Miniskript

DISMAT - Graph Homomorphisms[1,2]

Dozent: Prof. Bodirsky, M.
LaTeX: rydval.jakub@gmail.com
Version: August 6, 2017
Technische Universität Dresden

[1]Modul Math Ma DISMAT: Graph Homomorphisms
[2]Zusatzinhalt mit * gekennzeichnet

Contents

1 Basics

2 The H-colouring problem

Definition. Let H be a digraph. Then CSP $(H) := \{G \mid G$ finite digraph, $G \mapsto H\}$.

Definition. Let
- P be the class of all problems that can be solved in polynomial time,
- NP be the class of all problems whose solutions can be checked in polynomial time
- NP-hard be the class of all problems which have a polynomial-time reduction to any other NP problem
- NP-complete be the class of all problems which are NP and NP-hard

Example. Duality:
(1) $G \to \vec{P}_1 \iff \vec{P}_2 \nrightarrow G$.
(2) $\vec{P}_3 \nrightarrow G \iff G \to \vec{T}_3$.

2.1 Arc-consistency

Idea: Constraint propagation. Search for a node, where the list of possible values is empty.

Algorithm $AC_H(G)$**.** For solving CSP (H), H finite digraph

```
Input: finite digraph G
Data structure: L(x) ⊂ V(H) ∀x ∈ V(G)

  DO ∀x ∈ V(G):
    L(x) := V(H)
  DO WHILE list changes
    DO ∀(x, y) ∈ E(G):
      IF ∃u ∈ L(x)∄v ∈ L(y) : (u, v) ∈ E(H) THEN remove u from L(x)
      IF ∃v ∈ L(y)∄u ∈ L(x) : (u, v) ∈ E(H) THEN remove v from L(y)
      IF L(x) = ∅ reject
```

Observations:
- If $AC_H(G)$ rejects, then $G \nrightarrow H$
- Running time is linear in the size of the input
- AC cannot solve CSP $(\vec{C}_k)$

Claims. • CSP $(\vec{P}_k)$ *is solved by AC*
- CSP $(\vec{T}_k)$ *is solved by AC*
- CSP (K_k) *is not solved by AC*
- CSP $(\vec{C}_k)$ *is not solved by AC*

2.2 Power graph

Definition. The *power graph* $P(H)$ has non-empty subsets of $V(H)$ as vertices and an edge (S_1, S_2) iff

- for every $u \in S_1$, there is a $v \in S_2$ s.t. $(u, v) \in E(H)$
- for every $v \in S_S$, there is a $s \in S_1$ s.t. $(u, v) \in E(H)$

Lemma. *$AC_H(G)$ does not reject iff $G \to P(H)$.*

Proof. "$\Longrightarrow$": We show, that $x \mapsto L(x)$ is a homomorphism $G \to P(H)$. Let $(a, b) \in E(G)$, for each $u \in L(a)$, there is a $v \in L(b)$ s.t. $(u, v) \in E(H)$, for each $v \in L(b)$ there is $u \in L(a)$ s.t. $(u, v) \in E(H) \implies (L(a), L(b)) \in E(P(H))$. "$\Longleftarrow$": Let $h : G \to P(H)$. We show that $AC_H(G)$ never removes elements of $h(x)$ from $L(x)$. Suppose $(a, b) \in E(G)$, then $(h(a), h(b)) \in E(P(H))$. Then for each $u \in h(a) \exists v \in h(b)$ s.t. $(u, v) \in E(H)$, for each $v \in h(b) \exists u \in h(a)$ s.t. $(u, v) \in E(H) \implies u$ cannot be removed by $AC_H(G)$ from $L(x)$. □

Theorem (Feder, Vardi '93). *Let H be a finite digraph. T.f.a.e.:*

- *AC_H solves* CSP(H)
- $P(H) \to H$

Proof. "$\Longrightarrow$": $AC_H(G)$ does not reject G iff $G \to H$. By lemma above, $AC_H(P(H))$ does not reject, hence $P(H) \to H$. "$\Longleftarrow$": If $AC_H(G)$ does not reject, by lemma above, $G \to P(H)$, hence $G \to H$. □

2.3 Tree duality

Definition. A digraph H has *tree duality* iff there exists a set $\mathcal{N}$ of *orientations of trees* s.t. $G \to H$ iff $\forall T \in \mathcal{N} : T \nrightarrow G$.

Example. $\vec{P}_2$ has tree duality, where $\mathcal{N}$ is the set of *"zig-zag" graphs*, which is the set containing orientations of paths with exactly three levels.

Theorem. *AC_H solves* CSP(H) *iff H has tree duality.* □

2.4 Semilattice polymorphisms

Definition.
- A map $f : D^k \to D$ is called *totally symmetric* if $f(x_1, \dots, x_k) = f(y_1, \dots, y_k)$ whenever $\{x_1, \dots, x_k\} = \{y_1, \dots, y_k\}$.
- A map $f : D^2 \to D$ is called *semilattice operation* if
  - $f(x, x) = x$ (idempotent)
  - $f(x, y) = f(y, x)$ (commutative)
  - $f(f(x, y), z) = f(x, f(y, z))$ (associative)

Example. $(x_1, \dots, x_k) \mapsto \min\{x_1, \dots, x_k\}$ is totally symmetric.

Theorem. *Let H be a finite digraph. T.f.a.e.:*

(1) $P(H) \to H$
(2) H *has for every* k *a totally symmetric polymorphism of arrity* n.
(3) H *has a totally symmetric polymorphism of arrity* $2|V^H|$.

Proof. □

Theorem. $P(H) \to H$ *iff* H *is homomorphic equivalent to a graph with semilattice polymorphism.*

Remark. *T.f.a.e.:*

- $P(H) \to H$
- H *has tree duality*
- H *has totally symmetric polymorphism for all arities*
- H *is homomorphic eq. to a graph with a semilattice polymorphism*

Non-example. All polymorphisms of K_3 are of the form $(x_1, \ldots, x_n) \mapsto f(x_i)$ for some $i \in \{1, \ldots, n\}$, $f \in S_3$.

2.5 Path-consistency

Algorithm $PC_H(G)$**.** For solving CSP(H), H finite digraph

```
Input: finite digraph G
Data structure: L(x,y) ⊂ V(H)^2 ∀(x,y) ∈ V(G)^2

  DO ∀(x,y) ∈ V(G)^2:
    IF (x,y) ∈ E(G) THEN L(x,y) := E(H) ELSE L(x,y) := V(H)^2
  DO WHILE list changes
    DO ∀x,y,z ∈ V(G):
      DO ∀(u,v) ∈ L(x,y):
        IF ∄w ∈ V(H): (u,w) ∈ L(x,z) ∧ (w,v) ∈ L(z,y) THEN remove (u,v) from
          L(x,y)
        IF L(x,y) = ∅ reject
```

Observations:

- If $PC_H(G)$ rejects, then $G \nrightarrow H$
- Running time is cubic in the size of the input
- If AC_H solves CSP(H), then PC_H does too, since we also have lists $L(x,x)$
- PC cannot solve CSP(K_3) since $K_4 \nrightarrow K_3$ but PC cannot decide

2.6 Majority operations

Definition. Operation $f : G^3 \to G$ is called *majority* if $\forall x, y \in D : f(x,x,y) = f(x,y,x) = f(y,x,x) = x$.

Examples. • Let $f:(\vec{C}_k)^3 \to \vec{C}_k$ be the majority satisfying $f(x,y,z)=x$ if $|\{x,y,z\}|=3$.

- Let $f:(\vec{T}_k)^3 \to \vec{T}_k$ be the median majority (always returns the middle element) $f(x,y,z) := \min\{\max(x,y), \max\{y,z\}, \max\{x,z\}\}$

Lemma. *Let f be a k-ary polymorphism of H, G finite digraph, $x,y \in V(G)$, $L(x,y)$ be the list of (x,y) at the end of $PC_H(G)$. Then L is preserved by f.*

Proof. We show by induction over the execution of $PC_H(G)$, that $\forall x,y \in V(H)$ at all times, if $(u_1,v_1),...,(u_k,v_k) \in L(x,y)$, then $(f(u_1,...,u_k), f(v_1,...,v_k)) \in L(x,y)$. If $(x,y) \notin E(G)$.

