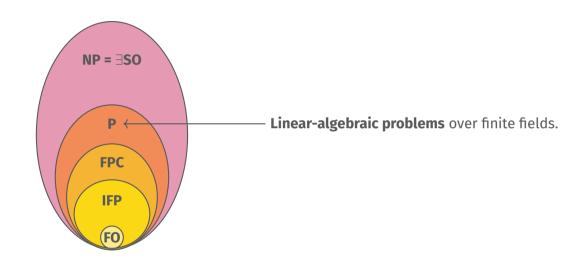
Linear-algebraic logics

Benedikt Pago ¹ ESSLLI 2025, Bochum

¹University of Cambridge



Strengthening FPC



Importing linear algebra into logic

Goal: Enrich FO/IFP with an operator to solve unordered systems of linear equations.

An FO-formula $\varphi(\bar{x}, \bar{y})$ defines a system of equations (a **matrix**) $M(\mathfrak{A}, \varphi)$ in \mathfrak{A} as follows.

- Row index set: $A^{\bar{x}}$.
- Column index set: $A^{\bar{y}}$.

• Entry
$$M(\mathfrak{A}, \varphi)[\bar{a}, \bar{b}] = \begin{cases} 1 & \text{if } \mathfrak{A} \models \varphi(\bar{a}, \bar{b}) \\ 0 & \text{if } \mathfrak{A} \not\models \varphi(\bar{a}, \bar{b}) \end{cases}$$

Example:

Let G = (V, E) be a graph. Then for $\varphi(x, y) = Exy$, $M(G, \varphi)$ is the $(V \times V)$ -adjacency matrix of G.

Rank operators

Let p be a prime. If $\varphi(\bar{x}, \bar{y})$ is a formula (or a numeric term), then $\operatorname{rk}_p(\bar{x}, \bar{y})\varphi$ is a numeric term. **Semantics:** For a two-sorted structure \mathfrak{A}^* ,

$$\llbracket \operatorname{rk}_p(\bar{x},\bar{y})\varphi \rrbracket^{\mathfrak{A}^*} = \operatorname{the} \operatorname{rank} \operatorname{of} M(\varphi,\mathfrak{A}^*), \operatorname{interpreted} \operatorname{as} \operatorname{a} \operatorname{matrix} \operatorname{over} \mathbb{F}_p.$$

- FO + rk_p is the extension of FO with rk_p .
- FO + rk is the extension of FO with rank operators for all primes p.
- IFP + rk_p , IFP + rk are the respective extensions of fixed-point logics.

The power of the rank operator

- **Rank** simulates *counting*: For any prime p, $\operatorname{rk}_p(\bar{x}, \bar{y})$ $(\bar{x} = \bar{y} \land \varphi(\bar{x}))$ is equivalent to the counting term $\#_{\bar{x}}[\varphi(\bar{x})]$.
- FO + rk_p expresses whether a system of linear equations over \mathbb{F}_p has a solution: $A \cdot \mathbf{x} = \mathbf{b}$ has a solution iff $\operatorname{rk}(A) = \operatorname{rk}(A|\mathbf{b})$.
- For any prime p, FO + rk_p expresses (s,t)-connectivity in undirected graphs.
- FO $+ \text{rk}_2$ distinguishes the Cai-Fürer-Immerman graphs that are indistinguishable in FPC.

Example: (s, t)-connectivity in rank logic

(s, t)-connectivity

Input: An undirected graph G = (V, E, s, t) with two distinguished vertices (constants) s and t. **Question:** Is there a path between s and t?

G = (V, E, s, t) has an s-t-path if and only if the following system of equations in \mathbb{F}_p has no solution:

Variables: $\{x_v \mid v \in V\}$.

$$x_s = 1$$

$$x_t = 0$$

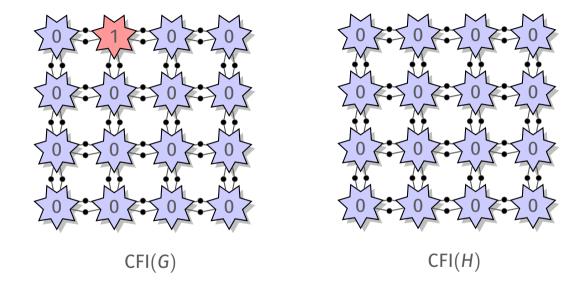
 $x_u - x_v = 0$ for every edge $uv \in E$

