Group Order Logic

Anatole Dahan

University of Cambridge
Université Paris-Cité
ENS Paris, Inria

Logic in Computer Science 2025

Motivation

Introduce ord, a permutation group operator.

- Quest of a logic for P (see [Gur88])
- Immerman-Vardi theorem: FP over *ordered structures*
- Over arbitrary structures:

$$\mathrm{FP} < \mathrm{FP} + \mathrm{C} < \mathrm{FP} + \mathrm{rk} < \mathrm{P}$$

- More general algebraic operator
- Over restricted classes of unordered structures:
  - $\mathrm{FP} + \mathrm{C} = \mathrm{P}$ for bounded tree-width [GM99]
  - $\mathrm{FP} + \mathrm{C} = \mathrm{P}$ when excluded minor [Gro17].
  - Canonisation : if $\mathcal{L} \geq \mathrm{FP}$ canonizes $\mathcal{C}$, $\mathcal{L}$ captures P on $\mathcal{C}$.

The role of permutation groups in Graph Isomorphism

Graph Automorphism problem ($\mathsf{GA}_{\mathcal{C}}$)	
Input:	$\mathcal{G} \in \mathcal{C}$
Output:	$S \subseteq \mathrm{Sym}(V_{\mathcal{G}})$ s.t. $\langle S \rangle = \mathrm{Aut}(\mathcal{G})$

- If $\mathcal{C}$ union-closed, $\mathsf{GI}_{\mathcal{C}} \leq_{\mathsf{P}} \mathsf{GA}_{\mathcal{C}}$
- Many results for Graph Iso and/or Canonisation on restricted classes of graphs [Bab79, Luk82, BL83, Bab16]. Primitive operations:

Perm. Group Membership Problem	
Input:	$S \subseteq \mathrm{Sym}(D)$ and $\sigma \in \mathrm{Sym}(D)$
Question:	Does $\sigma \in \langle S \rangle$?

$\leq_{\mathsf{L}}^{T}$

Perm. Group Order Problem	
Input:	$S \subseteq \mathrm{Sym}(D)$
Output:	$\lvert\langle S \rangle\rvert$

Both are in P: Schreier-Sims algorithm.

Plan

Definition of the operator

$\mathrm{FP} + \mathrm{rk} \leq \mathrm{FP} + \mathrm{ord}$

$\mathrm{FP} + \mathrm{ord} \not\leq \mathrm{FP} + \mathrm{rk}$

The ord operator

Definition

$\varphi(\vec{s}, \vec{t})$ (with $\mathrm{type}(\vec{s}) = \mathrm{type}(\vec{t}) = T$) *defines* $\sigma \in \mathrm{Sym}(A^T)$ if

$$\forall \vec{b}, \vec{c} \in A^T, \sigma(\vec{b}) = \vec{c} \iff (\mathfrak{A}, \vec{b}, \vec{c}) \models \varphi$$

- $\mathrm{graph}(\sigma) = \varphi(\mathfrak{A})$
- $\sigma = \mathrm{perm}(\varphi(\mathfrak{A}))$

Definition

A formula $\varphi(\vec{p}, \vec{s}, \vec{t})$ defines $S \subseteq \mathrm{Sym}(A^T)$ *binding* $\vec{p}$ if

$$\{\mathrm{perm}(\varphi(\mathfrak{A}, \vec{a})) \mid \vec{a} \in A^{\vec{p}}\} = S.$$

$(\mathrm{ord}_{\vec{p}.\vec{s}.\vec{t}}\ \varphi)$ is a *numerical predicate* (of arity $2 \cdot |T|$) encoding $|\langle S \rangle|$.

Plan

Definition of the operator

$\mathrm{FP} + \mathrm{rk} \leq \mathrm{FP} + \mathrm{ord}$

$\mathrm{FP} + \mathrm{ord} \not\leq \mathrm{FP} + \mathrm{rk}$

Outline of the proof

- If $\varphi_M(\vec{x}, \vec{y}, \lambda)$ defines a matrix,

$$\begin{aligned}(\mathsf{rk}_{\vec{x},\vec{y}}\varphi_M.p) &= \dim_{\mathbb{F}_p}(\mathrm{Im}_{\mathbb{F}_p}(M)) \\ &= \log_p |\mathrm{Im}_{\mathbb{F}_p}(M)|\end{aligned}$$

  where $\mathrm{Im}_{\mathbb{F}_p}(M) \leq \mathbb{F}_p^{A^{\vec{y}}}$ additive group.
- $\log_p$ is definable (Immerman-Vardi theorem)
- New goals:
  1. permutation representation of $\mathbb{F}_p^{A^{\vec{y}}}$
  2. define a generating set for $\mathrm{Im}_{\mathbb{F}_p}(M)$.

