Graph Homomorphisms and Universal Algebra
Course Notes

Manuel Bodirsky,
Institut für Algebra, TU Dresden,
Manuel.Bodirsky@tu-dresden.de

February 16, 2019

Disclaimer: these are course notes in draft state, and they probably contain many mistakes; please report them to manuel.bodirsky@tu-dresden.de.

Contents

1 The Basics 3
  1.1 Graphs and Digraphs ............................................. 3
  1.2 Graph Homomorphisms ........................................... 5
  1.3 The $H$-colouring Problem and Variants ....................... 8
  1.4 Cores ................................................................ 9
  1.5 Polymorphisms ..................................................... 12

2 The Arc-consistency Procedure 12
  2.1 The Power Graph .................................................... 15
  2.2 Tree Duality ......................................................... 16
  2.3 Totally Symmetric Polymorphisms ............................. 18
  2.4 Semilattice Polymorphisms ...................................... 19

3 The Path-consistency Procedure 20
  3.1 Majority Polymorphisms ......................................... 22
  3.2 Near-unanimity Polymorphisms ................................. 24
  3.3 Maltsev Polymorphisms .......................................... 25

4 Logic 27
  4.1 From Structures to Formulas .................................... 28
  4.2 From Formulas to Structures .................................... 29
  4.3 Primitive Positive Definability ............................... 29
  4.4 Cores and Constants ............................................. 30
  4.5 Primitive Positive Interpretations ............................ 31
  4.6 The Structure-Building Operators $H$, $C$, and $PP$ .......... 34
Prerequisites. This course is designed for students of mathematics or computer science that already had an introduction to discrete structures. Almost all notions that we use in this text will be formally introduced, with the notable exception of basic concepts from complexity theory. For example, we do not formally introduce the class of polynomial-time computable functions and NP-completeness, even though these concept are used when we discuss computational aspects of graph homomorphisms. Here we refer to an introduction to the theory of computation as for instance the book of Papadimitriou [42].

The text contains 64 exercises; the ones with a star are harder.
1 The Basics

1.1 Graphs and Digraphs

The concepts in this section are probably known to most students, and can safely be skipped; the section fixes standard terminology and conventions from graph theory and can be consulted later if needed. We want to remark that almost all definitions in this section have the section fixes standard terminology and conventions from graph theory and can be con-

The concepts in this section are probably known to most students, and can safely be skipped; the section fixes standard terminology and conventions from graph theory and can be consulted later if needed. We want to remark that almost all definitions in this section have generalisations to relational structures; however, we focus exclusively on graphs in this section since they allow to reach the key ideas of the underlying theory with a minimum of notation.

A directed graph (also digraph) $G$ is a pair $(V, E)$ of a set $V = V(G)$ of vertices and a binary relation $E = E(G)$ on $V$. Note that in general we allow that $V$ is an infinite set. For some definitions, we require that $V$ be finite, in which case we say that $G$ is a finite digraph. The elements $(u, v)$ of $E$ are called the arcs (or directed edges) of $G$. Note that we allow loops, i.e., arcs of the form $(u, u)$; a digraph without loops is called loopless. If $(u, v) \in E(G)$ is an arc, and $w \in V(G)$ is a vertex such that $w = u$ or $w = v$, then we say that $(u, v)$ and $w$ are incident.

An (undirected) graph is a pair $(V, E)$ of a set $V = V(G)$ of vertices and a set $E = E(G)$ of edges, each of which is an unordered pair of (not necessarily distinct) elements of $V$. In other words, we explicitly allow loops, which are edges that link a vertex with itself. Undirected graphs can be viewed as symmetric digraphs: a digraph $G = (V, E)$ is called symmetric if $(u, v) \in E$ if and only if $(v, u) \in E$. For a digraph $G$, we say that $G'$ is the undirected graph of $G$ if $G'$ is the undirected graph where $\{u, v\} \in E(G')$ iff $(u, v) \in E(G)$ or $(v, u) \in E(G)$. For an undirected graph $G$, we say that $G'$ is an orientation of $G$ if $G'$ is a directed graph such that $V(G') = V(G)$ and $E(G')$ contains for each edge $\{u, v\} \in E(G)$ either the arc $(u, v)$ or the arc $(v, u)$, and no other arcs.

For some notions for digraphs $G$ one can just use the corresponding notions for undirected graphs applied to the undirected graph of $G$; conversely, most notions for directed graphs, specialised to symmetric graphs, translate to notions for the respective undirected graphs.

1.1.1 Examples of graphs, and corresponding notation

- The complete graph on $n$ vertices $\{1, \ldots, n\}$, denoted by $K_n$. This is an undirected graph on $n$ vertices in which every vertex is joined with any other distinct vertex (so $K_n$ contains no loops).
- The cyclic graph on $n$ vertices, denoted by $C_n$; this is the undirected graph with the vertex set $\{0, \ldots, n-1\}$ and edge set
  \[ \{\{0,1\}, \ldots, \{n-2,n-1\}, \{n-1,0\}\} = \{\{u,v\} \mid u - v = 1 \mod n\}. \]
- The directed cycle on $n$ vertices, denoted by $\vec{C}_n$; this is the digraph with the vertex set $\{0, \ldots, n-1\}$ and the arcs $\{(0,1), \ldots, (n-2,n-1), (n-1,0)\}$.
- The path with $n+1$ vertices and $n$ edges, denoted by $P_n$; this is an undirected graph with the vertex set $\{0, \ldots, n\}$ and edge set $\{\{0,1\}, \ldots, \{n-1,n\}\}$.
- The directed path with $n+1$ vertices and $n$ edges, denoted by $\vec{P}_n$; this is a digraph with the vertex set $\{0, \ldots, n\}$ and edge set $\{(0,1), \ldots, (n-1,n)\}$.
• A tournament is a directed loopless graph $G$ with the property that for all distinct vertices $x, y$ either $(x, y)$ or $(y, x)$ is an edge of $G$, but not both.

• The transitive tournament on $n \geq 2$ vertices, denoted by $T_n$; this is a directed graph with the vertex set $\{1, \ldots, n\}$ where $(i, j)$ is an arc if and only if $i < j$.

Let $G$ and $H$ be graphs (we define the following notions both for directed and for undirected graphs). Then $G \sqcup H$ denotes the disjoint union of $G$ and $H$, which is the graph with vertex set $V(G) \cup V(H)$ (we assume that the two vertex sets are disjoint; if they are not, we take a copy of $H$ on a disjoint set of vertices and form the disjoint union of $G$ with the copy of $H$) and edge set $E(G) \cup E(H)$. A graph $G'$ is a subgraph of $G$ if $V(G') \subseteq V(G)$ and $E(G') \subseteq E(G)$. A graph $G'$ is an induced subgraph of $G$ if $V' = V(G') \subseteq V(G)$ and $(u, v) \in E(G')$ if and only if $(u, v) \in E(G')$ for all $u, v \in V'$. We also say that $G'$ is induced by $V'$ in $G$, and write $G[V']$ for $G'$. We write $G - u$ for $G[V(G) \setminus \{u\}]$, i.e., for the subgraph of $G$ where the vertex $u$ and all incident arcs are removed.

We call $|V(G)| + |E(G)|$ the size of a graph $G$; note that the size of a graph $G$ reflects the length of the representation of $G$ as a bit-string (under a reasonable choice of graph representations). This quantity will be important when we analyse the efficiency of algorithms on graphs.

1.1.2 Paths and Cycles

We start with definitions for directed paths; the corresponding terminology is then also used for undirected graphs as explained in the beginning of this section.

A sequence $(u_1, \ldots, u_k)$ of vertices of $G$ is called a path (from $u_1$ to $u_k$, of $G$) if $(u_i, u_{i+1}) \in E(G)$ or $(u_{i+1}, u_i) \in E(G)$ for every $1 \leq i < k$. If $(u_i, u_{i+1}) \in E(G)$ for every $1 \leq i \leq k - 1$, then the path is called directed. If no vertices of the path are repeated, we say that the path is simple. We write $|P| := k - 1$ for the length of a path $P = (u_1, \ldots, u_k)$ (i.e., we are counting the number of directed edges of $P$). The net length of $P$ is the difference between the number of forward and the number of backward edges. Hence, a path is directed if and only if its length equals its net length.

A sequence $(u_1, \ldots, u_k)$ is called a cycle (of $G$) if it is a path and additionally $(u_k, u_1) \in E^G$ or $(u_1, u_k) \in E^G$. If no vertices of the cycle are repeated we say that the cycle is simple. We write $|C| := k$ for the length of the cycle $C = (u_1, \ldots, u_k)$. The net length of $C$ is the net length of the path $(u_1, \ldots, u_k, u_1)$. A cycle $(u_1, \ldots, u_k)$ of $G$ is called directed if $(u_1, \ldots, u_k)$ is a directed path and additionally $(u_k, u_1) \in E^G$.

A digraph $G$ is called (weakly) connected if there is a path in $G$ between any two vertices of $G$. Equivalently, $G$ is connected if and only if it cannot be written as $H_1 \sqcup H_2$ for digraphs $H_1, H_2$ with at least one vertex each. A connected component of $G$ is a maximal (with respect to inclusion of the vertex sets) connected induced subgraph of $G$. A digraph $G$ is called strongly connected if for all vertices $x, y \in V(G)$ there is a directed path from $x$ to $y$ in $G$. Two vertices $u, v \in V(G)$ are at distance $k$ in $G$ if the shortest path from $u$ to $v$ in $G$ has length $k$.

Some particular notions for undirected graphs $G$. A (simple) cycle of $G$ is a sequence $(v_1, \ldots, v_k)$ of $k \geq 3$ pairwise distinct vertices of $G$ such that $(v_i, v_{i+1}) \in E(G)$ for all $1 \leq i < k - 1$. An undirected graph is called acyclic if is does not contain a cycle. A sequence $u_1, \ldots, u_k \in V(G)$ is called a (simple) path from $u_1$ to $u_k$ in $G$ iff $(u_i, u_{i+1}) \in E(G)$ for all $1 \leq i < k$ and if all vertices $u_1, \ldots, u_k$ are pairwise distinct. We allow the case that
is not the only natural graph property that can be described in terms of homomorphisms: be denoted by $D$. Let $\leq$ be a binary relation defined on $D$ as follows: we set $C_1 \leq C_2$ if there exists a graph $H_1 \in C_1$ and a digraph $H_2 \in C_2$ such that $H_1 \rightarrow H_2$ (note that this definition does not depend on the choice of the representatives $H_1$ of $C_1$ and $H_2$ of $C_2$). If $f$ is a homomorphism from $H_1$ to $H_2$, and $g$ is a homomorphism from $H_2$ to $H_3$, then the composition $f \circ g$ of these functions is a homomorphism from $H_1$ to $H_3$, and therefore the relation $\leq$ is transitive. Since every graph $H$ homomorphically maps to $H$, the order $\leq$ is also reflexive. Finally, $\leq$ is antisymmetric since its elements are equivalence classes of directed graphs with respect to homomorphic equivalence. Define $C_1 < C_2$ if $C_1 \leq C_2$ and $C_1 \neq C_2$. We call $(D, \leq)$ the homomorphism order of finite digraphs.

The equivalence classes of finite digraphs with respect to homomorphic equivalence will be denoted by $D$. Let $\leq$ be a binary relation defined on $D$ as follows: we set $C_1 \leq C_2$ if there exists a graph $H_1 \in C_1$ and a digraph $H_2 \in C_2$ such that $H_1 \rightarrow H_2$ (note that this definition does not depend on the choice of the representatives $H_1$ of $C_1$ and $H_2$ of $C_2$). If $f$ is a homomorphism from $H_1$ to $H_2$, and $g$ is a homomorphism from $H_2$ to $H_3$, then the composition $f \circ g$ of these functions is a homomorphism from $H_1$ to $H_3$, and therefore the relation $\leq$ is transitive. Since every graph $H$ homomorphically maps to $H$, the order $\leq$ is also reflexive. Finally, $\leq$ is antisymmetric since its elements are equivalence classes of directed graphs with respect to homomorphic equivalence. Define $C_1 < C_2$ if $C_1 \leq C_2$ and $C_1 \neq C_2$. We call $(D, \leq)$ the homomorphism order of finite digraphs.

The equivalence classes of finite digraphs with respect to homomorphic equivalence will be denoted by $D$. Let $\leq$ be a binary relation defined on $D$ as follows: we set $C_1 \leq C_2$ if there exists a graph $H_1 \in C_1$ and a digraph $H_2 \in C_2$ such that $H_1 \rightarrow H_2$ (note that this definition does not depend on the choice of the representatives $H_1$ of $C_1$ and $H_2$ of $C_2$). If $f$ is a homomorphism from $H_1$ to $H_2$, and $g$ is a homomorphism from $H_2$ to $H_3$, then the composition $f \circ g$ of these functions is a homomorphism from $H_1$ to $H_3$, and therefore the relation $\leq$ is transitive. Since every graph $H$ homomorphically maps to $H$, the order $\leq$ is also reflexive. Finally, $\leq$ is antisymmetric since its elements are equivalence classes of directed graphs with respect to homomorphic equivalence. Define $C_1 < C_2$ if $C_1 \leq C_2$ and $C_1 \neq C_2$. We call $(D, \leq)$ the homomorphism order of finite digraphs.

The homomorphism order on digraphs turns out to be a lattice where every two elements have a supremum (also called join) and an infimum (also called meet). In the proof of this result, we need the notion of direct products of graphs. This notion of graph product\footnote{Warning: there are several other notions of graph products that have been studied; see e.g. \cite{28}.} can be seen as a special case of the notion of direct product as it is used in model theory \cite{31}. The class of all graphs with respect to homomorphisms forms an interesting category in the sense of category theory \cite{28} where the product introduced above is the product in the sense of category theory, which is why this product is sometimes also called the categorical graph product.

Let $H_1$ and $H_2$ be two graphs. Then the (direct-, cross-, categorical-) product $H_1 \times H_2$ of $H_1$ and $H_2$ is the graph with vertex set $V(H_1) \times V(H_2)$; the pair $((u_1, u_2), (v_1, v_2))$ is in $E(H_1 \times H_2)$ if $u_1 \in E(H_1)$ and $(v_2, v_1) \in E(H_2)$. Note that the product is symmetric and associative in the sense that $H_1 \times H_2$ is isomorphic to $H_2 \times H_1$ and $H_1 \times (H_2 \times H_3)$ is isomorphic to $(H_1 \times H_2) \times H_3$, and we therefore do not specify the order of multiplication when multiplying more than two graphs. The $n$-th power $H^n$ of a graph $H$ is inductively defined as follows. $H^1$ is by definition $H$. If $H^i$ is already defined, then $H^{i+1}$ is $H^i \times H$. 1
Proposition 1.1. The homomorphism order \((\mathcal{D}; \leq)\) is a lattice; i.e., for all \(C_1, C_2 \in \mathcal{D}\)

- there exists an element \(C_1 \lor C_2 \in \mathcal{D}\), the join of \(C_1\) and \(C_2\), such that \(C_1 \leq (C_1 \lor C_2)\) and \(C_2 \leq (C_1 \lor C_2)\), and such that for every \(U \in \mathcal{D}\) with \(C_1 \leq U\) and \(C_2 \leq U\) we have \(C_1 \lor C_2 \leq U\).

- there exists an element \(C_1 \land C_2 \in \mathcal{D}\), the meet of \(C_1\) and \(C_2\), such that \((C_1 \land C_2) \leq C_1\) and \((C_1 \land C_2) \leq C_2\), and such that for every \(U \in \mathcal{D}\) with \(U \leq C_1\) and \(U \leq C_2\) we have \(U \leq C_1 \land C_2\).

Proof. Let \(H_1 \in C_1\) and \(H_2 \in C_2\). For the join, the equivalence class of the disjoint union \(H_1 \uplus H_2\) has the desired properties. For the meet, the equivalence class of \(H_1 \times H_2\) has the desired properties.

With the seemingly simple definitions of graph homomorphisms and direct products we can already formulate very difficult open combinatorial questions.

Conjecture 1 (Hedetniemi). Let \(G\) and \(H\) be finite graphs, and suppose that \(G \times H \to K_n\). Then \(G \to K_n\) or \(H \to K_n\).

This conjecture is easy for \(n = 1\) and \(n = 2\) (Exercise 4), and has been solved for \(n = 3\) by Norbert Sauer [19]. Already for \(n = 4\) the conjecture is open.

The smallest \(n \in \mathbb{N}\) such that \(G \to K_n\) is also called the chromatic number of \(G\), and denoted by \(\chi(G)\). Clearly, \(\chi(G \times H) \leq \min(\chi(G), \min(H))\). Hedetniemi’s conjecture can be rephrased as

\[
\chi(G \times H) = \min(\chi(G), \chi(H)).
\]

Clearly, \((\mathcal{D}, \leq)\) has infinite ascending chains, that is, sequences \(C_1, C_2, \ldots\) such that \(C_i < C_{i+1}\) for all \(i \in \mathbb{N}\). Take for instance \(C_i := \vec{P}_i\). More interestingly, \((\mathcal{D}, \leq)\) also has infinite descending chains.

Proposition 1.2. The lattice \((\mathcal{D}, \leq)\) contains infinite descending chains \(C_1 > C_2 > \cdots\).

Proof. For this we use the following graphs, called zig-zags, which are frequently used in the theory of graph homomorphisms. We may write an orientation of a path \(P\) as a sequence of 0’s and 1’s, where 0 represents a forward arc and 1 represents a backward arc. For two orientations of paths \(P\) and \(Q\) with the representation \(p_0, \ldots, p_n \in \{0, 1\}^*\) and \(Q = q_0, \ldots, q_m \in \{0, 1\}^*\), respectively, the concatenation \(P \circ Q\) of \(P\) and \(Q\) is the oriented path represented by \(p_0, \ldots, p_n, q_1, \ldots, q_m\). For \(k \geq 1\), the zig-zag of order \(k\), denoted by \(Z_k\), is the orientation of a path represented by \(11(01)^{k-1}1\). We recommend the reader to draw pictures of \(Z_k\) where forward arcs point up and backward arcs point down. Now, the equivalence classes of the graphs \(Z_1, Z_2, \ldots\) form an infinite descending chain.

Proposition 1.3. The lattice \((\mathcal{D}, \leq)\) contains infinite antichains, that is, sets of pairwise incomparable elements of \(\mathcal{D}\) with respect to \(\leq\).

Proof. Again, it suffices to work with orientations of paths. Consider the orientation of a path \(Z_{k,l} := 11(01)^{k-1}1^l\). Our infinite antichain now consists of the equivalence classes containing the graphs \(Z_{k,k}\) for \(k \geq 2\).
A strong homomorphism between two directed graphs $G$ and $H$ is a mapping from $V(G)$ to $V(H)$ such that $(f(u), f(v)) \in E(G)$ if and only if $(u, v) \in E(H)$ for all $u, v \in V(G)$. An isomorphism between two directed graphs $G$ and $H$ is a bijective strong homomorphism from $G$ to $H$, i.e., $f(u) \neq f(v)$ for any two distinct vertices $u, v \in V(G)$. Note that a homomorphism $h: G \to H$ is an isomorphism if and only if it is bijective, and $h^{-1}$ is a homomorphism from $H$ to $G$.

**Exercises.**

1. How many connected components do we have in $(P_3)^3$?
2. How many weakly and strongly connected components do we have in $(\vec{C}_3)^3$?
3. Let $G$ and $H$ be digraphs. Prove that $G \times H$ has a directed cycle if and only if both $G$ and $H$ have a directed cycle.
4. Prove the Hedetniemi conjecture for $n = 1$ and $n = 2$.
5. Show that the Hedetniemi conjecture is equivalent to each of the following two statements.
   - Let $n$ be a positive integer. If for two graphs $G$ and $H$ we have $G \not\to K_n$ and $H \not\to K_n$, then $G \times H \not\to K_n$.
   - Let $G$ and $H$ be graphs with $\chi(G) = \chi(H) = m$. Then there exists a graph $K$ with $\chi(K) = m$ such that $K \to G$ and $K \to H$.
6. Show that Hedetniemi’s conjecture is false for directed graphs. **Hint:** there are counterexamples $G, H$ with four vertices each.
7. Show that for every $k \in \mathbb{N}$, every pair of adjacent vertices of $(K_3)^k$ has exactly one common neighbour (that is, every edge lies in a unique subgraph of $(K_3)^k$ isomorphic to $K_3$).
8. Show that for every $k \in \mathbb{N}$, every pair of non-adjacent vertices in $(K_3)^k$ has at least two common neighbours.
9. Show that a digraph $G$ homomorphically maps to $\vec{P}_1$ if and only if $\vec{P}_2$ does not homomorphically map to $G$.
10. Construct an orientation of a tree that is not homomorphically equivalent to an orientation of a path.
11. Construct a balanced orientation of a cycle that is not homomorphically equivalent to an orientation of a path.
12. Show that a digraph $G$ homomorphically maps to $T_3$ if and only if $\vec{P}^3$ does not map to $G$.
13. Show that $G \to \vec{P}_n$, for some $n \geq 1$, if and only if any two paths in $G$ that start and end in the same vertex have the same net length.
14. Show that $G \to \vec{C}_n$, for some $n \geq 1$, if and only if any two paths in $G$ that start and end in the same vertex have the same net length modulo $n$. 

7
1.3 The $H$-colouring Problem and Variants

When does a given digraph $G$ homomorphically map to a digraph $H$? For every digraph $H$, this question defines a computational problem, called the $H$-colouring problem. The input of this problem consists of a finite digraph $G$, and the question is whether there exists a homomorphism from $G$ to $H$.

There are many variants of this problem. In the precoloured $H$-colouring problem, the input consists of a finite digraph $G$, together with a mapping $f$ from a subset of $V(G)$ to $V(H)$. The question is whether there exists an extension of $f$ to all of $V(G)$ which is a homomorphism from $G$ to $H$.

In the list $H$-colouring problem, the input consists of a finite digraph $G$, together with a set $S_x \subseteq V(H)$ for every vertex $x \in V(G)$. The question is whether there exists a homomorphism $h$ from $G$ to $H$ such that $h(x) \in S_x$ for all $x \in V(G)$.

It is clear that the $H$-colouring problem reduces to the precoloured $H$-colouring problem (it is a special case: the partial map might have an empty domain), and that the precoloured $H$-colouring problem reduces to the list $H$-colouring problem (for vertices $x$ in the domain of $f$, we set $S_x := \{f(x)\}$, and for vertices $x$ outside the domain of $f$, we set $S_x := V(H)$).

The constraint satisfaction problem is a common generalization of all those problems, and many more. It is defined not only for digraphs $H$, but more generally for relational structures $S$. Relational structures are the generalisation of graphs that can have many relations of arbitrary arity instead of just one binary edge relation. The constraint satisfaction problem will be introduced formally in Section 4.

Note that since graphs can be seen as a special case of digraphs, $H$-colouring is also defined for undirected graphs $H$. In this case we obtain essentially the same computational problem if we only allow undirected graphs in the input; this is made precise in Exercise 17.

For every finite graph $H$, the $H$-colouring problem is obviously in NP, because for every graph $G$ it can be verified in polynomial time whether a given mapping from $V(G)$ to $V(H)$ is a homomorphism from $G$ to $H$ or not. Clearly, the same holds for the precoloured and the list $H$-colouring problem.

We have also seen that the $K_n$-colouring problem is the classical $n$-colouring problem. Therefore, we already know graphs $H$ whose $H$-colouring problem is NP-complete. However, for many graphs and digraphs $H$ (see Exercise 18 and 19) $H$-colouring can be solved in polynomial time. The following research question is open.

**Question 1.** For which digraphs $H$ can the $H$-colouring problem be solved in polynomial time?

As we will see later, if we solve the classification question for the precoloured $H$-colouring problem, then we solve Question 1 and vice versa. Quite surprisingly, the same is true for the complexity of constraint satisfaction problems: a complete classification into NP-complete and P for the $H$-colouring problem would imply a classification for the class of all CSPs, and vice versa [22].

The list $H$-colouring problem, on the other hand, is quickly NP-hard, and therefore less difficult to classify. And indeed, a complete classification has been obtained by Bulatov [11]. Alternative proofs can be found in [3,13].

It has been conjectured by Feder and Vardi [22] that $H$-colouring is for any finite digraph $H$ either NP-complete or can be solved in polynomial time. This is the so-called dichotomy conjecture and it is open as well. It was shown by Ladner that unless P=NP there are infinitely
many complexity classes between P and NP; so the conjecture says that for $H$-colouring these intermediate complexities do not appear. It is known that the dichotomy conjecture is true for finite undirected graphs.

**Theorem 1.4** (of [26]). Let $H$ be a finite undirected graph. If $H$ homomorphically maps to $K_2$, or contains a loop, then $H$-colouring can be solved in polynomial time. Otherwise, $H$-colouring is NP-complete.

The case that $H$ homomorphically maps to $K_2$ will be the topic of Exercise 18. The proof of Theorem 1.4 can be found in Section 8.

**Exercises.**

15. Let $H$ be a finite directed graph. Find an algorithm that decides whether there is a strong homomorphism from a given graph $G$ to the fixed graph $H$. The running time of the algorithm should be polynomial in the size of $G$ (note that we consider $|V(H)|$ to be constant).

16. Let $H$ be a finite digraph such that CSP($H$) can be solved in polynomial time. Find a polynomial-time algorithm that constructs for a given finite digraph $G$ a homomorphism to $H$, if such a homomorphism exists.

17. Let $G$ and $H$ be directed graphs, and suppose that $H$ is symmetric. Show that $f : V(G) \rightarrow V(H)$ is a homomorphism from $G$ to $H$ if and only if $f$ is a homomorphism from the undirected graph of $G$ to the undirected graph of $H$.

18. Show that for any graph $H$ that homomorphically maps to $K_2$ the constraint satisfaction problem for $H$ can be solved in polynomial time.

19. Prove that CSP($T_3$) can be solved in polynomial time.

20. Prove that CSP($\vec{C}_3$) can be solved in polynomial time.

21. Let $N$ be the set $\{Z_1, Z_2, Z_3, \ldots\}$. Show that a digraph $G$ homomorphically maps to $\vec{P}_2$ if and only if no digraph in $N$ homomorphically maps to $G$.

22. Suppose that CSP($G$) and CSP($H$), for two digraphs $G$ and $H$, can be solved in polynomial time. Show that CSP($G \times H$) and CSP($G \uplus H$) can be solved in polynomial time as well.

1.4 **Cores**

An *endomorphism* of a graph $H$ is a homomorphism from $H$ to $H$. An *automorphism* of a graph $H$ is an isomorphism from $H$ to $H$. A finite graph $H$ is called a *core* if every endomorphism of $H$ is an automorphism. A subgraph $G$ of $H$ is called a *core of $H$* if $H$ is homomorphically equivalent to $G$ and $G$ is a core.

**Proposition 1.5.** Every finite graph $H$ has a core, which is unique up to isomorphism.
Proof. Any finite graph $H$ has a core, since we can select an endomorphism $e$ of $H$ such that the image of $e$ has smallest cardinality; the subgraph of $H$ induced by $e(V(H))$ is a core of $H$. Let $G_1$ and $G_2$ be cores of $H$, and $f_1 : H \to G_1$ and $f_2 : H \to G_2$ be homomorphisms. Let $e_1$ be the restriction of $f_1$ to $V(G_2)$. We claim that $e_1$ is the desired isomorphism. Suppose for contradiction that $e_1$ is not injective, i.e., there are distinct $x, y$ in $V(G_2)$ such that $e_1(x) = e_1(y)$. It follows that $f_2 \circ e_1$ cannot be injective, too. But $f_2 \circ e_1$ is an endomorphism of $G_2$, contradicting the assumption that $G_2$ is a core. Similarly, the restriction $e_2$ of $f_2$ to $V(G_1)$ is an injective homomorphism from $G_1$ to $G_2$, and it follows that $|V(G_1)| = |V(G_2)|$ and both $e_1$ and $e_2$ are bijective.

Now, since $|V(G_2)|$ is finite, $e_2 \circ e_1 \circ \cdots \circ e_2 \circ e_1 = (e_2 \circ e_1)^n = \text{id}$ for large enough $n$. Hence, $e_2 \circ e_1 \circ \cdots \circ e_2 = (e_1)^{-1}$, so the inverse of $e_1$ is a homomorphism, and hence an isomorphism between $G_1$ and $G_2$.

Since a core $G$ of a finite digraph $H$ is unique up to isomorphism, we call $G$ the core of $H$. Cores can be characterized in many different ways; for some of them, see Exercise 24.

There are examples of infinite digraphs that do not have a core in the sense defined above; see Exercise 27. Since a digraph $H$ and its core have the same CSP, it suffices to study CSP($H$) for core digraphs $H$ only. As we will see below, this has several advantages.

**Proposition 1.6.** Let $H$ be a core. Then CSP($H$) and the precoloured CSP for $H$ are linear-time equivalent.

Proof. The reduction from CSP($H$) to precoloured CSP($H$) is trivial, because an instance $G$ of CSP($H$) is equivalent to the instance $(G, c)$ of precoloured CSP($H$) where $c$ is everywhere undefined.

We show the converse reduction by induction on the size of the image of the partial mapping $c$ in instances of precoloured CSP($H$). Let $(G, c)$ be an instance of precoloured CSP($H$) where $c$ has an image of size $k \geq 1$. We show how to reduce the problem to one where the partial mapping has an image of size $k-1$. If we compose all these reductions (note that the size of the image is bounded by $|V(H)|$), we finally obtain a reduction to CSP($H$).

Let $x \in V(G)$ and $u \in V(H)$ be such that $c(x) = u$. We first identify all vertices $y$ of $G$ such that $c(y) = u$ with $x$. Then we create a copy of $H$, and attach the copy to $G$ by identifying $x \in V(G)$ with $u \in V(H)$. Let $G'$ be the resulting graph, and let $c'$ be the partial map obtained from $c$ by restricting it such that it is undefined on $x$, and then extending it so that $c(v) = v$ for all $v \in V(H)$, $v \neq u$, that appear in the image of $c$. Note that the size of $G'$ and the size of $G$ only differ by a constant.

We claim that $(G', c')$ has a solution if and only if $(G, c)$ has a solution. If $f$ is a homomorphism from $G$ to $H$ that extends $c$, we further extend $f$ to the copy of $H$ that is attached in $G'$ by setting $f(v')$ to $v$ if vertex $v'$ is a copy of a vertex $v \in V(H)$. This extension of $f$ clearly is a homomorphism from $G'$ to $H$ and extends $c'$.

Now, suppose that $f'$ is a homomorphism from $G'$ to $H$ that extends $c'$. The restriction of $f'$ to the vertices from the copy of $H$ that is attached to $x$ in $G'$ is an endomorphism of $H$, and because $H$ is a core, is an automorphism $\alpha$ of $H$. Moreover, $\alpha$ fixes $v$ for all $v \in V(H)$ in the image of $\alpha$. Let $\beta$ be the inverse of $\alpha$, i.e., let $\beta$ be the automorphism of $H$ such that $\beta(\alpha(v)) = v$ for all $v \in V(H)$. Let $f$ be the mapping from $V(G)$ to $V(H)$ that maps vertices that were identified with $x$ to $\beta(f'(x))$, and all other vertices $y \in V(G)$ to $\beta(f'(y))$. Clearly, $f$ is a homomorphism from $G$ to $H$. Moreover, $f$ maps vertices $y \in V(G)$, $y \neq x$, where $c$ is defined to $c(y)$, since the same is true for $f'$ and for $\alpha$. Moreover, because $x$ in $G'$ is identified
to \( u \) in the copy of \( H \), we have that \( f(x) = \beta(f'(x)) = \beta(f'(u)) = u \), and therefore \( f \) is an extension of \( c \).

We have already seen in Exercise 16 that the computational problem to construct a homomorphism from \( G \) to \( H \), for fixed \( H \) and given \( G \), can be reduced in polynomial-time to the problem of deciding whether there exists a homomorphism from \( G \) to \( H \). The intended solution of Exercise 16 requires in the worst-case \(|V(G)|^2\) many executions of the decision procedure for CSP(\( H \)). Using the concept of cores and the precoloured CSP (and its equivalence to the CSP) we can give a faster method to construct homomorphisms.

**Proposition 1.7.** If there is an algorithm that decides CSP(\( H \)) in time \( T \), then there is an algorithm that constructs a homomorphism from a given graph \( G \) to \( H \) (if such a homomorphism exists) which runs in time \( O(|V(G)|T) \).

**Proof.** We can assume without loss of generality that \( H \) is a core (since \( H \) and its core have the same CSP). By Proposition 1.6, there is an algorithm \( B \) for precoloured CSP(\( H \)) with a running time in \( O(T) \). For given \( G \), we first apply \( B \) to \((G,c)\) for the everywhere undefined function \( c \) to decide whether there exists a homomorphism from \( G \) to \( H \). If no, there is nothing to show. If yes, we select some \( x \in V(G) \), and extend \( c \) by defining \( c(x) = u \) for some \( u \in V(H) \). Then we use algorithm \( B \) to decide whether there is a homomorphism from \( G \) to \( H \) that extends \( c \). If no, we try another vertex \( u \in V(H) \). Clearly, for some \( u \) the algorithm must give the answer “yes”. We proceed with the extension \( c \) where \( c(x) = u \), and repeat the procedure with another vertex \( x \) from \( V(G) \). At the end, \( c \) is defined for all vertices \( x \) of \( G \), and \( c \) is a homomorphism from \( G \) to \( H \). Clearly, since \( H \) is fixed, algorithm \( B \) is executed at most \( O(|V(G)|) \) many times.

We want to mention without proof is that it is NP-complete to decide whether a given digraph \( H \) is not a core.

**Exercises.**

23. Show that \( Z_{k,l} \) is a core for all \( k, l \geq 2 \).

24. Prove that for every finite directed graph \( G \) the following is equivalent:
   - \( G \) is a core.
   - Every endomorphism of \( G \) is injective.
   - Every endomorphism of \( G \) is surjective.

