Linear Algebraic Quantifiers

Anuj Dawar

Department of Computer Science and Technology, University of Cambridge

RiC 2022, UCL, 22 September 2022

Descriptive Complexity

A central question in the field of *Descriptive Complexity* is the question of whether there is a *logic for* P.

On *ordered structures* FP—the extension of first-order logic with a fixed-point operator—suffices. **(Immerman-Vardi)**

FP is not sufficient in the absence of order. This can be shown by constructing properties in P not definable in $L^{\omega}_{\infty\omega}$—finite variable infinitary logic.

Many extensions of FP with additional operators have been studied.

These are studied through the expressive power of $L^{\omega}_{\infty\omega}(Q)$, the extension of $L^{\omega}_{\infty\omega}$ with a set Q of *quantifiers*.

Generalized Quantifiers

A *Lindström quantifier* of relational vocabulary σ is given by:

K—*a class of* σ*-structures, closed under isomorphisms.*

In this talk, we only consider *finite structures*.

$L(K)$ is the extension of a *logic* L with the quantifier for K.

More generally, for a collection Q of quantifiers, $L(Q)$ is the extension of L with *all* quantifiers in Q.

Logics

Logics L we are interested in for the purpose of this talk are

- *first-order logic*—$L_{\omega\omega}$ or FO.
- *infinitary logic*—$L_{\infty\omega}$ or $L_{\omega_1\omega}$.

  The closure of FO under infinitary (or countable) conjunctions.

- k-*variable infinitary logic*—$L^k_{\infty\omega}$.
- *finite-variable infinitary logic*—$L^\omega_{\infty\omega} = \bigcup_{k<\omega} L^k_{\infty\omega}$.

Note that the expressive power of $L_{\omega_1\omega}$ on finite structures is *complete*. That is to say, it can define every *isomorphism-closed* class of structures.

Logics with Generalized Quantifiers

If $\sigma = (R_1, \ldots, R_r)$ we get a formula

$$K\mathbf{x}(\varphi_1(\mathbf{x}_1), \ldots, \varphi_r(\mathbf{x}_r)).$$

$|\mathbf{x}_i| = \mathsf{ar}(R_i)$

The *arity* of the quantifier K is $\max_i \mathsf{ar}(R_i)$.

$L(K)$ is the *minimal* extension of L that can express K and is closed under the operations of L, such as

- *Boolean operations*
- *particularization* (i.e. existential quantification)

Equivalences

For a set of quantifiers Q, write

$$\mathbb{A} \equiv^k_Q \mathbb{B}$$

to denote that $\mathbb{A}$ and $\mathbb{B}$ are not distinguishable in $L^k_{\infty\omega}(Q)$.

For a relational vocabulary τ, we say that $\equiv^k_Q$ is *discrete* if for any pair $\mathbb{A}, \mathbb{B}$ of τ-structures

$$\mathbb{A} \equiv^k_Q \mathbb{B} \quad \text{if, and only if,} \quad \mathbb{A} \cong \mathbb{B}$$

The following are equivalent:

- There is some k such that $\equiv^k_Q$ is discrete on τ-structures.
- The expressive power of $L^\omega_{\infty\omega}(Q)$ is complete on τ-structures.

Arity Hierarchy

Let Q_n denote the collection of *all* n-ary quantifiers.

Theorem (Hella)
For every n, there is a vocabulary τ such that $\equiv^k_{Q_n}$ is not discrete on τ-structures for any k.

The class of structures not definable in $L^{\omega}_{\infty\omega}(Q_n)$ can be constructed to be decidable in P.

Note: τ necessarily contains relations of arity $\geq n+1$.

Unary and Binary Quantifiers

$L^{\omega}_{\infty\omega}(Q_1)$ has the same expressive power as $L^{\omega}_{\infty\omega}(C)$—where C is the collection of all *unary counting quantifiers*.

$\exists^{\geq n}$, $\exists^{\leq n}$

Graph properties in P not definable in $L^{\omega}_{\infty\omega}(C)$ were constructed by **(Cai-Fürer-Immerman)**.

$L^{\omega}_{\infty\omega}(Q_2)$ can express *all* properties of graphs.

These logics are not closed under *first-order interpretations*.

Closure under first-order reductions is a desirable property in *descriptive complexity*, as most interesting complexity classes have it.

First-Order Interpretations

An FO *interpretation* θ of a τ-structure $\mathbb{B}$ in a σ-structure $\mathbb{A}$ is a family of first-order formulas which define the *universe* and *relations* of $\mathbb{B}$ when interpreted in $\mathbb{A}$.

