On the Descriptive Complexity of Linear Algebra

Anuj Dawar

University of Cambridge

Aachen, 17 December 2007

Is There a Logic for P?

The question of whether or not there is a logic expressing exactly the PTime properties of *(unordered) relational structures* is the central problem in *Descriptive Complexity*.

If we assume structures are *ordered*, then LFP, the extension of first-order logic with least fixed points suffices. **(Immerman; Vardi 1982)**

In the absence of order LFP fails to express simple cardinality properties such as *evenness*.

Fixed-point Logic with Counting

Immerman had proposed FP + C—the extension of LFP 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 *numbers* in the range $0, \ldots, |A|$

If $\varphi(x)$ is a formula with free variable x, then $\nu = \#x\varphi$ denotes that ν is the number of elements of A that satisfy the formula φ.

We also have the order $\nu_1 < \nu_2$, which allows us (using recursion) to define arithmetic operations.

Infinitary Logic with Counting

Sentences of FP $+$ C can be translated into $C^{\omega}_{\infty\omega}$—an *infinitary logic with counting*.

$C^{\omega}_{\infty\omega}$ is obtained from first-order logic by allowing:

- *infinitary* conjunctions and disjunctions: $\bigvee\{\varphi \mid \varphi \in S\} \quad \bigwedge\{\varphi \mid \varphi \in S\}$
- *counting quantifiers*: $\exists^i x\, \varphi$
- only finitely many distinct variables in any formula.

$C^{k}_{\infty\omega}$ is the fragment of $C^{\omega}_{\infty\omega}$ where each formula has at most k variables.

FP $+$ C is the PTime-uniform fragment of $C^{\omega}_{\infty\omega}$ **(Otto 96)**.

Cai-Fürer-Immerman Graphs

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

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

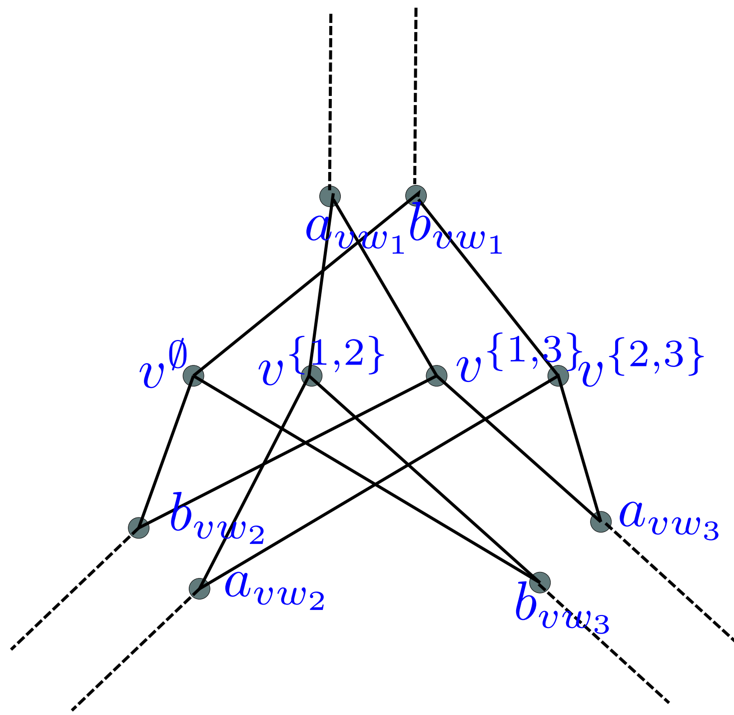
- $G_k \equiv^{C^k_{\infty\omega}} H_k$ for all k.
- There is a polynomial time decidable class of graphs that includes all G_k and excludes all H_k.

Still, FP + C is a *natural* level of expressiveness within PTime.

Constructing G_k and H_k

Given any graph G, we can define a graph X_G by replacing every edge with a pair of edges, and every vertex with a gadget.

The picture shows the gadget for a vertex v that is adjacent in G to vertices w_1, w_2 and w_3.
The vertex v^S is adjacent to $a_{vw_i} (i \in S)$ and $b_{vw_i} (i \notin S)$ and there is one vertex for all *even size* S.
The graph $\tilde{X}_G$ is like X_G except that at *one vertex* v, we include V^S for *odd size* S.