IB Obvious, since f is a polymorphism

IS Let $x,y,z \in V(G)$, $(u_1,v_1),...,(u_k,v_k) \in L(x,y)$ be arbitrary. From last step: $\forall i \in \{1,...,k\} \exists w_i : (u_i,w_i) \in L(x,z) \wedge (w_i,v_i) \in L(z,y)$. By induction assumption, $(f(u_1,...,u_k), f(w_1,...,w_k)) \in L(x,z) \wedge (f(w_1,...,w_k), f(v_1,...,v_k)) \in L(z,y)$. Hence, $(f(u_1,...,u_k), f(v_1,...,v_k))$ will not be removed from $L(x,y)$. □

Theorem. *PC_H solves* CSP(H) *if H has a majority polymorphism.*

Proof. Let $f: H^3 \to H$ be a majority polymorphism and G instance of CSP(H). Suppose $L(x,y) \neq \emptyset \forall (x,y) \in V(G)^2$ when $PC_H(G)$ terminates. To show: $\exists h: G \to H$. We show by induction on i that every $h: G' \to H$ homomorphism from G' induced subgraph of G on i vertices which preserves $L(x,y)$ can be extended to any other vertex of G.

IB Let $x_1,x_2,x_3 \in G$ be arbitrary and $h: \{x_1,x_2\} \to H$ homomorphism s.t. $(h(x_1),h(x_2)) \in L(x_1,x_2)$. It can be extended to x_3 s.t. $(h(x_1),h(x_3)) \in L(x_1,x_3)$ and $(h(x_3),h(x_2)) \in L(x_3,x_2)$, ow. $PC_H(G)$ would have removed $(h(x_1),h(x_2))$ from $L(x_1,x_2)$.

IS Let $h': G' \to H$ be a homomorphism that preserves lists, $x \in G \setminus G'$. Let $x_1,x_2,x_3 \in G'$, $h'_j := h|_{G' \setminus \{x_j\}}$. By induction assumption, h'_j can be extended to x s.t. the resulting homomorphism h_j preserves the lists. We show that the extension h of h' which maps x to $f(h_1(x),h_2(x),h_3(x))$ is a homomorphism that preserves the lists. To show: wlog $\forall y \in V(G')$: $(h(x),h(y)) \in L(x,y)$.
If $y \notin \{x_1,x_2,x_3\}$, then

$$h(y) = h'(y) = f(h'(y),h'(y),h'(y)) = f(h_1(y),h_2(y),h_3(y)).$$

Since $(h_i(x),h_i(y)) \in L(x,y) \forall i$ and f preserves $L(x,y)$ by the last lemma, we have $(h(x),h(y)) \in L(x,y)$.
If $y \in \{x_1,x_2,x_3\}$, then wlog suppose $y = x_1$. Then $\exists v \in H$ s.t. $(h_1(x),v) \in L(x,y)$, ow. $PC_H(G)$ would have removed $(h_1(x),h_1(x_2))$. We have

$$h(y) = h'(y) = f(v,h'(y),h'(y)) = f(v,h_2(y),h_3(y)).$$

Since $(h_1(x),v),(h_2(x),h_2(y)),(h_3(x),h_3(y)) \in L(x,y)$, the lemma above implies $(h(x),h(y)) \in L(x,y)$.

□

2.7 Relational Structures

- More general than digraphs.
- New phenomena: e.g. exist structures with Maltsev polymorphisms but no majority polymorphisms.
- Arise naturally even if we are only interested in digraphs.

Example. "Precoloured" H-Colouring. Input: finite digraph G, partial map $p : V(G) \to V(H)$. Question: does p have an extension to a homomorphism from G to H? Future observation: it is easy to adapt arc/path-consistency algorithms to precoloured H-colouring.

Definition. Let the *signature* $\tau = \{R_1, R_2, ...\}$ be a set of symbols R_i of arrity $k_i \in \mathbb{N}$. A *relational τ-structure $\underline{A}$* consists of a domain A and a relation $R_i^{\underline{A}} \subseteq A^{k_i}$ for each relational symbol $R_i \in \tau$ of arrity k_i.

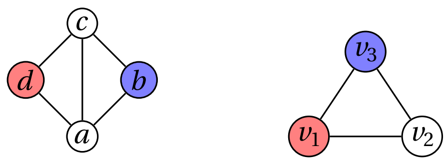
Definition. Let $\underline{A}, \underline{B}$ be τ-structures, $h : A \to B$ is called a homomorphism if for all $R \in \tau$:

$$(a_1, ..., a_k) \in R^{\underline{A}} \implies (h(a_1), ..., h(a_k)) \in R^{\underline{B}}.$$

A homomorphism from $\underline{A}$ to $\underline{A}$ is called an *Endomorphism*. An injective endomorphism which also preserves complements of all relations is called *embedding*.

Definition. Let $\underline{A}$ be a τ-structure. Then CSP $(\underline{A}) = \{\underline{B} \mid \underline{B}$ finite τ-structure s.t. $\underline{B} \to \underline{A}\}$.

Example. $H = (\{v_1, ..., v_n\}, E)$. Precolored problem: CSP $\big((\{v_1, ..., v_n\}; E, \{v_1\}, ..., \{v_n\})\big)$. Concrete example:



We consider $(\{a, b, c, d\}; \{\{a, b\}, ...\}, \{d\}, \emptyset, \{b\})$ as input to CSP $(\underline{A})$.

2.8 Primitive Positive Formulas

Definition. A τ-formula is a formula $\phi(x_1, ..., x_n)$ of the form $\exists x_{n+1}, ..., x_l(\psi_1 \wedge ... \wedge \psi_m)$, where ψ_i are *atomic*, i.e. of the form

- $R(y_1, ..., y_k)$, $R \in T$ of arity k, $y_1, ..., y_k \in \{x_1, ..., x_l\}$
- $y = y'$ for $y, y' \in \{x_1, ..., x_l\}$
- $\perp$ for the constant *false*.

Example. $\tau = \{E\}$, $\phi(x, y) := \exists u_1, u_2 E(x, u_1) \wedge E(u_1, u_2) \wedge E(u_2, y)$. Then $(V, E) \models \varphi(a, b)$ iff there is a path from a to b in (V, E) of length 3. For ex. $C_5 \models \varphi(a, b)$ iff $a \neq b$.

Definition. Let $\underline{B}$ be a structure with finite relational signature. Then CSP $(\underline{B})$ is the computational problem of deciding whether a given p.p. τ-sentence ϕ is true in $\underline{B}$. The p.p. τ-sentence ϕ is called an *instance* of CSP $(\underline{B})$.

3 Logic

3.1 From Structures to Formulas

Definition. To a finite τ-structure $\underline{A}$, we can associate a unique p.p. τ-formula called the *canonical conjunctive query* $\phi(\underline{A})$. Variables are the elements of $\underline{A}$, all existentially quantified (such formulas without free variables are called *sentences*), conjuncts $R(a_1,...,a_k)$ for $R \in \tau$, k-ary s.t. $(a_1,...,a_k) \in R^{\underline{A}}$.

Example. $\phi(K_3) = \exists u \exists v \exists w : E(u,v) \wedge E(v,u) \wedge E(v,w) \wedge E(w,v) \wedge E(u,w) \wedge E(w,u)$.

Proposition. *$\underline{A}$ finite τ-structure, $\underline{B}$ a τ-structure. Then $A \to B$ iff $B \models \phi(\underline{A})$.* $\square$

3.2 From Formulas to Structures

Definition. Let ϕ be a p.p.-formula, w.l.o.g. without $=, \perp$. Define the canonical structure $\underline{S}(\phi)$ as the τ-structure with domain consisting of all variables of ϕ and relations given by $(a_1,...,a_k) \in R^{\underline{S}(\phi)}$ iff $R(a_1,...,a_k)$ is conjunct in ϕ.

Proposition. *Let $\underline{B}$ be a τ-structure, ϕ p.p.-τ-sentence other than $\perp$. Then $\underline{B} \models \phi$ iff $\underline{S}(\phi) \to \underline{B}$.* $\square$

3.3 Primitive Positive Definability

Definition. If $\underline{A}$ a τ-structure, $\phi(x_1,...,x_k)$ a τ-formula. Then

$$\phi^{\underline{A}} := \{(a_1,...,a_k) \mid \underline{A} \models \phi(a_1,...,a_k)\}$$

is *the relation defined* by ϕ over $\underline{A}$.

Lemma. *$\underline{A}$, $\underline{B}$ relational structures s.t. $A = B$. Suppose all relations of $\underline{A}$ are p.p.-definable in $\underline{B}$. Then there is a polynomial-time reduction from* CSP $(\underline{A})$ *to* CSP $(\underline{B})$.

In particular:
- CSP $(\underline{B}) \in P \implies$ CSP $(\underline{A}) \in P$.
- CSP $(\underline{A})$ NP-hard $\implies$ CSP $(\underline{B})$ is NP-hard.