This defines a map from σ-structres to τ-structures, so we write $\mathbb{B} = \theta(\mathbb{A})$.

An FO *reduction* of a class of structures $\mathcal{C}$ to a class $\mathcal{D}$ is a single FO interpretation θ such that $\mathbb{A} \in \mathcal{C}$ if, and only if, $\theta(\mathbb{A}) \in \mathcal{D}$.
We write $\mathcal{C} \leq_{\mathsf{FO}} \mathcal{D}$.

Vectorized Quantifiers

Let $\sigma = (R_1, \ldots, R_r)$ be a relational vocabulary.

A minimal logic extending L, able to express a propety K of σ-structures, and *closed* under first-order interpretations is given by $L(\overline{K})$, where $\overline{K}$ is the collection $\{K_d \mid d \in \omega\}$ of Lindström quantifiers in the vocabularies

$$\sigma_d = (U_d, \sim_d, (R_{i,d})_{i \in [r]})$$

with $\mathsf{ar}(U_d) = d$, $\mathsf{ar}(\sim_d) = 2d$ and $\mathsf{ar}(R_{i,d}) = d \cdot \mathsf{ar}(R_i)$, and

$$\mathbb{A} \in K_d \quad \text{iff} \quad (U_d^{\mathbb{A}} / \sim_d^{\mathbb{A}}, (R_{i,d}^{\mathbb{A}})_{i \in [r]}) \in K.$$

Vectorizations of Unary Quantifiers

Note that $\overline{K} \not\subseteq Q_n$ for any $n \in \omega$.

Let

$$\overline{Q_n} = \bigcup_{K \in Q_n} \overline{K}$$

More generally, for any collection S of quantifiers, let $\overline{S}$ denote the collection of *vectorizations* of quantifiers in S.

Theorem
$L^{\omega}_{\infty\omega}(\overline{Q_1}) \leq L^{\omega}_{\infty\omega}(C)$.

In short, vectorization adds nothing to *unary* quantifiers.

Counting tuples can always be replaced by counting elements.

Vectorizations of Binary Quantifiers

Theorem
$L_{\infty\omega} \leq L_{\omega\omega}(\overline{Q_2})$

In short, with vectorized binary quantifiers, we can express *everything*.

This follows from the fact that for any vocabulary τ, there is a *first-order definable bi-interpretation* to the vocabulary with one binary relation.

So, for any class K of σ-structures, there is a *first-order interpretation* Φ and a class of graphs G such that

$$\Phi(\mathbb{A}) \in G \quad \text{iff} \quad \mathbb{A} \in K.$$

Restricted Classes of Binary Quantifiers

Thus, when it comes to vectorized quantifiers, the *arity hierarchy* has just two levels.

To get *interesting* classes of vectorized quantifiers beyond the unary, we consider *proper subclasses* of $\overline{Q_2}$.

One way to get interesting classes is to *strengthen* the requirement of *isomorphism invariance*.

One such stengthening gives us the *linear algebraic quantifiers*.

Isomorphism Closure

Fix a vocabulary $\sigma = (R_1, \ldots, R_r)$ where all relation symbols are *binary*.

Two σ-structures $\mathbb{A} = (A, R_1^A, \ldots, R_r^A)$ and $\mathbb{B} = (B, R_1^B, \ldots, R_r^B)$ are *isomorphic* if there is a bijection $\beta : A \to B$ with $\beta(R_i^A) = R_i^B$, for all $i \in [r]$.

Equivalently, if we fix bijections between A and $\{1, \ldots, n\}$ on the one hand and B and $\{1, \ldots, n\}$ on the other, then we can view each R_i^A or R_i^B as a $n \times n$ matrix with entries in $\{0, 1\}$.

An *isomorphism* is then an $n \times n$ *permutation matrix* P such that

$$PR_i^A P^{-1} = R_i^B \quad \text{for all } i.$$

Linear Algebraic Equivalence

For a field $\mathbb{F}$, say that $\mathbb{A} = (A, R_1^A, \ldots, R_r^A)$ and $\mathbb{B} = (B, R_1^B, \ldots, R_r^B)$ are $\mathbb{F}$*-linear algebraically equivalent* if

there is an invertible matrix $I \in \mathsf{GL}_n(\mathbb{F})$ *such that*

$$IR_i^A I^{-1} = R_i^B \quad \text{for all } i.$$

Since all the R_i are $\{0, 1\}$-matrices, the existence of such an I only depends on the *characteristic* of $\mathbb{F}$.