Coefficient matrix $M_G \in \mathbb{F}_p^{V^2 \times V}$ defined using formulas

$$\varphi_{+1}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) := ((\mathbf{x}_1 = \mathbf{s} \wedge \mathbf{x}_2 = \mathbf{s} \wedge \mathbf{y} = \mathbf{s}) \vee (\mathbf{x}_1 = \mathbf{t} \wedge \mathbf{x}_2 = \mathbf{t} \wedge \mathbf{y} = \mathbf{t}))$$
$$\vee (\mathbf{E}\mathbf{x}_1\mathbf{x}_2 \wedge \mathbf{x}_1 = \mathbf{y})$$

$$\varphi_{-1}(\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}) \coloneqq (\mathbf{E}\mathbf{x}_1\mathbf{x}_2 \wedge \mathbf{x}_2 = \mathbf{y})$$

Distinguishing Cai-Fürer-Immerman graphs in ${\sf FO}+{\sf rk_2}$



Distinguishing Cai-Fürer-Immerman graphs in $FO + rk_2$

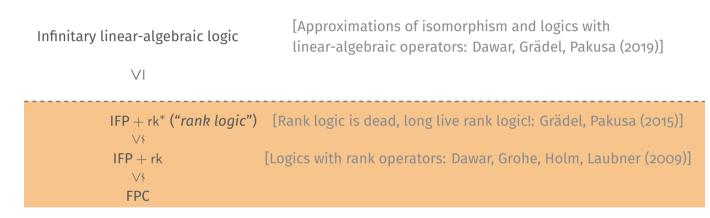
Lemma (Cai, Fürer, Immerman, 1992)

Let G be a connected graph, and $\lambda_0, \lambda_1 \colon V \to \mathbb{Z}_2$ two node labellings.

$$CFI(G, \lambda_0) \cong CFI(G, \lambda_1) \iff \sum_{v \in V} \lambda_0(v) = \sum_{v \in V} \lambda_1(v) \mod 2.$$

In CFI(G, λ), one can FO-define a system of linear equations over \mathbb{Z}_2 which has a solution if and only if $\sum_{v \in V} \lambda(v) = 0 \mod 2$.

A history of rank logics



contained in PTIME

Rank logic is dead, long live rank logic!

Let rk* denote the *uniform* rank operator that takes the prime p as input via a numerical term.

Theorem (Grädel, Pakusa, 2015)

$$IFP + rk \leq IFP + rk^* \leq PTIME$$
.

Proof.

- For contradiction, let $\psi \in IFP + rk$ be a sentence defining rk^* . There is a finite set Ω of primes p such that rk_p appears in ψ .
- Let \mathcal{K} be a class of *CFI graphs over* \mathbb{Z}_q , for a prime $q \notin \Omega$.
- **Technical result:** On K, ψ is equivalent to a sentence in FPC (coprimeness of the rank operators with q)
- FPC cannot distinguish CFI graphs $\implies \psi$ does not distinguish graphs in \mathcal{K} .
- But: rk* does distinguish them.

A game characterisation of IFP $+ rk^*$?

[Grädel, Pakusa]: The uniform operator rk* is the "right" rank operator.

Problem: How to show limitations of IFP $+ rk^*$?

There is a *game characterisation* for IFP + rk* [Dawar, Holm, 2012], but the "natural" game characterises a much richer logic.

Towards infinitary linear-algebraic logic

- Rank is just one example of an isomorphism-invariant property of matrices.
- What if we add an operator for every isomorphism-invariant matrix property?
- There can be operators that are not in PTIME or not even computable, but they are still limited by isomorphism-invariance.
- Equivalence in **infinitary FO** with **all linear-algebraic operators** turns out to have a useful game characterisation.

Isomorphism-invariant linear-algebraic operators

- An *m*-ary linear-algebraic operator is an \mathbb{N} -valued function $f(M_1, \ldots, M_m)$.
- f is isomorphism-invariant if $f(M_1, \ldots, M_m) = f(N_1, \ldots, N_m)$ whenever " $(M_1, \ldots, M_m) \cong (N_1, \ldots, N_m)$ ".
- The matrices (M_1, \ldots, M_m) are viewed as linear transformations of a vector space \mathbb{F}^A , and (N_1, \ldots, N_m) are linear transformations of \mathbb{F}^B .
- " $(M_1, \ldots, M_m) \cong (N_1, \ldots, N_m)$ " if there is a vector space isomorphism $S \colon \mathbb{F}^A \to \mathbb{F}^B$ that maps (M_1, \ldots, M_m) to (N_1, \ldots, N_m) .

