CSP in Prague

Goals:

(1) Define P, NP, CSP for relational structures
State the dichotomy conjecture

(2) relational clones, functional clones, Galois connection, Schaefer's duality, Post's lattice

(3) CSP(rel. structure), CSP(rel. clone), CSP(algebra)
CSP(variety)

(4) bounded width, near-unanimity, semilattice,
Horn clauses, CD(4)

(5) CSP(digraphs with no source/sink)

(6) dichotomy and forbidden lifts (MMSNP)

(7) SysPol, SysEq

Let I denote the set of all finite binary sequences (input) that is $I = \bigcup_{n=0}^{\infty} \{0,1\}^n$.

Def: A function $f: I \to I$ is in the class P (or computable in polynomial time) if there exists an algorithm and constants c, d such that for all $x \in I$ of size n the algorithm stops in $c \cdot n^d$ steps and computes $f(x)$.

(step is not defined properly, we would need Touring machines for that)

Encoding: numbers, sequences

Why polynomial? Data representation becomes unimportant, the definition of the step becomes unimportant.

Examples: - basic arithmetic
- Euclid's greatest common divisor algorithm
- primality testing (2004)
- linear programming (test if a set of linear inequalities is consistent)
factoring polynomials in $\mathbb{Q}[x]$
- hereditary graph properties (closed under vertex removal and edge contraction) e.g. embeddability onto the plane, torus

Def: A set $C \subseteq I$ of objects (or classification problem, or language) is in P if the characteristic function

$$f(x) = \begin{cases} 1 & \text{if } x \in C \\ 0 & \text{if } x \notin C \end{cases}$$ is computable in polynomial time.

Def: The set $C \subseteq I$ is in NP (or decidable in nondeterministic polynomial time) if there exists a function f in P and a constant k such that

(1) if $x \in C$ then $\exists y \in I$ with $|y| \leq |x|^k$ such that $f(x,y)=1$

(2) if $x \notin C$ then $\forall y \in I$ $f(x,y)=0$.

P = effectively computable

NP = effectively verifiable (y is the short proof)

Examples:

- composite numbers (also in P)
- solvable Diophantine equations of the form $Ax^2+By+C=0$ over the positive integers
- system of quadratic equations
- 3-colorability

NP-complete

- graph isomorphism problem in NP

Not: provable mathematical statements (undecidable)

Theorem: $P \subseteq NP$ Conjecture: $P \neq NP$

Def: Let $C, D \subseteq I$ be two classification problems. We say that C is polynomial time reducible to D (and write $C \trianglelefteq D$) if there exists a function $f: I \to I$ in P such that

$$\forall x \in I \quad x \in C \Leftrightarrow f(x) \in D.$$

(if D can be solved by an algorithm, then C can be solved with that algorithm with the help of f)

Prop: $\trianglelefteq$ is a quasi-order on the set of classification problems.

<u>Def</u>: Two classification problems $C, D \subseteq I$ are <u>polynomial time equivalent</u> ($C \equiv D$) if $C \trianglelefteq D$ and $D \trianglelefteq C$.

<u>Question</u>: How many $\equiv$ blocks does P have?
($\emptyset$ and I are isolated)

<u>Def</u>: Let $\mathcal{C} \subseteq P(I)$ be a set of classification problems (e.g. P or NP). A problem $D \subseteq I$ is <u>$\mathcal{C}$-hard</u> if $C \trianglelefteq D$ for all $C \in \mathcal{C}$. It is <u>$\mathcal{C}$-complete</u> if it is $\mathcal{C}$-hard and $D \in \mathcal{C}$.

<u>Question</u>: What is a P-complete problem?
What are the P-hard problems?

<u>Prop</u>: $\mathcal{C}$ has $\mathcal{C}$-hard problem iff $\mathcal{C}/\equiv$ has a largest element.

<u>Def</u>: A <u>Boolean formula</u> is a term of $(\{0,1\}; \wedge, \vee, ')$.
Let <u>SAT</u> denote the set of all satisfiable Boolean formulae, i.e. those $t(x_1,\dots,x_n)$ for which there exist $a_1,\dots,a_n \in \{0,1\}$ such that $t(a_1,\dots,a_n) = 1$.

<u>Theorem</u> (Cook 1971, Levin 1973) SAT is NP-complete.

<u>Proof Sketch</u>: Let $C \in NP$ with $f(x,y)$ verifier function. The algorithm of f makes at most $k = |x|^c$ steps and visits the states $s_1,\dots,s_k$.
(the next state depends only on x, y and the previous state)
For a fixed $x \in I$ we can construct (in polynomial time) a Boolean formula $t(\bar{y},\bar{z})$ such that

$t(\bar{y},\bar{z}) = 1 \iff \bar{y}$ encodes y,
$\bar{z}$ encodes a sequence $s_1,\dots,s_k$ of states
these states form the correct computation of $f(x,y)$ and returns 1.

<u>Def</u>: <u>3-SAT</u>: satisfiable Boolean formulas of the form

$$t(x_1,\dots,x_n) = \bigwedge_{i=1}^{k} C_i \quad \text{where} \quad C_i \in \{ x \vee y \vee z,\ \neg x \vee y \vee z,\ \neg x \vee \neg y \vee z,\ \neg x \vee \neg y \vee \neg z : x, y, z \in \{x_1,\dots,x_n\} \}$$

<u>Example</u>: $(x_1 \vee x_2 \vee x_3) \wedge (\neg x_4 \vee x_1 \vee x_3) \wedge (\neg x_2 \vee x_2 \vee x_4)$

<u>Theorem</u>: 3-SAT is NP-complete

<u>Sketch</u>: replace every $f(x,y)$ in the original Boolean formula with $f(x,y)=z$ ternary constraint where z is a new variable.

<u>In general</u>

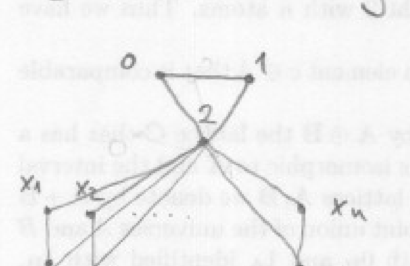
<u>Theorem</u>: Every system of equations can be replaced with an equivalent one in which every equation is of the form

$f(x_1,\dots,x_k) = y$

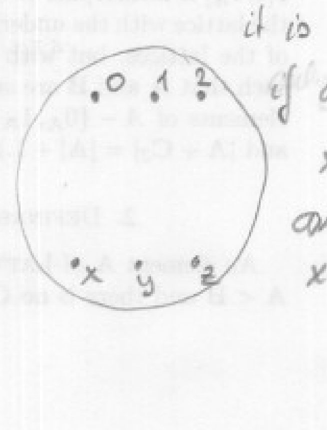
where f is a basic operation

<u>Theorem</u>: 3-colorability is NP-complete

<u>Sketch</u>:



HW: find graph, such that it is 3-colorable if and only if $x, y, z \in \{0,1\}$ and $x \vee y \vee z$



Def: Let $\mathcal{R}$ be a set of symbols with associated arities.

$\Big[$ i.e. $\mathcal{R}=(\mathcal{R};\tau)$ where $\mathcal{R}$ is a set, $\tau:\mathcal{R}\to\mathbb{N}$ and the arity of $R\in\mathcal{R}$ is $\tau(R)$. $\Big]$

$\mathbb{A}=(A;\mathcal{R})$ is a relational structure of signature $\mathcal{R}$ if A is a nonempty set and for every symbol $R\in\mathcal{R}$ of arity n there is an associated n-ary relation $R^{\mathbb{A}}\subseteq A^n$

Example: directed graphs $(V;E)$ $\quad E\subseteq V\times V$

4-coloured set $(A;B,Y)$ $\quad B,Y\subseteq A$ $\quad \mathcal{R}=\{B,Y\}$

black $\quad x\notin B \quad x\notin Y$

blue $\quad x\in B, \ x\notin Y$

yellow $\quad x\notin B, \ x\in Y$

green $\quad x\in B, \ x\in Y$

$\to$ same set of symbols and arities

Def: Let $\mathbb{A}$ and $\mathbb{B}$ be similar relational structures. A mapping $f:A\to B$ is a homomorphism if for every symbol $R\in\mathcal{R}$ and tuple $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ the tuple $(f(a_1),\dots,f(a_n))\in R^{\mathbb{B}}$.

