Linear Algebra in Finite Model Theory

Anuj Dawar

University of Cambridge

Les Houches, 14 May 2012

Logic for PTIME

By Fagin's theorem, a class of finite structures is definable in *existential second-order logic* if, and only if, it is in NP.

It is an open question (first asked by **Chandra and Harel 1982**) whether there is similarly a logic for PTime.

IFP is the extension of first-order logic with *inflationary fixed-points*.

By **(Immerman; Vardi'82)**, it captures PTime on *ordered structures*, but is too weak without order.

Finite Variable Logic

We write L^k for the first order formulas using only the variables $x_1, \ldots, x_k$.

$$(\mathbb{A}, \mathbf{a}) \equiv_k^L (\mathbb{B}, \mathbf{b})$$

denotes that there is no formula φ of L^k such that $\mathbb{A} \models \varphi[\mathbf{a}]$ and $\mathbb{B} \not\models \varphi[\mathbf{b}]$

For every formula φ of IFP there is a k such that if $\mathbb{A} \equiv_k^L \mathbb{B}$, then

$$\mathbb{A} \models \varphi \quad \text{if, and only if,} \quad \mathbb{B} \models \varphi.$$

Pebble Game

The k-pebble game is played on two structures $\mathbb{A}$ and $\mathbb{B}$, by two players—*Spoiler* and *Duplicator*—using k pairs of pebbles $\{(a_1, b_1), \ldots, (a_k, b_k)\}$.

Spoiler moves by picking a pebble and placing it on an element (a_i on an element of $\mathbb{A}$ or b_i on an element of $\mathbb{B}$).

Duplicator responds by picking the matching pebble and placing it on an element of the other structure

Spoiler wins at any stage if the partial map from $\mathbb{A}$ to $\mathbb{B}$ defined by the pebble pairs is not a partial isomorphism

If *Duplicator* has a winning strategy for q moves, then $\mathbb{A}$ and $\mathbb{B}$ agree on all sentences of L^k of quantifier rank at most q. **(Barwise)**

$\mathbb{A} \equiv_k^L \mathbb{B}$ if, for every q, *Duplicator* wins the q round, k pebble game on $\mathbb{A}$ and $\mathbb{B}$.
Equivalently (on finite structures) *Duplicator* has a strategy to play forever.

Fixed-point Logic with Counting

Immerman proposed IFPC—the extension of IFP with a mechanism for *counting*.

Two sorts of variables:

- $x_1, x_2, \ldots$ range over $|A|$—the domain of the structure;
- $\nu_1, \nu_2, \ldots$ which range over *non-negative integers*.

If $\varphi(x)$ is a formula with free variable x, then $\#x\varphi$ is a *term* denoting the *number* of elements of $\mathbb{A}$ that satisfy φ.

We have arithmetic operations ($+, \times$) on *number terms*.

Quantification over number variables is *bounded*: $(\exists \nu < t)\, \varphi$

Counting Quantifiers

C^k is the logic obtained from *first-order logic* by allowing:

- *counting quantifiers*: $\exists^i x\, \varphi$; and
- only the variables $x_1, \ldots . x_k$.

Every formula of C^k is equivalent to a formula of first-order logic, albeit one with more variables.

For every sentence φ of IFPC, there is a k such that if $\mathbb{A} \equiv^C_k \mathbb{B}$, then

$$\mathbb{A} \models \varphi \quad \text{if, and only if,} \quad \mathbb{B} \models \varphi.$$

where $\mathbb{A} \equiv^C_k \mathbb{B}$ denotes that $\mathbb{A}$ and $\mathbb{B}$ cannot be distinguished by any formula of C^k.

Counting Game

Immerman and Lander (1990) defined a *pebble game* for C^k.

This is again played by *Spoiler* and *Duplicator* using k pairs of pebbles $\{(a_1, b_1), \ldots, (a_k, b_k)\}$.