Definition (Simultaneous similarity)

We write $(M_1, ..., M_m) \cong (N_1, ..., N_m)$ if the tuples of matrices are simultaneously similar, which means: There exists an invertible matrix S such that $N_i \cdot S = S \cdot M_i$ for all $i \in [m]$.

Linear-algebraic logic

Let f be an m-ary isomorphism-invariant linear-algebraic operator over a finite field \mathbb{F} , and $t \in \mathbb{N}$. Let $\varphi_1, \ldots, \varphi_m$ be formulas. Then

$$Q_f^t(\varphi_1(\bar{x},\bar{y}),\ldots,\varphi_m(\bar{x},\bar{y}))$$

is a formula that is true in a structure \mathfrak{A}^* if

$$f(M(\varphi_1, \mathfrak{A}^*), \dots, M(\varphi_m, \mathfrak{A}^*)) \geq t.$$

Definition (LA [Dawar, Grädel, Pakusa, 2019])

The logic LA is the closure of infinitary FO under quantifiers \mathcal{Q}_f^t for all isomorphism-invariant linear-algebraic operators f, and all $t \in \mathbb{N}$.

For $k \in \mathbb{N}$, LA^k is the k-variable fragment.

Invertible-map equivalence

For $k \in \mathbb{N}$, Q a set of prime numbers, we write

$$\mathfrak{A} \equiv^{\mathsf{IM}}_{k,Q} \mathfrak{B}$$

if $\mathfrak A$ and $\mathfrak B$ agree on all sentences of $\mathsf{LA}^k(Q)\subseteq \mathsf{LA}^k$, the fragment containing only algebraic operators over fields $\mathbb F_p$ with $p\in Q$.

If $\mathfrak{A} \equiv^{\mathsf{IM}}_{\mathsf{h}\,\mathbb{P}} \mathfrak{B}$, then also no sentence in IFP $+ \mathsf{rk}^*$ distinguishes \mathfrak{A} and \mathfrak{B} .

The invertible-map game

 $\mathfrak{A} \equiv_{k,Q}^{\mathsf{IM}} \mathfrak{B}$ if and only if Duplicator has a winning strategy in the **invertible-map game**:

Definition (Dawar, Holm, 2012)

Let $\mathfrak{A}, \mathfrak{B}$ two structures, $k \in \mathbb{N}$ the number of pebbles.

The position after any round is $(\bar{a} \in A^{\ell}, \bar{b} \in B^{\ell})$ with $\ell \leq k$. In each round,

- Spoiler announces a prime $p \in Q$ and picks up some number $2m \le k$ of pebbles from each structure.
- Duplicator chooses all of the following:
 - 1. A partition **P** of $A^m \times A^m$ and a partition **Q** of $B^m \times B^m$ with the same number of parts.
 - 2. A bijection $\lambda : \mathbf{P} \to \mathbf{Q}$.
 - 3. An invertible matrix $S \in \mathbb{F}_p^{A^m \times B^m}$ such that for every $P \in \mathbf{P}$,

$$\chi^{P} = S \cdot \chi^{\lambda(P)} \cdot S^{-1},$$

where $\chi^P(\bar{u}, \bar{v}) = 1$ if $\bar{u}\bar{v} \in P$, and $\chi^P(\bar{u}, \bar{v}) = 0$, otherwise.

• Spoiler chooses $P \in P$, and places the pebbles on a tuple $\bar{w} \in P$, and a tuple $\bar{w}' \in \lambda(P)$.

Efficient decidability of the IM-equivalences

For every $k \in \mathbb{N}$, Q a *finite* set of primes, the following problem is in PTIME.

IM-equivalence

Input: Two structures $\mathfrak{A}, \mathfrak{B}$.

Question: Is $\mathfrak{A} \equiv_{k,0}^{\mathsf{IM}} \mathfrak{B}$?

The algorithm is a refinement of the k-dimensional Weisfeiler Leman graph isomorphism test. It computes a **colouring of the** k-tuples according to their LA $^k(Q)$ -type.