Proof. Let τ,σ be the signatures of $\underline{A}$, $\underline{B}$ respectively, ϕ a τ-sentence.
1. Replace each conjunct $R(y_1,...,y_k)$ in ϕ by $\psi(y_1,...,y_k)$, where ψ is the p.p.-definition of R over $\underline{B}$.
2. For each conjunct of the form $y = y'$, remove y' from the quantifier prefix and replace all occurrences of y' by y.
3. Rewrite formula to a p.p.-sentence by pulling out all quantifiers. Resulting formula: ϕ'.

Claim 1. $\underline{A} \models \phi \iff \underline{B} \models \phi'$.

Claim 2. *ϕ' can be computed in linear time from ϕ.*

□

Corollary. CSP (C_5) *is* NP*-hard.*

Proof. CSP (K_5) is NP-hard. E^{K_5} is p.p. definable in C_5. Claim follows by the lemma above. □

3.4 Cores

Definition. A structure $\underline{A}$ is called a *core* iff all its endomorphism are embeddings.

Proposition. *For finite structure* $\underline{A}$*, t.f.a.e.:*

1. $\underline{A}$ *is a core*
2. *All endomorphisms of* $\underline{A}$ *are injective.*
3. *All endomorphisms of* $\underline{A}$ *are surjective.*
4. *All endomorphisms of* $\underline{A}$ *are automorphisms.* □

Remark. None of these are necessarily equivalent for infinite $\underline{A}$. Counterexamples:

- $(\mathbb{N};<)$ and a map which moves everything except 0 by one to the left for 2 $\not\Leftrightarrow$ 1.
- $(\mathbb{Z};2\mathbb{Z})$ and $x \mapsto 2x$ for 3 $\not\Leftrightarrow$ 1.
- $(\mathbb{Z};\{(x,x+1) \mid x \in \mathbb{Z}\},\{(x,x+2) \mid x \in \mathbb{N}\}$ and $x \mapsto x+c$ for 2,3 $\not\Leftrightarrow$ 4.

Theorem. *Every finite relational structure* $\underline{B}$ *is homomorphically equivalent to a core, the core* $\underline{C}$ *is unique up to isomorphisms.*

Proof. For existence, pick a $e \in End(\underline{B})$ of minimal range. Then the substructure of $\underline{B}$ induced by $e(B)$ is a core, homomorphically equivalent to $\underline{B}$ via inclusion. For uniqueness, let $\underline{C}_1, \underline{C}_2$ be cores of $\underline{B}$. Let $e_i : B \to C_i$ and $f_1 := e_1|_{V(C_2)}, f_2 := e_2|_{V(C_1)}$. Claim is that $\underline{C}_2$ and $\underline{C}_1$ are isomorph via f_1. Suppose there exist $x, y \in V(C_2)$ s.t. $f_1(x) = f_2(y)$. Then $f_2 \circ f_1$ is not injective. This contradicts $\underline{C}_2$ being a core since $f_2 \circ f_1 \in End(\underline{C}_2)$. Similarly: f_2 is injective, C_1, C_2 both finite, hence $|C_1| = |C_2|$. Furthermore, $\exists n \in \mathbb{N}$ s.t. $(f_2 \circ f_1)^n = \text{id}$, thus $(f_1)^{-1} = (f_2 \circ f_1)^{n-1} \circ f_2$ is a homomorphism. □

3.5 Orbits

Proposition. *In a finite core* $\underline{C}$*, all orbits are p.p. definable.*

Proof. Let $C = \{c_1, ..., c_n\}$. Let $\psi_{c_1}(c_1)$ be the canonical conjunctive query except for the variable c_1 not being existentially quantified. Obviously, $\underline{C} \models \psi_{c_1}(c_1) \implies \forall \alpha \in \text{Aut}(\underline{C})$ is $\underline{C} \models \psi_{c_1}(\alpha(c_1))$. Suppose that $c_1' \in C$ s.t. $\underline{C} \models \psi_{c_1}(c_1')$. Let $c_2', ..., c_n' \in C$ be witnesses showing that $\underline{C} \models \psi_{c_1}(c_1')$. Then the map $c_i \mapsto c_{i'}$ is an endomorphism of $\underline{C}$, and also an automorphism since $\underline{C}$ is a finite core. Hence ψ_{c_1} defines orbit of c_1 in $\text{Aut}(\underline{C})$. □

Proposition. *If* $\underline{A}$ *is a finite core, then* CSP $(\underline{A})$ *and* CSP $(\underline{A}, \{a_1\}, ..., \{a_n\})$ *are linear-time equivalent.*

Proof. Let $\tau, \tau' = \tau \cup \{R_{a_1}, ..., R_{a_n}\}$ be the signatures of $\underline{A}$, $(\underline{A}, \{a_1\}, ..., \{a_n\})$, respectively. Let ϕ be a p.p τ'-sentence. If $R_{a_i}(x_1), ..., R_{a_i}(x_k)$ are conjuncts of ϕ, replace all occurences of $x_2, ..., x_k$ by x_1 in ϕ. Next, replace $R_{a_i}(x)$ by $\psi_{a_i}(x)$, where ψ_{a_i} is p.p definition of orbit of a_i over $\underline{A}$. Rewrite the resulting formula to a p.p τ-sentence ψ. Now $\underline{A} \models \psi$ iff $(\underline{A}, \{a_1\}, ..., \{a_n\}) \models \phi$. □

3.6 Polymorphisms and p.p. definability

Which relations R are p.p. definable in $\underline{A}$?

Lemma. *Let $\underline{A}$ be a structure and $R \subseteq A^k$ s.t. R is p.p. definable in $\underline{A}$. Then R is preserved by all polymorphisms of $\underline{A}$.*

Proof. Suppose that $\psi(x_1, ..., x_k)$ is a p.p. definition of R. Let $f \in \mathrm{Pol}(\underline{A})$ be n-ary. Let $t_1, ..., t_n \in R$. We have to show $f(t_1, ..., t_n) \in R$. We know: $\underline{A} \models \psi(t_i)$. Let $x_{k+1}, ..., x_l$ be existentially quantified variables of ψ. Let s_i be the extension of t_i that satisfies the quantifier-free part ψ' of ψ. Then since f is a polymorphism:

$$\underline{A} \models \psi'(f(s_1(1), ..., s_n(1)), ..., f(s_1(l), ..., s_n(l))).$$

Hence $\underline{A} \models \psi(f(s_1(1), ..., s_n(1)), ..., f(s_1(k), ..., s_n(k)))$. □

Theorem (Geiger '68, Boduszuk, Kalužnin, Kotov, Romov '69). *Let $\underline{A}$ be a finite structure. Then R is p.p. definable in $\underline{A}$ iff R is preserved by all polymorphisms of $\underline{A}$.*

Proof. If $R \subseteq A^k$ is preserved by $\mathrm{Pol}(\underline{A})$, then also by $\mathrm{Aut}(\underline{A})$. W.l.o.g. $R = O_1 \cup ... \cup O_\omega$, where O_i is an orbit of k-tuples of $\underline{A}$. Since $\underline{A}$ is finite, $\omega \in \mathbb{N}$. If $\omega = 0$, $\perp$ is a p.p. definition of $R = \emptyset$. For each $j \leq \omega$, fix a representative $a_j \in O_j$. Let $b_1, b_2, ..., b_m$ be an enumeration of A^ω s.t. $b_i = (a_1(i), ..., a_\omega(i))$ for all $i \in \{1, ..., k\}$. Let $\{q_1, ..., q_l\} := A^\omega \setminus \{b_1, ..., b_k\}$. Claim is that $\psi(b_1, ..., b_k) := \exists q_1, ..., q_l \, \phi(\underline{A}^\omega)$ is a p.p. definition of R. By assumption all homomorphisms from $\underline{A}^\omega$ to $\underline{A}$ preserve R. Therefore, they map $b_1, ..., b_k$ to tuple in R, so every tuple $(b'_1, ..., b'_k) \in A^k$ that satisfies ψ (represents a homomorphism $A^\omega \to A$, $b_i \mapsto b'_i$) is in R, since $a_i = (b_1(i), ..., b_k(i)) \in R \forall i$. Conversely, let $t \in R$, then $t \in O_j$ for some $j \leq \omega \implies$ there is $\alpha \in \mathrm{Aut}(\underline{A})$ s.t. $\alpha(a_j) = t$. The map $f(x_1, ..., x_\omega) := \alpha(x_j)$ is homomorphism $\underline{A}^\omega \to \underline{A}$, which shows that $\underline{A} \models \psi(t_1, ..., t_k)$. □

3.7 P.p. Interpretations and the CSP

Definition. A relational σ-structure $\underline{B}$ has a *primitive positive interpretation* I in a τ-structure $\underline{A}$ if $\exists d \in \mathbb{N}$, called the *dimension* of I, and

1. a p.p. τ-formula $\delta_I(x_1, ..., x_d)$ called the *domain formula*,
2. for each atomic σ-formula $\phi(y_1, ..., y_k)$ a primitive positive τ-formula $\phi_I(\underline{x}_1, ..., \underline{x}_k)$ ($\underline{x}_i$ d-tuples),
3. a surjective *coordinate map* $h : \{(a_1, ..., a_d) \in A^d \mid \underline{A} \models \delta_I(a_1, ..., a_d)\} \to B$,

such that for all atomic σ-formulas ϕ and all tuples $\underline{a}_i \in D_h$, $\underline{B} \models \phi(h(\underline{a}_1), ..., h(\underline{a}_k))$ iff $\underline{A} \models \phi_I(\underline{a}_1, ..., \underline{a}_k)$.