25. Show that the three properties in the previous exercise are no longer equivalent if \( G \) is infinite.

26. Prove that the core of a strongly connected digraph is strongly connected.

27. Show that the infinite tournament \((\mathbb{Q}; <)\) has endomorphisms that are not automorphisms. Show that every digraph that is homomorphically equivalent to \((\mathbb{Q}; <)\) also has endomorphisms that are not automorphisms.

28. Let \( H \) be a core of \( G \). Show that there exists a retraction from \( G \) to \( H \), i.e., a homomorphism \( e \) from \( G \) to \( H \) such that \( e(x) = x \) for all \( x \in V(H) \).
29. The set of automorphisms of a digraph $G$ forms a group; this group is called \textit{transitive} if for all $a, b \in V(G)$ there is an automorphism $f$ of $G$ such that $f(a) = b$. Show that if $G$ has a transitive automorphism group, then the core of $G$ also has a transitive automorphism group.

30. Show that the connected components of a core are cores that form an antichain in $(D; \leq)$; conversely, the disjoint union of an antichain of cores is a core.

31. Prove that the core of a graph with a transitive automorphism group is connected.

32. Determine the computational complexity of CSP($H$) for $H := (\mathbb{Z}, \{(x, y) : |x - y| \in \{1, 2\}\})$.

1.5 Polymorphisms

Polymorphisms are a powerful tool for analyzing the computational complexity of constraint satisfaction problems; as we will see, they are useful both for NP-hardness proofs and for proving the correctness of polynomial-time algorithms for CSPs.

Polymorphisms can be seen as multi-dimensional variants of endomorphisms.

Definition 1.8. A homomorphism from $H^k$ to $H$, for $k \geq 1$, is called a \textit{(k-ary) polymorphism} of $H$.

In other words, a mapping $f: V(H)^k \to V(H)$ is a polymorphism of $H$ iff $(f(u_1, \ldots, u_k), f(v_1, \ldots, v_k)) \in E(H)$ whenever $(u_1, v_1), \ldots, (u_k, v_k)$ are arcs in $E(H)$. Note that any graph $H$ has all \textit{projections} as polymorphisms, i.e., all mappings $p: V(H)^k \to V(H)$ that satisfy for some $i$ the equation $p(x_1, \ldots, x_k) = x_i$ for all $x_1, \ldots, x_k \in V(H)$.

Example 1. The function $(x, y) \mapsto \min(x, y)$ is a polymorphism of $\vec{T}_n = (\{0, \ldots, n-1\}; <)$.

An operation $f: V(H)^k \to V(H)$ is called

- \textit{idempotent} if $f(x, \ldots, x) = x$ for all $x \in V(H)$.
- \textit{conservative} if $f(x_1, \ldots, x_n) \in \{x_1, \ldots, x_n\}$ for all $x_1, \ldots, x_k \in V(H)$.

Definition 1.9. A digraph $H$ is called \textit{projective} if every idempotent polymorphism is a projection.

The following will be shown in Section 7.

Proposition 1.10. For all $n \geq 3$, the graph $K_n$ is projective.

2 The Arc-consistency Procedure

The \textit{arc-consistency procedure} is one of the most fundamental and well-studied algorithms that are applied for CSPs. This procedure was first discovered for constraint satisfaction problems in artificial intelligence [40,41]; in the graph homomorphism literature, the algorithm is sometimes called the \textit{consistency check algorithm}.

Let $H$ be a finite digraph, and let $G$ be an instance of CSP($H$). The idea of the procedure is to maintain for each vertex in $G$ a list of vertices of $H$, and each element in the list of $x$
AC_H(G) Input: a finite digraph G.
Data structure: a list L(x) ⊆ V(H) for each vertex x ∈ V(G).

Set L(x) := V(H) for all x ∈ V(G).
Do
For each (x, y) ∈ E(G):
    Remove u from L(x) if there is no v ∈ L(y) with (u, v) ∈ E(H).
    Remove v from L(y) if there is no u ∈ L(x) with (u, v) ∈ E(H).
    If L(x) is empty for some vertex x ∈ V(G) then reject
Loop until no list changes

Figure 1: The arc-consistency procedure for CSP(H).

represents a candidate for an image of x under a homomorphism from G to H. The algorithm successively removes vertices from these lists; it only removes a vertex u ∈ V(H) from the list for x ∈ V(G), if there is no homomorphism from G to H that maps x to u. To detect vertices x, u such that u can be removed from the list for x, the algorithm uses two rules (in fact, one rule and a symmetric version of the same rule): if (x, y) is an edge in G, then

- remove u from L(x) if there is no v ∈ L(y) with (u, v) ∈ E(H);
- remove v from L(y) if there is no u ∈ L(x) with (u, v) ∈ E(H).

If eventually we can not remove any vertex from any list with these rules any more, the graph G together with the lists for each vertex is called arc-consistent. Clearly, if the algorithm removes all vertices from one of the lists, then there is no homomorphism from G to H. The pseudo-code of the entire arc-consistency procedure is displayed in Figure 1.

Note that for any finite digraph H, if AC_H rejects an instance of CSP(H), then it clearly has no solution. The converse implication does not hold in general. For instance, let H be K_2, and let G be K_3. In this case, AC_H does not remove any vertex from any list, but obviously there is no homomorphism from K_3 to K_2.

However, there are digraphs H where the AC_H is a complete decision procedure for CSP(H) in the sense that it rejects an instance G of CSP(H) if and only if G does not homomorphically map to H. In this case we say that AC solves CSP(H).

Implementation. The running time of AC_H is for any fixed digraph H polynomial in the size of G. In a naive implementation of the procedure, the inner loop of the algorithm would go over all edges of the graph, in which case the running time of the algorithm is quadratic in the size of G. In the following we describe an implementation of the arc-consistency procedure, called AC-3, which is due to Mackworth [40], and has a worst-case running time that is linear in the size of G. Several other implementations of the arc-consistency procedure have been proposed in the Artificial Intelligence literature, aiming at reducing the costs of the algorithm in terms of the number of vertices of both G and H. But here we consider the size of H to be fixed, and therefore we do not follow this line of research. With AC-3, we rather present one of the simplest implementations of the arc-consistency procedure with a linear running time.

The idea of AC-3 is to maintain a worklist, which contains a list of arcs (x_0, x_1) of G that might help to remove a value from L(x_0) or L(x_1). Whenever we remove a value from a list
Input: a finite digraph $G$.
Data structure: a list $L(x)$ of vertices of $H$ for each $x \in V(G)$.
the worklist $W$: a list of arcs of $G$.

Subroutine Revise($(x_0, x_1), i$)
Input: an arc $(x_0, x_1) \in E(G)$, an index $i \in \{0, 1\}$.
change = false
for each $u_i$ in $L(x_i)$
    if there is no $u_{1-i} \in L(x_{1-i})$ such that $(u_0, u_1) \in E(H)$ then
        remove $u_i$ from $L(x_i)$
        change = true
    end if
end for
If change = true then
    if $L(x_i) = \emptyset$ then reject
    else
        for all arcs $(z_0, z_1) \in E(G)$ with $z_0 = x_i$ or $z_1 = x_i$ add $(z_0, z_1)$ to $W$
    end if
end if
$W := E(G)$
Do
    remove an arc $(x_0, x_1)$ from $W$
    Revise($(x_0, x_1), 0$)
    Revise($(x_0, x_1), 1$)
while $W \neq \emptyset$

Figure 2: The AC-3 implementation of the arc-consistency procedure for CSP($H$).

$L(x)$, we add all arcs that are in $G$ incident to $x$. Note that then any arc in $G$ might be added at most $2|V(H)|$ many times to the worklist, which is a constant in the size of $G$. Hence, the while loop of the implementation is iterated for at most a linear number of times. Altogether, the running time is linear in the size of $G$ as well.

**Arc-consistency for pruning search.** Suppose that $H$ is such that $AC_H$ does not solve CSP($H$). Even in this situation the arc-consistency procedure might be useful for *pruning the search space* in exhaustive approaches to solve CSP($H$). In such an approach we might use the arc-consistency procedure as a subroutine as follows. Initially, we run $AC_H$ on the input instance $G$. If it computes an empty list, we reject. Otherwise, we select some vertex $x \in V(G)$, and set $L(x)$ to $\{ u \}$ for some $u \in L(x)$. Then we proceed recursively with the resulting lists. If $AC_H$ now detects an empty list, we backtrack, but remove $u$ from $L(x)$. Finally, if the algorithm does not detect an empty list at the first level of the recursion, we end up with singleton lists for each vertex $x \in V(G)$, which defines a homomorphism from $G$ to $H$. 

14
2.1 The Power Graph

For which $H$ does the Arc-Consistency procedure solve $\text{CSP}(H)$? In this section we present an elegant and effective characterization of those finite graphs $H$ where $\text{AC}$ solves $\text{CSP}(H)$, found by Feder and Vardi [22].

Definition 2.1. For a digraph $H$, the power graph $P(H)$ is the digraph whose vertices are non-empty subsets of $V(H)$ and where two subsets $U$ and $V$ are joined by an arc if the following holds:

- for every vertex $u \in U$, there exists a vertex $v \in V$ such that $(u, v) \in E(H)$, and
- for every vertex $v \in V$, there exists a vertex $u \in U$ such that $(u, v) \in E(H)$.

The definition of the power graph resembles the arc-consistency algorithm, and indeed, we have the following lemma which describes the correspondence.

Lemma 2.2. $\text{AC}_H$ rejects $G$ if and only if $G \not\rightarrow P(H)$.

Proof. Suppose first that $\text{AC}_H$ does not reject $G$. For $u \in V(G)$, let $L(u)$ be the list derived at the final stage of the algorithm. Then by definition of $E(P(H))$, the map $x \mapsto L(x)$ is a homomorphism from $G$ to $P(H)$.

Conversely, suppose that $f: G \rightarrow P(H)$ is a homomorphism. We prove by induction over the execution of $\text{AC}_H$ that for all $x \in V(G)$ the elements of $f(x)$ are never removed from $L(x)$. To see that, let $(a, b) \in E(G)$ be arbitrary. Then $((f(a), f(b)) \in E(P(H))$, and hence for every $u \in f(a)$ there exists a $v \in f(b)$ such that $(u, v) \in E(H)$. By inductive assumption, $v \in L(b)$, and hence $u$ will not be removed from $L(a)$. This concludes the inductive step. □

Theorem 2.3. Let $H$ be a finite digraph. Then $\text{AC}$ solves $\text{CSP}(H)$ if and only if $P(H)$ homomorphically maps to $H$.

Proof. Suppose first that $\text{AC}$ solves $\text{CSP}(H)$. Apply $\text{AC}_H$ to $P(H)$. Since $P(H) \rightarrow P(H)$, the previous lemma shows that $\text{AC}_H$ does not reject $P(H)$. Hence, $P(H) \rightarrow H$ by assumption.

Conversely, suppose that $P(H) \rightarrow H$. If $\text{AC}_H$ rejects a graph $G$ then $G \not\rightarrow H$. If $\text{AC}_H$ does accept $G$, then the lemma asserts that $G \rightarrow P(H)$. Composing homomorphisms, we obtain that $G \rightarrow H$. □

Observation 2.4. Let $H$ be a core digraph. Note that if $P(H)$ homomorphically maps to $H$, then there also exists a homomorphism that maps $\{x\}$ to $x$ for all $x \in V(H)$. We claim that in this case the precoloured CSP for $H$ can be solved by the modification of $\text{AC}_H$ which starts with $L(x) := \{c(x)\}$ for all $x \in V(G)$ in the range of the precolouring function $c$, instead of $L(x) := V(H)$. This is a direct consequence of the proof of Theorem 2.3. If the modified version of $\text{AC}_H$ solves the precoloured CSP for $H$, then the classical version of $\text{AC}$ solves $\text{CSP}(H)$. Hence, it follows that the following are equivalent:

- $\text{AC}$ solves $\text{CSP}(H)$;
- the above modification of $\text{AC}_H$ solves the precoloured CSP for $H$;
- $P(H) \rightarrow H$.  

15
Note that the condition given in Theorem 2.3 can be used to decide algorithmically whether AC solves CSP($H$), because it suffices to test whether $P(H)$ homomorphically maps to $H$. Such problems about deciding properties of CSP($H$) for given $H$ are often called algorithmic Meta-problems. A naive algorithm for the above test would be to first construct $P(H)$, and then to search non-deterministically for a homomorphism from $P(H)$ to $H$, which puts the Meta-problem for solvability of CSP($H$) by $AC_H$ into the complexity class NExpTime (Non-deterministic Exponential Time). This can be improved.

Proposition 2.5. There exists a deterministic exponential time algorithm that tests for a given finite core digraph $H$ whether $P(H)$ homomorphically maps to $H$.

Proof. We first explicitly construct $P(H)$, and then apply $AC_H$ to $P(H)$. If $AC_H$ rejects, then there is certainly no homomorphism from $P(H) \to H$ by the properties of $AC_H$, and we return ‘false’. If $AC_H$ accepts, then we cannot argue right away that $P(H)$ homomorphically maps to $H$, since we do not know yet whether $AC_H$ is correct for CSP($H$).

But here is the trick. What we do in this case is to pick an arbitrary $x \in V(P(H))$, and remove all but one value $u$ from $L(x)$, and continue with the execution of $AC_H$. If $AC_H$ then detects the empty list, we try the same with another value $u'$ from $L(x)$. If we obtain failure for all values of $L(x)$, then clearly there is no homomorphism from $P(H)$ to $H$, and we return ‘false’.

Otherwise, if $AC_H$ still accepts when $L(x) = \{u\}$, then we continue with another element $y$ of $V(P(H))$, setting $L(y)$ to $\{v\}$ for some $v \in L(y)$. If $AC_H$ accepts, we continue like this, until at the end we have constructed a homomorphism from $P(H)$ to $H$. In this case we return ‘true’.

If $AC_H$ rejects for some $x \in V(P(H))$ when $L_x = \{u\}$ for all possible $u \in V(H)$, then the adaptation of $AC_H$ for the precoloured CSP would have given an incorrect answer for the previously selected variable (it said yes while it should have said no). By Observation 2.4, this means that $P(H)$ does not homomorphically map to $H$. Again, we return ‘false’.

The answer to the following question is not yet known.

Question 2. What is the computational complexity to decide for a given digraph $H$ whether $P(H) \to H$? What is the computational complexity when we further assume that $H$ is a core? Is this problem in P?

2.2 Tree Duality

Another mathematical notion that is closely related to the arc-consistency procedure is tree duality. The idea of this concept is that when a digraph $H$ has tree duality, then we can show that there is no homomorphism from a digraph $G$ to $H$ by exhibiting a tree obstruction in $G$. This is formalized in the following definition.

Definition 2.6. A digraph $H$ has tree duality iff there exists a (not necessarily finite) set $N$ of orientations of finite trees such that for all digraphs $G$ there is a homomorphism from $G$ to $H$ if and only if no digraph in $N$ homomorphically maps to $G$.

We refer to the set $N$ in Definition 2.6 as an obstruction set for CSP($H$). Note that no $T \in N$ homomorphically maps to $H$. The pair $(N, H)$ is called a duality pair. We have already encountered such an obstruction set in Exercise 19, where $H = T_2$, and $N = \{P_2\}$. 

16
In other words, \((\{\vec{P}_2\}, T_2)\) is a duality pair. Other duality pairs are \((\{\vec{P}_3\}, T_3)\) (Exercise 12), and \((\{Z_1, Z_2, \ldots, \vec{P}_2\})\) (Exercise 21).

Theorem 2.7 is a surprising link between the completeness of the arc-consistency procedure, tree duality, and the power graph, and was discovered by Feder and Vardi in the more general context of constraint satisfaction problems.

**Theorem 2.7.** Let \(H\) be a finite digraph. Then the following are equivalent.

1. \(H\) has tree duality;
2. \(P(H)\) homomorphically maps to \(H\);
3. The AC solves CSP\((H)\).
4. If every orientation of a tree that homomorphically maps to \(G\) also homomorphically maps to \(H\), then \(G\) homomorphically maps to \(H\).

**Proof.** The equivalence 2 \(\iff\) 3 has been shown in the previous section. We show 3 \(\implies\) 1, 1 \(\implies\) 4, and 4 \(\implies\) 2.

3 \(\implies\) 1: Suppose that AC solves CSP\((H)\). We have to show that \(H\) has tree duality. Let \(N\) be the set of all orientations of trees that does not homomorphically map to \(H\). We claim that if a digraph \(G\) does not homomorphically map to \(H\), then there is \(T \in N\) that homomorphically maps to \(G\).

By assumption, the arc-consistency procedure applied to \(G\) eventually derives the empty list for some vertex of \(G\). We use the computation of the procedure to construct an orientation \(T\) of a tree, following the exposition in [37]. When deleting a vertex \(u \in V(H)\) from the list of a vertex \(x \in V(G)\), we define an orientation of a rooted tree \(T_{x,u}\) with root \(r_{x,u}\) such that

1. There is a homomorphism from \(T_{x,u}\) to \(G\) mapping \(r_{x,u}\) to \(x\).
2. There is no homomorphism from \(T_{x,u}\) to \(H\) mapping \(r_{x,u}\) to \(u\).

The vertex \(u\) is deleted from the list of \(x\) because we found an arc \((x_0, x_1) \in E(G)\) with \(x_i = x\) for some \(i \in \{0, 1\}\) such that there is no arc \((u_0, u_1) \in E(H)\) with \(u_i = u\) and \(u_{1-i}\) in the list of \(x_1-i\). We describe how to construct the tree \(T\) for the case that \(i = 0\), i.e., for the case that there is an arc \((x, y) \in E(G)\) such that there is no arc \((u, v) \in E(H)\) where \(v \in L(y)\); the construction for \(i = 1\) is analogous.

Let \(p, q\) be vertices and \((p, q)\) an edge of \(T_{x,u}\), and select the root \(r_{x,u} = p\). If \(E(H)\) does not contain an arc \((u, v)\), then we are done, since \(T_{x,u}\) clearly satisfies property (1) and (2). Otherwise, for every arc \((u, v) \in E(H)\) the vertex \(v\) has already been removed from the list \(L(y)\), and hence by induction \(T_{y,v}\) having properties (1) and (2) is already defined. We then add a copy of \(T_{y,v}\) to \(T_{x,u}\) and identify the vertex \(r_{y,v}\) with \(q\).

We verify that the resulting orientation of a tree \(T_{x,u}\) satisfies (1) and (2). Let \(f\) be the homomorphism from \(T_{y,v}\) mapping \(r_{y,v}\) to \(v\), which exists due to (1). The extension of \(f\) to \(V(T_{x,u})\) that maps \(p \times x\) to a homomorphism from \(T_{x,u}\) to \(G\), and this shows that (1) holds for \(T_{x,u}\). But any homomorphism from \(T_{x,u}\) to \(H\) that maps \(r_{x,u}\) to \(u\) would also map the root of \(T_{y,v}\) to \(v\), which is impossible, and this shows that (2) holds for \(T_{x,u}\). When the list \(L(x)\) of some vertex \(x \in V(G)\) becomes empty, we can construct an orientation of a tree \(T\) by identifying the roots of all \(T_{x,u}\) to a vertex \(r\). We then find a homomorphism from \(T\) to \(G\) by mapping \(r\) to \(x\) and extending the homomorphism independently on each \(T_{x,u}\). But any
homomorphism from \( T \) to \( H \) must map \( r \) to some element \( u \in V(H) \), and hence there is a homomorphism from \( T_{x, u} \) to \( H \) that maps \( x \) to \( u \), a contradiction.

1 \( \Rightarrow \) 4: If \( H \) has an obstruction set \( N \) consisting of orientations of trees, and if \( G \) does not homomorphically map to \( H \), there exists an orientation of a tree \( T \in N \) that maps to \( G \) but not to \( H \).

4 \( \Rightarrow \) 2: To show that \( P(H) \) homomorphically maps to \( H \), it suffices to prove that every orientation \( T \) of a tree that homomorphically maps to \( P(H) \) also homomorphically maps to \( H \). Let \( f \) be a homomorphism from \( T \) to \( P(H) \), and let \( x \) be any vertex of \( T \). We construct a sequence \( f_0, \ldots, f_n \), for \( n = |V(T)| \), where \( f_i \) is a homomorphism from the subgraph of \( T \) induced by the vertices at distance at most \( i \) to \( x \) in \( T \), and \( f_{i+1} \) is an extension of \( f_i \) for all \( 1 \leq i \leq n \). The mapping \( f_0 \) maps \( x \) to some vertex from \( f(x) \). Suppose inductively that we have already defined \( f_i \). Let \( y \) be a vertex at distance \( i+1 \) from \( x \) in \( T \). Since \( T \) is an orientation of a tree, there is a unique \( y' \in V(T) \) of distance \( i \) from \( x \) in \( T \) such that \((y, y') \in E(T) \) or \((y', y) \in E(T) \). Note that \( u = f_i(y') \) is already defined. In case that \((y', y) \in E(T) \), there must be a vertex \( v \) in \( f(y) \) such that \((u, v) \in E(H) \), since \((f(y'), f(y)) \) must be a path in \( P(H) \), and by definition of \( P(H) \). We then set \( f_{i+1}(y) = v \). In case that \((y, y') \in E(T) \) we can proceed analogously. By construction, the mapping \( f_n \) is a homomorphism from \( T \) to \( H \).

\[ \square \]

2.3 Totally Symmetric Polymorphisms

There is also a characterization of the power of arc consistency which is based on polymorphisms, due to [18].

**Definition 2.8.** A function \( f : D^k \to D \) is called totally symmetric if \( f(x_1, \ldots, x_m) = f(y_1, \ldots, y_m) \) whenever \( \{x_1, \ldots, x_m\} = \{y_1, \ldots, y_m\} \).

**Theorem 2.9.** Let \( H \) be a finite digraph. Then the following are equivalent.

- \( P(H) \) homomorphically maps to \( H \);
- \( H \) has totally symmetric polymorphisms of all arities;
- \( H \) has a totally symmetric polymorphism of arity \( 2|V(H)| \).

**Proof.** Suppose first that \( g \) is a homomorphism from \( P(H) \) to \( H \), and let \( k \) be arbitrary. Let \( f \) be defined by \( f(x_1, \ldots, x_k) = g(\{x_1, \ldots, x_k\}) \). If \((x_1, y_1), \ldots, (x_k, y_k) \in E(H) \), then \( \{x_1, \ldots, x_k\} \) is adjacent to \( \{y_1, \ldots, y_k\} \) in \( P(H) \), and hence \((f(x_1, \ldots, x_k), f(y_1, \ldots, y_k)) \in E(H) \). Therefore, \( f \) is a polymorphism of \( H \), and it is clearly totally symmetric.

Conversely, suppose that \( f \) is a totally symmetric polymorphism of arity \( 2|V(H)| \). Let \( g : V(P(H)) \to V(H) \) be defined by

\[ g(\{x_1, \ldots, x_n\}) := f(x_1, \ldots, x_{n-1}, x_n, x_{n+1}, \ldots, x_n) \]

which is well-defined because \( f \) is totally symmetric. Let \((U, W) \in E(P(H)) \), and let \( x_1, \ldots, x_p \) be an enumeration of the elements of \( U \), and \( y_1, \ldots, y_q \) an enumeration of the elements of \( W \). The properties of \( P(H) \) imply that there are \( y_1', \ldots, y_p' \in U \) and \( x_1', \ldots, x_q' \in W \) such that \((x_1, y_1'), \ldots, (x_p, y_p') \in E(H) \) and \((x_1', y_1), \ldots, (x_q', y_q) \in E(H) \). Since \( f \) preserves \( E \),

\[ g(U) = g(\{x_1, \ldots, x_p\}) = f(x_1, \ldots, x_p, x_1', \ldots, x_q', x_1, \ldots, x_1) \]
is adjacent to
\[ g(W) = g(\{y_1, \ldots, y_q\}) = f(y_1', \ldots, y_{p'}, y_1, \ldots, y_q, y_1', \ldots, y_1'). \]

2.4 Semilattice Polymorphisms

Some digraphs have a single binary polymorphism that generates operations satisfying the
conditions in the previous theorem, as in the following statement. A binary operation
\( f : D^2 \to D \) is called commutative if it satisfies
\[ f(x, y) = f(y, x) \]
for all \( x, y \in D \).

It is called associative if it satisfies
\[ f(x, f(y, z)) = f(f(x, y), z) \]
for all \( x, y, z \in D \).

Definition 2.10. A binary operation is called a semilattice operation \( f \) if it is associative,
commutative, and idempotent.

Examples of semilattice operations are functions from \( D^2 \to D \) defined as \( (x, y) \mapsto \min(x, y) \); here the minimum is taken with respect to any fixed linear order of \( D \).

Theorem 2.11. Let \( H \) be a finite digraph. Then \( P(H) \to H \) if and only if \( H \) is homomorphically equivalent to a graph with a semilattice polymorphism.

Proof. Suppose first that \( P(H) \to H \). Thus, \( H \) and \( P(H) \) are homomorphically equivalent, and it suffices to show that \( P(H) \) has a semilattice polymorphism. The mapping \( (X, Y) \mapsto X \cup Y \) is clearly a semilattice operation; we claim that it preserves the edges of \( P(H) \). Let \((U, V) \) and \((A, B) \) be edges in \( P(H) \). Then for every \( u \in U \) there is a \( v \in V \) such that \((u, v) \in E(H) \), and for every \( u \in A \) there is a \( v \in B \) such that \((u, v) \in E(H) \). Hence, for every \( u \in U \cup A \) there is a \( v \in V \cup B \) such that \((u, v) \in E(H) \). Similarly, we can verify that for every \( v \in V \cup B \) there is a \( u \in U \cup A \) such that \((u, v) \in E(H) \). This proves the claim.

For the converse, suppose that \( H \) is homomorphically equivalent to a directed graph \( G \) with a semilattice polymorphism \( f \). Let \( h \) be the homomorphism from \( H \) to \( G \). The operation \( (x_1, \ldots, x_n) \mapsto f(x_1, f(x_2, f(\ldots, f(x_{n-1}, x_n) \ldots))) \) is a totally symmetric polymorphism of \( G \). Then Theorem 2.9 implies that \( P(G) \to G \). The map \( S \mapsto \{h(u) \mid u \in H\} \) is a homomorphism from \( P(H) \) to \( P(G) \). Therefore, \( P(H) \to P(G) \to G \to H \), as desired.

By verifying the existence of semilattice polymorphisms for a concrete class of digraphs,
we obtain the following consequence.

Corollary 2.12. \( \text{AC solves CSP}(H) \) if \( H \) is an orientation of a path.

Proof. Suppose that \( 1, \ldots, n \) are the vertices of \( H \) such that either \((i, i+1)\) or \((i+1, i)\) is an arc in \( E(H) \) for all \( i < n \). It is straightforward to verify that the mapping \( (x, y) \mapsto \min(x, y) \) is a polymorphism of \( H \). The statement now follows from Theorem 2.11.

We want to remark that there are orientations of trees \( H \) with an NP-complete \( H \)-colouring problem (the smallest known graph has 30 vertices, found by Jana Fischer [23]; see Figure 3).
So, unless \( P=NP \), this shows that there are orientations of trees \( H \) that do not have treeduality.
Exercises.

33. Recall that a digraph is called *balanced* if it homomorphically maps to a directed path. Let $H$ be a digraph.

- Prove: if $H$ is balanced, then $P(H)$ is balanced;
- Disprove: if $H$ is an orientation of a tree, then $P(H)$ is an orientation of a forest.

34. Up to isomorphism, there is only one unbalanced cycle $H$ on four vertices that is a core and not the directed cycle. Show that AC does not solve CSP($H$).

35. Show that AC solves CSP($T_n$), for every $n \geq 1$.

36. Let $H$ be a finite digraph. Show that $P(H)$ contains a loop if and only if $H$ contains a directed cycle.

37. Show that the previous statement is false for infinite digraphs $H$.

38. Show that an orientation of a tree homomorphically maps to $H$ if and only if it homomorphically maps to $P(H)$ (Hint: use parts of the proof of Theorem 2.7).

39. Let $H$ be a finite directed graph. Then $AC_H$ rejects an orientation of a tree $T$ if and only if there is no homomorphism from $T$ to $H$ (in other words, AC solves CSP($H$) when the input is restricted to orientations of trees).

3 The Path-consistency Procedure

The path-consistency procedure is a well-studied generalization of the arc-consistency procedure from artificial intelligence. The path-consistency procedure is also known as the pair-consistency check algorithm in the graph theory literature.
Many CSPs that cannot be solved by the arc-consistency procedure can still be solved in polynomial time by the path-consistency procedure. The simplest examples are \( H = K_2 \) (see Exercise 18) and \( H = \overrightarrow{C}_3 \) (see Exercise 20). The idea is to maintain a list of pairs from \( V(H)^2 \) for each pair of distinct elements from \( V(G) \) (similarly to the arc-consistency procedure, where we maintained a list of vertices from \( V(H) \) for each vertex in \( V(G) \)). We successively remove pairs from these lists when the pairs can be excluded locally.

If we modify the path-consistency procedure as presented in Figure 4 by also maintaining lists \( L(x, x) \) (i.e., we maintain lists also for pairs with non-distinct elements), and also process triples \( x, y, z \) that are not pairwise distinct, we obtain the so-called strong path-consistency procedure. This procedure is at least as strong as the arc-consistency procedure, because the lists \( L(x, x) \) and the rules of the strong path-consistency procedure for \( x = y \) simulate the rules of the arc-consistency procedure. We will from now on work with strong path consistency only, which has practical and theoretical properties that are superior to path consistency. Sometimes we might even write path consistency in the following even if strong path consistency is meant.

```
PC_H(G)
Input: a finite digraph G.
Data structure: for each \( x, y \in V(G) \), a list \( L(x, y) \) of pairs from \( V(H)^2 \)
For all \( (x, y) \in V(G)^2 \)
  If \( (x, y) \in E(G) \) then \( L(x, y) := E(H) \)
  else \( L(x, y) := V(H)^2 \)
Do
  For all distinct vertices \( x, y, z \in V(G) \):
    For each \( (u, v) \in L(x, y) \):
      If there is no \( w \in V(H) \) such that \( (u, w) \in L(x, z) \) and \( (w, v) \in L(z, y) \) then
        Remove \( (u, v) \) from \( L(x, y) \)
    If \( L(x, y) \) is empty then reject
Loop until no list changes
```

Figure 4: The strong path-consistency procedure for \( H \)-colouring

In Subsection 3.1 we will see many examples of digraphs \( H \) where the path-consistency algorithm solves the \( H \)-colouring problem, but the arc-consistency algorithm does not. The greater power of the path-consistency procedure comes at the price of a larger worst-case running time: while we have seen a linear-time implementation of the arc-consistency procedure, the best known implementations of the path-consistency procedure require cubic time in the size of the input (see Exercise 40).

The \( k \)-consistency procedure. The strong path-consistency procedure can be generalised further to the \( k \)-consistency procedure. In fact, arc- and path-consistency procedure are just the special case for \( k = 2 \) and \( k = 3 \), respectively. In other words, for directed graphs \( H \) the path-consistency procedure is the 3-consistency procedure and the arc-consistency procedure is the 2-consistency procedure.

The idea of \( k \)-consistency is to maintain sets of \((k-1)\)-tuples from \( V(H)^{k-1} \) for each \((k-1)\)-tuple from \( V(G)^{k-1} \), and to successively remove tuples by local inference. It is straightforward...
to generalize also the details of the path-consistency procedure. For fixed $H$ and fixed $k$, the running time of the $k$-consistency procedure is still polynomial in the size of $G$. But the dependency of the running time on $k$ is clearly exponential.

However, we would like to point out that strong path consistency alias 3-consistency is of particular theoretical importance, due to the following recent result.

**Theorem 3.3** (of [22]). If $\text{CSP}(H)$ can be solved by $k$-consistency for some $k \geq 3$, then $\text{CSP}(H)$ can also be solved by 3-consistency.

More on this result can be found in Section 9.

**Exercises**

40. Show that the path-consistency procedure for the $H$-colouring problem can (for fixed $H$) be implemented such that the worst-case running time is cubic in the size of the input graph. (Hint: use a worklist as in AC-3.)

### 3.1 Majority Polymorphisms

In this section, we present a powerful criterion that shows that for certain graphs $H$ the path-consistency procedure solves the $H$-colouring problem. Again, this condition was first discovered in more general form by Feder and Vardi [22]; it subsumes many criteria that were studied in artificial intelligence and in graph theory before.

**Definition 3.2.** Let $D$ be a set. A function $f$ from $D^3$ to $D$ is called a majority function if $f$ satisfies the following equations, for all $x, y \in D$:

$$f(x, x, y) = f(x, y, x) = f(y, x, x) = x$$

As an example, let $D$ be $\{1, \ldots, n\}$, and consider the ternary median operation, which is defined as follows. Let $x, y, z$ be three elements from $D$. Suppose that $\{x, y, z\} = \{a, b, c\}$, where $a \leq b \leq c$. Then median$(x, y, z)$ is defined to be $b$.

**Theorem 3.3** (of [22]). Let $H$ be a finite digraph. If $H$ has a polymorphism that is a majority function, then the $H$-colouring problem can be solved in polynomial time (by the strong path-consistency procedure).

For the proof of Theorem 3.3 we need the following lemma.

**Lemma 3.4.** Let $f$ be a $k$-ary polymorphism of a digraph $H$. Let $G$ be an instance of the $H$-colouring problem, and $L(x, y)$ be the final list computed by the strong path-consistency procedure for $x, y \in V(G)$. Then $f$ preserves $L(x, y)$, i.e., if $(u_1, v_1), \ldots, (u_k, v_k) \in L(x, y)$, then $(f(u_1, \ldots, u_k), f(v_1, \ldots, v_k)) \in L(x, y)$.

