

Model Theory on Finite Structures*

Anuj Dawar

Department of Computer Science

University of Wales Swansea

Swansea, SA2 8PP, U.K.

e-mail: `a.dawar@swansea.ac.uk`

1 Introduction

In mathematical logic, the notions of mathematical structure, language and proof themselves become the subject of mathematical investigation, and are treated as first class mathematical objects in their own right. Model theory is the branch of mathematical logic that is particularly concerned with the relationship between structure and language. It seeks to establish the limits of the expressive power of our formal language (usually the first order predicate calculus) by investigating what can or cannot be expressed in the language. The kinds of questions that are asked are:

What properties can or cannot be formulated in first order logic?

What structures or relations can or cannot be defined in first order logic?

How does the expressive power of different logical languages compare?

Model Theory arose in the context of classical logic, which was concerned with resolving the paradoxes of infinity and elucidating the nature of the infinite. The main constructions of model theory yield infinite structures and the methods and results assume that structures are, in general, infinite. As we shall see later, many, if not most, of these methods fail when we confine ourselves to finite structures. Many questions that arise in computer science can be seen as being model theoretic in nature, in that they investigate the relationship between a formal language and a structure. However, most structures of interest in computer science are finite. The interest in *finite* model theory grew out of questions in theoretical computer science (particularly, database theory and complexity theory).

*Notes for lecture presented at the Finite Model Theory Tutorial, Swansea, July 1996.

Before we proceed further, let us formalise our notions of structure and language. A signature (or vocabulary) σ is a finite sequence of relation and constant symbols:

$$\sigma = (R_1, \dots, R_m, c_1, \dots, c_n)$$

where, associated with each relation symbol R_i is an arity a_i . A structure \mathcal{A} over the signature σ is a tuple:

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

where

- A is a set, the *universe* of the structure \mathcal{A} ;
- each $R_i^{\mathcal{A}}$ is a relation over this set of arity a_i , i.e. $R_i^{\mathcal{A}} \subseteq A^{a_i}$; and
- each $c_i^{\mathcal{A}}$ is an element of A .

Note, in particular, that we do not have function symbols in our vocabularies. The formal languages most commonly studied in model theory is some variant of first order predicate logic, with which I will assume the reader is familiar. For the purpose of this lecture, it is the only logic we will consider. Thus, in the following, formula always means first order formula, and a sentence is a formula without free variables. The crucial link between structure and formula is the satisfaction relation. A structure that satisfies a sentence is said to be a model of that sentence.

Example 1 Consider the signature (E) , where E is a binary relation symbol. Finite structures (V, E) of this signature are directed graphs, i.e. E is a binary relation on V .

Moreover, the class of such finite structures satisfying the sentence

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

is the class of (loop-free, undirected) graphs.

Note, as in the above example, we do not distinguish between a relation symbol and the relation interpreting it in a structure, when this causes no confusion.

2 From Infinite to Finite Structures

As remarked above, if we confine ourselves to finite structures, many of the results and methods of model theory fail. By “confine ourselves”, I mean that we constrain the definition of structure given above so that the universe A must be a finite set. As an example, consider the compactness theorem. This is arguably the most fundamental theorem of model theory, as it is the foundation on which the rest of the subject is built.

Theorem 2 (Compactness) *If Σ is a set of sentences such that every finite subset of Σ has a model, then Σ has a model.*

If we understand “model” to mean “finite model”, then this statement is false. As a counterexample, consider the sentences:

$$\lambda_n = \exists x_1 \dots \exists x_n \bigwedge_{1 \leq i < j \leq n} (x_i \neq x_j).$$

That is, λ_n is true in exactly those structures in which there are at least n distinct elements.

Thus, the set of sentences

$$\Lambda = \{\lambda_n \mid n \in \omega\}$$

has the following properties:

- every finite subset Δ of Λ has a finite model. In fact, it is true in any structure with more than m elements, where $m = \max\{n \mid \lambda_n \in \Delta\}$.
- Λ does not have a finite model.

