \\ i-1, & p+1 \leq i \leq k, \\ k, & k+1 \leq i \leq k+2. \end{cases}$$

Thus $\mathrm{ofo}(\mathbf{a}\sigma)$ equals

$$(\sigma(1), \ldots, \sigma(q-1), \sigma(p), \sigma(q+1), \ldots, \sigma(p-1), p, p+1, \ldots, k-1, k).$$

Compare this with $\mathrm{ofo}(\mathbf{u}\sigma)$, which equals

$$(\sigma(1), \ldots, \sigma(q-1), p, \sigma(q+1), \ldots, \sigma(p-1), \sigma(p), p+1, \ldots, k-1, k).$$

	the last three entries of		
$(\sigma_k, \sigma_{k+1}, \sigma_{k+2})$	$\mathbf{a}\sigma$	$\mathbf{b}\sigma$	$\mathbf{c}\sigma$
$(k, k+2, k+1)$	$(k-1, k, k)$	$(k-1, k-1, k)$	$(d, k, k-1)$
$(k+1, k, k+2)$	$(k, k-1, k)$	$(k, k-1, k-1)$	$(k-1, d, k)$
$(k+1, k+2, k)$	$(k, k, k-1)$	$(k, k-1, k-1)$	$(k-1, k, d)$
$(k+2, k, k+1)$	$(k, k-1, k)$	$(k-1, k-1, k)$	$(k, d, k-1)$
$(k+2, k+1, k)$	$(k, k, k-1)$	$(k-1, k, k-1)$	$(k, k-1, d)$

Table 9: Last three entries of $\mathbf{a}\sigma$, $\mathbf{b}\sigma$ and $\mathbf{c}\sigma$.

We see that $\operatorname{ofo}(\mathbf{a}\sigma)$ can be obtained from $\operatorname{ofo}(\mathbf{u}\sigma) = \mathbf{k}\sigma_\Pi$ by interchanging the entries p and $\sigma(p)$. Therefore, $\operatorname{ofo}(\mathbf{a}\sigma) = \mathbf{k}\tau\sigma_\Pi$, where τ is the transposition of p and $\sigma(p)$. Since both τ and σ_Π are odd permutations, $\tau\sigma_\Pi$ is an even permutation. Moreover, if $k \equiv 0 \pmod 4$, then both p and $\sigma(p)$ are distinct from 1; hence $\tau(1) = 1$ and $\tau\sigma_\Pi(1) = 1$. Consequently, we have $f(\mathbf{a}) = f^+(\mathbf{k}) = \alpha \neq \beta = g^+(\mathbf{k}\tau\sigma_\Pi) = g(\mathbf{a}\sigma)$.

Case 2: $\{\sigma(k), \sigma(k+1), \sigma(k+2)\} = \{k, k+1, k+2\}$. We may assume that σ does not fix all three elements of $\{k, k+1, k+2\}$, because this situation is subsumed by Case 1. Then the restriction of σ to $[k-1]$ is a permutation of $[k-1]$, and $\sigma_\Pi(i) = \sigma(i)$ for all $i \in [k-1]$ and $\sigma_\Pi(k) = k$. Let $\ell := \sigma^{-1}(k-1)$. If $\ell \neq 1$, then let $d := \sigma(\ell - 1)$; if $\ell = 1$, then let $d := \sigma(2)$. Note that $d < k-1$. Let

$$\begin{aligned}\mathbf{a} &:= (1, 2, \ldots, k-2, d, k-1, k, k),\\ \mathbf{b} &:= (1, 2, \ldots, k-2, d, k-1, k, k-1),\\ \mathbf{c} &:= (1, 2, \ldots, k-2, d, d, k-1, k).\end{aligned}$$

It is clear that $\operatorname{ofo}(\mathbf{a}) = \operatorname{ofo}(\mathbf{b}) = \operatorname{ofo}(\mathbf{c}) = \mathbf{k}$, hence $f(\mathbf{a}) = f(\mathbf{b}) = f(\mathbf{c}) = \alpha$. Moreover, in each one of the tuples $\mathbf{a}\sigma$, $\mathbf{b}\sigma$, $\mathbf{c}\sigma$, the first $k-1$ entries are

$$\sigma(1), \ldots, \sigma(\ell-1), d, \sigma(\ell+1), \ldots, \sigma(k-1), \tag{5.4.5}$$

and the last three entries are presented in Table 9, for any possible combination of values of $\sigma(k), \sigma(k+1), \sigma(k+2)$.

Since d equals either $\sigma(\ell-1)$ or $\sigma(\ell+1)$, we obtain, by putting together the data from (5.4.5) and Table 9 in all possible ways, that

$$\begin{aligned}&\{\operatorname{ofo}(\mathbf{a}\sigma), \operatorname{ofo}(\mathbf{b}\sigma), \operatorname{ofo}(\mathbf{c}\sigma)\}\\ &= \{(\sigma(1), \ldots, \sigma(\ell-1), \sigma(\ell+1), \ldots, \sigma(k-1), k-1, k),\\ &\qquad (\sigma(1), \ldots, \sigma(\ell-1), \sigma(\ell+1), \ldots, \sigma(k-1), k, k-1)\}\\ &= \{(\sigma(1), \ldots, \sigma(k-1), k)\zeta, (\sigma(1), \ldots, \sigma(k-1), k)\xi\}\\ &= \{\mathbf{k}\sigma_\Pi\zeta, \mathbf{k}\sigma_\Pi\xi\},\end{aligned}$$

where ζ and ξ are the cycles

$$\zeta = (\ell \ \ \ell+1 \ \ \cdots \ \ k-1), \qquad \xi = (\ell \ \ \ell+1 \ \ \cdots \ \ k-1 \ \ k).$$

Since the lengths of the cycles ζ and ξ differ by 1, one of ζ and ξ is an odd permutation and the other is even. Therefore one of the permutations $\sigma_\Pi\zeta$ and $\sigma_\Pi\xi$ is odd and the other is even. Moreover, if $k \equiv 0 \pmod 4$, then $\ell \neq 1$; hence each one of σ_Π, ζ and ξ fixes 1, and so do $\sigma_\Pi\zeta$ and $\sigma_\Pi\xi$. Therefore, $\{g^*(\mathbf{k}\sigma_\Pi\zeta), g^*(\mathbf{k}\sigma_\Pi\xi)\} = \{\alpha, \beta\}$. We conclude that $f(\mathbf{a}) \neq g(\mathbf{a}\sigma)$ or $f(\mathbf{b}) \neq g(\mathbf{b}\sigma)$ or $f(\mathbf{c}) \neq g(\mathbf{c}\sigma)$.

Case 3: $\{\sigma(k), \sigma(k+1), \sigma(k+2)\} \neq \{k, k+1, k+2\}$. Let $r, s, t \in [k+2]$ be the elements satisfying $\{\sigma(r), \sigma(s), \sigma(t)\} = \{k, k+1, k+2\}$ and $r < s < t$. It also holds that $r < k$. Then the three occurrences of k in $\mathbf{u}\sigma$ are exactly at the r-th, s-th, and t-th positions. For $i \in [k+2] \setminus \{r, s, t\}$, the i-th component of $\mathbf{u}\sigma$ is $\sigma(i)$.

Next we define a tuple $\mathbf{a} \in A^{k+2}$. The definition depends on the values of r, s and t.

