Counting modulo quantifiers on finite structures

Juha Nurmonen *
Department of Mathematics
University of Helsinki
juha.nurmonen@helsinki.fi

Abstract

We give a combinatorial method for proving elementary equivalence in first-order logic FO with counting modulo n quantifiers $\mathbf{D}_n$. Inexpressibility results for $FO(\mathbf{D}_n)$ with built-in linear order are also considered. For instance, the class of linear orders of length divisible by $n+1$ cannot be expressed in $FO(\mathbf{D}_n)$. This result has several consequences, such as, comparing cardinalities or connectivity of ordered graphs are not definable in $FO(\mathbf{D}_n)$. We also show that the height of complete n-ary trees cannot be expressed in $FO(\mathbf{D}_n)$ with linear order. Interpreting the predicate $y = nx$ as a complete n-ary tree, we show that the predicate $y = (n+1)x$ cannot be defined in $FO(\mathbf{D}_n)$ with linear order. This proves the conjecture of Niwiński and Stolboushkin. We also discuss connection between our results and the well-known open problem in circuit complexity theory, whether $ACC = NC^1$.

1. Introduction

First-order logic FO has turned out to have quite a limited expressive power for many purposes in finite model theory, even in the presence of built-in linear order. Characterizing complexity classes by a logic, certain inductive extensions of first-order logic, such as least fixpoints of positive formulas, have been studied. For instance, problems in complexity classes *PTIME* and *PSPACE* have been proved to coincide with queries expressible in fixpoint logic and partial fixpoint logic (on the class of ordered finite structures), respectively [1, 15, 23].

The importance of first-order logic with linear order has turned out to be in characterizations of low level complexity classes by a logic. McNaughton and Papert [18] showed that star-free regular languages are exactly the ones definable in first-order logic. Star-free languages in A^* are the subsets obtained, when beginning with the letters of the alphabet A, by repeated applications of boolean operations and concatenation. Evidently all such

*Supported by the Academy of Finland. Extended abstract will appear in *Proceedings of the 11th Annual IEEE Symposium on Logic in Computer Science*, 1996.
Mathematics Subject Classification: 03C13, 03C80
Keywords: Ehrenfeucht-Fraïssé games, finite model theory, counting modulo quantifiers

languages are regular. On the other hand, in the presence of the so-called *BIT*-predicate, *FO* has been proved to coincide with the logarithmic time hierarchy [5].

For the circuit complexity classes AC^0 and NC^1 something further has to be considered in order to characterize these classes by a logic. Recall that NC^1 is the class of problems which can be computed by polynomial size circuits with fan-in two gates and depth $O(\log n)$, whereas in AC^0 polynomial size circuits with unbounded fan-in but only constant depth circuits are allowed. It is not difficult to see that $AC^0 \subseteq NC^1$. Consider next non-empty words of the alphabet $\{0,1\}$ and let

$$length(p) = \{w \in \{0,1\}^+ \mid |w| \equiv 0 \pmod p\} \quad \text{and}$$

$$sum(p) = \{w \in \{0,1\}^+ \mid \textstyle\sum_{i=0}^{|w|-1} w_i \equiv 0 \pmod p\},$$

where $|w|$ is the length of a word w and w_i is the i'th bit in w. From the work of Ajtai [2] and Furst, Saxe and Sipser [10] it follows that $sum(2)$ is not in AC^0, whereas it is in NC^1; consequently $AC^0 \subsetneq NC^1$.

Barrington [3] introduced the class ACC obtained from AC^0 by allowing gates, which count inputs modulo a constant p, for every p. Since AC^0 contains regular languages that are not star-free, for instance the languages $length(p)$, where $p > 1$, first-order logic is not strong enough to characterize AC^0. And as mentioned above, $sum(2)$ is not in AC^0, whence we also know that $AC^0 \subsetneq ACC$. One of the major open problems in circuit complexity theory is, whether $ACC = NC^1$.