(edge is mapped to edge, we do not care about non-edges)

Def: isomorphism: bijective, inverse is also a homomorphism (preserves edges and nonedges)

endomorphism: $f:\mathbb{A}\to\mathbb{A}$ homomorphism

automorphism: $f:\mathbb{A}\to\mathbb{A}$ isomorphism.

Def: Let $\mathbb{B}$ be a relational structure of finite signature. By the constraint satisfaction problem for $\mathbb{B}$ we mean the class

$$CSP(\mathbb{B})=\{\mathbb{A} : \mathbb{A} \text{ finite}, \mathbb{A}\to\mathbb{B}\}$$

Example:

$CSP(\Delta)$ $\quad$ 3-colorable graphs $\quad$ NP-complete

$CSP(\,|\,)$ $\quad$ bipartate graphs $\quad$ in P

<u>Example</u>: Let $\mathbb{B} = (\{0,1\}, R_0, R_1, R_2, R_3)$

where
$$\left.\begin{aligned} R_0 &= \{0,1\}^3 \setminus \{(0,0,0)\} \\ R_1 &= \{0,1\}^3 \setminus \{(1,0,0)\} \\ R_2 &= \{0,1\}^3 \setminus \{(1,1,0)\} \\ R_3 &= \{0,1\}^3 \setminus \{(1,1,1)\} \end{aligned}\right\} \text{ ternary relations}$$

then CSP($\mathbb{B}$) is polynomial time equivalent to 3-SAT.

for $t(x_1, \dots, x_n) = \bigwedge_{i=1}^{t} C_i$ we take

$A = \{x_1, \dots, x_n\}$ the set of variables

$R_0^A = \{(x, y, z) : \exists i \;\; C_i = x \wedge y \wedge z\}$

$R_1^A = \{(x, y, z) : \exists i \;\; C_i = \neg x \wedge y \wedge z\}$

$\vdots$

<u>Dichotomy Conjecture</u>: For every finite relational structure $\mathbb{B}$ the class CSP($\mathbb{B}$) is either in P or NP-complete.

<u>Alternate definition</u>: B is the set of possible values

$\mathcal{R}$ are the set of constraints

A is the set of variables

the tuples in R^A (for $R \in \mathcal{R}$) are the scope of the constraints

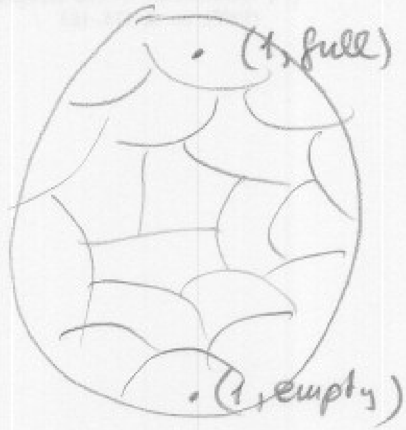
We are looking for an assignment that satisfies all constraints.

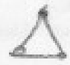
<u>Applications</u>:

- preparing a timetable / schedule
- satisfiability of a logical formula, system of equations
- finding a DNA sequence from a set of contigs
- laying out components on a circuit board

<u>Prop</u>: The homomorphism relation $\to$ is a preorder on the set of finite relational structures.
(use a fixed encoding so it is not a proper class)

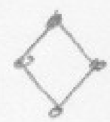
<u>Question</u>: Does it have a largest, smallest element?



<u>Question</u>: Are  and  in

 and the

same

 and  block?

<u>Def</u>: Let $\mathbb{A}$ be a relational structure and $B \subseteq A$ be a nonempty subset. We define the <u>restriction of $\mathbb{A}$ to B</u>:

$$\mathbb{A}|_B = (B; \mathcal{R}) \qquad R^{\mathbb{A}|_B} = R^{\mathbb{A}} \cap B^n$$ where n is the arity of $R \in \mathcal{R}$.

<u>Prop</u>: $\mathbb{A}|_B \to \mathbb{A}$, $b \mapsto b$ is a homomorphism.

<u>Prop</u>: If $f: \mathbb{A} \to \mathbb{A}$, then $\mathbb{A} \leftrightarrow \mathbb{A}|_{f(A)}$

<u>Prop</u>: If $\mathbb{A}, \mathbb{B}$ are finite, and $f: \mathbb{A} \to \mathbb{B}$, $g: \mathbb{B} \to \mathbb{A}$ are bijective then f, g are isomorphisms. (<u>not always true</u> unlike for algebras)

<u>Exercise</u>: Find $f: \mathbb{A} \to \mathbb{A}$ bijective hom, that is not automorphism.

<u>Def</u>: A relational structure is a <u>core</u> if all of its endomorphisms are automorphisms.

<u>Theorem</u>: Every $\leftrightarrow$ class contains an (up to isomorphism) uniquely determined core.

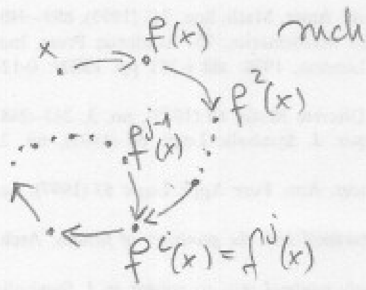
<u>Proof</u>: Take a structure $\mathbb{A}$ of minimal size in one of the $\Leftrightarrow$ blocks, and a homomorphism $f: \mathbb{A} \to \mathbb{A}$.
If f is not bijective, then $\mathbb{A} \Leftrightarrow \mathbb{A}|_{f(A)}$ contradiction.
So f is an automorphism (by the previous proposition).
This proves that $\mathbb{A}$ is a core.

If $\mathbb{A}$ and $\mathbb{B}$ are cores with $A \underset{g}{\overset{f}{\rightleftarrows}} B$, then
$g \circ f : \mathbb{A} \to \mathbb{A}$ and $f \circ g : \mathbb{B} \to \mathbb{B}$ must be bijective
so f and g must be bijective, so they are isomorphic.

<u>Def</u>: $f: \mathbb{A} \to \mathbb{A}$ is a <u>retraction</u> if it is a homomorphism and $\forall x \in A \quad f^2(x) = f(x)$.

<u>Lemma</u>: If A is a finite set, then there exists k such that for all mapping $f: A \to A$, $f^{2k} = f^k$.

<u>Proof</u>. Let $k = |A|!$. Take $x \in A$, and $i < j$ minimal such that $f^i(x) = f^j(x)$



$j < |A|$ because $x, f(x), \dots, f^{|A|}(x)$ cannot all be different.

so $j - i < |A|$, $j - i \mid |A|!$

$f^{|A|!} \in \{f^i(x), \dots, f^{j-1}(x)\}$ and therefore $f^{2|A|!}(x) = f^{|A|!}(x)$.

<u>Theorem</u>: Every finite relational structure $\mathbb{A}$ has a retraction $r: \mathbb{A} \to \mathbb{A}$ such that $r(\mathbb{A})$ is a core. (note, that $\mathbb{A} \Leftrightarrow r(\mathbb{A})$)

<u>Proof</u>: Let f be a homomorphism with minimal range, then $r = f^k$ is a retract and all homomorphisms of $r(A)$ are bijective, that is $r(A)$ is a core.