- If $t < k+2$, then let $d := \sigma(t+1)$, and let $\mathbf{a} \in A^{k+2}$ be the tuple obtained from $\mathbf{u}$ by changing the entries at positions $\sigma(r)$ and $\sigma(s)$ to d.
- If $t = k+2$ and $s < k+1$, then let $d := \sigma(s+1)$, and let $\mathbf{a} \in A^{k+2}$ be the tuple obtained from $\mathbf{u}$ by changing the entry at position $\sigma(r)$ to d.
- If $t = k+2$ and $s = k+1$, then let $d := \sigma(k)$ (recall that $r < k$), and let $\mathbf{a} \in A^{k+2}$ be the tuple obtained from $\mathbf{u}$ by changing the entry at position $\sigma(r)$ to d.

It is easy to verify that $\mathrm{ofo}(\mathbf{a}) = \mathbf{k}$ and $\mathrm{ofo}(\mathbf{a}\sigma) = \mathbf{k}\tau\sigma_\Pi$, where τ is the transposition of d and k. Since both τ and σ_Π are odd permutations, $\tau\sigma_\Pi$ is an even permutation. Moreover, if $k \equiv 0 \pmod 4$, then $r > 1$; hence both τ and σ_Π fix 1 and so does $\tau\sigma_\Pi$. Thus $f(\mathbf{a}) = f^+(\mathbf{k}) = \alpha \neq \beta = g^+(\mathbf{k}\tau\sigma_\Pi) = g(\mathbf{a}\sigma)$.

The three cases analysed above exhaust all possibilities We found for every permutation $\sigma \in S_{k+2}$ a tuple $\mathbf{a} \in A^{k+2}$ satisfying $f(\mathbf{a}) \neq g(\mathbf{a}\sigma)$. We conclude that $f \not\approx g$. □

5.4.3 *Reconstructible subclasses*

Theorem 5.4.5 immediately raises the question whether the class $\mathsf{OFO}^{(n)}$ is reconstructible – not just weakly reconstructible – for sufficiently large n. Unfortunately, we are not able to provide a definitive answer to this question. However, we will describe some reconstructible subclasses of OFO. In particular, if $|A| = 2$, then every function in OFO of sufficiently large arity is reconstructible.

Example 5.4.7. If $n > |A| + 1$ and $f\colon A^n \to B$ is totally symmetric and determined by ofo, then f is reconstructible. Recall from Proposition 2.6.4 that a function is totally symmetric and determined by ofo (or, equivalently, 2-set-transitive and determined by ofo) if and

only if it is determined by supp. Functions determined by supp are reconstructible by Proposition 3.3.3.

Example 5.4.7 can be generalized a little bit. We are going to show that if the invariance group of $f\colon A^n \to B$ includes $S_{[2,n]}$ and f is determined by ofo, then f is reconstructible.

Let $\mathrm{first}\colon A^+ \to A$ be the function that maps each string to its first letter, i.e., if $\mathbf{a} \in A^n$ for some $n \in \mathbf{N}$, then $\mathrm{first}(\mathbf{a}) = \mathrm{pr}_1^{(n)}(\mathbf{a})$. Let $(\mathrm{first}, \mathrm{supp})\colon A^+ \to A \times \mathcal{P}(A)$, $(\mathrm{first}, \mathrm{supp})(\mathbf{a}) = (\mathrm{first}(\mathbf{a}), \mathrm{supp}(\mathbf{a}))$. Then a function $f\colon A^n \to B$ is determined by $(\mathrm{first}, \mathrm{supp})$ if there exists a map $f^*\colon A \times \mathcal{P}(A) \to B$ such that $f = f^* \circ (\mathrm{first}, \mathrm{supp})|_{A^n}$ (see Definition 2.3.6).

Lemma 5.4.8. *Assume that $n \geq |A|$, and let $f\colon A^n \to B$. Then f is determined by* ofo *and $S_{[2,n]} \subseteq \mathrm{InvGr}\, f$ if and only if f is determined by* $(\mathrm{first}, \mathrm{supp})$.

Proof. Assume that $f = f^* \circ (\mathrm{first}, \mathrm{supp})|_{A^n}$ for some $f^*\colon A \times \mathcal{P}(A) \to B$. Define $f'\colon A^\sharp \to B$ by the rule $f'(\mathbf{a}) = f^*(\mathrm{first}(\mathbf{a}), \mathrm{supp}(\mathbf{a}))$ for all $\mathbf{a} = (a_1, \ldots, a_n) \in A^\sharp$. Since for all $\mathbf{a} = (a_1, \ldots, a_n) \in A^n$, it holds that $\mathrm{first}(\mathrm{ofo}(\mathbf{a})) = \mathrm{first}(\mathbf{a})$ and $\mathrm{supp}(\mathrm{ofo}(\mathbf{a})) = \mathrm{supp}(\mathbf{a})$, we have

$$f'(\mathrm{ofo}(\mathbf{a})) = f^*(\mathrm{first}(\mathrm{ofo}(\mathbf{a})), \mathrm{supp}(\mathrm{ofo}(\mathbf{a}))) = f^*(\mathrm{first}(\mathbf{a}), \mathrm{supp}(\mathbf{a})).$$

Therefore, $f = f' \circ \mathrm{ofo}|_{A^n}$. Furthermore, for every permutation $\sigma \in S_{[2,n]}$, the equalities $\mathrm{first}(\mathbf{a}\sigma) = \mathrm{first}(\mathbf{a})$ and $\mathrm{supp}(\mathbf{a}\sigma) = \mathrm{supp}(\mathbf{a})$ clearly hold. Thus,

$$f(\mathbf{a}\sigma) = f^*(\mathrm{first}(\mathbf{a}\sigma), \mathrm{supp}(\mathbf{a}\sigma)) = f^*(\mathrm{first}(\mathbf{a}), \mathrm{supp}(\mathbf{a})) = f(\mathbf{a}),$$

and we conclude that $S_{[2,n]} \subseteq \mathrm{InvGr}\, f$.

Assume then that $f = f^* \circ \mathrm{ofo}|_{A^n}$ and $S_{[2,n]} \subseteq \mathrm{InvGr}\, f$. Define the map $f'\colon A \times \mathcal{P}(A) \to B$ by the following rule: for any $a \in A$ and $S \subseteq A$ with $|S| = s$, if $a \in S$ then let $f'(a, S) := f^*(\mathbf{a})$, where $\mathbf{a} = (a_1, \ldots, a_s)$ is any tuple in $A^\sharp$ such that $a_1 = a$ and $\mathrm{supp}(\mathbf{a}) = S$; if $a \notin S$, then $f'(a, S)$ can be mapped to an arbitrary element of B. This definition is good, because if $\mathbf{a} = (a_1, \ldots, a_s)$ and $\mathbf{b} = (b_1, \ldots, b_s)$ are tuples in $A^\sharp$ such that $a_1 = a = b_1$ and $\mathrm{supp}(\mathbf{a}) = S = \mathrm{supp}(\mathbf{b})$, then there is a permutation $\sigma \in S_s$ such that $\sigma(1) = 1$ and $\mathbf{a}\sigma = \mathbf{b}$. Define $\tau \in S_n$ by the rule $\tau(i) = \sigma(i)$ for $i \in [s]$, and $\tau(i) = i$ for $i \in [n] \setminus [s]$; since $\tau(1) = \sigma(1) = 1$, we have $\tau \in S_{[2,n]} \subseteq \mathrm{InvGr}\, f$. Consequently,

$$\begin{aligned} f^*(\mathbf{a}) = f^*(\mathrm{ofo}(\mathbf{a})) &= f^*(\mathrm{ofo}(a_1, \ldots, a_s, \underbrace{a_1, \ldots, a_1}_{n-s})) \\ &= f^*(\mathrm{ofo}((a_1, \ldots, a_s, a_1, \ldots, a_1)\tau)) \\ &= f^*(\mathrm{ofo}(a_{\sigma(1)}, \ldots, a_{\sigma(s)}, a_1, \ldots, a_1)) \\ &= f^*(\mathrm{ofo}(\mathbf{a}\sigma)) = f^*(\mathbf{a}\sigma) = f^*(\mathbf{b}). \end{aligned}$$

