Counting and Addition cannot express Deterministic Transitive Closure

Matthias Ruhl
MIT Laboratory for Computer Science
Cambridge, MA 02139, USA
ruhl@theory.lcs.mit.edu

Abstract

An important open question in complexity theory is whether the circuit complexity class TC^0 is (strictly) weaker than LOGSPACE. This paper considers this question from the viewpoint of descriptive complexity theory.

TC^0 can be characterized as the class of queries expressible by the logic $FOC(<,+,\times)$, which is first-order logic augmented by counting quantifiers on ordered structures that have addition and multiplication predicates. We show that in first-order logic with counting quantifiers and only an addition predicate it is not possible to express "deterministic transitive closure" on ordered structures. As this is a LOGSPACE-complete problem, this logic therefore fails to capture LOGSPACE. It also directly follows from our proof that in the presence of counting quantifiers, multiplication cannot be expressed in terms of addition and ordering alone.

1. Introduction

The interest in finite model theory from a complexity theory point of view is motivated by the fact that "descriptive complexity theory" allows to rephrase complexity theoretic questions in a purely logical framework [15, 16, 17]. This allows one to attack these questions from a new perspective and using different tools, such as Ehrenfeucht-Fraïssé-games.

In this paper, we study the expressive power of first-order logic augmented with counting quantifiers on ordered structures. Expressions in first-order logic are built from relational expressions $Rx_1x_2\ldots x_r$ and equalities $x_1 = x_2$ using the connectives $\wedge$, $\vee$, $\neg$, and the quantifiers $\exists$ and $\forall$. The limitations of the expressiveness of first-order logic are well-known (see, e.g., [5]), most notably that it lacks any ability to 'count'. It is not even possible to express the fact that a structure has even size.

Adding 'counting quantifiers' to the logic remedies this fact. Counting quantifiers are expressions of the form $\exists^{\geq y} x \varphi(x)$ and express that "there are at least y distinct elements x that satisfy $\varphi(x)$". There has been a great interest in recent years in the expressiveness of first-order logic augmented with counting quantifiers, which we will call FOC in this paper.

This is mostly due to the fact that this logic, in the presence of an ordering, and addition and multiplication predicates (we call this logic "$FOC(<,+,\times)$"), captures the circuit complexity class TC^0 [3], the class of uniform polynomial-size, constant depth, threshold circuits. It is an important open question whether TC^0 is weaker than *LOGSPACE*; even whether it is strictly weaker than *NP* is unknown [2].

To see whether a logic captures *LOGSPACE* it is sufficient to determine whether it can express "deterministic transitive closure". Deterministic transitive closure (DTC) is the problem where given a directed graph whose vertices all have out-degree at most 1, and two nodes s and t, one has to decide whether there is a path from s to t. DTC is *LOGSPACE*-complete under quantifier-free reductions [8].

The main result of the present paper is that first-order with counting quantifiers on ordered structures with an addition predicate (we call this logic "$FOC(<,+)$") and a binary relation E, i.e. on structures of the form

$$\mathcal{A} = (\{0,1,\ldots,N\},<,+,E),$$

cannot express the deterministic transitive closure of E, and thus fails to capture *LOGSPACE*.

We prove this main result by giving an explicit winning strategy for the second player in an Ehrenfeucht-Fraïssé-game.

From a descriptive complexity theory point of view, it shows that the multiplication predicate must be essential should $FOC(<,+,\times)$ in fact equal *LOGSPACE*. Moreover, from our proof we can also directly conclude the stronger result that $FOC(<,+) \neq FOC(<,+,\times)$ meaning that multiplication is essential to capturing TC^0, too. We thus obtain

$$FOC(<,+) \subsetneq FOC(<,+,\times) = TC^0 \overset{?}{\neq} LOGSPACE.$$

1.1. Related work

Most of the previous work on the expressibility of counting quantifiers considered two-sorted structures, which consist of a finite "vertex domain" (the 'actual' structure) and a (possibly infinite) number domain.

Infinite number domains with arbitrary operations, as introduced by Grädel and Gurevich in their 'meta-finite model theory' [11], were considered by Benedikt and Keisler [4], who proved separations for several variations of counting quantifiers on such structures.

In the work more closely related to this paper, finite structures of the form

$$\mathcal{A} = \Big(\{0,1,\dots,N\},\{v_0,v_1,\dots,v_N\},<,+,\times,R_1^{\mathcal{A}},\dots,R_r^{\mathcal{A}}\Big)$$

were considered. Here, the relations $R_i^{\mathcal{A}}$ apply only to the vertex domain $\{v_0,\dots,v_N\}$, and the ordering and arithmetic operations apply only to the number domain $\{0,1,\dots,N\}$. For a counting formula $\exists^{\geq y}x\ \varphi(x)$, x ranges over the vertex domain, while y ranges over the number domain.

By splitting the structure in this way, it is possible to consider structures that are *not* ordered. Etessami [8] showed that if one has only a successor relation S on the vertex domain, then first-order logic with counting, addition and multiplication cannot express the transitive closure of S, and therefore fails to capture $LOGSPACE$. The proof in the journal version of the paper relies on the fact that first-order logic with counting quantifiers can only express local properties, which follows from [22]. Libkin [18, 19, 20] also considered local properties of a variety of logics involving counting quantifiers.

Unfortunately, in the presence of a total ordering, these proof techniques do not apply anymore, since all elements of the structure are directly "connected" by the ordering.

The result of this paper may therefore be one of the very few non-trivial statements about the expressibility of first-order logic with counting quantifiers on ordered structures. By avoiding two-sorted structures, it also seems more natural than other results in this area.

To prove our main result, we give an explicit winning strategy for player II in an Ehrenfeucht-Fraïssé-game for the logic FOC. Winning strategies for Ehrenfeucht-Fraïssé-games for first order logic *without* counting quantifiers, but in the presence of an addition predicate, have been studied before. Most of them are related to techniques used by Presburger for the quantifier elimination of $Th(\mathbb{Z})$ [23]; a very readable exposition of such a strategy can be found in section 3.3 of [12]. Lynch [21] also gave a similar strategy when proving inexpressibility results for first-order logic on structures with an addition relation.

The main technical contribution of this paper is the extension of the strategy in the presence of counting quantifiers, corresponding to a 'set move' in the Ehrenfeucht-Fraïssé-game.