<u>Prop</u>: $\mathbb{A} \leftrightarrow \mathbb{B}$ relational structures, then $CSP(\mathbb{A}) = CSP(\mathbb{B})$
(we can restrict ourselves to cores)

<u>Motivation</u>: Which $CSP(\mathbb{B})$ classification problems are polynomial time equivalent? (As a trivial example, for $\mathbb{B}$ and its core)

<u>Theorem</u>: $CSP(\underbrace{(B;R)}_{\mathbb{B}})$ and $CSP(\overbrace{(B;R\cup\{=^B\})}^{\mathbb{B}'})$ are polynomial time equivalent (Jeavons 1998)

<u>Proof</u>: $CSP((B;R))$ is trivially poly-time reducible to $CSP((B;R\cup\{=\})$: take an instance $\mathbb{A}=(A;R)$ add the empty relation for $=$ to get $\mathbb{A}'=(A;R\cup\{=\})$.
Clearly $\mathbb{A}\to\mathbb{B}$ if and only if $\mathbb{A}'\to\mathbb{B}'$.

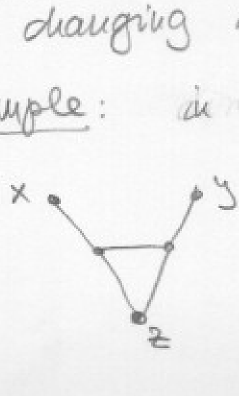
For the reverse, take an instance $\mathbb{A}'=(A';R\cup\{=\})$ for $CSP(\mathbb{B}')$. Compute the transitive closure of $=^{\mathbb{A}'}$ which is an equivalence relation on A'. From each equivalence block take a representative, and let A be the set of representatives. For each tuple

$(a_1',\dots,a_n')\in R^{\mathbb{A}'}$ we add a tuple $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ where a_i is the representative of a_i'.

All of this can be done in polynomial time. Now
$\mathbb{A}'\to\mathbb{B}'$ if and only if $\mathbb{A}\to\mathbb{B}$.

<u>Motivation</u>: What other relations can we add without changing the complexity of $CSP(\mathbb{B})$?

<u>Example</u>: in $CSP(\triangle)$



$R=\{(x,y,z) : \text{if } x=y \text{ then } z=x\}$

<u>Exercise</u>: What binary relations can be expressed?

Def: For a set Γ of finitary relations on a set A, let $\langle \Gamma \rangle$ denote the set of all relations that can be expressed by primitive positive formulas over Γ, that is

(1) relations in $\Gamma \cup \{=\}$
(2) conjunction
(3) existential quantification.

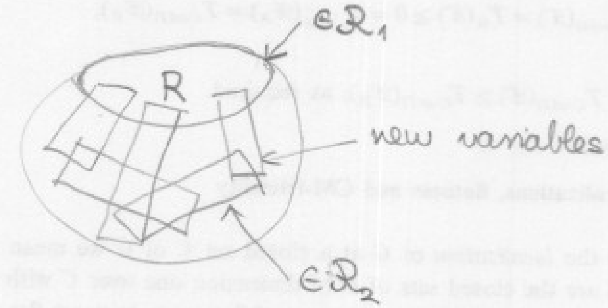
The set Γ is a relational clone if $\Gamma = \langle \Gamma \rangle$.

Prop $\langle - \rangle$ is a closure operator on the sets of relations of A, therefore the set of relational clones form an (algebraic) complete lattice.

Example: $R = \{ (x,y,z) : (\exists u,v)(x \neq u \wedge y \neq v \wedge u \neq v \wedge u \neq z \wedge v \neq z) \}$

Theorem: If $\langle \mathcal{R}_1 \rangle \subseteq \langle \mathcal{R}_2 \rangle$ then $CSP((B;\mathcal{R}_1))$ is polynomial time reducible to $CSP((B;\mathcal{R}_2))$ [Jeavons 1998]

Proof: Each $R \in \mathcal{R}_1$ can be replaced with a finite $\mathcal{R}_2$ configuration



So we convert an instace $\mathbb{A}_1 = (A_1; \mathcal{R}_1)$ into a larger instance $\mathbb{A}_2 = (A_2; \mathcal{R}_2)$ where the number of new variables depend only on the number of tuples in $R^{\mathbb{A}_1}$ relations.

Prop: Γ is a relational clone if and only if

(1) contains the $=$ relation
(2) closed under projections
(3) closed under direct products

Motivation: How many new variables we need?
Can we decide if $\langle \mathcal{R}_1 \rangle \subseteq \langle \mathcal{R}_2 \rangle$?

Def: A relation $R \subseteq A^k$ is *invariant* under an n-ary operation $f: A^n \to A$ (or f is a *polymorphism* of R) if

whenever $r_1 = (a_{11}, a_{12}, \ldots, a_{1k}) \in R$
$r_2 = (a_{21}, a_{22}, \ldots, a_{2k}) \in R$
$\vdots$
$r_n (a_{n1}, a_{n2}, \ldots, a_{nk}) \in R$

$\boxed{\text{unary polymorphism} \overset{\shortparallel}{} \text{endomorphism}}$

then $f(r_1, \ldots, r_n) = (f(a_{11}, \ldots, a_{n1}), \ldots, f(a_{1k}, \ldots, a_{nk})) \in R$.

Example: unary polymorphisms of $\triangle = S_3$ (symmetric group)

Def: Γ set of relations on A the *polymorphysms of Γ*

$$Pol(\Gamma) = \{ f: A^n \to A \mid f \text{ is a polymorphism of every } R \in \Gamma \}$$

Def: For a set Φ of (finitary) operations on A the set of *invariant relations of Φ* is

$$Inv(\Phi) = \{ R \subseteq A^n : R \text{ is invariant under all } f \in \Phi \}$$

Prop: $\left.\begin{array}{l} \Gamma \subseteq Inv(Pol(\Gamma)) \\ \Phi \subseteq Pol(Inv(\Phi)) \end{array}\right\}$ in fact Pol and Inv form a Galois connection

$Inv(\Phi)$ is always a relational clone
$Pol(\Gamma)$ is a functional clone

Def: Φ is a *functional clone* if
(1) contains the projections: $\pi: A^n \to A$, $(a_1, \ldots, a_n) \mapsto a_i$
(2) closed under compositions

These are the trivial directions.

Moreover: $\left.\begin{array}{l} Pol(Inv(Pol(\Gamma))) = Pol(\Gamma) \\ Inv(Pol(Inv(\Phi))) = Inv(\Phi) \end{array}\right\}$ true for all Galois connection

Free algebras:

Theorem: Let $\mathbb{A}=(A;\Phi)$ be an algebra and n be an integer.

$$A^n = \{ (a_1,\dots,a_n) : a_i \in A \}$$

Then the n-generated free algebra in the variety generated by $\mathbb{A}$ is the subalgebra

$$\mathbb{F}_n \le \mathbb{A}^{(A^n)} \quad \text{generated by the}$$

elements $g_1,\dots,g_n \in A^{(A^n)}$ where $g_i((a_1,\dots,a_n)) = a_i$

Proof: Clearly $\mathbb{F}_n$ is n-generated. We need to show that for any two n-ary terms s,t

$$\mathbb{A} \models s(x_1,\dots,x_n) \approx t(x_1,\dots,x_n) \iff s(g_1,\dots,g_n) = t(g_1,\dots,g_n) \text{ in } \mathbb{F}.$$

$\mathbb{F}$ is a product, so $s(g_1,\dots,g_n)$ and $t(g_1,\dots,g_n)$ are calculated coordinatewise and they are equal iff for all coordinates $(a_1,\dots,a_n)\in A^n$

$$(s(g_1,\dots,g_n))(a_1,\dots,a_n) = s(g_1(a_1,\dots,a_n),\dots,g_n(a_1,\dots,a_n)) = s(a_1,\dots,a_n)$$

$$(t(\quad))(\quad) = \qquad\qquad\qquad \overset{\shortparallel}{= t(\quad)}$$

Theorem: Let Γ be a set of relations on a finite set A. Then the n-generated free algebra $\mathbb{F}_n$ for $(A;\mathrm{Pol}(\Gamma))$ is in $\langle\Gamma\rangle$.