In general, several types of counting quantifiers have been considered in finite model theory. Corredor [7] considered certain cardinality quantifiers and gave a characterization when any cardinality quantifier is definable from another cardinality quantifier. Our approach works for arbitrary (relational) vocabulary. In Section 3 we give a general criterion that guarantees elementary equivalence of two finite structures in *FO* with *counting modulo n quantifier* $\mathbf{D}_n$, where n is a positive integer. The method is based on the work of Hanf [12]. Especially in the context of finite model theory, this method was considered in [9, 20]. Our criterion has been tailored for the logic $FO(\mathbf{D}_n)$. It gives an easy combinatorial way to prove undefinability results for $FO(\mathbf{D}_n)$. We show that it is enough to count the number of isomorphism types of neighborhoods of a fixed radius of points in our structures. If the result of this counting satisfies the simple conditions, which we shall give in Section 3, elementary equivalence of the structures considered is guaranteed.

Our main interest concerns inexpressibility results in $FO(\mathbf{D}_n)$ with built-in linear order. In Section 4 we show that many properties known not to be expressible in first-order logic, are not expressible in $FO(\mathbf{D}_n)$, either. Counterexamples are mostly based on the result, that sufficiently large linear orders of modulo n equal length cannot be separated in $FO(\mathbf{D}_n)$. We show that the Rescher and Härtig quantifiers are not definable in $FO(\mathbf{D}_n)$, and hence $FO(\mathbf{D}_n)$ fails to compare cardinalities. Connectivity of ordered graphs is also shown not to be expressible in $FO(\mathbf{D}_n)$. We also give a characterization for the logic $FO(\mathbf{D}_n)$ to be as strong as the logic $FO(\mathbf{D}_m)$ on ordered structures, where m and n are positive integers.

First-order logic with counting modulo quantifiers and built-in linear order cannot define any non-regular languages [21]. In [4] the $ACC = NC^1$ problem was reduced to the question whether there are regular languages with non-solvable syntactic monoid in ACC. Niwiński and Stolboushkin [19] reformulated this question in the following form (for more detailed discussion, see [4, 5, 6, 21]):

Is there a numerical relation R such that first-order logic with counting modulo quantifiers and built-in linear order can express more regular languages with R than without?

Niwiński and Stolboushkin [19] attacked this question and considered the relation $y = 2x$. It had been open so far, if FO with linear order and the relation $y = 2x$ can express that the size of a model is divisible by three. In [19] a negative answer to this problem was given. Niwiński and Stolboushkin also conjectured that this holds even in $FO(\mathbf{D}_2)$. Using the extra predicate $y = nx$ we construct in Section 5 complete n-ary trees of height m and $m+1$, for a suitable $m \in \mathbb{N}$. We then prove that these trees are elementarily equivalent with respect to $FO(\mathbf{D}_n)$. Since complete n-trees have cardinality divisible by $n+1$ if and only if their height is odd, this proves the conjecture for every n. (A similar construction was used in [19].)

2. Preliminaries

By a vocabulary σ we mean a finite set of relation symbols R_i, $1 \leq i \leq s$, each of which has a fixed arity. A σ-structure $\mathbb{A}$ is a set A, the *universe* of $\mathbb{A}$, with a mapping associating a relation $R_i(\mathbb{A})$ over A with each $R_i \in \sigma$, where $R_i(\mathbb{A})$ has the same arity as R_i ($R_i(\mathbb{A})$ is often denoted shortly by R_i, if the notation is clear from the context). Throughout the rest of this paper all structures considered are finite, i.e. the universe of every structure is finite. Without loss of generality, we assume that the universe of any structure is of the form $\{0, \ldots, n\}$ for some n, and $\leqslant$ is the standard linear ordering on $\{0, \ldots, n\}$.