Properties

1. For any graph G, $X_G \not\cong \tilde{X}_G$.

2. If G has no balanced separator of fewer than k vertices, then $X_G \equiv^{C^k_{\infty\omega}} \tilde{X}_G$.

(Cai, Fürer, Immerman)

Indeed, it suffices that G is *connected* and has *treewidth* at least k.

(D., Richerby 07)

The latter condition is also necessary.

(1) allows us to construct a polynomial time property separating X_G and $\tilde{X}_G$.

(2) is proved by a game argument.

Bijection Games

$C^k_{\infty\omega}$ 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 $h : A \longrightarrow B$ 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, $\mathbb{A} \equiv^{C^k_{\infty\omega}} \mathbb{B}$.

Cops and Robbers

If G has treewidth k or more, than the *robber* has a winning strategy in the k-*cops and robbers* game played on G. **(Seymour-Thomas 93)**

We use this to construct a winning strategy for Duplicator in the k-pebble bijection game on X_G and $\tilde{X}_G$.

- A bijection $h : X_G \to \tilde{X}_G$ is *good bar* v if it is an isomorphism everywhere except at the vertices v^S.
- If h is good bar v and there is a path from v to u, then there is a bijection h' that is good bar u such that h and h' differ only at vertices corresponding to the path from v to u.
- Duplicator plays bijections that are good bar v, where v is the robber position in G when the cop position is given by the currently pebbled elements.

Undefinability Results for $C^{\omega}_{\infty\omega}$

Other undefinability results for $C^{\omega}_{\infty\omega}$ have been obtained:

- 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 FP + C.
- 3-colourability of graphs. **(D. 1998)**

Both proofs rely on gadgets very similar to those of Cai-Fürer-Immerman.

Question: Is there a natural polynomial-time computable property that is not definable in FP + C?

Solvability of Linear Equations

It has recently been shown that the problem of solving linear equations over the two element field $\mathbb{Z}_2$ is not definable in $C^{\omega}_{\infty\omega}$. **(Atserias, Bulatov, D. 07)**

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 – 2

Consider a system of linear equations over $\mathbb{Z}_2$ where each equation has three variables:

$$x_1 + x_2 + x_3 = a \quad (a = 0 \text{ or } 1).$$

We consider this system as a structure over the domain $\{x_1, \ldots, x_n\}$ of variables with two ternary relations:

$$R_0 = \{(x_i, x_j, x_k) \mid x_i + x_j + x_k = 0 \text{ is an equation}\}$$
$$R_1 = \{(x_i, x_j, x_k) \mid x_i + x_j + x_k = 1 \text{ is an equation}\}$$

Let $\text{Solv}_3(\mathbb{Z}_2)$ be the class of those structures representing solvable systems.

Systems of Linear Equations – 3

Alternatively,

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.

Solv$_3(\mathbb{Z}_2) \leq_{\text{FO}}$ Solv$(\mathbb{Z}_2)$ by an easy first-order reduction.

Undefinability in $C^{\omega}_{\infty\omega}$

Take G a 3-regular, connected graph with treewidth $> k$.

Define equations $\mathbf{E}_G$ with two variables x^e_0, x^e_1 for each edge e.

For each vertex v with edges e_1, e_2, e_3 incident on it, we have eight equations:

$$E_v : \qquad x^{e_1}_i + x^{e_2}_j + x^{e_3}_k \equiv i + j + k \pmod 2$$

The system of equations $\tilde{\mathbf{E}}_G$ is obtained from $\mathbf{E}_G$ by replacing, for exactly one vertex v, E_v by:

$$E'_v : \qquad x^{e_1}_i + x^{e_2}_j + x^{e_3}_k \equiv i + j + k + 1 \pmod 2$$

Facts about the Construction – I

Lemma $\mathbf{E}_G \equiv^{C^k_{\infty\omega}} \tilde{\mathbf{E}}_G$

This can be established by showing that Duplicator has a winning strategy in the k-pebble *bijection game* played on $\mathbf{E}_G$ and $\tilde{\mathbf{E}}_G$.

Alternatively, we can show a *first-order reduction* from the Cai-Fürer-Immerman graphs.

There is a first-order transduction Φ such that:

- $\Phi : X_G \mapsto \mathbf{E}_G$
- $\Phi : \tilde{X}_G \mapsto \tilde{\mathbf{E}}_G$

Facts about the Construction – II

Lemma $\mathbf{E}_G$ is satisfiable.

by setting the variables x_i^e to i.