After completing this paper, we noticed a reference in [8] to an (as yet) unpublished manuscript of Lindell that seems to imply the result stated in this paper. Our result was derived independently, and might also be interesting in its own right due to its proof technique.

1.2. Outline of paper

This paper is structured as follows. In section 2, we present the notions and definitions from finite model theory used in this paper. In section 3 we state and prove our main theorem. In the last section 4 we summarize our results and discuss possible future research directions.

2. Logics and games

In this section we give the definitions necessary for the rest of the paper, in particular of the logic $FOC(<,+)$ which will be the main concern of this paper. We then describe the Ehrenfeucht-Fraïssé-game for this logic, a game-theoretic method to prove inexpressibility results. Our notation follows [5, 6].

2.1. Remarks on Notation

Our notation slightly deviates from the other literature on counting quantifiers. This is due to the fact that we consider only one-sorted structures. In the presence of a total ordering on the structure, a separate number domain does not give any additional expressibility[1], so for simplicity we avoid using it.

Usually the name $FO(\mathbf{C})$ is given to first-order logic with quantifiers on two-sorted structures with the BIT predicate on the "number domain". In order not to confuse the reader, we will call first-order order logic with counting on single-sorted domains FOC.

2.2. Structures

All structures we consider in this paper are finite with domains $\{0,1,\dots,N\}$ where $N\in\mathbb{N}$. If we consider σ-structures (where σ is the set $\{R_1,\dots,R_r\}$ of relations on the structure) and σ includes one or more of the relation symbols $<$, $+$ and $\times$, then these relations are always interpreted as the "natural" ordering, addition and multiplication relations, respectively, on the set $\{0,\dots,N\}$. Note that $+$ and $\times$ are always relations, not functions, in this paper.

[1] One can identify each number i with the unique 'vertex' element v_i that satisfies $\exists^{=i}y\ y<x$, and in this way use all relations of the number domain also on the vertex domain, and vice versa.

2.3. FOC

The logic FOC studied in the following is the extension of first order logic obtained by adding *counting quantifiers*. These quantifiers have the following form:

$\exists^{\geq y} x\varphi$ where x, y are variables and φ is a FOC-formula.

The variable x in $\exists^{\geq y} x\varphi$ is bound by the quantifier, while y is still free. The formula is satisfied by a structure $\mathcal{A} = (A, \overline{R})$ and a variable assignment β iff there are at least $\beta(y)$ distinct elements $a \in A$, such that $(\mathcal{A}, \beta\frac{a}{x}) \models \varphi$.

Definition 1 **(FOC, $FOC(<,+)$, $FOC(<,+,\times)$, ...)** *FOC is the logic obtained by adding counting quantifiers to first order logic. For all $\tau \subseteq \{+,\times,<\}$, $FOC(\tau)$ is FOC restricted to structures that have the relations from τ, interpreted in the 'natural' way.* □

Note that $FOC(+)$, $FOC(<)$ and $FOC(<,+)$ have the same expressive power, since an ordering can be defined in terms of an addition, and vice versa[2]:

$$\begin{aligned} a < b &\iff \exists x(a + x = b \wedge x + x \neq x), \\ a + b = c &\iff \exists^{=b} x(a < x \wedge x \leq c). \end{aligned}$$

2.4. Capturing complexity

Central to the relationship between finite model theory and complexity theory is the notion of a logic *capturing* a complexity class. Complexity classes are usually defined in terms of languages, but strings over a finite alphabet can easily be encoded as (ordered) relational structures. This means that strings and structures can be used interchangeably, which leads to the following definition.

Definition 2 (Capturing a complexity class) *A logic L is said to* capture *a complexity class C iff for every class K of σ-structures in C there is a sentence $\varphi \in L$ (and vice versa), such that for all σ-structures $\mathcal{A}$ the following holds:*

$$\mathcal{A} \in K \iff \mathcal{A} \models \varphi$$

($\mathcal{A}$ is in K iff $\mathcal{A}$ satisfies the sentence φ). □

Following Fagin's 1974 result [9] that the logic Σ_1^1 (existential second order logic) captures *NP*, logical characterizations have been found for many other complexity classes such as *P* [13, 24], *PSPACE* [1], and *LOGSPACE* [14]. For the latter characterizations the structures have to be ordered, as otherwise the logics fail to express even simple statements such as 'the structure has an even size'. It is an open problem whether there exist logical characterizations of these classes that also hold for structures without an ordering.

As mentioned in the introduction, Barrington et al. showed the following theorem in [3].

Theorem 1 (Barrington, Immerman, Straubing) *$FOC(<,+,\times)$ captures TC^0.* □

To be precise, instead of $+$ and $\times$, Barrington et al. use a predicate called BIT, where $BIT(i, j)$ is true iff the i-th bit in the binary representation of j is 1. But BIT and $\{+,\times\}$ have the same expressive power when added to first-order logic with counting quantifiers (for a proof see, e.g, section 1.2.1 in [17]).

2.5. Ehrenfeucht-Fraïssé Games

Ehrenfeucht-Fraïssé games (EF-games) are a game-theoretic method to prove inexpressibility results for logics. They were invented by Ehrenfeucht [7] based on work by Fraïsse [10]. We will give a short introduction to EF-games, and refer the reader to [5] for a more thorough coverage. Whenever we use the term "EF-game" in this paper, we mean an EF-game for the logic FOC.

An EF-game proceeds as follows. Given are two structures $\mathcal{A}$ and $\mathcal{B}$ (with domains A and B, respectively) of the same signature and a number $M \geq 1$. The game consists of M moves, where two players I and II (also called "spoiler" and "duplicator", respectively) choose elements $(a_i)_{i=1,\ldots,M}$ from $\mathcal{A}$ and elements $(b_i)_{i=1,\ldots,M}$ from $\mathcal{B}$, according to the following rules.

Every move starts by player I deciding whether to make a *point move* or a *set move*. Then the following happens (assume this is the m^{th} move and $a_1, b_1, \ldots, a_{m-1}, b_{m-1}$ have already been chosen).

Point Move:

1. Player I chooses a structure ($\mathcal{A}$ or $\mathcal{B}$). If I chooses $\mathcal{A}$, I picks an element a_m from that structure, otherwise, I picks an element b_m from $\mathcal{B}$.