Consider a σ-structure $\mathbb{A}$ and assume that $\leqslant$ is the linear order on A. Let $\mathbb{A}^{\leqslant}$ be the resulting ordered σ-structure. A subset $X \subseteq A$ is denoted simply by $[a, b]$, if the members of X form an interval $[a, b] = \{x \mid a \leqslant x \leqslant b\}$ on A. Disjoint union of structures $\mathbb{A}$ and $\mathbb{B}$ is obtained by adjoining $\mathbb{A}$ and the isomorphic copy of $\mathbb{B}$ on the set $\{|A|, \ldots, |A| + |B| - 1\}$ under the bijection $i \mapsto i + |A|$. This disjoint union is denoted by $\mathbb{A} \dot{\cup} \mathbb{B}$.

The definitions of sentences and semantics of first-order logic FO are the standard ones. Equality is treated as a special relation symbol that is not a member of the vocabulary.

2.1. Counting modulo quantifiers

We now give a precise definition of the logic $FO(\mathbf{D}_n)$, where n is a positive integer. Formulas of this logic are defined as for first-order logic FO with the following additional rule:

if φ is a formula, then $\mathbf{D}_n x \varphi(x, \overline{y})$ is a formula.

The semantics of $FO(\mathbf{D}_n)$ is defined with the corresponding rule:

$$\mathbb{A} \models \mathbf{D}_n x \varphi(x, \overline{b}) \text{ if and only if } \left|\{a \mid \mathbb{A} \models \varphi(a, \overline{b})\}\right| \equiv 0 \pmod{n}.$$

In the case $n = 1$, the quantifier $\mathbf{D}_1$ becomes trivial and first-order definable. Hence in our results, $FO(\mathbf{D}_1)$ can be replaced by FO. The logic $FO(\mathcal{D})$ for $\mathcal{D}$ a finite set of counting modulo quantifiers is defined similarly.

A class $\mathcal{C}$ of σ-structures is said to be definable in $FO(\mathcal{D})$, if there is a sentence φ of $FO(\mathcal{D})$ such that for every σ-structure $\mathbb{A}$, $\mathbb{A} \in \mathcal{C}$ if and only if $\mathbb{A} \models \varphi$.

The quantifier rank of a formula of $FO(\mathcal{D})$ is defined as the maximum number of nested quantifiers (counting both the first-order quantifiers and the quantifiers in $\mathcal{D}$) occuring in the formula. Two models $\mathbb{A}$ and $\mathbb{B}$ are said to be elementarily equivalent with respect to $FO(\mathcal{D})$ up to a quantifier rank r, if for any sentence φ of $FO(\mathcal{D})$ with quantifier rank at most r, $\mathbb{A} \models \varphi$ if and only if $\mathbb{B} \models \varphi$; we denote this by $\mathbb{A} \equiv^r_{FO(\mathcal{D})} \mathbb{B}$.

Observe that for $k < n$, the sentence $\psi^{k,n}_\varphi$ defined by

$$\exists x_1 \ldots \exists x_k \mathbf{D}_n x(\varphi(x) \wedge \bigwedge_{i=1}^{k}(\neg x = x_i) \wedge \bigwedge_{i=1}^{k} \varphi(x_i) \wedge \bigwedge_{\substack{i,j=1 \\ i \neq j}}^{k} (\neg x_i = x_j))$$

expresses that there are $k \pmod{n}$ points satisfying φ. Similarly, the quantifier $\mathbf{D}_n$ is definable in $FO(\mathbf{D}_m)$, whenever m is divisible by n. Namely, let $m = nr$ and $\varphi(x)$ be a formula. Then we have

$$\mathbf{D}_n x \varphi(x) \iff \bigvee_{i=0}^{r-1} \psi^{ni,m}_\varphi.$$

For $\mathcal{D}$ and $\mathcal{D}'$ sets of counting modulo quantifiers, the logic $FO(\mathcal{D})$ is *at most as strong as* the logic $FO(\mathcal{D}')$, if every sentence of the logic $FO(\mathcal{D})$ is also definable in $FO(\mathcal{D}')$; we denote this by $FO(\mathcal{D}) \leq FO(\mathcal{D}')$. If $FO(\mathcal{D}) \leq FO(\mathcal{D}')$ and $FO(\mathcal{D}') \leq FO(\mathcal{D})$, then we denote $FO(\mathcal{D}) \equiv FO(\mathcal{D}')$. The observation above is actually a special case of a more general result.