Subgoal 1: Permutation representation of $\mathbb{F}_p^{A^{\vec{y}}}$.

- For $p \in \mathbb{N}^*$,

$$\begin{aligned} \mathrm{repr}_p : \mathbb{F}_p &\to S_p \\ k &\mapsto (i \mapsto i + k \mod p) \end{aligned}$$

  is FPC-definable.
- For T_1, T_2,

$$\begin{aligned} \iota_{T_1,T_2} : \mathrm{Sym}(A^{T_2})^{A^{T_1}} &\to \mathrm{Sym}(A^{T_1} \times A^{T_2}) \\ (g_{\vec{a}})_{\vec{a} \in A^{T_1}} &\mapsto ((\vec{a}, \vec{b}) \mapsto (\vec{a}, (g_{\vec{a}}(\vec{b})))) \end{aligned}$$

  is FPC-definable.
- Conclusion: $\iota_{\vec{y},\mu} : \mathbb{F}_p^{A^{\vec{y}}} \simeq \mathrm{Sym}(A^{\vec{y}} \times A^{<})$ is FPC-definable.

Subgoal 2: Generating set for $\mathrm{Im}_{\mathbb{F}_p}(M)$

- $((\mathbb{F}_p)^{A^{\vec{x}}}, +)$ generated by $\{\lambda \cdot \hat{e}_{\vec{a}} \mid \vec{a} \in A^{\vec{x}}, \lambda < p\}$.

$\rightsquigarrow$ $\mathrm{Im}_{\mathbb{F}_p}(M)$ is generated by $\{M \cdot (\lambda \cdot \hat{e}_{\vec{a}}) \mid \vec{a} \in A^{\vec{x}}, \lambda < p\}$.

- Given φ_M,

$$(\vec{a}, \lambda) \mapsto \iota_{\vec{y},\mu}(M \cdot (\lambda \cdot \hat{e}_{\vec{a}}))$$

FPC-definable. □

Remark

Proof generalizes: FP + ord solves arbitrary systems of linear equations over any abelian group.

Plan

Definition of the operator

$\mathrm{FP} + \mathrm{rk} \leq \mathrm{FP} + \mathrm{ord}$

$\mathrm{FP} + \mathrm{ord} \not\leq \mathrm{FP} + \mathrm{rk}$

Preliminaries

- Lichter '21: $\mathrm{FP} + \mathrm{rk} < \mathrm{P}$
- Last remark: decision problem separation
- The separating query is defined on a class of structures with Abelian Colours.
- We show $\mathrm{FP} + \mathrm{ord}$ canonises (and thus captures P on) structures with Abelian Colours, $\rightsquigarrow$ $\mathrm{FP} + \mathrm{rk} < \mathrm{FP} + \mathrm{ord}$.

Structures with Abelian Colours

- Structure $\mathfrak{A}$ ordered partition
$$A_1 \preceq A_2 \preceq \cdots \preceq A_m$$
- For each $i \leq m$, abelian group Γ_i acting transitively on A_i ($\rightsquigarrow |\Gamma_i| = |A_i|$)
- For each i, $\mathfrak{A}$ equipped with an enumeration $(\gamma_j^i)_{j<|A_i|}$ of Γ_i

$$\forall a \in A_i, (\mathrm{map}_a^i)^{-1} := j \mapsto \gamma_j^i(a) \text{ bijection}$$

$\rightsquigarrow$ $a \mapsto \mathrm{map}_a^i$ linear family of definable orderings of A_i.

- $\mathcal{O}(A_i) := \{\mathrm{map}_a^i, a \in A_i\}$, $\mathcal{O}(A) := \prod_{i=1}^m \mathcal{O}(A_i)$.