**Proof.** We prove by induction over the execution of the algorithm that for all $x, y \in V(G)$ and $(u_1, v_1), \ldots, (u_k, v_k) \in L(x, y)$, at all times in the execution the pair $(f(u_1, \ldots, u_k), f(v_1, \ldots, v_k))$ is in the current list for $x, y$. In the beginning, this is true because $f$ is a polymorphism of $H$. For the inductive step, let $x, y, z \in V(G)$ and $(u_1, v_1), \ldots, (u_k, v_k) \in L(x, y)$ be arbitrary. By definition of the procedure, for each $i \in \{1, \ldots, k\}$ there exists a $w_i$ such that $(u_i, w_i) \in L(x, z)$ and $(w_i, v_i) \in L(z, y)$. By inductive assumption, $(f(u_1, \ldots, u_k), f(w_1, \ldots, w_k)) \in L(x, z)$ and $(f(w_1, \ldots, w_k), f(v_1, \ldots, v_k)) \in L(z, y)$. Hence, $(f(u_1, \ldots, u_k), f(v_1, \ldots, v_k))$ will not be removed in the next step of the algorithm. □
Proof of Theorem 3.3. Suppose that $H$ has a majority polymorphism $f: V(H)^3 \to V(H)$, and let $G$ be an instance of the $H$-colouring problem. Clearly, if the path-consistency procedure derives the empty list for some pair $(u, v)$ from $V(G)^2$, then there is no homomorphism from $G$ to $H$.

Now suppose that after running the path-consistency procedure on $G$ the list $L(x, y)$ is non-empty for all pairs $(x, y)$ from $V(G)^2$. We have to show that there exists a homomorphism from $G$ to $H$. We say that a homomorphism $h$ from an induced subgraph $G'$ of $G$ to $H$ preserves the lists iff $(h(x), h(y)) \in L(x, y)$ for all $x, y \in V(G')$. The proof shows by induction on $i$ that any homomorphism from a subgraph of $G$ on $i$ vertices that preserves the lists can be extended to any other vertex in $G$ such that the resulting mapping is a homomorphism to $H$ that preserves the lists.

For the base case of the induction, observe that for all vertices $x_1, x_2, x_3 \in V(G)$ every mapping $h$ from $\{x_1, x_2\}$ to $V(H)$ such that $(h(x_1), h(x_2)) \in L(x_1, x_2)$ can be extended to $x_3$ such that $(h(x_1), h(x_3)) \in L(x_1, x_3)$ and $(h(x_3), h(x_2)) \in L(x_3, x_2)$ (and hence preserves the lists), because otherwise the path-consistency procedure would have removed $(h(x_1), h(x_2))$ from $L(x_1, x_2)$.

For the inductive step, let $h'$ be any homomorphism from a subgraph $G'$ of $G$ on $i \geq 3$ vertices to $H$ that preserves the lists, and let $x$ be any vertex of $G$ not in $G'$. Let $x_1, x_2, x_3$ be some vertices of $G'$, and $h'_j$ be the restriction of $h'$ to $V(G') \setminus \{x_j\}$, for $1 \leq j \leq 3$.

By inductive assumption, $h'_j$ can be extended to $x$ such that the resulting mapping $h_j$ is a homomorphism to $H$ that preserves the lists. We claim that the extension $h$ of $h'$ that maps $x$ to $f(h_1(x), h_2(x), h_3(x))$ is a homomorphism to $H$ that preserves the lists.

For all $y \in V(G')$, we have to show that $(h(x), h(y)) \in L(x, y)$ (and that $(h(y), h(x)) \in L(y, x)$, which can be shown analogously). If $y \notin \{x_1, x_2, x_3\}$, then $h(y) = h'(y) = f(h'(y), h'(y)) = f(h_1(y), h_2(y), h_3(y))$, by the properties of $f$. Since $(h_i(x), h_i(y)) \in L(x, y)$ for all $i \in \{1, 2, 3\}$, and since $f$ preserves $L(x, y)$ by Lemma 3.4, we have $(h(x), h(y)) \in L(x, y)$, and are done in this case.

Clearly, $y$ can be equal to at most one of $\{x_1, x_2, x_3\}$. Suppose that $y = x_1$ (the other two cases are analogous). There must be a vertex $v \in V(H)$ such that $(h_1(x), v) \in L(x, y)$ (otherwise the path-consistency procedure would have removed $(h_1(x), h_1(x_2))$ from $L(x, x_2)$).

By the properties of $f$, we have $h(y) = h'(y) = f(v, h'(y), h'(y)) = f(v, h_2(y), h_3(y))$. Because $(h_1(x), v), (h_2(x), h_2(y)), (h_3(x), h_3(y))$ are in $L(x, y)$, Lemma 3.4 implies that $(h(x), h(y)) = (f(h_1(x), h_2(x), h_3(x)), f(v, h_2(y), h_3(y)))$ is in $L(x, y)$, and we are done.

Therefore, for $i = |V(G)|$, we obtain a homomorphism from $G$ to $H$.  

As an example, let $H$ be the transitive tournament on $n$ vertices, $T_n$. Suppose the vertices of $T_n$ are the first natural numbers, $\{1, \ldots, n\}$, and $(u, v) \in E(T_n)$ iff $u < v$. Then the median operation is a polymorphism of $T_n$, because if $u_1 < v_1, u_2 < v_2$, and $u_3 < v_3$, then clearly $\text{median}(u_1, u_2, u_3) < \text{median}(v_1, v_2, v_3)$. This yields a new proof that the $H$-colouring problem for $H = T_n$ is tractable.

Corollary 3.5. The path-consistency procedure solves the $H$-colouring problem for $H = T_n$.

Another class of examples of graphs having a majority polymorphism are unbalanced cycles, i.e., orientations of $C_n$ that do not homomorphically map to a directed path $[20]$. We only prove a weaker result here.

Proposition 3.6. Directed cycles have a majority polymorphism.
Proof. Let \( f \) be the ternary operation that maps \( u, v, w \) to \( u \) if \( u, v, w \) are pairwise distinct, and otherwise acts as a majority operation. We claim that \( f \) is a polymorphism of \( C_n \). Let \((u, u'), \( (v, v'), \( (w, w') \in E(C_n) \) be arcs. If \( u, v, w \) are all distinct, then \( u', v', w' \) are clearly all distinct as well, and hence \((f(u, v, w), f(u', v', w')) = (u, u') \in E(C_n) \). Otherwise, if two elements of \( u, v, w \) are equal, say \( u = v \), then \( u' \) and \( v' \) must be equal as well, and hence \((f(u, v, w), f(u', v', w')) = (u, u') \in E(C_n) \).

3.2 Near-unanimity Polymorphisms

Majority functions are a special case of so-called near-unanimity functions. A function \( f \) from \( D^k \) to \( D \) is called a \((k\text{-ary}) \) near unanimity (short, an \( nu \)) if \( f \) satisfies the following equations, for all \( x, y \in D \):

\[
f(x, \ldots, x, y) = f(x, \ldots, y, x) = \cdots = f(y, x, \ldots, x) = x
\]

Obviously, the majority operations are precisely the ternary near-unanimity function. Similarly as in Theorem 3.3 it can be shown that the existence of a \( k \)-ary \( nu \) polymorphism of \( H \) implies that the \( k \)-consistency procedure solves CSP\((H)\). Hence, Theorem 3.1 implies the following.

**Theorem 3.7.** Let \( H \) be a directed graph with a near unanimity polymorphism. Then \( PC \) solves CSP\((H)\).

Exercises.

41. A quasi majority function is a function from \( D^3 \) to \( D \) satisfying \( f(x, x, y) = f(x, y, x) = f(y, x, x) = f(x, x, x) \) for all \( x, y \in D \). Use Theorem 1.4 to show that a finite undirected graph \( H \) has an \( H \)-colouring problem that can be solved in polynomial time if \( H \) has a quasi majority polymorphism, and is NP-complete otherwise.

42. Show that every orientation of a path has a majority operation.

43. There is only one unbalanced cycle \( H \) on four vertices that is a core and not the directed cycle (we have seen this graph already in Exercise 34). Show that for this graph \( H \) the \( H \)-colouring problem can be solved by the path-consistency procedure.

44. (*) Show that every unbalanced orientation of a cycle has a majority polymorphism.

45. Modify the path-consistency procedure such that it can deal with instances of the precoloured \( H \)-colouring problem. Show that if \( H \) has a majority operation, then the modified path-consistency procedure solves the precoloured \( H \)-colouring problem.

46. Modify the path-consistency procedure such that it can deal with instances of the list \( H \)-colouring problem. Show that if \( H \) has a \( conservative \) majority operation, then the modified path-consistency procedure solves the list \( H \)-colouring problem.

47. An interval graph \( H \) is an (undirected) graph \( H = (V; E) \) such that there is an interval \( I_x \) of the real numbers for each \( x \in V \), and \((x, y) \in E \) iff \( I_x \) and \( I_y \) have a non-empty intersection. Note that with this definition interval graphs are necessarily reflexive, i.e., \((x, x) \in E \). Show that the precoloured \( H \)-colouring problem for interval graphs \( H \) can be solved in polynomial time. Hint: use the modified path-consistency procedure in Exercise 45.
48. Show that the digraph \((\mathbb{Z}; \{(x, y) \mid x - y = 1\})\) has a majority polymorphism.

49. Prove that \(H\)-colouring can be solved in polynomial time when \(H\) is the digraph from the previous exercise.

50. Show that the digraph \(H = (\mathbb{Z}; \{(x, y) \mid x - y \in \{1, 3\}\})\) has a majority polymorphism, and give a polynomial time algorithm for its \(H\)-colouring problem.

### 3.3 Maltsev Polymorphisms

**Definition 3.8.** An ternary function \(f : D^3 \rightarrow D\) is called
- a **minority operation** if it satisfies
  \[
  \forall x, y \in D. f(y, x, x) = f(x, y, x) = f(x, x, y) = y
  \]
- a **Maltsev operation** if it satisfies
  \[
  \forall x, y \in D. f(y, x, x) = f(x, x, y) = y
  \]

**Example 2.** Let \(D := \{0, \ldots, n - 1\}\). Then the function \(f : D^3 \rightarrow D\) given by \((x, y, z) \mapsto x - y + z \mod n\) is a Maltsev operation, since \(x - x + z = z\) and \(x - z + z = x\). For \(n = 2\), this is even a minority operation. If \(n > 2\), this function is not a minority, since then \(1 - 2 + 1 = 0 \not\equiv 2 \mod n\).

The function \(f\) from the example above is a polymorphism of \(\vec{C}_n\). To see this, suppose that \(u_1 - v_1 \equiv 1 \mod n\), \(u_2 - v_2 \equiv 1 \mod n\), and \(u_3 - v_3 \equiv 1 \mod n\). Then
\[
f(u_1, u_2, u_3) \equiv u_1 - u_2 + u_3 \equiv (v_1 + 1) - (v_2 + 1) + (v_3 + 1) \equiv f(v_1, v_2, v_3) + 1 \mod n.
\]

The following result appeared in 2011.

**Theorem 3.9** (Kazda [33]). If digraph \(G\) has a Maltsev polymorphism then \(G\) also has a majority polymorphism.

Hence, for digraphs \(H\) with a Maltsev polymorphism, strong path consistency solves the \(H\)-colouring problem, and in fact even the precoloured \(H\)-colouring problem. Theorem 3.9 is an immediate consequence of Theorem 3.12 below; to state it, we need the following concepts.

**Definition 3.10.** A graph \(G\) is called
- **rectangular** if \((x, y), (x', y), (x', y') \in E(G)\) implies that \((x, y') \in E(G)\).
- **\(k\)-rectangular** if whenever \(G\) contains directed paths of length \(k\) from \(x\) to \(y\), from \(x'\) to \(y\), and from \(x'\) to \(y'\), then also from \(x\) to \(y'\).
- **totally rectangular** if \(G\) is \(k\)-rectangular for all \(k \geq 1\).

We start with the fundamental observation: digraphs with a Maltsev polymorphism \(m\) are rectangular. This follows immediately from the definition of polymorphisms: we must have \((m(x, x', x'), m(y, y, y')) \in E(G)\), but \(m(x, x', x') = x\) and \(m(y, y, y') = y'\), so \((x, y') \in E(G)\). The converse does not hold, as the following example shows.
Example 3. The graph \(\{a, b, c\}; \{(a, a), (a, b), (b, c), (c, c)\}\) is rectangular (draw a picture!), but has no Maltsev polymorphism \(m\). Indeed, such an \(m\) would have to satisfy \(m(a, a, c) = c\) and \(m(a, c, c) = a\). Now \((m(a, a, c), m(a, b, c)) \in E(G)\) and \((m(a, b, c), m(a, c, c)) \in E(G)\), but \(G\) has no vertex \(x\) such that \((c, x) \in E(G)\) and \((x, a) \in E(G)\).

An example of a totally rectangular digraph is given in Figure 5. The next lemma points out an important consequence of \(k\)-rectangularity.

Lemma 3.11. Let \(G\) be a finite totally rectangular digraph with a cycle of net length \(d > 0\). Then \(G\) contains a directed cycle of length \(d\).

Proof. Let \(C = (u_0, \ldots, u_{k-1})\) be a cycle of \(G\) of net length \(d\); we prove the statement by induction on \(k\). Clearly, \(C\) can be decomposed into maximal directed paths, that is, there is a minimal set \(D\) of directed paths such that each pair \((u_0, u_1), (u_1, u_2), \ldots, (u_{k-1}, u_0)\) is contained in exactly one of the paths of \(D\). If the decomposition \(D\) consists of a single directed path then we have found a directed cycle and are done. Let \(P\) be the shortest directed path of \(D\), leading from \(u\) to \(v\) in \(G\). Then there are directed paths \(Q\) and \(Q'\) in \(D\) such that \(Q\) starts in \(u\) and \(Q'\) ends in \(v\), and \(P \neq Q\) or \(P \neq Q'\). By assumption, \(|Q|, |Q'| \geq \ell := |P|\). By \(\ell\)-rectangularity, there exists a directed path \(P'\) of length \(\ell\) from the vertex \(t\) of \(Q'\) at position \(|Q'| - \ell\) to the vertex \(t\) of \(Q\) at position \(\ell\). Now we distinguish the following cases.

- \(Q = Q'\): the cycle that starts in \(s\), follows the path \(Q\) until \(t\), and then returns to \(s\) via the path \(P'\) is shorter than \(C\) but still has net length \(d\).
- \(Q \neq Q'\). The cycle starting in \(s\), following \(Q\) for the final \(|Q| - \ell\) vertices of \(Q\), the cycle \(C\) until \(Q'\), the first \(|Q'| - \ell\) vertices of \(Q'\) until \(t\), and then \(P'\) back to \(s\) is a cycle which is shorter than \(C\) but still has net length \(d\).

In both cases, the statement follows by induction. \(\square\)

The following is a strengthening of Theorem 3.9; we only prove that 1 implies 2, and 2 implies 3, which suffices for the already mentioned consequence that for digraphs \(H\) with a Maltsev polymorphism, path-consistency solves the \(H\)-colouring problem.

Theorem 3.12 (Theorem 3.3 and Corollary 4.12 in [17]). Let \(G\) be a finite digraph. Then the following are equivalent.

1. \(G\) has a Maltsev polymorphism.
2. \(G\) is totally rectangular.
3. If $G$ is acyclic, then the core of $G$ is a simple directed path. Otherwise, the core of $G$ is a disjoint union of simple directed cycles.

4. $G$ has a minority and a majority polymorphism.

**Proof.** The implication from 4 to 1 is trivial since every minority operation is in particular Mal'tsev. To show that 1 implies 2, one can easily produce the required directed path for $k$.

The implication from 4 to 1 is trivial since every minority operation is in particular Mal'tsev. For the implication from 2 to 3, let us assume that $G$ is connected.

The general case then follows by applying the following argument to each of its connected components, and the observation that directed paths homomorphically map to longer directed paths and to directed cycles.

We first consider the case that $G$ is acyclic, and claim that in this case $G$ is balanced, i.e., there exists a surjective homomorphism $h$ from $G$ to $P_n$ for some $n \geq 1$. Otherwise, there exist $u, v \in V_G$ and two paths $P$ and $Q$ from $u$ to $v$ of different net lengths $\ell_1$ and $\ell_2$ (see Exercise 13). Put these two paths together at $u$ and $v$ to form an unbalanced cycle $C$. Then Lemma 3.11 implies that $G$ contains a directed cycle contrary to our assumptions.

Now, choose $n$ with $G \to P_n$ minimal, and fix $u \in h^{-1}(0)$ and $v \in h^{-1}(n)$. Then it is easy to see from $n$-rectangularity that there must exist a path of length $n$ in $G$ from $u$ to $v$, and hence the core of $G$ is $P_n$.

Now suppose that $G$ contains a directed cycle; let $C$ be the shortest directed cycle of $G$. We prove that $G$ homomorphically maps to $C$. It is easy to see that it suffices to show that for any two vertices $u, v$ of $G$ and for any two paths $P$ and $Q$ from $u$ to $v$ we have that their net lengths are congruent modulo $|C|$ (see Exercise 14). Otherwise, let $P$ and $Q$ be paths of net length $\ell_1$ and $\ell_2$ from $u$ to $v$ in $G$ such that $d := \ell_1 - \ell_2 \neq 0$ modulo $|C|$; without loss of generality, $\ell_2 < \ell_1$, so $d > 0$. We can assume that $u$ is an element of $C$, since otherwise we can choose a path $S$ from a vertex of $C$ to $u$ by connectivity of $G$, and append $S$ to both $P$ and $Q$. We can also assume that $d < m$ because if not, we can append $C$ to $Q$ to increase the length of $Q$ by a multiple of $m$, until $d = \ell_1 - \ell_2 < m$. Lemma 3.11 then implies that $G$ contains a directed cycle of length $d$, a contradiction to the choice of $C$.

For the missing implication from 3 to 4, we refer to [33] or [17].

**Exercises.**

51. Let $H$ be the graph $(\{0, 1, \ldots, 6\}; \{(0, 1), (1, 2), (3, 2), (4, 3), (4, 5), (5, 6)\})$. For which $k$ is it $k$-rectangular?

**4 Logic**

Let $\tau$ be a relational signature, i.e., a set of relation symbols, typically denoted by $R, S, T$, and each equipped with an *arity* from $\mathbb{N}$. A relational structure $\mathfrak{A}$ over the signature $\tau$ (also called $\tau$-structure) consists of a set $A$ (the *domain* or base set) together with a relation $R^\mathfrak{A} \subseteq A^k$ for each relation symbol $R$ of arity $k$ from $\tau$. It causes no harm to allow structures whose domain is empty.

A *homomorphism* $h$ from a structure $\mathfrak{A}$ with domain $A$ to a structure $\mathfrak{B}$ with domain $B$ and the same signature $\tau$ is a mapping from $A$ to $B$ that *preserves* each relation for the symbols in $\tau$; that is, if $(a_1, \ldots, a_k)$ is in $R^\mathfrak{A}$, then $(h(a_1), \ldots, h(a_k))$ must be in $R^\mathfrak{B}$. An *isomorphism* is a bijective homomorphism $h$ such that the inverse mapping $h^{-1} : B \to A$ that sends $h(x)$ to $x$ is a homomorphism, too.
A first-order $\tau$-formula $\phi(x_1, \ldots, x_n)$ is called primitive positive (in database theory also conjunctive query) if it is of the form

$$\exists x_{n+1}, \ldots, x_\ell (\psi_1 \land \cdots \land \psi_m)$$

where $\psi_1, \ldots, \psi_m$ are atomic $\tau$-formulas, i.e., formulas of the form $R(y_1, \ldots, y_k)$ with $R \in \tau$ and $y_i \in \{x_1, \ldots, x_\ell\}$, of the form $y = y'$ for $y, y' \in \{x_1, \ldots, x_\ell\}$, or $\bot$ (for false). As usual, formulas without free variables are called sentences. Note that we do not need a symbol $\top$ for true since we can use the primitive positive sentence $\exists x. x = x$ to express it; we sometimes use $\top$ as a shortcut for $\exists x. x = x$.

It is possible to rephrase the $H$-colouring problem and its variants using primitive positive sentences.

**Definition 4.1.** Let $\mathfrak{B}$ be a structure with a finite relational signature $\tau$. Then $\text{CSP}(\mathfrak{B})$ is the computational problem of deciding whether a given primitive positive $\tau$-sentence $\phi$ is true in $\mathfrak{B}$.

The given primitive positive $\tau$-sentence $\phi$ is also called an instance of $\text{CSP}(\mathfrak{B})$. The conjuncts of an instance $\phi$ are called the constraints of $\phi$. A mapping from the variables of $\phi$ to the elements of $\mathfrak{B}$ that is a satisfying assignment for the quantifier-free part of $\phi$ is also called a solution to $\phi$.

**Example 4** (Disequality constraints). Consider the problem $\text{CSP}(\{1, 2, \ldots, n\}; \neq)$. An instance of this problem can be viewed as an (existentially quantified) set of variables, some linked by disequality constraints. Such an instance holds in $\langle \{1, 2, \ldots, n\}; \neq \rangle$ if and only if the graph whose vertices are the variables, and whose edges are the inequality constraints, has a homomorphism to $K_n$.

### 4.1 From Structures to Formulas

To every finite relational $\tau$-structure $\mathfrak{A}$ we can associate a $\tau$-sentence, called the canonical conjunctive query of $\mathfrak{A}$, and denoted by $\phi(\mathfrak{A})$. The variables of this sentence are the elements of $\mathfrak{A}$, all of which are existentially quantified in the quantifier prefix of the formula, which is followed by the conjunction of all formulas of the form $R(a_1, \ldots, a_k)$ for $R \in \tau$ and tuples $(a_1, \ldots, a_k) \in R^\mathfrak{A}$.

For example, the canonical conjunctive query $\phi(K_3)$ of the complete graph on three vertices $K_3$ is the formula

$$\exists u \exists v \exists w \left( E(u, v) \land E(v, u) \land E(v, w) \land E(w, v) \land E(u, w) \land E(w, u) \right).$$

The proof of the following proposition is straightforward.

**Proposition 4.2.** Let $\mathfrak{B}$ be a structure with finite relational signature $\tau$, and let $\mathfrak{A}$ be a finite $\tau$-structure. Then there is a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ if and only if $\phi(\mathfrak{A})$ is true in $\mathfrak{B}$.

---

2 We deliberately use the word *disequality* instead of *inequality*, since we reserve the word *inequality* for the relation $x \leq y$. 

28
4.2 From Formulas to Structures

To present a converse of Proposition 4.2, we define the canonical structure $S(\phi)$ (in database theory this structure is called the canonical database) of a primitive positive $\tau$-formula, which is a relational $\tau$-structure defined as follows. We require that $\phi$ does not contain $\bot$. If $\phi$ contains an atomic formula of the form $x = y$, we remove it from $\phi$, and replace all occurrences of $x$ in $\phi$ by $y$. Repeating this step if necessary, we may assume that $\phi$ does not contain atomic formulas of the form $x = y$.

Then the domain of $S(\phi)$ is the set of variables (both the free variables and the existentially quantified variables) that occur in $\phi$. There is a tuple $(v_1, \ldots, v_k)$ in a relation $R$ of $S(\phi)$ iff $\phi$ contains the conjunct $R(v_1, \ldots, v_k)$. The following is similarly straightforward as Proposition 4.2.

**Proposition 4.3.** Let $B$ be a structure with signature $\tau$, and let $\phi$ be a primitive positive $\tau$-sentence other than $\bot$. Then $B \models \phi$ if and only if $S(\phi)$ homomorphically maps to $B$.

Due to Proposition 4.3 and Proposition 4.2, we may freely switch between the homomorphism and the logic perspective whenever this is convenient. In particular, instances of CSP($B$) can from now on be either finite structures $A$ or primitive positive sentences $\phi$.

Note that the $H$-colouring problem, the precoloured $H$-colouring problem, and the list $H$-colouring problem can be viewed as constraint satisfaction problems for appropriately chosen relational structures.

4.3 Primitive Positive Definability

Let $A$ be a $\tau$-structure, and let $A'$ be a $\tau'$-structure with $\tau \subseteq \tau'$. If $A$ and $A'$ have the same domain and $R^A = R^{A'}$ for all $R \in \tau$, then $A$ is called the $\tau$-reduct (or simply reduct) of $A'$, and $A'$ is called a $\tau'$-expansion (or simply expansion) of $A$. When $A$ is a structure, and $R$ is a relation over the domain of $A$, then we denote the expansion of $A$ by $R$ by $(A, R)$.

When $A$ is a $\tau$-structure, and $\phi(x_1, \ldots, x_k)$ is a formula with $k$ free variables $x_1, \ldots, x_k$, then the relation defined by $\phi$ is the relation

$$\{(a_1, \ldots, a_k) \mid A \models \phi(a_1, \ldots, a_k)\}.$$ 

If the formula is primitive positive, then this relation is called primitive positive definable.

**Example 5.** The relation $E' := \{(a, b) \in \{0, 1, 2, 3, 4\}^2 \mid a \neq b\}$ is primitive positive definable in $C_5$: the primitive positive definition is

$$\exists p_1, p_2 \ (E(x_1, p_1) \land E(p_1, p_2) \land E(p_2, x_2))$$

The following lemma says that we can expand structures by primitive positive definable relations without changing the complexity of the corresponding CSP. Hence, primitive positive definitions are an important tool to prove NP-hardness: to show that CSP($B$) is NP-hard, it suffices to show that there is a primitive positive definition of a relation $R$ such that CSP($B, R$) is already known to be NP-hard. Stronger tools to prove NP-hardness of CSPs will be introduced in Section 5.

**Lemma 4.4.** Let $B$ be a structure with finite relational signature, and let $R$ be a relation that has a primitive positive definition in $B$. Then CSP($B$) and CSP($B, R$) are linear-time equivalent.
Proof. It is clear that CSP(\(\mathcal{B}\)) reduces to the new problem. So suppose that \(\phi\) is an instance of CSP((\(\mathcal{B}, R\)). Replace each conjunct \(R(x_1, \ldots, x_l)\) of \(\phi\) by its primitive positive definition \(\psi(x_1, \ldots, x_l)\). Move all quantifiers to the front, such that the resulting formula is in prenex normal form and hence primitive positive. Finally, equalities can be eliminated one by one: for equality \(x = y\), remove \(y\) from the quantifier prefix, and replace all remaining occurrences of \(y\) by \(x\). Let \(\psi\) be the formula obtained in this way.

It is straightforward to verify that \(\phi\) is true in \((\mathcal{B}, R)\) if and only if \(\psi\) is true in \(\mathcal{B}\), and it is also clear that \(\psi\) can be constructed in linear time in the representation size of \(\phi\). 

Exercises.

52. Show that the relation \(\{(a, b, c) \in \{0, 1, 2\}^3 \mid a = b \text{ or } b = c \text{ or } a = c\}\) has a primitive positive definition over \(K_3\).

4.4 Cores and Constants

An automorphism of a structure \(\mathcal{B}\) with domain \(B\) is an isomorphism between \(\mathcal{B}\) and itself. The set of all automorphisms \(\alpha\) of \(\mathcal{B}\) is denoted by \(\text{Aut}(\mathcal{B})\), and forms a permutation group. When \(G\) is a permutation group on a set \(B\), and \(b \in B\), then a set of the form

\[S = \{\alpha(b) \mid \alpha \in G\}\]

is called an orbit of \(G\) (the orbit of \(b\)).

Let \((b_1, \ldots, b_k)\) be a \(k\)-tuple of elements of \(\mathcal{B}\). A set of the form \(S = \{(\alpha b_1, \ldots, \alpha b_k) \mid \alpha \in \text{Aut}(\mathcal{B})\}\) is called an orbit of \(k\)-tuples of \(\mathcal{B}\) (it is an orbit of the componentwise action of \(G\) on set \(X^k\) of \(k\)-tuples from \(X\)).

Lemma 4.5. Let \(\mathcal{B}\) be a structure with a finite relational signature and domain \(B\), and let \(R = \{(b_1, \ldots, b_k)\}\) be a \(k\)-ary relation that only contains one tuple \((b_1, \ldots, b_k) \in B^k\). If the orbit of \((b_1, \ldots, b_k)\) in \(\mathcal{B}\) is primitive positive definable, then there is a polynomial-time reduction from CSP((\(\mathcal{B}, R\)) to CSP(\(\mathcal{B}\)).

Proof. Let \(\phi\) be an instance of CSP((\(\mathcal{B}, R\)) with variable set \(V\). If \(\phi\) contains two constraints \(R(x_1, \ldots, x_k)\) and \(R(y_1, \ldots, y_k)\), then replace each occurrence of \(y_1\) by \(x_1\), then each occurrence of \(y_2\) by \(x_2\), and so on, and finally each occurrence of \(y_k\) by \(x_k\). We repeat this step until all constrains that involve \(R\) are imposed on the same tuple of variables \((x_1, \ldots, x_k)\).

Replace \(R(x_1, \ldots, x_k)\) by the primitive positive definition \(\theta\) of its orbit in \(\mathcal{B}\). Finally, move all quantifiers to the front, such that the resulting formula \(\psi\) is in prenex normal form and thus an instance of CSP(\(\mathcal{B}\)). Clearly, \(\psi\) can be computed from \(\phi\) in polynomial time. We claim that \(\phi\) is true in \((\mathcal{B}, R)\) if and only if \(\psi\) is true in \(\mathcal{B}\).

Suppose \(\phi\) has a solution \(s : V \rightarrow B\). Let \(s'\) be the restriction of \(s\) to the variables of \(V\) that also appear in \(\phi\). Since \((b_1, \ldots, b_n)\) satisfies \(\theta\), we can extend \(s'\) to the existentially quantified variables of \(\theta\) to obtain a solution for \(\psi\). In the opposite direction, suppose that \(s'\) is a solution to \(\psi\) over \(\mathcal{B}\). Let \(s\) be the restriction of \(s'\) to \(V\). Because \((s(x_1), \ldots, s(x_k))\) satisfies \(\theta\) it lies in the same orbit as \((b_1, \ldots, b_k)\). Thus, there exists an automorphism \(\alpha\) of \(\mathcal{B}\) that maps \((s(x_1), \ldots, s(x_k))\) to \((b_1, \ldots, b_k)\). Then the extension of the map \(x \mapsto \alpha s(x)\) that maps variables \(y_i\) of \(\phi\) that have been replaced by \(x_i\) in \(\psi\) to the value \(b_i\) is a solution to \(\phi\) over \((\mathcal{B}, R)\).
The definition of cores can be extended from finite digraphs to finite structures: as in the case of finite digraphs, we require that every endomorphism be an automorphism. All results we proved for cores of digraphs remain valid for cores of structures. In particular, every finite structure \( \mathcal{C} \) is homomorphically equivalent to a core structure \( \mathcal{B} \), which is unique up to isomorphism (see Section 1.4). For core structures, all orbits are primitive positive definable. This can be shown as in the proof of Proposition 1.6.

**Proposition 4.6.** Let \( \mathcal{B} \) be a finite core structure. Then orbits of \( k \)-tuples of \( \mathcal{B} \) are primitive positive definable.

Proposition 4.6 and Lemma 4.5 have the following consequence.

**Corollary 4.7.** Let \( \mathcal{B} \) be a finite core structure with elements \( b_1, \ldots, b_n \) and finite signature. Then \( \text{CSP}(\mathcal{B}) \) and \( \text{CSP}(\langle \mathcal{B}, \{b_1\}, \ldots, \{b_n\} \rangle) \) are polynomial time equivalent.

**Exercises.**

53. Show that if \( m \) is the number of orbits of \( k \)-tuples of a finite structure \( \mathcal{A} \), and \( \mathcal{C} \) is the core of \( \mathcal{A} \), then \( \mathcal{C} \) has at most \( m \) orbits of \( k \)-tuples.

**Solution:** Let \( f \) be a homomorphism from \( \mathcal{A} \) to \( \mathcal{C} \), and \( g \) a homomorphism from \( \mathcal{C} \) to \( \mathcal{A} \). We show that there exists an injection \( I \) from the set \( O \) of orbits of \( k \)-tuples of \( \mathcal{C} \) to the orbits of \( k \)-tuples of \( \mathcal{A} \). Our injection has the property that every \( O \in \mathcal{C} \) contains a tuple \( t \) such that \( g(t) \in I(O) \). It suffices to show that when two \( k \)-tuples \( c_1, c_2 \) from \( \mathcal{C} \) are mapped by \( g \) to \( k \)-tuples in the same orbit in \( \mathcal{A} \), then \( c_1 \) and \( c_2 \) lie in the same orbit in \( \mathcal{C} \). Let \( a \in \text{Aut}(\mathcal{A}) \) map \( g(c_2) \) to \( g(c_1) \). Then \( e_1 := f \circ a \circ g \in \text{End}(\mathcal{C}) = \text{Aut}(\mathcal{C}) \). Likewise, \( e_2 := f \circ g \in \text{End}(\mathcal{C}) = \text{Aut}(\mathcal{C}) \). But then \( e_2^{-1} \circ e_1 \) maps \( c_2 \) to \( c_1 \), so they are in the same orbit of \( \mathcal{C} \).

54. Show that if \( \mathcal{A} \) is a finite structure, and \( \mathcal{C} \) its core, and if \( \mathcal{A} \) and \( \mathcal{C} \) have the same number of orbits of pairs, then \( \mathcal{A} \) and \( \mathcal{C} \) are isomorphic.

**Solution.** Let \( a_1, a_2 \in A \) be distinct, and let \( f: \mathcal{A} \to \mathcal{C} \) be any homomorphism. It suffices to show that \( f(a_1) \neq f(a_2) \), because then \( f \) is injective, and hence \( \mathcal{A} \) is a core and therefore \( \mathcal{A} \cong \mathcal{C} \).