2.1. Theorem. **([7])** *For m and n positive integers, $FO(\mathbf{D}_n) \leq FO(\mathbf{D}_m)$ if and only if n divides m.*

A game theoretical condition for elementary equivalence in $FO(\mathbf{D}_n)$ of two structures can be given by modifying the $(k, \mathbf{Q})$-pebble games introduced by Kolaitis and Väänänen [16] (see also [22]). We call this game the *$(r, \mathbf{D}_n)$-game*. The rules of the game are as follows.

> Suppose that a positive integer r and σ-structures $\mathbb{A}$ and $\mathbb{B}$ are given. The players are called the spoiler and the duplicator. There are r rounds in this game. In each round $i \leq r$, the spoiler begins by choosing a quantifier move or a first-order move. In a first-order move the spoiler and the duplicator play as in an ordinary first-order Ehrenfeucht-Fraïssé game. Suppose then the spoiler selected a quantifier move. Then the spoiler selects one of the structures $\mathbb{A}$ and $\mathbb{B}$ (say $\mathbb{A}$), and a subset $X \subseteq A$. The duplicator answers by choosing a subset from the other structure, in this case $Y \subseteq B$, that satisfies $|Y| \equiv |X| \pmod{n}$. Then the spoiler picks an element $b_i \in B$ and the duplicator picks an element $a_i \in A$, such that $a_i \in X$ if and only if $b_i \in Y$. The duplicator wins, if the mapping $a_i \mapsto b_i$, $i \leq r$, is a partial isomorphism $\mathbb{A} \to \mathbb{B}$; otherwise the spoiler wins.

Notice that first-order moves are special cases of a quantifier move. Namely, the spoiler can choose $X = \emptyset$ and the duplicator has to answer by $Y = \emptyset$. Then the spoiler selects a point outside from Y and the duplicator selects a point outside from X.

The proof of the following theorem is standard and is included in [16].

2.2. Theorem. *Assume r is a positive integer and $\mathbb{A}$ and $\mathbb{B}$ are σ-structures. If the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over the structures $\mathbb{A}$ and $\mathbb{B}$, then $\mathbb{A} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}$.*

This $(r, \mathbf{D}_n)$-game corresponds actually the logic, where there is a quantifier for each $k < n$ expressing that there are $k \pmod n$ points satisfying a formula $\varphi(x, \overline{y})$. As observed above, these quantifiers can be easily defined in $FO(\mathbf{D}_n)$ (with a small incrediment of quantifier rank).

3. The combinatorial method

In this section we shall give a combinatorial condition that guarantees a winning strategy for the duplicator in the $(r, \mathbf{D}_n)$-game over structures $\mathbb{A}$ and $\mathbb{B}$. According to Theorem 2.2, this means that any structures $\mathbb{A}$ and $\mathbb{B}$ satisfying this condition are elementarily equivalent with respect to $FO(\mathbf{D}_n)$, up to the quantifier rank r.

Let $\mathbb{A}$ be a finite σ-structure, where $\sigma = \{R_1, \ldots, R_s\}$. Recall the definition of the *Gaifman graph* of $\mathbb{A}$: Let a and b be two points in A. Then a and b are *adjacent*, if there is some R_i and tuple $t \in R_i(\mathbb{A})$ such that a and b are entries in the tuple t. The *degree* $deg(a)$ of a point a is the number of points adjacent to a but not equal to a. Whenever $X \subseteq A$, $\mathbb{A}\restriction X$ is the structure with universe X where the interpretation of R_i is the set of tuples t in $R_i(\mathbb{A})$ such that every entry of t is in X, for $1 \le i \le s$.