Lemma $\tilde{\mathbf{E}}_G$ is unsatisfiable.

Consider the subsystem consisting of equations involving only the variables x_0^e.

The sum of all *left-hand sides* is

$$2\sum_e x_0^e \equiv 0 \pmod 2$$

However, the sum of *right-hand sides* is 1.

Computational Problems from Linear Algebra

Linear Algebra is a testing ground for exploring the boundary of the expressive power of FP $+$ C.

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 $\mathbb{Z}_2$:

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

Many properties of M are invariant under permutations of I, *e.g.* non-singularity.

Matrix Multiplication

We can write a formula $\mathrm{prod}(x, y, A, B)$ that defines the *product* of two matrices:

$$\exists \nu_1 \exists \nu_2 (\nu_1 = \# z(A(x, z) \wedge B(z, y))) \wedge (\nu_1 = 2 \cdot \nu_2 + 1)$$

A simple application of **lfp** then allows us to define $\mathrm{upower}(x, y, \nu, A)$ which gives the matrix A^ν.

We can, instead, represent numbers in *binary*, i.e. a unary relation Γ interpreted over the number domain codes the number $\sum_{\gamma \in \Gamma} 2^\gamma$.

Repeated squaring then allows us to define $\mathrm{power}(x, y, \Gamma, A)$ giving A^N where Γ codes a value N which may be exponential.

Non-Singularity

(Blass-Gurevich 04) show that *non-singularity* of a matrix over $\mathbb{Z}_2$ can be expressed in FP $+$ C.

GL$(n, \mathbb{Z}_2)$—the *general linear group* of degree n over $\mathbb{Z}_2$—is the group of non-singular $n \times n$ matrices over $\mathbb{Z}_2$.

The order of GL$(n, \mathbb{Z}_2)$ divides

$$N = \prod_{i=0}^{n-1} (2^n - 2^i).$$

Thus, A is *non-singular* if, and only if, $A^N = \mathbf{I}$

Inverting a Matrix

Over $\mathbb{Z}_2$, *testing non-singularity* is the same as *finding the determinant* (as there is only one possible *non-zero* value).

This allows us to write a formula of FP $+$ C to *invert* a matrix A by the rule:

$$(A^{-1})_{ij} = 1 \quad \Leftrightarrow \quad \overline{A_{ji}} \text{ is non-singular,}$$

where $\overline{A_{ji}}$ denotes the *minor matrix* obtained from A by deleting row j and column i.

One can do a fair amount of linear algebra in FP $+$ C, but not compute the *rank of a matrix*. This would allow us to define the solvability of systems of equations.

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 FP + C as it amounts to checking $(A_G^n)_{st}$, where A_G is the adjacency matrix of G.

Representing Finite Fields

We can represent matrices M over a finite field $\mathbb{F}_q$ by taking, for each $a \in \mathbb{F}_q$ a binary relation $A_a \subseteq I \times I$ with

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

Alternatively, we could have the elements of $\mathbb{F}_q$ (along with the field operations) as a *separate sort* and include a ternary relation R

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

These two representations are inter-definable.

Computing over Finite Fields

Over $\mathbb{F}_q$,

- *non-singularity* of matrices is definable;
- *inverse* of a matrix is definable; and
- *non-solvability* of systems of equations is *undefinable*

in $\mathsf{FP} + \mathsf{C}$ by adaptations of the proofs that work over $\mathbb{Z}_2$.

Rossman shows that *determinants* can be computed in *choiceless polynomial time with counting*, and this is improved to $\mathsf{FP} + \mathsf{C}$ by **Holm**.

For q *prime*, these problems are all complete for $\mathrm{mod}_q\mathrm{L}$ under logspace reductions.

Open Problems

If we add an *operator for matrix rank* to the logic $\mathrm{FP} + \mathrm{C}$, what can it express? Could it be all of PTime? Can we find a problem in PTime that is not definable?

What might be a more general *linear-algebraic* operator to add to the logic?

Is the *solvability of systems of linear equations* expressible in choiceless polynomial time with counting? Or in fixed-point logics with symmetric choice?

Is *general graph matching* definable in $\mathrm{FP} + \mathrm{C}$?

Bipartite graph matching is, by **(Blass, Gurevich, Shelah 02)**.