Finite Model Theory and Graph Isomorphism. I.

Anuj Dawar

University of Cambridge Computer Laboratory
visiting RWTH Aachen

Beroun, 12 December 2013

Finite Model Theory

In the 1980s, the term *finite model theory* came to be used to describe the study of the expressive power of logics (from first-order to second-order logic and in between), on the class of all finite structures.

The motivation for the study is that problems in computer science (especially in *complexity theory* and *database theory*) are naturally expressed as questions about the expressive power of logics.
And, the structures involved in computation are finite.

Example - Vertex Cover

For each k, we can write a *first-order formula* in the language of graphs which says that there is a vertex cover of size at most k.

$$\exists x_1 \cdots \exists x_k (\forall y \forall z (E(y,z) \Rightarrow (\bigvee_{1 \leq i \leq k} y = x_i \vee \bigvee_{1 \leq i \leq k} z = x_i)$$

Here, quantifiers range over vertices of the graph

Example - 3-Colourability

3-colourability of graphs can be expressed by a formula when we allow quantification over *sets of vertices*.

$$
\begin{aligned}
\exists R \subseteq V\, \exists B \subseteq V\, \exists G \subseteq V \quad & \\
& \forall x (Rx \lor Bx \lor Gx) \land \\
& \forall x (\neg(Rx \land Bx) \land \neg(Bx \land Gx) \land \neg(Rx \land Gx)) \land \\
& \forall x \forall y (Exy \to (\neg(Rx \land Ry) \land \\
& \qquad \neg(Bx \land By) \land \\
& \qquad \neg(Gx \land Gy)))
\end{aligned}
$$

Model Theoretic Questions

The kind of questions we are interested in are about the *expressive power* of logics. Given a formula φ, its class of models is the collection of *finite* relational structures $\mathbb{A}$ in which it is true.

$$\mathrm{Mod}(\varphi) = \{\mathbb{A} \mid \mathbb{A} \models \varphi\}$$

What classes of structures are definable in a given logic $\mathcal{L}$?

How do syntactic restrictions on φ relate to semantic restrictions on $\mathrm{Mod}(\varphi)$?

How does the computational complexity of $\mathrm{Mod}(\varphi)$ relate to the syntactic complexity of φ?

Descriptive Complexity

A class of finite structures is definable in existential second-order logic if, and only if, it is decidable in NP.

(Fagin 1974)

A class of ordered finite structures is definable in least fixed-point logic if, and only if, it is decidable in P.

(Immerman; Vardi 1982)

Open Question: Is there a logic that captures P without order?

Can *model-theoretic* methods cast light on questions of computational complexity?

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 φ of the language such that

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

Graphs

For concreteness, we consider *finite graphs*.

These are structures in a vocabulary with just one binary relation E, which is interpreted as an *irreflexive, symmetric* relation.

We will also have occasion to look at vocabularies with additional constants (s, t) in addition to the binary relation E.

Occasionally, we also consider *coloured graphs*. These may be

- structures in a vocabulary with one binary relation E and some number of *unary relations* $C_1, \ldots, C_n$; or
- structures in a vocabulary with *two* binary relations: E and $\preceq$. The latter is a *linear pre-order*.

First-Order Logic

terms – c, x

atomic formulae – $E(t_1, t_2), t_1 = t_2, t_1 \preceq t_2, C(t)$

boolean operations – $\varphi \wedge \psi$, $\varphi \vee \psi$, $\neg\varphi$

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

Examples

A *vertex cover* of size k:

$$\exists x_1 \cdots \exists x_k (\forall y \forall z (E(y,z) \Rightarrow (\bigvee_{1 \leq i \leq k} y = x_i \vee \bigvee_{1 \leq i \leq k} z = x_i)$$

Graphs which contain a *triangle*:

$$\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge x \neq y \wedge E(x,y) \wedge E(y,z) \wedge E(x,z))$$

Unions of cycles:

$$\forall x (\exists ! y E(x,y) \wedge \exists ! z E(z,y))$$

Can we define the class of connected graphs or 3-colourable graphs? No, but how to prove it?

Model Comparison Games

Inexpressiblity results in *Finite Model Theory* are often proved by means of *games*.

In this tutorial, we examine a number of *Model Comparison Games*.

These are typically two-player games played on a pair of graphs G and H.
The games are used to establish that G and H cannot be *distinguished* in some logic under consideration.

Spoiler and Duplicator

The two players in our games are generally called *Spoiler* and *Duplicator*. The game board consists of two graphs G and H.

> *Spoiler tries to prove that G and H are different.*
> *Duplicator tries to pretend that they are really the same*

We say the two graphs are *indistinguishable* (according to the rules of the game) if *Duplicator* has a winning strategy.
If the structures *are* the same (i.e. they are *isomorphic*), then *Duplicator* necessarily has a winning strategy.

In general, the relation of *indistinguishability* gives us an *approximation* of isomorphism.

Some Games

Classes of games that will come up in this tutorial include:

> *Ehrenfeucht-Fraïssé games; pebble games; counting games; bijection games; partition games; and invertible map games*

Associated with them are various *logics* for which they are used to establish inexpressiveness results.