Write $\mathbb{A} \cong_p \mathbb{B}$ to denote that the two structures are $\mathbb{F}_p$-linear algebraically equivalent, where
$p \in \{0\} \cup \text{Primes}$ and $\mathbb{F}_p$ is the *prime field* of characteristic p.

Module Isomorphism

There is a way to see the $\mathbb{F}_p$-linear algebraic equivalence of $\mathbb{A} = (A, R_1^A, \ldots, R_r^A)$ and $\mathbb{B} = (B, R_1^B, \ldots, R_r^B)$ as the *isomorphism* of a pair of *modules* over the *polynomial ring*

$$\mathbb{F}_p[x_1, \ldots, x_r].$$

This is useful in establishing that the problem of deciding $\mathbb{A} \cong_p \mathbb{B}$ is in polynomial time.

Linear Algebraic Quantifiers

Write L_p for the collection of all quantifiers over vocabularies of *binary* relations which are invariant under $\cong_p$.

For $\Omega \subseteq \{0\} \cup \mathsf{Primes}$, let

$$L_\Omega = \bigcup_{p \in \Omega} L_p.$$

Rank Quantifiers

For any $p \in \{0\} \cup \mathsf{Primes}$, and $t \in \omega$, let rk_p^t be the quantifier consisting of structures (A, M) where $M \subseteq A \times A$ and

M seen as a matrix in $\mathbb{F}_p^{A \times A}$ has rank at least t.

Rk_p is the collection of quantifiers $\{\mathsf{rk}_p^t \mid t \in \omega\}$.

Rk is the collection of quantifiers $\bigcup_p \mathsf{Rk}_p$.

$L^{\omega}_{\infty\omega}(\overline{\mathsf{Rk}})$ subsumes *rank logic*, the extension of fixed-point logic with *rank operators* which has been studied in descriptive complexity as a candidate logic for P.

Linear Algebraic Logic

For any $\Omega \subseteq \{0\} \cup \mathsf{Primes}$, we define the Ω-linear algebraic logics.

$$\mathsf{LA}^k(\Omega) = L^k_{\infty\omega}(\overline{L_\Omega})$$

$$\mathsf{LA}^\omega(\Omega) = L^\omega_{\infty\omega}(\overline{L_\Omega})$$

Also, write $\equiv^{\mathsf{LA}^k(\Omega)}$ to denote indistinguishability in $\mathsf{LA}^k(\Omega)$. That is, it is another name for $\equiv^k_{\overline{L_\Omega}}$.

This relation is decidable in *polynomial time* (for fixed k) using the module isomorphism algorithm of **Chistov et al.**

Invertible Map Game

The game is played between *Spoiler* and *Duplicator* on $\mathbb{A}$ and $\mathbb{B}$.
We have (as usual) k pebbles each on elements of $\mathbb{A}$ and $\mathbb{B}$.

Play proceeds in the following steps:

1. *Spoiler* announces $p_1, \ldots, p_{2m} \in [k]$ to move.
2. *Spoiler* chooses a *characteristic* p.
3. *Duplicator* gives a *partition* of $\mathbb{A}^{2m}$ into parts $P_1, \ldots, P_t$ and of $\mathbb{B}^{2m}$ into parts $Q_1, \ldots, Q_t$.

   Note: P_i *can be thought of as a* $\mathbb{A}^m \times \mathbb{A}^m$ 0-1 *matrix* M_i *with* $(M_i)_{\overline{a}\overline{b}} = 1$ *iff* $\overline{a}\overline{b} \in P_i$. *Similarly,* Q_i *is a* $\mathbb{B}^m \times \mathbb{B}^m$ *matrix* N_i.

   The partitions must satisfy the condition that there is an *invertible* $I \in \mathbb{F}_p^{\mathbb{B}^m \times \mathbb{A}^m}$ such that $M_i = I^{-1} N_i I$ for all i.
4. *Spoiler* chooses some $i \in \{1, \ldots, t\}$ and an $\overline{a} \in P_i$ and $\overline{b} \in Q_i$ on which the $2m$ pebbles are placed.

Characteristic Zero

Theorem (Holm; D. Vagnozzi)
$\mathsf{LA}^{\omega}(\{0\}) \leq L^{\omega}_{\infty\omega}(C)$.

Linear algebra over fields of *characteristic zero* can be *simulated by counting*.

This essentially follows from the following observation.

