Formulas, Games, and Circuits

Anuj Dawar

Computer Laboratory
University of Cambridge

Athens
June 2000

Formulas

Vocabulary σ – consisting of relation and constant symbols.

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 – $\exists x \varphi$, $\forall x \varphi$

Other extensions

operators – *e.g.* fixed-point operators $\mathbf{lfp}_{R,\mathbf{x}}\varphi$.

second order quantifiers $\exists R \varphi$.

infinitary connectives $\bigvee\{\varphi \mid \varphi \in S\}$.

Finite Structures

In general, finite relational structures

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

where A is a finite set.

A structure in the vocabulary (E) of one binary relation is a finite (directed) graph (V, E).

The models of the first order sentence

$$\forall x \neg Exx \wedge \forall x \forall y (Exy \rightarrow Eyx)$$

are the (loop-free, undirected) graphs.

Binary Strings

In the vocabulary

$$(<, B),$$

with one binary relation $<$ and one unary relation B,

the class of structures in which $<$ is a linear order of the universe is the class of *binary strings*.

$$\exists x(\forall y(x \leq y) \wedge \neg B(x))$$

The collection of binary strings in which the least significant digit is 0.

Expressive Power

The expressive power of first order logic on finite structures is weak.

For any first order sentence φ,

$$\mathsf{Mod}_{\mathcal{F}}(\varphi) \in \mathsf{DSPACE}(\log n)$$

Second Order Logic

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

A structure $\mathcal{A}$ satisfies $\exists P \varphi$ if there is a relation R on the universe of $\mathcal{A}$ such that $(\mathcal{A}, R)$ satisfies φ.

Σ_1^1 – existential second order logic

Theorem (Fagin) $\Sigma_1^1 = \mathsf{NP}$

Fixed Point Logic

Let $\varphi(R, x_1, \ldots, x_k)$ be a first order formula over the signature $\sigma \cup \{R\}$

Associated operator Φ:

$$\Phi(R^{\mathcal{A}}) = \{(a_1, \ldots a_k) \mid (\mathcal{A}, R^{\mathcal{A}}) \models \varphi(R, x_1, \ldots, x_k)\}$$

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 is the logic obtained by adding an operation to first order logic 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, $\textbf{lfp}_{R,xy}\varphi(u, v)$ is a formula in two free variables that expresses the transitive closure of E.

$\forall u \forall v \textbf{lfp}_{R,xy}\varphi(u, v)$ expresses connectivity

Consider only structures with a distinguished relation $<$ which is always a linear order of the universe.

Theorem (Immerman, Vardi)
On ordered structures LFP $=$ P

LFP $=$ P on the class of binary strings.

LFP is weaker than P on the class of graphs.

Elementary Equivalence I

For two structures $\mathcal{A}$ and $\mathcal{B}$, we say

$$\mathcal{A} \equiv_p \mathcal{B}$$

if for any sentence φ with $qr(\varphi) \leq p$,

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

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.

Elementary Equivalence II

For two structures $\mathcal{A}$ and $\mathcal{B}$, we say

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

if for any sentence φ with no more than k variables,

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

For a class of structures S, definable by an LFP sentence, there is a k such that S is closed under $\equiv^k$