2. Player II then selects an element from the other structure, so if I chooses $\mathcal{A}$, II picks an element b_m from $\mathcal{B}$, and if I chose $\mathcal{B}$, II picks an element a_m from $\mathcal{A}$.

Set Move:

1. Player I chooses a structure ($\mathcal{A}$ or $\mathcal{B}$) – for the following we assume I chose $\mathcal{A}$ (otherwise exchange the roles of $\mathcal{A}$ and $\mathcal{B}$). Player I then picks an $i < m$ and a set $A_0 \subseteq A$ with $|A_0| = a_i$.

2. Player II picks a subset $B_0 \subseteq B$ with $|B_0| = b_i$.

[2] Here $\exists^{=b} x\varphi$ is used as shorthand for $\exists^{\geq b} x\varphi \wedge \forall y(\exists^{\geq y} x\varphi \rightarrow y \leq b)$. We also write $x + y = z$ instead of $+xyz$.

3. Player I chooses an element b_m from B_0.

4. Player II selects an element a_m from A_0.

Note that if we have $a_i = b_i = 1$ for some i, then the point move is just a special case of the set move. We nevertheless make the distinction, since it helps structure our reasoning later on; we can first consider the 'simple' point move, and then extend our results to the more complex set move.

Player II wins a M-Move EF-game iff after M moves the mapping $(a_1, a_2, \ldots, a_M) \mapsto (b_1, b_2, \ldots, b_M)$ is a partial isomorphism from $\mathcal{A}$ to $\mathcal{B}$, i.e. it preserves equality and the relations on the two structures. Otherwise, player I wins.

Obviously, if $\mathcal{A}$ and $\mathcal{B}$ are isomorphic, player II can always win by mirroring the moves of player I in the other structure. But more generally the following theorem holds – a variant of the theorem due to Ehrenfeucht for first-order logic. A proof can be found in [8].

Theorem 2
The following two statements are equivalent:

(i) Player II has a winning strategy for the M-move EF-game on two structures $\mathcal{A}$ and $\mathcal{B}$.

(ii) $\mathcal{A}$ and $\mathcal{B}$ satisfy the same FOC formulas of quantifier rank $\leq M$. $\square$

For inexpressibility results we use the following corollary of Theorem 2:

Corollary 3
Let K and L be classes of finite structures, such that there exist sequences $(\mathcal{A}_i)_{i\in\mathbb{N}}$ in K and $(\mathcal{B}_i)_{i\in\mathbb{N}}$ in L, where for every $M \geq 1$ player II has a winning strategy for the M-move EF-game on $\mathcal{A}_M$ and $\mathcal{B}_M$.

Then K and L cannot be distinguished by a FOC-formula. $\square$

3. Main Theorem

"Deterministic transitive closure" is the following question: Given a directed graph $G = (V, E)$, where every node has out-degree at most 1, and two nodes $s, t \in V$; is there a path in G from s to t? This problem is obviously in $LOGSPACE$. Our main theorem, which we prove in this section, is the following.

Theorem 4
Deterministic transitive closure (DTC) cannot be expressed in $FOC(<, +)$.

It then immediately follows that

Corollary 5
$FOC(<, +)$ does not capture $LOGSPACE$. $\square$

3.1. Proof of main theorem

For each natural number M we construct two structures $\mathcal{A}_M = (\{0, \ldots, N_M\}, <, +, E^{\mathcal{A}_M})$ and $\mathcal{B}_M = (\{0, \ldots, N_M\}, <, +, E^{\mathcal{B}_M})$, where E is a binary relation that represents a directed graph where every vertex has an out-degree of at most 1. We will have that

(i) 0 and N_M are connected via an $E^{\mathcal{A}_M}$-path

(ii) 0 and N_M are *not* connected via an $E^{\mathcal{B}_M}$-path

(iii) Player II has a winning strategy for the M-move Ehrenfeucht-Fraïssé Game on $\mathcal{A}_M$ and $\mathcal{B}_M$.

Since the first and last element of the ordering, 0 and N_M, are FO-definable in ordered structures, Corollary 3 then immediately implies that DTC cannot be expressed in $FOC(<, +)$.

So let $M \geq 1$ be fixed for the rest of this proof, and we just write $\mathcal{A}$, $\mathcal{B}$, N instead of $\mathcal{A}_M$, $\mathcal{B}_M$, N_M.

3.2. Construction of $\mathcal{A}$ and $\mathcal{B}$

To define the size of the structures $\mathcal{A}$ and $\mathcal{B}$, we use a function $r : \{4, \ldots, M+4\} \to \mathbb{N}$ that will also play a role later in the proof. During the proof we will repeatedly make use of the fact that $r(m)$ is 'much larger' than $r(m+1)$ for all $m \in \{4, \ldots, M+3\}$. In fact, the exact definition of r does not matter much, as long as it satisfies all size constraints imposed by the proof. When reading the proof, it is therefore helpful to ignore the exact definition of r, and just convince oneself that all constraints in the proof can be satisfied simultaneously.

The function r is recursively defined as follows:

- $r(M+4) := 1$
- $r(m) := \left((6r(m+1))^{12m} \cdot \alpha \right)^{\alpha}$,
  where $\alpha = \mathrm{lcm}(1, 2, \ldots, r(m+1)) + 2$.

Set $R := 3r(4)^3 \cdot r(4)!$ and fix the size of our structures as $N := (4R+1)R$.

We define the edge relations as follows:

$$
\begin{aligned}
E^{\mathcal{A}} &:= \{(a, b) \mid a + R = b\} \\
E^{\mathcal{B}} &:= \{(a, b) \mid a + 2R = b\}
\end{aligned}
$$

Obviously 0 and N are connected via an $E^{\mathcal{A}}$-path (since N is a multiple of R) but not via an $E^{\mathcal{B}}$-path (since N is not a multiple of $2R$).

3.3. Strategy

We have to show that these two structures cannot be distinguished using an M-move Ehrenfeucht-Fraïssé-game. To this end we state a strategy for player II that ensures that all mappings $(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)$ occurring during the game will be partial isomorphisms.

The crucial strategy element for player II is to make certain that all partial isomorphisms $(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)$ occurring during the game can be extended to linear combinations $\sum\alpha_i a_i\mapsto\sum\alpha_i b_i$ with "simple" coefficients α_i. If this were not the case, player I could quickly establish that the two structures are not isomorphic.