The neighborhood $N(d, a)$ of radius d of $a \in A$ is defined recursively by

$$N(1, a) = \{a\};$$

$$N(d+1, a) = \{v \mid v \text{ is adjacent to some } b \in N(d, a)\} \cup N(d, a).$$

Thus $N(d, a)$ consists of all points whose distance from a is *strictly* less than d. The *d-type* of a point a in a structure $\mathbb{A}$ is the isomorphism type of $(\mathbb{A}\restriction N(d, a), a)$, where a is treated as a constant. Thus two points a and b in $\mathbb{A}$ have the same d-type, if and only if $\mathbb{A}\restriction N(d, a) \cong \mathbb{A}\restriction N(d, b)$ under an isomorphism that maps a to b.

We fix now some notation. Consider a σ-structure $\mathbb{A}$ and suppose $X \subseteq A$. Let τ be a d-type. We denote

$$T^X_{\mathbb{A},\tau} = \{x \in X \mid x \text{ has type } \tau \text{ in } \mathbb{A}\} \quad \text{and}$$

$$K^X_{\mathbb{A},\tau} = \{x \in A \setminus X \mid x \text{ has type } \tau \text{ in } \mathbb{A}\} = T^{A \setminus X}_{\mathbb{A},\tau}.$$

Furthermore, let $k^X_{\mathbb{A},\tau} = \left|T^X_{\mathbb{A},\tau}\right|$. In the case $X = A$ we usually omit the superscripts.

Let d, m and n be positive integers. We call structures $\mathbb{A}$ and $\mathbb{B}$ *d-equivalent*, if for each d-type τ both structures have exactly the same number of points with d-type τ. The structures $\mathbb{A}$ and $\mathbb{B}$ are *(d, m)-equivalent*, if for every d-type τ they have either exactly the same number of points with d-type τ, or both structures have at least m points with d-type τ, i.e. $\min(k_{\mathbb{A},\tau}, m) = \min(k_{\mathbb{B},\tau}, m)$. We say that the structures $\mathbb{A}$ and $\mathbb{B}$ are *$(d, m, \mathbf{D}_n)$-equivalent*, if for each d-type τ there are either equally many points with d-type τ, or at least m points with d-type τ but modulo n equally many; that is, for each d-type τ

$$\min(k_{\mathbb{A},\tau}, m) = \min(k_{\mathbb{B},\tau}, m) \quad \text{and} \quad k_{\mathbb{A},\tau} \equiv k_{\mathbb{B},\tau} \pmod{n}.$$

Note that d-equivalent structures are $(d, m, \mathbf{D}_n)$-equivalent, and $(d, m, \mathbf{D}_n)$-equivalent structures are (d, m)-equivalent. For instance, considering the structures of the empty vocabulary, it is easy to see that this hierarchy is strict. Notice also that $(d, m, \mathbf{D}_1)$-equivalence is the same as (d, m)-equivalence.

Fagin, Stockmeyer and Vardi [9] proved, that (d, m)-equivalence of two structures is enough to guarantee elementary equivalence of these structures up to a certain quantifier rank.

3.1. Theorem. ([9]) *Let r and f be positive integers. There are positive integers d and m, such that whenever $\mathbb{A}$ and $\mathbb{B}$ are (d, m)-equivalent structures where every point has degree at most f, then $\mathbb{A} \equiv^r_{FO} \mathbb{B}$.*

In [20] we proved that d-equivalence is actually enough to guarantee elementary equivalence in $FO(\mathbf{Q}_u)$, where $\mathbf{Q}_u$ is the set of all unary generalized quantifiers.