Lemma. *Let $\underline{A}$ be p.p. interpretable in $\underline{B}$. Then there is a polynomial-time reduction from* $\mathrm{CSP}(\underline{A})$ *to* $\mathrm{CSP}(\underline{B})$. □

Remark. Primitive positive interpretations can be composed: if $\underline{C}_1$ has a d_1-dimensional p.p. interpretation I_1 in $\underline{C}_2$, and $\underline{C}_2$ has an d_2-dimensional p.p. interpretation I_2 in $\underline{C}_3$, then $\underline{C}_1$ has a natural $(d_1 \cdot d_2)$-dimensional p.p. interpretation in $\underline{C}_3$, which we denote by $I_1 \circ I_2$. The coordinate map of $I_1 \circ I_2$ is defined by

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

Theorem (Hell-Nešetřil '90). *Let H be a finite undirected graph. Then either*

1. *H is bipartite (then* $\mathrm{CSP}(H) \in P$*) or*
2. *H interprets every finite structure primitively positively, up to homomorphic equivalence (then* $\mathrm{CSP}(H) \in NP$*-complete).*

Definition. Let $\mathcal{C}$ be a class of finite structures.

1. $H(\mathcal{C})$ is the class of all finite structures which are homomorphic equivalent to some structure from $\mathcal{C}$.
2. $C(\mathcal{C})$ is the class of all structures obtained by expanding a core structure in $\mathcal{C}$ by singleton relations $\{a\}$.
3. $PP(\mathcal{C})$ is the class of all finite structures which interpretable in some structure from $\mathcal{C}$.

Let $\mathcal{D}$ be the smallest class containing $\mathcal{C}$ which is closed under H, C, PP.

Lemma. *All idempotent polymorphisms of K_3 are projections.* □

Consequence. *$R \subseteq (V(K_3))^k$ preserved by S_3. Then R is p.p. definable in K_3.*

Proof. Let $f \in \mathrm{Pol}(K_3)$. Then $\hat{f}(x) := f(x, ..., x)$ is a endomorphism of K_3. This implies $\hat{f} \in S_3$ since K_3 is a finite core. The map $g(x_1, ..., x_k) := (\hat{f})^{-1}(f(x_1, ..., x_n))$ is an idempotent polymorphism of K_3, thus a projection onto x_i for some $i \leq n$ by the lemma above, which means $f(x_1, ..., x_n) = \hat{f}(x_i)$. Thus f preserves R. Hence, R is p.p. definable. □

Theorem. *$PP(K_3)$ contains all finite structures.* □

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

Proof. Let $\underline{B} \in \mathcal{C}$ be a core, $c \in B$, $\underline{C} := (\underline{B}, \{c\})$. The orbit O of c is p.p. definable in $\underline{B}$. We give a 2-dimensional p.p. interpretation of a structure $\underline{A}$ with the same signature $\tau \cup \{R_c\}$ as $\underline{C}$. Let $R_c^{\underline{A}} := \{(a, a) \mid a \in O\}$ and for $R \in \tau$ and the arity of R is k then define

$$R^{\underline{A}} := \{((a_1, b_1), ..., (a_k, b_k)) \in (A^2)^k \mid (a_1, ..., a_k) \in R^{\underline{B}} \wedge b_1 = ... = b_k \in O\}.$$

Then $\underline{A}$ is homomorphic equivalent to $\underline{C} = (\underline{B}, \{c\})$:

1. $a \mapsto (a, c)$ is a homomorphism from $\underline{C}$ to $\underline{A}$
   - $(a_1, ..., a_k) \in R^{\underline{C}}$ for $R \in \tau \implies ((a_1, c), ..., (a_k, c)) \in R^{\underline{A}}$.

- $R_c^{\underline{C}} = \{c\}$ is preserved since $(c,c) \in R_c^{\underline{A}}$.

2. We will define a homomorphism h from $\underline{A}$ to $\underline{C}$. For every $a \in O$, fix $\alpha_a \in \mathrm{Aut}(\underline{B})$ s.t. $\alpha_a(a) = c$. Define $h(a,b) := \alpha_b(a)$ if $b \in O$, otherwise arbitrarily.
   - $R \in \tau$ k-ary, $t = ((a_1,b_1),\dots,(a_k,b_k)) \in R^{\underline{A}}$. Then $b_1 = \dots = b_k =: b \in O$ and we have that $h(t) = (\alpha_b(a_1),\dots,\alpha_b(a_k)) \in R^{\underline{C}}$ since α_b preserves $R^{\underline{B}}$. For $(a,a) \in R_c^{\underline{A}}$, we have $h(a,a) = \alpha_a(a) = c \in R_c^{\underline{C}}$. □

Theorem. $\mathcal{D} = H(PP(\mathcal{C}))$.

Proof. It is enough to show that $H(PP(\mathcal{C}))$ is closed under H, C, PP. □

Definition. 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. *Let G be a finite, non-bipartite graph. Then $H(PP(G))$ contains a diamond-free core with a K_3.*

Proof. We may assume:

1. $G' \in H(PP(G))$ not bipartite $\implies |G'| \geq |G|$, otherwise replace G with G'.
2. G contains a K_3. If not, let k be the length of the shortest cycle in G, $E(G)^{k-2}$ is p.p. definable in G and $G' := (V(G), E(G)^{k-2})$ contains a triangle.
3. Every vertex of G lies in a K_3. Otherwise, replace G by a subgraph defined by $\exists u,v(E(x,u) \wedge E(u,v) \wedge E(v,x))$.

Claim 1. G does not contain K_4. Otherwise, if $a \in V(G)$ lies in a K_4. The subgraph G' induced by $\{x \in V(G) \mid E(x,a)\}$ is not bipartite (contains K_3) and strictly smaller than G. A contradiction to our first assumption.

Claim 2. G is diamond-free. To see this, let R be defined as follows:

$$R(x,y) :\Longleftrightarrow \exists u,v(E(x,u) \wedge E(x,v) \wedge E(u,v) \wedge E(u,y) \wedge E(v,y))$$

and let T be the transitive closure of R. Then: T is reflexive (since every vertex lies in a triangle), obviously symmetric and transitive. Since G is finite, there exists $n \in \mathbb{N}$ s.t. $\exists u_1,\dots,u_n(R(x,u_1) \wedge R(u_1,u_2) \wedge \dots \wedge R(u_n,y))$ defines T. The factor graph G/T is not bipartite since $T \cap E = \emptyset$. Otherwise, let $(a,b) \in T \cap E$. Choose (a,b) s.t. the shortest sequence $a = a_0, a_1, \dots, a_n = b$ with $R(a_0,a_1) \wedge R(a_1,a_2) \wedge \dots \wedge R(a_{n-1},a_n)$ is the shortest possible. This sequence cannot be of the form $R(a_0,a_1)$ because G does not contain K_4.

- Suppose $n = 2k$. Let u_i and v_i be the top and bottom vertices in the diamond $R(a_{i-1},a_i)$. Let S be the set defined by

$$\exists x_1,\dots,x_k\big(E(u_{k+1},x_1) \wedge E(v_{k+1},x_1) \wedge R(x_1,x_2) \wedge \dots R(x_{k-1},x_k) \wedge E(x_k,x)\big).$$

  We observe that $a_0, u_1, v_1 \in S$ form a triangle. If $a_n \in S$ we obtain a contradiction to minimal choice of n. Hence the graph G' induced by p.p. definable set S is non-bipartite and $|G'| < |G|$. Contradiction to the first assumption.