The canonisation algorithm

Algorithm 1: Canonisation procedure

Input : $\mathfrak{A} = (A, E, \prec, \Phi)$ a structure with Abelian colours

Output: A numerical relation $E^{<}$ isomorphic to E

$\mathcal{C} := \mathcal{O}(A)$;

for $(i, j) \in [m]^2$ **do**

  find $E^{<}_{i,j}$, the smallest lexicographical encoding of $E \cap (A_i \times A_j)$ compatible with $\mathcal{C}$, i.e. $\exists \sigma \in \mathcal{C}, \mathrm{enc}(E, \sigma)_{\upharpoonright A_i \times A_j} = E^{<}_{i,j}$;

  $\mathcal{C} \leftarrow \{\sigma \in \mathcal{C}, \mathrm{enc}(E, \sigma)_{\upharpoonright A_i \times A_j} = E^{<}_{i,j}\}$;

return $E^{<} := \bigcup_{i,j} E^{<}_{i,j}$

(same algorithm as [Pak15, chapter 6])

The canonisation algorithm

Algorithm 1: Canonisation procedure

Input : $\mathfrak{A} = (A, E, \prec, \Phi)$ a structure with Abelian colours

Output: A numerical relation $E^{<}$ isomorphic to E

$\mathcal{C} := \mathcal{O}(A)$;

for $(i, j) \in [m]^2$ **do**

  find $E^{<}_{i,j}$, the smallest lexicographical encoding of $E \cap (A_i \times A_j)$ compatible with $\mathcal{C}$, i.e. $\exists \sigma \in \mathcal{C}, \mathrm{enc}(E, \sigma)_{\restriction A_i \times A_j} = E^{<}_{i,j}$;

  $\mathcal{C} \leftarrow \{\sigma \in \mathcal{C}, \mathrm{enc}(E, \sigma)_{\restriction A_i \times A_j} = E^{<}_{i,j}\}$;

return $E^{<} := \bigcup_{i,j} E^{<}_{i,j}$

(same algorithm as [Pak15, chapter 6])

Representing labeling cosets: three challenges

- The usual representation ($\mathcal{C} = \sigma H$) of cosets is not isomorphism-invariant.
- Computation of subgroups is not isomorphism-invariant.

- When $A \neq A^{<}$, labeling cosets are not group cosets (i.e. $\mathcal{C} \nsubseteq \mathrm{Sym}(A)$).

Representing labeling cosets: three challenges

- The usual representation ($\mathcal{C} = \sigma H$) of cosets is not isomorphism-invariant.
- Computation of subgroups is not isomorphism-invariant.

Fix: Morphism-definability

- When $A \neq A^<$, labeling cosets are not group cosets (i.e. $\mathcal{C} \not\subseteq \mathrm{Sym}(A)$).

Morphism-definability

Definition

R a relation symbol of arity $2k$.
$\varphi_m(R, \vec{x}, \vec{y})$ *defines a morphism* $m : G \to \mathrm{Sym}(A^{|\vec{x}|})$ on $\mathfrak{A}$, where $G \leq \mathrm{Sym}(A^k)$ if, for all $\sigma \in G$,

$$\varphi_m(\mathfrak{A}, R \leftarrow \mathrm{graph}(\sigma)) = \mathrm{graph}(m(\sigma))$$

$H \trianglelefteq G \leq \mathrm{Sym}(A^T)$ is morphism-definable from G in $\mathfrak{A}$ if:

- There is a definable generating set for G in $\mathfrak{A}$
- there is a $\mathcal{L}$-formula φ_m which defines a morphism $m : G \to \mathrm{Sym}(A^{T'})$ on $\mathfrak{A}$ such that $\ker(m) = H$.

Properties of morphism-definability

- If H is morphism-definable from G in $\mathfrak{A}$, then $\mathrm{FP} + \mathrm{ord}$ defines $|H|$ and membership to H.
- Moreover, the morphism m defining H in G defines a bijection between cosets of H in G and $\mathrm{Im}(m)$.

- If H_1 and H_2 are morphism-definable from G in $\mathfrak{A}$, then so is $H_1 \cap H_2$.

Properties of morphism-definability

- If H is morphism-definable from G in $\mathfrak{A}$, then $\mathrm{FP} + \mathrm{ord}$ defines $|H|$ and membership to H.
- Moreover, the morphism m defining H in G defines a bijection between cosets of H in G and $\mathrm{Im}(m)$.