Proof: $\mathrm{Pol}(\Gamma)$ is closed under composition, so

$$\begin{aligned}\mathbb{F}_n &= \{ f(g_1,\dots,g_n) : f\in \mathrm{Pol}(\Gamma) \} \\ &= \{ f: A^n\to A : f\in \mathrm{Pol}(\Gamma) \} \\ &= \{ f: A^n \to A : \forall R\in\Gamma \ k\text{-ary}, \forall M \in A^{n\times k} \text{ with rows in } R \\ &\qquad f \text{ applied to the columns is in } R \}\end{aligned}$$

might be infinitely many, but finite many are enough to exclude elements not in $\mathbb{F}_n$.

This is a conjunction saying that certain coordinates of f (at the columns of M) are in relation R, which is a primitive positive formula (without any existential quantifier)

<u>Theorem</u> Let Γ be a set of relations on a finite set A. Then $\langle\Gamma\rangle = Inv(Pol(\Gamma))$

<u>Proof</u>: We have seen that $\Gamma \subseteq Inv(Pol(\Gamma))$ and that $Inv(Pol(\Gamma))$ is a relational clone. Since $\langle\Gamma\rangle$ is the smallest relational clone containing Γ, we get $\langle\Gamma\rangle \subseteq Inv(Pol(\Gamma))$.

Now take $R \subseteq A^k$, $R \in Inv(Pol(\Gamma))$, that is $R \leq (A; Pol(\Gamma))^k$

$R = \{r_1, \ldots, r_n\}$ $\qquad r_1 = (a_{11}, \ldots, a_{1k}) \in R$

$$r_n = (a_{n1}, \ldots, a_{nk}) \in R$$

If you look at $\mathbb{F}_n$, then the generators $g_1, \ldots, g_n$ of $\mathbb{F}_n$ restricted to certain coordinates (k-many) give exactly the tuples. However, R is closed under the operations, so nothing new could be generated, and R is just the projection of $\mathbb{F}_n$ to these k coordinates (maybe with repetitions).

But $\mathbb{F}_n \in \langle\Gamma\rangle$, thus $R \in \langle\Gamma\rangle$.

<u>Answer</u>: $R \in \langle\mathcal{R}\rangle$ is decidable, we might need up to $A^{A^{|R|}}$ many new variables.

<u>Theorem</u>: Similar theorem holds for functions $\langle\Phi\rangle = Pol(Inv(\Gamma))$

<u>Theorem</u>: Let $\mathbb{B} = (B; \mathcal{R})$ be a core. Then $CSP(\mathbb{B})$ is polynomial time equivalent to $CSP((B; \mathcal{R} \cup \underbrace{\{\{b\} \subseteq B : b \in B\}}))$

many constant relations.

<u>Proof</u>: Let $B = \{b_1, \ldots, b_n\}$ and consider the set

$$S = \{(f(b_1), \ldots, f(b_n)) \in B^n : f : \mathbb{B} \to \mathbb{B} \text{ automorphism}\}$$

S is a one-generated subalgebra of $(B; Pol(\mathcal{R}))^n$, so $S \in \langle\mathcal{R}\rangle$. Show that both poly-time equivalent to $CSP((B; \mathcal{R} \cup \{=, S\})$.

We know that $\mathrm{CSP}(\mathbb{B})$ and $\mathrm{CSP}((B; \mathcal{R} \cup \{=, S\}))$ are poly-time equivalent.

Put $\mathbb{C} = (B; \mathcal{R} \cup \{\varrho_b : b \in B\})$

where $\varrho_b^{\mathbb{C}} = \{b\} \subseteq B$. singleton unary relations.

Clearly, $\mathrm{CSP}(\mathbb{B})$ can be reduced to $\mathrm{CSP}(\mathbb{C})$, so it is enough to show that $\mathrm{CSP}(\mathbb{C})$ can be reduced in polynomial time to $\mathrm{CSP}((B; \mathcal{R} \cup \{=, S\})$

Take $\mathbb{A} = (A; \mathcal{R} \cup \{\varrho_b : b \in B\})$ instance, and define

$\mathbb{D} = (\underbrace{A \dot\cup B}_{\text{disjunct union}}; \mathcal{R} \cup \{=, S\})$ where

$$R^{\mathbb{D}} = R^{\mathbb{A}} \quad \text{for all } R \in \mathcal{R}$$

$$S^{\mathbb{D}} = S^{B} \quad \text{(the rel. defined on } B\text{)}$$

and

$$=^{\mathbb{D}} = \{(a, b) : a \in \varrho_b\}$$

(This is like appending the $\triangle$ on the side and connecting the unary rels to one of the edges).

f $\mathbb{A} \to \mathbb{C}$, then $\mathbb{D} \to (B; \mathcal{R} \cup \{=, S\})$ with the definition $b \mapsto b$

If $f : \mathbb{D} \to (B; \mathcal{R} \cup \{=, S\})$, then $f|_B$ defines an automorphism of B, and $(f|_B)^{-1} \circ f|_A : \mathbb{A} \to \mathbb{C}$. ☒

<u>Note</u>: All these poly-time equivalences also give poly-time algorithms to translate one solution to a corresponding solution.

Theorem: Let $\mathbb{B}$ be a relational structure. If $CSP(\mathbb{B})$ is in P, then there exists a polynomial time algorithm, that also finds a homomorphism if one exists.

Proof: Let $\mathbb{C}$ be the core of $\mathbb{B}=(B;\mathcal{R})$, and $\mathbb{D}=(C;\mathcal{R}\cup\{\varrho_c : c\in C\})$, where $R^{\mathbb{D}}=R^{\mathbb{C}}$ and $\varrho_c^{\mathbb{D}}=\{c\}\subseteq C$ unary. We know that $CSP(\mathbb{B})$ and $CSP(\mathbb{D})$ are polynomial time equivalent (which can also translate solutions in polynomial time) so it is enough to prove the theorem for $\mathbb{D}$.

Let $\mathbb{A}=(A;\mathcal{R}\cup\{\varrho_c : c\in C\})$ be any input structure. If $\mathbb{A}\notin CSP(\mathbb{D})$, then there is no homomorphism $f:\mathbb{A}\to\mathbb{D}$. So assume that $\mathbb{A}\in CSP(\mathbb{D})$. List the elements $A=\{a_1,\dots,a_n\}$. By induction we will define a sequence $c_1,\dots,c_n\in C$ of elements. Suppose that c_j is defined for all $j\leq i$ for some i such that $\mathbb{A}_i\in CSP(\mathbb{D})$ where

$$\mathbb{A}_i=(A;\mathcal{R}\cup\{\varrho_c : c\in C\})$$

$$R^{\mathbb{A}_i}=R^{\mathbb{A}} \qquad \varrho_c^{\mathbb{A}_i}=\varrho_c^{\mathbb{A}}\cup\{a_j : j\leq i \text{ and } c_j=c\}.$$

Note, that $\mathbb{A}_0=\mathbb{A}$, so the basis of induction is $i=0$. Since there a homomorphism from $\mathbb{A}_i$ to $\mathbb{D}$, there must be at least one choice of $c_{i+1}\in C$ for which $\mathbb{A}_{i+1}\in CSP(\mathbb{D})$. We can find that element with at most $|C|$ applications of the decision procedure for $CSP(\mathbb{D})$. So with at most $|A|\cdot|C|$ applications of $CSP(\mathbb{D})$ we have a structure $\mathbb{A}_n\in CSP(\mathbb{D})$.