Let \( g: \mathcal{C} \to \mathcal{A} \) be a homomorphism. Let \( I \) be the injection from the orbits of pairs of \( \mathcal{C} \) to the orbits of pairs of \( \mathcal{A} \) constructed in Exercise 53. By assumption, this injection must be a bijection, and hence for distinct \( a_1, a_2 \in A \) there are \( c_1, c_2 \in C \) such that \( g(c_1, c_2) = (a_1, a_2) \). Since \( f \circ g \in \text{End}(\mathcal{C}) = \text{Aut}(\mathcal{C}) \), the pairs \( (c_1, c_2) \) and \( (f(a_1), f(a_2)) \) lie in the same orbit, and in particular we have \( f(a_1) \neq f(a_2) \).

### 4.5 Primitive Positive Interpretations

Primitive positive interpretations are a powerful generalisation of primitive positive definability that can be used to also relate structures with different domains.

**Definition 4.8.** A relational \( \sigma \)-structure \( \mathcal{B} \) has a primitive positive interpretation \( I \) in a \( \tau \)-structure \( \mathcal{A} \) if there exists a natural number \( d \), called the dimension of \( I \), and

- a primitive positive \( \tau \)-formula \( \delta_I(x_1, \ldots, x_d) \) – called the domain formula,
• for each atomic $\sigma$-formula $\phi(y_1, \ldots, y_k)$ a primitive positive $\tau$-formula $\phi_I(x_1, \ldots, x_k)$ where the $x_i$ denote disjoint $d$-tuples of distinct variables – called the defining formulas,

• the coordinate map: a surjective map $h: D \to B$ where

$$D := \{(a_1, \ldots, a_d) \in A^d \mid \mathfrak{A} \models \delta_I(a_1, \ldots, a_d)\}$$

such that for all atomic $\sigma$-formulas $\phi$ and all tuples $\bar{\pi}_i \in D$

$$\mathfrak{B} \models \phi(h(\bar{\pi}_1), \ldots, h(\bar{\pi}_k)) \iff \mathfrak{A} \models \phi(\bar{\pi}_1, \ldots, \bar{\pi}_k).$$

Note that the dimension $d$, the set $D$, and the coordinate map $h$ determine the defining formulas up to logical equivalence; hence, we sometimes denote an interpretation by $I = (d, D, h)$. Note that the kernel of $h$ coincides with the relation defined by $(y_1 = y_2)_I$, for which we also write $=_{I}$, the defining formula for equality.

**Example 6.** Let $G$ be an undirected graph. Then the line graph $L(G)$ of $G$ is the graph with vertices $E(G)$ and edge set

$$E(L(G)) := \{\{\{u, v\}, \{v, w\}\} \mid \{u, v\}, \{v, w\} \in E(G)\}.$$

The line graph is primitively positively interpretable in $G$.

**Example 7.** Let $G$ be a graph and let $F$ be an equivalence relation on $V(G)$. Then $G/F$ is the graph whose vertices are the equivalence classes of $F$, and where $S$ and $T$ are equivalent if there are $s \in S$ and $t \in T$ such that $\{s, t\} \in E(G)$. If $F$ has a primitive positive definition in $G$, then $G/F$ has a primitive positive interpretation in $G$.

**Theorem 4.9.** Let $\mathfrak{B}$ and $\mathfrak{C}$ be structures with finite relational signatures. If there is a primitive positive interpretation of $\mathfrak{B}$ in $\mathfrak{C}$, then there is a polynomial-time reduction from CSP($\mathfrak{B}$) to CSP($\mathfrak{C}$).

**Proof.** Let $d$ be the dimension of the primitive positive interpretation $I$ of the $\tau$-structure $\mathfrak{B}$ in the $\sigma$-structure $\mathfrak{C}$, let $\delta_I(x_1, \ldots, x_d)$ be the domain formula, let $h: \delta_I(\mathfrak{C}^d) \to D(\mathfrak{B})$ be the coordinate map, and let $\phi_I(x_1, \ldots, x_{dk})$ be the formula for the $k$-ary relation $R$ from $\mathfrak{B}$.

Let $\phi$ be an instance of CSP($\mathfrak{B}$) with variable set $U = \{x_1, \ldots, x_n\}$. We construct an instance $\psi$ of CSP($\mathfrak{C}$) as follows. For distinct variables $V := \{y_1^1, \ldots, y_n^d\}$, we set $\psi_1$ to be the formula

$$\bigwedge_{1 \leq i \leq n} \delta(y_1^1, \ldots, y_d^1).$$

Let $\psi_2$ be the conjunction of the formulas $\theta_I(y_{i_1}^1, \ldots, y_{i_k}^d, y_{i_1}^1, \ldots, y_{i_k}^d)$ over all conjuncts $\theta = R(x_{i_1}, \ldots, x_{i_k})$ of $\phi$. By moving existential quantifiers to the front, the sentence

$$\exists y_1^1, \ldots, y_n^d (\psi_1 \land \psi_2)$$

can be re-written to a primitive positive $\sigma$-formula $\psi$, and clearly $\psi$ can be constructed in polynomial time in the size of $\phi$.

We claim that $\phi$ is true in $\mathfrak{B}$ if and only $\psi$ is true in $\mathfrak{C}$. Let $C$ be the domain of $\mathfrak{C}$, $B$ the domain of $\mathfrak{B}$, and suppose that $f: U \to C$ satisfies all conjuncts of $\psi$ in $\mathfrak{C}$. Hence, by construction of $\psi$, if $\phi$ has a conjunct $\theta = R(x_{i_1}, \ldots, x_{i_k})$, then

$$\mathfrak{C} \models \theta_I((f(y_{i_1}^1), \ldots, f(y_{i_k}^d)), \ldots, (f(y_{i_1}^1), \ldots, f(y_{i_k}^d))).$$
By the definition of interpretations, this implies that
\[ \forall \models R(h(f(y_{i_1}^1), \ldots, f(y_{i_k}^d)), \ldots, h(f(y_{i_k}^1), \ldots, f(y_{i_k}^d))). \]

Hence, the mapping \( g: U \to B \) that sends \( x_i \) to \( h(f(y_i^1), \ldots, f(y_i^d)) \) satisfies all conjuncts of \( \phi \) in \( \forall \).

Now, suppose that \( f: U \to B \) satisfies all conjuncts of \( \phi \) over \( \forall \). Since \( h \) is a surjective mapping from \( \delta(\forall^d) \) to \( B \), there are elements \( c_1^1, \ldots, c_i^d \) in \( \forall \) such that \( h(c_1^1, \ldots, c_i^d) = f(x_i) \), for all \( i \in \{1, \ldots, n\} \). We claim that the mapping \( g: V \to C \) that maps \( y_i^j \) to \( c_i^j \) is a homomorphism from \( \psi \) to \( \forall \). By construction, any constraint in \( \psi \) either comes from \( \psi_1 \) or from \( \psi_2 \). If it comes from \( \psi_1 \) then it must be of the form \( \delta_I(y_1^1, \ldots, y_i^d) \), and is satisfied since the pre-image of \( h \) is \( \delta_I(\forall^d) \). If the constraint comes from \( \psi_2 \), then it must be a conjunct of a formula \( \theta_I(y_1^1, \ldots, y_i^d, \ldots, y_{i_k}^1, \ldots, y_{i_k}^d) \) that was introduced for a constraint \( \theta = R(x_1, \ldots, x_{i_k}) \) in \( \forall \). It therefore suffices to show that
\[ \forall \models \theta_I(g(y_1^1), \ldots, g(y_i^d), \ldots, g(y_{i_k}^1), \ldots, g(y_{i_k}^d)). \]

By assumption, \( R(f(x_1), \ldots, f(x_{i_k})) \) holds in \( \forall \). By the choice of \( c_1^1, \ldots, c_i^d \), this shows that \( R(h(c_1^1, \ldots, c_i^d), \ldots, h(c_1^1, \ldots, c_i^d)) \) holds in \( \forall \). By the definition of interpretations, this is the case if and only if \( \theta_I(c_1^1, \ldots, c_i^d, \ldots, c_{i_k}^1, \ldots, c_{i_k}^d) \) holds in \( \forall \), which is what we had to show.

In many hardness proofs we use Theorem 4.9 in the following way.

**Corollary 4.10.** Let \( \forall \) be a finite relational structure. If there is a primitive positive interpretation of \( K_3 \) in \( \forall \), then \( \text{CSP}(\forall) \) is NP-hard.

**Proof.** This is a direct consequence of Theorem 4.9 and the fact that \( \text{CSP}(K_3) \) is NP-hard (see, e.g., [24]).

Indeed, \( K_3 \) belongs to one of the most expressive finite structures, in the following sense.

**Theorem 4.11.** For every \( n \geq 3 \), every finite structure has a primitive positive interpretation in \( K_n \).

**Proof.** Let \( \forall \) be a finite \( \tau \)-structure with the domain \( A = \{1, \ldots, k\} \). Our interpretation \( I \) of \( \forall \) in \( K_n \) is \( 2k \)-dimensional. The domain formula \( \delta_I(x_1, \ldots, x_k, x_1', \ldots, x_k') \) expresses that for exactly one \( i \leq k \) we have \( x_i = x_i' \). Note that this formula is preserved by all permutations of \( \{1, \ldots, k\} \). We will see in Proposition 5.12 that every such formula is equivalent to a primitive positive formula over \( K_n \). Equality is interpreted by the formula
\[ =_I (x_1, \ldots, x_k, x_1', \ldots, x_k', y_1, \ldots, y_k, y_1', \ldots, y_k') := \bigwedge_{i=1}^k ((x_i = x_i') \leftrightarrow (y_i = y_i')). \]

Note that \( =_I \) defines an equivalence relation on the set of all \( 2k \)-tuples \((u_1, \ldots, u_k, u_1', \ldots, u_k')\) that satisfy \( \delta_I \). The coordinate map sends this tuple to \( i \) if and only if \( u_i = u_i' \). When \( R \in \tau \) is \( m \)-ary, then the formula \( R(x_1, \ldots, x_m)_I \) is any primitive positive formula which is equivalent to the following disjunction of conjunctions with \( 2mk \) variables \( x_{1,1}, \ldots, x_{m,k}, x_{1,1}', \ldots, x_{m,k}' \): for each tuple \((t_1, \ldots, t_m) \in R^\forall \) the disjunction contains the conjunct \( \bigwedge_{i \leq m} x_{i,t_i} = x_{i,t_i}' \); again, Proposition 5.12 implies that such a primitive positive formula exists.
Primitive positive interpretations can be composed: if

- $\mathcal{C}_1$ has a $d_1$-dimensional pp-interpretation $I_1$ in $\mathcal{C}_2$, and
- $\mathcal{C}_2$ has an $d_2$-dimensional pp-interpretation $I_2$ in $\mathcal{C}_3$,

then $\mathcal{C}_1$ has a natural $(d_1d_2)$-dimensional pp-interpretation in $\mathcal{C}_3$, which we denote by $I_1 \circ I_2$. To formally describe $I_1 \circ I_2$, suppose that the signature of $\mathcal{C}_1$ is $\tau_i$ for $i = 1, 2, 3$, and that $I_1 = (d_1, S_1, h_1)$ and $I_2 = (d_2, S_2, h_2)$. Let $\phi$ be a primitive positive $\tau_2$-formula, let $\phi_{I_2}$ denote the $\tau_3$-formula obtained from $\phi$ by replacing each atomic $\tau_2$-formula $\psi$ in $\phi$ by the $\tau_3$-formula $\psi_{I_2}$. Note that $\phi_{I_2}$ is again primitive positive. The domain map of $I_1 \circ I_2$ is defined by

$$(a_1^1, \ldots, a_{d_2}^1, \ldots, a_1^{d_1}, \ldots, a_{d_2}^{d_1}) \mapsto h_1(h_2(a_1^1, \ldots, a_{d_2}^1), \ldots, h_2(a_1^{d_1}, \ldots, a_{d_2}^{d_1})).$$

### 4.6 The Structure-Building Operators $H$, $C$, and $PP$

In the previous three sections we have seen several conditions on $\mathfrak{A}$ and $\mathfrak{B}$ that imply that $\text{CSP}(\mathfrak{A})$ reduces to $\text{CSP}(\mathfrak{B})$; in this section we compare them. Let $\mathcal{C}$ be a class of finite structures. We write

1. $H(\mathcal{C})$ for the class of structures homomorphically equivalent to structures in $\mathcal{C}$.
2. $C(\mathcal{C})$ for the class of all structures obtained by expanding a core structure in $\mathcal{C}$ by singleton relations $\{a\}$.
3. $PP(\mathcal{C})$ for the class of all structures with a primitive positive interpretation in a structure from $\mathcal{C}$.

Let $\mathcal{D}$ be the smallest class containing $\mathcal{C}$ and closed under $H$, $C$, and $PP$. Barto, Opršal, and Pinsker [8] showed that $\mathcal{D} = H(PP(\mathcal{C}))$. In other words, if there is a chain of applications of the three operators $H$, $C$, and $PP$ to derive $\mathfrak{A}$ from $\mathfrak{B}$, then there is also a two-step chain to derive $\mathfrak{A}$ from $\mathfrak{B}$, namely by interpreting a structure $\mathfrak{B}'$ that is homomorphically equivalent to $\mathfrak{A}$. This insight is conceptually important for the CSP since it leads to a better understanding of the power of the available tools.

**Proposition 4.12** (from [8]). Suppose that $\mathfrak{B}$ is a core, and that $\mathcal{C}$ is the expansion of $\mathfrak{B}$ by constants. Then $\mathcal{C}$ is homomorphically equivalent to a structure with a primitive positive interpretation in $\mathfrak{B}$. In symbols,

$$C(\mathcal{C}) \subseteq H(PP(\mathcal{C})).$$

**Proof.** Let $c \in B$. By Proposition 4.6, the orbit $O$ of $c$ has a primitive positive definition $\phi(x)$ in $B$. We give a 2-dimensional primitive positive interpretation of a structure $\mathfrak{A}$ with the same signature $\tau$ as $\mathcal{C}$. The domain formula $\delta(x_1, x_2)$ for $\mathfrak{A}$ is $\phi(x_2)$. If $R \in \tau$ and $k$ is the arity of $R$ then

$$R^\mathfrak{A} := \{(a_1, b_1), \ldots, (a_k, b_k) \in (A^2)^k \mid (a_1, \ldots, a_k) \in R^\mathfrak{B} \text{ and } b_1 = \cdots = b_k \in O\}.$$

Otherwise, if $R \notin \tau$, then $R^\mathcal{C} = \{c\}$ and we define $R^\mathfrak{A} := \{(a, a) \mid a \in O\}$. It is clear that $\mathfrak{A}$ has a primitive positive interpretation in $\mathfrak{B}$.

We claim that $\mathfrak{A}$ and $\mathcal{C}$ are homomorphically equivalent. The homomorphism from $\mathcal{C}$ to $\mathfrak{A}$ is given by $a \mapsto (a, c)$.
• if \((a_1, \ldots, a_k) \in R^\mathcal{C} = R^\mathcal{B}\) then \(((a_1, c), \ldots, (a_k, c)) \in R^\mathcal{A};

• the relation \(R^\mathcal{C} = \{c\}\) is preserved since \((c, c) \in R^\mathcal{A}.

To define a homomorphism \(h\) from \(\mathfrak{A}\) to \(\mathfrak{C}\) we pick for each \(a \in O\) an automorphism \(\alpha_a \in \text{Aut}(\mathfrak{B})\) such that \(\alpha_a(a) = c\). Note that \(b \in O\) since \(\mathfrak{B} \models \delta(a, b)\), and we define \(h(a, b) := \alpha_b(a)\). To check that this is indeed a homomorphism, let \(R \in \tau\) be \(k\)-ary, and let \(t = ((a_1, b_1), \ldots, (a_k, b_k)) \in R^\mathcal{A}\). Then \(b_1 = \cdots = b_k =: b \in O\) and we have that \(h(t) = (\alpha_b(a_1), \ldots, \alpha_b(a_k))\) is in \(R^\mathcal{C}\) since \((a_1, \ldots, a_k) \in R^\mathcal{B} = R^\mathcal{C}\) and \(\alpha_b\) preserves \(R^\mathcal{B} = R^\mathcal{C}\).

If \(R^\mathcal{A} = \{(a, a) \mid a \in O\}\), then \(R\) is preserved as well, because \(h((a, a)) = \alpha_a(a) = c \in \{c\} = R^\mathcal{C}\).

\[\square\]

**Theorem 4.13** (from [8]). Suppose that \(\mathfrak{A}\) can be obtained from \(\mathfrak{C}\) by applying \(H\), \(C\), and \(PP\). Then \(\mathfrak{A} \in H(PP(\mathfrak{C}))\). That is, \(\mathfrak{A}\) is homomorphically equivalent to a structure with a primitive positive interpretation in \(\mathfrak{B}\).

**Proof.** We have to show that \(H(PP(\mathfrak{C}))\) is closed under \(H\), \(C\), and \(PP\). Homomorphic equivalence is transitive so \(H(H(\mathfrak{C})) \subseteq H(\mathfrak{C})\).

We show that if \(\mathfrak{A}\) and \(\mathfrak{B}\) are homomorphically equivalent, and \(\mathfrak{C}\) has a \(d\)-dimensional primitive positive interpretation \(I_1\) in \(\mathfrak{B}\), then \(\mathfrak{C}\) is homomorphically equivalent to a structure \(\mathfrak{D}\) with a \(d\)-dimensional primitive positive interpretation \(I_2\) in \(\mathfrak{A}\). Let \(h_1: A \to B\) be the homomorphism from \(\mathfrak{A}\) to \(\mathfrak{B}\), and \(h_2\) the homomorphism from \(\mathfrak{B}\) to \(\mathfrak{A}\). The interpreting formulas of \(I_2\) are the same as the interpreting formulas of \(I_1\); this describes the structure \(\mathfrak{D}\) up to isomorphism. We claim that the map \(g_1(I_2(a_1, \ldots, a_d)) := I_1(h_1(a_1), \ldots, h_1(a_d))\) is a homomorphism from \(\mathfrak{D}\) to \(\mathfrak{C}\). Indeed, for a \(k\)-ary relation symbol from the signature of \(\mathfrak{C}\) and \(\mathfrak{D}\), let \(((a_1^1, \ldots, a_1^k), \ldots, (a_d^1, \ldots, a_d^k)) \in R^\mathfrak{D}\); hence, the \(dk\)-tuple \((a_1^1, \ldots, a_d^1), \ldots, (a_1^k, \ldots, a_d^k)\) satisfies the primitive positive defining formula for \(R(x_1, \ldots, x_d^k)\), and

\[\begin{align*}
(h_1(a_1^1), \ldots, h_1(a_d^1), \ldots, h_1(a_1^k), \ldots, h_1(a_d^k))
\end{align*}\]

satisfies this formula, too. This in turn implies that

\[\begin{align*}
(I_1(h_1(a_1^1), \ldots, h_1(a_d^1)), \ldots, I_1(h_1(a_1^k), \ldots, h_1(a_d^k))) \in R^\mathcal{C}.
\end{align*}\]

Similarly, \(g_2(I_1(b_1, \ldots, b_d)) := I_2(h_2(b_1), \ldots, h_2(b_d))\) is a homomorphism from \(\mathfrak{C}\) to \(\mathfrak{D}\). So we conclude that

\[
PP(H(PP(\mathfrak{C}))) \subseteq H(PP(H(PP(\mathfrak{C}))))
\]

because primitive positive interpretability is transitive, too. Finally, Proposition 4.12 shows that

\[
C(H(PP(\mathfrak{C}))) \subseteq H(PP(H(PP(\mathfrak{C}))))
\]

where the last inclusion again follows from the observations above. \(\square\)

There are finite idempotent structures \(\mathfrak{B}\) that show that \(H(PP(\mathfrak{B}))\) can be strictly larger than \(PP(\mathfrak{B})\).
We finally show that \( A \) classes of \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \) in \( B \) of \( A \). Let \( A \) be the \( \tau \)-structure with domain \( \mathbb{Z}_2 \) such that for \( a = 0 \) and \( a = 1 \)
\[
R^A_{a,0} := \{(x, y, z) \in (\mathbb{Z}_2)^3 \mid x + y + z = a\}.
\]

Let \( \mathcal{B} \) be the structure with domain \( (\mathbb{Z}_2)^2 \) and signature \( \{R_{a,b} \mid a, b \in \mathbb{Z}_2\} \) such that
\[
R^\mathcal{B}_{a,b} := \{(x, y, z) \in ((\mathbb{Z}_2)^2)^3 \mid x + y + z = (a, b)\}.
\]

Now observe that
- \((x_1, x_2) \mapsto x_1\) is a homomorphism from \( \mathcal{B}' \) to \( \mathfrak{A} \), and \( x \mapsto (x, 0)\) is a homomorphism from \( \mathfrak{A} \) to \( \mathcal{B}' \). Therefore \( \mathfrak{A} \in H(\mathcal{B}') \).
- Trivially, \( \mathcal{B}' \in \text{PP}(\mathcal{B}) \) and consequently \( \mathfrak{A} \in H(\text{PP}(\mathcal{B})) \).
- \( \text{Pol}(\mathcal{B}) \) is idempotent.

We finally show that \( \mathfrak{A} \notin \text{PP}(\mathcal{B}) \). Suppose for contradiction that there is a \( \phi \)-interpretation of \( \mathfrak{A} \) in \( \mathcal{B} \) with coordinate map \( c: C \to A \) where \( C \subseteq B^n \) is primitive positive definable in \( \mathcal{B} \). The kernel \( K \) of \( c \) has a primitive positive definition \( \phi \) in \( \mathcal{B} \). The two equivalence classes of \( K \) are \( \phi \)-definable relations over \( \mathcal{B} \), too: the formula \( \exists x(\phi(x, y) \land R_{a,b}(x)) \) defines the equivalence class of \( (a, b) \). But the relations with a primitive positive definition in \( \mathcal{B} \) are precisely affine linear subspaces of the vector space \( (\mathbb{Z}_2)^2 \), so their cardinality must be a power of 4. And two powers of 4 cannot add up to a power of 4.

We will revisit primitive positive interpretations in Section \( \S \) where we study them from a universal-algebraic perspective.

## 5 Relations and Functions

### 5.1 Function Clones

For \( n \geq 1 \) and a set \( D \), denote by \( \mathcal{O}^{(n)}_D \) the set \( D^{D^n} := (D^n \to D) \) of \( n \)-ary functions on \( D \). The elements of \( \mathcal{O}^{(n)}_D \) will typically be called the \textit{operations} of arity \( n \) on \( D \), and \( D \) will be called the \textit{domain}. The set of all operations on \( D \) of finite arity will be denoted by \( \mathcal{O}_D := \bigcup_{n \geq 1} \mathcal{O}^{(n)}_D \). A \textit{function clone} (over \( D \)) is a subset \( \mathcal{C} \) of \( \mathcal{O}_D \) satisfying the following two properties:

- \( \mathcal{C} \) contains all projections, that is, for all \( 1 \leq k \leq n \) it contains the operation \( \pi_k^n \in \mathcal{O}^{(n)}_D \) defined by \( \pi_k^n(x_1, \ldots, x_n) = x_k \), and
- \( \mathcal{C} \) is \textit{closed under composition}, that is, for all \( f \in \mathcal{C} \cap \mathcal{O}^{(n)}_D \) and \( g_1, \ldots, g_n \in \mathcal{C} \cap \mathcal{O}^{(m)}_D \) it contains the operation \( f(g_1, \ldots, g_n) \in \mathcal{O}^{(m)}_D \) defined by
  \[
  (x_1, \ldots, x_m) \mapsto f(g_1(x_1, \ldots, x_m), \ldots, g_n(x_1, \ldots, x_m)).
  \]

A \textit{clone} is an abstraction of a function clone that will be introduced later in the course. In the literature, function clones are often called clones, or \textit{concrete clones}; we prefer to use the terms ‘function clone’ and ‘clone’ in analogy to ‘permutation group’ and ‘group’.

When \( \mathcal{C} \) is a function clone, then \( \mathcal{C}' \) is called a \textit{subclone} of \( \mathcal{C} \) if \( \mathcal{C}' \) is a function clone and \( \mathcal{C}' \subseteq \mathcal{C} \). When \( \mathcal{F} \) is a set of functions, we write \( \langle \mathcal{F} \rangle \) for the smallest function clone \( \mathcal{C} \) which contains \( \mathcal{F} \), and call \( \mathcal{C} \) the clone \textit{generated} by \( \mathcal{F} \).
5.2 Inv-Pol

The most important source of function clones in this text are polymorphism clones of digraphs and, more generally, structures.

Let \( f \) be from \( B \) and let \( R \subseteq B^m \) be a relation. Then we say that \( f \) preserves \( R \) (and that \( R \) is invariant under \( f \)) iff \( f(r_1, \ldots, r_n) \in R \) whenever \( r_1, \ldots, r_n \in R \), where \( f(r_1, \ldots, r_n) \) is calculated componentwise. When \( B \) is a relational structure with domain \( B \) then \( \text{Pol}(B) \) contains precisely those functions that preserve \( B \). It is easy to verify that \( \text{Pol}(B) \) is a function clone. Conversely, when \( F \) is a set of operations on \( B \), then we write \( \text{Inv}(F) \) for the set of all relations on \( B \) that are invariant under all functions in \( F \). It will be convenient to define the operator \( \text{Pol} \) also for sets \( R \) of relations over \( B \), writing \( \text{Pol}(R) \) for the set of operations of \( O_B \) that preserve all relations from \( R \).

**Proposition 5.1.** Let \( B \) be any structure. Then \( \text{Inv}(\text{Pol}(B)) \) contains the set of all relations that are primitive positive definable in \( B \).

**Proof.** Suppose that \( R \) is \( k \)-ary, has a primitive positive definition \( \psi(x_1, \ldots, x_k) \), and let \( f \) be an \( l \)-ary polymorphism of \( B \). To show that \( f \) preserves \( R \), let \( t_1, \ldots, t_l \) be \( k \)-tuples from \( R \). Let \( x_{k+1}, \ldots, x_n \) be the existentially quantified variables of \( \psi \). Write \( s_i \) for the \( n \)-tuple which extends the \( k \)-tuple \( t_i \) such that \( s_i \) satisfies the quantifier-free part \( \psi'(x_1, \ldots, x_k, x_{k+1}, \ldots, x_n) \) of \( \psi \). Then the tuple \( f(s_1, \ldots, s_l) \) satisfies \( \psi' \) since \( f \) is a polymorphism. This shows that \( B \models \psi(f(t_1, \ldots, t_l)) \) which is what we had to show. \( \square \)

**Theorem 5.2 (of [10][25]).** Let \( B \) be a finite structure. A relation \( R \) has a primitive positive definition in \( B \) if and only if \( R \) is preserved by all polymorphisms of \( B \).

**Proof.** One direction has been shown in Proposition 5.1. For the other direction, let \( R \) be a \( k \)-ary relation that is preserved by all polymorphisms of \( B \). In particular, \( R \) is preserved by all automorphisms of \( B \), and hence \( R \) is a union of orbits \( O_1, \ldots, O_w \) of \( k \)-tuples in the automorphism group of \( B \). If \( R \) is empty, there is nothing to show (but we use the assumption that \( \bot \) is allowed as a primitive positive formula), so let us assume that \( w \geq 1 \). Fix for each \( 1 \leq j \leq w \) a \( k \)-tuple \( a_j \) from \( O_j \). Let \( b_1, b_2, \ldots \) be an enumeration of all \( w \)-tuples in \( B^w \) with the additional property that for \( 1 \leq i \leq k \) we have \( b_i = (a_1[i], \ldots, a_w[i]) \).

Let \( q_1, \ldots, q_l \) be the elements of \( B^w \) without \( b_1, \ldots, b_k \). Write \( \psi \) for the quantifier-free part of the canonical query of \( B^w \) (see Section 4.1). We claim that the formula \( \exists q_1, \ldots, q_l \psi \) is a primitive positive definition of \( R \).

Since \( R \) is preserved by all polymorphisms of \( B \), all homomorphisms from \( B^w \) to \( B \) map \( b_1, \ldots, b_k \) to a tuple in \( R \). This shows that every tuple that satisfies \( \exists q_1, \ldots, q_l \psi \) is in \( R \).

Conversely, let \( t \in R \). Then \( t \in O_j \) for some \( 1 \leq j \leq w \) and there is an automorphism \( \alpha \) of \( B \) sending \( a_j \) to \( t \). Then the map \( f(x_1, \ldots, x_w) := \alpha(x_j) \) is a homomorphism from \( B^w \) to \( B \) that provides a witness \( f(b_i) \) for the variable \( x_i \) of \( \psi \) showing that \( t \) satisfies \( \exists q_1, \ldots, q_l \psi \). \( \square \)

**Corollary 5.3.** The complexity of \( \text{CSP}(B) \) only depends on \( \text{Pol}(B) \). If \( C \) is such that \( \text{Pol}(B) \subseteq \text{Pol}(C) \), then \( \text{CSP}(C) \) reduces in polynomial time to \( \text{CSP}(B) \).

**Proof.** Direct consequence of Theorem 5.2 and Lemma 4.4. \( \square \)
5.3 Essentially Unary Clones

We say that an operation \( f : B^k \to B \) is essentially unary iff there is an \( i \in \{1, \ldots, k\} \) and a unary operation \( f_0 \) such that \( f(x_1, \ldots, x_k) = f_0(x_i) \) for all \( x_1, \ldots, x_k \in B \). Operations that are not essentially unary are called essential\(^3\). We say that \( f \) depends on argument \( i \) if there are \( r, s \in B^k \) such that \( f(r) \neq f(s) \) and \( r_j = s_j \) for all \( j \in \{1, \ldots, k\} \setminus \{i\} \).

Lemma 5.4. Let \( f \in \mathcal{O} \) be an operation. Then the following are equivalent.

1. \( f \) is essentially unary.
2. \( f \) preserves \( P^3_B := \{(a, b, c) \in B^3 \mid a = b \text{ or } b = c \} \).
3. \( f \) preserves \( P^4_B := \{(a, b, c, d) \in B^4 \mid a = b \text{ or } c = d \} \).
4. \( f \) depends on at most one argument.

Proof. Let \( k \) be the arity of \( f \). The implication from (1) to (2) is obvious, since unary operations clearly preserve \( P^3_B \).

To show the implication from (2) to (3), we show the contrapositive, and assume that \( f \) violates \( P^4_B \). By permuting arguments of \( f \), we can assume that there are 4-tuples \( a^1, a^2, a^3, a^4 \in P^4_B \) with \( f(a^1), f(a^2) \notin P^4_B \) and \( l \leq k \) such that in \( a^1, a^2 \) the first two coordinates are equal, and in \( a^3, a^4 \) the last two coordinates are equal. Let \( c := (a^1_1, a^2_1, a^1_4, a^2_4) \). Since \( f(a^1), f(a^2) \notin P^4_B \) we have \( f(a^1_1, a^1_2, a^2_4) \neq f(a^2_1, a^2_2, a^1_4) \), and therefore \( f(c) \neq f(a^1_1, a^1_2, a^1_4) \) or \( f(c) \neq f(a^2_1, a^2_2, a^2_4) \). Let \( d = (a^1_1, a^1_2) \) in the first case, and \( d = (a^2_1, a^2_2) \) in the second case. Likewise, we have \( f(c) \neq f(a^1_3, a^1_4, a^1_5) \) or \( f(c) \neq f(a^2_3, a^2_4, a^2_5) \), and let \( e = (a^3_1, a^3_2) \) in the first, and \( e = (a^4_1, a^4_2) \) in the second case. Then for each \( i \leq k \), the tuple \((d_i, e_i, f(c))\) is from \( P^3_B \), but \((f(d_i), f(e_i), f(c)) \notin P^3_B \).

The proof of the implication from (3) to (4) is again by contraposition. Suppose \( f \) depends on the \( i \)-th and \( j \)-th argument, \( 1 \leq i \neq j \leq k \). Hence there exist tuples \( a_1, b_1, a_2, b_2 \in B^k \) such that \( a_1, b_1 \) and \( a_2, b_2 \) only differ at the entries \( i \) and \( j \), respectively, and such that \( f(a_1) \neq f(b_1) \) and \( f(a_2) \neq f(b_2) \).

For the implication from (4) to (1), suppose that \( f \) depends only on the first argument. Let \( i \leq k \) be maximal such that there is an operation \( g \) with \( f(x_1, \ldots, x_k) = g(x_{i-1}, x_i) \). If \( i = 1 \) then \( f \) is essentially unary and we are done. Otherwise, observe that since \( f \) does not depend on the \( i \)-th argument, neither does \( g \), and so there is an \((i - 1)\)-ary operation \( g' \) such that for all \( x_1, \ldots, x_n \in B \) we have \( f(x_1, \ldots, x_n) = g(x_1, \ldots, x_i) = g'(x_1, \ldots, x_{i-1}) \), contradicting the choice of \( i \).

\( \Box \)

5.4 Minimal Clones

A trivial clone is a clone all of whose operations are projections. Note that it follows from Lemma 5.3 that for any set \( B = \{b_1, \ldots, b_n\} \) the clone \( \text{Pol}(B; P^4_B, \{b_1, \ldots, b_n\}) \) is trivial.

Definition 5.5. A clone \( \mathcal{E} \) is minimal if it is non-trivial, and for every non-trivial \( \mathcal{E}' \subseteq \mathcal{E} \) we have \( \mathcal{E}' = \mathcal{E} \).

---

\(^3\)This is standard in clone theory, and it makes sense also when studying the complexity of CSPs, since the essential operations are those that are essential for complexity classification.
Definition 5.6. A function \( f \in O \) is minimal if \( f \) is of minimal arity such that every \( g \) generated by \( f \) is either a projection or generates \( f \).

Theorem 5.7. Every non-trivial clone \( C \) contains a minimal operation.