Another crucial foundational theorem in classical logic is the completeness theorem. This theorem links the semantic notion of truth with the syntactic notion of provability. Recall the following definition:

Definition 3 *A sentence is valid if, and only if, it is true in all structures.*

The completeness theorem tells us that validity has a purely syntactic characterisation in an appropriate proof system. Seen abstractly, i.e. shorn of any reference to a particular proof system, the theorem says:

Theorem 4 (Completeness) *The set of valid sentences is recursively enumerable.*

If Val is the set of valid sentences, then its “dual” set, in some sense is Sat —the set of satisfiable sentences, i.e. those sentences that have a model. Clearly, Sat is the set of negations of those sentences that are in Val . Since these sets are essentially complements of each other, and since Val is r.e. but not decidable, it follows that Sat is co-r.e. but not r.e.

The situation is rather different when we confine ourselves to finite structures. That is, we define Val_F to be the set of all sentences true in all finite structures, and we define Sat_F to be the set of those sentences that have a finite model. In this case, it is quite clear that Sat_F is r.e. Indeed, a semi-decision procedure for Sat_F is obtained by enumerating, for any sentence φ , all finite structures until we find one that satisfies φ . Thus, a proof that Sat_F is not decidable immediately yields the result that Val_F is not r.e. Such a result was established by Trakhtenbrot:

Theorem 5 (Trakhtenbrot) *Sat_F is not decidable.*

Proof (sketch): The proof proceeds by a reduction from the Halting problem for Turing machines. Given such a machine M , we construct a first order sentence φ_M such that

$$\mathcal{A} \models \varphi_M$$

if, and only if,

- there is a discrete linear order on the universe of \mathcal{A} with minimal and maximal elements;
- each element of \mathcal{A} (along with appropriate relations) encodes a configuration of the machine M ;
- the minimal element encodes the starting configuration of M on empty input;
- for each element a of \mathcal{A} the configuration encoded by its successor is the configuration obtained by M in one step starting from the configuration in a ; and
- the configuration encoded by the maximal element of \mathcal{A} is a halting configuration.

■

For pointers to a detailed proof, see the bibliographic notes below.

The proof of Theorem 5 contains the germ of the idea which came to dominate research in finite model theory: the encoding of computations into formulas. The very same construction is at the heart of many results relating computational complexity to definability in various logics.

Besides the compactness and completeness theorems, a large number of other basic results of model theory have been shown to fail on finite structures. Among them are:

- the Beth Definability Theorem;
- the Craig Interpolation Theorem;
- various preservation theorems;
- the Löwenheim-Skolem Theorem.

To a large extent, classical model theory can be described as the study of the structure of the elementary equivalence relation. Two structures \mathcal{A} and \mathcal{B} are said to be elementarily equivalent, denoted $\mathcal{A} \equiv \mathcal{B}$, if for every sentence φ ,

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

This is crucial to establishing inexpressibility results. For instance, by proving that all dense linear orders without endpoints are elementarily equivalent, we show that other properties that might distinguish two such orders (such as cardinality) are not definable.

On finite structures, the elementary equivalence relation is trivial, in that any two elementarily equivalent structures are isomorphic:

$$\mathcal{A} \equiv \mathcal{B} \text{ if, and only if, } \mathcal{A} \cong \mathcal{B}$$

Indeed, any finite structure is completely described up to isomorphism by a single sentence. Given a structure $\mathcal{A} = (A, R_1, \dots, R_m)$, where A is a set of n elements, we construct a sentence

$$\varphi_{\mathcal{A}} = \exists x_1 \dots \exists x_n (\psi \wedge \forall y \bigvee_{1 \leq i \leq n} y = x_i)$$

where, $\psi(x_1, \dots, x_n)$ is the conjunction of all atomic and negated atomic formulas that hold in \mathcal{A} .

