Fixed-Point Logics and Computation

Symposium on the
Unusual Effectiveness of Logic in Computer Science

Anuj Dawar
University of Cambridge

Mathematical Logic

Mathematical logic seeks to formalise the process of mathematical reasoning and turn this process itself into a subject of mathematical enquiry.

It investigates the relationships among:

- Structure
- Language
- Proof

Proof-theoretic vs. *Model-theoretic* views of logic.

Computation as Logic

If logic aims to reduce reasoning to symbol manipulation,

> *On the one hand, computation theory provides a formalisation of "symbol manipulation".*

> *On the other hand, the development of computing machines leads to "logic engineering".*

The validities of first-order logic are r.e.-complete.

Proof Theory in Computation

As all programs and data are strings of symbols in a formal system, one view sees all computation as inference.

For instance, the functional programming view:

- Propositions are types.
- Programs are (constructive proofs).
- Computation is proof transformation.

Model Theory in Computation

A model-theoretic view of computation aims to distinguish computational *structures* and languages used to talk about them.

Data Structure	Programming Language
Database	Query Language
Program/State Space	Specification Language

The structures involved are rather different from those studied in classical model theory. *Finite Model Theory.*

First-Order Logic

terms – $c, x, f(t_1, \ldots, t_a)$

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

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

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

Formulae are interpreted in structures:

$$\mathbb{A} = (A, R_1, \ldots, R_m, f_1, \ldots, f_n, c_1, \ldots, c_n)$$

Success of First-Order Logic

First-order logic is very successful at its intended purpose, the formalisation of mathematics.

Many natural mathematical theories can be expressed as first-order theories.

These include *set theory*, fundamental to the foundations of mathematics.

Gödel's completeness theorem guarantees that the consequences of these theories can be effectively obtained.

Finite Structures

The completeness theorem fails when restricted to finite structures.

> The sentences of first-order logic, valid on finite structures are not recursively enumarable.

(Trakhtenbrot 1950)

On finite structures, first-order logic is both too strong and too weak.

First-Order Logic is too Strong

For every finite structure $\mathbb{A}$, there is a sentence $\varphi_{\mathbb{A}}$ such that

$$\mathbb{B} \models \varphi_{\mathbb{A}} \quad \text{if, and only if,} \quad \mathbb{B} \cong \mathbb{A}$$

For any isomorphism-closed class of finite structures, there is a first-order theory that defines it.

First-Order Logic is too Weak

For any first-order sentence φ, its class of finite models

$$\mathrm{Mod}_{\mathcal{F}}(\varphi) = \{\mathbb{A} \mid \mathbb{A} \text{ finite, and } \mathbb{A} \models \varphi\}$$

is trivially decidable (in LogSpace).

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

- The class of sets with an even number of elements.
- The class of graphs (V, E) that are connected.

Inductive Definitions

In computing (and logic), many classes of structures are naturally defined *inductively*.

viz. The definition of the terms and formulae of first-order logic.

Includes definitions of syntax and semantics of most *languages*, of *data structures* (trees, lists, etc.), of *arithmetic functions*.

Definition by Fixed Point

The collection of first-order terms can be defined as *the least set* containing all constants, all variables and such that $f(t_1, \ldots, t_a)$ is a term whenever $t_1, \ldots, t_a$ are terms and f is a function symbol of arity a.

The addition function is defined as the least function satisfying:

$$\begin{aligned} x + 0 &= x \\ x + s(y) &= s(x + y). \end{aligned}$$

In each case, the set defined is the least fixed point of a monotone operator on sets.

From Metalanguage to Language

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

> If φ is a formula, *positive* in the relational variable R, then so is
>
> $$[\mathbf{lfp}_{R,\mathbf{x}}\varphi](\mathbf{t}).$$

The formula is read as:

> the tuple $\mathbf{t}$ is in the least fixed point of the operator that maps R to $\varphi(R, \mathbf{x})$.

Connectivity

The formula

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

is satisfied in a graph (V, E) if, and only if, it is connected.

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

Immerman-Vardi Theorem

Consider finite structures with a distinguished relation $<$ that is interpreted as a linear order of the universe.

> A class of finite ordered structures is definable by a sentence of LFP if, and only if, membership in the class is decidable by a deterministic Turing machine in *polynomial time*.
>
> (Immerman, Vardi 1982).

In the absence of the order assumption, there are easily computable properties that are not definable in LFP.

Iterated Fixed Points

The least fixed point of the operator defined by a formula $\varphi(R, \mathbf{x})$ on a structure $\mathbb{A}$ can be obtained by an iterative process:

$$\begin{aligned} R^0 &= \emptyset \\ R^{m+1} &= \{\mathbf{a} \mid \mathbb{A}, R^m \models \varphi[\mathbf{a}/\mathbf{x}]\} \end{aligned}$$

There is a k such that if $\mathbb{A}$ has n elements, the fixed point is reached in at most n^k stages.

On infinite structures, we have to also take unions at limit stages.

Inflationary Fixed Point Logic

If $\varphi(R, \mathbf{x})$ is not necessarily positive in R, the following iterative process still gives an increasing sequence of stages:

$$
\begin{aligned}
R^0 &= \emptyset \\
R^{m+1} &= R^m \cup \{\mathbf{a} \mid \mathbb{A}, R^m \models \varphi[\mathbf{a}/\mathbf{x}]\}
\end{aligned}
$$

The limit of this sequence is the *inflationary fixed point* of the operator defined by φ.

IFP is the set of formulae obtained by closing first-order logic under the formula formation rule:

$$[\mathbf{ifp}_{R,\mathbf{x}}\varphi](\mathbf{t}).$$

LFP vs. IFP

It is clear that every formula of LFP is equivalent to one of IFP.