Proof. Consider the set of all clones contained in \( C \), partially ordered by inclusion. From this poset we remove the trivial clone; the resulting poset will be denoted by \( P \). We use Zorn’s lemma to show that \( P \) contains a minimal element. Observe that in \( P \), all descending chains \( C_1 \supseteq C_2 \supseteq \cdots \) are bounded, i.e., for all such chains there exists a \( D \in P \) such that \( C_i \supseteq D \) for all \( i \geq 1 \). To see this, observe that the set \( \bigcup_{i \geq 1} \text{Inv}(C_i) \) is closed under primitive positive definability in the sense that it is the set of relations that is primitive positive definable over some relational structure \( B \) (since only a finite number of relations can be mentioned in a formula, and since each of the \( C_i \) is closed under primitive positive definability). Moreover, one of the relations \( P_B^3, \{b_1\}, \ldots, \{b_n\} \) is not contained in \( \bigcup_{i \geq 1} \text{Inv}(C_i) \); otherwise, there would be a \( j \in \mathbb{N} \) such that \( \text{Inv}(C_j) \) contains all these relations, and hence \( C_j \) is the trivial clone contrary to our assumptions. Hence, \( \text{Pol}(B) \) is a non-trivial lower bound of the descending chain \( (C_i)_{i \geq 0} \). By Zorn’s lemma, \( P \) contains a minimal element, and this element contains a minimal operation in \( C \). \( \square \)

Lemma 5.8. Let \( B \) be a relational structure and let \( R \) be a \( k \)-ary relation that intersects \( m \) orbits of \( \text{Aut}(B) \). If \( B \) has a polymorphism \( f \) that violates \( R \), then \( B \) also has an at most \( m \)-ary polymorphism that violates \( R \).

Proof. Let \( f' \) be an polymorphism of \( B \) of smallest arity \( l \) that violates \( R \). Then there are \( k \)-tuples \( t_1, \ldots, t_l \in R \) such that \( f'(t_1, \ldots, t_l) \notin R \). For \( l > m \) there are two tuples \( t_i \) and \( t_j \) that lie in the same orbit of \( k \)-tuples, and therefore \( B \) has an automorphism \( \alpha \) such that \( \alpha t_i = t_j \). By permuting the arguments of \( f' \), we can assume that \( i = 1 \) and \( j = 2 \). Then the \((l-1)\)-ary operation \( g \) defined as

\[
g(x_2, \ldots, x_l) := f'(\alpha x_2, x_2, \ldots, x_l)
\]

is also a polymorphism of \( B \), and also violates \( R \), a contradiction. Hence, \( l \leq m \). \( \square \)

For essentially unary clones \( B \), we can bound the arity of minimal functions above \( B \).

Proposition 5.9. Let \( B \) be an arbitrary structure with \( r \) orbitals. Then every minimal clone above \( \text{End}(B) \) is generated by a function of arity at most \( 2r - 1 \).

Proof. Let \( C \) be a minimal clone above \( \text{End}(B) \). If all the functions in \( C \) are essentially unary, then \( C \) is generated by a unary operation together with \( \text{End}(B) \) and we are done. Otherwise, let \( f \) be an essential operation in \( C \). By Lemma 5.4, the operation \( f \) violates \( P_B^3 \) over the domain \( B \) of \( B \); recall that \( P_B^3 \) is defined by the formula \((x = y) \lor (y = z)\). The subset of \( P_B^3 \) that contains all tuples of the form \((a, a, b)\), for \( a, b \in B \), clearly consists of \( r \) orbit in \( B \). Similarly, the subset of \( P_B^3 \) that contains all tuples of the form \((a, b, c)\), for \( a, b \in B \), consists of the same number of orbits. The intersection of these two relations consists of exactly one orbit (namely, the triples with three equal entries), and therefore \( P_B^3 \) is the union of \( 2r - 1 \) different orbits. The assertion now follows from Lemma 5.8. \( \square \)

In the remainder of this section, we show that a minimal operation has one out of the following five types, due to Rosenberg [45]. A \( k \)-ary operation \( f \) is a semiprojection iff there exists an \( i \leq k \) such that \( f(x_1, \ldots, x_k) = x_i \) whenever \( |\{x_1, \ldots, x_k\}| < k \).
Lemma 5.10 (Świerczkowski; Satz 4.4.6 in [43]). Every at least 4-ary operation that turns into a projection whenever two arguments are the same is a semiprojection.

Proof. Let $f$ be an operation on the finite set $B$ of arity at least $n \geq 4$ as in the statement of the lemma. By assumption there exists an $i \in \{1, \ldots, n\}$ such that

\[ f(x_1, x_1, x_3, \ldots, x_n) = x_i \quad (1) \]

Let $k, l \in \{1, \ldots, n\}$ be distinct. We assume that $k \neq i$; this is without loss of generality since otherwise we can change the roles of $k$ and $l$. For notational simplicity, we assume in the following that $k < l$; the case that $l < k$ is analogous.

We claim that $f(x_1, \ldots, x_{k-1}, x_l, x_{k+1}, \ldots, x_n) = x_i$. If $\{k, l\} = \{1, 2\}$ then the claim is true. If $\{k, l\} \cap \{1, 2\} = \{k\}$, consider the function defined by

\[ f(x_1, x_1, x_3, \ldots, x_{l-1}, x_1, x_{l+1}, \ldots, x_n) \]

Then (1) implies that this function equals $x_i$. Since $f(x_1, x_2, x_3, \ldots, x_{l-1}, x_1, x_{l+1}, \ldots, x_n)$ by assumption is a projection, too, it must be the $i$-th projection, which proves the claim.

Finally, if $\{k, l\} \cap \{1, 2\} = \emptyset$, consider the operation defined by

\[ f(x_1, x_1, x_3, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_{l-1}, x_1, x_{l+1}, \ldots, x_n) \]

Again, (1) implies that this function equals $x_i$. By assumption the operation $f(x_1, x_2, x_3, \ldots, x_{k-1}, x_1, x_{k+1}, \ldots, x_{l-1}, x_1, x_{l+1}, \ldots, x_n)$ is a projection, too, so it must be the $i$-th projection, which concludes the proof.

Theorem 5.11. Let $f$ be a minimal operation. Then $f$ has one of the following types:

1. A unary operation with the property that $f(f(x)) = f(x)$ or $f(f(x)) = x$.
2. An essentially binary idempotent operation.
3. A majority operation.
4. A minority operation.
5. An idempotent $k$-ary semiprojection, for $k \geq 3$, which is not a projection.

Proof. There is nothing to show when $f$ is unary or binary. If $f$ is ternary, we have to show that $f$ is majority, Mal'tsev, or a semiprojection. By minimality of $f$, the binary operation $f_1(x, y) := f(y, x, x)$ is a projection, that is, $f_1(x, y) = x$ or $f_1(x, y) = y$. Note that in particular $f(x, x, x) = x$. Similarly, the other operations $f_2(x, y) := f(x, y, x)$, and $f_3(x, y) := f(x, x, y)$ obtained by identifications of two variables must be projections. We therefore distinguish eight cases.

1. $f(y, x, x) = x, f(x, y, x) = x, f(x, x, y) = x$.
   In this case, $f$ is a majority.
2. $f(y, x, x) = x, f(x, y, x) = x, f(x, x, y) = y$.
   In this case, $f$ is a semiprojection.
3. $f(y, x, x) = x, f(x, y, x) = y, f(x, x, y) = x$.
   In this case, $f$ is a semiprojection.
4. \( f(y, x, x) = x, f(x, y, x) = y, f(x, x, y) = y \).
   
   The operation \( g(x, y, z) := f(y, x, z) \) is a Maltsev operation.

5. \( f(y, x, x) = y, f(x, y, x) = x, f(x, x, y) = y \).
   
   In this case, \( f \) is a semiprojection.

6. \( f(y, x, x) = y, f(x, y, x) = x, f(x, x, y) = y \).
   
   In this case, \( f \) is a Maltsev operation.

7. \( f(y, x, x) = y, f(x, y, x) = y, f(x, x, y) = x \).
   
   The operation \( g(x, y, z) := f(x, z, y) \) is a Maltsev operation.

8. \( f(y, x, x) = y, f(x, y, x) = y, f(x, x, y) = y \).
   
   In this case, \( f \) is a Maltsev operation.

We claim that if \( f \) is a Maltsev operation, then it either it is a minority operation (and we are done) or it generates a Majority operation. Indeed, if \( f \) is not a minority then minimality of \( f \) implies that \( f(x, y, x) = x \). Now consider the function \( g \) defined by \( g(x, y, z) = f(x, f(x, y, z), z) \). We have

\[
\begin{align*}
g(x, x, y) &= f(x, f(x, x, y), y) = f(x, y, y) = x \\
g(x, y, x) &= f(x, f(x, y, x), x) = f(x, x, x) = x \\
g(y, x, x) &= f(y, f(y, x, x), x) = f(y, y, x) = x.
\end{align*}
\]

Note that every ternary function generated by a majority is again a majority. Also note that a function cannot be a majority and a minority at the same time unless the domain has only one element, so we obtain in this case a contradiction to the minimality of \( f \).

Finally, let \( f \) be \( k \)-ary, where \( k \geq 4 \). By minimality of \( f \), the operations obtained from \( f \) by identifications of arguments of \( g \) must be projections. The lemma of Świerczkowski implies that \( f \) is a semiprojection.

Proposition 5.12. For all \( n \geq 3 \), the graph \( K_n \) is projective (i.e., all idempotent polymorphisms of \( K_n \) are projections). All relations that are preserved by Sym\(i\{0, \ldots, n-1\}\) are primitive positive definable in \( K_n \).

This provides for example a solution to Exercise 52.

Proof. By Theorem 5.7 it suffices to show that the clone of idempotent polymorphisms of \( K_n \) does not contain a minimal operation. Hence, by Theorem 5.11 we have to verify that \( \text{Pol}(K_n) \) does not contain an essentially binary idempotent, a Maltsev, a majority, or a \( k \)-ary semiprojection for \( k \geq 3 \).

1. Let \( f \) be a binary idempotent polymorphism of \( K_n \).

   Observation 1. \( f(u, v) \in \{u, v\} \): otherwise, \( i := f(u, v) \) is adjacent to both \( u \) and \( v \), but \( f(i, i) = i \) is not adjacent to \( i \), in contradiction to \( f \) being a polymorphism.

   Observation 2. If \( f(u, v) = u \), then \( f(v, u) = u \): this is clear if \( u = v \), and if \( u \neq v \) it follows from \( f \) being a polymorphism.

By Observation 1, it suffices to show that there cannot be distinct \( u, v \) and distinct \( u', v' \) such that \( f(u, v) = u \) and \( f(u', v') = v' \). Suppose for contradiction that there are such \( u, v, u', v' \).
Case 1. $u = u'$. Since $f(u, v') = f(u', v') = v'$, we have $f(v', u) = u$ by Observation 2. This is in contradiction to $f(u, v) = u$ since $u = u'$ is adjacent to $v'$, and $E(v, u)$.

Case 2. $u \neq u'$.

Case 2.1. $f(u', u) = u$: this is impossible because $f(u, v) = u$, $E(u, u')$, and $E(u, v)$.

Case 2.2. $f(u', u) = u'$: this is impossible because $f(v', u') = u'$, $E(u', v')$, and $E(u', u)$.

2. Since $(1, 0), (1, 2), (0, 2) \in E(K_n)$, but $(0, 0) \notin E(K_n)$, the graph $K_n$ has no Maltsev polymorphism (it is not rectangular; see Section 3.3).

3. If $f$ is a majority, note that $f(0, 1, 2) = f(x_0, x_1, x_2)$ where $x_i$ is some element distinct from $i$ if $f(0, 1, 2) = i$, and $x_i := f(0, 1, 2)$ otherwise. But $(i, x_i) \in E(K_n)$, so $f$ is not a polymorphism of $K_n$.

4. Finally, let $f$ be a $k$-ary semiprojection for $k \geq 3$ which is not a projection. Suppose without loss of generality that $f(x_1, \ldots, x_k) = x_1$ whenever $|\{x_1, \ldots, x_k\}| < k$ (otherwise, permute the arguments of $f$). Since $f$ is not a projection, there exist pairwise distinct $a_1, \ldots, a_k \in V(K_n)$ such that $c := f(a_1, \ldots, a_k) \neq a_1$. Let $b_1, \ldots, b_k$ be such that $b_i$ is any element of $V(K_n) \setminus \{c\}$ if $c = a_i$, and $b_i := c$ otherwise. Note that $b_1 = a_1$ since $c \neq a_1$, and that $f(b_1, \ldots, b_n) = b_1 = a_1$ because $f$ is a semiprojection. But $(a_i, b_i) \in E(K_n)$ for all $i \leq k$, so $f$ is not a polymorphism of $K_n$.

The second part of the statement follows from Theorem 5.2. □

5.5 Schaefer’s Theorem

Schaefer’s theorem states that every CSP for a 2-element template is either in P or NP-hard. Via the Inv-Pol Galois connection (Section 5.2), most of the classification arguments in Schaefer’s article follow from earlier work of Post [44], who classified all clones on a two-element domain. We present a short proof of Schaefer’s theorem here.

Note that on Boolean domains, there is precisely one minority operation, and precisely one majority operation.

**Theorem 5.13** (Post [44]). Every minimal function on a two element set is among one of the following:

- a unary constant function.
- the unary function $x \mapsto 1 - x$.
- the binary function $(x, y) \mapsto \min(x, y)$.
- the binary function $(x, y) \mapsto \max(x, y)$.
- the Boolean minority operation.
- the Boolean majority operation.

**Proof.** If $f$ is unary the statement is trivial, so let $f$ be a minimal at least binary function above $C$. Note that $f$ defines a function in $C$, so it must be the identity by minimality of $f$, and hence $f$ is idempotent.
There are only four binary idempotent operations on \( \{0, 1\} \), two of which are projections and therefore cannot be minimal. The other two operations are min and max. Next, note that a semi-projection of arity at least three on a Boolean domain must be a projection. Thus, Theorem 5.11 implies that \( f \) is the majority or a minority operation.

**Theorem 5.14.** A Boolean relation \( R \) is preserved by the minority operation if and only if it has a definition by a conjunction of linear equalities modulo 2.

**Proof.** This statement follows from basic facts in linear algebra. Let \( R \) be \( n \)-ary. We view \( R \) as a subset of the Boolean vector space \( \{0, 1\}^n \). By definition, \( R \) is called **affine** if it is the solution space of a system of linear equations, and it is well-known that affine spaces are precisely those that are closed under **affine combinations**, i.e., linear combinations of the form \( \alpha_1 x_1 + \cdots + \alpha_n x_n \) such that \( \alpha_1 + \cdots + \alpha_n = 1 \). In particular, if \( R \) is affine it is preserved by \( (x_1, x_2, x_3) \mapsto x_1 + x_2 + x_3 \) which is the minority operation. Conversely, if \( R \) is preserved by the minority operation, then \( x_1 + \cdots + x_n \), for odd \( n \), can be written as

\[
\text{minority}(x_1, x_2, \text{minority}(x_3, x_4, \cdots \text{minority}(x_{n-2}, x_{n-1}, x_n)))
\]

and hence is contained in \( R \).

The following definition is very useful for proving that certain Boolean relations \( R \) can be defined in syntactically restricted propositional logic.

**Definition 5.15.** When \( \phi \) is a propositional formula in CNF that defines a Boolean relation \( R \), we say that \( \phi \) is **reduced** if when we remove a literal from a clause in \( \phi \), the resulting formula is not equivalent to \( \phi \).

Clearly, every Boolean relation has a reduced definition: simply remove literals from any definition in CNF until the formula becomes reduced.

**Lemma 5.16.** A Boolean relation \( R \) has a Horn definition if and only if \( R \) is preserved by min.

**Proof.** Let \( R \) be a Boolean relation preserved by min. Let \( \phi \) be a reduced propositional formula in CNF that defines \( \phi \). Now suppose for contradiction that \( \phi \) contains a clause \( C \) with two positive literals \( x \) and \( y \). Since \( \phi \) is reduced, there is an assignment \( s_1 \) that satisfies \( \phi \) such that \( s_1(x) = 1 \), and such that all other literals of \( C \) evaluate to 0. Similarly, there is a satisfying assignment \( s_2 \) for \( \phi \) such that \( s_2(y) = 1 \) and all other literal \( s \) of \( C \) evaluate to 0. Then \( s_0: x \mapsto \min(s_1(x), s_2(y)) \) does not satisfy \( C \), and does not satisfy \( \phi \), in contradiction to the assumption that min preserves \( R \).

A binary relation is called **bijunctive** if it can be defined by a propositional formula that is a conjunction of clauses of size two (aka 2CNF formulas).

**Lemma 5.17.** A Boolean relation \( R \) is preserved by the majority operation if and only if it is bijunctive.

**Proof.** We present the proof that when \( R \) is preserved by the majority, and \( \phi \) is a reduced definition of \( R \), then all clauses \( C \) have at most two literals. Suppose for contradiction that \( C \) has three literals \( l_1, l_2, l_3 \). Since \( \phi \) is reduced, there must be satisfying assignments \( s_1, s_2, s_3 \) to \( \phi \) such that under \( s_i \) all literals of \( C \) evaluate to 0 except for \( l_i \). Then the mapping \( s_0: x \mapsto \text{majority}(s_1(x), s_2(x), s_3(x)) \) does not satisfy \( C \) and therefore does not satisfy \( \phi \), in contradiction to the assumption that majority preserves \( R \).
The following relation is called the *(Boolean) not-all-equal relation.*

\[ \text{NAE} := \{(0,0,0),(0,1,1),(1,0,1),(1,1,0),(0,1,1),(1,0,1)\} \]

**Theorem 5.18** (Schaefer [46]). Let \( \mathcal{B} \) be a structure over a two-element universe. Then either \( (\{0,1\}; \text{NAE}) \) has a primitive positive definition in \( \mathcal{B} \), and \( \text{CSP}(\mathcal{B}) \) is \( \text{NP} \)-complete, or

1. \( \mathcal{B} \) is preserved by a constant operation.

2. \( \mathcal{B} \) is preserved by min. In this case, every relation of \( \mathcal{B} \) has a definition by a propositional Horn formula.

3. \( \mathcal{B} \) is preserved by max. In this case, every relation of \( \mathcal{B} \) has a definition by a dual-Horn formula, that is, by a propositional formula in CNF where every clause contains at most one negative literal.

4. \( \mathcal{B} \) is preserved by the majority operation. In this case, every relation of \( \mathcal{B} \) is bijunctive.

5. \( \mathcal{B} \) is preserved by the minority operation. In this case, every relation of \( \mathcal{B} \) can be defined by a conjunction of linear equations modulo 2.

In case (1) to case (5), then for every finite-signature reduct \( \mathcal{B}' \) of \( \mathcal{B} \) the problem \( \text{CSP}(\mathcal{B}') \) can be solved in polynomial time.

**Proof.** If \( \text{Pol}(\mathcal{B}) \) contains a constant operation, then we are in case one; so suppose in the following that this is not the case. If NAE is primitive positive definable in \( \mathcal{B} \), then \( \text{CSP}(\mathcal{B}) \) is \( \text{NP} \)-hard by reduction from positive not-all-equal-3SAT [24]. Otherwise, by Theorem 5.2 there is an operation \( f \in \text{Pol}(\mathcal{B}) \) that violates NAE. If \( f \) equals the identity then \( f \) is idempotent. Otherwise, \( f \) equals \( \neg \). But then \( \neg f \in \text{Pol}(\mathcal{B}) \) is idempotent and also violates NAE. So let us assume in the following that \( f \) is idempotent. Then \( f \) generates an at least binary minimal operation \( g \in \text{Pol}(\mathcal{B}) \).

By Theorem 5.13 the operation \( g \) equals min, max, the Boolean minority, or the Boolean majority function.

- \( g = \text{min} \) or \( g = \text{max} \). If \( \mathcal{B} \) is preserved by min, then by Lemma 5.16 all relations of \( \mathcal{B} \) can be defined by propositional Horn formulas. It is well-known that positive unit-resolution is a polynomial-time decision procedure for the satisfiability problem of propositional Horn-clauses [47]. The case that \( g = \text{max} \) is dual to this case.

- \( g = \text{majority} \). By Lemma 5.17 all relations of \( \mathcal{B} \) are bijunctive. Hence, in this case the instances of \( \text{CSP}(\mathcal{B}) \) can be viewed as instances of the 2SAT problem, and can be solved in linear time [1].

- \( g = \text{minority} \). By Theorem 5.14 every relation of \( \mathcal{B} \) has a definition by a conjunction of linear equalities modulo 2. Then \( \text{CSP}(\mathcal{B}) \) can be solved in polynomial time by Gaussian elimination.

This concludes the proof of the statement. \( \square \)
6 Maltsev Polymorphisms

Recall from Section 3.3 the definition of a Maltsev operation: this is a ternary operation \( f: D^3 \rightarrow D \) satisfying
\[
\forall x, y \in D. f(y, x, x) = f(x, x, y) = y.
\]
As we have seen, every digraph with a Maltsev polymorphism also has a majority polymorphism. However, when considering arbitrary relational structures then there are many examples with a Maltsev polymorphism but without a majority polymorphism. In this section, we present the algorithm of Bulatov and Dalmau for \( \text{CSP}(\mathcal{A}) \) when \( \mathcal{A} \) is preserved by a Maltsev polymorphism \[14\].

**Theorem 6.1.** Let \( \mathcal{A} \) be a finite structure with finite relational signature and a Maltsev polymorphism. Then \( \text{CSP}(\mathcal{A}) \) can be solved in polynomial time.

6.1 Examples

The most prominent class of structures with a Maltsev polymorphism comes from groups. For any group \( G \), the operation \( m \) given by \((x, y, z) \mapsto x + y^{-1} + z \) is obviously Maltsev. Note that if the group \( G \) is \( F = (\mathbb{Z}_p; +, 0) \) then the \( k \)-ary relations preserved by \( m \) are precisely the affine subspaces of \( F^k \) (with the same argument as given for Theorem 5.14 in the Boolean case). In this case one can use Gaussian elimination to solve \( \text{CSP}(\mathcal{A}) \). This approach can be extended to the case that \( G \) is finite abelian, but it is not clear how to extend this approach to, say, \( G = S_3 \) (the full symmetric group on three elements).

For general finite groups \( G \), and if all relations of \( \mathcal{A} \) are cosets \( gH := \{gh \mid h \in H\} \) of subgroups \( H \) of \( G^m \), then Feder and Vardi \[22\] showed how to solve \( \text{CSP}(\mathcal{A}) \) in polynomial time using a previously known algorithm to find generators for a group. We will not discuss this approach, but rather present the far more general algorithm of Bulatov and Dalmau which works for all finite structures preserved by a Maltsev polymorphism. First we have a look at two examples of Maltsev polymorphisms that do not come from groups in the way described above.

**Example 9.** On the domain \( \{0, 1, 2\} \), let \( m \) be a minority, and define \( m(x, y, z) = 2 \) whenever \(|\{x, y, z\}| = 3\). Note that \( m \) preserves the equivalence relation with the equivalence classes \( \{2\} \) and \( \{0, 1\} \). Also note that \( m \) preserves all relations of the form (for \( i \in \{0, 1\} \))
\[
\{(2, \ldots, 2)\} \cup \{(x_1, \ldots, x_n) \in \{0, 1\}^n \mid x_1 + x_2 + \cdots + x_n = i \mod 2\}.
\]

**Example 10.** On the domain \( \{0, 1, 2\} \), let \( m \) be a minority, and define \( m(x, y, z) = x \) whenever \(|\{x, y, z\}| = 3\). Then \( m \) preserves for every permutation \( \pi \) of \( \{0, 1, 2\} \) the relation \( \{(x, y) \mid \pi(x) = y\} \). Moreover, \( m \) preserves the binary relations \( R \) that are maximal with the property that \( |\text{pr}_1 R|, |\text{pr}_2 R| \leq 2 \).

**Exercises.**

55. Check the claims made in Example 9. Are all relations that are preserved by \( m \) primitive positive definable over the given relations?

56. Check the claims made in Example 10. Are all relations that are preserved by \( m \) primitive positive definable over the given relations?
57. Show that if a Maltsev operation $m$ preserves the graph of a Maltsev operation $m'$ on the same domain, then $m = m'$.

6.2 Compact Representations of Relations

Our presentation of the proof closely follows that of Bulatov and Dalmau [14].

**Definition 6.2** (Forks and Representations). Let $R \subseteq A^n$ be a relation.

- A fork of $R$ is a triple $(i, a, b)$ such that there exist $s, t \in R$ with $(s_1, \ldots, s_{i-1}) = (t_1, \ldots, t_{i-1})$, $s_i = a$, and $t_i = b$. We say that $s$ and $t$ witness $(i, a, b)$.

- $R' \subseteq R$ is called a representation of $R$ if every fork of $R$ is also a fork of $R'$.

- A representation $R'$ of $R$ is called compact if its cardinality is at most twice the number of forks of $R$.

Clearly, every relation has a compact representation. Let $R \subseteq A^n$. For $i_1, \ldots, i_n \in \{1, \ldots, n\}$, we write $\text{pr}_{i_1, \ldots, i_k}(R)$ for the $k$-ary relation on $A$ obtained as the projection of $R$ to the arguments $i_1, \ldots, i_k$. For $t = (t_1, \ldots, t_n)$, we also write $\text{pr}_{i_1, \ldots, i_k}(t)$ for the tuple $(t_{i_1}, \ldots, t_{i_k})$. For an operation $m: A^k \to A$ and a relation $R$ on $A$, we write $\langle R \rangle_m$ for the smallest relation that contains $R$ and is preserved by $m$.

**Lemma 6.3.** Let $A$ be a finite set and let $m: A^3 \to A$ be a Maltsev operation. Let $R \subseteq A^k$ be a relation preserved by $m$, and let $R'$ be a representation of $R$. Then $R = \langle R' \rangle_m$.

**Proof.** We show by induction on $i \in \{1, \ldots, n\}$ that $\text{pr}_{1, \ldots, i}(R') = \text{pr}_{1, \ldots, i}(R)$. Clearly, $\text{pr}_{1, \ldots, i}(R') \subseteq \text{pr}_{1, \ldots, i}(R)$, so we only need to show the converse inclusion. The case $i = 1$ follows from that fact that $R$ has for every $t \in R$ the fork $(1, t_1, t_1)$, and since $R'$ must also have this fork it must contain a tuple $t'$ such that $t'_1 = t_1$.

So let us assume that the statement holds for $i < n$. We have to show that for every $t \in R$ we have $(t_1, \ldots, t_{i+1}) \in \text{pr}_{1, \ldots, i+1}(R')$. By induction hypothesis there exists a tuple $s \in \langle R \rangle_m$ such that $(s_1, \ldots, s_i) = (t_1, \ldots, t_i)$. Then $(i + 1, s_{i+1}, t_{i+1})$ is a fork of $R$, so there exist tuples $s', s'' \in R'$ witnessing it. Then the tuple $t' := m(s, s', s'') \in \langle R' \rangle_m$ is such that

$$(t'_1, \ldots, t'_t, t'_{i+1}) = (m(t_1, s'_1, s''_1), \ldots, m(t_i, s'_i, s''_i), m(s_{i+1}, s_{i+1}, t_{i+1}))$$

$$= (t_1, \ldots, t_i, t_{i+1})$$

(since $s'_i = s''_i$).

Hence, $(t_1, \ldots, t_i, t_{i+1})$ is a tuple from $\text{pr}_{1, \ldots, i+1}(R')$, as required. 

**Exercises.**

58. Let $A$ be a finite set. How many forks does the full $n$-ary relation $A^n$ have? Explicitly construct a compact representation for $A^n$.

59. Let $R$ be the relation $\{(x, y, z, u) \in \{0, 1\}^4 \mid x + y + z = 1 \mod 2\}$. Find a smallest possible representation $R'$ for $R$. Explicitly compute $\langle R' \rangle_m$ where $m$ is the Boolean minority.
6.3 The Bulatov-Dalmau Algorithm

Let \( \exists x_1, \ldots, x_n (\varphi_1 \land \cdots \land \varphi_m) \) be an instance of CSP(\( \mathfrak{A} \)). For \( \ell \leq n \), we write \( R_\ell \) for the relation

\[ \{ (s_1, \ldots, s_n) \in A^n \mid \mathfrak{A} \models (\varphi_1 \land \cdots \land \varphi_\ell)(s_1, \ldots, s_n) \}. \]

The idea of the algorithm is to inductively construct a compact representation \( R'_\ell \) of \( R_\ell \), adding constraints one by one. Initially, for \( \ell = 0 \), we have \( R_0 = A^n \), and it is easy to come up with a compact representation for this relation. Note that when we manage to compute the compact representation \( R'_n \) for \( R_n \), we can decide satisfiability of the instance: it is unsatisfiable if and only if \( R'_n \) is empty. For the inductive step, we need a procedure called \textit{Next} which is more involved; we first introduce two auxiliary procedures.

The procedure \textit{Nonempty}

The procedure \textit{Nonempty} receives as input

\begin{itemize}
  \item a compact representation \( R' \) of a relation \( R \),
  \item a sequence \( i_1, \ldots, i_k \) of elements in \([n]\) where \( n \) is the arity of \( R \), and
  \item a \( k \)-ary relation \( S \) which is also preserved by \( m \).
\end{itemize}

The output of the procedure is either a tuple \( t \in R \) such that \( (t_{i_1}, \ldots, t_{i_k}) \in S \), or ‘No’ if no such tuple exists. The procedure can be found in Figure 6. For its correctness we note the following:

\begin{itemize}
  \item \( R' \subseteq U \subseteq R \): initially we start from \( U := R' \subseteq R \), and only add tuples to \( U \) obtained by applying \( m \) to tuples in \( U \), so the added tuples are again in \( R \).
  \item It follows that if \textit{Nonempty} returns a tuple \( (t_{i_1}, \ldots, t_{i_k}) \), then this tuple is indeed from \( \text{pr}_{i_1, \ldots, i_k} R \) and the output of the algorithm is correct.
  \item When the algorithm exits the while loop then \( \text{pr}_{i_1, \ldots, i_k} (U)_m = \text{pr}_{i_1, \ldots, i_k} U \). Since \( R' \subseteq U \) we have that \( (U)_m = R \). Hence, every tuple \( t \in \text{pr}_{i_1, \ldots, i_k} R = \text{pr}_{i_1, \ldots, i_k} (U)_m \) is contained in \( \text{pr}_{i_1, \ldots, i_k} U \), and so the answer of the algorithm is also correct when it returns ‘No’.
\end{itemize}

We mention that this procedure does not use the particular properties of a Maltsev polymorphism, but works for any explicitly given polymorphism.
Procedure \textit{Fix-values}(R', c_1, \ldots, c_k).

Set $j := 0$; $U_j := R'$.
While $j < k$ do:
    Set $U_{j+1} := \emptyset$.
    For each $(i, a, b) \in [n] \times A^2$:
        If $\exists s, t \in U_j$ witnessing $(i, a, b)$ (assuming $s = t$ if $a = b$):
            If $r := \text{Nonempty}(U_j, j+1, i, \{(c_{j+1}, a)\}) \neq \text{‘No’}$
                If ($i > j + 1$) or ($a = b = c_i$):
                    Set $U_{j+1} := U_{j+1} \cup \{r, m(r, s, t)\}$
    Set $j := j + 1$.
Return $U_k$.

Figure 7: The procedure \textit{Fix-values}.

\textbf{Running time.} The number of iterations of the while loop can be bounded by the size $|U|$ of the set $U$ at the end of the execution of the procedure. Hence, when we want to use this procedure to obtain a polynomial-time running time, we have to make sure that the size of $U$ remains polynomial in the input size. The way this is done in the Bulatov-Dalmau algorithm is to guarantee that at each call of $\text{Nonempty}$ the size $L$ of $pr_{i_1, \ldots, i_k} R$ is polynomial in the input size. Then $|U|$ is bounded by $L + |R'|$ which is also polynomial.

We have to test all tuples $r, s, t \in U$; this can be implemented so that $|U|^3$ steps suffice. In each step we have to compute $m(r, s, t)$ and test whether $pr_{i_1, \ldots, i_k} m(r, s, t) \in pr_{i_1, \ldots, i_k} U$, which can be done in $O(kL)$. In the important case that $L$ is bounded by a constant in the size of the input $N$, the running time of $\text{Nonempty}$ is in $O(N^4)$.

\textbf{The procedure \textit{Fix-values}}

The procedure \textit{Fix-values} receives as input

- a compact representation $R'$ of an $n$-ary relation $R$ preserved by $m$, and
- a sequence $c_1, \ldots, c_k \in A$ for $k \leq n$.

The output of \textit{Fix-values} is a compact representation of the relation

$$R \cap (\{c_1\} \times \cdots \times \{c_k\} \times A \times \cdots \times A).$$

The procedure can be found in Figure 7. The algorithm computes inductively a compact representation $U_j$ of the relation

$$R_j = R \cap (\{c_1\} \times \cdots \times \{c_j\} \times A \times \cdots \times A)$$

This is immediate for $U_0 = R'$, and the set $U_k$ is the relation that we have to compute.

For its correctness, suppose inductively that $U_j$ is a compact representation of $R_j$. We have to show that the set $U_{j+1}$ computed by the procedure is a compact representation of $R_{j+1}$:
1. \(U_{j+1} \subseteq R_{j+1}\). Suppose that the procedure adds \(\{r, m(r, s, t)\}\) to \(U_{j+1}\), where \(r\) and \(s\) witness the fork \((i, a, b)\) of \(U_j\) processed in the for-loop of the procedure. Note that \(r \in R_{j+1}\) since \(r \in U_j \subseteq R_j\) and \(r_{j+1} = c_{j+1}\). Since \(m\) preserves \(R\) and is idempotent, it also preserves \(R_j\), and since \(r, s, t \in R_j\) it follows that \(m(r, s, t) \in R_j\). To show that \(m(r, s, t) \in R_{j+1}\) it suffices to show that \(s_{j+1} = t_{j+1}\) because then \(m(r, s, t)_{j+1} = r_{j+1} = c_{j+1}\) since \(m\) is Maltsev. If \(i > j + 1\) then we have that \(s_{j+1} = t_{j+1}\) since \(s, t\) witness \((i, a, b)\). Otherwise, we must have \(a = b = c_i\) because of the innermost if-clause of the procedure. But then \(s = t\) by the stipulation of the algorithm on the choice of \(s\) and \(t\).

