Pebble Games for Logics with Counting and Rank

Anuj Dawar  
University of Cambridge  

Visiting ENS, Cachan  

GaLoP, 28 March 2009
Expressive Power of Logics

We are interested in the *expressive power* of logics on finite structures.

We consider finite structures in a *relational vocabulary*.

A finite set \( A \), with relations \( R_1, \ldots, R_m \) and constants \( c_1, \ldots, c_n \).

A *property* of finite structures is any *isomorphism-closed* class of structures.

For a logic (i.e., a *description* or *query* language) \( \mathcal{L} \), we ask for which properties \( P \), there is a sentence \( \varphi \) of the language such that

\[
A \in P \quad \text{if, and only if,} \quad A \models \varphi.
\]

In our examples, we will confine ourselves to vocabularies with just one binary relation \( E \).
First-Order Logic

terms – $c, x$

atomic formulae – $R(t_1, \ldots, t_a), t_1 = t_2$

boolean operations – $\varphi \land \psi, \varphi \lor \psi, \neg \varphi$

first-order quantifiers – $\exists x \varphi, \forall x \varphi$

Graphs which contain a triangle:
$\exists x \exists y \exists z (x \neq y \land y \neq z \land x \neq y \land E(x, y) \land E(y, z) \land E(x, z))$

Unions of cycles: $\forall x (\exists! y E(x, y) \land \exists! z E(z, y))$

Can we define the class of connected graphs? No, but how do we prove it?
Quantifier Rank

The quantifier rank of a formula $\varphi$, written $qr(\varphi)$ is defined inductively as follows:

1. if $\varphi$ is atomic then $qr(\varphi) = 0$,

2. if $\varphi = \neg\psi$ then $qr(\varphi) = qr(\psi)$,

3. if $\varphi = \psi_1 \lor \psi_2$ or $\varphi = \psi_1 \land \psi_2$ then
   \[ qr(\varphi) = \max(qr(\psi_1), qr(\psi_2)). \]

4. if $\varphi = \exists x\psi$ or $\varphi = \forall x\psi$ then $qr(\varphi) = qr(\psi) + 1$

In a finite relational vocabulary, it is easily proved that in a finite vocabulary, for each $q$, there are (up to logical equivalence) only finitely many sentences $\varphi$ with $qr(\varphi) \leq q$. 
Finitary Elementary Equivalence

For two structures $A$ and $B$, we say $A \equiv_p B$ if for any sentence $\varphi$ with $qr(\varphi) \leq p$,

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

Key fact:

a class of structures $S$ is definable by a first order sentence if, and only if, $S$ is closed under the relation $\equiv_p$ for some $p$.

In a finite relational vocabulary, for any structure $A$ there is a sentence $\theta_A^p$ such that

$$B \models \theta_A^p \text{ if, and only if, } A \equiv_p B$$
Ehrenfeucht-Fraïssé Game

The $p$-round Ehrenfeucht game on structures $\mathcal{A}$ and $\mathcal{B}$ proceeds as follows:

- There are two players called Spoiler and Duplicator.
- At the $i$th round, Spoiler chooses one of the structures (say $\mathcal{B}$) and one of the elements of that structure (say $b_i$).
- Duplicator must respond with an element of the other structure (say $a_i$).
- If, after $p$ rounds, the map $a_i \mapsto b_i$ is a partial isomorphism, then Duplicator has won the game, otherwise Spoiler has won.

**Theorem (Fraïssé 1954; Ehrenfeucht 1961)**

Duplicator has a strategy for winning the $p$-round Ehrenfeucht game on $\mathcal{A}$ and $\mathcal{B}$ if, and only if, $\mathcal{A} \equiv_p \mathcal{B}$.
Proof by Example

Suppose $A \not \equiv_3 B$, in particular, suppose $\theta(x, y, z)$ is quantifier free, such that:

\[
A \models \exists x \forall y \exists z \theta \quad \text{and} \quad B \models \forall x \exists y \forall z \neg \theta
\]

**round 1:** *Spoiler* chooses $a_1 \in A$ such that $A \models \forall y \exists z \theta[a_1]$.  
*Duplicator* responds with $b_1 \in B$.

**round 2:** *Spoiler* chooses $b_2 \in B$ such that $B \models \forall z \neg \theta[b_1, b_2]$.  
*Duplicator* responds with $a_2 \in A$.

**round 3:** *Spoiler* chooses $a_3 \in A$ such that $A \models \theta[a_1, a_2, a_3]$.  
*Duplicator* responds with $b_3 \in B$.

*Spoiler* wins, since $B \not \models \theta[b_1, b_2, b_3]$.  

Using Games

To show that a class of structures $S$ is not definable in $\text{FO}$, we find, for every $p$, a pair of structures $A_p$ and $B_p$ such that

- $A_p \in S$, $B_p \in \overline{S}$; and
- Duplicator wins a $p$ round game on $A_p$ and $B_p$.

**Example:**

$C_n$—a cycle of length $n$.

Duplicator wins the $p$ round game on $C_{2p} \oplus C_{2p}$ and $C_{2p+1}$.