Then, for any $\mathbf{a} \in A^n$, $\operatorname{ofo}(\mathbf{a}) \in A^\sharp$, and we have

$$f'(\operatorname{first}(\mathbf{a}), \operatorname{supp}(\mathbf{a})) = f'(\operatorname{first}(\operatorname{ofo}(\mathbf{a})), \operatorname{supp}(\operatorname{ofo}(\mathbf{a}))) = f^*(\operatorname{ofo}(\mathbf{a})).$$

Therefore, $f = f' \circ (\operatorname{first}, \operatorname{supp})|_{A^n}$. □

Lemma 5.4.9. *Assume that $f = f^* \circ (\operatorname{pr}_i^{(n)}, \operatorname{supp}|_{A^n})$ for some $i \in [n]$ and for some $f^* \colon A \times \mathcal{P}(A) \to B$. Then $f_I = f^* \circ (\operatorname{pr}_{\delta_I(i)}^{(n-1)}, \operatorname{supp}|_{A^{n-1}})$ for all $I \in \binom{[n]}{2}$.*

Proof. For any $I \in \binom{[n]}{2}$ and $\mathbf{a} \in A^{n-1}$, we have

$$\begin{aligned} f_I(\mathbf{a}) &= f(\mathbf{a}\delta_I) \\ &= f^*(\operatorname{pr}_i^{(n)}(\mathbf{a}\delta_I), \operatorname{supp}(\mathbf{a}\delta_I)) = f^*(\operatorname{pr}_{\delta_I(i)}^{(n-1)}(\mathbf{a}), \operatorname{supp}(\mathbf{a})). \end{aligned}$$ □

Theorem 5.4.10. *Let $n, k \in \mathbf{N}_+$ with $n \geq k+2$. Assume that $|B| = k$ and $f \colon A^n \to B$ is determined by* ofo *and $S_{[2,n]} \subseteq \operatorname{InvGr} f$. Then f is reconstructible.*

Proof. Lemma 5.4.8 implies that $f = f^* \circ (\operatorname{pr}_1^{(n)}, \operatorname{supp}|_{A^n})$ for some $f^* \colon A \times \mathcal{P}(A) \to B$. By Lemma 5.4.9, $f_I = f^* \circ (\operatorname{pr}_1^{(n-1)}, \operatorname{supp}|_{A^{n-1}})$ for all $I \in \binom{[n]}{2}$. Let $g \colon A^n \to B$ be a reconstruction of f. Then for every $I \in \binom{[n]}{2}$, there exists a permutation $\rho^I \in S_{n-1}$ such that

$$g_I = f^* \circ (\operatorname{pr}_1^{(n-1)}, \operatorname{supp}|_{A^{n-1}}) \circ \underline{\rho^I} = f^* \circ (\operatorname{pr}_{\rho^I(1)}^{(n-1)}, \operatorname{supp}|_{A^{n-1}}).$$

Let $r_I := \rho^I(1)$ and $s_I := \min \delta_I^{-1}(r_I)$. Then clearly either $s_I = \min I$ or $s_I \notin I$.

Assume first that there exists $s \in [n]$ such that $\delta_I(s) = r_I$ for all $I \in \binom{[n]}{2}$. Let $\mathbf{a} \in A^n$. Since $n > k$, we have $\mathbf{a} = \mathbf{b}\delta_I$ for some $\mathbf{b} \in A^{n-1}$ and $I \in \binom{[n]}{2}$. Therefore

$$\begin{aligned} g(\mathbf{a}) = g(\mathbf{b}\delta_I) &= g_I(\mathbf{b}) = f^*(b_{r_I}, \operatorname{supp}(\mathbf{b})) \\ &= f^*(a_s, \operatorname{supp}(\mathbf{a})) = f^*(\operatorname{pr}_s^{(n)}, \operatorname{supp}|_{A^n})(\mathbf{a}) = f(\mathbf{a}\tau), \end{aligned}$$

where $\tau = (1\ s) \in S_n$. Since this holds for all $\mathbf{a} \in A^n$, we conclude that $f \simeq g$.

Assume then that for every $s \in [n]$ there exists $I \in \binom{[n]}{2}$ such that $\delta_I(s) \neq r_I$. Consider first the case that for all $I \in \binom{[n]}{2}$, $\delta_I^{-1}(r_I) = I$. This implies that $r_I = s_I = \min I$ for all $I \in \binom{[n]}{2}$. Let $\mathbf{a} \in A^n$. Then $\mathbf{a} = \mathbf{b}\delta_I$ for some $\mathbf{b} \in A^{n-1}$ and $I \in \binom{[n]}{2}$. We have

$$g(\mathbf{a}) = g(\mathbf{b}\delta_I) = g_I(\mathbf{b}) = f^*(b_{r_I}, \operatorname{supp}(\mathbf{b})) = f^*(a_{s_I}, \operatorname{supp}(\mathbf{a})).$$

We claim that g is totally symmetric. For, let $\sigma \in S_n$. Then

$$\begin{aligned} g(\mathbf{a}\sigma) = g(\mathbf{b}\delta_I\sigma) &= g(\mathbf{b}\sigma_I\delta_{\sigma^{-1}(I)}) = g_{\sigma^{-1}(I)}(\mathbf{b}\sigma_I) \\ &= f^*(\operatorname{pr}_{r_{\sigma^{-1}(I)}}^{(n-1)}, \operatorname{supp}|_{A^{n-1}})(\mathbf{b}\sigma_I) = f^*(b_{r_I}, \operatorname{supp}(\mathbf{b}\sigma_I)) \\ &= f^*(b_{r_I}, \operatorname{supp}(\mathbf{b})) = f^*(a_{s_I}, \operatorname{supp}(\mathbf{a})) = g(\mathbf{a}), \end{aligned}$$

where the second equality holds by Lemma 4.1.9, and the fifth equality holds because $\sigma_I(r_{\sigma^{-1}(I)}) = \sigma_I(\min \sigma^{-1}(I)) = \min I = r_I$ by Fact 4.1.3. We conclude that g is totally symmetric and hence reconstructible by Proposition 3.3.1; thus $f \simeq g$.