For example, if we have $a_2=5\cdot a_1$ in one structure, but $b_2\neq 5\cdot b_1$ in the other structure, then player I could play $2\cdot a_1, 3\cdot a_1, 5\cdot a_1$ in $\mathcal{A}$, and player II would be forced to respond with $2\cdot b_1$, $3\cdot b_1$, $5\cdot b_1$ since the new elements can be expressed as sums of already chosen elements. Apparently player II would lose in this case.

More precisely, the linear combinations player II must preserve have the following form.

Definition 3 ($L_d(\overline{a})$)

$$L_d(a_1,\ldots,a_m):=\left\{\sum_{i=1}^m\frac{p_i}{q_i}\cdot a_i\in\mathbb{Z}\;\middle|\;p_i,q_i\in\mathbb{Z},\,|p_i|,|q_i|\le d,\,q_i\neq 0\right\}\;\Box$$

We can now define sets W_m ($4\le m\le M+4$) that are winning situations for player II. The function r used in the definition is the one we used above to define the size N of our structures. Note that r decreases rapidly; intuitively, at the beginning of the game, player II has to preserve a large number of linear equations to account for all possible strategies player I might take, while as the game progresses, player II has to preserve fewer and fewer linear combinations.

Definition 4 (W_m)

$$\begin{aligned}W_m:=\Big\{\;&(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)\;\Big|\\&(a_1,a_2,a_3,a_4)=(0,1,R,N),\\&(b_1,b_2,b_3,b_4)=(0,1,2R,N),\\&\pi:L_{r(m)}(a_1,\ldots,a_m)\to L_{r(m)}(b_1,\ldots,b_m)\text{ with}\\&\pi\left(\sum_{i=1}^m\frac{p_i}{q_i}a_i\right)=\sum_{i=1}^m\frac{p_i}{q_i}b_i\\&\text{is a (well-defined) isomorphism}\Big\}\;\Box\end{aligned}$$

"Well-defined isomorphism" means that

$$\sum_{i=1}^m\frac{p_i}{q_i}a_i\in\mathbb{Z}\iff\sum_{i=1}^m\frac{p_i}{q_i}b_i\in\mathbb{Z}$$

and

$$\sum_{i=1}^m\frac{p_i}{q_i}a_i=\sum_{i=1}^m\frac{p'_i}{q'_i}a_i\iff\sum_{i=1}^m\frac{p_i}{q_i}b_i=\sum_{i=1}^m\frac{p'_i}{q'_i}b_i$$

for all p_i, p'_i, q_i, q'_i with absolute value $\le r(m)$, and that π is an isomorphism preserving $<$, $+$ and E.

Note that for every mapping $(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)\in W_m$ we must then necessarily have $a_i\equiv b_i \mod \operatorname{lcm}(1,2,\ldots,r(m))$ for all $i\in\{1,\ldots,m\}$, since otherwise π would not preserve integrality.

Our claim that player II has a winning strategy for the M-move EF-game can be split into the following two lemmas.

Lemma 6
$(0,1,R,N)\mapsto(0,1,2R,N)\in W_4$ *(i.e. W_4 is not empty)*

Lemma 7
If a game-situation $(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)\in W_m$ ($m<M+4$) arises, player II can always enforce that a_{m+1} and b_{m+1} are chosen such that $(a_1,\ldots,a_{m+1})\mapsto(b_1,\ldots,b_{m+1})$ is in W_{m+1}.

I.e., we actually show a stronger statement than player II just having a winning strategy for the M-move EF-game. We show that II can win a M-move game, where four elements in each structure ($(0,1,R,N)$ and $(0,1,2R,N)$) are already fixed at the beginning of the game.

Proof of Lemma 6: We have to show that the mapping $(0,1,R,N)\mapsto(0,1,2R,N)$ can be extended to an isomorphism $\pi:L_{r(4)}(0,1,R,N)\to L_{r(4)}(0,1,2R,N)$. Intuitively, the reason for this being possible is that the elements of the two quadruples belong to the same residue classes for all moduli less than $r(4)$, and that 1, $2R$ and N are so 'far apart' that they satisfy only trivial addition relations.

More formally, first, we have that for all p_i, q_i ($1\le i\le 3$) of no more than $r(4)$ in absolute value, the following holds.

$$\frac{p_1}{q_1}\cdot 1+\frac{p_2}{q_2}\cdot R+\frac{p_3}{q_3}\cdot N\in\mathbb{Z}\iff\frac{p_1}{q_1}\cdot 1+\frac{p_2}{q_2}\cdot 2R+\frac{p_3}{q_3}\cdot N\in\mathbb{Z}$$

To see this, just note that R, $2R$ and N are multiples of $r(4)!$, and therefore q_2 and q_3 evenly divide R, $2R$, and N. Thus, both sums are integral if and only if p_1/q_1 is an integer.

Next, we have to check whether π preserves equality and ordering. It suffices to show that for all p_i, q_i ($1\le i\le 6$) of no more than $r(4)$ in absolute value, the following holds.

$$\operatorname{sign}\left(\frac{p_1}{q_1}\cdot 1+\frac{p_2}{q_2}\cdot R+\frac{p_3}{q_3}\cdot N-\left(\frac{p_4}{q_4}\cdot 1+\frac{p_5}{q_5}\cdot R+\frac{p_6}{q_6}\cdot N\right)\right) \tag{1}$$

$$=\operatorname{sign}\left(\frac{p_1}{q_1}\cdot 1+\frac{p_2}{q_2}\cdot 2R+\frac{p_3}{q_3}\cdot N-\left(\frac{p_4}{q_4}\cdot 1+\frac{p_5}{q_5}\cdot 2R+\frac{p_6}{q_6}\cdot N\right)\right) \tag{2}$$

To see that this equality holds, note that N was chosen such that it is much larger than R, and R is much larger than 1. If $\frac{p_3}{q_3} \neq \frac{p_6}{q_6}$ we have

$$\left|\frac{p_1}{q_1}\right|+\left|\frac{p_4}{q_4}\right|+\left(\left|\frac{p_2}{q_2}\right|+\left|\frac{p_5}{q_5}\right|\right)\cdot 2R \le 8r(4)\cdot R < \frac{N}{r(4)^2} < \left|\frac{p_3}{q_3}-\frac{p_6}{q_6}\right|\cdot N$$

Thus, the values of expressions (1) and (2) are both equal to the sign of $\frac{p_3}{q_3}-\frac{p_6}{q_6}$.