This means that first order logic can make all the distinctions that are to be made between finite structures. Still, the expressive power of first order logic on finite structures is weak. For any first order sentence φ , $\text{Mod}(\varphi) \in \text{DSPACE}(\log n)$, where $\text{Mod}(\varphi)$ is the set of all finite models of φ . What accounts for this disparity? Essentially, classical model theory is concerned with the expressive power of *theories*, i.e. (possibly infinite) sets of sentences. Two structures that are elementarily equivalent cannot be distinguished by any first order theory. In contrast, any isomorphism closed class of finite structures S can be defined by a theory:

$$\{\neg \varphi_{\mathcal{A}} \mid \mathcal{A} \notin S\}.$$

To establish inexpressibility results for first order *sentences*, we need to weaken the relation of elementary equivalence.

3 Ehrenfeucht-Fraïssé Games

One way to stratify the relation of elementary equivalence is by quantifier rank. The quantifier rank of a formula is the depth of nesting of quantifiers within it. It is formally defined by induction as follows:

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

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

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

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

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

The crucial observation about the relation \equiv_p that we use is:

Proposition 6 *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 one direction, it is clear that if $S = \text{Mod}(\varphi)$ for some φ , then S is closed under the relation \equiv_p , where $p = qr(\varphi)$. In fact, this is the only direction of Proposition 6 we shall use. To establish the other direction, one has to note that there are, up to logical equivalence, only finitely many sentences of any fixed quantifier rank. Here, we make crucial use of the fact that there are no function symbols in our vocabulary. What makes the equivalence relations \equiv_p useful to consider is that they have an elegant characterisation in terms of two player games. In order to introduce these games, we first need a definition.

Definition 7 *A map f is a partial isomorphism between structures \mathcal{A} and \mathcal{B} , if:*

- *the domain $\text{dom}(f) \subseteq A$;*
- *the range $\text{rng}(f) \subseteq B$; and*
- *f is an isomorphism between the substructure of \mathcal{A} generated by its domain and the substructure of \mathcal{B} generated by its range.*

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 8 (Fraïssé; Ehrenfeucht) *Duplicator has a strategy for winning the p -round Ehrenfeucht game on \mathcal{A} and \mathcal{B} if, and only if, $\mathcal{A} \equiv_p \mathcal{B}$.*

In lieu of proof, let us consider an example. Suppose $\mathcal{A} \not\equiv_3 \mathcal{B}$. In particular, suppose $\theta(x, y, z)$ is a quantifier free formula, such that:

$$\mathcal{A} \models \exists x \forall y \exists z \theta$$

$$\mathcal{B} \models \forall x \exists y \forall z \neg \theta$$

round 1

Spoiler chooses $a_1 \in A$ such that

$$\mathcal{A} \models \forall y \exists z \theta[a_1]$$

Duplicator responds with $b_1 \in B$.

round 2

Spoiler chooses $b_2 \in B$ such that

$$\mathcal{B} \models \forall z \neg \theta[b_1, b_2]$$

Duplicator responds with $a_2 \in A$.

round 3

Spoiler chooses $a_3 \in A$ such that

$$\mathcal{A} \models \theta[a_1, a_2, a_3]$$

Duplicator responds with $b_3 \in B$.

Spoiler wins, since $\mathcal{B} \models \neg \theta[b_1, b_2, b_3]$.

It is easy enough to generalise the above example into a proof of one direction of Theorem 8: namely that on any pair of structures which are distinguished by a sentence of quantifier rank p , Spoiler has a strategy to win the p round game. Again, this is the only direction of the theorem that we will use, and we will usually state it as the contrapositive of the above: if Duplicator wins the p round game on \mathcal{A} and \mathcal{B} , then $\mathcal{A} \equiv_p \mathcal{B}$.

Example 9 Consider two structures S_p and S_{p+1} in the empty vocabulary (*i.e.* without relation or constant symbols), one with p elements, and the other with $p + 1$ elements (see Figure 1). It is easy to see that Duplicator wins the p round game. Since one of the structures has even size and the other has odd size, we conclude that the property of having even size is not definable in first order logic, as it is not closed under \equiv_p for any p .

Fix a signature ($<$) with one binary relation symbol. Let L_n denote the (unique up to isomorphism) structure in this signature that is a linear order of length n .