Every formula of IFP is equivalent, *on finite structures*, to one of LFP.

(Gurevich-Shelah, 1986)

The restriction to finite structures is not necessary.

(Kreutzer, 2002)

Partial Fixed Point Logic

For any formula $\varphi(R, \mathbf{x})$ and structure $\mathbb{A}$, we can define the iterative sequence of stages

$$\begin{aligned} R^0 &= \emptyset \\ R^{m+1} &= \{\mathbf{a} \mid \mathbb{A}, R^m \models \varphi[\mathbf{a}/\mathbf{x}]\}. \end{aligned}$$

This sequence is not necessarily increasing, and may or may not converge to a fixed point.

The *partial fixed point* is the limit of this sequence if it exists, and $\emptyset$ otherwise.

PFP is the set of formulae obtained by closing first-order logic under the formula formation rule:

$$[\mathbf{pfp}_{R,\mathbf{x}}\varphi](\mathbf{t}).$$

Abiteboul-Vianu Theorem

A class of finite ordered structures is definable by a sentence of PFP if, and only if, membership in the class is decidable by a deterministic Turing machine using a *polynomial amount of space*.

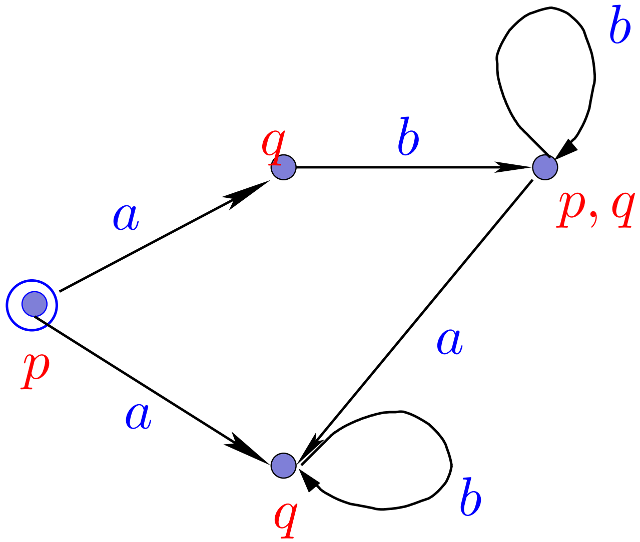
Every formula of PFP is equivalent (*on finite structures*) to one of LFP if, and only if, every polynomial space decidable property is also decidable in polynomial time.

(Abiteboul-Vianu 1995)

Similar re-formulations of various complexity-theoretic questions (including the P vs. NP question) in terms of fixed-point logics.

State Transition Systems

A class of structures of great importance in verification are *state transition systems*, which are models of program behaviour.



$\mathbb{A} = (S, (E_a)_{a \in A}, (p)_{p \in P})$, where A is a set of actions and P is a set of propositions.

Modal Logic

The formulae of Hennessy-Milner logic are given by:

- T and F
- $p \qquad\qquad (p \in P)$
- $\varphi \wedge \psi$; $\varphi \vee \psi$; $\neg\varphi$
- $[a]\varphi$; $\langle a \rangle\varphi \qquad (a \in A)$.

For the semantics, note

$$\mathcal{K}, v \models \langle a \rangle\varphi$$

iff for some w with $v \xrightarrow{a} w$, we have $\mathcal{K}, w \models \varphi$.

Dually for $[a]$.

Modal μ-calculus

Generally, logics more expressive than H-M are considered.

The *modal μ-calculus (L_μ)* extends H-M with recursion (and extends a variety of other extensions, such as CTL, PDL, CTL*).

An additional collection of variables $X_1, X_2, \ldots$

$\mu X : \varphi$ is a formula if φ is a formula containing only positive occurrences of X.

$$\mathcal{K}, v \models \mu X : \varphi$$

iff v is in the least set X such that $X \leftrightarrow \varphi$ in $(\mathcal{K}, X)$.

LFP and the μ-calculus

Suppose φ is a formula of LFP with no more than k first-order variables (and no parameters to fixed-point operators).

There is a formula $\hat{\varphi}$ of the L_μ such that

$$\mathbb{A} \models \varphi \quad \text{if, and only if,} \quad \hat{\mathbb{A}}^k \models \hat{\varphi},$$

where $\hat{\mathbb{A}}^k$ is the transition system with states corresponding to k-tuples of $\mathbb{A}$, k actions corresponding to substitutions, and propositions corresponding to the relations of $\mathbb{A}$.

This gives a computational equivalence between many problems of LFP and L_μ.

IFP and the μ-calculus

While every formula of IFP is equivalent to one of LFP, the translation does not preserve number of variables.

Some of the desirable computational properties of L_μ do not lift to IFP.

Modal logic with an inflationary fixed point operator is more expressive than L_μ.

Modal Fixed-Point Logics

MIC – the modal inflationary calculus.

	L_μ	MIC
Finite Model Property	Yes	No
Satisfiability	Decidable	Not Arithmetic
Model-checking	NP ∩ CO-NP	PSPACE-complete
Languages defined	Regular	Some context-sensitive
		all linear-time.

(D., Grädel, Kreutzer 2001)

Modal versions of partial and nondeterministic fixed-point logic can also be separated.

In Summary

- Model-theoretic methods concerned with studying the expressive power of logical languages.
- First-order logic does not occupy a central place.
- A variety of fixed-point extensions of first-order logic used to study complexity.
- Convergence of methods with fixed-point modal logics studied in verification.
- Fine structure of fixed-point logics can be studied in the modal context.