Logics for Polynomial Time

Tutorial Part 3: Logics with Rank Operators

Anuj Dawar

University of Cambridge

JAF, Fontainebleau, 19 June 2009

Recapitulation

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 whether there is similarly a logic for PTime.

This is equivalent to the question of whether there is a problem in PTime that is complete under *first-order reductions*.

Recapitulation II

IFP extends first-order logic with *inflationary fixed-points*.

By the theorem of Immerman and Vardi, it captures PTime on *ordered structures*, but is too weak without order.

IFP $+$ C, the extension of IFP with counting is also too weak by the (somewhat contrived) example of Cai et al.

Undefinability Results for IFP + C

Other undefinability results for IFP + C 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 IFP + C.
- 3-colourability of graphs. **(D. 1998)**

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

Question: Is there a natural polynomial-time computable property that is not definable in IFP + 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 IFP $+$ C. **(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.

Undefinability in IFP $+$ C

Take $\mathcal{G}$ a 3-regular, connected graph with treewidth $> k$.

Define equations $\mathbf{E}_{\mathcal{G}}$ with two variables x_0^e, x_1^e for each edge e.

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

$$E_v : \qquad x_i^{e_1} + x_j^{e_2} + x_k^{e_3} \equiv i + j + k \pmod 2$$

$\tilde{\mathbf{E}}_{\mathcal{G}}$ is obtained from $\mathbf{E}_{\mathcal{G}}$ by replacing, for exactly one vertex v, E_v by:

$$E'_v : \qquad x_i^{e_1} + x_j^{e_2} + x_k^{e_3} \equiv i + j + k + 1 \pmod 2$$

We can show: $\mathbf{E}_{\mathcal{G}}$ is satisfiable; $\tilde{\mathbf{E}}_{\mathcal{G}}$ is unsatisfiable; $\mathbf{E}_{\mathcal{G}} \equiv^{C^k} \tilde{\mathbf{E}}_{\mathcal{G}}$

Computational Problems from Linear Algebra

Linear Algebra is a testing ground for exploring the boundary of the expressive power of IFP $+$ 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 $\mathbb{Z}_2$:

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

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

Matrix Multiplication

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

$$(\exists \nu_2 < t)(t = 2 \cdot \nu_2 + 1) \quad \text{for} \quad t = \#z(A(x, z) \wedge B(z, y))$$

A simple application of **ifp** then allows us to define upower(x, y, ν, A) which gives the matrix A^ν:

$$[\mathbf{ifp}_{R,uv} \ (\nu = 0 \wedge u = v \vee (\exists \mu < \nu)\,(\nu = \mu + 1 \wedge \text{prod}(u, v, B/R(\mu), A))](x, y),$$

where prod$(u, v, B/R(\mu), A)$ is obtained from prod(u, v, A, B) by replacing the occurrence of $B(z, v)$ by $R(z, v, \mu)$.

Matrix Exponentiation

We can, instead, represent numbers up to $2^{|A|}$ in *binary*.

That is, a unary relation Γ interpreted over the number domain (using numbers up to $|A|$) codes the number $\sum_{\gamma \in \Gamma} 2^{\gamma}$.

Repeated squaring then allows us to define power(x, y, Γ, 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 IFP $+$ 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, $A^N = \mathbf{I}$

Moreover, the inverse A^{-1} is given by A^{N-1}.

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

IFP $+$ C over Finite Fields

Over $\mathbb{F}_q$, *matrix multiplication*; *non-singularity* of matrices; the *inverse* of a matrix; are all definable in IFP $+$ C.

determinants and more generally, the coefficients of the *characteristic polynomial* can be expressed IFP $+$ C.

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

solvability of systems of equations is *undefinable*.

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

Rank Operators

We introduce an operator for *matrix rank* into the logic.

We have, as with IFP $+$ C, 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 $\mathbb{F}_q$, an operator rk^q which defines the rank of the matrix with entries $\eta[a, b](\mathrm{mod} q)$.

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

IFP $+$ rk vs. IFP $+$ C

Adding rank operators to IFP, we obtain a proper extension of IFP $+$ C.

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

In IFP $+$ rk 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 k, we have an operator rk_n^p which binds $2k$ variables and defines the rank of the $n^k \times n^k$ 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 $\mathbb{F}_2$ with variables x_v for each $v \in V$, and equations

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

$\mathbf{E}_{G,s,t}$ 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 $+$ rk^p, be the logic extending first-order logic with the rk^p operator of all arities.

> On *ordered structures*, FO $+$ rk^p captures $\mathrm{Mod}_p\mathrm{L}$.

Arity Hierarchy

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

This is not the case with IFP $+$ rk.

We prove

> For each k, there is a property definable in FO $+$ rk$^2_{k+1}$ that is not definable in IFP $+$ rk$_k$.

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

What might a pebble game for IFP + rk look like?

We could, as in the *Immerman-Lander* game, let *Spoiler* pick a relation and have *Duplicator* respond with one of equal rank.

> This works if we restrict the players to playing *definable* relations. A rather unsatisfactory solution.

Is there a game to be obtained by modifying the Hella game, replacing bijections with *invertible linear maps*?

Research Directions

- Find a game (like the bijection game) for proving inexpressibility results in FO $+$ rk and IFP $+$ rk.
- Are there any problems in PTime that are not definable in IFP $+$ rk?
- Show for some problem definable in IFP $+$ rk that it is not definable in FO $+$ rk.
- Show for any concrete problem (say an NP-complete one) that it is not definable in IFP $+$ rk.
- Are rk^p and rk^q interdefinable for $p \neq q$?

Research Directions II

- Could IFP $+$ rk be sufficient to capture PTime on bounded-degree graphs?
- How does the expressive power of IFP $+$ rk compare with $\tilde{\mathsf{C}}\mathsf{PT}(\mathsf{Card})$ or SSC-IFP?
- Is *general graph matching* definable in IFP $+$ C?

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