> *For any vocabulary σ of binary relations, and two σ-structures $\mathbb{A}$ and $\mathbb{B}$,*
>
> $$\mathbb{A} \equiv^3_C \mathbb{B} \quad \Rightarrow \quad \mathbb{A} \cong_0 \mathbb{B}.$$

$\equiv^3_C$ can be characterized in terms of *coherent algebras*, and isomorphism of such algebras is witnessed by invertible matrices.

Charecteristic Two

Theorem (D., Grohe, Holm, Laubner 2009)
$L^3_{\omega\omega}(L_2) \not\leq L^\omega_{\infty\omega}(C)$

Cai, Fürer and Immerman give a construction of pairs of graphs $G_k, H_k (k \in \omega)$ such that

- $G_k \equiv^k_C H_k$; and
- $G_k \not\cong H_k$.

We can show that there is a single formula φ of $L^3_{\omega\omega}(L_2)$ (indeed of $L^3_{\omega\omega}(\mathsf{Rk}_2)$) such that

$$G_k \models \varphi; \quad H_k \not\models \varphi \quad \text{for all } k.$$

Distinct Characteristics

Theorem (D., Holm 2012)
For $p, q \in \text{Primes}$ with $p \neq q$,

$$L^{\omega}_{\omega\omega}(L_p) \not\leq L^{\omega}_{\infty\omega}(L_q).$$

For any prime p, we can construct a class of structures $\mathsf{CFI}(p)$ which codes solvable systems of equations over $\mathbb{F}_p$.
We use a simple version of the *invertible map game* to show that this is not expressible in $L^{\omega}_{\infty\omega}(L_q)$.

Note: We do not consider vectorizations here.

Rank Logics

Let $p \in \mathsf{Primes}$ and $P = \mathsf{Primes} \setminus \{p\}$.

Theorem (Grädel, Pakusa 2017)

$$L^{\omega}_{\omega\omega}(\mathsf{Rk}_p) \not\leq L^{\omega}_{\infty\omega}(\bigcup_{q \in P} \overline{\mathsf{Rk}_q})$$

This is proved by showing that the structures in $\mathsf{CFI}(p)$ can be constructed to be *homogeneous* in a way that guarantees that the quantifiers Rk_q, even vectorized, can be defined in $L^{\omega}_{\infty\omega}(C)$.

Vectorizations

Let $p \in \mathsf{Primes}$ and $P = \mathsf{Primes} \setminus \{p\}$.

Theorem (D. Grädel, Pakusa 2019)

$$\mathsf{LA}^{\omega}(\{p\}) \not\leq \mathsf{LA}^{\omega}(P).$$

In short, as long as Ω does not contain *all primes*, $\mathsf{LA}^{\omega}(\Omega)$ is *not complete*.

This is established by showing that on the structures in $\mathsf{CFI}(p)$, the equivalence relation $\equiv^{\mathsf{LA}^{k}(P)}$ can itself be defined in $L^{\omega}_{\infty\omega}(C)$.

This uses the homogeneity of structures in $\mathsf{CFI}(p)$, along with the fact that the automorphism groups of the structures are Abelian p-groups. This enables us to represent them as *semisimple* $\mathbb{F}_q$-algebras and apply *Maschke's theorem*.

Rank Logic Again

Theorem (Lichter 2021)
There is a polynomial-time decidable property that is not definable in $L^{\omega}_{\infty\omega}(\overline{\mathsf{Rk}})$.

The construction is a CFI-like collection of structures encoding systems of linear equations over the *ring* $\mathbb{Z}/\mathbb{Z}_{2^m}$ for growing values of m.

The proof uses the **Grädel-Pakusa** argument to show that the quantifiers Rk_p for $p \neq 2$ are useless on these structures.

It then uses the *invertible map game* to show that $\mathsf{LA}^{\omega}(\{2\})$ does not distinguish them.

All Characteristics

Theorem (D., Grädel, Lichter 2022)
Taking Ω to be the set of all characteristics,

> *There is a polynomial-time decidable property that is not definable in* $\mathsf{LA}^\omega(\Omega)$.

The proof combines the construction of **(Lichter 2021)** with the algebraic machinery of **(D., Grädel, Pakusa 2019)**.

In particular, this shows that the expressive power of LA^ω is not complete, and for each k, the equivalence relation $\equiv^{\mathsf{LA}^k}$ is not *discrete*.

Conclusions

Linear Algebraic quantifiers are a *natural* class of generalized quantifiers obtained by replacing *isomorphism invariance* by a stronger condition.

They extend the expressive power of counting quantifiers, but still have nice *algorithmic* properties, like polynomial-time decidable equivalence.

We have developed sophisticated algebraic machinery for analysing their expressive power, and show it is not complete.