Games

Game played by two players—Spoiler and Duplicator

Two structures $\mathcal{A}$ and $\mathcal{B}$

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

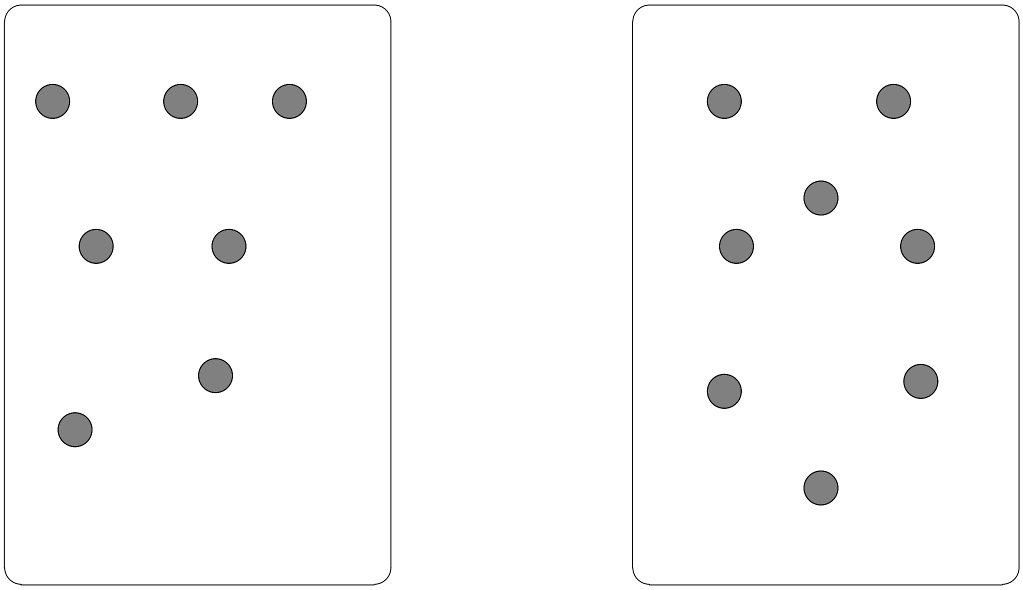
Spoiler moves by picking a pebble and placing it on an element.

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 winning strategy for p moves of the k pebble game on structures $\mathcal{A}$ and $\mathcal{B}$, then $\mathcal{A}$ and $\mathcal{B}$ agree on all first-order sentences of quantifier rank up to n with at most k distinct variables.

Example 1

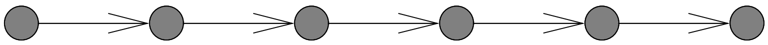


p $\qquad\qquad$ $p+1$

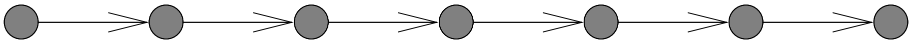
The two structures are equivalent with respect to $\equiv_p$

Thus, Evenness is not first order definable.

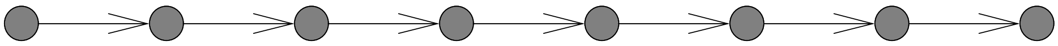
Example 2



L_6



L_7



L_8

$$L_6 \not\equiv_3 L_7$$

$$L_7 \equiv_3 L_8$$

In general, for $m, n \geq 2^p - 1$,

$$L_m \equiv_p L_n$$

Circuits

A circuit (*with inputs* $x_1, \ldots, x_n$)

is a directed acyclic graph whose source nodes are labelled

$$x_i \quad \text{or} \quad \neg x_i,$$

all other nodes are labelled

$$\vee \quad \text{or} \quad \wedge,$$

and there is one distinguished *output* sink node.

A circuit defines a Boolean function on the variables $x_1, \ldots, x_n$.

Circuit Families

Any set

$$S \subseteq \{0,1\}^*$$

is recognized by some circuit family $\mathcal{C}$, where

$\mathcal{C}$ is a function such that

$\mathcal{C}(n)$ is a circuit on n inputs.

Measures of Complexity

Depth: *the longest path in the circuit* as a function of n

Size: *the number of gates in the circuit* as a function of n

Uniformity: *the complexity of $\mathcal{C}$*

Complexity Classes

AC^0 — The sets accepted by a family of circuits of polynomial size and bounded depth.

$P/$poly — The sets accepted by a family of circuits of polynomial size and polynomial depth.

Note that even AC^0 contains undecidable sets, as there is no uniformity condition.

However, *parity*—the set of strings with an even number of 1's— is not in AC^0.

For $\mathcal{D}$ among LOGTIME, LOGSPACE, PTIME:

$\mathcal{D}$-uniform $P/$poly is the complexity class PTIME

φ – a first order sentence of vocabulary $\tau = (R_1, \ldots, R_s)$.

$\mathcal{A}$ – a finite relational structure of vocabulary τ with universe $\{1, \ldots, n\}$.

The condition $\mathcal{A} \models \varphi$ can be expressed as a propositional formula φ'.