Finally, consider the case that there exists $J \in \binom{[n]}{2}$ such that $\delta_J^{-1}(r_J) \neq J$. Then $s_J \notin J$. By our assumption, there exists $K \in \binom{[n]}{2}$ such that $\delta_K(s_J) \neq r_K$, i.e., $s_J \notin \delta_K^{-1}(r_K)$. We may assume, without loss of generality, that s_J and s_K lie in different blocks of the partition $\langle J, K\rangle_{\mathrm{part}} \in \mathrm{Part}(n)$. (If this is not the case, then it necessarily holds that $J \cap K \neq \emptyset$, $s_J \in K \setminus J$, $s_K \in J \setminus K$. Since $n \geq 4$, there exists a set $L \in \binom{[n]}{2}$ that is disjoint from J. Now, depending on whether or not L is disjoint from K and on the membership of s_L in the sets J, K and L, we can replace the sets J and K in the argument with certain other sets. Namely, if $L \cap K = \emptyset$ and $s_L \in K$ or $L \cap K \neq \emptyset$ and $s_L \in L$, then take sets K and L; otherwise take J and L.)

Since $n \geq k+2$, for any $S \subseteq A$ with $|S| \geq 2$ and for any $\alpha, \beta \in S$ with $\alpha \neq \beta$, there exists a tuple $\mathbf{u} \in A^n$ such that $\operatorname{supp} \mathbf{u} = S$, $u_{\min J} = u_{\max J}$, $u_{\min K} = u_{\max K}$, $u_{s_J} = \alpha$, and $u_{s_K} = \beta$. Such a tuple $\mathbf{u}$ satisfies $\mathbf{u} = \mathbf{v}\delta_J = \mathbf{w}\delta_K$ for tuples $\mathbf{v}, \mathbf{w} \in A^{n-1}$ with $u_i = v_{\delta_J(i)} = w_{\delta_K(i)}$ for all $i \in [n]$, and we have

$$\begin{aligned} f^*(\alpha, S) &= f^*(u_{s_J}, \operatorname{supp}(\mathbf{u})) = f^*(v_{r_J}, \operatorname{supp}(\mathbf{v})) \\ &= g_J(\mathbf{v}) = g(\mathbf{u}) = g_K(\mathbf{w}) \\ &= f^*(w_{r_K}, \operatorname{supp}(\mathbf{w})) = f^*(u_{s_K}, \operatorname{supp}(\mathbf{u})) = f^*(\beta, \operatorname{supp} u)). \end{aligned}$$

This implies that $f^*(\alpha, S) = f^*(\beta, S)$ for all $\alpha, \beta \in S$ and $S \subseteq A$. Therefore, f^* restricted to the range of $(\mathrm{first}, \operatorname{supp})|_{A^n}$ does not depend on its first argument. This means that f is determined by supp and is hence reconstructible by Proposition 3.3.3. Thus $f \simeq g$. □

An important consequence of Theorem 5.4.10 is that pseudo-Boolean functions determined by ofo are reconstructible.

Theorem 5.4.11. *Assume that $|A| = 2$ and $n \geq 4$. If $f\colon A^n \to B$ is determined by* ofo*, then f is reconstructible.*

Proof. By Proposition 5.3.3, $\operatorname{InvGr} f = S_{\Pi^{\uparrow n-2}}$ for some interval partition $\Pi \in \mathrm{Part}(2)$. There are only two (interval) partitions of $[2]$, namely $\{[2]\}$ and $\{\{1\},\{2\}\}$, and their expansions are $\{[2]\}^{\uparrow n-2} = \{[n]\}$ and $\{\{1\},\{2\}\}^{\uparrow n-2} = \{\{1\},[2,n]\}$. Thus $\operatorname{InvGr} f$ is either S_n or $S_{[2,n]}$. Theorem 5.4.10 now shows that f is reconstructible. □

According to Proposition 5.4.1, the lower bound $n \geq 4$ in Theorem 5.4.11 cannot be decreased. Observe also that the nonreconstructible ternary functions g and g' of Example 3.3.5 are determined by ofo.

A

POST CLASSES

The clones on the two-element set $\{0,1\}$ were determined by Post [75]. *Post classes,* i.e., clones on $\{0,1\}$, are listed below, and the lattice of clones on $\{0,1\}$, the so-called *Post's lattice,* is presented in Figure 1. We make use of the notation appearing in the paper by Foldes and Pogosyan [32], and Figure 1 is modeled after the illustration in [32].

- Ω is the clone of all Boolean functions.
- $T_0 := \mathrm{Pol}(0) = \{f \in \Omega \mid f(0,\dots,0) = 0\}$
  (0-preserving functions).
- $T_1 := \mathrm{Pol}(1) = \{f \in \Omega \mid f(1,\dots,1) = 1\}$
  (1-preserving functions).
- $T_c := T_0 \cap T_1$
  (constant-preserving functions).
- $M := \mathrm{Pol}\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$
  (monotone functions, i.e., functions $f\colon \{0,1\}^n \to \{0,1\}$ satisfying $f(a_1,\dots,a_n) \leq f(b_1,\dots,b_n)$ whenever $a_i \leq b_i$ for all $i \in [n]$).
- $M_0 := M \cap T_0, \quad M_1 := M \cap T_1, \quad M_c := M \cap T_c$.
- $S := \mathrm{Pol}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
  (self-dual functions, i.e., functions $f\colon \{0,1\}^n \to \{0,1\}$ satisfying $f(a_1,\dots,a_n) = 1 - f(1-a_1,\dots,1-a_n)$ for all $a_1,\dots,a_n \in \{0,1\}$).
- $S_c := S \cap T_c, \quad SM := S \cap M$.
- $L := \mathrm{Pol}\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$
  (polynomial operations of the group $(\{0,1\};+)$ of addition modulo 2, i.e., affine functions).
- $L_0 := L \cap T_0, \quad L_1 := L \cap T_1, \quad LS := L \cap S, \quad L_c := L \cap T_c$.

For $a \in \{0,1\}$, a set $S \subseteq \{0,1\}^n$ is *a-separating* if there is an index $i \in [n]$ such that for every $(a_1,\dots,a_n) \in S$ we have $a_i = a$. For $m \geq 2$, a function $f\colon \{0,1\}^n \to \{0,1\}$ is *a-separating of rank m* if every subset of $f^{-1}(a)$ of cardinality at most m is a-separating. A function $f\colon \{0,1\}^n \to \{0,1\}$ is *a-separating* if $f^{-1}(a)$ is a-separating.

- For $m \geq 2$, U_m is the clone of 1-separating functions of rank m.
- For $m \geq 2$, W_m is the clone of 0-separating functions of rank m.
- $U_\infty := \bigcap_{m \geq 2} U_m, \quad W_\infty := \bigcap_{m \geq 2} W_m$
  (1-separating and 0-separating functions, respectively).
- $T_c U_m := T_c \cap U_m, \quad T_c W_m := T_c \cap W_m, \quad$ for $m = 2, \ldots, \infty$.
- $M U_m := M \cap U_m, \quad M W_m := M \cap W_m, \quad$ for $m = 2, \ldots, \infty$.
- $M_c U_m := M_c \cap U_m, \quad M_c W_m := M_c \cap W_m, \quad$ for $m = 2, \ldots, \infty$.
- Λ is the clone of polynomial operations of the meet-semilattice $(\{0,1\}; \wedge)$.
- $\Lambda_0 := \Lambda \cap T_0, \quad \Lambda_1 := \Lambda \cap T_1, \quad \Lambda_c := \Lambda \cap T_c$.
- V is the clone of polynomial operations of the join-semilattice $(\{0,1\}; \vee)$.
- $V_0 := V \cap T_0, \quad V_1 := V \cap T_1, \quad V_c := V \cap T_c$.
- $\Omega(1) := \{f \in \Omega \mid \operatorname{ess} f \leq 1\}$
  (projections, negations, constants).
- $I^* := \Omega(1) \cap S$
  (projections, negations).
- $I := \Omega(1) \cap M$
  (projections, constants).
- $I_0 := I \cap T_0, \quad I_1 := I \cap T_1, \quad I_c := I \cap T_c$.