Many of these logics arose in the long-standing *quest* for a logic for P.

We will also see how the *indistinguishability* relations defined by the games relate to *isomorphism*, and look at other ways to characterise these equivalences.

The Power of First-Order Logic

For every finite graph G, there is a sentence φ_G such that

$$H \models \varphi_G \quad \text{if, and only if,} \quad H \cong G$$

Given a graph G with n elements, we define

$$\varphi_G = \exists x_1 \ldots \exists x_n \psi \land \forall y \bigvee_{1 \leq i \leq n} y = x_i$$

where, $\psi(x_1, \ldots, x_n)$ is the conjunction of all atomic and negated atomic formulas (e.g. $E(x_i, x_j)$ and $\neg E(x_i, x_j)$) that hold in G.

First-Order Logic is Weak

For any first-order sentence φ, the collection of finite graphs that satisfy it

$$\mathrm{Mod}(\varphi) = \{G \mid G \models \varphi\}$$

is trivially decidable (in LogSpace).

There are computationally easy classes that are not defined by any first-order sentence.

- The class of graphs with an *even* number of vertices.
- The class of graphs that are *connected*.

Quantifier Rank

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

1. if φ is atomic then $\mathrm{qr}(\varphi) = 0$,
2. if $\varphi = \neg\psi$ then $\mathrm{qr}(\varphi) = \mathrm{qr}(\psi)$,
3. if $\varphi = \psi_1 \vee \psi_2$ or $\varphi = \psi_1 \wedge \psi_2$ then $\mathrm{qr}(\varphi) = \max(\mathrm{qr}(\psi_1), \mathrm{qr}(\psi_2))$.
4. if $\varphi = \exists x\psi$ or $\varphi = \forall x\psi$ then $\mathrm{qr}(\varphi) = \mathrm{qr}(\psi) + 1$

It is easily proved that in any finite vocabulary, for each p, there are (up to logical equivalence) only finitely many sentences φ with $\mathrm{qr}(\varphi) \leq p$.

Finitary Elementary Equivalence

For two graphs G and H, we say $G \equiv_p H$ if for any sentence φ with $\mathrm{qr}(\varphi) \leq p$,

$$G \models \varphi \text{ if, and only if, } H \models \varphi.$$

Key fact:

> *a property of graphs P is definable by a first order sentence if, and only if, P is closed under the relation $\equiv_p$ for some p.*

For any graph G there is a sentence θ^p_G such that

$$H \models \theta^p_G \quad \text{if, and only if,} \quad G \equiv_p H$$

Ehrenfeucht-Fraïssé Game

The p-round Ehrenfeucht game on graphs G and H proceeds as follows:

- There are two players called *Spoiler* and *Duplicator*.
- At the ith round, *Spoiler* chooses one of the two graphs (say H) and one of the vertices of that graph (say b_i).
- *Duplicator* must respond with an element of the other graph (say a_i).
- If, after p rounds, the map $a_i \mapsto b_i$ is *not* a partial isomorphism, then *Spoiler* 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 G and H if, and only if, $G \equiv_p H$.

Proof by Example

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

$$G \models \exists x \forall y \exists z \theta \quad \text{and} \quad H \models \forall x \exists y \forall z \neg\theta$$

round 1: Spoiler chooses $a_1 \in V(G)$ *such that* $G \models \forall y \exists z \theta[a_1]$.
Duplicator responds with $b_1 \in V(H)$.

round 2: Spoiler chooses $b_2 \in V(H)$ *such that* $H \models \forall z \neg\theta[b_1, b_2]$.
Duplicator responds with $a_2 \in V(G)$.

round 3: Spoiler chooses $a_3 \in V(G)$ *such that* $G \models \theta[a_1, a_2, a_3]$.
Duplicator responds with $b_3 \in V(H)$.

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

Using Games

To show that a property of graphs P is not definable in FO, we find, for every p, a pair of graphs G_p and H_p such that

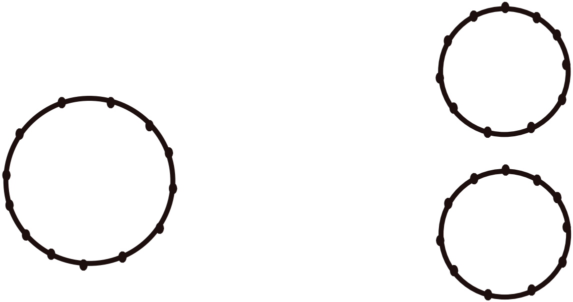
- $G_p \in P$, $H_p \in \overline{P}$; and
- *Duplicator* wins a p-round game on G_p and H_p.

Example:
C_n—a cycle of length n.
Duplicator wins the p round game on $C_{2^p} \oplus C_{2^p}$ and C_{2^p+1}.

- 2-Colourability is not definable in FO.
- Even cardinality is not definable in FO.
- Connectivity is not definable in 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 $\geq 2^{p-r}$.