Propositions:

$$R(a_1, \ldots, a_l) \qquad a_1, \ldots, a_l \in \{1, \ldots, n\}.$$

Translate the structure of φ inductively:

$\exists x \psi$

$$\bigvee_{i \in \{1,\ldots,n\}} \psi'[i]$$

$\forall x \psi$

$$\bigwedge_{i \in \{1,\ldots,n\}} \psi'[i]$$

The propositional formula depends only on φ and n, not on $\mathcal{A}$.

This propositional formula can be represented as a circuit.

Inputs to the circuit are

$$R_i(a_1, \ldots, a_l)$$

and

$$\neg R_i(a_1, \ldots, a_l)$$

Gates are *unbounded* fan-in AND and OR gates.

For each n, there is a circuit that works on all structures of that size.

Corresponding to each first order formula φ, there is a function $\mathcal{C}$ such that:

> $\mathcal{C}(n)$ is a circuit which takes on its inputs the bit string encoding of a τ-structure with n elements

The output of $\mathcal{C}(n)$ is 1 on input $\mathcal{A}$ if, and only if,

$$\mathcal{A} \models \varphi.$$

$\mathcal{C}(n)$ has depth $O(p)$, where p is the quantifier rank of φ.

$\mathcal{C}(n)$ has size bounded by $O(p \cdot n^k)$, where k is the number of variables in φ.

$\mathcal{C}$ is of very low complexity.

First order definable sets are in *uniform* AC^0.

Numerical Predicates

Let P be a global predicate on numbers alone:

$$P(n) \subseteq \{1, \ldots, n\}^l.$$

For instance:

$<$ – a binary global relation.

$+$ – a ternary global relation.

Such a relation is a *numerical predicate*.

For a $\tau \cup \{P\}$ formula φ and a τ structure $\mathcal{A}$ with universe $\{1, \ldots, n\}$, we say:

$$\mathcal{A} \models \varphi$$

if

$$(\mathcal{A}, P(n)) \models \varphi$$

Adding numerical predicates increases expressive power:

$$\exists x[\forall y(y \leq x) \wedge \exists z(z + z = x)].$$

In general, for any complexity class $\mathcal{D}$ satisfying some closure properties,

$\mathcal{D}$-uniform AC^0 is the same as $\mathsf{FO}(N_{\mathcal{D}})$

(Gurevich, Lewis; Barrington).

$\mathsf{FO}(N_{\mathcal{D}})$ is the class of properties expressible in first order logic with all numerical predicates in $\mathcal{D}$.

Uniform AC^0

LOGTIME-uniform AC^0 can be characterised as any of the following:

- $FO(<, \textbf{bit})$ (Immerman)
- $FO(<, +, \times, \textbf{exp})$ (Folklore)
- $FO(<, +, \times)$ (adapt from Bennett)
- $FO(+, \times)$ $\exists z(x + z = y)$
- $FO(\textbf{bit})$ (D., Doets, Lindell and Weinstein)

But, $FO(+)$ is weaker. (adapt from Presburger)

$\textbf{bit}(i, j) \leftrightarrow j = 1 \bmod 2^i$

An LFP formula φ, on structures with n elements translates into a first order formula φ_n.

There is a polynomial p such that

$$\mathsf{qr}(\varphi_n) \leq p(n).$$

There is a constant k such that

$$\mathsf{var}(\varphi_n) \leq k$$

This gives a circuit

of depth $\leq p(n)$

of width $\leq n^k$

and hence, size $\leq p(n) \cdot n^k$

Polynomial Time

PTIME can be characterised as any of the following:

- LFP$(<)$ (Immerman; Vardi)
- LFP$(<, \mathbf{bit})$
- LFP$(+)$
- LFP$(<, +, \times)$
- LFP$(+, \times)$
- LFP$(\mathbf{bit})$

Open Questions

On the class of structures

$$(n, +, \times)$$

is there a formula of LFP that is not equivalent to a first order formula?

In the language of finite ordered graphs $(E, <)$, is there for every k, a first order sentence that is not equivalent to one with just k variables?