A first limitation of invertible-map equivalences

Fact:

For every prime p, $\equiv_{k,p}^{\text{IM}}$ is an approximation to graph isomorphism that is strictly finer than $\equiv_{\mathcal{C}^k}$.

Theorem (Dawar, Grädel, Pakusa, 2019)

If $Q \neq \mathbb{P}$, then there is no fixed $k \in \mathbb{N}$ such that $\equiv_{k,0}^{\mathsf{IM}}$ is as fine as isomorphism on all structures.

Proof sketch. For a prime $p \notin Q$, non-isomorphic CFI graphs over \mathbb{Z}_p are $\equiv_{k,Q}^{\mathsf{IM}}$ -equivalent. This is shown with a sophisticated algebraic argument, but essentially the same "coprimeness trick" as in Rank logic is dead, long live rank logic!

Question: Is \equiv_{h}^{IM} the same as isomorphism?

An inexpressibility result for IFP $+ rk^*$ and LA

contained in PTIME

An inexpressibility result for IFP $+ rk^*$ and LA

Theorem (Lichter, 2021)

IFP $+ rk^*$ does not capture PTIME.

The **technical contribution** is this:

Theorem (Lichter, 2021)

For every fixed $k \in \mathbb{N}$, there are non-isomorphic CFI-structures over some ring $\mathbb{Z}_{2^{q(k)}}$ that are $\equiv_{k,2}^{\text{IM}}$ -equivalent.

The proof is a Duplicator winning strategy in the IM-game. Combining this with the already known "coprimeness argument" yields:

Theorem (Dawar, Grädel, Lichter, 2022)

There is no $k \in \mathbb{N}$ such that $\equiv_{k,\mathbb{P}}^{\mathsf{IM}}$ is isomorphism.

Winning the invertible-map game

Theorem (Lichter, 2021)

For every fixed $k \in \mathbb{N}$, there are non-isomorphic CFI-structures over some ring $\mathbb{Z}_{2q(k)}$ that are \equiv_{k}^{IM} -equivalent.

- The hard part is not the construction of the structures, but the construction of the invertible matrices in Duplicator's winning strategy.
- Recall that Spoiler moves $2m \le k$ pebbles each round. The winning strategy is defined by induction on m, and the size of the ring $\mathbb{Z}_{2q(m)}$ grows with m.
- In the case m = 1, CFI-structures over \mathbb{Z}_4 suffice.

Winning the invertible-map game

Definition

Let $\mathfrak{A}, \mathfrak{B}$ two structures, $k \in \mathbb{N}$ the number of pebbles.

The position after any round is $(\bar{a} \in A^{\ell}, \bar{b} \in B^{\ell})$ with $\ell \leq k$. In each round,

- Spoiler announces a prime $p \in Q$ and picks up some number $2m \le k$ of pebbles from each structure.
- Duplicator chooses all of the following:
 - 1. A partition **P** of $A^m \times A^m$ and a partition **Q** of $B^m \times B^m$ with the same number of parts.
 - 2. A bijection $\lambda : \mathbf{P} \to \mathbf{Q}$.
 - 3. An invertible matrix $S \in \mathbb{F}_p^{A^k \times B^k}$ such that for every $P \in \mathbf{P}$,

$$\chi^{\mathsf{P}} = \mathsf{S} \cdot \chi^{\lambda(\mathsf{P})} \cdot \mathsf{S}^{-1},$$

where $\chi^P(\bar{u}, \bar{v}) = 1$ if $\bar{u}\bar{v} \in P$, and $\chi^P(\bar{u}, \bar{v}) = 0$, otherwise.

- Spoiler chooses $P \in P$, and places the pebbles on a tuple $\bar{w} \in P$, and a tuple $\bar{w}' \in \lambda(P)$.
- Spoiler wins if the pebbles do not define a local isomorphism.

The picture now

```
PTIME [Separating rank logic from polynomial time: Lichter (2021),
Limitations of the invertible-map equivalences: Dawar, Grädel, Lichter (2022)]

Infinitary linear-algebraic logic

VI

IFP + rk* ("rank logic") 

Group order logic [Group Order Logic: Dahan (2025)]
```

contained in PTIME

 $\begin{array}{c}
\checkmark \\
\mathsf{IFP} + \mathsf{rk} \\
\checkmark \\
\mathsf{FPC}
\end{array}$

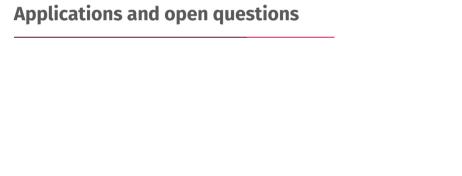
Group order logic

Group order logic is IFP extended by a group order operator.