- Suppose $n = 2k+1$, we can argue analogously with S defined by

$$\exists x_1, ..., x_k \big(E(u_{k+1}, x_1) \wedge E(v_{k+1}, x_1) \wedge R(x_1, x_2) \wedge ... R(x_{k-1}, x_k) \big)$$

  and again obtain a contradiction.

Hence, G/T is not bipartite. This implies that T is the trivial equivalence relation, which implies that G does not contain any diamonds. $\square$

Lemma. *Let G be diamond-free, $h : (K_3)^k \to G$ a homomorphism. Then: $h((K_3)^k) \cong (K_3)^m$ for some $m \leq k$.* $\square$

Lemma. *Let G be a finite graph with a K_3 subgraph, diamond-free, core. There is a $k \in \mathbb{N}$ s.t. $(K_3)^k \in PP(C(G))$.* $\square$

Remark: This implies $K_3 \in H(PP(G))$ by the first lemma, since $H(PP(C(G))) \subseteq H(PP(G))$.

Proof of the first lemma. Let $I = \{i_1, ..., i_l\} \subseteq \{1, ..., k\}$, $pr_I : \{0,1,2\}^k \to \{0,1,2\}^l$ defined via $pr_I := (x_{i_1}, ..., x_{i_l})$. Let $h : (K_3)^k \to G$ be a homomorphism. Choose $I \subseteq \{1, ..., k\}$ maximal such that $\ker(h) \subseteq \ker(pr_I)$ (i.e. if two elements have the same image, their coordinates must coincide on I. Such an I exists, since we can always choose $I := \emptyset \implies \ker(pr_\emptyset) = \{0,1,2\}^k$).

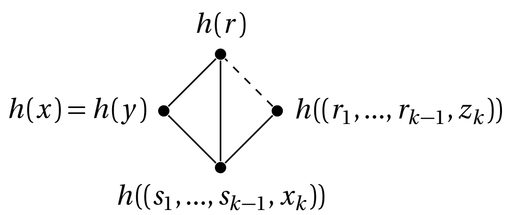
We need to prove: $\ker(h) = \ker(pr_I)$. For $j \notin I$ exist $x, y \in (K_3)^k$ such that $h(x) = h(y)$ but $x_j \neq y_j$. To show: for all $z_1, ..., z_k, z'_j \in \{0,1,2\}$:

$$h(z_1, ..., z_j, ... z_k) = h(z_1, ..., z'_j, ..., z_k),$$

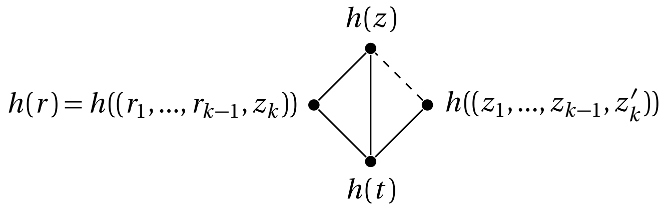
i.e. if we two elements only differ on a coordinate outside of I, the images under h still coincide ($\ker(pr_I) \subseteq \ker(h)$). We can w.l.o.g. assume that $z_j \neq x_j$, $z'_j = x_j$, and $j = k$. Now, the proof goes as follows:

- From exercises, we know that every two vertices of $(K_3)^k$ have a common neighbour. Let r be a common neighbour of x and z, then it also is a neighbour of $(z_1, ..., z_{k-1}, z'_k)$, since $z'_k = x_k$.
- For all $i \neq k$, choose $s_i \notin \{r_i, y_i\}$. Since $x_k \notin \{r_k, y_k\}$, $(s_1, ..., s_{k-1}, x_k)$ is a common neighbour of r and y.
- $(r_1, ..., r_{k-1}, z_k)$ is a common neighbour of x and $(s_1, ..., s_{k-1}, x_k)$.
- For all $i \neq k$, choose $t_i \notin \{z_i, r_i\}$, then choose $t_k \notin \{z_k, z'_k\}$. Then t is a common neighbour of z and $(z_1, ..., z_{k-1}, z'_k)$ and $(r_1, ..., r_{k-1}, z_k)$.

From the relations above imply that $h(r) = h(r_1, ..., r_{k-1}, z_k)$ since otherwise we would get a diamond



But this also implies $h(z) = h(z_1, ..., z_{k-1}, z'_k)$ since otherwise we would get a diamond



□

Proof of the second lemma. Let G be diamond-free with K_3 subgraph. We will construct a sequence of subgraphs $G_1 \subsetneq G_2 \subsetneq ...$ of G s.t. $G_i \cong (K_3)^{k_i}, k_i \in \mathbb{N}$. Let G_1 be the K_3 copy in G. Induction on i: Suppose G_i has already been defined. If $G_i \cong (K_3)^{k_i}$ is p.p definable in G, then we are done. Otherwise $\exists f \in \mathrm{Pol}(G)$ idempotent (since it preserves the singleton relations) s.t. $f(v_1, ..., v_n) \notin V(G_i)$ for $v_1, ..., v_k \in V(G_i)$, then $G_i \lneq f(G_i^k) =: G_{i+1}$ and $G_{i+1} \cong (K_3)^{k_{i+1}}$ for some k_{i+1} by the previous lemma. Since this chain is strictly increasing and G finite, the claim follows.

4 Universal algebra

Definition. • A τ-structure $\underline{A}$ s.t. τ only consists of functional symbols is called *algebra.*

- τ-*terms* are words of the form $f\, t_1 \cdots t_n$, where $f \in \tau$, n-ary and $t_1,\dots,t_n$ are τ-terms, the variables $x_1,\dots$ are always τ-terms.
- a *term operation* is an evaluation map $(t\, x_1 \cdots x_n)^{\underline{A}} : A^n \to A, (a_1,\dots,a_n) \mapsto t(a_1,\dots,a_n)$
- Let $\mathrm{Clo}(\underline{A})$ be the set of all term operations of $\underline{A}$, it contains all projections $(x_i)^{\underline{A}}$ and is closed under compositions. Hence it is a clone.
- Let $\underline{S}$ be a relational structure. An algebra $\underline{A}$ with s.t. $\mathrm{Clo}(\underline{A}) = \mathrm{Pol}(\underline{S})$ is called a *polymorphism algebra* of $\underline{S}$.

4.1 Operations on algebras

Definition. Let $\mathcal{C}$ be a class of τ-algebras.

1. $H(\mathcal{C})$ is the class of all homomorphic images of $\underline{A} \in \mathcal{C}$.
2. $S(\mathcal{C})$ is the class of all subalgebras of $\underline{A} \in \mathcal{C}$.
3. $P(\mathcal{C})$ is the class of all products of algebras from $\mathcal{C}$.
4. $P_{\mathrm{fin}}(\mathcal{C})$ is the class of all finite products of algebras from $\mathcal{C}$.

A class of τ-algebras $\mathcal{V}$ is called a *variety* resp. *pseudovariety* if it is closed under H, S, P resp. H, S, P_{fin}. Let $\mathcal{V}(\mathcal{C})$ resp. $\mathcal{V}_{\mathrm{fin}}(\mathcal{C})$ denote the smallest variety resp. pseudovariety which contains $\mathcal{C}$.

Proposition. $\mathcal{V}(\mathcal{C}) = HSP(\mathcal{C})$, $\mathcal{V}_{\mathrm{fin}}(\mathcal{C}) = HSP_{\mathrm{fin}}(\mathcal{C})$ □

Lemma. *Let $\underline{A}, \underline{B}$ be polymorphism algebras of $\underline{S}$, $\underline{T}$. Then $\underline{A} \in HSP(\underline{B})$ iff $\underline{S} \in PP(\underline{T})$.*

Proof. We only show the first implication. There $\exists \underline{C} \leq \underline{B}^d$ and $h : \underline{C} \to \underline{A}$. Construction of a p.p. interpretation of $\underline{S}$ in $\underline{T}$:

- All operations of $\underline{B}$ preserve $\underline{C}$ (seen as d-ary relation). By the BKKR Theorem, $\underline{C}$ has a p.p. definition $\psi(x_1,\dots,x_d) =: \delta_I(x_1,\dots,x_d)$ in $\underline{B}$.
- Choose h as the coordinate map. Let $f^{\underline{A}}$ be a operation of $\underline{A}$, $R^{\underline{S}}$ a relation of S. Then $R^{\underline{S}}$ is preserved by $f^{\underline{A}}$ which implies that $f^{\underline{B}}$ preserves $h^{-1}(R^{\underline{A}})$. Hence, polymorphisms of $\underline{T}$ preserve $h^{-1}(R^{\underline{S}})$, which yields $\phi(x_1,\dots,x_n) =: R(x_1,\dots,x_n)$, a p.p. definition of it in $\underline{T}$.
- $\ker h$ is a congruence of $\underline{C}$, hence it is, seen as a $2d$-ary relation over $\underline{B}$ preserved by all operations of $\underline{B}$. By BKKR, it has a p.p. definition in $\underline{T}$. This definition becomes the formula $=_I$ □

Corollary. Let $\underline{B}$ be a polymorphism algebra of $\underline{T}$, $\underline{A} \in HSP_{\mathrm{fin}}(\underline{B})$ s.t. $|A| = 3$ and all operations are unary, then $K_3 \in PP(\underline{T})$.