At each move, *Spoiler* picks a subset of the universe (say $X \subseteq B$)

Duplicator responds with a subset of the other structure (say $Y \subseteq A$) of the same *size*.

Spoiler then places a b_i pebble on an element of Y and *Duplicator* must place a_i on an element of X.

Spoiler wins at any stage if the partial map from $\mathbb{A}$ to $\mathbb{B}$ defined by the pebble pairs is not a partial isomorphism

If *Duplicator* has a winning strategy for q moves, then $\mathbb{A}$ and $\mathbb{B}$ agree on all sentences of C^k of quantifier rank at most q.

Bijection Games

$\equiv_k^C$ is characterised by a k-pebble *bijection game*. **(Hella 96)**.

The game is played on structures $\mathbb{A}$ and $\mathbb{B}$ with pebbles $a_1, \ldots, a_k$ on $\mathbb{A}$ and $b_1, \ldots, b_k$ on $\mathbb{B}$.

- *Spoiler* chooses a pair of pebbles a_i and b_i;
- *Duplicator* chooses a bijection $h : A \to B$ such that for pebbles a_j and $b_j (j \neq i)$, $h(a_j) = b_j$;
- *Spoiler* chooses $a \in A$ and places a_i on a and b_i on $h(a)$.

Duplicator loses if the partial map $a_i \mapsto b_i$ is not a partial isomorphism.

Duplicator has a strategy to play forever if, and only if, $\mathbb{A} \equiv_k^C \mathbb{B}$.

Cai-Fürer-Immerman Graphs

There are polynomial-time decidable properties of graphs that are not definable in IFPC. **(Cai, Fürer, Immerman, 1992)**

More precisely, we can construct a sequence of pairs of graphs $G_k, H_k (k \in \omega)$ such that:

- $G_k \equiv_k^C H_k$ for all k.
- There is a polynomial time decidable class of graphs that includes all G_k and excludes all H_k.

Still, IFPC is a *natural* level of expressiveness within PTime.

Restricted Graph Classes

If we restrict the class of structures we consider, IFPC may be powerful enough to express all polynomial-time decidable properties.

1. IFPC captures PTime on *trees*. **(Immerman and Lander 1990)**.
2. IFPC captures PTime on any class of graphs of *bounded treewidth*. **(Grohe and Mariño 1999)**.
3. IFPC captures PTime on the class of *planar graphs*. **(Grohe 1998)**.
4. IFPC captures PTime on any *proper minor-closed class of graphs*. **(Grohe 2010)**.

In each case, the proof proceeds by showing that for any G in the class, a *canonical, ordered* representaton of G can be interpreted in G using IFPC.

Undefinability Results for IFPC

Some other undefinability results for IFPC:

- Isomorphism on *multipedes*—a class of structures defined by **(Gurevich-Shelah 96)** to exhibit a *first-order definable* class of *rigid* structures with no order definable in IFPC.
- 3-colourability of graphs is not invariant under $\equiv_k^C$ for any k. **(D. 1998)**

Both proofs rely on a construction very similar to that of Cai-Fürer-Immerman.

Question: What are natural polynomial-time computable properties that are not definable in IFPC?

Solvability of Linear Equations

It has been shown that the problem of solving linear equations over the two element field $\mathbf{GF}(2)$ is not definable in IFPC. **(Atserias, Bulatov, D. 09)**

The question arose in the context of classification of *Constraint Satisfaction Problems*.

The problem is clearly solvable in polynomial time by means of Gaussian elimination.

> We see how to represent systems of linear equations as *unordered* relational structures.

Systems of Linear Equations

Consider structures over the domain $\{x_1, \ldots, x_n, e_1, \ldots, e_m\}$, (where $e_1, \ldots, e_m$ are the equations) with relations:

- unary E_0 for those equations e whose r.h.s. is 0.
- unary E_1 for those equations e whose r.h.s. is 1.
- binary M with $M(x, e)$ if x occurs on the l.h.s. of e.