	Rank logic	Group order logic
Definable object	Matrix $A \in \mathbb{F}_p^{l imes J}$	Generating set of a
	(i.e. generating set of a vector	permutation group
	space)	$\Gamma = \langle \gamma_1, \ldots, \gamma_n \rangle$
Isomorphism-invariant	rk(A)	Γ
property		

Theorem (Dahan, 2025)

- Group order subsumes rank: rk(A) is definable from the size of the column space of A.
- Group order is more powerful than rank: It captures PTIME on CFI graphs, even over rings.



Applications in CSP and Graph Isomorphism

Graph isomorphism: For every $k \in \mathbb{N}$, every finite set of primes Q, the algorithm deciding $\equiv_{k,Q}^{\mathsf{IM}}$ is a *polynomial time* graph isomorphism *heuristic* stronger than k-dimensional Weisfeiler-Leman.

Definition (Temporal CSP)

A *temporal* CSP has an infinite template structure that is FO-definable in $(\mathbb{Q}, <)$.

[Bodirsky, Rydval, Pakusa, 2020] fully classified the descriptive complexity of temporal CSPs:

$$Datalog \leq IFP = FPC \leq IFP + rk_2.$$

In particular, there is a natural IFP + rk_2 -algorithm that solves all these temporal CSPs up to Datalog-reductions.

Why not rank logic over the ring \mathbb{Z} ?

- Rank logic apparently *cannot solve* equation system over *rings* (Lichter).
- Why not define a notion of "rank" over rings, or most generally, over \mathbb{Z} ?
- Possible idea: Use the **Smith normal form** of integer matrices as "rank".
- Such a \mathbb{Z} -rank logic should be able to distinguish all CFI graphs over rings.
- Many interesting CSP and graph isomorphism algorithms solve systems of linear equations over Z.

\mathbb{Z} -affine CSP algorithms

- Let $\mathfrak A$ be an instance of CSP($\mathfrak B$), and $k \in \mathbb N$. The width-k relaxation of " $\mathfrak A \to \mathfrak B$?" is a system of linear equations $\mathsf L^{k,\mathfrak B}_{\mathsf{CSP}}(\mathfrak A)$ which asks to assign weights to solutions of subinstances of size k.
- $L_{CSP}^{k,\mathfrak{B}}(\mathfrak{A})$ has a $\{0,1\}$ -solution if and only if $\mathfrak{A}\to\mathfrak{B}$.
- Solving $L_{CSP}^{k,\mathfrak{B}}(\mathfrak{A})$ over \mathbb{Z} is in polynomial time, and used in many **CSP heuristics** like BLP+AIP, BA^k, \mathbb{Z} -affine k-consistency, cohomological k-consistency.
- $L_{CSP}^{k,\mathfrak{B}}(\mathfrak{A})$ is FO-definable in \mathfrak{A} , so most of these algorithms could be expressed in a rank logic over \mathbb{Z} .

Lower bounds for \mathbb{Z} -affine algorithms using CFI structures

Theorem (Lichter, P., 2025)

There is a polynomial-time solvable CSP which is not solved by the \mathbb{Z} -affine algorithms, except by cohomological k-consistency.

The example is a **combination of CFI structures** over \mathbb{Z}_2 and \mathbb{Z}_3 .

Cohomological *k***-consistency**

Cohomological k-consistency [O'Conghaile 2022]

```
1: Input: Instance \mathfrak{A}.

2: Let \mathcal{H}_0(X) := \operatorname{Hom}(\mathfrak{A}[X], \mathfrak{B}) for every X \in \binom{A}{\leq k}.

3: repeat

4: Let \mathcal{H}'_i(X) \subseteq \mathcal{H}_i(X) be the partial homomorphisms

5: that are not removed by the k-consistency procedure.

6: Let \mathcal{H}_{i+1}(X) \subseteq \mathcal{H}'_i(X) be the partial homomorphisms f: X \to B

7: such that \operatorname{L}^{k,\mathfrak{B}}_{\operatorname{CSP}}(\mathfrak{A}), augmented with the equation x_{X,f} = 1, has a \mathbb{Z}-solution.

8: until \mathcal{H}_{i+1} = \mathcal{H}_i

9: If \mathcal{H}_i(X) = \emptyset for some X \in \binom{A}{\leq k}, then return \mathfrak{A} \not\to \mathfrak{B}.
```