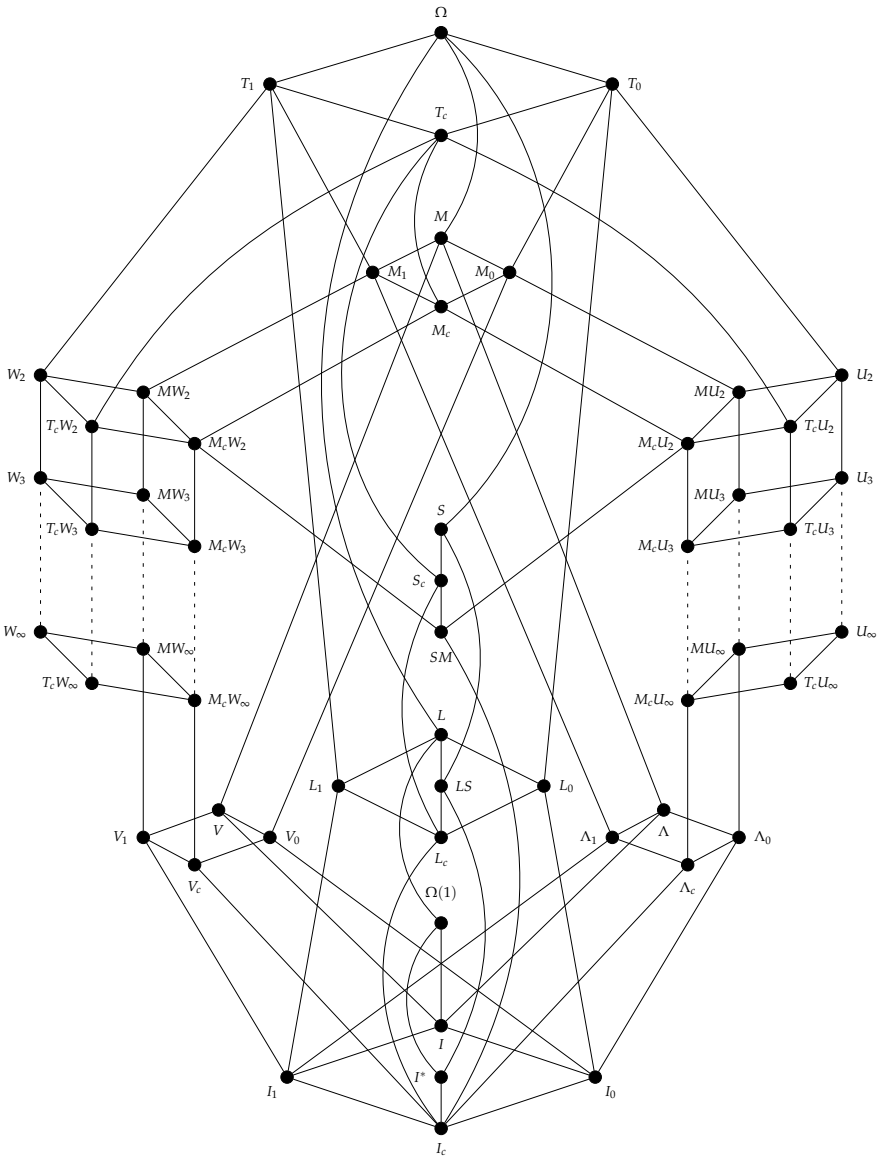


Figure 1: Post's lattice.

BIBLIOGRAPHY

[1] R. A. Beaumont, R. P. Peterson, Set-transitive permutation groups, *Canad. J. Math.* **7** (1955) 35–42.

[2] M. Behrisch, Galois theory for semiclones, *Algebra Universalis* **76** (2016) 385–413.

[3] C. Berge, R. Rado, Note on isomorphic hypergraphs and some extensions of Whitney's theorem to families of sets, *J. Comb. Theory Ser. B* **13** (1972) 226–241.

[4] J. Berman, A. Kisielewicz, On the number of operations in a clone, *Proc. Amer. Math. Soc.* **122** (1994) 359–369.

[5] V. G. Bodnarchuk, L. A. Kaluzhnin, V. N. Kotov, B. A. Romov, Galois theory for Post algebras. I, II (Russian), *Kibernetika* **5**(3) (1969) 1–10, **5**(5) (1969) 1–9. English translation: Galois theory for Post algebras. I, II, *Cybernetics* **5**(5) (1969) 243–252, 531–539. В. Г. Боднарчук, Л. А. Калужнин, В. Н. Котов, Б. А. Ромов, Теория Галуа для алгебр Поста. I, II, *Кибернетика* **5**(3) (1969) 1–10, **5**(5) (1969) 1–9.

[6] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997) 235–265.

[7] M. Bouaziz, M. Couceiro, M. Pouzet, Join-irreducible Boolean functions, *Order* **27** (2010) 261–282.

[8] P. J. Cameron, *Introduction to Algebra,* Oxford University Press, Oxford, 1998.

[9] P. J. Cameron, Homogeneous permutations, *Electron. J. Combin.* **9**(2) (2002) #R2, 9 pp.

[10] P. Clote, E. Kranakis, Boolean functions, invariance groups, and parallel complexity, *SIAM J. Comput.* **20** (1991) 553–590.

[11] M. Couceiro, S. Foldes, On closed sets of relational constraints and classes of functions closed under variable substitutions, *Algebra Universalis* **54** (2005) 149–165.

[12] M. Couceiro, S. Foldes, Functional equations, constraints, definability of function classes, and functions of Boolean variables, *Acta Cybernet.* **18** (2007) 61–75.

[13] M. Couceiro, E. Lehtonen, Generalizations of Świerczkowski's lemma and the arity gap of finite functions, *Discrete Math.* **309** (2009) 5905–5912.

[14] M. Couceiro, E. Lehtonen, The arity gap of polynomial functions over bounded distributive lattices, *40th IEEE International Symposium on Multiple-Valued Logic* (*ISMVL 2010*), IEEE Computer Society, Los Alamitos, 2010, pp. 113–116.

[15] M. Couceiro, E. Lehtonen, Galois theory for sets of operations closed under permutation, cylindrification, and composition, *Algebra Universalis* **67** (2012) 273–297.

[16] M. Couceiro, E. Lehtonen, Majors of functions, *Order* **35** (2018) 233–246.

[17] M. Couceiro, E. Lehtonen, K. Schölzel, Hypomorphic Sperner systems and non-reconstructible functions, *Order* **32** (2015) 255–292.

[18] M. Couceiro, E. Lehtonen, K. Schölzel, Set-reconstructibility of Post classes, *Discrete Appl. Math.* **187** (2015) 12–18.

[19] M. Couceiro, E. Lehtonen, T. Waldhauser, On the arity gap of aggregation functions, in: D. Dubois, M. Grabisch, R. Mesiar, E. P. Klement (eds.), *32nd Linz Seminar on Fuzzy Set Theory* (*LINZ 2011*) – *Decision Theory: Qualitative and Quantitative Approaches,* Johannes Kepler Universität, Linz, 2011, pp. 25–28.