3.2. Theorem. ([20]) *Let r be a positive integer. There is a positive integer d, such that whenever $\mathbb{A}$ and $\mathbb{B}$ are d-equivalent structures, then $\mathbb{A} \equiv^r_{FO(\mathbf{Q}_u)} \mathbb{B}$.*

We consider now $(d, m, \mathbf{D}_n)$-equivalent structures and prove a similar result for $FO(\mathbf{D}_n)$. The following lemma is a key tool in the induction step in the proof of this result. It shows that in each round in an $(r, \mathbf{D}_n)$-game we can consider neighborhoods of smaller radius.

3.3. Lemma. *If $\mathbb{A}$ and $\mathbb{B}$ are $(d, m, \mathbf{D}_n)$-equivalent structures and $e < d$, then $\mathbb{A}$ and $\mathbb{B}$ are also $(e, m, \mathbf{D}_n)$-equivalent.*

Proof. Let π be an e-type. We say that a d-type τ *refines* π, $\tau \succ \pi$, if every point with d-type τ also has e-type π. Since $e < d$, every point $x \in T_{\mathbb{A},\pi}$ has a unique d-type τ that refines π. Consequently,

$$k_{\mathbb{A},\pi} = \sum_{\tau \succ \pi} k_{\mathbb{A},\tau} \quad \text{and} \quad k_{\mathbb{B},\pi} = \sum_{\tau \succ \pi} k_{\mathbb{B},\tau}\,.$$

If $\mathbb{A}$ and $\mathbb{B}$ are $(d, m, \mathbf{D}_n)$-equivalent structures, then $k_{\mathbb{A},\tau} \equiv k_{\mathbb{B},\tau} \pmod{n}$ for each $\tau \succ \pi$, and if $k_{\mathbb{A},\pi} < m$, then $k_{\mathbb{A},\tau} < m$ and $k_{\mathbb{A},\pi} = k_{\mathbb{B},\pi}$, i.e.

$$\min(k_{\mathbb{A},\pi}, m) = \min(k_{\mathbb{B},\pi}, m) \quad \text{and} \quad k_{\mathbb{A},\pi} \equiv k_{\mathbb{B},\pi} \pmod{n}.$$

Therefore $\mathbb{A}$ and $\mathbb{B}$ are also $(e, m, \mathbf{D}_n)$-equivalent. $\square$

We can now prove our combinatorial argument.

3.4. Theorem. *Let σ be a relational vocabulary and suppose r, f and n are positive integers. There are positive integers d and m, such that whenever $\mathbb{A}$ and $\mathbb{B}$ are $(d, m, \mathbf{D}_n)$-equivalent σ-structures where every point has degree at most f, then $\mathbb{A} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}$.*

Proof. Suppose (w.l.o.g) that $f \geq 2$. Let $d = 3^r$ and $m = r \cdot f^{d-1}$ and assume that σ-structures $\mathbb{A}$ and $\mathbb{B}$ are $(d, m, \mathbf{D}_n)$-equivalent where every point has degree at most f. We show that the duplicator can play in the $(r, \mathbf{D}_n)$-game over $\mathbb{A}$ and $\mathbb{B}$ so that after j rounds, where $j \leq r$, when points $a_1, \ldots, a_j \in A$ and $b_1, \ldots, b_j \in B$ have been chosen, the following condition holds:

$(*)_j$ $\theta_j : \mathbb{A}\restriction \bigcup_{i\leq j} N(3^{r-j}, a_i) \cong \mathbb{B}\restriction \bigcup_{i\leq j} N(3^{r-j}, b_i)$,
where θ_j is an isomorphism mapping a_i to b_i for $1 \leq i \leq j$.

This condition holds vacuously for $j = 0$. Suppose then it holds for $j < r$. We show that the duplicator can ensure that after the round $(j+1)$ in the $(r, \mathbf{D}_n)$-game, the condition holds also for $(j+1)$.