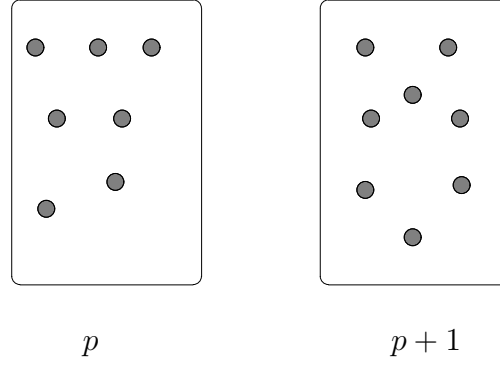


Figure 1: The structures S_p and S_{p+1}

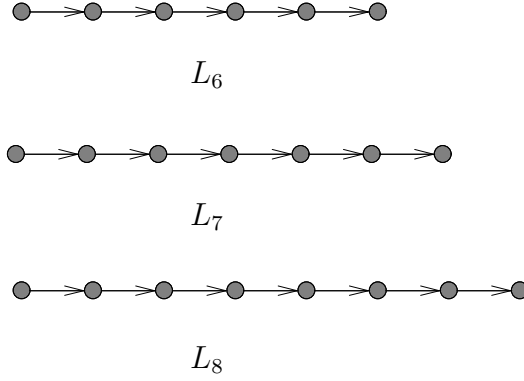


Figure 2: L_6 , L_7 and L_8

Example 10 Consider the structures L_6 , L_7 and L_8 , depicted in Figure 2. It is easily verified that Spoiler wins the 3-round game on L_6 and L_7 but Duplicator wins the 3-round game on L_7 and L_8 .

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

$$L_m \equiv_p L_n$$

Duplicator's strategy is to maintain the following condition after r rounds of the game:

for $1 \leq i < j \leq r$,

- either $\text{length}(a_i, a_j) = \text{length}(b_i, b_j)$
- or $\text{length}(a_i, a_j), \text{length}(b_i, b_j) \geq 2^{p-r} - 1$

We conclude that evenness is not first order definable, even on linear orders. Indeed, the above implies that the only first order definable sets of linear orders are the finite or co-finite ones.

Now, consider a signature with two binary relations $(E, <)$. We will consider structures $G = (V, E, <)$ over this signature which interpret the symbol $<$ as a linear order. These structures can be thought of as ordered (directed) graphs. We seek to prove that there is no sentence γ in this vocabulary such that:

$$G \models \gamma \text{ if, and only if, } (V, E) \text{ is connected.}$$

Let γ' be the formula obtained by replacing every occurrence of Exy in γ by the following formula

$$\pi(x, y) = y = x + 2 \vee (x = \max \wedge y = \min + 1) \vee (x = \min \wedge y = \max + 1).$$

In the above, the symbols “min”, “max”, “+1” and “+2” are to be interpreted with respect to the linear order in the obvious way. It can be easily checked that they can be replaced by appropriate definitions, so that π is a formula in the vocabulary $(E, <)$. The relation defined by π is essentially “add 2 (mod n)”.

Thus, γ' is a formula that uses only the vocabulary $(<)$, and is true in a structure L_n if the graph defined by π on L_n is connected. But, the graph defined by π is either a single cycle or two disjoint cycles, depending on whether n is odd or even (this is illustrated for $n = 6$ and $n = 7$ in Figure 3). Thus, γ' defines evenness on

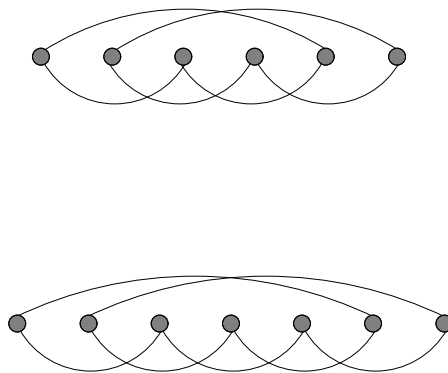


Figure 3: The graphs defined by $\pi(x, y)$.

linear orders, which we know is not possible.

We conclude that there is no sentence that defines connectivity on ordered graphs. Indeed, there is no sentence that defines connectivity on graphs, as any such sentence would also work on ordered graphs.