4.2 Identities

Let τ be a functional signature. A τ-sentence is called *universal conjunctive* if it is of the form $\forall x_1,\dots,x_n : \psi_1(\cdot) \wedge \dots \wedge \psi_m(\cdot)$, where $\psi_1,\dots,\psi_m$ are atomic.

Example. • Semilattice operation:

$$\forall x,y,z: f(x,y)=f(y,x)\wedge f(f(x,y),z)=f(x,f(y,z))\wedge f(x,x)=x.$$

- Majority operation.
- Maltsev operation.

Theorem (Birkhoff). *Let $\underline{A}, \underline{B}$ be finite τ-algebras. TFAE:*

(1) $\underline{A}\in HSP_{\text{fin}}(\underline{B})$.
(2) $\underline{A}\in HSP(\underline{B})$.
(3) *All universal conjunctive sentences, which are true in $\underline{B}$, are true in $\underline{A}$.*

Proof. Script. □

Consequence: $K_3\notin PP(\underline{T})$, $\underline{B}$ polymorphism algebra of $\underline{T}$. By the previous lemma, $HSP_{\text{fin}}(\underline{B})$ contains no polymorphism algebras $\underline{A}$ of K_3. Then $\exists$ universal conjunctive sentence ϕ which is true in $\underline{B}$ but not in $\underline{A}$.

4.3 Abstract clones

Definition. An (*abstract*) *clone* is a structure $\underline{C}=(C^{(0)},C^{(1)},\ldots;(\pi_i^k)_{1\le i\le k},(comp_l^k)_{k,l\ge1})$ where:

- $C^{(k)}$ are called the k-ary operations of $\underline{C}$
- π_i^k are constants in $C^{(k)}$ (the *projections*)
- $comp_l^k: C^{(k)}\times(C^{(l)})^k\to C^{(l)}$ is a operation of arity $k+1$

s.t.

$$\begin{aligned} comp_k^k(f,\pi_1^k,\ldots,\pi_k^k)&=f\\ comp_l^k(\pi_i^k,f_1,\ldots,f_k)&=f_i\\ comp_l^k(f,comp_l^m(g_1,h_1,\ldots,h_m),\ldots,comp_l^m(g_k,h_1,\ldots,h_m))&=\\ comp_l^m(comp_m^k(f,g_1,\ldots,g_k),h_1,\ldots,h_m).& \end{aligned}$$

4.4 Clone homomorphisms

Definition. $\underline{C}$, $\underline{D}$ clones, $\mu:\underline{C}\to\underline{D}$ *clone homomorphism* if

- $\mu(C^i)\subseteq D^{(i)}$
- $\mu((\pi_i^k)^{\underline{C}})=(\pi_i^k)^{\underline{D}}$, $i\le k$
- $\mu(comp(f,g_1,\ldots,g_n))=comp(\mu(f),\mu(g_1),\ldots,\mu(g_n))$, $f\in C^{(n)}$, $g_1,\ldots,g_n\in C^{(m)}$.

Example. • Every clone has a homomorphism into the clone of all functions on an singleton.

- All algebras $\underline{A}$ s.t. $|A|\ge2$, where all operations are projections, have isomorphic clones. These are denoted with $\underline{\text{Proj}}$. For ex. $\underline{\text{Proj}}=\text{Pol}(\{0,1,2\};\neq,\{0\},\{1\},\{2\})=\text{Pol}(\{0,1\};\{(0,0,1),(0,1,0),(1,0,0)\})$.

Addition to the Birkhoff's Theorem:

Theorem (Birkhoff). *Let $\underline{A}, \underline{B}$ be finite τ-algebras. TFAE:*

(1) $\underline{A} \in HSP_{\text{fin}}(\underline{B})$.
(2) $\underline{A} \in HSP(\underline{B})$.
(3) *All universal conjunctive sentences, which are true in $\underline{B}$, are true in $\underline{A}$.*
(4) $\mu : \mathrm{Clo}(\underline{B}) \to \mathrm{Clo}(\underline{A})$, $\mu(t^{\underline{B}}) := t^{\underline{A}}$ *is a well defined surjective clone homomorphism.*

Proof. μ is well defined $\iff (t^{\underline{B}} = s^{\underline{B}} \implies t^{\underline{A}} = s^{\underline{A}}) \iff$ (3). □

Consequence. *$\underline{S}$ finite structure. TFAE:*

(1) $\forall$ *finite structures* $\underline{T}$ $\exists$: $\underline{T} \in PP(\underline{S})$
(2) $K_3 = (\{0,1,2\}; \neq, \{0\}, \{1\}, \{2\}) \in PP(\underline{S})$
(3) $\mathrm{Clo}(\underline{B}) = \mathrm{Pol}(\underline{S}) \implies \exists \underline{A} \in HSP_{fin}(\underline{B})$ *s.t.* $\mathrm{Clo}(\underline{A}) = \underline{\mathrm{Proj}}$.
(4) $\exists \mu : \mathrm{Pol}(\underline{S}) \to \underline{\mathrm{Proj}}$ *clone homomorphism.*

Question: Which clones don't have a clone homomorphism to $\underline{\mathrm{Proj}}$.

Lemma. *$\underline{C}$ clone, $\underline{F}$ clone of finite algebra s.t. $\underline{C} \not\to \underline{F} \implies \exists$ p.p. τ-sentence which is true in $\underline{C}$ but not in $\underline{F}$ (τ signature of abstract clones).*

Proof. Let $\underline{E}$ be expansion of $\underline{C}$ by constants $c_e \forall e \in E$, $V := \{\psi$ atomic sentences $| \underline{E} \models \psi\}$, $U :=$ f.o. theory of $\underline{F}$. Suppose $\exists \underline{M} \models U \cup V$. Then the τ-reduct of restriction of $\underline{M}$ to $\bigcup_i M^{(i)}$ is isomorphic to $\underline{F}$ (since all f.o. sentences which completely describe $\underline{F}$ have to be true in this reduct), we identify it with $\underline{F}$.

For all constants c_e, $c_e^{\underline{M}} \in \underline{F}$. Since $\underline{M}$ satisfies all atomic formulas that hold in $\underline{E}$, we have that the $\mu : \underline{C} \to \underline{F}, e \mapsto c_e^{\underline{M}}$ is a clone homomorphism. Contradiction. So $U \cup V$ is unsatisfiable, then by compactness of first-order logic, $\exists V' \subseteq V$ finite s.t. $U \cup V'$ is unsatisfiable. Replace the constant symbols c_e in the sentences from V' with existentially quantified variables and let ψ be their conjunction. Then ψ is a p.p. sentence which is false in $\underline{F}$. □

4.5 Taylor terms

Definition. A *Taylor term* of a τ-algebra $\underline{B}$ is a τ-term $t(x_1, \ldots, x_n)$, $n \geq 2$ s.t. $\exists$ variables $(z_{i,j}), (z'_{i,j}) \in \{x, y\}^{n \times n}$, $z_{i,i} \neq z'_{i,i} \forall i$ and $\underline{B} \models \forall x, y \bigwedge_{i=1}^{n} \big(t(z_{i,1}, \ldots, z_{i,n}) = t(z'_{i,1}, \ldots, z'_{i,n})\big)$.