If, on the other hand, $\frac{p_3}{q_3}=\frac{p_6}{q_6}$ holds, but $\frac{p_2}{q_2}\neq\frac{p_5}{q_5}$, then we have

$$\left|\frac{p_1}{q_1}\right|+\left|\frac{p_4}{q_4}\right| \le 2r(4) \le \frac{R}{r(4)^2} < \left|\frac{p_2}{q_2}-\frac{p_5}{q_5}\right|\cdot R$$

and the expressions (1) and (2) are both equal to the sign of $\frac{p_2}{q_2}-\frac{p_5}{q_5}$. In the case where $\frac{p_2}{q_2}=\frac{p_5}{q_5}$ and $\frac{p_3}{q_3}=\frac{p_6}{q_6}$, the expressions are identical.

Checking that π respects $+$ can be done in a similar fashion; a little calculation shows that

$$\frac{p_1}{q_1}+\frac{p_2}{q_2}R+\frac{p_3}{q_3}N+\frac{p'_1}{q'_1}+\frac{p'_2}{q'_2}R+\frac{p'_3}{q'_3}N=\frac{p''_1}{q''_1}+\frac{p''_2}{q''_2}R+\frac{p''_3}{q''_3}N$$

holds if and only if for all $i\in\{1,2,3\}$:

$$\frac{p_i}{q_i}+\frac{p'_i}{q'_i}=\frac{p''_i}{q''_i}$$

And the same is true if we replace R by $2R$. So these relations are trivially preserved by π.

The mapping π then also respects E, since the edge-relation is defined in terms of the addition relation and the fixed elements R and $2R$. ■

Proof of Lemma 7: We will show this lemma by stating an explicit strategy for player II. First we consider the easier point move case. As mentioned in the introduction, strategies for this case can also be found in [12, 21]. Then we will state the set move strategy which will be a non-trivial generalization of the point move.

Assume that the game situation $(a_1,\ldots,a_m)\mapsto(b_1,\ldots,b_m)\in W_m$ has arisen, where $(a_1,\ldots,a_4)=(0,1,R,N)$ and $(b_1,\ldots,b_4)=(0,1,2R,N)$. Let π be the induced isomorphism between $L_{r(m)}(a_1,\ldots,a_m)$ and $L_{r(m)}(b_1,\ldots,b_m)$. In the following we will abbreviate the tuples $(a_1,\ldots,a_m)$ and $(b_1,\ldots,b_m)$ as $\overline{a}$ and $\overline{b}$, respectively.

Point Move

Assume that player I chooses a new element a_{m+1} in structure $\mathcal{A}$ (the case of player I choosing an element of $\mathcal{B}$ is handled symmetrically). We have to choose a new element b_{m+1} such that $(\overline{a},a_{m+1})\mapsto(\overline{b},b_{m+1})$ is in W_{m+1}. We distinguish two cases.

In the first case, a_{m+1} is "close" to the previously chosen elements, and already in the domain of π. Here we can just set $b_{m+1}:=\pi(a_{m+1})$. In the second case, a_{m+1} is "far" from all previously chosen elements, i.e. does not satisfy any non-trivial addition relations with them. In this case it suffices for b_{m+1} to satisfy the same ordering constraints as a_{m+1} and belong to the same residue classes as a_{m+1} for moduli less than $r(m+1)$. We will see that this is always possible, since $r(m)$ was chosen large enough to leave plenty of 'room' between the elements $\{b_i\}$.

We will now give the details of the strategy in the two cases.

Case 1: $a_{m+1}\in L_{3r(m+1)^6}(\overline{a})$

Here, a_{m+1} is a linear combination $a_{m+1}=\sum_{i=1}^{m}\frac{p'_i}{q'_i}a_i$ of $\{a_1,\ldots,a_m\}$ with "small" coefficients. Therefore any linear combination $\sum_{i=1}^{m+1}\frac{p_i}{q_i}a_i$ of $\{a_1,\ldots,a_{m+1}\}$ can be rewritten as a linear combination

$$\sum_{i=1}^{m}\left(\frac{p_i}{q_i}+\frac{p_{m+1}p'_i}{q_{m+1}q'_i}\right)a_i$$

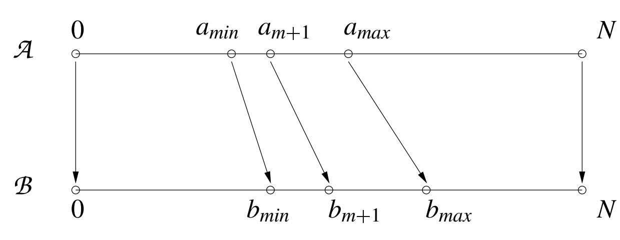
of $\{a_1,\ldots,a_m\}$ with "slightly larger" coefficients. So we have

$$L_{r(m+1)}(\overline{a},a_{m+1})\subseteq L_{6r(m+1)^8}(\overline{a})\subseteq L_{r(m)}(\overline{a}),$$

where the last inclusion holds by definition of $r(m)$. Thus, by setting $b_{m+1}:=\pi(a_{m+1})$ we have an isomorphism between $L_{r(m+1)}(\overline{a},a_{m+1})$ and $L_{r(m+1)}(\overline{b},b_{m+1})$ that is just a restriction of the old isomorphism π.

Case 2: $a_{m+1}\notin L_{3r(m+1)^6}(\overline{a})$

Let a_{min} and a_{max} be the greatest (respectively least) elements of $L_{3r(m+1)^6}(\overline{a})$ less (respectively greater) than a_{m+1}, and b_{min} and b_{max} be their images under π.



We claim that it is sufficient for player II to choose b_{m+1} such that

- $b_{m+1} \in \{b_{min}+1, \ldots, b_{max}-1\}$, and
- $a_{m+1} \equiv b_{m+1} \bmod \operatorname{lcm}(1,2,\ldots,r(m+1))$

Let us first see that it is always possible to find such a b_{m+1}. If $b_{max} - b_{min} > \operatorname{lcm}(1,\ldots,r(m+1))$, then such a b_{m+1} obviously exists, since there has to be an element belonging to the same residue class as a_{m+1} between b_{min} and b_{max}.