2. All forks \((i, a, b)\) of \(R_{j+1}\) are forks of \(U_{j+1}\). If \(R_{j+1}\) has the fork \((i, a, b)\), then by inductive assumption \(U_j\) must contain witnesses \(s, t\) for \((i, a, b)\). Therefore, the first if-clause of the procedure is positive. Moreover, \(s_{j+1} = c_{j+1}\) and \(s_i = a\), so \(r := \text{Nonempty}(U_j, j + 1, i, \{(c_{j+1}, a)\}) \neq \text{`No'}\). Also note that if \(i \leq j + 1\), then \(a = s_i = c_i = t_i = b\). So all the if-clauses of the procedure are positive, and the procedure adds \(r\) and \(m(r, s, t)\) to \(U_{j+1}\). The tuples \(r\) and \(m(r, s, t)\) witness \((i, a, b)\). Since \(s, t\) witness \((i, a, b)\) we have that \((s_1, \ldots, s_{i-1}) = (t_1, \ldots, t_{i-1})\). Hence, \(\text{pr}_1, \ldots, \text{pr}_{i-1}(m(r, s, t)) = (r_1, \ldots, r_{i-1})\). Furthermore, we have that \(\text{pr}_i(m(r, s, t)) = m(a, a, b) = b\).

3. The representation \(U_{j+1}\) of \(R_{j+1}\) is compact since at most two tuples are added to \(U_{j+1}\) for each fork of \(R_{j+1}\).

**Running time.** The while loop is performed \(k \leq n\) times; the inner for-loop is executed for each \((i, a, b) \in [n] \times A^2\), which is linear for fixed \(A\). The cost of each iteration is dominated by the cost of calling the procedure \(\text{Nonempty}\). Note that when calling \(\text{Nonempty}\), the size of \(\text{pr}_{j+1, i} U_j\) is polynomial in the input size (even constant size when \(A\) is fixed), so the cost of \(\text{Nonempty}\) is in \(O(N^4)\) where \(N\) is the size of the input. Therefore, the total time complexity of the procedure \(\text{Fix-values}\) is polynomial in the input size (for fixed \(A\) it is in \(O(N^5)\)).

**The procedure Next**

Now comes the heart of the algorithm, which is the procedure \(\text{Next}\) that updates a compact representation of the solution space when constraints are added one by one. The input of the procedure is

- a compact representation \(R'\) of a relation \(R \subseteq A^n\) that is preserved by \(m\),
- a sequence \(i_1, \ldots, i_k\) of elements from \([n]\),
- a \(k\)-ary relation \(S\) which is also preserved by \(m\).

The output of the procedure is a compact representation of the relation

\[
R^* := \{ t \in R \mid (t_{i_1}, \ldots, t_{i_k}) \in S \}.
\]

The procedure \(\text{Next}\) can be found in Figure 8. Observe that

- the condition \(\text{Nonempty}(R', i_1, \ldots, i_k, i, S \times \{a\}) \neq \text{`No'}\) from the first if-clause is satisfied if and only if there exists a tuple \(t \in R\) such that \((t_{i_1}, \ldots, t_{i_k}) \in S\) and \(t_i = a\).

Hence, if such a tuple does not exist, then \((i, a, b)\) cannot be a fork of \(R^*\), and nothing needs to be done.
Procedure \textit{Next}(R', i_1, \ldots, i_k, S).

Set \( U := \emptyset \).

For each \((i, a, b) \in [n] \times A^2:\)

If \( \text{Nonempty}(R', i_1, \ldots, i_k, i, S \times \{a\}) =: t \neq 'No': \)

If \( \text{Nonempty}(\text{Fix-values}(R', t_1, \ldots, t_{i-1}), i_1, \ldots, i_k, i, S \times \{b\}) =: t' \neq 'No': \)

Set \( U := U \cup \{t, t'\} \).

Return \( U_k \).

Figure 8: The procedure \textit{Next}.

- the condition \( \text{Nonempty}(\text{Fix-values}(R', t_1, \ldots, t_{i-1}), i_1, \ldots, i_k, i, S \times \{b\}) \neq 'No' \) from the second if-clause is satisfied if and only if there exists a tuple \( t' \in R \) such that
  - \( (t'_1, \ldots, t'_{i-1}) = (t_1, \ldots, t_{i-1}) \),
  - \( (t'_1, \ldots, t'_{i_k}) \in S \), and
  - \( t'_i = b \).

If this condition holds, and since \( t_i = a \), we have that \( t \) and \( t' \) witness \((i, a, b)\). It only remains to show that if \((i, a, b)\) is a fork of \( R^* \), then such a tuple \( t' \) must exist. So let \( r \) and \( s \) be witnesses for \((i, a, b)\) in \( R^* \). Then the tuple \( t' := m(t, r, s) \) has the desired properties:

- for \( j < i \) we have that \( t'_j = m(t_j, r_j, s_j) = t_j \);
- \( t' \in S \) because \((r_{i_1}, \ldots, r_{i_k}), (s_{i_1}, \ldots, s_{i_k}), (t_{i_1}, \ldots, t_{i_k}) \in S \) and \( m \) preserves \( S \);
- \( t'_i = m(t_i, r_i, s_i) = m(a, a, b) = b \).

- The cardinality of \( U \) is bounded by twice the number of forks of \( R^* \), so the representation computed by the algorithm is compact.

**Running time.** The for-loop of the procedure \textit{Next} is performed \( n|A|^2 \) times and the cost of each iteration is polynomial in the cost of \( \text{Nonempty} \) and \( \text{Fix-values} \). Also note that \( k \) is bounded by the maximal arity of the relations in \( A \), so constant for fixed \( A \). It follows that \( \text{pr}_{i_1, \ldots, i_k}(R) \) is polynomial, so the running time of the calls to \( \text{Nonempty} \) are polynomial. For fixed \( A \), the global running time of the procedure \textit{Next} is in \( O(N^6) \) where \( N \) is the size of the input.

**Proof of Theorem 6.1.** Starting from an empty list of constraints, we add constraints on the variables \( x_1, \ldots, x_n \) one by one, and maintain a compact representation of the \( n \)-ary relation defined by the constraints considered so far. Initially, we start with a compact representation of the full relation \( A^n \). In later steps, we use the procedure \textit{Next} to compute a compact representation when a constraint is added, in \( O(N^6) \) for fixed \( A \) and \( N \) the size of the input. The instance is unsatisfiable if and only if at the final stage we end up with an empty representation. The entire running time of the algorithm is in \( O(N^7) \).
Exercises.

60. Let \( \mathfrak{A} \) be the structure \((\{0, 1\}; L_0, L_1)\) where \( L_i := \{(x, y, z) \mid x + y + z = i \mod 2\} \), which has the Boolean minority \( m \) as polymorphism. Consider the instance

\[
\exists x_1, \ldots, x_5 \left( L_1(x_1, x_2, x_3) \land L_1(x_2, x_3, x_4) \land L_1(x_3, x_4, x_5) \land L_0(x_1, x_3, x_5) \right)
\]

Compute compact representations \( R_\ell' \) of \( R_\ell \), for \( \ell \in \{1, 2, 3, 4\} \).

61. \((\ast)\) Let \( \mathfrak{B} \) be a structure with a Maltsev polymorphism \( f \) and an infinite relational signature. Note that we have defined CSP\((\mathfrak{B})\) only if \( \mathfrak{B} \) has a finite signature. If we want to define CSP\((\mathfrak{B})\) also for structures \( \mathfrak{B} \) with an infinite signature, it is important to discuss how the relation symbols in the signature of \( \mathfrak{B} \) are represented in the input. We choose to represent a relation symbol \( R \) from \( \mathfrak{B} \) by listing the tuples in \( R^\mathfrak{B} \). Adapt the Dalmau algorithm such that it can solve CSP\((\mathfrak{B})\) in polynomial time for this choice of representing the relations in \( \mathfrak{B} \).

62. \((\ast)\) The graph isomorphism problem (GI) is a famous computational problem that is neither known to be solvable in polynomial time, nor expected to be NP-hard. An instance of GI consists of two graphs \( G \) and \( H \), and the question is to decide whether \( G \) and \( H \) are isomorphic. Consider the variant of the graph-isomorphism problem where the vertices are coloured, each color appears at most \( k \) times for some constant \( k \), and the isomorphism between \( H \) and \( G \) that we are looking for is required to additionally preserve the colours. Show that this problem can be solved in polynomial time using Dalmau’s algorithm (use the previous exercise).

7 Universal Algebra

7.1 Algebras and Clones

In universal algebra, an algebra is simply a structure with a purely functional signature.

The clone of an algebra. Algebras give rise to clones in the following way. When \( \mathbf{A} \) is an algebra with signature \( \tau \) (also called \( \tau \)-algebra) and domain \( A \), we denote by \( \text{Clo}(\mathbf{A}) \) the set of all term functions of \( \mathbf{A} \), that is, functions with domain \( A \) of the form \((x_1, \ldots, x_n) \mapsto t(x_1, \ldots, x_n)\) where \( t \) is any term over the signature \( \tau \) whose set of variables is contained in \( \{x_1, \ldots, x_n\} \). Clearly, \( \text{Clo}(\mathbf{A}) \) is a function clone since it is closed under compositions, and contains the projections.

Polymorphism algebras. In the context of complexity classification of CSPs, algebras arise as follows.

Definition 7.1. Let \( \mathfrak{B} \) be a structure with domain \( B \). An algebra \( \mathbf{B} \) with domain \( B \) such that \( \text{Clo}(\mathbf{B}) = \text{Pol}(\mathfrak{B}) \) is called a polymorphism algebra of \( \mathfrak{B} \).

Note that the signature of a polymorphism algebra is always infinite, since we have polymorphisms of arbitrary finite arity. Also note that a structure \( \mathfrak{B} \) has many different polymorphism algebras, since Definition 7.1 does not prescribe how to assign function symbols to the polymorphisms of \( \mathfrak{B} \).
Any clone \( \mathcal{C} \) on a set \( D \) can be viewed as an algebra \( \mathfrak{A} \) with domain \( D \) whose signature consists of the operations of \( \mathcal{C} \) themselves; that is, when \( f \in \mathcal{C} \), then \( f^\mathfrak{A} := f \). Hence, we are allowed to use concepts that will be defined for algebras also for clones. In particular, the polymorphism clone \( \text{Pol}(\mathfrak{B}) \) of a structure \( \mathfrak{B} \) might be viewed as an algebra, to which we refer to as the polymorphism algebra of \( \mathfrak{B} \).

### 7.2 Subalgebras, Products, Homomorphic Images

In this section we recall some basic universal-algebraic facts that will be used in the following subsections.

**Subalgebras.** Let \( \mathfrak{A} \) be a \( \tau \)-algebra with domain \( A \). A subalgebra of \( \mathfrak{A} \) is a \( \tau \)-algebra \( \mathfrak{B} \) with domain \( B \subseteq A \) such that for each \( f \in \tau \) of arity \( k \) we have \( f^\mathfrak{B}(b_1, \ldots, b_k) = f^\mathfrak{A}(b_1, \ldots, b_k) \) for all \( b_1, \ldots, b_k \in B \).

**Products.** Let \( \mathfrak{A}, \mathfrak{B} \) be \( \tau \)-algebras with domain \( A \) and \( B \), respectively. Then the product \( \mathfrak{A} \times \mathfrak{B} \) is the \( \tau \)-algebra with domain \( A \times B \) such that for each \( f \in \tau \) of arity \( k \) we have \( f^{\mathfrak{A} \times \mathfrak{B}}((a_1, b_1), \ldots, (a_k, b_k)) = (f^\mathfrak{A}(a_1, \ldots, a_k), f^\mathfrak{B}(b_1, \ldots, b_k)) \) for all \( a_1, \ldots, a_k \in A \) and \( b_1, \ldots, b_k \in B \). More generally, when \( (\mathfrak{A}_i)_{i \in I} \) is a sequence of \( \tau \)-algebras, indexed by some set \( I \), then \( \prod_{i \in I} \mathfrak{A}_i \) is the \( \tau \)-algebra \( \mathfrak{A} \) with domain \( A^I \) such that \( f^\mathfrak{A}((a^I_1), \ldots, (a^I_k)) \) for all \( a^I_1, \ldots, a^I_k \in A_i \).

**Lemma 7.2.** Let \( \mathfrak{A} \) be the polymorphism algebra of a finite structure \( \mathfrak{A} \). Then the (domains of the) subalgebras of \( \mathfrak{A}^k \) are precisely the relations that have a primitive positive definition in \( \mathfrak{A} \).

**Proof.** A relation \( R \subseteq A^k \) is a subalgebra of \( \mathfrak{A}^k \) if and only if for all \( m \)-ary \( f \) in the signature of \( \mathfrak{A} \) and \( t_1, \ldots, t_m \in R \), we have \( (f(t_1^1, \ldots, t_m^1), \ldots, f(t_1^k, \ldots, t_m^k)) \in R \), which is the case if and only if \( R \) is preserved by all polymorphisms of \( \mathfrak{A} \), which is the case if and only if \( R \) is primitive positive definable in \( \mathfrak{A} \) by Theorem 5.2.

**Homomorphic Images.** Let \( \mathfrak{A} \) and \( \mathfrak{B} \) be \( \tau \)-algebras. Then a homomorphism from \( \mathfrak{A} \) to \( \mathfrak{B} \) is a mapping \( h: A \rightarrow B \) such that for all \( k \)-ary \( f \in \tau \) and \( a_1, \ldots, a_k \in A \) we have

\[
h(f^\mathfrak{A}(a_1, \ldots, a_k)) = f^\mathfrak{B}(h(a_1), \ldots, h(a_k)).
\]

When \( g: C \rightarrow D \) is a map, then the kernel of \( g \) is the equivalence relation \( E \) on \( C \) where \( (c, c') \in E \) if \( g(c) = g(c') \). For \( c \in C \), we denote by \( c/E \) the equivalence class of \( c \) in \( E \), and by \( C/E \) the set of all equivalence classes of elements of \( C \).

**Definition 7.3.** A congruence of an algebra \( \mathfrak{A} \) is an equivalence relation that is preserved by all operations in \( \mathfrak{A} \).

**Lemma 7.4.** Let \( \mathfrak{B} \) be a finite structure, and \( \mathfrak{B} \) be a polymorphism algebra of \( \mathfrak{B} \). Then the congruences of \( \mathfrak{B} \) are exactly the primitive positive definable equivalence relations over \( \mathfrak{B} \).

**Proof.** A direct consequence of theorem 5.2.

**Proposition 7.5 (see [16]).** Let \( \mathfrak{A} \) be an algebra. Then \( E \) is a congruence of \( \mathfrak{A} \) if and only if \( E \) is the kernel of a homomorphism from \( \mathfrak{A} \) to some other algebra \( \mathfrak{B} \).
Example 11. Let $G = (V, E)$ be the undirected graph with $V = \{a_1, \ldots, a_4, b_1, \ldots, b_4\}$ such that $a_1, \ldots, a_4$ and $b_1, \ldots, b_4$ induce a clique, for each $i \in \{1, \ldots, 4\}$ there is an edge between $a_i$ and $b_i$, and otherwise there are no edges in $G$. Let $A$ be a polymorphism algebra of $G$. Then $A$ homomorphically maps to a two-element algebra $B$. Why?

By Proposition 7.5, it suffices to show that $A$ has a congruence with two equivalence classes. By Lemma 7.4, it suffices to show that an equivalence relation of index two is primitive positive definable. Here is the primitive positive definition:

$$\exists u, v \left( E(x, u) \land E(y, u) \land E(x, v) \land E(y, v) \land E(u, v) \right)$$

The equivalence classes of this relation are precisely $\{a_1, \ldots, a_4\}$ and $\{b_1, \ldots, b_4\}$.

Example 12. Let $A$ be the algebra with domain $A := S_3 = \{ \text{id}, (231), (312), (12), (23), (13) \}$ (the symmetric group on three elements), and a single binary operation, the composition function of permutations. Note that $A$ has the subalgebra induced by $\{ \text{id}, (231), (312) \}$. Also note that $A$ homomorphically maps to $(\{0,1\}, +)$ where $+$ is addition modulo 2: the preimage of 0 is $\{\text{id}, (231), (312)\}$ and the preimage of 1 is $\{(12), (23), (13)\}$.

When $A$ is a $\tau$-algebra, and $h: A \to B$ is a mapping such that the kernel of $h$ is a congruence of $A$, we define the quotient algebra $A/h$ of $A$ under $h$ to be the algebra with domain $h(A)$ where

$$f^{A/h}(h(a_1), \ldots, h(a_k)) = h(f^A(a_1, \ldots, a_k))$$

where $a_1, \ldots, a_k \in A$ and $f \in \tau$ is $k$-ary. This is well-defined since the kernel of $h$ is preserved by all operations of $A$. Note that $h$ is a surjective homomorphism from $A$ to $A/h$.

The following is well known (see e.g. Theorem 6.3 in [16]).

Lemma 7.6. Let $A$ and $B$ be algebras with the same signature, and let $h: A \to B$ be a homomorphism. Then the image of any subalgebra $A'$ of $A$ under $h$ is a subalgebra of $B$, and the preimage of any subalgebra $B'$ of $B$ under $h$ is a subalgebra of $A$.

Proof. Let $f \in \tau$ be $k$-ary. Then for all $a_1, \ldots, a_k \in A'$,

$$f^B(h(a_1), \ldots, h(a_k)) = h(f^A(a_1, \ldots, a_k)) \in h(A'),$$

so $h(A')$ is a subalgebra of $C$. Now suppose that $h(a_1), \ldots, h(a_k)$ are elements of $B'$; then $f^B(h(a_1), \ldots, h(a_k)) \in B'$ and hence $h(f^A(a_1, \ldots, a_k)) \in B'$. So, $f^A(a_1, \ldots, a_k) \in h^{-1}(B')$ which shows that $h^{-1}(B')$ induces a subalgebra of $A$. □

7.3 Varieties and Pseudovarieties.

When $\mathcal{K}$ is a class of algebras of the same signature, then

- $\text{P}(\mathcal{K})$ denotes the class of all products of algebras from $\mathcal{K}$.
- $\text{P}^\text{fin}(\mathcal{K})$ denotes the class of all finite products of algebras from $\mathcal{K}$.
- $\text{S}(\mathcal{K})$ denotes the class of all subalgebras of algebras from $\mathcal{K}$.
- $\text{H}(\mathcal{K})$ denotes the class of all homomorphic images of algebras from $\mathcal{K}$.
Note that closure under homomorphic images implies in particular closure under isomorphism. For the operators $P, P^{\text{fin}}, S$ and $H$ we often omit the brackets when applying them to single algebras, i.e., we write $H(A)$ instead of $H(\{A\})$. The elements of $\text{HS}(A)$ are also called the factors of $A$.

A class $\mathcal{V}$ of algebras with the same signature $\tau$ is called a pseudovariety if $\mathcal{V}$ contains all homomorphic images, subalgebras, and direct products of algebras in $\mathcal{V}$, i.e., $H(\mathcal{V}) = S(\mathcal{V}) = P^{\text{fin}}(\mathcal{V}) = \mathcal{V}$. The class $\mathcal{V}$ is called a variety if $\mathcal{V}$ also contains all (finite and infinite) products of algebras in $\mathcal{V}$. So the only difference between pseudovarieties and varieties is that pseudovarieties need not be closed under direct products of infinite cardinality. The smallest pseudovariety (variety) that contains an algebra $A$ is called the pseudovariety (variety) generated by $A$.

**Lemma 7.7 (HSP lemma).** Let $A$ be an algebra.

- The pseudovariety generated by $A$ equals $\text{HSP}^{\text{fin}}(A)$.
- The variety generated by $A$ equals $\text{HSP}(A)$.

**Proof.** Clearly, $\text{HSP}^{\text{fin}}(A)$ is contained in the pseudovariety generated by $A$, and $\text{HSP}(A)$ is contained in the variety generated by $A$. For the converse inclusion, it suffices to verify that $\text{HSP}^{\text{fin}}(A)$ is closed under $H$, $S$, and $P^{\text{fin}}$. It is clear that $H(\text{HSP}^{\text{fin}}(A)) = \text{HSP}^{\text{fin}}(A)$. The second part of Lemma 7.6 implies that $S(\text{HSP}^{\text{fin}}(A)) \subseteq \text{HS}(\text{SP}^{\text{fin}}(A)) = \text{HSP}^{\text{fin}}(A)$. Finally, $P^{\text{fin}}(\text{HSP}^{\text{fin}}(A)) \subseteq H P^{\text{fin}} S P^{\text{fin}}(A) \subseteq H S P^{\text{fin}}(A) = \text{HSP}^{\text{fin}}(A)$.

The proof that $\text{HSP}(A)$ is closed under $H$, $S$, and $P$ is analogous.

**Exercises.**

63. Show that the operators $HS$ and $SH$ are distinct.

64. Show that the operators $SP$ and $PS$ are distinct.

### 7.4 Pseudovarieties and Primitive Positive Interpretations

**Theorem 7.8.** Let $\mathcal{C}$ be a finite structure with polymorphism algebra $C$. Then $\mathcal{B} \in \text{PP}(\mathcal{C})$ if and only if there exists $B \in \text{HSP}^{\text{fin}}(\mathcal{C})$ such that $\text{Clo}(B) \subseteq \text{Pol}(\mathcal{B})$.

**Proof.** We only prove the ‘if’ part of the statement here; the proof of the ‘only if’ part is similarly easy. There exists a finite number $d \geq 1$, a subalgebra $D$ of $C^d$, and a surjective homomorphism $h$ from $D$ to $B$. We claim that $\mathcal{B}$ has a first-order interpretation $I$ of dimension $d$ in $\mathcal{C}$. All operations of $\mathcal{C}$ preserve $D$ (viewed as a $d$-ary relation over $\mathcal{C}$), since $D$ is a subalgebra of $C^d$. By Theorem 5.2, this implies that $D$ has a primitive positive definition $\delta(x_1, \ldots, x_d)$ in $\mathcal{C}$, which becomes the domain formula $\delta_I$ of $I$. As coordinate map we choose the mapping $h$. Let $f \in \tau$ be arbitrary. By assumption, $f^B$ preserves $R$. It is easy to verify that then $f^C$ preserves $h^{-1}(R)$. Hence, all polymorphisms of $\mathcal{C}$ preserve $h^{-1}(R)$, and the relation $h^{-1}(R)$ has a primitive positive definition in $\mathcal{C}$ (Theorem 5.2), which becomes the defining formula for $\overline{R}(x_1, \ldots, x_k)$ in $I$. Finally, since $h$ is an algebra homomorphism, the kernel $K$ of $h$ is a congruence of $D$. It follows that $K$, viewed as a $2d$-ary relation over $\mathcal{C}$, is preserved by all operations from $\mathcal{C}$. Theorem 5.2 implies that $K$ has a primitive positive definition in $\mathcal{C}$. This definition becomes the formula $=_I$. It is straightforward to verify that $I$ is a primitive positive interpretation of $\mathcal{B}$ in $\mathcal{C}$. 

\[\square\]
7.5 Birkhoff’s Theorem

Varieties (which have been defined in Section 7.2) are a fascinatingly powerful concept to study classes of algebras. The central theorem for the study of varieties is Birkhoff’s HSP theorem, which links varieties with universal conjunctive theories. By Birkhoff’s theorem, there is also a close relationship between varieties and the concept of an abstract clone, as we will see in Section 7.6. We present it here only for varieties generated by a single finite algebra.

A sentence in a functional signature is called an identity if it is of the form

$$\forall x_1, \ldots, x_n. s = t$$

where $s$ and $t$ are $\tau$-terms.

**Theorem 7.9** (Birkhoff [9]; see e.g. [30] or [16]). Let $\tau$ be a functional signature, and $A$ and $B$ finite algebras with signature $\tau$. Then the following are equivalent.

1. All identities that hold in $B$ also hold in $A$;
2. $A \in \operatorname{HSP}^{\text{fin}}(B)$;
3. $A \in \operatorname{HSP}(B)$;

**Proof.** Trivially, 2. implies 3. To show that 3. implies 1., let $\phi = \forall x_1, \ldots, x_n. s = t$ be an identity that holds in $B$. Then $\phi$ is preserved in powers $A = B^I$ of $B$. To see this, let $a_1, \ldots, a_n \in A$ be arbitrary. Since $B \models \phi$ we have $s^B(a_1[j], \ldots, a_n[j]) = t^B(a_1[j], \ldots, a_n[j])$ for all $j \in I$, and thus $s^A(a_1, \ldots, a_n) = t^A(a_1, \ldots, a_n)$ by the definition of products. Since $a_1, \ldots, a_n$ were chosen arbitrarily, we have $A \models \phi$. Moreover, $\phi$ is true in subalgebras of algebras that satisfy $\phi$ (this is true for universal sentences in general). Finally, suppose that $B$ is an algebra that satisfies $\phi$, and $\mu$ is a surjective homomorphism from $B$ to some algebra $A$. Let $a_1, \ldots, a_n \in A$; by surjectivity of $\mu$ we can choose $b_1, \ldots, b_n$ such that $\mu(b_i) = a_i$ for all $i \leq n$. Then

$$s^B(b_1, \ldots, b_n) = t^B(b_1, \ldots, b_n) \Rightarrow \mu(s^B(b_1, \ldots, b_n)) = \mu(t^B(b_1, \ldots, b_n))$$

$$\Rightarrow t^A(\mu(b_1), \ldots, \mu(b_n)) = s^A(\mu(b_1), \ldots, \mu(b_n))$$

$$\Rightarrow t^A(a_1, \ldots, a_n) = s^A(a_1, \ldots, a_n).$$

1. implies 2.: Let $a_1, \ldots, a_k$ be the elements of $A$, define $m := |B|^k$, and let $C$ be $B^k$. Let $c_1^1, \ldots, c_m^m$ be the elements of $C$; write $c_i$ for $(c_1^i, \ldots, c_m^i)$. Let $S$ be the smallest subalgebra of $B^m$ that contains $c_1, \ldots, c_k$; so the elements of $S$ are precisely those of the form $t^{B^m}(c_1, \ldots, c_k)$, for a $k$-ary $\tau$-term $t$. Define $\mu: S \to B$ by

$$\mu(t^{B^m}(c_1, \ldots, c_k)) := t^A(a_1, \ldots, a_k).$$

**Claim 1:** $\mu$ is well-defined. Suppose that $t^{B^m}(c_1, \ldots, c_k) = s^{B^m}(c_1, \ldots, c_k)$; then $t^B = s^B$ by the choice of $S$, and by assumption we have $t^A(b_1, \ldots, b_k) = s^A(b_1, \ldots, b_k)$.

**Claim 2:** $\mu$ is surjective. For all $i \leq k$, the element $c_i$ is mapped to $a_i$. 55
Claim 3: $\mu$ is a homomorphism from $S$ to $A$. Let $f \in \tau$ be of arity $n$ and let $s_1, \ldots, s_m \in S$. For $i \leq n$, write $s_i = t_s^S(c_1, \ldots, c_k)$ for some $\tau$-term $t$. Then
\[
\mu(f^S(s_1, \ldots, s_n)) = \mu(f(t_s^S(c_1, \ldots, c_k), \ldots, t_n^S(c_1, \ldots, c_k))) \\
= \mu(f(t_1^S, \ldots, t_n^S)(c_1, \ldots, c_k)) \\
= \mu((f(t_1, \ldots, t_n))^S(c_1, \ldots, c_k)) \\
= (f(t_1, \ldots, t_n))^A(a_1, \ldots, a_k) \\
= f^A(t_1^A(a_1, \ldots, a_k), \ldots, t_n^A(a_1, \ldots, a_k)) \\
= f^A(\mu(s_1), \ldots, \mu(s_n)).
\]
Therefore, $A$ is the homomorphic image of the subalgebra $S$ of $B^m$, and so $A \in \text{HSP}^{\text{fin}}(B)$.

Theorem 7.9 is important for analysing the constraint satisfaction problem for a structure $B$, since it can be used to transform the ‘negative’ statement of not interpreting certain finite structures into a ‘positive’ statement of having polymorphisms satisfying non-trivial identities: this will be the content of the following two sections.

7.6 (Abstract) Clones

Clones (in the literature often abstract clones) relate to function clones in the same way as (abstract) groups relate to permutation groups: the elements of a clone correspond to the functions of a function clone, and the signature contains composition symbols to code how functions compose. Since a function clone contains functions of various arities, a clone will be formalized as a multi-sorted structure, with a sort for each arity.

Definition 7.10. A clone $C$ is a multi-sorted structure with sorts $\{C^i \mid i \in \mathbb{N}\}$ and the signature $\{\pi_i^k \mid 1 \leq i \leq k\} \cup \{\text{comp}^k_l \mid k, l \geq 1\}$. The elements of the sort $C^k$ will be called the $k$-ary operations of $C$. We denote a clone by
\[
C = (C^0, C^1, \ldots; (\pi^k_i)_{1 \leq i \leq k}, (\text{comp}^k_l)_{k, l \geq 1})
\]
and require that $\pi^k_i$ is a constant in $C^k$, and that $\text{comp}^k_l : C^k \times (C^l)^k \rightarrow C^l$ is an operation of arity $k + 1$. Moreover, it holds that
\[
\text{comp}^k_l(f, \pi^k_1, \ldots, \pi^k_k) = f \quad (2) \\
\text{comp}^k_l(\pi^k_i, f_1, \ldots, f_k) = f_i \quad (3) \\
\text{comp}^k_l(f, \text{comp}^m_l(g_1, h_1, \ldots, h_m), \ldots, \text{comp}^m_l(g_k, h_1, \ldots, h_m)) = \\
\text{comp}^m_l(\text{comp}^m_l(f, g_1, \ldots, g_k), h_1, \ldots, h_m). \quad (4)
\]

The final equation generalises associativity in groups and monoids, and we therefore refer to it by associativity. We also write $f(g_1, \ldots, g_k)$ instead of $\text{comp}^k_l(f, g_1, \ldots, g_k)$ when $l$ is clear from the context. So associativity might be more readable as
\[
f(g_1(h_1, \ldots, h_m), \ldots, g_k(h_1, \ldots, h_m)) = f(g_1, \ldots, g_k)(h_1, \ldots, h_m).
\]

Every function clone $C$ gives rise to an abstract clone $C$ in the obvious way: $\pi^k_i \in C^k$ denotes the $k$-ary $i$-th projection in $C$, and $\text{comp}^k_l(f, g_1, \ldots, g_k) \in C^l$ denotes the composed function $(x_1, \ldots, x_l) \mapsto f(g_1(x_1, \ldots, x_l), \ldots, g_k(x_1, \ldots, x_l)) \in C$.
Example 13. $\forall x_1, x_2. f(x_1, x_2) = f(x_2, x_1)$ holds in an algebra $A$ if and only if

$$\text{Clo}(A) \models \text{comp}^2_2(f^A, \pi^2_1, \pi^2_2) = \text{comp}^2_2(f^A, \pi^2_2, \pi^2_1).$$

In the following, we will also use the term ‘abstract clone’ in situations where we want to stress that we are working with a clone and not with a function clone.

Definition 7.11. Let $C$ and $D$ be clones. A function $\xi : C \to D$ is called a (clone) homomorphism iff

- $\xi$ preserves arities of functions, i.e., $\xi(C^{(i)}) \subseteq D^{(i)}$ for all $i \in \mathbb{N}$;
- $\xi((\pi^k)^C) = (\pi^k)^D$ for all $1 \leq i \leq k$;
- $\xi(f(g_1, \ldots, g_n)) = \xi(f)(\xi(g_1), \ldots, \xi(g_n))$ for all $n, m \geq 1$, $f \in C^{(n)}$, and $g_1, \ldots, g_n \in C^{(m)}$.

Example 14. We write $\text{Proj}$ for the abstract clone of an algebra with at least two elements all of whose operations are projections; note that any such algebra has the same abstract clone (up to isomorphism), and that $\text{Proj}$ has a homomorphism into any other clone.

Example 15. All abstract clones of an algebra on a one-element are isomorphic, too, but of course not isomorphic to $\text{Proj}$. Any clone homomorphically maps to this trivial clone.

Proposition 7.12 (Formulation of Birkhoff’s theorem for clones). Let $C$ and $D$ be function clones on finite sets. Then the following are equivalent.

1. There is a surjective clone homomorphism from $C$ to $D$;
2. there are algebras $A$ and $B$ with the same signature $\tau$ such that $\text{Clo}(A) = D$, $\text{Clo}(B) = C$, and all universal conjunctive $\tau$-sentences that hold in $B$ also hold in $A$;
3. there are algebras $A$ and $B$ with the same signature such that $\text{Clo}(A) = D$, $\text{Clo}(B) = C$, and $A \in \text{HSP}^{\text{fin}}(B)$ (equivalently, $A \in \text{HSP}(B)$).

In the study of the complexity of CSPs, the equivalence between (1) and (3) in the above is the most relevant, since (3) is related to our most important tool to prove NP-hardness of CSPs (because of the link between pseudovarieties and primitive positive interpretations from Theorem 7.8), and since (1) is the universal-algebraic property that will be used in the following (see e.g. Theorem 7.17 below).

The following lemma is central for our applications of abstract clones when studying the complexity of CSPs.

