Complexity as Expressive Power

Anuj Dawar

Computer Laboratory
University of Cambridge

BCTCS, Bristol, April 2002

Logic and Complexity Theory

Study of Logic intersects Computational Complexity in many ways

Complexity of decidable logics; of logical inference and of logical theories.

By Cook's theorem, complexity of propositional logic captures nondeterministic polynomial time complexity.

Complexity classes can be characterised by functions that are provably total in weak arithmetic.

Descriptive Complexity

Fagin's Theorem

A property is expressible in existential second-order logic if, and only if, it is decidable in NP

Computational Complexity:

space, time or other resources on a machine model of computation

complexity of a language - i.e. a set of strings

Descriptive Complexity:

classes of structures - *e.g.* a collection of graphs

the complexity of describing the collection

Relational Structures

In general, finite relational structures

$\mathcal{A} = (A, R_1, \ldots, R_m, c_1, \ldots, c_n)$

The description language is Predicate Logic

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

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

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

Existential second-order logic comprises formulas of the form:

$$\exists P_1 \ldots \exists P_m \varphi$$

where φ is first-order.

Complexity of Structure Classes

What does it mean for a class of structures to be decidable in NP*?*

For a structure $\mathcal{A}$ and an order $<$ of its elements, we define a string $[\mathcal{A}]_<$ that encodes it.

> For instance, we could represent a k-ary relation on n elements as a binary string of length n^k.

To say that the property defined by φ is decidable in NP means that the set of strings

$$\{[\mathcal{A}]_< \mid \mathcal{A} \models \varphi\}$$

is in NP.

Complexity of First and Second-Order Logic

If φ is a first-order formula, then the property defined by φ is in L.

Fagin's Theorem
A property is decidable in NP if, and only if, it is definable by a formula of existential second-order logic.

A logical characterisation of NP?

A complexity-theoretic characterisation of second-order logic?

Isomorphism invariance

Properties of structures definable in first or second-order logic are invariant under isomorphisms.

For any fixed relational signature σ, there are sets of strings that represent isomorphism-invariant classes of σ-structures.

> Existential second-order logic characterises the fragment of NP that is closed under isomorphism.

A logical characterisation of a complexity class implies that the resource restrictions commute in a reasonable fashion with the invariance conditions.

The isomorphism closure of any NP decidable collection of strings is itself in NP.

Is there a logic for P?

Question
Is there a logic that characterises the properties of finite relational structures that are decidable in P?

Chandra-Harel

The isomorphism closure of a polynomial-time decidable collection of strings is not necessarily in P.

Are the polynomial-time, isomorphism-closed classes recursively enumerable?

Inductive Logic

Let $\varphi(R, \mathbf{x})$ *be a first-order formula in the vocabulary* $\sigma \cup \{R\}$

Associated operator Φ*:*

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

Φ *is monotone if for any relations* R *and* S *such that* $R \subseteq S$*,* $\Phi(R) \subseteq \Phi(S)$

If Φ *is monotone, it has a least fixed point.*

LFP

The language LFP is obtained by closing first order logic under an operation for forming the least fixed points of positive formulas:

Example:

Let $\varphi(R, x, y)$ be $x = y \vee \exists z(E(x, z) \wedge R(z, y))$

Then, $[\mathbf{lfp}_{R,x,y}\varphi](u, v)$ is a formula in two free variables that expresses the transitive closure of E.

$\forall u \forall v \, [\mathbf{lfp}_{R,x,y}\varphi](u, v)$ expresses connectedness.

Polynomial time complexity

If φ is a sentence of LFP, then the set of strings:

$$\{[\mathcal{A}]_< \mid \mathcal{A} \models \varphi \text{ and } < \text{ is an order on } A\}$$

is in P.

If the signature includes a distinguished symbol $<$ always interpreted as an order, then a class of structures is definable by a formula φ of LFP if, and only if,

$$\{[\mathcal{A}]_< \mid \mathcal{A} \models \varphi\}$$

is decidable in P.

(Immerman and Vardi)

Expressive power of LFP

Without the order, LFP is too weak to express all properties in P.

Various extensions of LFP have been studied in attempts to characterise P

- Counting;
- Generalized Quantifiers;
- Choice.

One could equally well ask, what is the exact power of LFP, in terms of complexity?

Finite variable logic

L^k — First order formulas using only the variables $x_1, \ldots, x_k$.

$$\mathcal{A} \equiv^k \mathcal{B}$$

if $\mathcal{A}$ and $\mathcal{B}$ are not distinguished by any sentence of L^k.