Then the map

$$f(a_i)=c_i \quad \text{is a homomorphism } \mathbb{A}\to\mathbb{D}.$$

Def.: An operation $f: A^n \to A$ is *idempotent* if
$$f(a, \dots, a) = a \quad \text{for all } a \in A.$$

Def. $f: A^n \to A$ *projection* iff $f(x_1, \dots, x_n) = x_i$

Theorem. Let $\mathbb{B} = (\{0,1\}; \mathcal{R})$ any relational structure on the two-element set. Then $\mathbb{B}$ has one of the following polymorphisms

(1) the constant 0 operation (unary)

(2) 1 (unary)

(3) the binary join $\vee$ $(x \vee y = 0 \Leftrightarrow x = y = 0)$

(4) the binary meet $\wedge$ $(x \wedge y = 1 \Leftrightarrow x = y = 1)$

(5) the ternary mod-2 addition $+$ $\quad p(x,y,z) = x + y + z$

(6) the majority operation m
$$m(x,y,z) = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x) = \begin{cases} x & \text{if } x = y \\ y & \text{if } y = z \\ z & \text{if } z = x \end{cases}$$

(7) <u>or else</u> every polymorphism of $\mathbb{B}$ is a projection or the negate of a projection
$$\neg x = \begin{cases} 0 & \text{if } x = 1 \\ 1 & \text{if } x = 0 \end{cases}$$

Note: This is the bottom of Post's Lattice of clones

Proof: If $\mathbb{B}$ is not a core, then it has an endomorphism to a proper subset, that is it has a polymorphism of type (1) or (2). So we can assume that $\mathbb{B}$ is a core and $\mathrm{End}(\mathbb{B}) = \mathrm{Pol}_1(\mathbb{B}) \subseteq \{id, \neg\}$.

It is enough to describe the idempotent polymorphisms, since if t is not idempotent, then $t(x, \dots, x) = \neg x$ and $\neg t(x_1, \dots, x_n)$ becomes idempotent.

Take an idempotent polymorphism t of minimal arity that is not a projection (so we are not in case (7)).

If t is binary, then

$$\begin{array}{c|cc} t & 0 & 1 \\ \hline 0 & 0 & ? \\ 1 & ? & 1 \end{array} \quad \text{and } t \neq \pi_1, \pi_2 \text{ so } t = \begin{array}{c|cc} \vee & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \quad \text{or} \quad \begin{array}{c|cc} \wedge & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}.$$

If t is ternary, then $t(x,x,y)$ is a projection, so $t(1,1,0) = \neg t(0,0,1)$, that is t is uniquelly determined by $t(0,0,1)$, $t(0,1,0)$ and $t(1,0,0)$.
If $t(0,0,1) = t(0,1,0) = t(1,0,0) = 0$, then t is the majority operation, and we are in case (6). If $t(0,0,1) = t(0,1,0) = t(1,0,0) = 1$, then $t = p$ ternary addition and we are in case (5). So either one or two of them equals 1.

If only one of them, say $t(1,0,0)=1$, $t(0,1,0)=0$, $t(0,0,1)=0$, then $t(x,y,z) = x$, which is a contradiction.

If two of them equals 1, say $t(1,0,0)=1$, $t(0,1,0)=1$, $t(0,0,1)=0$ then

$$t(x,y,t(x,y,z)) \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = t \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

is a majority operation, so we are again in case (6)

All we have to prove now is that the arity of t cannot be larger than 3.

Consider $t(x_1, \dots, x_n)$, and suppose that $t(0, \dots, 0, 1) = 1$. Then $t(y, y, x_3, \dots, x_n) = x_n$, $t(y, x_2, y, x_4, \dots, x_n) = x_n$ and $t(x_1, y, y, x_4, \dots, x_n) = x_n$ that is $t(x_1, \dots, x_n) = x_n$ which is a contradiction. This proves that

$t(0,\dots,0,1) = t(0,\dots,0,1,0) = \dots = t(1,0,\dots,0) = 0$ and
$t(1,\dots,1,0) = t(1,\dots,1,0,1) = \dots = t(0,1,\dots,1) = 1$

<u>Def</u>: An operation t is a <u>near-unanimity operation</u> if

$$t(x,\dots,x,y) = t(x,\dots,x,y,x) = \dots = t(y,x,\dots,x) = x \quad \forall x,y \in A.$$

<u>Proof continued</u>: So we have shown that t must be a near-unanimity operation.

If $t(0,0,1,1\dots 1) = 1$, then $t(y,y,x_3,\dots,x_n)$ must be a projection to x_3 or x_4 or ... or x_n. But $t(0,0,\dots,0,1,0,\dots 0) = 0$ shows that it cannot be any one, so we got a contradiction. The case when $t(0,0,1,\dots,1) = 0$ is handled similarly. ∎

<u>Goal</u>: To show that in cases (1)–(6) CSP($\mathbb{B}$) is in P, and in case (7) CSP($\mathbb{B}$) is NP-complete, so the dichotomy conjecture holds for two-element structures. (Schaefer, 1978)

<u>Lemma</u>: If all polymorphisms of $\mathbb{B}$ are projections or (case 7) permutations applied to projections, then CSP($\mathbb{B}$) is NP-complete.

<u>Proof</u>: $\mathrm{Aut}(\mathbb{B}) = \mathrm{Pol}_1(\mathbb{B}) \leq S_B$ a permutation group on B,

so $\forall f \in \mathrm{Pol}(\mathbb{B})$ $\quad f(x_1,\dots,x_n) = \sigma(x_i)$ for $\sigma(x) = f(x,\dots,x) \in \mathrm{Aut}(\mathbb{B})$.

This means that $\mathbb{B}$ is a core, so CSP($\mathbb{B}$) is poly-time equivalent to $\mathrm{CSP}(\underbrace{(B; \mathcal{R} \cup \{\{b\} : b \in B\})}_{\mathbb{C}.})$ ↑ unary constant relations,

Every relation is preserved by $\mathrm{Pol}(\mathbb{C})$, so for $0,1 \in B$ the relation

$$\{0,1\}^3 \setminus \{(0,0,0)\} \in \langle \mathcal{R}^{\mathbb{B}} \cup \{\{b\} : b \in B\} \rangle$$, that is

3-SAT is poly-time reducible to CSP($\mathbb{C}$) ∎

Note, maybe we should have introduced CSP($\{0,1\}$, not all equal).

Lemma: If $\mathbb{B}=(\{0,1\},\mathcal{R})$ and $\wedge$ is a polymorphism of $\mathbb{B}$, then CSP($\mathbb{B}$) is in P. (cases (3) and (4)).

Proof: Let $\rho_1^{\mathbb{B}}=\{1\}\subseteq B$. We can assume, that $\mathcal{R}$ contains ρ_1, and $R^{\mathbb{B}}$ is closed under intersections and projections. (we have added more relations only).

Take an instance $\mathbb{A}=(A;\mathcal{R})$. If $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ for $R\in\mathcal{R}$ and $a_i\in\rho_1^{\mathbb{A}}$, then we can remove $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ and add $(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n)$ to $(R|_{\{1,\dots,i-1,i+1,\dots,n\}})^{\mathbb{A}}$.