Lemma 7.13. Let $C$ be a clone and let $F$ be the clone of a finite algebra such that there is no clone homomorphism from $C$ to $F$. Then there is a primitive positive sentence in the language $\tau$ of (abstract) clones that holds in $C$ but not in $F$.

Proof. Let $E$ be the expansion of $C$ by constant symbols such that every element $e$ of $E$ is named by a constant $c_e$. Let $V$ be the set of atomic sentences that hold in $E$. Let $U$ be the first-order theory of $F$. Suppose that $U \cup V$ has a model $M$. There might be elements in $M$ outside of $\bigcup_i M^{(i)}$. But the $\tau$-reduct of the restriction of $M$ to $\bigcup_i M^{(i)}$ must be isomorphic to $F$, since each of the $M^{(i)}$ is finite; we identify it with $F$. Note that for all constants $c_e$ we
have that \( c^M_e \in F \). Since \( M \) satisfies all atomic formulas that hold in \( E \), we have that the mapping \( e \mapsto c^M_e \), for \( e \) an element of \( E \), is a homomorphism from \( C \) to \( F \), in contradiction to our assumptions.

So \( U \cup V \) is unsatisfiable, and by compactness of first-order logic there exists a finite subset \( V' \) of \( V \) such that \( V \cup U \) is unsatisfiable. Replace each of the new constant symbols in \( V' \) by an existentially quantified variable; then the conjunction of the resulting sentences from \( V \) is a primitive positive sentence, and it must be false in \( F \).

7.7 Taylor Terms

The following goes back to Walter Taylor [49]. We slightly deviate from the historic definition in that we do not require idempotency – this allows us to give stronger formulations of several results in the following.

**Definition 7.14** (Taylor operations). A function \( f : B^n \to B \), for \( n \geq 2 \), is called a Taylor operation if for each \( 1 \leq i \leq n \) there are variables \( z_1, \ldots, z_n, z'_1, \ldots, z'_n \in \{x, y\} \) with \( z_i \neq z'_i \) such that for all \( x, y \in B \)

\[
f(z_1, \ldots, z_n) = f(z'_1, \ldots, z'_n).
\]

Examples for Taylor operations are binary commutative operations, majority operations, and Maltsev operations. We do not insist on idempotency for Taylor operations. Note that an \( n \)-ary operation \( f \) is Taylor if and only if it satisfies a set of \( n \) equations that can be written as

\[
\begin{array}{c}
\begin{pmatrix}
  x & \ldots & ? \\
  ? & \ldots & ? \\
  \vdots & \ddots & \vdots \\
  ? & \ldots & x
\end{pmatrix}
\end{array}
= \begin{array}{c}
\begin{pmatrix}
  y & \ldots & ? \\
  ? & \ldots & ? \\
  \vdots & \ddots & \vdots \\
  ? & \ldots & y
\end{pmatrix}
\end{array}
\]

where \( f \) is applied row-wise and \( ? \) stands for either \( x \) or \( y \).

**Definition 7.15** (Taylor terms). Let \( B \) be a \( \tau \)-algebra. A Taylor term of \( B \) is a \( \tau \)-term \( t(x_1, \ldots, x_n) \), for \( n \geq 2 \), such that \( t^B \) is a Taylor operation.

Note that a term \( t(x_1, \ldots, x_n) \) is a Taylor term in \( B \) if and only if \( \text{Clo}(B) \models \Phi_n(t^B) \), where \( \Phi_n(f) \) is the sentence

\[
\bigwedge_{i \leq n} \exists z, z' \in \{\pi_1^2, \pi_2^2\}^n (z_i \neq z'_i \land \text{comp}_2^n(f, z_1, \ldots, z_n) = \text{comp}_2^n(f, z'_1, \ldots, z'_n)) \tag{5}
\]

The following lemma is entirely obvious and I don’t know why the formal proof is so long, there must be a better way of presenting it (if giving a proof is necessary at all).

**Lemma 7.16.** \( \Phi_n(f) \) is equivalent to

\[
\bigwedge_{i \leq n} \exists v, v' \in \{\pi_1^n, \ldots, \pi_n^n\}^n (v_i \neq v'_i \land \text{comp}_n^n(f, v_1, \ldots, v_n) = \text{comp}_n^n(f, v'_1, \ldots, v'_n))
\]
Proof. Let \( i \in \{1, \ldots, n\} \) be arbitrary. Suppose that \( z, z' \in \{\pi_1^n, \pi_2^n\}^n \) are as in Equation 5. Then define \( v, v' \in \{\pi_1^n, \ldots, \pi_n^n\}^n \) as follows: if \( z_j = \pi_k^n \) for \( k \in \{1, 2\} \), then \( v_j := \pi_k^n \), and similarly if \( z'_j = \pi_k^n \) for \( k \in \{1, 2\} \), then \( v'_j := \pi_k^n \). Then \( v \) and \( v' \) witness that the formula given in the statement is true: \( z_i \neq z'_i \) implies that \( v_i \neq v'_i \). Moreover, \( \text{comp}_n^1(f, z_1, \ldots, z_i) = \text{comp}_n^1(f, z'_1, \ldots, z'_i) \) implies that

\[
\text{comp}_n^2(\text{comp}_n^2(f, z_1, \ldots, z_n), \pi_1^n, \pi_2^n) = \text{comp}_n^2(\text{comp}_n^2(f, z'_1, \ldots, z'_n), \pi_1^n, \pi_2^n)
\]

We compute

\[
\begin{align*}
\text{comp}_n^2(\text{comp}_n^2(f, z_1, \ldots, z_n), \pi_1^n, \pi_2^n) &= \text{comp}_n^2(f, \text{comp}_n^2(z_1, \pi_1^n, \pi_2^n), \ldots, \text{comp}_n^2(z_n, \pi_1^n, \pi_2^n)) \\
&= \text{comp}_n^1(f, v_1, \ldots, v_n)
\end{align*}
\]

and similarly \( \text{comp}_n^2(\text{comp}_n^2(f, z'_1, \ldots, z'_n), \pi_1^n, \pi_2^n) = \text{comp}_n^2(f, v'_1, \ldots, v'_n) \) and hence

\[
\text{comp}_n^1(f, v_1, \ldots, v_n) = \text{comp}_n^1(f, v'_1, \ldots, v'_n)
\]

as required.

Conversely, let \( i \leq n \), and suppose that \( v, v' \in \{\pi_1^n, \ldots, \pi_n^n\}^n \) are as in the formula above. Define \( z, z' \in \{\pi_1^n, \pi_2^n\}^n \) as follows. If \( v_j = v'_j \) define \( z_j := \pi_1^n \), and \( z_j := \pi_2^n \) otherwise. Similarly, if \( v'_j = v'_j \) then \( z'_j := \pi_1^n \), and \( z'_j := \pi_2^n \) otherwise. Then \( z \) and \( z' \) witness that \( \Phi_n(f) \) is true: since \( v_i \neq v'_i \) we have \( z_i \neq z'_i \), and

\[
\begin{align*}
\text{comp}_n^2(\text{comp}_n^1(f, v_1, \ldots, v_n), z_1, \ldots, z_n) &= \text{comp}_n^2(f, \text{comp}_n^1(v_1, \ldots, v_n), \ldots, \text{comp}_n^1(v_n, z_1, \ldots, z_n)) \\
&= \text{comp}_n^1(f, z_1, \ldots, z_n)
\end{align*}
\]

Similarly, \( \text{comp}_n^2(\text{comp}_n^1(f, v'_1, \ldots, v'_n), z'_1, \ldots, z'_n) = \text{comp}_n^2(f, z'_1, \ldots, z'_n) \). Hence,

\[
\text{comp}_n^2(f, z_1, \ldots, z_n) = \text{comp}_n^2(f, z'_1, \ldots, z'_n)
\]

as required. \( \square \)

Walter Taylor did not just introduce Taylor operations, but he proved a beautiful statement about their existence. The following is a slightly expanded presentation of the proof of Lemma 9.4 in [29].

**Theorem 7.17.** Let \( \mathbf{B} \) be an idempotent algebra. Then the following are equivalent.

1. There is no homomorphism from \( \text{Clo}(\mathbf{B}) \) to \( \text{Proj} \).
2. \( \mathbf{B} \) has a Taylor term.

**Proof.** To show the easy implication from (2) to (1), suppose for contradiction that there is a homomorphism \( \xi \) from \( \text{Clo}(\mathbf{B}) \) to \( \text{Proj} \). Let \( f \) be the element of \( \text{Clo}(\mathbf{B}) \) that is denoted by \( e^\mathbf{B} \). By definition of \( \text{Proj} \) we have \( \xi(f) = \pi_t^n \) for some \( t \leq n \). By assumption, \( \mathbf{B} \) satisfies

\[
\forall x, y. t(z_1, \ldots, z_n) = t(z'_1, \ldots, z'_n)
\]
for \( z_1, \ldots, z_n, z'_1, \ldots, z'_n \in \{x, y\} \) such that \( z_i \neq z'_i \). Then Clo(\( B \)) satisfies

\[
\text{comp}_2^n(f, \pi_{i_1}^2, \ldots, \pi_{i_n}^2) = \text{comp}_2^n(f, \pi_{j_1}^2, \ldots, \pi_{j_n}^2)
\]

(7)

for \( i_1, \ldots, i_n, j_1, \ldots, j_n \in \{1, 2\} \) such that \( i_1 = 1 \) if and only if \( z_1 = x \), \( j_1 = 1 \) if and only if \( z'_1 = x \), and \( i_t \neq j_t \). Since \( \xi(f) = \pi_1^2 \) we therefore obtain that \( \pi_1^2 = \pi_2^2 \), which does not hold in \( \text{Proj} \), a contradiction.

To show the implication from (1) to (2), suppose that Clo(\( B \)) does not homomorphically map to \( \text{Proj} \). Then Lemma 7.13 implies that there is a primitive positive sentence in the language of clones that holds in Clo(\( B \)) but not in \( \text{Proj} \). Note that by introducing new existentially quantified variables we can assume that this sentence is of the form \( \exists u_1, \ldots, u_r. \phi \) where \( \phi \) is a conjunction of atoms of the form \( y = \text{comp}_m^n(z_0, x_1, \ldots, x_m) \) or of the form \( y = \pi_1^m \) for \( y, x_0, x_1, \ldots, x_m \in \{u_1, \ldots, u_r\} \) and \( l, m \in \mathbb{N} \). For example the equation

\[
\text{comp}_2^2(u, \text{comp}_2^2(u, \pi_2^2, \pi_1^2)) = \text{comp}_2^2(\text{comp}_2^2(u, \pi_2^2, \pi_1^2), u)
\]

involving the free variable \( u \) is equivalent to

\[
\exists u_1, u_2, u_3 \ (u_1 = \text{comp}_2^2(u, \pi_2^2, \pi_1^2) \\
\wedge u_2 = \text{comp}_2^2(f, u, u_1) \\
\wedge u_3 = \text{comp}_2^2(u, u_1, u) \\
\wedge u_2 = u_3).
\]

For \( l, m \in \mathbb{N} \) and \( n = lm \) we write \( f \ast g \) as a shortcut for

\[
\text{comp}_m^l(f, \text{comp}_m^l(g, \pi_1^m, \ldots, \pi_n^m), \ldots, \text{comp}_m^l(g, \pi_{n-1}^m+1, \ldots, \pi_n^m)).
\]

Note that

\[
\text{Clo}(B) \models (g = \text{comp}_m^l(f \ast g, \pi_1^l, \ldots, \pi_j^l, \ldots, \pi_{i_1}^l, \ldots, \pi_{i_n}^l))
\]

(8)

and \( \text{Clo}(B) \models (f = \text{comp}_m^l(f \ast g, \pi_1^l, \ldots, \pi_j^l, \ldots, \pi_{i_1}^l, \ldots, \pi_{i_n}^l)) \)

(9)

since \( B \) is idempotent. For \( i \in \{1, \ldots, r\} \), let \( k_i \in \mathbb{N} \) be the arity of \( u_i \), and define

\[
u := u_1 \ast (u_2 \ast (\ldots (u_{r-1} \ast u_r) \ldots)).
\]

(10)

Observe that for each \( i \) we can obtain \( u_i \) from \( u \) by composing \( u \) with projections. In order to formalise this, we need a compact notation for strings of arguments consisting of projection constants. In this notation, \( [8] \) reads as \( y = \text{comp}_m^l(x \ast y, (1, \ldots, l)^m) \), and \( [9] \) reads as \( x = \text{comp}_m^n(x \ast y, 1^m, \ldots, l^m) \). Similarly, setting \( k := k_1 \cdots k_r \) we have

\[
u_i = \text{comp}_k^{k_i}(u, p_i) \text{ where } p_i := (1^{k_1-k_{i-1}}, \ldots, k_i^{k_1-k_{i-1}}, k_i+1-k_i) \in \{\pi_1^{k_i}, \ldots, \pi_{k_i}^{k_i}\}^k.
\]

Let \( n := k^2 \). Then every term of the form

\[
t := \text{comp}_k^{k_i}(u, u_i, \ldots, u_{i_k})
\]

can be written as

\[
\text{comp}_l^v(u \ast u, q^v)
\]

60
for $\mathbf{q}^t \in \{\pi_1^i, \ldots, \pi_{r_1}^i\}^n$ obtained from $\mathbf{p}^i$ by replacing character $l \leq k_i$ by the string $\mathbf{p}^{k_i}$; see Figure 9 for an illustration. Similarly, every term of the form $t := u_i$ can be written as $\text{comp}_{k_i}^n(u \ast u, \mathbf{q}^t)$ for $\mathbf{q}^t \in \{\pi_{n_1}^{k_i}, \ldots, \pi_{n_r}^{k_i}\}^n$ obtained by $k_i$ times concatenating $\mathbf{p}^i$ with itself. In this way, every conjunct of $\phi$ of the form 

$$u_j = \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}})$$

can be written in the form

$$\text{comp}_{k_j}^n(u \ast u, \mathbf{q}^{t_1}) = \text{comp}_{k_j}^n(u \ast u, \mathbf{q}^{t_2})$$

for $t_1 := u_j$ and $t_2 := \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}})$. Conjuncts of $\phi$ of the form $u_j = \pi_{l^m}$ can be rewritten similarly. Let $\psi$ be the conjunction of all these equations; note that $\phi$ implies $\psi$. Let $\theta$ be the formula obtained from $\psi$ by replacing each occurrence of $u \ast u$ by a variable symbol $f$. Note that the sentence $\exists f. \theta$ holds in Clo($B$). It suffices to show that every $f \in \text{Clo}(B)$ that satisfies $\theta$ is a Taylor operation.

Suppose for contradiction that for $\ell \in \{1, \ldots, n\}$ there are no $\bar{v}, \bar{v}' \in \{\pi_{n_1}^{r_1}, \ldots, \pi_{n_m}^{r_m}\}$ for some $m \leq n$ with $\bar{v}_\ell \neq \bar{v}'_\ell$ such that $\text{comp}_{k_\ell}^n(f, \bar{v}) = \text{comp}_{k_\ell}^n(f, \bar{v}')$ (otherwise, $f$ is a Taylor operation by the argument from Lemma 7.16).

We claim that the assignment $\rho$ that maps $u_s$ to $\text{comp}_{k_\ell}^n(\pi_{n_1}^{\ell_1}, \mathbf{q}^{u_s}) = \bar{q}^{u_s}_\ell$, for $s \in \{1, \ldots, r\}$, satisfies all conjuncts of $\phi$, contradicting our assumptions. First note that $\bar{q}^{u_s}_\ell = \bar{p}^{\ell_1}$, where $\ell_1 \in \{1, \ldots, k\}$ is such that $\ell = (\ell_1 - 1)k + \ell_2$ for some $\ell_2 \in \{1, \ldots, k\}$. Indeed, consider a conjunct of $\phi$

$$u_j = t \text{ for } t = \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}}).$$

By construction, $\theta$ contains the conjunct

$$\text{comp}(f, \mathbf{q}^{u_s}) = \text{comp}(f, \mathbf{q}^t).$$

Figure 9: An illustration of $u \ast u$ and $u := f \ast g$ for the proof of Taylor’s theorem, and how to recover the composed term $f(g(x,y), g(y,x))$ from $u \ast u$ by identifying arguments.

for $\mathbf{q}^t \in \{\pi_1^i, \ldots, \pi_{r_1}^i\}^n$ obtained from $\mathbf{p}^i$ by replacing character $l \leq k_i$ by the string $\mathbf{p}^{k_i}$; see Figure 9 for an illustration. Similarly, every term of the form $t := u_i$ can be written as $\text{comp}_{k_i}^n(u \ast u, \mathbf{q}^t)$ for $\mathbf{q}^t \in \{\pi_{n_1}^{k_i}, \ldots, \pi_{n_r}^{k_i}\}^n$ obtained by $k_i$ times concatenating $\mathbf{p}^i$ with itself. In this way, every conjunct of $\phi$ of the form

$$u_j = \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}})$$

can be written in the form

$$\text{comp}_{k_j}^n(u \ast u, \mathbf{q}^{t_1}) = \text{comp}_{k_j}^n(u \ast u, \mathbf{q}^{t_2})$$

for $t_1 := u_j$ and $t_2 := \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}})$. Conjuncts of $\phi$ of the form $u_j = \pi_{l^m}$ can be rewritten similarly. Let $\psi$ be the conjunction of all these equations; note that $\phi$ implies $\psi$. Let $\theta$ be the formula obtained from $\psi$ by replacing each occurrence of $u \ast u$ by a variable symbol $f$. Note that the sentence $\exists f. \theta$ holds in Clo($B$). It suffices to show that every $f \in \text{Clo}(B)$ that satisfies $\theta$ is a Taylor operation.

Suppose for contradiction that for $\ell \in \{1, \ldots, n\}$ there are no $\bar{v}, \bar{v}' \in \{\pi_{n_1}^{r_1}, \ldots, \pi_{n_m}^{r_m}\}$ for some $m \leq n$ with $\bar{v}_\ell \neq \bar{v}'_\ell$ such that $\text{comp}_{k_\ell}^n(f, \bar{v}) = \text{comp}_{k_\ell}^n(f, \bar{v}')$ (otherwise, $f$ is a Taylor operation by the argument from Lemma 7.16).

We claim that the assignment $\rho$ that maps $u_s$ to $\text{comp}_{k_\ell}^n(\pi_{n_1}^{\ell_1}, \mathbf{q}^{u_s}) = \bar{q}^{u_s}_\ell$, for $s \in \{1, \ldots, r\}$, satisfies all conjuncts of $\phi$, contradicting our assumptions. First note that $\bar{q}^{u_s}_\ell = \bar{p}^{\ell_1}$, where $\ell_1 \in \{1, \ldots, k\}$ is such that $\ell = (\ell_1 - 1)k + \ell_2$ for some $\ell_2 \in \{1, \ldots, k\}$. Indeed, consider a conjunct of $\phi$

$$u_j = t \text{ for } t = \text{comp}_{k_j}^n(u_i, u_{i_1}, \ldots, u_{i_{k_i}}).$$

By construction, $\theta$ contains the conjunct

$$\text{comp}(f, \mathbf{q}^{u_s}) = \text{comp}(f, \mathbf{q}^t).$$

61
So by assumption we must have
\[ \text{comp}(\pi^n_q, q^n) = \bar{q}^u_{ij} = \bar{q}^f = \text{comp}(\pi^n_q, q^f). \] (11)

Then \( \rho \) satisfies this conjunct since
\[ \text{comp}_{k_3}^k(\rho(u_i), \rho(u_i), \ldots) = \text{comp}_{k_3}^k(\bar{q}^u_{ii}, \bar{q}^u_{ii}, \ldots) \]
\[ = \text{comp}_{k_3}^k(\bar{q}^t_{ii}, \bar{q}^t_{ii}, \ldots) \]
\[ = \bar{q}^t_{ij} \] (by definition of \( \bar{q}^t \))
\[ = \bar{q}^u_{ij} \] (by (11))
\[ = \rho(u_j) \]

\[ \square \]

**Lemma 7.18.** Let \( \mathcal{B} \) and \( \mathcal{C} \) be homomorphically equivalent structures. Then \( \mathcal{B} \) has a Taylor polymorphism if and only if \( \mathcal{C} \) has a Taylor polymorphism.

**Proof.** Let \( h \) be a homomorphism from \( \mathcal{B} \) to \( \mathcal{C} \), and \( g \) be a homomorphism from \( \mathcal{C} \) to \( \mathcal{B} \). Suppose that \( f \) is a Taylor polymorphism for \( \mathcal{B} \) of arity \( n \). It suffices to show that the operation \( f' \) given by \( (x_1, \ldots, x_n) \to h(f(g(x_1), \ldots, g(x_n))) \) is a Taylor polymorphism of \( \mathcal{C} \). Indeed, for all \( i \leq n \) we have that
\[
f'(v^i_{1,i}, \ldots, v^i_{n,i}) = h(f(g(v^i_{1,i}), \ldots, g(v^i_{n,i})))
\]
\[
= h(f(g(v'_i, \ldots, g(v'_n))))
\]
\[
= f'(v'_1, \ldots, v'_n)
\]

\[ \square \]

**Lemma 7.19.** Let \( \mathcal{B} \in \text{C}(\mathcal{C}) \) and suppose that \( \mathcal{C} \) has a Taylor polymorphism. Then \( \mathcal{B} \) has a Taylor polymorphism.

**Proof.** Suppose that \( \mathcal{C} \) is a core and that \( \mathcal{B} \) has been obtained by expanding \( \mathcal{C} \) by adding unary singleton relations. Let \( f \) be the Taylor polymorphism of \( \mathcal{C} \). Then \( f(x) := f(x, \ldots, x) \) is an automorphism with inverse \( i \in \text{Pol}(\mathcal{C}) \). The function \( i(f(x, \ldots, x)) \) is a Taylor operation and idempotent, and therefore a polymorphism of \( \mathcal{B} \).

Alternatively, one can prove the lemma by observing that any \( \mathcal{B}' \in \text{PP}(\mathcal{C}) \) has a Taylor polymorphism, using Lemma 7.18 and the fact that \( \text{C}(\mathcal{C}) \subseteq \text{H}(\text{PP}(\mathcal{C})) \).

\[ \square \]

**Corollary 7.20.** Let \( \mathcal{B} \) be a finite structure. Then the following are equivalent.

- \( K_3 \notin \text{H}(\text{PP}(\mathcal{B})) \)
- \( \mathcal{B} \) has a Taylor polymorphism.

**Proof.** If \( \mathcal{B} \) has a Taylor polymorphism, then so has any structure in \( \text{PP}(\mathcal{B}) \), and so has any structure in \( \text{H}(\text{PP}(\mathcal{B})) \) by Lemma 7.18.

Conversely, suppose that \( K_3 \notin \text{H}(\text{PP}(\mathcal{B})) \). If \( \mathcal{B}' \) is the core of \( \mathcal{B} \), and \( \mathcal{C} \) is the expansion of \( \mathcal{B}' \) by all unary singleton relations, then \( \text{C}(\mathcal{B}) \subseteq \text{H}(\text{PP}(\mathcal{B})) \) implies that \( K_3 \) is not primitive positive interpretable in \( \mathcal{C} \). Hence, the idempotent clone \( \text{Pol}(\mathcal{C}) \) does not homomorphically map to \( \text{Proj} \). Theorem 7.17 shows that \( \mathcal{C} \) and thus also \( \mathcal{B}' \) must have a Taylor polymorphism. Lemma 7.18 implies that \( \mathcal{B} \) has a Taylor polymorphism.

\[ \square \]
Corollary 7.21. Let $\mathcal{B}$ be a finite structure. Then $\mathcal{B}$ has a Taylor polymorphism, or $\text{CSP}(\mathcal{B})$ is NP-hard.

Proof. If $K_3 \in \text{H}(\text{PP}(\mathcal{B}))$ then $\text{CSP}(\mathcal{B})$ is NP-hard by Corollary 4.10. Otherwise, $\mathcal{B}$ has a Taylor polymorphism by Corollary 7.20. 

The following has been conjectured (in slightly different, but equivalent form) by Bulatov, Jeavons, and Krokhin in [15], and is known under the name tractability conjecture.

Conjecture 2 (Tractability Conjecture). Let $\mathcal{B}$ be a finite relational structure. If $\text{Pol}(\mathcal{B})$ contains a Taylor polymorphism, then $\text{CSP}(\mathcal{B})$ is in P.

8 Undirected Graphs

This section contains a proof of the dichotomy for finite undirected graphs of Hell and Nešetřil, Theorem 1.4. We prove something stronger, namely that the tractability conjecture (Conjecture 2) is true for finite undirected graphs $\mathcal{B}$. More specifically, the following is true.

Theorem 8.1. Let $\mathcal{B}$ be a finite undirected graph. Then either

- $\mathcal{B}$ is bipartite, or
- $\text{H}(\text{PP}(\mathcal{B}))$ contains all finite structures.

In the former case, $\mathcal{B}$ has a quasi-majority polymorphism (which is a Taylor polymorphism; see Exercise 41) and $\text{CSP}(\mathcal{B})$ is clearly in P, and in the latter case $\text{CSP}(\mathcal{B})$ is NP-complete by Theorem 4.9.

This theorem has a remarkable consequence in universal algebra, whose significance goes beyond the study of the complexity of CSPs, and which provide a strengthening of Taylor’s theorem (Theorem 7.17), discovered by Siggers in 2010 (see Section 8.2).

8.1 The Hell-Nešetřil Theorem

The graph $K_4 - \{0,1\}$ (a clique where one edge is missing) is called a diamond. A graph is called diamond-free if it does not contain a copy of a diamond.

Lemma 8.2. Let $\mathcal{B}$ be a finite undirected graph which is not bipartite. Then $\mathcal{B}$ interprets primitively positively a graph that is homomorphically equivalent to a diamond-free core containing a triangle.

Proof. We may assume that

1. $\text{H}(\text{PP}(\mathcal{B}))$ does not contain a non-bipartite graph with fewer vertices than $\mathcal{B}$, since otherwise we could replace $\mathcal{B}$ by this graph. In particular, $\mathcal{B}$ must then be a core.
2. $\mathcal{B}$ contains a triangle: if the length of the shortest odd cycle is $k$, then $(\mathcal{B}; E^{k-2})$, where $E^{k-2}$ is defined via the usual composition of binary relations and so primitive positive definable in $\mathcal{B}$, is a graph and contains a triangle, so it can replace $\mathcal{B}$.
3. every vertex of $\mathcal{B}$ is contained in a triangle: Otherwise, we can replace $\mathcal{B}$ by the subgraph of $\mathcal{B}$ induced by set defined by the primitive positive formula $\exists u, v (E(x, u) \land E(x, v) \land E(u, v))$ which still contains a triangle.
**Claim 1.** \( \mathfrak{B} \) does not contain a copy of \( K_4 \). Otherwise, if \( a \) is an element from a copy of \( K_4 \) then the subgraph of \( \mathfrak{B} \) induced by the set defined by the primitive positive formula \( E(a, x) \) is a non-bipartite graph. Moreover, by Theorem 4.13 this subgraph is homomorphically equivalent to a graph with a primitive positive interpretation in \( \mathfrak{B} \), contrary to our initial assumption.

**Claim 2.** The graph \( \mathfrak{B} \) must also be diamond-free. To see this, let \( R \) be the binary relation with the primitive positive definition

\[
R(x, y) :\Leftrightarrow \exists u, v \left( E(x, u) \land E(x, v) \land E(u, v) \land E(u, y) \land E(v, y) \right)
\]

and let \( T \) be the transitive closure of \( R \). The relation \( T \) is clearly symmetric, and since every vertex of \( \mathfrak{B} \) is contained in a triangle, it is also reflexive, and hence an equivalence relation of \( \mathfrak{B} \). Since \( B \) is finite, for some \( n \) the formula \( \exists u_1, \ldots, u_n \left( R(x, u_1) \land R(u_1, u_2) \land \cdots \land R(u_n, y) \right) \) defines \( T \), showing that \( T \) is primitively positively definable in \( \mathfrak{B} \).

We claim that the graph \( \mathfrak{B}/T \) (see Example 7) is not bipartite. It suffices to show that \( T \cap E = \emptyset \). Otherwise, let \( (a, b) \in T \cap E \). Choose \( (a, b) \) in such a way that the shortest sequence \( a = a_0, a_1, \ldots, a_n = b \) with \( R(a_0, a_1), R(a_1, a_2), \ldots, R(a_{n-1}, a_n) \) in \( \mathfrak{B} \) is shortest possible; see Figure 10. This chain cannot have the form \( R(a_0, a_1) \) because \( \mathfrak{B} \) does not contain \( K_4 \) subgraphs. Suppose first that \( n = 2k \) is even. Let the vertices \( u_1, v_1, u_{k+1} \) and \( v_{k+1} \) be as depicted in Figure 10. Let \( S \) be the set defined by

\[
\exists x_1, \ldots, x_k \left( E(u_{k+1}, x_1) \land E(v_{k+1}, x_1) \land R(x_1, x_2) \land \cdots \land R(x_{k-1}, x_k) \land E(x_k, x) \right).
\]

Note that \( a_0, u_1, v_1 \in S \) form a triangle. If \( a_n \in S \) then we obtain a contradiction to the minimal choice of \( n \). Hence, the subgraph induced by the primitively definable set \( S \) is non-bipartite and strictly smaller than \( \mathfrak{B} \), in contradiction to the initial assumption.

If \( n = 2k + 1 \) is odd, we can argue analogously with the set \( S \) defined by the formula

\[
\exists x_1, \ldots, x_k \left( R(a_{k+1}, x_1) \land R(x_1, x_2) \land \cdots \land R(x_{k-1}, x_k) \land R(x_k, x) \right)
\]

and again obtain a contradiction. Hence \( \mathfrak{B}/T \) is not bipartite. The initial assumption for \( \mathfrak{B} \) then implies that \( T \) must be the trivial equivalence relation, which in turn implies that \( \mathfrak{B} \) does not contain any diamonds. \( \square \)

**Lemma 8.3** (from [12]). Let \( \mathfrak{B} \) be a diamond-free undirected graph and let \( h: (K_3)^k \rightarrow \mathfrak{B} \) be a homomorphism. Then the image of \( h \) is isomorphic to \( (K_3)^m \) for some \( m \leq k \).

**Proof.** Let \( I \subseteq \{1, \ldots, k\} \) be a maximal set such that \( \ker(h) \subseteq \ker(pr_I) \). Such a set exists, because \( \ker(pr_0) \) is the total relation. We claim that \( \ker(h) = \ker(pr_I) \); this clearly implies the statement.

---

Figure 10: Diagram for the proof of Lemma 8.2
By the maximality of \( I \), for every \( j \in \{1, \ldots, k\} \setminus I \) there are \( x, y \in (K_3)^k \) such that \( h(x) = h(y) \) and \( x_j \neq y_j \). We have to show that for all \( z_1, \ldots, z_k, z'_k \in \{0, 1, 2\} \)

\[
h(z_1, \ldots, z_j, \ldots, z_k) = h(z_1, \ldots, z_{j-1}, z'_j, z_{j+1}, \ldots, z_k).
\]

We may suppose that \( z_j \neq x_j \) and \( z'_j = x_j \). To simplify notation, we assume that \( j = k \). As we have seen in Exercises 7 and 8, any two vertices in \((K_3)^k\) have a common neighbour.

- Let \( r \) be a common neighbour of \( x \) and \((z, z_k) := (z_1, \ldots, z_k)\). Note that \( r \) and \((z, z'_k)\) are adjacent, too.

- For all \( i \neq k \) we choose an element \( s_i \) of \( K_3 \) that is distinct from both \( r_i \) and \( y_i \). Since \( x_k \) is distinct from \( r_k \) and \( y_k \) we have that \((s, x_k) := (s_1, \ldots, s_{k-1}, x_k)\) is a common neighbour of \( r \) and \( y \).

- The tuple \((r, z_k) := (r_1, \ldots, r_{k-1}, z_k)\) is a common neighbour of both \( x \) and \((s, x_k)\).

- Finally, for \( i \neq k \) choose \( t_i \) to be distinct from \( z_i \) and \( r_i \), and choose \( t_k \) to be distinct from \( z_k \) and from \( z'_k \). Then \( t := (t_1, \ldots, t_{k-1}, t_k)\) is a common neighbour of \((z, z_k)\), of \((z, z'_k)\), and of \((r, z_k)\).

The situation is illustrated in Figure 11. Since \( \mathcal{B} \) is diamond-free, \( h(x) = h(y) \) implies that \( h(r) = h(r, z_k) \) and for the same reason \( h(z, z_k) = h(z, z'_k) \) which completes the proof.

**Lemma 8.4** (from [12]). If a finite diamond-free graph \( \mathcal{B} \) contains a triangle, then for some \( k \in \mathbb{N} \) there is a primitive positive interpretation of \((K_3)^k\) with constants in \( \mathcal{B} \).