We need to check only the quantifier move (for the treatment of first-order moves, see [9]). Let the spoiler choose the structure $\mathbb{A}$ and a subset $X \subseteq A$ (the case, where the spoiler selects the structure $\mathbb{B}$, is symmetrical). Denote

$$N_{\mathbb{A}} = \bigcup_{i\leq j} N(2\cdot 3^{r-j-1}, a_i) \quad \text{and} \quad N_{\mathbb{B}} = \bigcup_{i\leq j} N(2\cdot 3^{r-j-1}, b_i).$$

We now describe the strategy for the duplicator to choose the set Y and verify that such a strategy exists. First, denote $X_\tau = T^X_{\mathbb{A},\tau}$ and $\overline{X}_\tau = K^X_{\mathbb{A},\tau}$. Notice that since every point has unique 3^{r-j-1}-type, we can write X as the disjoint union $\dot\bigcup_\tau X_\tau$. We now define sets Y_τ, for each 3^{r-j-1}-type τ. Let $Y_\tau = \theta_j[X_\tau \cap N_{\mathbb{A}}] \cup Z_\tau$, where

- if $X_\tau \subseteq N_{\mathbb{A}}$, then $Z_\tau = \emptyset$;
- if $X_\tau \setminus N_{\mathbb{A}} \neq \emptyset$ and $\overline{X}_\tau \setminus N_{\mathbb{A}} = \emptyset$ (that is, $X_\tau \setminus N_{\mathbb{A}} = T_{\mathbb{A},\tau} \setminus N_{\mathbb{A}}$), let $Z_\tau = T_{\mathbb{B},\tau} \setminus N_{\mathbb{B}}$;
- if $\overline{X}_\tau \setminus N_{\mathbb{A}} \neq \emptyset \neq X_\tau \setminus N_{\mathbb{A}}$, let $Z_\tau \subseteq T_{\mathbb{B},\tau} \setminus N_{\mathbb{B}}$ be a non-empty subset of minimal cardinality satisfying $|Z_\tau| \equiv |X_\tau \setminus N_{\mathbb{A}}| \pmod{n}$.

Finally, define $Y = \dot\bigcup_\tau Y_\tau$ where the disjoint union is taken over every 3^{r-j-1}-type τ.

Suppose τ is a 3^{r-j-1}-type and let ℓ_τ be the number of points in $N_{\mathbb{A}}$ with type τ. Because the condition $(*)_j$ holds, the number of points in $N_{\mathbb{B}}$ with 3^{r-j-1}-type τ is also ℓ_τ. Since $2\cdot 3^{r-j-1} < 3^r = d$, we have $2\cdot 3^{r-j-1} \leq d-1$. For each $i \leq j$, because every point has degree at most f, the number of points in $N(2\cdot 3^{r-j-1}, a_i)$ is at most $\sum_{k=0}^{d-2} f^k < f^{d-1}$. In j such neighborhoods there are less than $j \cdot f^{d-1} < r \cdot f^{d-1} = m$ points. Hence, in $N_{\mathbb{A}}$ (and in $N_{\mathbb{B}}$) there are less than m points, so $\ell_\tau < m$.

According to Lemma 3.3, $\mathbb{A}$ and $\mathbb{B}$ are also $(e, m, \mathbf{D}_n)$-equivalent, where $e = 3^{r-j-1}$. Therefore we know, that

$$T_{\mathbb{A},\tau} \setminus N_{\mathbb{A}} = \emptyset \quad \text{if and only if} \quad T_{\mathbb{B},\tau} \setminus N_{\mathbb{B}} = \emptyset \tag{1}$$

and

$$|T_{\mathbb{B},\tau} \setminus N_{\mathbb{B}}| \equiv |T_{\mathbb{A},\tau} \setminus N_{\mathbb{A}}| \pmod{n}.$$

Hence we can find the sets Z_τ as described in the definition of the sets Y_τ. Since these sets Z_τ have the same cardinality modulo n as the sets $X_\tau \setminus N_{\mathbb{A}}$, we have $|Y_\tau| \equiv |X_\tau| \pmod{n}$ for each 3^{r-j-1}-type τ and so $|Y| \equiv |X| \pmod{n}$.