So assume that $b_{max} - b_{min} \leq \operatorname{lcm}(1,\ldots,r(m+1))$ holds. Since, by definition, $r(m) \geq \operatorname{lcm}(1,2,\ldots,r(m+1))$ we have $\{1,\ldots,\operatorname{lcm}(1,2,\ldots,r(m+1))\} \subseteq L_{r(m)}(\overline{a})$ (as "linear combinations" of $a_2 = b_2 = 1$). Since π is the identity mapping on these linear combinations of 1 and preserves the addition predicate, we have that $a_{max} - a_{min} = b_{max} - b_{min}$. Furthermore we have for all $k \leq \operatorname{lcm}(1,2,\ldots,r(m+1))$ that

$$\frac{a_{max}+k}{\operatorname{lcm}(1,2,\ldots,r(m+1))} \in \mathbb{Z} \Leftrightarrow \frac{b_{max}+k}{\operatorname{lcm}(1,2,\ldots,r(m+1))} \in \mathbb{Z}$$

and therefore $a_{max} \equiv b_{max} \bmod \operatorname{lcm}(1,2,\ldots,r(m+1))$, and the same for a_{min} and b_{min}.

So a_{min} and b_{min} (and a_{max} and b_{max}) belong to the same residue classes modulo $\operatorname{lcm}(1,2,\ldots,r(m+1))$. It then follows with $a_{max} - a_{min} = b_{max} - b_{min}$ that for each residue class a_{m+1} modulo $\operatorname{lcm}(1,2,\ldots,r(m+1))$ between a_{min} and a_{max} the same residue class exists between b_{min} and b_{max}, and we can choose a b_{m+1} according to the restrictions given above.

After having seen that we can always choose a b_{m+1} according to the restrictions given above, we now have to show that this choice of b_{m+1} necessarily leads to a mapping $(\overline{a}, a_{m+1}) \mapsto (\overline{b}, b_{m+1}) \in W_{m+1}$.

So let b_{m+1} be chosen as above and let $\pi' : L_{r(m+1)}(\overline{a}, a_{m+1}) \to L_{r(m+1)}(\overline{b}, b_{m+1})$ be the extension of the mapping $(\overline{a}, a_{m+1}) \mapsto (\overline{b}, b_{m+1})$. We have to show that π' is a well-defined isomorphism, which requires checking the same properties as in the proof of Lemma 6.

- First, we have that

$$\sum_{i=1}^{m+1} \frac{p_i}{q_i} a_i \in \mathbb{Z} \Longleftrightarrow \sum_{i=1}^{m+1} \frac{p_i}{q_i} b_i \in \mathbb{Z},$$

since for every i both a_i and b_i lie in the same residue class[3] modulo $\operatorname{lcm}(1,\ldots,r(m+1))$ and therefore modulo $\operatorname{lcm}(q_1, q_2, \ldots, q_{m+1})$.

- π' respects equality and ordering. Let $a = \sum_{i=1}^{m+1} \frac{p_i}{q_i} a_i$ and $a' = \sum_{i=1}^{m+1} \frac{p'_i}{q'_i} a_i$ be two elements of $L_{r(m+1)}(\overline{a}, a_{m+1})$ with $a < a'$ (the case $a = a'$ is handled in the same manner). If $\frac{p_{m+1}}{q_{m+1}} = \frac{p'_{m+1}}{q'_{m+1}}$ then the inequality is equivalent to

$$\sum_{i=1}^{m} \frac{p_i}{q_i} a_i < \sum_{i=1}^{m} \frac{p'_i}{q'_i} a_i$$

This inequality is independent of a_{m+1}, so since π' agrees with π on $L_{r(m+1)}(\overline{a})$ and π respects the ordering, we have that

$$\sum_{i=1}^{m} \frac{p_i}{q_i} b_i < \sum_{i=1}^{m} \frac{p'_i}{q'_i} b_i$$

And adding $\frac{p_{m+1}}{q_{m+1}} b_{m+1} = \frac{p'_{m+1}}{q'_{m+1}} b_{m+1}$ on both sides of the inequality does not change its validity.

If, on the other hand $\frac{p_{m+1}}{q_{m+1}} \neq \frac{p'_{m+1}}{q'_{m+1}}$ (say it is $>$), then the inequality can be solved for a_{m+1}:

$$a_{m+1} < \sum_{i=1}^{m} \left(\frac{q_{m+1} q'_{m+1}}{p_{m+1} q'_{m+1} - p'_{m+1} q_{m+1}} \right) \left(\frac{p'_i q_i - p_i q'_i}{q_i q'_i} \right) a_i$$

The linear combination on the right is an element of $L_{2r(m+1)^4}(\overline{a})$, and therefore an element of $L_{3r(m+1)^6}(\overline{a})$. Since we chose b_{m+1} such that it satisfies the same ordering-relations as a_{m+1} regarding the elements of $L_{3r(m+1)^6}(\overline{b})$, this inequality is preserved by π'.

- To see that π' preserves $+$, consider an equality of the following form:

$$\sum_{i=1}^{m} \frac{p_i}{q_i} a_i + \sum_{i=1}^{m} \frac{p'_i}{q'_i} a_i = \sum_{i=1}^{m} \frac{p''_i}{q''_i} a_i$$

If $\frac{p_{m+1}}{q_{m+1}} + \frac{p'_{m+1}}{q'_{m+1}} = \frac{p''_{m+1}}{q''_{m+1}}$, then the equality is independent of the value of a_{m+1}, and thus preserved by π'. If it depends on the value of a_{m+1}, we can solve the equation for a_{m+1}, obtaining

$$a_{m+1} = \sum_{i=1}^{m} \frac{\frac{p_i}{q_i} + \frac{p'_i}{q'_i} - \frac{p''_i}{q''_i}}{\frac{p''_{m+1}}{q''_{m+1}} - \frac{p_{m+1}}{q_{m+1}} - \frac{p'_{m+1}}{q'_{m+1}}} \cdot a_i$$

But this implies $a_{m+1} \in L_{3r(m+1)^6}(\overline{a})$, in contradiction to the choice of a_{m+1}.

- And finally, E is preserved, since it is defined in terms of the addition predicate.