[20] M. Couceiro, E. Lehtonen, T. Waldhauser, Decompositions of functions based on arity gap, *Discrete Math.* **312** (2012) 238–247.

[21] M. Couceiro, E. Lehtonen, T. Waldhauser, The arity gap of order-preserving functions and extensions of pseudo-Boolean functions, *Discrete Appl. Math.* **160** (2012) 383–390

[22] M. Couceiro, E. Lehtonen, T. Waldhauser, Parametrized arity gap, *Order* **30** (2013) 557–572.

[23] M. Couceiro, M. Pouzet, On a quasi-ordering on Boolean functions, *Theoret. Comput. Sci.* **396** (2008) 71–87.

[24] B. A. Davey, H. A. Priestley, *Introduction to Lattices and Order,* 2nd ed., Cambridge University Press, New York, 2002.

[25] K. Denecke, M. Erné, S. L. Wismath (eds.), *Galois Connections and Applications,* Math. Appl., vol. 565, Kluwer Academic Publishers, Dordrecht, 2004.

[26] K. Denecke, S. L. Wismath, *Universal Algebra and Applications in Theoretical Computer Science,* Chapman & Hall/CRC, Boca Raton, 2002.

[27] J. D. Dixon, B. Mortimer, *Permutation Groups,* Grad. Texts in Math., vol. 163, Springer-Verlag, New York, 1996.

[28] O. Ekin, S. Foldes, P. L. Hammer, L. Hellerstein, Equational characterizations of Boolean function classes, *Discrete Math.* **211** (2000) 27–51.

[29] M. N. Ellingham, Recent progress in edge-reconstruction, Seventeenth Manitoba Conference on Numerical Mathematics and Computing, *Congr. Numer.* **62** (1988) 3–20.

[30] A. Feigelson, L. Hellerstein, The forbidden projections of unate functions, *Discrete Appl. Math.* **77** (1997) 221–236.

[31] S. Foldes, *Fundamental Structures of Algebra and Discrete Mathematics,* John Wiley & Sons, Inc., New York, 1994.

[32] S. Foldes, G. R. Pogosyan, Post classes characterized by functional terms, *Discrete Appl. Math.* **142** (2004) 35–51.

[33] D. Geiger, Closed systems of functions and predicates, *Pacific J. Math.* **27** (1968) 95–100.

[34] R. L. Goodstein, The solution of equations in a lattice, *Proc. Roy. Soc. Edinburgh Sect. A* **67** (1965/1967) 231–242.

[35] M. Grech, A. Kisielewicz, Symmetry groups of Boolean functions, *European J. Combin.* **40** (2014) 1–10.

[36] J. A. Green, On the structure of semigroups, *Ann. of Math.* (2) **54** (1951) 163–172.

[37] F. Harary, On the reconstruction of a graph from a collection of subgraphs, in: *Theory of Graphs and Its Applications* (Proc. Sympos. Smolenice, 1963), Publ. House Czechoslovak Acad. Sci., Prague, 1964, pp. 47–52.

[38] W. Harnau, Ein verallgemeinerter Relationenbegriff für die Algebra der mehrwertigen Logik, Teil I (Grundlagen), Teil II (Relationenpaare), Teil III (Beweis), *Rostock. Math. Kolloq.* **28** (1985) 5–17, **31** (1987) 11–20, **32** (1987) 15–24.

[39] M. A. Harrison, On the classification of Boolean functions by the general linear and affine groups, *J. Soc. Indust. Appl. Math.* **12**(2) (1964) 285–299.

[40] L. Hellerstein, On generalized constraints and certificates, *Discrete Math.* **226** (2001) 211–232.

[41] J. Henno, Green relations in Menger systems (Russian), Я. Хенно, Эквивалентности Грина в системах Менгера, *Tartu Riikl. Ül. Toimetised* **277** (1971) 37–46.

[42] E. Horváth, G. Makay, R. Pöschel, T. Waldhauser, Invariance groups of finite functions and orbit equivalence of permutation groups, *Open Math.* **13** (2015) 83–95.

[43] A. Hulanicki, S. Świerczkowski, Number of algebras with a given set of elements, *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **8** (1960) 283–284.

[44] J. I. Janov, A. A. Muchnik, Existence of k-valued closed classes without a finite basis (Russian), *Dokl. Akad. Nauk SSSR* **127** (1959) 44–46.
Ю. И. Янов, А. А. Мучник, О существовании k-значных замкнутых классов не имеюших конечного базиса, *Докл. АН СССР* **127** (1959) 44–46.

[45] P. J. Kelly, A congruence theorem for trees, *Pacific J. Math.* **7** (1957) 961–968.

[46] S. Kerkhoff, R. Pöschel, F. M. Schneider, A short introduction to clones, Proceedings of the Workshop on Algebra, Coalgebra and Topology (WACT 2013), *Electron. Notes Theor. Comput. Sci.* **303** (2014) 107–120.

[47] A. Kisielewicz, Symmetry groups of Boolean functions and constructions of permutation groups, *J. Algebra* **199** (1998) 379–403.

[48] S. Kitayev, *Patterns in Permutations and Words,* Monogr. Theoret. Comput. Sci. EATCS Ser., Springer, Heidelberg, 2011.

[49] W. L. Kocay, A family of nonreconstructible hypergraphs, *J. Combin. Theory Ser. B* **42** (1987) 46–63.

[50] W. L. Kocay, Z. M. Lui, More non-reconstructible hypergraphs, *Discrete Math.* **72** (1988) 213–224.

[51] S. Lang, *Algebra,* rev. 3rd ed., Springer, New York, 2002.

[52] D. Lau, *Function Algebras on Finite Sets. A Basic Course on Many-Valued Logic and Clone Theory,* Springer Monogr. Math., Springer, Berlin, 2006.

[53] E. Lehtonen, Descending chains and antichains of the unary, linear, and monotone subfunction relations, *Order* **23** (2006) 129–142.

[54] E. Lehtonen, A note on minors determined by clones of semilattices, *Novi Sad J. Math.* **40**(3) (2010) 75–81.

[55] E. Lehtonen, Closed classes of functions, generalized constraints, and clusters, *Algebra Universalis* **63** (2010) 203–234.

[56] E. Lehtonen, Totally symmetric functions are reconstructible from identification minors, *Electron. J. Combin.* **21**(2) (2014) #P2.6, 24 pp.

[57] E. Lehtonen, Reconstructing multisets over commutative groupoids and affine functions over nonassociative semirings, *Internat. J. Algebra Comput.* **24** (2014) 11–31.

[58] E. Lehtonen, Reconstructing permutations from identification minors, *Electron. J. Combin.* **22**(4) (2015) #P4.20, 21 pp.

[59] E. Lehtonen, On functions with a unique identification minor, *Order* **33** (2016) 71–80.

[60] E. Lehtonen, Content and singletons bring unique identification minors, *J. Aust. Math. Soc.*, to appear.

[61] E. Lehtonen, J.-L. Marichal, B. Teheux, Associative string functions, *Asian-Eur. J. Math.* **7**(4) (2014) 1450059, 18 pp.

[62] E. Lehtonen, J. Nešetřil, Minors of Boolean functions with respect to clique functions and hypergraph homomorphisms, *European J. Combin.* **31** (2010) 1981–1995.