$\rightsquigarrow$ solves the coset representation issue

- If H_1 and H_2 are morphism-definable from G in $\mathfrak{A}$, then so is $H_1 \cap H_2$.

Properties of morphism-definability

- If H is morphism-definable from G in $\mathfrak{A}$, then $\mathrm{FP} + \mathrm{ord}$ defines $|H|$ and membership to H.
- Moreover, the morphism m defining H in G defines a bijection between cosets of H in G and $\mathrm{Im}(m)$.

$\rightsquigarrow$ solves the coset representation issue

- If H_1 and H_2 are morphism-definable from G in $\mathfrak{A}$, then so is $H_1 \cap H_2$.

$\rightsquigarrow$ solves the subgroup computation issue

Representing labeling cosets: three challenges

- The usual representation ($\mathcal{C} = \sigma H$) of cosets is not isomorphism-invariant.
- Computation of subgroups is not isomorphism-invariant.

Fix: Morphism-definability

- When $A \neq A^<$, labeling cosets are not group cosets (i.e. $\mathcal{C} \not\subseteq \mathrm{Sym}(A)$).

Representing labeling cosets: three challenges

- The usual representation ($\mathcal{C} = \sigma H$) of cosets is not isomorphism-invariant.
- Computation of subgroups is not isomorphism-invariant.

Fix: Morphism-definability

- When $A \neq A^{<}$, labeling cosets are not group cosets (i.e. $\mathcal{C} \nsubseteq \mathrm{Sym}(A)$).

Fix: Labeling group

Labeling group

- Algorithmic perspective:
  - encoding of $\mathfrak{A} \approx$ one fixed $\sigma : A \to A^<$.
  - Represent labeling $\ell : A \to A^<$ by the unique $\tau \in \mathrm{Sym}(A)$ s.t. $\ell = \sigma\tau$.
  - Extends to cosets: $\ell G = \sigma\tau G$, and $\tau G \subseteq \mathrm{Sym}(A)$.
  - Choice of σ not isomorphism-invariant.

Labeling group

- Algorithmic perspective:
  - encoding of $\mathfrak{A} \approx$ one fixed $\sigma : A \to A^<$.
  - Represent labeling $\ell : A \to A^<$ by the unique $\tau \in \mathrm{Sym}(A)$ s.t. $\ell = \sigma\tau$.
  - Extends to cosets: $\ell G = \sigma\tau G$, and $\tau G \subseteq \mathrm{Sym}(A)$.
  - Choice of σ not isomorphism-invariant.
- Unordered setting with Abelian colouring:
  - families $\mathcal{O}(A_i)$ of labelings of A_i indexed by A_i ($a \mapsto \mathsf{map}_a^i$)
  - Represent labeling $\ell : A \to A^<$ by $(\tau_a)_{a \in A}$ s.t.

$$\forall i, \forall a \in A_i, \mathsf{map}_a^i \tau_a = \ell_{\restriction A_i}$$
$$\rightsquigarrow \tau_a = (\mathsf{map}_a^i)^{-1}\ell.$$

  - Yields $\varphi : \mathcal{C}^* \to \mathrm{Sym}(A)^A$. Thus, $\iota \circ \varphi : \mathcal{C}^* \to \mathrm{Sym}(A \times A)$. ($\iota := \iota_{A,A}$)

Definition of ι

Labeling group

- $\exists \mathcal{G} \leq \mathrm{Sym}(A \times A)$ with definable generating set, s.t. $(\iota \circ \varphi)(\mathcal{O}(A)) \subseteq \mathcal{G}$ ▸ Definition of $\mathcal{G}$
- $(\iota \circ \varphi)(\mathcal{O}(A))$ is a coset of a morphism-definable subgroup $\Gamma^* \leq \mathcal{G}$. ▸ Definition of Γ^*
- Given an encoding of $E \cap (A_i \cap A_j)$, the corresponding labelings in $\mathcal{O}(A)$ form a coset of a morphism-definable subgroup $\mathrm{Aut}(E_{i,j})^*$ of Γ^* ▸ Definition of $\mathrm{Aut}(E_{i,j})^*$