**Proof.** We construct a strictly increasing sequence of subgraphs \( G_1 \subset G_2 \subset \cdots \) of \( \mathcal{B} \) such that \( G_i \) is isomorphic to \((K_3)^{k_i}\) for some \( k_i \in \mathbb{N} \). Let \( G_1 \) be any triangle in \( \mathcal{B} \). Suppose now that \( G_i \) has already been constructed. If the domain of \( G_i \) is primitively positively definable in \( \mathcal{B} \) with constants, then we are done. Otherwise, there exists an idempotent polymorphism \( f \) of \( \mathcal{B} \) and \( v_1, \ldots, v_k \in G_i \) such that \( f(v_1, \ldots, v_k) \notin G_i \). The restriction of \( f \) to \( G_i \) is a homomorphism from \((K_3)^{k_i}\) to the diamond-free graph \( \mathcal{B} \). Lemma 8.3 shows that \( G_{i+1} := f((G_i)^k) \) induces a copy of \((K_3)^{k_{i+1}}\) for some \( k_{i+1} \leq k \). Since \( f \) is idempotent, we have that \( G_i \subseteq G_{i+1} \), and by the choice of \( f \) the containment is strict. Since \( \mathcal{B} \) is finite, for some \( m \) the set \( G_m \) must have a primitive positive definition in \( \mathcal{B} \) with constants.

\[ \]
Proof of Theorem 8.1. Let \( \mathfrak{B} \) be a finite undirected graph that is not bipartite. By Lemma 8.2 \( \mathfrak{B} \) interprets primitively positively a graph that is homomorphically equivalent to a diamond-free core \( \mathfrak{C} \) containing a triangle. Then Lemma 8.4 applied to \( \mathfrak{C} \) implies that for some \( k \in \mathbb{N} \) there is a primitive positive interpretation of \( (K_3)^k \) with constants in \( \mathfrak{C} \). Since \( \mathfrak{C} \) is a core, and since \( (K_3)^k \) is homomorphically equivalent to \( K_3 \), it follows that there is a primitive positive interpretation of a structure that is homomorphically equivalent to \( K_3 \) in \( \mathfrak{C} \). The structure \( K_3 \) interprets all finite structures primitive positively (Theorem 4.11), so Theorem 4.13 implies that \( \text{H(PP(\mathfrak{B}))} \) contains all finite structures.

8.2 Siggers Operations of Arity 6

An operation \( s : B^6 \to B \) is called Siggers operation if

\[
s(x, y, x, z, y, z) = s(y, x, z, x, z, y)
\]
holds for all \( x, y, z \in B \).

Theorem 8.5 ([48]). Let \( \mathfrak{B} \) be a finite structure. Then either \( \mathfrak{B} \) interprets all finite structures up to homomorphic equivalence, or \( \mathfrak{B} \) has a Siggers polymorphism.

Proof. Pick \( k \geq 1 \) and \( a, b, c \in B^k \) such that \( \{(a_i, b_i, c_i) \mid i \leq k\} = B^3 \). Let \( R \) be the binary relation on \( B^k \) such that \((a_i, b_i, c_i, a_i, b_i, c_i) \) and \( v = s(a, c, a, c, b) \). We make the following series of observations.

- The vertices \( a, b, c \) of \((B^6; R)\) induce a copy of \( K_3 \): each of the six edges of \( K_3 \) is witnessed by one of the six 6-ary projections from \( \text{Pol}(\mathfrak{B}) \).

- The relation \( R \) is symmetric: Suppose that \((u, v) \in R \) and let \( s \in \text{Pol}(\mathfrak{B}) \) be such that \( s(a, b, a, c, b, c) = u \) and \( s(b, a, c, a, c, b) = v \). Define \( s'(x_1, \ldots, x_6) := s(x_2, x_1, x_4, x_3, x_6, x_5) \); then

\[
\begin{align*}
v &= s(b, a, c, a, c, b) = s'(a, b, a, c, b, c) \\
u &= s(a, b, a, c, b, c) = s'(b, a, c, a, c, b)
\end{align*}
\]

and hence \( s' \) witnesses that \((v, u) \in R \).

- If the graph \((B^6; R)\) contains a loop \((w, w) \in R \), then there exists a 6-ary \( s \in \text{Pol}(\mathfrak{B}) \) such that

\[
s(a, b, a, c, b, c) = w = s(b, a, c, a, c, b).
\]

The operation \( s \) is Siggers: for all \( x, y, z \in B \) there exists an \( i \leq k \) such that \((x, y, z) = (a_i, b_i, c_i) \), and the above implies that

\[
s(a_i, b_i, a_i, c_i, b_i, c_i) = s(b_i, a_i, c_i, a_i, c_i, b_i)
\]

and we are done in this case.

So we may assume in the following that \((B^6; R)\) is a simple (i.e., undirected and loopless) graph that contains a copy of \( K_3 \). The relation \( R \) (as a 12-ary relation over \( B \)) is preserved by \( \text{Pol}(\mathfrak{B}) \), and hence \((B^6; R)\) has a primitive positive interpretation in \( \mathfrak{B} \). By Theorem 8.1 applied to the undirected graph \((B^6; R)\), there is a primitive positive interpretation in \((B^6; R)\) of all finite structures up to homomorphic equivalence, and hence also in \( \mathfrak{B} \), and this concludes the proof. 

\[
\end{proof}
\]

66
9 Bounded Width

Equipped with the universal-algebraic approach, we come back to one of the questions that occupied us at the beginning of the course: which $H$-colouring problems can be solved by the path-consistency procedure, $PC_H$, introduced in Section 3? We have seen in Section 3.1 that when $H$ has a majority or a semilattice polymorphism, then $PC_H$ solves the $H$-colouring problem. But these were just sufficient, not necessary conditions.

A necessary and sufficient polymorphism condition for solvability by $PC_H$ has been found by Barto and Kozik [5]. Their result is much stronger: it characterises not just the strength of $PC_H$, but more generally of $k$-consistency (introduced in Section 3), and not just for $H$-colouring, but for CSPs of finite structures in general. Before we state their result in Theorem 9.2 below, it is convenient to use a more flexible terminology to discuss the idea of $k$-consistency for general relational structures more precisely.

When generalising 3-consistency for the $H$-colouring problem to $k$-consistency for CSPs of arbitrary finite structures $\mathfrak{B}$, there are two essential parameters:

- the first is the arity $l$ of the relations maintained for all $l$-tuples of variables in the instance. For $PC_H$, for instance, we have $l = 2$.

- the second is the number of variables considered at a time within the main loop of the algorithm. For $PC_H$, for instance, we have $k = 3$.

Hence, for each pair $(l, k) \in \mathbb{N}^2$, we obtain a different form of consistency, called $(l, k)$-consistency.

Note that it is easy to come up with finite structures $\mathfrak{B}$ whose CSP cannot be solved by $(l, k)$-consistency when $\mathfrak{B}$ might contain relations of arity larger than $k$ (there is no possibility of the $(l, k)$-consistency algorithm to take constraints into account that are imposed on more than $k$ variables). We say that $CSP(\mathfrak{B})$ has width $(l, k)$ if it can be solved by $(l, k)$-consistency, and that is has has bounded width) if it has width $(l, k)$ for some $l, k \in \mathbb{N}$. We mention that this is the case if and only if $CSP(\mathfrak{B})$ can be solved by Datalog (see [22]). The following lemma suggests that the universal-algebraic approach can be used to study the question for which structures $\mathfrak{B}$ the problem $CSP(\mathfrak{B})$ has bounded width.

**Lemma 9.1.** Let $\mathfrak{A}$ and $\mathfrak{B}$ be structures with finite relational signature such that $\mathfrak{A} \in H(PP(\mathfrak{B}))$. If $CSP(\mathfrak{B})$ has bounded width, then so does $CSP(\mathfrak{A})$.

**Proof.** Let $\tau$ be the signature of $\mathfrak{A}$ and $\sigma$ the signature of $\mathfrak{B}$. Suppose that $CSP(\mathfrak{B})$ has width $(l, k)$. Let $d$ be the dimension of the primitive positive interpretation $I$ of $\mathfrak{A}$ in $\mathfrak{B}$, let $\delta_I(x_1, \ldots, x_d)$ be the domain formula, and let $h: D \to A$ be the coordinate map where $D := \{(b_1, \ldots, b_d) \in B^d \mid \mathfrak{B} \models \delta_I(b_1, \ldots, b_d)\}$. Let $\phi$ be an unsatisfiable instance of $CSP(\mathfrak{A})$ with variable set $U = \{x_1, \ldots, x_n\}$. From $\phi$ we construct an unsatisfiable instance $\psi$ of $CSP(\mathfrak{B})$. This instance will be used as a “guide” when we inductively show that $(l, k)$-consistency derives false on $\phi$.

For fresh and pairwise distinct variables $V := \{y^d_i \mid 1 \leq i \leq d, 1 \leq j \leq n\}$ let $\psi_1$ be

$$\bigwedge_{1 \leq i \leq n} \delta_I(y^1_i, \ldots, y^d_i).$$

Let $\psi_2$ be the conjunction of the formulas $\theta_I(y^1_{i_1}, \ldots, y^d_{i_1}, \ldots, y^1_{i_k}, \ldots, y^d_{i_k})$ over all conjuncts $\theta = R(x_1, \ldots, x_{i_k})$ of $\phi$. By moving existential quantifiers to the front, the sentence

$$\exists y^1_1, \ldots, y^d_n (\psi_1 \land \psi_2)$$

67
can be re-written to a primitive positive $\sigma$-formula $\psi$.

We claim that $\psi$ is unsatisfiable in $\mathfrak{B}$. Suppose for contradiction that $f : V \to B$ satisfies all conjuncts of $\psi$ in $\mathfrak{B}$. By construction of $\psi$, if $\phi$ has a conjunct $\theta = R(x_1, \ldots, x_{i_k})$, then

$$\mathfrak{B} \models \theta_1((f(y_{i_1}^1), \ldots, f(y_{i_k}^d)), \ldots, (f(y_{i_1}^1), \ldots, f(y_{i_k}^d))).$$

By the definition of interpretations, this implies that

$$\mathfrak{A} \models \theta(h(f(y_{i_1}^1), \ldots, f(y_{i_k}^d)), \ldots, h(f(y_{i_1}^1), \ldots, f(y_{i_k}^d))).$$

Hence, the mapping $g : U \to A$ that sends $x_i$ to $h(f(y_{i_1}^1), \ldots, f(y_{i_k}^d))$ satisfies all conjuncts of $\phi$ in $\mathfrak{A}$, in contradiction to the assumption that $\phi$ is unsatisfiable.

Since CSP($\mathfrak{B}$) has width $(l, k)$ we consequently have that the $(l, k)$-consistency procedure applied to $\psi$ derives false. This derivation can be used to show that the $(l, k)$-consistency procedure applied to $\phi$ derives false, too. We leave the details to the reader. \[\square\]

A weak near unanimity operation is an operation that satisfies

$$\forall x, y. w(x, \ldots, x, y) = w(x, \ldots, y, x) = \cdots = w(y, x, \ldots, x).$$

We write WNU($k$) for the $k$-ary weak near unanimity operations. Again, we warn the reader that many authors additionally assume that weak near unanimity operations are idempotent; we do not make this assumption since it gives us more flexibility of the terminology.

**Example 16.** Consider the algebra $\mathbf{A}_n := (\{0, \ldots, n - 1\}; m)$ where $m(x, y, z) := x - y + z$. Then $\text{Clo}(\mathbf{A}_n)$ consists of precisely the operations defined as

$$g(x_0, \ldots, x_{k-1}) := \sum_i a_i x_i$$

where $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ with $\sum_i a_i = 1$. We claim that $\mathfrak{A}_n$ has an WNU($k$) term if and only if $\gcd(k, n) = 1$:

- if $\gcd(k, n) = 1$ then there is an $a$ such that $ak \equiv 1 \mod n$. Hence, $\sum_i a_i x_i \in \text{WNU}(k)$ and we have $\sum_i a = ka = 1$ so this operation is in $\text{Clo}(\mathbf{A}_n)$.
- Conversely, let $g \in \text{WNU}(k)$. In particular, we have

$$g(0, \ldots, 0, 1) = a_k$$

$$\equiv g(1, 0, \ldots, 0) = a_1$$

and it follows that $a := a_0 \equiv \cdots \equiv a_{k-1} \mod n$. But $1 = \sum_i a_i = ka \mod n$, which implies that $n$ and $m$ are pairwise prime.

For example, $\text{Clo}(\mathfrak{A}_6)$ has a WNU(5) term, but not WNU($k$) term for $k \leq 4$.

**Theorem 9.2.** Let $\mathfrak{B}$ be a finite structure. Then the following are equivalent.

1. CSP($\mathfrak{B}$) has width $(l, k)$ for some $l, k \in \mathbb{N}$.
2. $H(\text{PP}(\mathfrak{B}))$ does not contain $([0, \ldots, p - 1]; L_0, \ldots, L_{p-1})$ where $p$ is a prime and $L_i := \{(x, y, z) \mid x + y + z = i \mod p\}$. 

68
3. CSP($\mathcal{B}$) can be solved by a remarkably weak form of consistency, called singleton linear arc-consistency (SLAC), which will be introduced below.

4. CSP($\mathcal{B}$) has width $(2, k)$ where $k$ is the maximal arity of $\mathcal{B}$.

5. $\mathcal{B}$ has polymorphisms $f \in WNU(3)$ and $g \in WNU(4)$ satisfying

$$\forall x, y. f(y, x, x) = g(y, x, x, x).$$

6. $\mathcal{B}$ has a binary polymorphism $f_2$ and polymorphisms $f_n \in WNU(n)$ for every $n \geq 3$ and

$$\forall x, y. f_n(x, y, \ldots, y) = f_2(x, y).$$

7. $\mathcal{B}$ has ternary polymorphisms $p, q$ such that $p \in WNU(3)$ and

$$\forall x, y. (p(x, x, y) = q(x, y, x) \land q(x, x, y) = q(x, y, y)).$$

Item 3. mentions a procedure that we only introduce informally here, called Singleton Linear Arc Consistence (SLAC). It comes close to strategies that humans perform when solving Sudoku puzzles. First, Linear Arc Consistency (LAC) is the restriction of the arc consistency procedure for arbitrary relational signatures where, informally, each inference uses at most one fact that has been derived previously. SLAC is the extension of LAC which performs the following with an instance $I$ of CSP($\mathcal{B}$):

1. Run LAC on $I$; if LAC derives false, return No.

2. Create a copy $I'$ of $I$.

3. Pick some variable $x$ of $I'$ and some value $v$ from $\mathcal{B}$; set $x := v$.

4. If LAC derives false on $I'$, remove $v$ from the list for $x$ in $I$.

5. Otherwise, do nothing ($I$ is unchanged).

We repeat these steps until for no pair $(x, v)$ a value can be removed from $I$, in which case we return Yes.

We do not give a complete proof of the important Theorem 9.2, but only show some of the easy implications, and we explain how to deduce the remaining implications from statements that can be found explicitly in the literature.

Proof. $1 \Rightarrow 2$. By Lemma 9.1 it suffices to show that CSP($\{0, \ldots, p-1\}; L_0, \ldots, L_{p-1}$) does not have width $(l, k)$. Two proof sketches of this fact can be found in [22]. A stronger non-expressibility can be found in [2] (the given CSP is not even expressible in least fixed point logic with counting quantifiers).

The implication from $2 \Rightarrow 1$ was open for a while, has been conjectured by Larose and Zadori [39] (and in equivalent form, by Feder and Vardi [22]; also see [38]), and was proven by Barto and Kozik [5]; the proof requires several important concepts, e.g., Prague strategies and absorption theory.

The (unexpected) implication from $2 \Rightarrow 3$ is from [35].

The implication from $3 \Rightarrow 4$ is easy: a derivation of false by SLAC can be simulated by a derivation of false by $(2, k)$-consistency where $k$ is the maximal arity of the relations in $\mathcal{B}$. 

69
The implication from 4. to 5. has an elegant short proof, see [36]. The equivalences between the final three items when we additionally require idempotency for the terms has been shown in [32] (e.g., for 6., see Proposition 4.1 in [32]). But since a structure has polymorphism satisfying an equation without nesting (and the equations under consideration are of this type) if and only if its core does, and since a core has such a polymorphism if and only if it has a polymorphism that is additionally idempotent, the idempotent case implies the statement as given in the theorem.

The implication from 6. to 2. is easy: first note that if \( B \) has a \( \text{WNU}(k) \)-polymorphism, then so do have all structures in \( \text{H}(\text{PP}(B)) \) (recall that we do not require idempotency from the operations in \( \text{WNU}(k) \)). But the structure \( \{0, \ldots, p - 1\}; L_0, \ldots, L_{p-1} \) does not have \( \text{WNU}(k) \) polymorphisms for both \( k = 3 \) and \( k = 4 \) (see Example 16).

To link the equivalent items in Theorem 9.2 with some central and old concepts in universal algebra we have to restrict to the idempotent setting. Most of the results have originally been obtained and stated in this context. Recall that a lattice \( (L; \land, \lor) \) is called meet semi-distributive (SD(\( \land \))) if it satisfies

\[
\forall a, b, c \ (a \land b = a \land c \Rightarrow a \land (b \lor c) = a \land b).
\]

Join semi-distributivity (SD(\( \lor \))) is defined dually. The smallest lattices satisfying one, but not both, semi-distributivity conditions are shown in Figure 12.

Figure 12: The left diagram shows the lattice \( D_1 \) which fails SD(\( \land \)) and the right diagram shows the lattice \( D_2 \) which fails SD(\( \lor \)) (and which is the congruence lattice of \( S^2 \) where \( S \) is the 2-element semilattice).

The first two items in the following theorem are simply translations of the respective items in Theorem 9.2; the other items are more specific to the idempotent case.

**Theorem 9.3.** Let \( A \) be a finite idempotent algebra. Then the following are equivalent.

1. For all structures \( \mathfrak{B} \) with finite relational signature and \( \text{Clo}(A) \subseteq \text{Pol}(B) \) we have \( \text{CSP}(\mathfrak{B}) \) can be solved by \((l,k)\)-consistency, for some \( l,k \in \mathbb{N} \).

2. For all structures \( \mathfrak{B} \) with \( \text{Pol}(\mathfrak{B}) = \text{Clo}(A) \) we have \((\{0, \ldots, p - 1\}; L_0, \ldots, L_{p-1}) \notin \text{H}(\text{PP}(\mathfrak{B})) \).

3. There is no homomorphism from \( \text{Clo}(A) \) to \( \text{Clo}(\{0, \ldots, p - 1\}; m) \) where \( m(x,y,z) := x - y + z \).

4. All algebras in \( \text{HSP}(A) \) have a meet-semi-distributive congruence lattice.
5. HSP(\(A\)) omits types 1 and 2 (in the sense of tame congruence theory which is an important part of universal algebra that has not been touched in this course).

A guide to references. The equivalence of 1. and 2. follows from the equivalence of the corresponding items in Theorem 9.2. The equivalence between 2. and 3. is easy but uses idempotency. The equivalence between 3., 4., and 5. is classic, and can be found in (Theorem 8.1, (1) \(\Leftrightarrow\) (10) and Theorem 9.10).

In the following we point out some immediate consequences of Theorem 9.2.

**Corollary 9.4.** Let \(H\) be a finite digraph. Then strong path consistency solves CSP(\(H\)) if and only if \(H\) has weak near unanimity polymorphisms \(f\) and \(g\) satisfying

\[
\forall x, y. g(y, x, x) = f(y, x, x)
\]

Another remarkable Corollary is that for the \(H\)-colouring problem, \((2, 3)\)-consistency is as powerful as \((2, k)\)-consistency for all \(k \geq 3\) (we already stated this in Theorem 3.1). One technical step of the proof of Theorem 9.2 is to reduce the argument to an argument about the strength of \((2,3)\)-consistency, essentially via the following proposition.

**Proposition 9.5** (From [4].) Let \(\mathfrak{B}\) be a relational structure whose relations have arity at most \(k\). Then there is a binary relational structure \(\mathfrak{A}\) with domain \(B^k\) such that \(\text{Pol}(\mathfrak{B})\) and \(\text{Pol}(\mathfrak{A})\) are isomorphic.

**Proof.** First we replace every relation \(R\) in \(\mathfrak{B}\) of arity \(l < k\) by the \(k\)-ary relation

\[
\{(r_1, \ldots, r_l, b_{l+1}, \ldots, b_k) \mid (r_1, \ldots, r_l) \in R, b_{l+1}, \ldots, b_k \in B\}.
\]

This clearly does not change the set of polymorphisms of \(\mathfrak{B}\), and therefore we may assume that every relation in \(\mathfrak{B}\) has arity precisely \(k\).

Next we introduce the relations in \(\mathfrak{A}\). For every \(k\)-ary relation \(R\) in \(\mathfrak{B}\) we introduce in \(\mathfrak{A}\) the unary relation \(R\) (on \(A = B^k\)), and for all \(i, j \in \{1, k\}\) we add a binary relation \(S_{i,j}\) defined as

\[
S_{i,j} := \{((u_1, \ldots, u_k), (v_1, \ldots, v_k)) \mid u_i = v_j\}.
\]

Let \(f \in \text{Pol}(\mathfrak{B})\) be arbitrary of arity \(n\). Define the function \(\bar{f}: A^n \to A\) by

\[
\bar{f}((u_1^1, \ldots, u_k^1), \ldots, (u_1^n, \ldots, u_k^n)) := (f(u_1^1, \ldots, u_k^1), \ldots, f(u_1^n, \ldots, u_k^n)).
\]

Since the relation \(S_{i,j}\), viewed as a \(2k\)-ary relation over \(B\), is primitively positively definable in \(\mathfrak{B}\), it is preserved by \(f\). Therefore it is easy to see that \(\bar{f}\) preserves \(S_{i,j}\). Analogously, it can be verified that \(\bar{f}\) preserves the unary relations of \(\mathfrak{A}\).

Now suppose that \(h: A^n \to A\) is a polymorphism of \(\mathfrak{A}\). Let \(h_i: (B^k)^n \to B\) be the function where \(h_i((u_1^1, \ldots, u_k^1), \ldots, (u_1^n, \ldots, u_k^n))\) is defined to be the \(i\)-th component of the tuple

\[
h((u_1^1, \ldots, u_k^1), \ldots, (u_1^n, \ldots, u_k^n)) \in B^k.
\]

Since \(h\) preserves \(S_{i,i}\), we have that

\[
h_i((u_1^1, \ldots, u_k^1), \ldots, (u_1^n, \ldots, u_k^n)) = h_i((v_1^1, \ldots, v_k^1), \ldots, (v_1^n, \ldots, v_k^n))
\]
whenever $u_l^i = v_l^i$ for all $l \in \{1, \ldots, n\}$. Hence, $h_i$ depends only on $u_1^i, \ldots, u_n^i$, and thus there exists an $n$-ary operation $f_i$ on $B$ such that $h_i((u_1^i, \ldots, u_n^i), \ldots, (u_1^i, \ldots, u_n^i)) = f_i(u_1^i, \ldots, u_n^i)$. Note that $f_i$ is a polymorphism of $\mathfrak{B}$.

Now, let $i, j \in \{1, \ldots, k\}$ be distinct. For any $u_1^1, \ldots, u_k^n \in A$ we choose arbitrarily $v_1^1, \ldots, v_k^n \in A$ such that $u_l^i = v_l^j$ for all $l \in \{1, \ldots, n\}$. Then

\[
\begin{align*}
  f_i(u_1^i, \ldots, u_n^i) &= h_i((u_1^i, \ldots, u_k^i), \ldots, (u_1^i, \ldots, u_k^i)) \\
  &= h_j((v_1^i, \ldots, v_k^i), \ldots, (v_1^i, \ldots, v_k^i)) \\
  &= h_j((u_1^j, \ldots, u_k^j), \ldots, (u_1^j, \ldots, u_k^j)) \\
  &= f_j(u_1^j, \ldots, u_k^j)
\end{align*}
\]

Therefore, $f := f_1 = f_2 = \cdots = f_k$. We have shown that $h = f$ for some $f \in \text{Pol}(\mathfrak{B})$, and the statement follows.

Similarly, one can show the following.

**Proposition 9.6.** For every structure $\mathfrak{A}$ with finite signature there is a binary relational structure $\mathfrak{B}$ such that $\text{PP}(\mathfrak{A}) = \text{PP}(\mathfrak{B})$.

**Proof.** For finite structures $\mathfrak{A}$, the theorem is a consequence of Proposition 9.5 using Birkhoff’s theorem (Theorem 7.9). But the statement also holds for arbitrary infinite structures, and the proof is similar to the proof of Proposition 9.5 (in particular, the same definition for the structure $\mathfrak{B}$ works).

## 10 Cyclic Polymorphisms

In this section, for several results that we present we do not give a proof.

### 10.1 Digraphs without Sources and Sinks

A *source* in a digraph is a vertex with no incoming edges, and a *sink* is a vertex with no outgoing edges. In this section we mention an important result about finite digraphs with no sources and no sinks. Note that undirected graphs $(V,E)$, viewed as directed graphs where for every $\{u,v\} \in E$ we have $(u,v) \in E$ and $(v,u) \in E$, are examples of such graphs.

**Theorem 10.1** (Barto, Kozik, Nieven [7]). Let $H$ be a digraph without sources and sinks. If $H$ has a Taylor polymorphism, then $H$ is homomorphically equivalent to a disjoint union of cycles.

**Proof.** The proof of this deep theorem is out of the scope of this course. An important part of the proof is using absorption theory, which has been developed for this theorem.

If a graph $H$ is homomorphically equivalent to a disjoint union of cycles, then $\text{CSP}(H)$ is in P (e.g., we can use the algorithm PC$_H$ to solve it; see Section 3). On the other hand, a digraph without a Taylor polymorphism has an NP-hard CSP. Therefore, Theorem 10.1 shows that the Feder-Vardi conjecture is true for digraphs without sources and sinks: their CSPs are in P or NP-complete.
10.2 Cyclic Terms

An operation \( c: A^n \to A \), for \( n \geq 2 \), is cyclic if it satisfies for all \( a_1, \ldots, a_n \in A \) that \( c(a_1, \ldots, a_n) = c(a_2, \ldots, a_n, a_1) \). Cyclic operations are weak near unanimity operations, and in particular Taylor operations; the converse is a deep result of Barto and Kozic (Theorem \[10.4\] below). When \( a = (a_0, a_1, \ldots, a_{k-1}) \) is a \( k \)-tuple, we write \( \rho(a) \) for the \( k \)-tuple \( (a_1, \ldots, a_{k-1}, a_0) \).

Definition 10.2. An \( n \)-ary relation \( R \) on a set \( A \) is called cyclic if for all \( a \in A^k \)

\[ a \in R \Rightarrow \rho(a) \in R. \]

Lemma 10.3 (from \[6\]). A finite idempotent algebra \( A \) has a \( k \)-ary cyclic term if and only if every nonempty cyclic subalgebra of \( A^k \) contains a constant tuple.

Proof. Let \( \tau \) be the signature of \( A \). For the easy direction, suppose that \( A \) has a cyclic \( \tau \)-term \( t(x_1, \ldots, x_k) \). Let \( a = (a_0, a_1, \ldots, a_{k-1}) \) be an arbitrary tuple in a cyclic subalgebra \( A \) of \( A^k \). As \( R \) is cyclic, \( \rho(a), \ldots, \rho^{k-1}(a) \in R \), and since \( R \) is a subalgebra, \( b := t^A(a, \rho(a), \ldots, \rho^{k-1}(a)) \in R \). Since \( t \) is cyclic, the \( k \)-tuple \( b \) is constant.

To prove the converse direction, we assume that every nonempty cyclic subalgebra of \( A^k \) contains a constant tuple. For a \( \tau \)-term \( f(x_0, x_1, \ldots, x_{k-1}) \), let \( S(f) \) be the set of all \( a \in A^k \) such that \( f^A(a) = f^A(\rho(a)) = \cdots = f^A(\rho^{k-1}(a)) \). Choose \( f \) such that \( |S(f)| \) is maximal (here we use the assumption that \( A \) is finite). If \( |S(f)| = |A|^k \), then \( f^A \) is cyclic and we are done. Otherwise, arbitrarily pick \( a = (a_0, a_1, \ldots, a_{k-1}) \in A^k \setminus S(f) \). For \( i \in \{0, \ldots, k-1\} \), define \( b_i := f(\rho^i(a)) \), and let \( B := \{b, \rho(b), \ldots, \rho^{k-1}(b)\} \).

We claim that the smallest subalgebra \( C \) of \( A^k \) that contains \( B \) is cyclic. So let \( c \in C \) be arbitrary. Since \( C \) is generated by \( B \), there exists a \( \tau \)-term \( s(x_0, x_1, \ldots, x_{k-1}) \) such that \( c = s^A(b, \rho(b), \ldots, \rho^{k-1}(b)) \). Then \( \rho(c) = s^A(\rho(b), \rho^2(b), \ldots, \rho^{k-1}(b), b) \in C \), proving the claim.

According to our assumption, the algebra \( C \) contains a constant tuple \( d \). Then there exists a \( \tau \)-term \( r(x_0, \ldots, x_{k-1}) \) such that \( d = r^C(b, \rho(b), \ldots, \rho^{k-1}(b)) \). Note that

\[ r^A(b_0) = r^A(b_1) = \cdots = r^A(b_{k-1}) \]

since \( d \) is constant (also see Figure \[13\]). It follows that \( b \in S(r) \).

Now consider the \( \tau \)-term \( t(x_0, x_1, \ldots, x_{k-1}) \) defined by

\[ t(x) := r(f(x), f(\rho(x)), \ldots, f(\rho^{k-1}(x))) \].

Figure 13: Diagram for the proof of Lemma 10.3.
where \( x := (x_0, x_1, \ldots, x_{k-1}) \). We claim that \( S(f) \subseteq S(t) \), but also that \( a \in S(t) \). This is clearly in contradiction to the maximality of \( |S(f)| \). Let \( e \in S(f) \). Then
\[
t^A(\rho^i(e)) = r^A(f^A(\rho^i(e), f^A(\rho^{i+1}(e)), \ldots, f^A(\rho^{i-1}(e))))
\]
\[
= r^A(f^A(e), f^A(e), \ldots, f^A(e)) \quad \text{(since } e \in S(f) \text{)}
\]
\[
= f^A(e) \quad \text{(since } A \text{ is idempotent)}
\]
for all \( i \in \{0, \ldots, k-1\} \). Therefore, \( e \in S(t) \). On the other hand,
\[
t^A(\rho^i(a)) = r^A(f^A(\rho^i(a), f^A(\rho^{i+1}(a)), \ldots, f^A(\rho^{i-1}(a))))
\]
\[
= r^A(b_1, b_{i+1}, \ldots, b_{i-1})
\]
\[
= r^A(\rho^i(b))
\]
which is constant for all \( i \) by the choice of \( r \). Therefore, \( a \in S(t) \) and the contradiction is established.

\[\text{Theorem 10.4 (of [6]). Let } A \text{ be a finite algebra. Then the following are equivalent.}\]

\begin{itemize}
  \item \( A \) has a Taylor term;
  \item \( A \) has a cyclic term;
  \item for all prime numbers \( p > |A| \), the algebra \( A \) has a \( p \)-ary cyclic term.
\end{itemize}

\textbf{Proof.} The statement can be found for finite idempotent algebras in [6], but since a structure has a Taylorpolymorphism if and only if its core does (recall that in this text we do not require that Tayloroperations are idempotent), and since a core has a Taylorpolymorphism if and only if it has an idempotent Taylorpolymorphism, the idempotent case implies the statement as given in the theorem. Again, the full proof of this theorem is out of the scope of our course. We mention that Barto and Kozik use absorption theory [6] and explicitly use a strong version of Theorem 10.1.

As an application, we derive the classification of the complexity of \( H \)-colouring for finite undirected graphs \( H \) (Theorem 1.4).

\textbf{Proof.} If the core \( G \) of \( H \) equals \( K_2 \) or has just one vertex, then \( \text{CSP}(H) \) can be solved in polynomial time, e.g. by the Path Consistency Procedure, Section 5. Otherwise, \( G \) is not bipartite and there exists a cycle \( a_0, a_1, \ldots, a_{2k}, a_0 \) of odd length in \( H \). If \( H \) has no Taylor polymorphism, then by Corollary 7.21 \( \text{CSP}(H) \) is NP-hard.

Otherwise, if \( H \) has a Taylor polymorphism, then Theorem 10.4 asserts that there exists a \( p \)-ary cyclic polymorphism \( c \) of \( H \) where \( p \) is a prime number greater than \( \max\{2k, |A|\} \). Since the edges in \( H \) are undirected, we can also find a cycle \( a_0, a_1, \ldots, a_{p-1}, a_0 \) in \( H \). Then \( c(a_0, a_1, \ldots, a_{p-1}) = c(a_1, \ldots, a_{p-1}, a_0) \), which implies that \( H \) contains a loop, a contradiction to the assumption that the core of \( H \) has more than one element.

\[\]
10.3 Siggers Operations of Arity 4

Interestingly, whether a finite algebra has a Taylor term (equivalently: a weak near unanimity term, or a cyclic term) can be tested by searching for a single 4-ary term $s$ that satisfies

$$\mathbf{A} \models \forall x, y, z. s(x, y, z, y) = s(y, z, x, x),$$

a so-called 4-ary Siggers term. In particular, the question whether a given finite structure has a cyclic term is in the complexity class NP. Siggers originally found a 6-ary term (see Section 8.2), which has been improved later to the 4-ary term given above. The proof given below is from [36], where the authors also prove that the result is optimal in the sense that there is no equivalent characterisation using a single ternary Taylor term.

**Theorem 10.5** (due to [48]; see [36]). Let $\mathbf{A}$ be a finite algebra. Then $\mathbf{A}$ has a cyclic term if and only if $\mathbf{A}$ has a 4-ary Siggers term.

**Proof.** Suppose that $\mathbf{A}$ has a cyclic term. Let $p = 3k + 2$ be some prime number larger than $|\mathbf{A}|$ and let $c(x_1, \ldots, x_p)$ be a cyclic term of $\mathbf{A}$, which exists by Theorem 10.4. Define $s(x, y, z, w)$ to be the term

$$c(x, x, \ldots, x, y, \ldots, y, w, z, \ldots, z),$$

where the variable $x$ occurs $k + 1$ times, the variable $w$ occurs once, and the variables $y$ and $z$ occur $k$ times each. Then

$$s(x, y, z, y) = c(x, x, \ldots, x, y, \ldots, y, y, z, \ldots, z) \quad (k + 1 \text{ times } x, k + 1 \text{ times } y, k \text{ times } z)$$

$$= c(y, y, \ldots, y, z, z, \ldots, z, x, x, \ldots, x) \quad (\text{by cyclicity of } c)$$

$$= s(y, z, x, x).$$

Conversely, a Siggers term is a Taylor term, and therefore the other direction follows from Theorem 10.4. 

**References**


77