Example. • Semilattice operation $f(x, y) = f(y, x)$:

$$(z_{i,j}) := \begin{pmatrix} x & y \\ y & x \end{pmatrix}, \quad (z'_{i,j}) := \begin{pmatrix} y & x \\ x & y \end{pmatrix}$$

• Majority operation $f(x, y, x) = f(x, x, y) = f(y, x, x) \, (= x)$:

$$(z_{i,j}) := \begin{pmatrix} x & x & y \\ x & y & x \\ x & x & y \end{pmatrix}, \quad (z'_{i,j}) := \begin{pmatrix} y & x & x \\ y & x & x \\ x & y & x \end{pmatrix}$$

- Maltsev operation $f(x,x,y) = f(y,x,x) = f(y,y,y)\ (= y)$:

$$(z_{i,j}) := \begin{pmatrix} y & x & x \\ x & x & y \\ y & y & y \end{pmatrix}, \quad (z'_{i,j}) := \begin{pmatrix} x & x & y \\ y & y & y \\ y & x & x \end{pmatrix}$$

Theorem (Taylor; Hobby & McKenzie, Chapter 9). *Let $\underline{B}$ be an idempotent Algebra (i.e. all its operations are idempotent). TFAE:*

(1) $\mathrm{Clo}(\underline{B}) \twoheadrightarrow \underline{\mathrm{Proj}}$
(2) *$\underline{B}$ has a Taylor term.*

Proof. Script. □

Lemma. *Let $\underline{S} \in H(\underline{T})$. Then $\underline{T}$ has a Taylor polymorphism $\implies$ $\underline{S}$ has a Taylor polymorphism.*

Proof. Let $h : \underline{T} \to \underline{S}$, $g : \underline{S} \to \underline{T}$, $(x_1, ..., x_n) \mapsto t(x_1, ..., x_n)$ a Taylor polymorphism of $\underline{T} \implies (x_1, ..., x_n) \mapsto h(t(g(x_1), ..., g(x_n)))$ is a polymorphism and $\forall 1 \le i \le n$, $(z_{i,j}), (z'_{i,j}) \in \{x, y\}^{n \times n}$, $z_{i,i} \neq z'_{i,i}$: $h(t(g(z_{1,i}), ..., g(z_{n,i}))) = h(t(g(z'_{1,i}), ..., g(z'_{n,i})))$. □

Lemma. *Let $\underline{S} \in PP(\underline{T})$. Then $\underline{T}$ has a Taylor polymorphism $\implies$ $\underline{S}$ has a taylor polymorphism.*

Proof. By Birkhoff's Theorem, all universal conjunctive sentences which hold in $\mathrm{Pol}(\underline{T})$ also hold in $\mathrm{Pol}(\underline{S})$, since $\mathrm{Pol}(\underline{S}) \in HSP(\mathrm{Pol}(\underline{T}))$ by the Lemma at the beginning of this chapter. □

Lemma. *Let $\underline{S} \in C(\underline{T})$. Then $\underline{T}$ has a Taylor polymorphism $\implies$ $\underline{S}$ has a taylor polymorphism.*

Proof. First proof: let t be a Taylor polymorphism of $\underline{T}$, wlog. $\underline{T}$ core (ow. take a core of $\underline{T}$). The unary polymorphism $\hat{t}(x) := t(x, ..., x)$ has an inverse $\hat{t}^{-1} \in \mathrm{Pol}(\underline{T})$. Then $\hat{t}^{-1}(t(x_1, ..., x_n)) \in \mathrm{Pol}(\underline{S})$ is an indempotent Taylor polymorphism. Second proof: $C(\underline{T}) \subseteq H(PP(\underline{T}))$ □

Corollary. *Let $\underline{T}$ be a finite structure. Then t.f.a.e.:*

(1) $K_3 \notin H(PP(\underline{T}))$
(2) *$\underline{T}$ has a Taylor polymorphism.*

Proof. (2)$\implies$(1): Every structure $\underline{S} \in H(PP(\underline{T}))$ has a Taylor polymorphism. (1)$\implies$(2): Let $\underline{T}'$ be the core of $\underline{T}$, $\underline{C}$ be the expansion of $\underline{T}'$ with all constants, then $\underline{C} \in C(H(\underline{T})) \subseteq H(PP(\underline{T}))$. Thus $K_3 \notin PP(\underline{C})$, then $\mathrm{Pol}(\underline{C}) \twoheadrightarrow \underline{\mathrm{Proj}}$ by the consequence of Birkhoff's Theorem. Furthermore, $\mathrm{Pol}(\underline{C})$ idempotent. Then, by the Taylor's Theorem, $\mathrm{Pol}(\underline{C})$ contains a Taylor operation $\implies$ $\underline{T}'$ and $\underline{T}$ have a Taylor polymorphism. □

Corollary. *If $\underline{T}$ has no Taylor polymorphism $\implies$ $\mathrm{CSP}(\underline{T})$ is NP-hard.*

Theorem (Tractability Conjecture, Bulatov 2017). *If $\underline{T}$ has a Taylor polymorphism, then* $\mathrm{CSP}(\underline{T}) \in P$. □

Warning Examples.
- There are finite cores $\underline{T}$ s.t. $K_3 \in PP(C(\underline{T})) \subseteq H(PP(\underline{T}))$ but $K_3 \notin PP(\underline{T})$.
- There are finite structures $\underline{T}$ with impotent $\mathrm{Pol}(\underline{T})$ s.t. $PP(\underline{T}) \subsetneq H(PP(\underline{T}))$. I.e.: $\underline{T} := (\mathbb{Z}_2^2; R_{a,b})$ for $a, b \in \{0,1\}$, where

$$R_{a,b}^{\underline{T}} := \{(x, y, z) \in T^3 \mid x + y + z = (a, b).$$

  Let $\underline{T}'$ be a reduct of $\underline{T}$ with signature $\tau = \{R_{0,1}, R_{0,0}\}$. Then $\underline{S} \in H(\underline{T}')$ for a certain structure $\underline{S}$ with domain $S = \mathbb{Z}_2$. Furthermore $\underline{T}' \in PP(\underline{T})$, $\underline{S} \in H(PP(\underline{T})) \setminus PP(\underline{T})$.

Definition. Let $\underline{A}$ be an algebra, $s \in \mathrm{Clo}(\underline{A})$ is called *Siggers* if

$$\forall x, y, z : s(x, y, x, z, y, z) = s(y, x, z, x, z, y).$$

Proposition. *$\underline{T}$ has Siggers term iff $\underline{T}$ has Taylor term.*

Proof. We only prove one direction since any Siggers term is a Taylor term. Let $\underline{B}$ be a finite algebra with a Taylor term. Choose $k \in \mathbb{N}$, $a, b, c \in B^k$ s.t. $B^3 = \{(a_i, b_i, c_i) \mid i \leq k\}$. For $u, v \in B^k$, define $R(u, v) := \exists s \in \mathrm{Clo}(\underline{B}) : u = s(a, b, a, c, b, c) \wedge v = s(b, a, c, a, c, b)$. Then

- R is symmetric: if $R(u, v)$ via s, then $R(v, u)$ via $s'(x_1, x_2, x_3, x_4, x_5, x_6) := s(x_2, x_1, x_4, x_3, x_6, x_5)$
- Nodes a, b, c induce a K_3 in the graph $G := (B^k, R)$ via projections.
- R is preserved by $\mathrm{Clo}(\underline{B})$.
- G has Taylor polymorphism.

If $\exists u \in G : R(u, u)$, then $\underline{B}$ has Siggers. If not, then G is loopless, undirected, finite s.t. $K_3 \in H(PP(G))$. Contradiction to G having a Taylor polymorphism. □

5 Functions and Relations

5.1 Pol-Inv

Let O_B be the clone of all operations on B, R_B be the set of all relations of finite arity on B. Let $\underline{F} \subseteq O_B, \Phi \subseteq R_B$. Then

- $\mathrm{Inv}(F) := \{R \in R_B \mid \forall f \in F : f$ preserves $R\}$.
- $\mathrm{Pol}(\Phi) := \{f \in O_B \mid \forall R \in \Phi : f$ preseves $R\}$.
- $\langle F \rangle$ is the smallest clone containing F.
- $\langle \Phi \rangle$ is the smallest set of relations containing Φ which is closed under p.p. definability.

Lemma. (1) $\mathrm{Inv}\,\mathrm{Pol}\,\Phi = \langle \Phi \rangle$
(2) $\mathrm{Pol}\,\mathrm{Inv}\,F = \langle F \rangle$

Proof. Proof for (2): One inclusion is obvious. For the other: Let $f \in Pol\mathrm{Inv}\,F$ be k-ary, $B^k = \{b_1, ..., b_n\}$, $R := \{(g(b_1), ..., g(b_n)) \mid g \in \langle F \rangle\}$. Then:

- $R \in \mathrm{Inv}\,F \implies f$ preserves R.
- $(\pi_i^k(b_1), ..., \pi_i^k(b_n)) \in R$, since $\pi_i^k \in \langle F \rangle$

Previous points imply $(f(b_1), ..., f(b_n)) \in R \implies (f(b_1), ..., f(b_n)) = (g(b_1), ..., g(b_n))$ for some $g \in \langle F \rangle$. □

Definition. A map $f : B^k \to B$ *depends on the argument* i if $\exists r, s \in B^k$ s.t. $f(r) \neq f(s)$ but $\pi_j^k(r) = \pi_j^k(s) \forall j \in \{1, ..., n\} \setminus \{i\}$.