Solv$(\mathbb{Z}_2)$ is the class of structures representing solvable systems.

Constraint Satisfaction Problems

For a fixed finite structure $\mathbb{B}$, CSP$(\mathbb{B})$ is the class of structures $\mathbb{A}$ for which there is a *homomorphism* $\mathbb{A} \longrightarrow \mathbb{B}$.

It follows from results of **(Atserias, Bulatov, D. 09)** and **(Barto, Kozik 09)** that, for every $\mathbb{B}$, either

- $\overline{\text{CSP}(\mathbb{B})}$ is definable in Datalog (and therefore CSP$(\mathbb{B})$ is definable in IFP); or
- CSP$(\mathbb{B})$ is not invariant under $\equiv_k^C$ for any k.

This gives a rich source of examples of problems (including problems in PTime) not definable in IFPC.

Computational Problems from Linear Algebra

Linear Algebra is a testing ground for exploring the boundary of the expressive power of IFPC.

It may also be a possible source of new operators to extend the logic.

For a set I, and binary relation $A \subseteq I \times I$, take the matrix M over the two element field $\mathbf{GF}(2)$:

$$M_{ij} = 1 \quad \Leftrightarrow \quad (i,j) \in A.$$

Most interesting properties of M are invariant under permutations of I.

Matrix Operations

It is easy to see we can write a formula prod(x, y, A, B) that defines the *product* of two matrices.

With a little more effort, we can show that matrix *exponentiation* is definable.

Using this, **(Blass-Gurevich 04)** show that *non-singularity* of a matrix over $\mathbb{Z}_2$ can be expressed in IFPC, and we can define the *inverse*.

Computational Complexity

$\oplus$L is the complexity class containing languages L for which there is a *nondeterministic, logspace* machine M such that

> $x \in L$ if, and only if, the number of accepting paths of M on input x is *odd*.

$\oplus$L contains L and is (as far as we know) incomparable with NL.

$\oplus$GAP is a natural $\oplus$L-complete problem under logspace reductions.

> $\oplus$GAP: given an *acyclic, directed* graph G with vertices s, t, is the number of distinct paths from s to t *odd*?

Computational Complexity II

The following are all $\oplus$L-complete under logspace reductions:

- Non-singularity of matrices over $\mathbb{Z}_2$;
- Inverting a matrix over $\mathbb{Z}_2$;
- Determining the rank of a matrix over $\mathbb{Z}_2$.

(Buntrock, Damm, Hertrampf, Meinel 92)

Note: $\oplus$GAP is definable in IFPC as it amounts to checking $\left(A_G^n\right)_{st}$, where A_G is the adjacency matrix of G.

IFPC over Finite Fields

Over $\mathbf{GF}(q)$, *matrix multiplication*; *non-singularity* of matrices; the *inverse* of a matrix; are all definable in IFPC.

determinants and more generally, the coefficients of the *characteristic polynomial* can be expressed IFPC.

(D., Grohe, Holm, Laubner, 2009)

solvability of systems of equations is *undefinable*.

the *rank* of a matrix is *undefinable*.

Rank Operators

(D., Grohe, Holm, Laubner, 2009) introduce an operator for *matrix rank* into the logic.

We have, as with IFPC, terms of *element sort* and *numeric sort*.

> We interpret $\eta(x, y)$—a *term* of numeric sort—in $\mathbb{A}$ as defining a *matrix* with rows and columns indexed by elements of A with entries $\eta[a, b]$.
>
> $\mathsf{rk}_{x,y}\eta$ is a *term* denoting the number that is the rank of the matrix defined by $\eta(x, y)$.

To be precise, we have, for each finite field $\mathbf{GF}(q)$ (q prime), an operator rk^q which defines the rank of the matrix with entries $\eta[a, b](\mathrm{mod}\, q)$.