[63] E. Lehtonen, R. Pöschel, Permutation groups, pattern involvement, and Galois connections, *Acta Sci. Math. (Szeged)* **83** (2017) 355–375.

[64] E. Lehtonen, Á. Szendrei, Equivalence of operations with respect to discriminator clones, *Discrete Math.* **309** (2009) 673–685.

[65] E. Lehtonen, Á. Szendrei, The submaximal clones on the three-element set with finitely many relative $\mathcal{R}$-classes, *Discuss. Math. Gen. Algebra Appl.* **30** (2010) 7–33.

[66] E. Lehtonen, Á. Szendrei, Clones with finitely many relative $\mathcal{R}$-classes, *Algebra Universalis* **65** (2011) 109–159.

[67] E. Lehtonen, Á. Szendrei, Partial orders induced by quasilinear clones, *Contributions to General Algebra* **20**, Proceedings of the Salzburg Conference 2011 (AAA81), Verlag Johannes Heyn, Klagenfurt, 2012, pp. 51–84.

[68] A. I. Mal'cev, Iterative algebras and Post varieties (Russian), *Algebra Logika* **5**(2) (1966) 5–24.
А. И. Мальцев, Итеративные алгебры и многообразия Поста, *Алгебра и логика* **5**(2) (1966) 5–24.

[69] B. Manvel, P. K. Stockmeyer, On reconstruction of matrices, *Math. Mag.* **44** (1971) 218–221.

[70] B. D. McKay, Small graphs are reconstructible, *Australas. J. Combin.* **15** (1997) 123–126.

[71] M. Monks, The solution to the partition reconstruction problem, *J. Combin. Theory Ser. A* **116** (2009) 76–91.

[72] N. Pippenger, Galois theory for minors of finite functions, *Discrete Math.* **254** (2002) 405–419.

[73] R. Pöschel, Concrete representation of algebraic structures and a general Galois theory, in: H. Kautschitsch, W. B. Müller, W. Nöbauer (eds.), *Contributions to General Algebra* (Proc. Klagenfurt Conf., Klagenfurt, 1978), Johannes Heyn, Klagenfurt, 1979, pp. 249–272.

[74] R. Pöschel, L. A. Kalužnin, *Funktionen- und Relationenalgebren. Ein Kapitel der diskreten Mathematik,* VEB Deutscher Verlag der Wissenschaften, Berlin, 1979.

[75] E. L. Post, *The Two-Valued Iterative Systems of Mathematical Logic,* Annals of Mathematics Studies, no. 5, Princeton University Press, Princeton, 1941.

[76] H. J. Prömel, B. Voigt, Hereditary attributes of surjections and parameter sets, *European J. Combin.* **7** (1986) 161–170.

[77] J.-X. Rampon, What is reconstruction for ordered sets?, *Discrete Math.* **291** (2005) 191–233.

[78] I. G. Rosenberg, Á. Szendrei, Degrees of clones and relations, *Houston J. Math.* **9** (1983) 545–580.

[79] A. Salomaa, On essential variables of functions, especially in the algebra of logic, *Ann. Acad. Sci. Fenn. Ser. A I. Math.* **339** (1963) 3–11.

[80] P. K. Stockmeyer, A census of nonreconstructible digraphs. I. Six related families, *J. Combin. Theory Ser. B* **31** (1981) 232–239.

[81] L. Szabó, Concrete representation of related structures of universal algebras. I, *Acta Sci. Math.* (*Szeged*) **40** (1978) 175–184.

[82] Á. Szendrei, *Clones in Universal Algebra,* Séminaire de Mathématiques Supérieures, vol. 99, Presses de l'Université de Montréal, Montreal, 1986.

[83] Á. Szendrei, Rosenberg-type completeness criteria for subclones of Słupecki's clone, *IEEE 42nd International Symposion on Multiple-Valued Logic* (*ISMVL 2012*), IEEE Computer Society, Los Alamitos, 2012, pp. 349–354.

[84] S. M. Ulam, *A Collection of Mathematical Problems,* Interscience Tracts in Pure and Applied Mathematics, no. 8, Interscience Publishers, New York–London, 1960.

[85] C. Wang, Boolean minors, *Discrete Math.* **141** (1995) 237–258.

[86] C. WANG, A. C. WILLIAMS, The threshold order of a Boolean function, *Discrete Appl. Math.* **31** (1991) 51–69.

[87] R. WILLARD, Essential arities of term operations in finite algebras, *Discrete Math.* **149** (1996) 239–259.

[88] I. E. ZVEROVICH, Characterizations of closed classes of Boolean functions in terms of forbidden subfunctions and Post classes, *Discrete Appl. Math.* **149** (2005) 200–218.

$\mathbf{N}$	set of all nonnegative integers	4
$\mathbf{N}_+$	set of all positive integers	4
$[a, b]$	interval $\{a, \ldots, b\}$	4
$[n]$	the set $\{1, \ldots, n\}$	4
$\mathcal{P}(S)$	power set of a set S	4
$\binom{S}{k}$	set of all k-element subsets of a set S	4
A^n	Cartesian power of a set A	4
A^*	set of all words over A	4
A^+	set of all nonempty words over A	4
ε	empty word	4
$A^n_{\neq}$	set of all n-tuples over A with pairwise distinct entries	4
$A^\sharp$	set of all tuples over A with pairwise distinct entries	4
$x/\equiv$	$\equiv$-equivalence class of x	4
$A/\equiv$	quotient set of A by $\equiv$	4
x/Π	block of partition Π containing x	4
$\equiv_\Pi$	equivalence relation corresponding to a partition Π	4
$\sqsubseteq$	refinement relation of partitions	5
$\mathrm{Part}(n)$	set of all partitions of $[n]$	5
$\mathrm{Part}_m(n)$	set of all m-partitions of $[n]$	5
Δ_n	trivial partition of $[n]$	5
$\mathrm{IntPart}(n)$	set of all interval partitions of $[n]$	5
$\mathrm{IntPart}_m(n)$	set of all interval m-partitions of $[n]$	5
$\langle \mathcal{S} \rangle_{\mathrm{part}}$	partition of $[n]$ induced by $\mathcal{S}$	5
$g \circ f$, gf	composite function	6
φ'	map φ lifted to power sets	6
$\mathrm{Im}\, f$	range (image) of a function f	6
$f\|_S$	restriction of a function f to a subset S of its domain	6
$\ker f$	kernel of a function f	6
id	identity map	7
S_n	symmetric group	7
A_n	alternating group	7
S_X	group of permutations fixing $[n] \setminus X$	7
A_X	group of even permutations fixing $[n] \setminus X$	7
$G \leq G'$	subgroup relation	7
$\langle P \rangle$	permutation group generated by a set P of permutations	7