Open problems

- Can IFP + rk_2 solve systems of linear equations over \mathbb{Z}_4 ? This is not ruled out by Lichter's result.
- Define a rank logic over $\mathbb Z$ and a useful game for it.
- Inexpressibility results for group order logic?
- Find a tractable CSP that is **not solved** by **cohomological** *k***-consistency**.
- Can rank logic/group order logic simulate any group-theoretic graph isomorphism algorithm, for example for the class of bounded-degree graphs?

References i

- [1] Manuel Bodirsky, Wied Pakusa, and Jakub Rydval. "Temporal Constraint Satisfaction Problems in Fixed-Point Logic". In: Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science. LICS '20. Saarbrücken, Germany: Association for Computing Machinery, 2020, pp. 237–251. 10.1145/3373718.3394750. https://doi.org/10.1145/3373718.3394750.
- [2] Adam Ó Conghaile. **"Cohomology in Constraint Satisfaction and Structure Isomorphism".** In: 47th International Symposium on Mathematical Foundations of Computer Science, MFCS 2022, August 22-26, 2022, Vienna, Austria. Ed. by Stefan Szeider, Robert Ganian, and Alexandra Silva. 241. LIPIcs. Schloss Dagstuhl Leibniz-Zentrum für Informatik, 2022, 75:1–75:16. 10.4230/LIPICS.MFCS.2022.75. https://doi.org/10.4230/LIPIcs.MFCS.2022.75.
- [3] Anatole Dahan. "Group Order Logic". In: CoRR abs/2505.15359 (2025). 10.48550/ARXIV.2505.15359. arXiv: 2505.15359. https://doi.org/10.48550/arXiv.2505.15359.

References ii

- [4] Anuj Dawar, Erich Grädel, and Moritz Lichter. "Limitations of the invertible-map equivalences". In: Journal of Logic and Computation (Sept. 2022). ISSN: 0955-792X. 10.1093/logcom/exaco58. https://academic.oup.com/logcom/advance-article/doi/10.1093/logcom/exaco58/6687793?guestAccessKey=7349c158-be02-4116-815a-840ac7880a03.
- Anuj Dawar, Erich Grädel, and Wied Pakusa. "Approximations of Isomorphism and Logics with Linear-Algebraic Operators". In: 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019). 132. Leibniz International Proceedings in Informatics (LIPIcs). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019, 112:1–112:14. ISBN: 978-3-95977-109-2. 10.4230/LIPIcs.ICALP.2019.112. http://drops.dagstuhl.de/opus/volltexte/2019/10688.
- Anuj Dawar and Bjarki Holm. "Pebble Games with Algebraic Rules". In: Automata, Languages, and Programming 39th International Colloquium, ICALP 2012, Warwick, UK, July 9-13, 2012, Proceedings, Part II. Ed. by Artur Czumaj et al. 7392. Lecture Notes in Computer Science. Springer, 2012, pp. 251–262. 10.1007/978-3-642-31585-5_25. https://doi.org/10.1007/978-3-642-31585-5%5C_25.

References iii

- [7] Anuj Dawar et al. "Logics with rank operators". In: 2009 24th Annual IEEE Symposium on Logic In Computer Science. IEEE. 2009, pp. 113–122.
- [8] Erich Grädel and Wied Pakusa. "Rank logic is dead, long live rank logic!" In: The Journal of Symbolic Logic 84.1 (Mar. 2019). https://www.cambridge.org/core/journals/journal-of-symbolic-logic/article/rank-logic-is-dead-long-live-rank-logic/F161E336281F2B67E8B3E4CDA5614933.
- [9] M. Lichter and B. Pago. Limitations of Affine Integer Relaxations for Solving Constraint Satisfaction Problems. Ed. by Keren Censor-Hillel et al. Dagstuhl, Germany, 2025. 10.4230/LIPIcs.ICALP.2025.166. https://drops.dagstuhl.de/entities/document/10.4230/LIPIcs.ICALP.2025.166.
- [10] Moritz Lichter. "Separating Rank Logic from Polynomial Time". In: J. ACM (Nov. 2022). https://doi.org/10.1145/3572918.