IFPrk vs. IFPC

Adding rank operators to IFP, we obtain a proper extension of IFPC.

$$\#x\varphi \quad = \quad \mathsf{rk}_{x,y}[x = y \wedge \varphi(x)]$$

In IFPrk we can express the solvability of linear systems of equations, as well as the Cai-Fürer-Immerman graphs and the order on multipedes.

FO(rk)

More generally, for each prime p and each arity m, we have an operator rk^p_m which binds $2m$ variables and defines the rank of the $n^m \times n^m$ matrix defined by a formula $\varphi(\mathbf{x}, \mathbf{y})$.

FO(rk), the extension of first-order logic with the rank operators is already quite powerful.

- it can express *deterministic transitive closure*;
- it can express *symmetric transitive closure*;
- it can express solvability of linear equations.

Symmetric Transitive Closure

Let $G = (V, E)$ be an *undirected graph* and let s and t be vertices in V.

Define the system of equations $\mathbf{E}_{G,s,t}$ over $\mathbf{GF}(2)$ with variables x_v for each $v \in V$, and equations

- for each edge $e = u, v \in E$: $x_u + x_v = 0$;
- $x_s = 1 \quad x_t = 0$.

$\mathbf{E}_{G,s,t}$ is solvable if, and only if, there is no path from s to t in G.

Capturing $\mathrm{Mod}_p\mathrm{L}$

For each number p, the complexity class $\mathrm{Mod}_p\mathrm{L}$ is defined like $\oplus$L but with acceptance condition:

> $x \in L$ if, and only if, the number of accepting paths of M on input x is not $0 (\mathrm{mod} p)$.

For *prime* p, let FO$\left(\mathsf{rk}^p\right)$, be the logic extending first-order logic with the rk^p operator of all arities.

> On *ordered structures*, FO$\left(\mathsf{rk}^p\right)$ captures $\mathrm{Mod}_p\mathrm{L}$.

Arity Hierarchy

In the case of IFPC, adding counting operators of arities higher than 1 does not increase expressive power. These can all already be defined in IFPC with *unary* counting.

This is not the case with IFPrk.

We prove

> For each m, there is a property definable in FO$\left(\text{rk}^2_{m+1}\right)$ that is not definable in IFP$\left(\text{rk}_m\right)$.

The proof is based on a construction due to Hella, and requires vocabularies of increasing arity.

It is conceivable that *over graphs*, the arity hierarchy collapses.

Games for Logics with Rank

Define the equivalence relation $\mathbb{A} \equiv^{R}_{k,\Omega,m} \mathbb{B}$ to mean that $\mathbb{A}$ and $\mathbb{B}$ are not distinguished by any formula of FO(rk) with at most k variables using operators rk^{p}_{m} for p in the finite set of primes Ω.

This equivalence relation has a characterisation in terms of *games*.

(**Holm 2009**)

This game can been used to show that for *distinct* primes p, q, solvability of linear equations $\mathrm{mod}\ q$ cannot be defined in IFP with operators rk^{p}_{1}.

Games for Logics with Rank

The game is played with k pairs of pebbles. At each move

- *Spoiler* picks $2m$ pebbles from $\mathbb{A}$ and the corresponding pebbles from $\mathbb{B}$ and $p \in \Omega$.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of $A^m \times A^m$
  - a partition $\mathbf{Q}$ of $B^m \times B^m$
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that for all labellings $\gamma : \mathbf{P} \to \mathbf{GF}(p)$

$$\text{rank}(M^{\mathbf{P}}_{\gamma}) = \text{rank}(M^{\mathbf{Q}}_{\gamma \circ f^{-1}})$$

- *Spoiler* chooses a part $P \in \mathbf{P}$ and places the chosen pebbles on a tuple in P and the matching pebbles on a tuple in $f(P)$.

Partition Games

We can formulate a general framework of *partition games*.