By extension, also write

$$(\mathcal{A}, \mathbf{a}) \equiv^k (\mathcal{B}, \mathbf{b})$$

to mean that for any formula φ of L^k,

$$\mathcal{A} \models \varphi[\mathbf{a}] \text{ if, and only if, } \mathcal{B} \models \varphi[\mathbf{b}]$$

For every formula φ of LFP, there is a k such that the query defined by φ is closed under $\equiv^k$.

Pebble games

Played on two structures $\mathcal{A}$ and $\mathcal{B}$

k pairs of pebbles $\{(a_1, b_1), \ldots, (a_k, b_k)\}$

Spoiler moves by picking a pebble and placing it on an element.

Duplicator responds by picking the matching pebble and placing it on an element of the other structure

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

If Duplicator has a strategy to play forever, then $\mathcal{A} \equiv^{\|} \mathcal{B}$

(Barwise 1977)

Reduced structure

The LFP definable queries are those computable in polynomial time on a reduced structure with universe $A^k/\equiv^k$.

Similarly, the logic $\Sigma_1^{1,\omega}$ defines the NP computable properties on these structures.

Crucial to a proof is the fact that the equivalence relation $\equiv^k$ and an ordering of the equivalence classes are both definable in LFP.

LFP $= \Sigma_1^{1,\omega}$ if, and only if, P=NP.

(D., 1998)

Transition Systems

Fixing a set P of atomic propositions, and a set A of actions

A transition system is

$$M = (S, A^M, P^M)$$

- S is a set of *states*;
- For each $a \in A$, $a^M \subseteq S \times S$ is a *binary relation*.
- For each $p \in P$, $p^M \subseteq S$ is a *unary relation*.

Bisimulation

For two systems

$$M = (S_1, A^M, P^M)$$
$$N = (S_2, A^N, P^N)$$

and $s \in S_1$ and $t \in S_2$

write,

$$(M, s) \sim (N, t)$$

if, there is a relation $B \subseteq S_1 \times S_2$ such that:

- if $B(u, v)$ then $p_i^M(u) \Leftrightarrow p_i^N(v)$;
- if $B(u, v)$, and $a_i^M(u, w)$ then there is a r such that $a_i^N(v, r)$ and $B(w, r)$;
- if $B(u, v)$, and $a_i^N(v, w)$ then there is a r such that $a_i^M(u, r)$ and $B(r, w)$; and
- $B(w, v)$.

Modal Logic

Hennessy-Milner logic:

The formulas of the logic are given by:

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

For any $s \in S$

- $(M, s) \models p$ if $p \in \mathcal{P}(s)$.
- $(M, s) \models \langle a\rangle\varphi$ if for some t with $(s, t) \in a^M$, $(M, t) \models \varphi$.
- $(M, s) \models [a]\varphi$ if for every t with $(s, t) \in a^M$, $(M, t) \models \varphi$.
- Boolean connectives as usual.

μ-calculus

The μ-calculus L_μ is an extension of modal logic.

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

Formulas of μ-calculus:

- all the rules of modal logic
- X
- $\mu_X \varphi$; $\nu_X \varphi$ — when X occurs only positively in φ.

$(M, \bar{X}^M, s) \models \mu_X \varphi$ if

s is in the least set X such that $X \leftrightarrow \varphi$ in $M, \bar{X}$

μ-calculus and LFP

Every formula of the μ-calculus can be expressed in LFP.

> Every property expressible in the μ-calculus is decidable in polynomial time.

Every formula of LFP can be translated (modulo first-order parameters) to one of the μ-calculus over a suitable *cartesian power* of structures $\mathcal{M} = (M, R)$

$$\mathcal{M}^k = (M^k, A^M, R)$$

where,

> $a_i(\mathbf{x}, \mathbf{y})$ if, and only if, $\mathbf{x}$ and $\mathbf{y}$ differ only in the ith component.
>
> R_i is as in $\mathcal{M}$, padded out if necessary.

Bisimulation Invariance

Every property definable in μ-calculus is bisimulation invariant and polynomial time computable.

Higher dimensional μ-calculus:

modal logic + fixed points of arbitrary arities

expresses exactly the properties which are bisimulation invariant and polynomial time computable.

(Otto)

Monadic Second-Order Logic

Monadic Second-Order Logic (MSO) is the extension of first-order logic by quantification over sets.

Every formula of the μ-calculus is equivalent to one of MSO.

> A property is expressible in the μ-calculus if, and only if, it is definable in MSO and it is bisimulation-invariant.

(Janin-Walukiewicz)

Is this true when restricted to finite structures?

Are there NP-complete bisimulation-invariant problems that are definable in MSO?

Conclusions

Descriptive complexity has provided logical characterisations of computational complexity classes

The success of these in providing logical techniques to answer hard questions in complexity has been limited.

At the same time, the characterisations provide an insight into the expressive power of logical constructs

The expressive power can be analysed using the interplay of complexity and invariance conditions.