- 2-Colourability is not definable in $\text{FO}$.
- Even cardinality is not definable in $\text{FO}$.
- Connectivity is not definable in $\text{FO}$.
Using Games

An illustration of the game for undefinability of *connectivity* and *2-colourability*.

*Duplicator*’s strategy is to ensure that after \( r \) moves, the distance between corresponding pairs of pebbles is either *equal* or \( \geq 2^{p-r} \).
**Inductive Definitions**

Let \( \varphi(R, x_1, \ldots, x_k) \) be a first-order formula in the vocabulary \( \sigma \cup \{R\} \)

Associate an operator \( \Phi \) on a given structure \( A \):

\[
\Phi(R^A) = \{ a \mid (A, R^A, a) \models \varphi(R, x) \}
\]

We define the *increasing* sequence of relations on \( A \):

\[
\Phi^0 = \emptyset \\
\Phi^{m+1} = \Phi^m \cup \Phi(\Phi^m)
\]

The *inflationary fixed point* of \( \Phi \) is the limit of this sequence.

On a structure with \( n \) elements, the limit is reached after at most \( n^k \) stages.
The logic **IFP** is formed by closing first-order logic under the rule:

If $\varphi$ is a formula of vocabulary $\sigma \cup \{R\}$ then $[\text{ifp}_{R,x\varphi}(t)]$ is a formula of vocabulary $\sigma$.

The formula is read as:

the tuple $t$ is in the inflationary fixed point of the operator defined by $\varphi$

**LFP** is the similar logic obtained using *least fixed points* of *monotone* operators defined by *positive* formulas.

**LFP** and **IFP** have the same expressive power (**Gurevich-Shelah; Kreutzer**).
Transitive Closure

The formula

$$\text{ifp}_{T, xy}(x = y \lor \exists z(E(x, z) \land T(z, y)))](u, v)$$

defines the reflexive and transitive closure of the relation $E$

The expressive power of IFP properly extends that of first-order logic.

On structures which come equipped with a linear order IFP expresses exactly the properties that are in $P$.

(Immerman; Vardi)

Open Question: Is there a logic that expresses exactly the properties for unordered structures?
Finite Variable Logic

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

$$A \equiv^k B$$

denotes that $A$ and $B$ agree on all sentences of $L^k$.

For any $k$,

$$A \equiv^k B \implies A \equiv_k B$$

However, for any $q$, there are $A$ and $B$ such that

$$A \equiv_q B \text{ and } A \not\equiv^2 B.$$
Axiomatisability

Any class of finite structures closed under isomorphisms is *axiomatised* by a first-order theory.

A class of finite structures is closed under $\equiv_q$ (for some $q$) if, and only if, it is *finitely axiomatised*, i.e. defined by a single FO sentence.

A class of finite structures is closed under $\equiv^k$ if, and only if, it is axiomatisable in $L^k$ (possibly by an infinite collection of sentences).

Every sentence of IFP is equivalent, *on finite structures*, to an $L^k$ theory, for some $k$.

$$\varphi(R, x_1, \ldots, x_l) \in L^k$$

Each stage of the induction $\varphi^m$ can be written as a formula in $L^{k+l}$. 

Anuj Dawar

March 2009
Pebble Games

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

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

\textit{Duplicator} responds by picking the matching pebble and placing it on an element of the other structure.

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

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

To show that a class of structures $S$ is not definable in first-order logic:

$$\forall k \ \forall q \ \exists A, B \ (A \in S \land B \notin S \land A \equiv^k_q B)$$

To show that $S$ is not axiomatisable with a finite number of variables:

$$\forall k \ \exists A, B \ \forall q \ (A \in S \land B \notin S \land A \equiv^k_q B)$$
Evenness

To show that *Evenness* is not definable in IFP, it suffices to show that:

for every $k$, there are structures $A_k$ and $B_k$ such that $A_k$ has an even number of elements, $B_k$ has an odd number of elements and

$$A \equiv^k B.$$ 

It is easily seen that *Duplicator* has a strategy to play forever when one structure is a set containing $k$ elements (and no other relations) and the other structure has $k + 1$ elements.
Hamiltonicity

Take $K_{k,k}$—the complete bipartite graph on two sets of $k$ vertices.

and $K_{k,k+1}$—the complete bipartite graph on two sets, one of $k$ vertices, the other of $k + 1$.

These two graphs are $\equiv^k$ equivalent, yet one has a Hamiltonian cycle, and the other does not.
Fixed-point Logic with Counting

Immerman proposed IFP + 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 numbers in the range $0, \ldots, |A|$

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

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

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

- 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 $\varphi$ of IFP + $C$, there is a $k$ such that if $A \equiv^{C^k} B$, then

$$A \models \varphi \text{ if, and only if, } B \models \varphi.$$
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 $A$ to $B$ defined by the
pebble pairs is not a partial isomorphism.

