Topics in Logic and Complexity
Handout 3

Anuj Dawar

MPhil Advanced Computer Science, Lent 2012

Fixed-point Logic with Counting

Immerman proposed $\mathrm{IFP} + \mathrm{C}$—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 $\phi(x)$ is a formula with free variable x, then $\#x\phi$ 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*: $(\exists x < t)\, \phi$

Evenness

There are an even number of elements satisfying $\phi(x)$.

$$\exists \nu < \#x\phi(\nu + \nu = \#x\phi)$$

Counting Quantifiers

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

- allowing *counting quantifiers*: $\exists^i x\, \phi$; 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 $\mathrm{IFP} + \mathrm{C}$, there is a k such that if $\mathbb{A} \equiv^{C^k} \mathbb{B}$, then

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

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 $\{(a_1, b_1), \ldots, (a_k, b_k)\}$.

Spoiler picks a subset of the universe (say $X \subseteq B$)

Duplicator responds with $Y \subseteq A$ such that $|X| = |Y|$.

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

$\equiv^{C^k}$ is also 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, $\mathbb{A} \equiv^{C^k} \mathbb{B}$.

Equivalence of Games

To show that the games do, indeed, capture $\equiv^{C^k}$, we can show the following series of implications for any structures $\mathbb{A}, \mathbb{B}$ and k-tuples of elements $\mathbf{a}$, $\mathbf{b}$.

1\. $\Rightarrow$ 2. $\Rightarrow$ 3.

1. $(\mathbb{A}, \mathbf{a}) \not\equiv^{C^k} (\mathbb{B}, \mathbf{b})$
2. *Spoiler* wins the k-pebble counting game starting from $(\mathbb{A}, \mathbf{a})$ and $(\mathbb{B}, \mathbf{b})$.
3. *Spoiler* wins the k-pebble bijection game starting from $(\mathbb{A}, \mathbf{a})$ and $(\mathbb{B}, \mathbf{b})$.

Equivalence of Games

4\. $\Rightarrow$ 5. $\Rightarrow$ 6.

4. $(\mathbb{A}, \mathbf{a}) \equiv^{C^k} (\mathbb{B}, \mathbf{b})$
5. *Duplicator* wins the k-pebble bijection game starting from $(\mathbb{A}, \mathbf{a})$ and $(\mathbb{B}, \mathbf{b})$.
6. *Duplicator* wins the k-pebble counting game starting from $(\mathbb{A}, \mathbf{a})$ and $(\mathbb{B}, \mathbf{b})$.

Solvability of Linear Equations

We can now use the games to show that some natural problems in P are not definabile in IFP + C.

We consider the problem of solving linear equations over the two element field $\mathbb{Z}_2$.

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.

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

Undefinability in IFP + C

Take $\mathcal{G}$ to be a *toroidal grid* of size $k \times k$.

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, e_4 incident on it, we have 16 equations:

$$E_v : \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} + x_d^{e_4} \equiv a + b + c + d \pmod 2$$

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

$$E'_v : \qquad x_a^{e_1} + x_b^{e_2} + x_c^{e_3} + x_d^{e_4} \equiv a + b + c + +d + 1 \pmod 2$$

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

Satisfiability

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.

Cops and Robbers

The *cops and robbers* game is a way of measuring the connectivity of a graph.

It is a game played on an undirected graph $G = (V, E)$ between a player controlling k *cops* and another player in charge of a *robber*.

At any point, the cops are sitting on a set $X \subseteq V$ of the nodes and the robber on a node $r \in V$.

A move consists in the cop player removing some cops from $X' \subseteq X$ nodes and announcing a new position Y for them. The robber responds by moving along a path from r to some node s such that the path does not go through $X \setminus X'$.

The new position is $(X \setminus X') \cup Y$ and s. If a cop and the robber are on the same node, the robber is caught and the game ends.

Cops and Robbers on the Grid

If G is the $k \times k$ toroidal grid, than the *robber* has a winning strategy in the k-*cops and robbers* game played on G.

To show this, we note that for any set X of at most k vertices, the graph $G \setminus X$ contains a connected component with at least half the vertices of G.

If all vertices in X are in distinct rows then $G \setminus X$ is connected.

Otherwise, $G \setminus X$ contains an entire row column and in its connected component there are at least $k - 1$ vertices from at least $k/2$ columns.

Robber's strategy is to stay in the large component.

Cops, Robbers and Bijections

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

- A bijection $h : \mathbf{E}_G \to \tilde{\mathbf{E}}_G$ is *good bar* v if it is an isomorphism everywhere except at the variables $x^e a$ for edges e incident on v.
- 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.

Reading List for the Second and Third Handout

1. Ebbinghaus and Flum, Chapters 11 and 12, Section 3.3.
2. Libkin, Sections 8.1, 10.2, 11.1–11.2
3. Immerman, Sections 12.1–12.4, 13.2–13.3