- *Spoiler* picks m pebbles from $\mathbb{A}$ and the corresponding pebbles from $\mathbb{B}$.
- *Duplicator* reponds with
  - a partition $\mathbf{P}$ of A^m
  - a partition $\mathbf{Q}$ of B^m
  - a bijection $f : \mathbf{P} \to \mathbf{Q}$ such that a condition *(*)* holds.
- *Spoiler* chooses a part $P \in \mathbf{P}$ and places the chosen pebbles on a tuple in P and the matching pebbles on a tuple in $f(P)$.

Varying the condition *(*)* gives us the games for $\equiv_k^L$, $\equiv_k^C$ and $\equiv_{k,\Omega,m}^R$.

Approximations of Isomorphism

For each k, the relation $\equiv_k^C$ is decidable in *polynomial time*.

It provides an approximation of *graph isomorphism*.

This is also known as the *Weisfeiler-Lehman* method.

The *CFI* construction shows that there is no k for which $\equiv_k^C$ coincides with graph isomorphism.

Approximations of Isomorphism

Grohe's capturing result on proper minor-closed classes of graphs shows the following.

> For any *proper minor-closed class* C of graphs, there is a k such that $\equiv_k^C$ coincides with isomorphism on C.

What can we say about the equivalence relations $\equiv_{k,\Omega,m}^R$?

We can use the game characterisation to iteratively compute this relation, *but* the condition:

> for all labellings $\gamma : \mathbf{P} \to \mathbf{GF}(p)$, $\mathsf{rank}(M_\gamma^{\mathbf{P}}) = \mathsf{rank}(M_{\gamma \circ f^{-1}}^{\mathbf{Q}})$

seems inherently exponential.

Invertible Map Game

We define a variant parition game with a *stronger* condition:

> There is an invertible matrix S such that for all labellings $\gamma : \mathbf{P} \to \mathbf{GF}(p)$, $M_{\gamma}^{\mathbf{P}} = S(M_{\gamma \circ f^{-1}}^{\mathbf{Q}})S^{-1}$

Since this (unlike the rank function) is *linear* on the space of matrices, it is sufficient to check it on a basis, which is given by the individual parts of $\mathbf{P}$.

We use a result of **(Chistov, Karpinsky, Ivanyov 1997)** that *simultaneous similarity* of a collection of matrices is decidable in polynomial time to get a family of polynomial-time equivalence relations $\equiv^{\mathsf{IM}}_{k,\Omega,m}$.

Approximations of Isomorphism

This gives us a family of polynomial-time isomorphism tests.

- $\equiv^{\mathsf{IM}}_{k,\Omega,m}$ refines $\equiv^{R}_{k,\Omega,m}$
- $\equiv^{\mathsf{IM}}_{k,\Omega,m}$ gets finer as we increase any of k, m or Ω.
- The CFI graphs are distinguished by $\equiv^{\mathsf{IM}}_{4,\{2\},1}$

(D., Holm 2012)

Equations over Groups and Rings

We can define systems of equations, not just over *fields* but over *finite rings* or *groups*.

For rings and *Abelian* groups, the problems are solvable in polynomial time.

There is no corresponding notion of *rank*, and it is not clear that these problems can be expressed in IFPrk.

We can show that the solvability problems for rings, fields and Abelian groups can be reduced (in IFPC) to that for *finite, commutative, local rings*.

(D., Grädel, Holm, Kopczynski, Pakusa 2012)

Research Directions

- What is the relationship between the families of equivalence relation $\equiv^{R}_{k,\Omega,m}$ and $\equiv^{\mathsf{IM}}_{k,\Omega,m}$? Are the latter definable in IFPrk?
- Is solvability of systems of linear equations over finite rings in IFPrk? Over finite Abelian groups?
- Are there any problems in PTime that are not definable in IFPrk?
- Show for some problem definable in IFPrk that it is not definable in FO(rk).
- Show for any concrete problem (say an NP-complete one) that it is not definable in IFPrk.