Lemma. *Let $f : B^k \to B$. Then t.f.a.e.:*

(1) *f is essentially unary, i.e. $\exists i \in \{1, ..., k\}, \tilde{f} : B \to B$ s.t. $f(x_1, ..., x_n) = \tilde{f}(x_i)$*
(2) *f preserves $P_B^3 := \{(x, y, z) \in B^3 \mid x = y \vee y = z\}$.*
(3) *f preserves $P_B^4 := \{(x, y, u, v) \mid x = y \vee u = v\}$*
(4) *f depends only on one argument*

Proof. Exercise. □

Example. $\mathrm{Pol}(K_n; \{1\}, ..., \{n\}) = \underline{\mathrm{Proj}} = \mathrm{Pol}(P^3_{\{1,...,n\}}, \{1\}, ..., \{n\})$.

5.2 Minimal clones

Definition. A clone $F \subseteq O_B$ is called

- *trivial* if $F \cong \underline{\mathrm{Proj}}$
- *minimal* if $\tilde{F} \subset F$ a non-trivial clone $\implies \tilde{F} = F$.

An operation $f \in O_B$ is called *minimal* if $\langle f \rangle$ is minimal and f is of minimal arity (implies that every g generated by f is a projection or generates f).

Lemma. *Every non-trivial clone F contains a minimal operation.*

Proof. Consider any strict decreasing chain of non-trivial clones $F \supset F_1 \supset F_2 \supset \ldots$. The set $\bigcup_{i\geq 1} \operatorname{Inv}(F_i)$ is closed under p.p. definability. Thus $F_i \supseteq \operatorname{Pol} \bigcup_{i\geq 1} \operatorname{Inv}(F_i)$ for all i. It also does not contain the relations $R_B^3, \{b_1\}, \ldots, \{b_n\}$, otherwise, these would be contained in some $\operatorname{Inv} F_i$, since the chain is strictly decreasing—contradiction to minimality. Hence, $\operatorname{Pol} \bigcup_{i\geq 1} \operatorname{Inv}(F_i)$ is a non-trivial lower bound of this chain. By Zorn's Lemma, this partial order contains a minimal element, which is generated by a minimal operation. □

Definition. A map $f : B^k \to B$ is called a *semiprojection* if $f(x_1, \ldots, x_k) = x_i$ if $|\{x_1, \ldots, x_k\}| < k$.

Theorem (Rosenberg's 5 types). *Every minimal operation on a finite B is one of these:*

(1) *f is unary and $f(f(x)) = x$ or $f(f(x)) = f(x)$.*
(2) *f is binary and $f(x, x) = x$.*
(3) *f is Maltsev*
(4) *f is majority*
(5) *f is a semiprojection of arity less than $|B|$*

Lemma (Swierczkowski). *Let f be a k-ary operation s.t. the outcome of identifying of any two arguments is a projection. Then f is a semi-projection.* □

Proof of last Theorem. Nothing to prove if f is unary or binary. Let f be ternary. By minimality of f, $f_1(x, y) := f(y, x, x)$, $f_2(x, y) := f(x, y, x)$, $f_3(x, y) := f(x, x, y)$ are projections. We consider all 8 possible cases:

$(f_1, f_2, f_3)(x, y)$	resulting type
(x, x, x)	f is majority
(x, x, y)	f is 3rd semi-projection
(x, y, x)	f is 2nd semi-projection
(y, x, x)	f is 1st semi-projection
(y, x, y)	f is Maltsev
(x, y, y)	$g(x, y, z) := f(y, x, z)$ is Maltsev
(y, y, x)	$g(x, y, z) := f(x, z, y)$ is Maltsev
(y, y, y)	f is minority, thus Maltsev

Let f be k-ary for $k \geq 4$. By minimality of f, the outcomes of identifying variables are projections. By the lemma of Swierczkowski, f is a semi-projection. □

Theorem (Post '41). *The minimal operations $f : \{0, 1\}^k \to \{0, 1\}$ are*

(1) *The unary constant functions*
(2) *The negation $\neg$*
(3) $(x, y) \mapsto \min\{x, y\}, (x, y) \mapsto \max\{x, y\}$
(4) *Minority*
(5) *Majority*

Proof. Trivial for f unary. If f is binary, $\hat{f}(x) := f(x, x) = x \implies f$ is idempotent $\implies$ 4 possibilities, 2 of them are projections, 2 maximum and minimum. If f is k-ary for

$k \geq 3$, then we get some of the Rosemberg's types and semi-projections on $\{0,1\}$ are projections. □

Lemma. *The minimal operations which are Maltsev, are minorities $f(x,y,x) = y$.*

Proof. Suppose $f(x,y,x) = x$. Consider $g(x,y,z) := f(x, f(x,y,z), z)$. Then we have $g(x,x,y) = f(x,y,y) = x$, $g(x,y,x) = f(x,x,x) = x$ and $g(y,x,x) = f(y,y,x) = x$. Contradiction to f being minimal since g cannot generate f and is no projection. □

Theorem (Schaefer '78). *Let $\underline{B}$ be a relational structure with $|B| = 2$. Then either* $\mathrm{Pol}(\underline{B}) \to \underline{\mathrm{Proj}}$ *(and* $\mathrm{CSP}(\underline{B})$ *is NP-complete), or one of the following statements holds (and* $\mathrm{CSP}(\underline{B}) \in P$*)*

(1) *$\underline{B}$ is preserved by a constant operation.*
(2) *$\underline{B}$ is preserved by a minimum or maximum,* $\mathrm{CSP}(\underline{B})$ *can be solved by $AC_{\underline{B}}$.*
(3) *$\underline{B}$ is preserved by the majority,* $\mathrm{CSP}(\underline{B})$ *can be solved by $PC_{\underline{B}}$*
(4) *$\underline{B}$ is preserved by the minority,* $\mathrm{CSP}(\underline{B})$ *can be solved by Gaussian elimination.* □

Lemma. *A relation $R \subseteq \{0,1\}^k$ is preserved by a minority iff R is the space of solutions of a system of linear equations over* GF_2.

More generally:

Proposition (linear algebra). *T.f.a.e.:*

- *R is (affine) linear subspace of V^k*
- *R is a space of solutions of (inhomogeneous) homogeneous system of linear equations*
- *R is invariant under (affine) linear combinations $\alpha_1 x_1 + \ldots + \alpha_n x_n$ (s.t. $\alpha_1 + \ldots + \alpha_n = 1$)*

Theorem (Bulatov & Dalman). *Let $\underline{B}$ be a finite structure of a finite signature with Maltsev polymorphisms. Then* $\mathrm{CSP}(\underline{B}) \in P$.

Remark:

- Generalizes linear systems over finite fields being in P, but not the solving algorithm
- The new algorithm for solving the CSP s (next section) also works for the so called *edge polymorphisms*

Examples.

- Let G be a group, $m(x,y,z) := x \cdot y^{-1} \cdot z$. If $G = \mathbb{Z}_p$, then the relations preserved by m are precisely the affine subspaces of GF_p^k. In this case we can solve $\mathrm{CSP}(G)$ with Gaussian elimination. We can extend this to abelian groups (m becomes minority), there are however no known extensions for general finite groups (for example S_3).
- Let m be the minority on $\{0,1,2\}$ s.t. $m(x,y,z) = 2$ whenever $|\{x,y,z\}| = 3$. Then $(\{0,1,2\}, m)$ has a congruence with equivalence classes $\{2\}, \{0,1\}$,
$$\{(2,\ldots,2)\} \cup \{(x_1,\ldots,x_n) \in \{0,1\} \mid x_1 + \ldots + x_n \equiv_2 1\} \in \mathrm{Inv}(m).$$
- Let m be the minority on $\{0,1,2\}$ s.t. $m(x,y,z) = x$ whenever $|\{x,y,z\}| = 3$. There are no non-trivial congruences preserved by m. We have $R_f \in \mathrm{Inv}(m)$, where $R_f = \{(x, \pi(x)) \mid x \in \{0,1,2\}\}$ and $f \in S_3$. Moreover: $R \in \mathrm{Inv}(m)$, where R is maximal binary relation s.t. $|\pi_1^2(R)| \leq 2$, $|\pi_2^2(R)| \leq 2$.

5.3 compact representations of relations

Definition. Let $R \subseteq A^n$.