If $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ and $(0,\dots,0)\notin R^{\mathbb{B}}$, then $\exists 1\le i\le n$ such that $R^{\mathbb{B}}\subseteq B\times\dots\times B\times\{1\}\times B\times\dots\times B$ (we use the $\wedge$ op. here) so we can remove $(a_1,\dots,a_n)\in R^{\mathbb{A}}$ and add a_i to $\rho_1^{\mathbb{A}}$ and $(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n)$ to $(R|_{\{1,\dots,n\}\setminus\{i\}})^{\mathbb{A}}$. Under some measure (e.g. the number of elements in the tuples in $\mathcal{R}\setminus\{\rho_1\}$) we have a smaller instance, so after polynomial many steps we cannot do either of these steps. Then the map $f: A\to B$

We will generalize this with bounded width.

$$f(x)=\begin{cases}1 & \text{if } x\in\rho_1^{\mathbb{A}}\\ 0 & \text{otherwise}\end{cases}$$ is a homomorphism.

unless we have $R^{\mathbb{A}}\neq\emptyset$ while $R^{\mathbb{B}}=\emptyset$ for some $R\in\mathcal{R}$.

do this first

Lemma: If $\mathbb{B}$ has a constant polymorphism, then CSP($\mathbb{B}$) is in P. (cases (1) and (2)).

Proof: We work with unary constant polymorphisms. So $u\in Pol_1(\mathbb{B})$ with $u(x)=b$ for some fixed $b\in B$.
Then for any $R\in\mathcal{R}$ if $R^{\mathbb{B}}\neq\emptyset$, then $(b,\dots,b)\in R^{\mathbb{B}}$
So if $\exists R\in\mathcal{R}$ such that $R^{\mathbb{A}}\neq\emptyset$ and $R^{\mathbb{B}}=\emptyset$, then no solution, otherwise the map $f: A\to B$, $f(x)=b$ is a solution.

PG

Lemma: If $\mathbb{B} = (\{0,1\}; R)$ and $p(x,y,z) = x+y+z \pmod 2$ is a polymorphism of $\mathbb{B}$, then $CSP(\mathbb{B})$ is in P.

Proof: Every subalgebra of $(\{0,1\}; p)^n$ is an affine subspace in the n-dimensional vectorspace over the 2-element field $\mathbb{F}$. Every affine subspace can be characterized by a system of linear equations over $\mathbb{F}$, using the operation $+$ and constants 0 and 1. Thus they are in the relational clone generated by $\underbrace{\{(000),(011),(101),(110)\}}_{\text{graph of } +}, \{0\}, \{1\}$. So we have proven that

$$\langle R \rangle \subseteq \langle \text{graph of } +, \{0\}, \{1\} \rangle, \text{ so } CSP(\mathbb{B}) \text{ is}$$

poly-time reducible to $CSP(\{0,1\}; \{\text{graph of } +, \{0\}, \{1\}\})$. But the latter is poly-time solvable (linear algebra).

Corollary: Actually, we have proven, that the functional clone generated by $p(x,y,z) = x+y+z \pmod 2$ corresponds to the relational clone generated by the graph of $+$, $\{0\}$ and $\{1\}$.

Def: The graph of an operation $f: A^n \to A$ is the $n+1$-ary relation

$$f^\circ = \{(a_1, \dots, a_n, f(a_1, \dots, a_n)) : a_1, \dots, a_n \in A\}.$$

Exercise: For the 7 minimal clones generated by $0, 1, \vee, \wedge, p, m$ and $\neg$ find a finite set of relations that generates the corresponding relational clone.

Exercise: For which minimal clone $C \in \{\langle 0 \rangle, \langle 1 \rangle, \langle \vee \rangle, \langle \wedge \rangle, \langle p \rangle, \langle m \rangle, \langle \neg \rangle\}$ is it true that every clone is either below C or above one of the other 6 minimal clones?

Lemma: Let $R \subseteq A^n$ be a relation invariant under a k-ary near-unanimity operation t. Then for any $f \in A^n$

$$f \in R \iff f|_K \in R|_K \text{ for all } K \subseteq \{1,\dots,n\},\ |K| < k.$$

Proof: It is enough to show that for all $\ell \geq k$ if

$f|_K \in R|_K$ for all $K \subseteq \{1,\dots,n\}$ with $|K| < \ell$, then
$f|_L \in R|_L$ for all $L \subseteq \{1,\dots,n\}$ with $|L| \leq \ell$.

Let $L = \{1,2,\dots,\ell\}$ and $f = (a_1, a_2, \dots, a_n)$.

$f|_{L\setminus\{1\}} \in R|_{L\setminus\{1\}}$, so $\exists f_1 = (?, a_2, \dots, a_k, a_{k+1}, \dots, a_\ell, ?, \dots, ?) \in R$

$\vdots$

$f|_{L\setminus\{k\}} \in R|_{L\setminus\{k\}}$ $\qquad \exists f_k = (a_1, \dots, a_{k-1}, ?, a_{k+1}, \dots, a_\ell, ?, \dots, ?) \in R$

apply t $\qquad t(f_1, \dots, f_k) = (a_1, a_2, \dots, a_k, a_{k+1}, \dots, a_\ell, ?, \dots, ?) \in R.$

that is $\quad t(f_1, \dots, f_k)|_L \in R|_L$. ∎

Corollary: If $\mathbb{B}$ has a k-ary near-unanimity polymorphism, then $CSP(\mathbb{B})$ is poly-time equivalent to

$$CSP((B; \{S \in \langle \mathcal{R} \rangle : \text{arity of } S \text{ is at most } k-1\})).$$

We have show actually more, but we need a few definitions first to express it.

Def: $\mathbb{A}, \mathbb{B}$ similar relational structures. A partial map $f: A \to B$ is a <u>partial homomorphism</u> if $f: \mathbb{A}|_{dom(f)} \to \mathbb{B}$ is a homomorphism.

<u>Def</u>: Let $f, g: \mathbb{A} \to \mathbb{B}$ be partial homomorphisms.

Then $f \subseteq g \iff \mathrm{dom}(f) \subseteq \mathrm{dom}(g)$ and $f = g|_{\mathrm{dom}(f)}$.

g is an <u>extension</u> of f, f is a <u>subfunction</u> of g.

<u>Note</u>: We can regard a partial homomorphism $f: \mathbb{A} \to \mathbb{B}$ as $f \in B^{\mathrm{dom}(f)}$. The set of homomorphisms is $\mathbb{B}^{\mathbb{A}}$, the set of partial hom. with domain $K \subseteq A$ is $\mathbb{B}^{(\mathbb{A}|_K)}$.

<u>Prop</u>: If $\mathbb{B}$ is a relational structure with $\underline{B} = (B; \mathrm{Pol}\,\mathbb{B})$ the corresponding algebra, then for any $K \subseteq A$

$$\mathbb{B}^{(\mathbb{A}|_K)} \leq \underline{B}^K$$

So if $f_1, \dots, f_n$ are partial homomorphisms with domain K and t is a polymorphism, then

$f(x) = t(f_1(x), \dots, f_n(x))$ is another partial hom.

<u>Proof</u>: Trivial, just check the definitions.

<u>Def</u>: A nonempty family $\mathcal{F}$ of partial homomorphisms from $\mathbb{A}$ to $\mathbb{B}$ is a (j,k)<u>-strategy</u> (with $0 \leq j < k$) if

(1) $\mathcal{F}$ is closed under subfunctions

(2) If $f \in \mathcal{F}$ with $|\mathrm{dom}(f)| \leq j$ and $\mathrm{dom}(f) \subseteq K \subseteq A$ with $|K| \leq k$, then $\exists g \supseteq f$ with $\mathrm{dom}(g) = K$.

(j,k)-<u>forth property</u>

For $I \subseteq A$ we define $\mathcal{F}_I = \{ f \in \mathcal{F} : \mathrm{dom}(f) = I \}$.