S_Π	group of all permutations preserving the blocks of a partition Π	7
A_Π	group of all even permutations preserving the blocks of a partition Π	7
$\leq_\Pi$	standard ordering of the blocks of a partition Π	8
$\leq_\Pi^\sigma$	ordering of the blocks of a partition Π relative to a permutation σ	8
nat_Π	natural surjection $[n] \to \Pi$	9
h_Π^σ	order-isomorphism $([m]; \leq) \to (\Pi; \leq_\Pi^\sigma)$	9
h_Π	order-isomorphism $([m]; \leq) \to (\Pi; \leq_\Pi)$	9
δ_Π	rigid surjection with kernel Π	9
σ_Π	minor of a permutation σ relative to a partition Π	9, 47
Π/Γ	a partition of a partition Π relative to a partition Γ	9
$\Phi^\flat$	flattening of a partition Φ	9
$\mathbf{1}_M$	multiplicity function	14
$\lvert M\rvert$	cardinality of a multiset M	14
$\mathcal{M}(X)$	set of all finite multisets	14
$\langle a_i : i \in I\rangle$	multiset	14
$M \uplus M'$	sum of multisets M and M'	14
$M \setminus M'$	difference of multisets M and M'	14
$M \cap M'$	intersection of multisets M and M'	14
$\mathcal{F}_{AB}^{(n)}$	set of all n-ary functions from A to B	15
$\mathcal{O}_A^{(n)}$	set of all n-ary operations on A	15
$\mathcal{F}_{AB}$	set of all functions of several arguments from A to B	15
$\mathcal{O}_A$	set of all operations on A	15
$\mathcal{C}^{(n)}$	n-ary part of a set $\mathcal{C}$ of functions	15
$\mathrm{Ess}\, f$	set of indices of essential arguments of f	16
$\mathrm{ess}\, f$	essential arity of f	16
$\underline{\sigma}$	map $A^V \to A^W$ acting on tuples induced by a map $\sigma\colon W \to V$	16
$f \leq g$	minor relation of functions	16
$f \equiv g$	minor-equivalence of functions	17
$f \simeq g$	similarity of functions	18
f_Π	minor of f relative to a partition Π	20
f_I	identification minor of f	20
$\mathrm{diag}\, f$	diagonal of f	21
supp	function mapping each $\mathbf{a} \in A^*$ to the set of entries of $\mathbf{a}$	23
oddsupp	function mapping each $\mathbf{a} \in A^*$ to the set of elements occurring an odd number of times in $\mathbf{a}$	23

$\operatorname{gap} f$	arity gap of f	23
$\operatorname{qa} f$	quasi-arity of f	24
$\operatorname{InvGr} f$	invariance group of f	24
ofo	function mapping each $\mathbf{a} \in A^*$ to the list of elements occurring in $\mathbf{a}$ in the order of first occurrence	25, 74
ms	function mapping each $\mathbf{a} \in A^*$ to its content, i.e., the multiset of entries of $\mathbf{a}$	25
sng	function mapping each $\mathbf{a} \in A^*$ to the list of its singletons, i.e., elements occurring exactly once in $\mathbf{a}$	25
cs	function mapping each $\mathbf{a} \in A^*$ to its content and singletons	25
$f(g_1, \ldots, g_n)$	composition of functions of several arguments	26
$\operatorname{pr}_i^{(n)}$	i-th n-ary projection	27
$\mathcal{L}_A$	lattice of clones on A	27
$\mathcal{I}_A$	clone of projections on A	27
ζ, τ, Δ, ∇, $*$	operations of iterative algebra	27
$\mathcal{R}_A^{(m)}$	set of all m-ary relations on A	28
$\mathcal{R}_A$	set of all finitary relations on A	28
$\mathbf{M} \prec \rho$	$\mathbf{M}$ is a matrix whose columns are tuples in the relation ρ	28
$f(\mathbf{M})$	application of f to the rows of a matrix $\mathbf{M}$	28
$f \triangleright \rho$	a function f preserves a relation ρ	28
$\operatorname{Pol} \mathcal{R}$	polymorphisms of a set $\mathcal{R}$ of relations	28
$\operatorname{Inv} \mathcal{F}$	invariants of a set $\mathcal{F}$ of functions	28
$\mathcal{K}_{AB}^{(m)}$	set of all m-ary constraints from A to B	29
$\mathcal{K}_{AB}$	set of all finitary constraints from A to B	29
$f \leq_{\mathcal{C}} g$	$\mathcal{C}$-minor relation of functions	31
$f \equiv_{\mathcal{C}} g$	$\mathcal{C}$-equivalence relation of functions	31
$\dot\cup$	disjoint union of posets	31
$\times_{\mathrm{lex}}$	lexicographic product of posets	31
$\mathcal{O}$	collection of objects	33
I_n	index set	33
O_i	derived object	33
$\operatorname{deck} O$	deck of an object O	33
$\operatorname{set\text{-}deck} O$	set-deck of an object O	34
$\vee$, $\wedge$	lattice operations (join and meet)	42
$\mathcal{A}_{\min}$	minimal elements of a set $\mathcal{A} \subseteq \mathcal{P}([n])$	42
$\mathbf{P}$	set of all finite permutations	47
$\tau \leq \sigma$	minor relation of permutations	47
r	rank function	48
$\sigma \oplus \tau$	direct sum of permutations σ and τ	50
$\sigma[\tau_1, \ldots, \tau_n]$	inflation of a permutation σ by $\tau_1, \ldots, \tau_n$	50

$\mathrm{Comp}^{(n)} S$	set of all n-permutations compatible with a set $S \subseteq S_\ell$ of permutations	52
$\mathrm{Min}^{(\ell)} T$	set of all ℓ-minors of a set $T \subseteq S_n$ of permutations	52
$\mathrm{gComp}^{(n)} G$	subgroup of S_n generated by $\mathrm{Comp}^{(n)} G$	53
$\mathrm{gMin}^{(\ell)} H$	subgroup of S_ℓ generated by $\mathrm{Min}^{(\ell)} H$	53
$d(B, C)$	distance between sets B and C	55
$\Pi^{\downarrow}$	compression of a partition Π	55
$\Pi^{\uparrow}$	expansion of a partition Π	55
$\mu(\Pi)$	minimum distance between nontrivial blocks of a partition Π	60
θ_n, λ_k^ℓ	special permutations	61
$\mathrm{Aut}\,\rho$	automorphisms of a relation ρ	62
$\mathrm{fiip}(\sigma)$	finest invariant interval partition of a permutation σ	62
ΔS	set of differences between elements of a subset S of a group	64, 72
$\mathbf{a} \approx \mathbf{b}$	tuples $\mathbf{a}$ and $\mathbf{b}$ are order-isomorphic	65
$\sigma^{(\leq k)}$	special minor of a permutation σ	69
η_Π	function mapping each element to the minimum of its Π-block	73
$\mathsf{OFO}^{(n)}$	set of all n-ary functions that are, up to similarity, determined by ofo	75
OFO	set of all functions that are, up to similarity, determined by ofo	75
$A_n^\sharp$	set of all nonempty words over A of length at most n with pairwise distinct entries	75
first	function that maps each string to its first letter	86

DECLARATION

Erklärung gemäß §6 Abs. 2, Ziffer 2 der Habilitationsordnung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbst und ohne unzulässige Hilfe Dritter und ohne andere als die darin angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen wörtlich oder inhaltlich übernommenen Stellen wurden als solche gekennzeichnet.

Bei allen eingereichten gemeinschaftlichen Arbeiten erstreckt sich meine Mitarbeit auf sämtliche Aspekte des Forschungsprozesses, einschließlich der Ideenfindung, der Ausarbeitung und der Dokumentation der Ergebnisse.

Es wurden zuvor keine Habilitationsvorhaben unternommen.

Ich erkenne die Habilitationsordnung der Fakultät für Mathematik und Naturwissenschaften der Technischen Universität Dresden vom 12. Dezember 2010, in der geänderten Fassung mit Gültigkeit vom 19. Februar 2014, an.

Erkko Lehtonen