Set Move

Player I chooses an element a_i and a set $A_0 \subseteq \{0,1,\ldots,N\}$ with $|A_0| = a_i$ (again the case of player I choosing an element and subset from $\mathcal{B}$ is handled symmetrically). Player

[3] For a_{m+1} and b_{m+1} we have this by choice of b_{m+1}, for the other i this holds since π preserves integrality, i.e. since we have $\frac{p+a_i}{q} \in \mathbb{Z} \Leftrightarrow \frac{p+b_i}{q} \in \mathbb{Z}$ for all $p, q \leq r(m+1)$.

II has to answer with a set B_0 with $|B_0| = b_i$. We want to choose B_0 in such a way that whatever element player I chooses in it, we can answer according to our point move strategy with an element of A_0.

In the point move case we distinguished between two cases for a new element: whether it is in the set $L_{3r(m+1)^6}(\overline{a})$ or not. Since we want to eventually apply our point move strategy, we do the same here. Let $A_1 := A_0 \cap L_{3r(m+1)^6}(\overline{a})$ and $A_2 := A_0 \setminus A_1$. We will choose B_1 and B_2 such that should player I choose an element b_{m+1} from B_1, we can answer (according to our point move strategy) with an element a_{m+1} of A_1 and likewise for B_2 and A_2.

- Set $B_1 := \{\pi(a) \mid a \in A_1\}$, the images of A_1 under π. Clearly, if player I chooses any element in B_1 we can answer with its pre-image under π from A_1; this is case 1 of the point move.

- For the definition of B_2, recall case 2 in the point move. We found that a b_{m+1} could be answered by any a_{m+1} that is in the same residue class modulo $\mathrm{lcm}(1,2,\dots,r(m+1))$ and in the same 'interval' between elements of $L_{3r(m+1)^6}(\overline{a})$ and $L_{3r(m+1)^6}(\overline{b})$, respectively.

  For $c,d \in L_{3r(m+1)^6}(\overline{a})$, such that $c < d$ and there are no further elements of $L_{3r(m+1)^6}(\overline{a})$ between c and d, and $r \in \{0,1,\dots,\mathrm{lcm}(1,2,\dots,r(m+1))-1\}$, let $I_{c,d,r}$ and $I'_{c,d,r}$ be the following sets:

$$I_{c,d,r} := \{a \mid c < a < d, a \equiv r \bmod \mathrm{lcm}(1,2,\dots,r(m+1))\}$$
$$I'_{c,d,r} := \{b \mid \pi(c) < b < \pi(d), \quad b \equiv r \bmod \mathrm{lcm}(1,2,\dots,r(m+1))\}$$

  When player I chooses an element in $I'_{c,d,r}$ we can answer with any element from $I_{c,d,r}$. So let n be minimal such that for appropriately chosen c_j, d_j, r_j

$$A_2 \subseteq \bigcup_{j=1}^{n} I_{c_j,d_j,r_j}.$$

  We then set

$$B_2 := \bigcup_{j=1}^{n} I'_{c_j,d_j,r_j},$$

  and as in case 2 of the point move it is clear that if player I chooses any element from B_2, say from I'_{c_l,d_l,r_l}, we can answer with any element of $I_{c_l,d_l,r_l} \cap A_2$; and the latter set is non-empty since n was chosen minimally.

It follows from the previous discussion that if player II chooses $B_0 \subseteq B_1 \cup B_2$ arbitrary with $|B_0| = b_i$, then player II will always be able to answer player I's choice of $b_{m+1} \in B_0$ with an $a_{m+1} \in A_0$ according to the point move strategy. So all that remains to be shown is that $|B_1 \cup B_2| \geq b_i$ holds, i.e., that we can actually choose a B_0 of the required size.

To this end we will show that

(i) $s := |L_{3r(m+1)^6}(\overline{a})| + \sum_{i=1}^{n} |I_{c_j,d_j,r_j}|$ is an element of $L_{r(m)}(\overline{a})$, and that

(ii) $\pi(s) = |B_1 \cup B_2|$.

Since we know that $a_i \leq s$, and that π preserves the ordering, the inequality $\pi(a_i) \leq \pi(s)$ must also hold, i.e. we have $b_i \leq |B_1 \cup B_2|$, and the proof is finished.

First, we bound the size of $L_{3r(m+1)^6}(\overline{a})$. In the linear combinations $\sum_{i=1}^{m} \frac{p_i}{q_i} a_i$ of elements $a_1,\dots,a_m$ that make up $L_{3r(m+1)^6}(\overline{a})$, each of the $2m$ p_j's and q_j's appearing in the linear combinations can have values from $\{0,\pm1,\pm2,\dots,\pm3r(m+1)^6\}$. Since $\frac{p_j}{q_j} = \frac{-p_j}{-q_j}$, etc., a lot of these choices lead to the same values. The number $(6r(m+1)^6)^{2m}$ therefore is a conservative upper bound for the number of elements in $L_{3r(m+1)^6}(\overline{a})$.

This implies that $|L_{3r(m+1)^6}(\overline{a})|$ is an element of $L_{(6r(m+1)^6)^{2m}}(\overline{a})$ and of $L_{(6r(m+1)^6)^{2m}}(\overline{b})$ – as a 'linear combination' of $a_1 = b_1 = 1$.

We now turn to $\sum_{i=1}^{n} |I_{c_j,d_j,r_j}|$. First, the number of 'intervals' $]c_j,d_j[$ in $L_{3r(m+1)^6}(\overline{a})$ is bounded by the number of elements of that set, and therefore we have

$$n \leq (6r(m+1)^6)^{2m} \cdot \mathrm{lcm}(1,\dots,r(m+1)).$$

As for $|I_{c_j,d_j,r_j}|$, its size is equal to either

$$\left\lfloor \frac{d_j - c_j - 1}{\mathrm{lcm}(1,2,\dots,r(m+1))} \right\rfloor \quad \text{or} \quad \left\lceil \frac{d_j - c_j - 1}{\mathrm{lcm}(1,2,\dots,r(m+1))} \right\rceil.$$

This means that there is some

$$e_j \in \{0,\pm1,\pm2,\dots,\pm\mathrm{lcm}(1,2,\dots,r(m+1))\}$$

such that

$$|I_{c_j,d_j,r_j}| = \frac{d_j - c_j - 1 + e_j}{\mathrm{lcm}(1,2,\dots,r(m+1))}.$$

Similarly, we have that

$$|I'_{c_j,d_j,r_j}| = \frac{\pi(d_j) - \pi(c_j) - 1 + e_j}{\mathrm{lcm}(1,2,\dots,r(m+1))}.$$

Using $c_j, d_j \in L_{3r(m+1)^6}(\overline{a})$ this implies that

$$|I_{c_j,d_j,r_j}| \in L_{(6r(m+1)^6)^2 \mathrm{lcm}(1,\dots,r(m+1))}(\overline{a}).$$

And therefore

$$s = |L_{3r(m+1)^6}(\overline{a})| + \sum_{i=1}^{n} |I_{c_j,d_j,r_j}|$$
$$\in L_{(n+1)((6r(m+1)^6)^{2m}\mathrm{lcm}(1,\dots,r(m+1)))^{(n+1)}}(\overline{a}) \subseteq L_{r(m)}(\overline{a})$$

Here we used the (easily verified) fact, that the sum of k elements of $L_d(\overline{a})$ is in $L_{kd^k}(\overline{a})$.