<u>Lemma</u>: If $\mathcal{F}$ is a (j,k)-strategy for $\mathbb{A}$ and $\mathbb{B}$, then there is a (j,k)-strategy $\overline{\mathcal{F}}$ such that $\overline{\mathcal{F}}_I \leq \underline{B}^I$ (subuniverse) for all $I \subseteq A$.

(where $\underline{B} = (B; \mathrm{Pol}(\mathbb{B}))$.

<u>Proof</u>: For $I \subseteq A$ define

$$\overline{\mathcal{F}}_I = \{ t(f_1, \ldots, f_n) : t \in \mathrm{Pol}_n \mathbb{B},\ f_1, \ldots, f_n \in \mathcal{F}_I \}.$$

Clearly this is a subuniverse, so we need to show that it is a (j,k)-strategy as well.

If $\begin{array}{c} f_1 \subseteq g_1 \\ \vdots \\ f_n \subseteq g_n \end{array}$ with $\begin{array}{l} \mathrm{dom}(f_1) = \ldots = \mathrm{dom}(f_n) \\ \mathrm{dom}(g_1) = \ldots = \mathrm{dom}(g_n) \end{array}$

then $t(f_1, \ldots, f_n) \subseteq t(g_1, \ldots, g_n)$, so $\overline{\mathcal{F}}$ is closed under subfunctions. The same argument shows that it also has the (j,k)-forth property.

<u>Lemma</u>: Suppose that $\mathbb{B}$ has an r-ary near-unanimity polymorphism, max arity of $\mathbb{B} \leq r-1$, and $\mathcal{F}$ is a $(j, j+1)$-strategy for $\mathbb{A}$ and $\mathbb{B}$ with $r-1 \leq j$. Then there is a $(j+1, j+2)$-strategy as well.

<u>Proof</u>: For each $f \in \mathcal{F}$ with $\mathrm{dom}(f) = \{a_1, \ldots, a_{j+1}\}$ and $a_{j+2} \in A \setminus \mathrm{dom}(f)$ we will construct $g : A \to B$ such that $f \subseteq g$, $\mathrm{dom}(g) = \{a_1, \ldots, a_{j+2}\}$ and the projection of g to any $j+1$ coordinate is in $\mathcal{F}$.

This is enough, as then g is a partial-hom. (because $r-1 \leq j+1$) and the collection of these g partial operations together with $\mathcal{F}$ is a $(j+1, j+2)$-strategy.

(this is weaker than we stated, but we need later that $r \leq j+1$)

$$\begin{array}{llllllll}
 & a_1 \ldots & a_r & a_{r+1} \ldots & a_{j+1} & a_{j+2} & & \\
f: & b_1 & b_r & b_{r+1} \ldots & b_{j+1} & - & \in \mathcal{F} & \\
\hline
\exists f_1: & - & b_2 \ldots & \ldots & b_{j+1} & c_1 & \in \mathcal{F} & \text{extension of } f|_{\{a_2,\ldots,a_{j+1}\}} \\
\exists f_2: & b_1 & - & b_3 \ldots & b_{j+1} & c_2 & & \\
\vdots & & & & & & & \\
\exists f_r: & b_1 \ldots & b_{r-1} - & b_{r+1} \ldots & b_{j+1} & c_r & (r \leq j+1) & \\
\hline
\end{array}$$

Let g: $b_1 \ldots \quad b_{j+1} \; t(c_1,\ldots,c_r)$

If you take any projection, say to $\{a_2,\ldots,a_{j+2}\}$ then by the $(j,j+1)$-forth property again

$$\begin{array}{lllllll}
f_1: & - & b_2 \ldots & & b_{j+1} & c_1 & \in \mathcal{F} \\
\exists f_2': & - & d_2 \, b_3 \ldots & & b_{j+1} & c_2 & \\
\exists f_3': & - & b_2 \, d_3 \, b_4 \ldots & & b_{j+1} & c_3 & \\
\vdots & & & & & & \\
\exists f_r': & - & b_2 \ldots b_{r-1} \, d_r \, b_{r+1} \ldots & & b_{j+1} & c_r & \in \mathcal{F} \\
\hline
\text{apply } t: & & b_2 \, b_3 \ldots & & b_{j+1} & t(c_1,\ldots,c_r) & \in \overline{\mathcal{F}}
\end{array}$$

we can assume that $\mathcal{F} = \overline{\mathcal{F}}$.

Similarly for the other projections.

Def: $\mathbb{B}$ has width j __________ if $\exists \ell$ such that
$CSP(\mathbb{B}) = \{ \mathbb{A} : \exists (j,\ell)\text{-strategy for } \mathbb{A} \text{ and } \mathbb{B} \}$

Prop: $CSP(\mathbb{B}) \subseteq \{ \mathbb{A} : \qquad \}$ always.

Take a homomorphism $f: \mathbb{A} \to \mathbb{B}$ and all of it's subfunctions, then that is a (j,ℓ)-strategy.

<u>Comment</u>: k needs to be larger than the maximum arity of $\mathbb{B}$, otherwise there are tuples in $\mathbb{A}$ that can never be verified (taken into account).

<u>Lemma</u>: Given $\mathbb{B}$, j and k, then for any $\mathbb{A}$ we can construct a (j,k)-strategy in polynomial time in $|A|$. or show that $\mathbb{A} \notin CSP(\mathbb{B})$.

<u>Proof</u>: Take all partial homomorphisms of domain size less than or equal to k. If condition (1) or (2) is not satisfied in the definition of (j,k)-strategy, then we remove the offending partial homomorphism. If we reach $\mathcal{F} = \emptyset$, then there is no homomorphism from $\mathbb{A}$ to $\mathbb{B}$ (the subfunctions of a full homomorphism can never been removed). Otherwise we end up with a (j,k)-strategy in polinomial time.

<u>Corollary</u>: If $\mathbb{B}$ has finite width, then $CSP(\mathbb{B})$ is in P.

<u>Theorem</u>: If $\mathbb{B}$ has an r-ary near-unanimity polymorphism, then $\mathbb{B}$ has width $r-1$. (case 6).
(that is $CSP(\mathbb{B})$ is in P).

<u>Proof</u>: Let $k = \max(\text{max arity of } \mathbb{B}, r)$. Then by the previous lemma we get an (r,k)-strategy $\mathcal{F}$ (or else $\mathbb{A} \notin CSP(\mathbb{B})$). Let $\tilde{\mathbb{B}}$ be the structure containing the projections of the relations to coordinates of size $\leq r-1$. We know that $\mathcal{F}$ is also an (r,k)-strategy for $\tilde{\mathbb{A}}$ and $\tilde{\mathbb{B}}$ (where $\tilde{\mathbb{A}}$ is obtained in the obvious way) and any hom. from $\tilde{\mathbb{A}}$ to $\tilde{\mathbb{B}}$ is a hom. from $\mathbb{A}$ to $\mathbb{B}$. But then we have an $(r, r+1)$-strategy which we can push to an $(|A|-1, |A|)$-strategy, which means that the empty partial mapping $\emptyset \in \mathcal{F}$ can be extended to a full homomorphism.

Corollary: Dichotomy holds for 2-element structures.

Proof: Use the previous lemmas and theorems.

Lemma: If $\mathbb{B}$ has a $\wedge$ polymorphism, then $\mathbb{B}$ has width 1.