Note that what the above construction achieves is a reduction from the problem of evenness of linear orders to the problem of connectivity. Since we had already established that the former problem is not first order definable, and the reduction is given by a first order formula (in fact, by the formula π), we conclude that the latter problem is not definable either.

4 0–1 Law

In Section 2, we investigated the failure of methods from classical model theory when restricted to finite structures. Section 3 explored one method, the Ehrenfeucht-Fraïssé game, which does survive the transition to finiteness. In this section, we look at a direction that has emerged from the study of finite structures, and does not have a direct counterpart in the context of classical model theory. This is the study of asymptotic probabilities and 0–1 laws.

Let S be any isomorphism closed class of σ -structures. Let C_n be the set of all σ structures whose universe is $\{0, \dots, n-1\}$. We define $\mu_n(S)$ as:

$$\mu_n(S) = \frac{\text{card}(S \cap C_n)}{\text{card}(C_n)}$$

In other words, $\mu_n(S)$ is the proportion of structures of size n that are in S . It is only for the sake of concreteness that we restrict our universe to be $\{0, \dots, n-1\}$. The asymptotic probability, $\mu(S)$, of S is defined as

$$\mu(S) = \lim_{n \rightarrow \infty} \mu_n(S)$$

if this limit exists.

Asymptotic probabilities (particularly of graph properties) have been extensively studied in combinatorics. It turns out that for many interesting properties S , $\mu(S)$ is defined and is either 0 or 1. Thus, for example:

- $\mu(\text{connectivity}) = 1$
- $\mu(\text{3-colourability}) = 0$
- $\mu(\text{planarity}) = 0$
- $\mu(\text{Hamiltonicity}) = 1$
- $\mu(\text{rigidity}) = 1$
- $\mu(k\text{-clique}) = 1$ for fixed k .

In contrast, it is clear that:

- $\mu(\text{even number of nodes})$ is not defined
- $\mu(\text{even number of edges}) = 1/2$.

A very general result establishing limits on the expressive power of first order logic on finite structures is the following:

Theorem 11 (Glebskii *et al.*; Fagin) *For every sentence φ in a relational signature, $\mu(\text{Mod}(\varphi))$ is defined and is either 0 or 1.*

The rest of this section is devoted to a proof of Theorem 11.

Definition 12 *In a relational signature σ , an atomic type*

$$\tau(x_1, \dots, x_k)$$

is the conjunction of a maximally consistent set of atomic and negated atomic formulas.

In other words, τ is a complete description of a k -tuple with respect to the relations in σ . Note, that for a fixed k and σ , there are a some fixed number of atomic types. This number is exponential in k , provided σ contains at least one non-unary symbol. Let $\tau(x_1, \dots, x_k)$ and $\tau'(x_1, \dots, x_{k+1})$ be two atomic types such that τ' is consistent with τ . The τ, τ' -extension axiom, $\eta_{\tau, \tau'}$ is the sentence:

$$\forall x_1 \dots \forall x_k \exists x_{k+1} (\tau \rightarrow \tau').$$

That is, $\eta_{\tau, \tau'}$ asserts that every tuple of type τ can be extended to a tuple of type τ' .

The remarkable fact about extension axioms is that they are almost always true.

Proposition 13 *For any extension axiom $\eta_{\tau, \tau'}$,*

$$\mu(\text{Mod}(\eta_{\tau, \tau'})) = 1.$$

Proof (idea): The following presents the intuition behind the proof, omitting tedious combinatorial calculations:

Given a σ -structure \mathcal{A} of size n , and a k -tuple a in \mathcal{A} satisfying τ , there is a probability

$$\sim \frac{c_1}{2^n}$$

that there is no extension of a satisfying τ' , where c_1 is some constant (depending only on k and σ). This is because each of the $n - k$ elements not in the tuple a meets the requirements for τ' with some constant probability, independent of n .

There are roughly

$$\sim \frac{n^k}{c_2}$$

tuples in \mathcal{A} satisfying τ , for some constant c_2 . This is because there are n^k tuples in all, and some fixed number of types.