If Duplicator has a winning strategy for $q$ moves, then $A$ and $B$ agree on
all sentences of $C^k$ of quantifier rank at most $q$. 
Cai-Fürer-Immerman Graphs

There are polynomial-time decidable properties of graphs that are not definable in IFP + C. \textit{(Cai, Fürer, Immerman, 1992)}

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

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

Still, IFP + C is a \textit{natural} level of expressiveness within $P$. 
**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

If \( G \) is connected and has treewidth at least \( k \), then:

1. \( X_G \not\equiv \tilde{X}_G \); and

2. \( X_G \equiv^C \tilde{X}_G \).

(1) allows us to construct a polynomial time property separating \( X_G \) and \( \tilde{X}_G \). (2) is proved by a game argument.

The original proof of \((\text{Cai, Fürer, Immerman})\) relied on the existence of balanced separators in \( G \). The characterisation in terms of treewidth is from \((\text{D., Richerby 07})\).
Bijection Games

$\equiv_{C^k}$ is characterised by a $k$-pebble bijection game. (Hella 96).

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

- **Spoiler** chooses a pair of pebbles $a_i$ and $b_i$;
- **Duplicator** chooses a bijection $h : A \rightarrow B$ 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, $A \equiv_{C^k} B$. 

Anuj Dawar March 2009
TreeWidth

The \textit{treewidth} of a graph is a measure of its interconnectedness.

A graph has treewidth $k$ if it can be covered by subgraphs of at most $k + 1$ nodes in a tree-like fashion.
**TreeWidth**

*Formal Definition:*

For a graph $G = (V, E)$, a *tree decomposition* of $G$ is a relation $D \subset V \times T$ with a tree $T$ such that:

- for each $v \in V$, the set $\{t \mid (v, t) \in D\}$ forms a connected subtree of $T$; 

- for each edge $(u, v) \in E$, there is a $t \in T$ such that $(u, t), (v, t) \in D$.

The *treewidth* of $G$ is the least $k$ such that there is a tree $T$ and a tree-decomposition $D \subset V \times T$ such that for each $t \in T$,

$$|\{v \in V \mid (v, t) \in D\}| \leq k + 1.$$
Cops and Robbers

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.
Strategies and Decompositions

**Theorem (Seymour and Thomas 93):**
There is a winning strategy for the *cop player* with $k$ cops on a graph $G$ if, and only if, the tree-width of $G$ is at most $k - 1$.

It is not difficult to construct, from a tree decomposition of width $k$, a winning strategy for $k + 1$ cops.

Somewhat more involved to show that a winning strategy yields a decomposition.
Cops, Robbers and Bijections

If $G$ has treewidth $k$ or more, than the robber has a winning strategy in the $k$-cops and robbers game played on $G$.

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 $h : X_G \rightarrow \tilde{X}_G$ 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.
Solvability of Linear Equations

A natural P problem that has been shown to be undefinable in IFP + C is the problem of solving linear equations over the two element field $\mathbb{Z}_2$.

(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

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 \( e \).

\( \text{Solv}(\mathbb{Z}_2) \) is the class of structures representing solvable systems.
Undenability in \( \text{IFP} + \mathbb{C} \)

Take \( G \) a 3-regular, connected graph with treewidth \( > k \).

Define equations \( \mathcal{E}_G \) 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:

\[
\mathcal{E}_v : \quad x^e_{i} + x^e_{j} + x^e_{k} \equiv i + j + k \pmod{2}
\]

\( \tilde{\mathcal{E}}_G \) is obtained from \( \mathcal{E}_G \) by replacing, for exactly one vertex \( v \), \( \mathcal{E}_v \) by:

\[
\mathcal{E}'_v : \quad x^e_{i} + x^e_{j} + x^e_{k} \equiv i + j + k + 1 \pmod{2}
\]

We can show: \( \mathcal{E}_G \) is satisfiable; \( \tilde{\mathcal{E}}_G \) is unsatisfiable; \( \mathcal{E}_G \equiv^C_k \tilde{\mathcal{E}}_G \)
Computational Problems from Linear Algebra

*Linear Algebra* is a testing ground for exploring the boundary of the expressive power of \( \text{IFP} + C \).

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 \( \mathbb{Z}_2 \):

\[
M_{ij} = 1 \iff (i, j) \in A.
\]

Most interesting properties of \( M \) are invariant under permutations of \( I \).
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

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

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

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

These two representations are inter-definable.
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.
Rank Operators

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

$rk_{x,y} \varphi$ is a *term* denoting the number that is the rank of the matrix defined by $\varphi(x, y)$.

More generally, we could have, for each finite field $\mathbb{F}_q$, an operator $rk^q$.

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

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

$$\# x \varphi = \text{rk}_{x,y}[x = y \land \varphi(x)]$$

In $\text{IFP} + \text{rank}$ we can express the solvability of linear systems of equations, as well as the Cai-Fürer-Immerman graphs and the order on multipedes.
Games for Logics with Rank

What might a pebble game for IFP + rank 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?
Open Questions

With a suitable notion of game, we could try and tackle problems like:

- Are there any problems in $P$ that are not definable in $\text{IFP} + \text{rank}$?

- Show for any concrete problem (say an $\text{NP}$-complete one) that it is not definable in $\text{IFP} + \text{rank}$.

- Are $\text{rk}^p$ and $\text{rk}^q$ interdefinable for $p \neq q$?

- etc.