We also established that $\pi(|L_{3r(m+1)^6}(\overline{a})|) = |L_{3r(m+1)^6}(\overline{b})|$, and that $\pi(|I_{c_j,d_j,r_j}|) = |I'_{c_j,d_j,r_j}|$. Since s can be expressed as the sum of these values in $L_{r(m)}(\overline{a})$, so can $\pi(s)$ in $L_{r(m)}(\overline{b})$, and therefore $\pi(s) = |B_1 \cup B_2|$, as claimed. ■

3.4. $FOC(<,+)$ is weaker than $FOC(<,+,\times)$

The previous proof gives us an immediate corollary:

Corollary 8
$FOC(<,+)$ is strictly weaker than $FOC(<,+,\times)$.

Proof: The two structures given in the preceding proof are distinguishable in $FOC(<,+,\times)$ since we just have to ask whether the only element to which 0 has an edge evenly divides the maximum element. ■

4. Conclusion

We have shown that the logic $FOC(<,+)$ does not capture *LOGSPACE*, since it cannot express deterministic transitive closure. This may be one of the first meaningful results about the expressibility of first-order logic augmented with counting quantifiers in the presence of an ordering and non-trivial arithmetic operators.

As Corollary 8 shows, the proof breaks down in presence of a multiplication predicate. This is not surprising, as this case corresponds to the open question TC^0 vs. *LOGSPACE*. The intuitive reason why the problem becomes much harder is that we used the fact that the combinatorial structure of the addition operation is very simple. But, as number theory evidences, addition and multiplication taken together exhibit a very involved structure. Therefore constructing an explicit EF-game strategy for this general case seems to be very difficult.

A natural next question therefore is: if not multiplication, what other (most likely weaker) operations can we add to *FOC*, and still prove inexpressibility results?

Acknowledgments

This work was carried out while the author was at the 'Institute for Mathematical Logic' of the Albert-Ludwigs-Universität in Freiburg, Germany. My thanks go to Martin Grohe, who suggested to work on this problem and gave many helpful comments on an earlier draft of this paper. I also thank Yevgeniy Dodis, Venkatesan Guruswami, Madhu Sudan and Salil Vadhan for numerous additional suggestions, and the anonymous referees for their detailed comments that helped to improve the presentation.

References

[1] S. Abiteboul and V. Vianu. Fixpoint extensions of first-order logic and datalog-like languages. *Proceedings LICS'89*, pages 71–79, 1989.

[2] E. Allender. Circuit complexity before the dawn of the new millennium. *Proceedings FST&TCS'96, LNCS 1180*, pages 1–18, 1996.

[3] D. Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *Journal of Computer and System Sciences*, 41:274–306, 1990.

[4] M. Benedikt and J. Keisler. Expressive power of unary counters. *J. Mycielski (ed.), Structures in Logic and Computer Science, LNCS 1261*, pages 34–50, 1997.

[5] H. Ebbinghaus and J. Flum. *Finite Model Theory*. Springer Verlag, 1995.

[6] H. Ebbinghaus, J. Flum, and W. Thomas. *Mathematical Logic*. Springer Verlag, 1994.

[7] A. Ehrenfeucht. An application of games to the completeness problem for formalized theories. *Fundamenta Mathematicae*, 49:129–141, 1961.

[8] K. Etessami. Counting quantifiers, successor relations and logarithmic space. *Journal of Computer and System Sciences*, 54:400–411, 1997.

[9] R. Fagin. Generalized first-order spectra and polynomial-time recognizable sets. *R.M. Karp (ed.), Complexity of Computation, SIAM-AMS Proceedings*, 7:43–73, 1974.

[10] R. Fraïsse. Sur quelques classifications des systèmes de relations. *Université d'Alger, Publications Scientifiques, Série A*, 1:35–182, 1954.

[11] E. Grädel and Y. Gurevich. Metafinite model theory. *Information and Computation*, 140:26–81, 1998.

[12] W. Hodges. *Model Theory*. Cambridge University Press, 1993.

[13] N. Immerman. Relational queries computable in polynomial time. *Information and Control*, 68:86–104, 1986.

[14] N. Immerman. Expressibility as a complexity measure: results and directions. *Second Structure in Complexity Conference*, pages 194–202, 1987.

[15] N. Immerman. Languages that capture complexity classes. *SIAM Journal of Computing*, 16(4):760–778, 1987.

[16] N. Immerman. Descriptive and computational complexity. *Computational Complexity Theory, AMS Proc. Symp. in Applied Math.*, 38:75–91, 1989.

[17] N. Immerman. *Descriptive and Computational Complexity*. Springer Verlag, 1998.

[18] L. Libkin. On the forms of locality over finite models. *Proceedings LICS'97*, pages 204–215, 1997.

[19] L. Libkin. On counting logics and local properties. *Proceedings LICS'98*, pages 501–512, 1998.

[20] L. Libkin and L. Wong. Unary quantifiers, transitive closure, and relations of large degree. *Proceedings STACS'98, LNCS 1373*, pages 183–193, 1998.

[21] J. F. Lynch. On sets of relations definable by addition. *Journal of Symbolic Logic*, 47(3):659–668, 1982.

[22] J. Nurmonen. On winning strategies with unary quantifiers. *Journal of Logic and Computation*, 6(6):779–798, 1996.

[23] M. Presburger. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. *Sprawozdanie z I Kongresu Mat. Krajów Slowiańskich*, pages 92–101, 1930.

[24] M. Vardi. The complexity of relational query languages. *Proceedings STOC'82*, pages 137–146, 1982.