From the above two fact, we conclude that the expected number of counterexamples to $\eta_{\tau, \tau'}$ in \mathcal{A} is

$$\sim c \frac{n^k}{2^n}$$

for some constant c . (This ignores the fact that the events are not all independent, but the larger n gets, the closer we are to independence.)

Since the expected number of counterexamples to $\eta_{\tau, \tau'}$ in a structure \mathcal{A} goes to 0 as n grows, the probability that \mathcal{A} satisfies $\eta_{\tau, \tau'}$ goes to 1. ■

Next, we note that, if S_1 and S_2 are classes of structures such that $\mu(S_1) = \mu(S_2) = 1$, then

$$\mu(S_1 \cap S_2) = 1.$$

It follows that for any finite set Δ of extension axioms, $\mu(\text{Mod}(\Delta)) = 1$.

Let Γ be the set of all extension axioms for a fixed signature σ . Since, by the above, every finite subset of Γ has a model (in fact, almost all finite structures are models), it follows by the Compactness theorem that Γ has a model. The model of Γ is necessarily an infinite one.

We next see that Γ is a complete theory. That is, for every first order sentence φ

$$\text{Either } \Gamma \models \varphi \text{ or } \Gamma \models \neg\varphi.$$

Another way of saying the same thing is that any two models of Γ are elementarily equivalent. We prove this by noting that if $\mathcal{A} \models \Gamma$ and $\mathcal{B} \models \Gamma$, then, for every p ,

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

This is so by an application of the Ehrenfeucht-Fraïssé game. Indeed, the extension axioms seem to be designed for playing the game, since they assert that as long as we know the current configuration of a tuple, we can match *any* possible extension to that tuple.

Now, let φ be any first order sentence. By the completeness of Γ ,

1. either

$$\Gamma \models \varphi;$$

2. or

$$\Gamma \models \neg\varphi.$$

In the first case, by an application of the Compactness theorem, there is a finite set $\Delta \subseteq \Gamma$, such that:

$$\Delta \models \varphi.$$

Since $\mu(\text{Mod}(\Delta)) = 1$, it follows that $\mu(\text{Mod}(\varphi)) = 1$.

Similarly, in the second case, $\mu(\text{Mod}(\neg\varphi)) = 1$, and therefore $\mu(\text{Mod}(\varphi)) = 0$. We have thus established the 0–1 law.

Note the extensive use made of the compactness theorem in establishing a result solely about finite structures.

Bibliographic Notes

Trakhtenbrot's result originally appeared in [7]. For a textbook presentation of the proof, see [1]. For a discussion of the failure of model theoretic results on finite structures, including definability, interpolation and various preservation theorems, see [6].

The equivalence relations \equiv_p were characterised by Fraïssé [4] in terms of sequences of partial isomorphisms and by Ehrenfeucht [2] in terms of two player games. A full proof of both results can be found in [1]. The application of the game given here to finite linear orders is from [6].

The 0–1 law for first order logic was established independently by Glebskiĭ *et al.* [5] and Fagin [3]. The proof given above follows closely the proof of Fagin, bar the use of games.

References

- [1] H-D. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer, 1995.
- [2] A. Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fund. Math.*, 49:129–141, 1961.
- [3] R. Fagin. Probabilities on finite models. *Journal of Symbolic Logic*, 41(1):50–58, March 1976.
- [4] R. Fraïssé. Sur quelques classifications des systèmes de relations. *Publications Scientifiques de l'Université d'Algerie, Séries A*, 1:35–182, 1954.
- [5] Y. V. Glebskiĭ, D. I. Kogan, M.I. Ligon'kiĭ, and V. A. Talanov. Range and degree of realizability of formulas in the restricted predicate calculus. *Kibernetika*, 2:17–28, 1969.
- [6] Y. Gurevich. Toward logic tailored for computational complexity. In M. Richter et al., editors, *Computation and Proof Theory*, pages 175–216. Springer Lecture Notes in Mathematics, 1984.
- [7] B. A. Trakhtenbrot. Impossibility of an algorithm for the decision problem in finite classes. *Doklady Akademii Nauk SSSR*, 70:569–572, 1950.