Proof: Let k be the max arity of $\mathbb{B}$, $j=1$, and take a $(1,k)$-strategy for $\mathbb{A}$ and $\mathbb{B}$. For any $a \in A$, $\overline{\mathcal{F}}_{\{a\}} \subseteq A$. Let $g : A \to B$ defined as

$$g(a) = \bigwedge\{f(a) : f \in \mathcal{F}_{\{a\}}\} \in B.$$

For any $(a_1, \dots, a_n) \in R^{\mathbb{A}}$, $R \in \mathcal{R}$ $\quad (n \leq k)$

$\exists\ g_1 \in \overline{\mathcal{F}}_{\{a_1\}}$:

$$\begin{array}{c|cccc|l}
 & a_1 & a_2 & \dots & a_n & \\
\hline
g_1 & g(a_1) & ? & \dots & ? & \in \overline{\mathcal{F}}_{\{a_1,\dots,a_n\}} \\
g_2 & ? & g(a_2) & ? \dots & ? & \\
\vdots & & & & & \\
g_n & ? & \dots & ? & g(a_n) & \in \overline{\mathcal{F}}_{\{a_1,\dots,a_n\}} \\
\hline
\wedge \quad g' & g(a_1) & g(a_2) & \dots & g(a_n) & \in \mathcal{F}_{\{a_1,\dots,a_n\}}
\end{array}$$

so $(g(a_1), \dots, g(a_n)) \in R^{\mathbb{B}}$. This proves that g is a homomorphism. ▨

(Maybe we should have done this first).

CSP for algebras

Def: By an instance of CSP we mean a triple $I = (V, A, \mathcal{C})$ where V is a set of variables, A is the domain, $\mathcal{C}$ is a set of constraints, and each $C \in \mathcal{C}$ is a pair $C = (S, R)$ where $S \subseteq V$ is the scope of the constraint and $R \subseteq B^S$ is the constraint relation.

A solution is a mapping $f: V \to B$ such that for any constraint $C = (S, R) \in \mathcal{C}$ we have $f|_S \in R$.

Def: Let Γ be a set of relations on A. By $CSP(\Gamma)$ we mean the problem of deciding whether an instance of CSP with constraint relations in Γ have a solution.

Lemma: If Γ is finite, then $CSP(\Gamma)$ is poly-time equivalent to $CSP((B; \Gamma))$ (CSP for rel. structures).

Def: If $\underline{A} = (A; \mathcal{F})$ is an algebra on a finite set, then by $CSP(\underline{A})$ we mean $CSP(\mathrm{Inv}(\Gamma))$.

Def: Γ is tractable if $CSP(\Gamma)$ is in P,
is locally tractable if $CSP(\Gamma_0)$ is in P for all finite $\Gamma_0 \subseteq \Gamma$.

Note: If $\underline{A}$ has finitely many operations, then CSP($\underline{A}$) is a decision problem (we can check in poly-time if the relations are subuniverses) but in general CSP($\underline{A}$) is a relative decision problem (we must trust that all relations are subuniverses).

Def: An instance is k-minimal if

(1) $\forall K \subseteq V$ of size at most k there exists a constraint $C = (S, R) \in \mathcal{C}$ such that $K \subseteq S$,

(2) If $(S_1, R_1), (S_2, R_2) \in \mathcal{C}$ and $K \subseteq S_1 \cap S_2$, $|K| \leq k$, then $R_1|_K = R_2|_K$.

Lemma: For a fixed k, any instance can be converted to a k-minimal instance in poly-time.
If the original instance was for CSP(Γ), then the k-minimal instance is for CSP($\langle\Gamma\rangle$).

Def: $\underline{A}$ has relational width k, if every k-minimal instance of CSP($\underline{A}$) in which all constraint relations are non-empty has a solution.

(this is "global" relational width)

Lemma: If $\underline{A}$ has a near-unanimity term operation of arity r then $\underline{A}$ has relational width $r-1$.

Proof: The original proof for CSP($\mathbb{B}$) works, except we need to construct all partial homomorphisms in polynomial time. However, the max arity is not fixed, so this could take exponential time. But we can construct an $r-1$-minimal instance in poly-time. If none of the relations are empty, then we know that this can be turned into a $(r-1,\ell)$-strategy where ℓ is larger than the max arity. We do not need to construct this, it is enough to know that it exists, because then we are guaranteed the existence of a homomorphism, and that is what we need.

(It is important, that the instance of CSP(Γ) contains the full relations, not just encoded tuples)

Question: If CSP($(A;\Gamma)$) has width ℓ for all finite $\Gamma \subseteq \mathrm{Inv}(\underline{A})$, then does $\underline{A}$ have rel' width ℓ?

Lemma If $\underline{A}$ has a semilattice term operation, then $\underline{A}$ has relational width 1. (so CSP($\underline{A}$) is in P).

Thm: If $\underline{A}$ is a two-element algebra, then CSP($\underline{A}$) is NP-complete if $\underline{A}$ is term equivalent to a perm. group on $\{0,1\}$, otherwise CSP($\underline{A}$) is in P.

(this is the global version, we would need the $p(x,y,z)=x+y+z$ case too, but that works as well for arbitrary sets of relations)

Lemma: If $\underline{A} \leq \underline{B}$, then CSP($\underline{A}$) is poly-time reducible to CSP($\underline{B}$).

Proof: Ever relation $R \leq A^n$ is a relation of $\mathbb{B}$.
Every CSP($\mathbb{B}$) for $\underline{A}/\vartheta$ is polytime reducible to some CSP($\mathbb{B}$) for $\underline{A}$.

Lemma: If $\underline{A}$ is idempotent, and ϑ is a congruence of $\underline{A}$ then CSP($\underline{A}/\vartheta$) is locally poly-time reducible to CSP($\underline{A}$). (the degree of the polynomial depends on the max. arity of the relations).

Proof: Take a relation $R \subseteq (A/\vartheta)^n$. The elements of R are $(a_1/\vartheta, \dots, a_n/\vartheta) \in R$. Define

$$\bar{R} = \bigcup \{(a_1/\vartheta) \times \dots \times (a_n/\vartheta) : (a_1/\vartheta, \dots, a_n/\vartheta) \in R\}$$

This is a subuniverse of $\underline{A}^n$ because $\underline{A}$ is idempotent (so $(a_1/\vartheta) \times \dots \times (a_n/\vartheta) \leq \underline{A}^n$) and ϑ^n is a congruence on $\underline{A}^n$.

Then the instance $(V; \{(S, \bar{R}) : (S, R) \in \mathcal{C}\})$ of CSP($\underline{A}$) has a solution if and only if $(V; \mathcal{C})$ of CSP($\underline{A}/\vartheta$) has a solution.

Exercise: Show that if $\underline{A}$ is of finite signature, and $\vartheta \in \mathrm{Con}\,\underline{A}$, does CSP($\underline{A}/\vartheta$) poly-time reducible to CSP($\underline{A}$). ?

Lemma: If n is a fixed integer, then CSP($\underline{A}^n$) is poly-time reducible to CSP($\underline{A}$).

Def: If p is a unary polynomial of $\underline{A}$, then define $p(\underline{A}) = (p(A); \{p(f(x_1,\dots,x_n)) : f \in \mathrm{Clo}\,\underline{A}\})$.

Lemma: If p is a unary polynomial of $\underline{A}$, then $\mathrm{CSP}(p(\underline{A}))$ is locally poly-time equivalent to $\mathrm{CSP}(\underline{A})$.

Proof: Take finite $\Gamma \subseteq \mathrm{Inv}(p(\underline{A}))$.

For $R \in \Gamma$, $R \subseteq (p(A))^n$ define $\bar{R}$ to be the subalgebra of $\underline{A}^k$ generated by R, and let $\bar{\Gamma} = \{\bar{R} : R \in \Gamma\}$.

Take an instance $I = (V; \mathcal{C})$ of $\mathrm{CSP}(\Gamma)$. Put $\bar{\mathcal{C}} = \{(S, \bar{R}) : (S, R) \in \mathcal{C}\}$. We claim that the instance $(V; \bar{\mathcal{C}})$ of $\mathrm{CSP}(\bar{\Gamma})$ has a solution iff $(V; \mathcal{C})$ does.

$\Leftarrow$ trivial.