Stratifying Isomorphism

In order to study the expressive power of *first-order logic* on finite structures, we considered one stratification of isomorphism:

$$G \equiv_p H$$

if G and H cannot be distinguished by any sentence with *quantifier rank* at most p.

An alternative stratification that is useful in studying *fixed-point logics* is based on the number of variables.

$$G \equiv^k H$$

if G and H cannot be distinguished by any sentence with at most k *distinct variables*.

Inductive Definitions

Let $\varphi(R, x_1, \ldots, x_k)$ be a first-order formula in the vocabulary $\sigma \cup \{R\}$
Associate an operator Φ on a given σ-structure $\mathbb{A}$:

$$\Phi(R^{\mathbb{A}}) = \{\mathbf{a} \mid (\mathbb{A}, R^{\mathbb{A}}, \mathbf{a}) \models \varphi(R, \mathbf{x})\}$$

We define the *increasing* sequence of relations on $\mathbb{A}$:

$$\Phi^0 = \emptyset$$

$$\Phi^{m+1} = \Phi^m \cup \Phi(\Phi^m)$$

The *inflationary fixed point* of Φ is the limit of this sequence.
On a structure with n elements, the limit is reached after at most n^k stages.

IFP

The logic FP is formed by closing first-order logic under the rule:

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

The formula is read as:

the tuple $\mathbf{t}$ is in the inflationary fixed point of the operator defined by φ

Transitive Closure

The formula

$$[\mathbf{ifp}_{T,xy}(x = y \vee \exists z(E(x,z) \wedge T(z,y)))](u,v)$$

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

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

On structures which come equipped with a linear order FP 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 $x_1, \ldots, x_k$.

$$G \equiv^k H$$

denotes that G and H agree on all sentences of L^k.

For any k, $\quad G \equiv^k H \quad \Rightarrow \quad G \equiv_k H$

However, for any p, there are G and H such that

$$G \equiv_p H \quad \text{and} \quad G \not\equiv^2 H.$$

Definability and Invariance

A class of graphs is closed under $\equiv_p$ (for some p) if, and only if, it is *defined* by a 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).

For every φ sentence of FP there is a k such that $\mathrm{Mod}(\varphi)$ is closed under $\equiv^k$.

Indeed, for graphs of fixed size n, φ is equivalent to a sentence of L^k.

FP and L^k

Given $\psi(R, x_1, \ldots, x_l) \in L^k$, each stage of the induction ψ^m can be written as a formula in L^{k+l}.

Let the variables occurring in ψ be $x_1, \ldots, x_k$ and $y_1, \ldots, y_l$ be new.

ψ^{m+1} is obtained from $\psi(R, \mathbf{x})$ by replacing all sub-formulas $R(t_1, \ldots, t_l)$ with

$$\exists y_1 \ldots \exists y_l \, (\bigwedge_{1 \leq i \leq l} y_i = t_i) \wedge \varphi^m(\mathbf{y})$$

Pebble Games

The k-pebble game is played on two graphs G and H, 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 a vertex (a_i on a vertex in G or b_i on a vertex in H).*
>
> *Duplicator responds by picking the matching pebble and placing it on an element of the other graph*
>
> *Spoiler wins at any stage if the partial map from G to H defined by the pebble pairs is not a partial isomorphism*
>
> *If Duplicator has a winning strategy for p moves, then G and H agree on all sentences of L^k of quantifier rank at most p.* **(Barwise)**

Using Pebble Games

To show that a property of graphs P is not definable in first-order logic:
$\forall k \, \forall p \, \exists G, H \, (G \in P \wedge H \notin P \wedge G \equiv_p^k H)$

To show that P is not axiomatisable with a finite number of variables:
$\forall k \, \exists G, H \, \forall p \, (G \in P \wedge H \notin P \wedge G \equiv_p^k H)$

Evenness

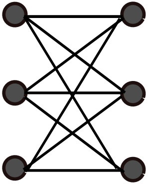
To show that *Evenness* is not definable in FP, it suffices to show that:

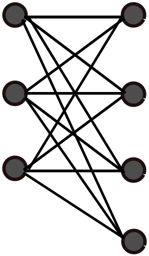
> *for every k, there are graphs G_k and H_k such that G_k has an even number of vertices, H_k has an odd number of elements and*
>
> $$G_k \equiv^k H_k.$$

It is easily seen that *Duplicator* has a strategy to play forever when one graph has k vertices and no edges and the other grahs has $k + 1$ vertices and no edges.

Matching

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 perfect matching, and the other does not.

Stratifications of Isomorphism

In a *finite, relational* vocabulary, there are only finitely many sentences of quantifier rank at most p.
Thus, the relation $\equiv_p$ has only finitely many equivalence classes.

As approximations of isomorphism, these are very coarse.

The relation $\equiv^k$ has infintiely many classes for all $k \geq 2$.

Still, for any k, and *randomly chosen* graphs G_1 and G_2, we have $G_1 \equiv^k G_2$.
Indeed, there is a single $\equiv^k$-equivalence class that contains *almost all* graphs.