Labeling group

- $\exists \mathcal{G} \leq \mathrm{Sym}(A \times A)$ with definable generating set, s.t. $(\iota \circ \varphi)(\mathcal{O}(A)) \subseteq \mathcal{G}$ ▸ Definition of $\mathcal{G}$
- $(\iota \circ \varphi)(\mathcal{O}(A))$ is a coset of a morphism-definable subgroup $\Gamma^* \leq \mathcal{G}$. ▸ Definition of Γ^*
- Given an encoding of $E \cap (A_i \cap A_j)$, the corresponding labelings in $\mathcal{O}(A)$ form a coset of a morphism-definable subgroup $\mathrm{Aut}(E_{i,j})^*$ of Γ^* ▸ Definition of $\mathrm{Aut}(E_{i,j})^*$

Requires Γ_i abelian for all i.

Conclusion

- How far goes the canonisation power of $\mathrm{FP} + \mathrm{ord}$?
- $\mathrm{FO} + \mathrm{ord}$?
- $\mathrm{CPT} + \mathrm{ord}$?
- Inexpressibility results?

Technical definitions: $\mathcal{G}$

$\mathcal{O}(A)$ elements out of reach. But, any $\pi \in \mathcal{O}(A)$ is a product of elements of $\mathcal{O}(A_i)$ which are definable.

$$\mathcal{G} := \langle \bigcup_i \iota \circ \varphi_i(\mathcal{O}(A_i)) \rangle$$

$$\text{where } \varphi_i(\sigma)_a := \begin{cases} \varphi(\sigma)_a & \text{if } a \in A_i \\ 1 & \text{otherwise} \end{cases}$$

Technical definitions: Γ^*, $\mathrm{Aut}(E_{i,j})^*$

Let $\Gamma := \prod_i \Gamma_i$

- $\varphi : \mathcal{O}(A) \to \mathrm{Sym}(A)^A$ is compatible with

$$\begin{aligned} \psi : \Gamma &\to \mathrm{Sym}(A)^A \\ \gamma &\mapsto (\gamma_{\restriction A_{i(a)}})_{a \in A} \end{aligned}$$

  (in the sense that $\varphi(\pi\gamma) = \varphi(\pi)\psi(\gamma)$).

- $\mathcal{O}(A) = \pi\Gamma$ for some (any) $\pi \in \mathcal{O}(A)$.

$\rightsquigarrow$ $\varphi(\mathcal{O}(A)) = \varphi(\pi)\psi(\Gamma)$.

$$\begin{aligned} \Gamma^* &:= \psi(\Gamma) \\ \mathrm{Aut}(E_{i,j}) &:= \{\sigma \in \Gamma_i\Gamma_j \mid \forall a \in A_i, b \in A_j, E(a,b) \iff E(\sigma(a), \sigma b)\} \\ \mathrm{Aut}(E_{i,j})^* &:= \psi(\mathrm{Aut}(E_{i,j})) \end{aligned}$$

References I

- László Babai, *Monte-Carlo algorithms in graph isomorphism testing*, Université de Montréal Technical Report, DMS (1979), no. 79-10.
- ———, *Graph Isomorphism in Quasipolynomial Time*, January 2016.
- László Babai and Eugene M. Luks, *Canonical labeling of graphs*, Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing - STOC '83, ACM Press, 1983, pp. 171–183.
- Martin Grohe and Julian Mariño, *Definability and Descriptive Complexity on Databases of Bounded Tree-Width*, Database Theory — ICDT'99 (Gerhard Goos, Juris Hartmanis, Jan Van Leeuwen, Catriel Beeri, and Peter Buneman, eds.), vol. 1540, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999, pp. 70–82.
- Martin Grohe, *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, 1 ed., Cambridge University Press, August 2017.
- Yuri Gurevich, *Logic and the Challenge of Computer Science*, Current Trends in Theoretical Computer Science ed. Egon Boerger (1988).

References II

Eugene M. Luks, *Isomorphism of graphs of bounded valence can be tested in polynomial time*, Journal of Computer and System Sciences **25** (1982), no. 1, 42–65.

Wied Pakusa, *Linear equation systems and the search for a logical characterisation of polynomial time*, Ph.D. thesis, RWTH Aachen University, 2015.