Let the spoiler choose $b_{j+1} \in B$. Assume b_{j+1} has 3^{r-j-1}-type τ. If $b_{j+1} \in N_{\mathbb{B}}$, then $N(3^{r-j-1}, b_{j+1}) \subseteq \bigcup_{i\leq j} N(3^{r-j}, b_i)$ and the duplicator can choose $a_{j+1} \in N_{\mathbb{A}}$ such that $\theta_j(a_{j+1}) = b_{j+1}$. Obviously the condition $(*)_{j+1}$ holds with $\theta_{j+1} = \theta_j \restriction \bigcup_{i\leq j+1} N(3^{r-j-1}, a_i)$. Suppose then $b_{j+1} \notin N_{\mathbb{B}}$. If $b_{j+1} \in Z_\tau$, we have $Z_\tau \neq \emptyset$ and therefore $X_\tau \setminus N_{\mathbb{A}} \neq \emptyset$. Now choose a_{j+1} to be any point of $X_\tau \setminus N_{\mathbb{A}}$. Suppose finally $b_{j+1} \in K^Y_{\mathbb{B},\tau}$. According to the condition (1), we can find $a_{j+1} \in \overline{X}_\tau \setminus N_{\mathbb{A}}$. In either case we have

$$a_{j+1} \in X \quad \text{if and only if} \quad b_{j+1} \in Y.$$

If $b_{j+1} \notin N_{\mathbb{B}}$, then $\mathbb{B}\restriction\bigcup_{i\le j} N(3^{r-j-1}, b_i)$ contains no points adjacent to a point in $\mathbb{B}\restriction N(3^{r-j-1}, b_{j+1})$, and similarly in $\mathbb{A}$. Since a_{j+1} and b_{j+1} have the same 3^{r-j-1}-type, there is an isomorphism $\eta_{j+1} : N(3^{r-j-1}, a_{j+1}) \cong N(3^{r-j-1}, b_{j+1})$ that maps a_{j+1} to b_{j+1}. Hence also the condition $(*)_{j+1}$ holds with

$$\theta_{j+1} = \theta_j\restriction \bigcup_{i\le j} N(3^{r-j-1}, a_i) \ \cup\ \eta_{j+1}\restriction N(3^{r-j-1}, a_{j+1}).$$

In particular, after the last round we know that the condition $(*)_r$ holds. This means that

$$\mathbb{A}\restriction\{a_1, \ldots, a_r\} \cong \mathbb{B}\restriction\{b_1, \ldots, b_r\}$$

under an isomorphism mapping a_i to b_i, for $1 \le i \le r$. Hence the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over $\mathbb{A}$ and $\mathbb{B}$. According to Theorem 2.2, $\mathbb{A} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}$. $\square$

In general $(d, m, \mathbf{D}_n)$-equivalence does not give both sufficient and necessary condition for definability in $FO(\mathbf{D}_n)$. However, in the case, when there is an upper bound for the degrees of points in structures of a class, the definability of the class is completely characterized in this way.

3.5. Corollary. *Suppose n and f are positive integers. Let $\mathcal{C}$ be a class of finite σ-structures such that every point in a structure $\mathbb{A} \in \mathcal{C}$ has degree at most f. Then $\mathcal{C}$ is not definable in $FO(\mathbf{D}_n)$ if and only if for every positive integers d and m there are $(d, m, \mathbf{D}_n)$-equivalent σ-structures $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$.*

Proof. Suppose that for all positive integers d and m there are $(d, m, \mathbf{D}_n)$-equivalent σ-structures $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$. Assume on the contrary that a sentence φ of $FO(\mathbf{D}_n)$ defines the class $\mathcal{C}$ and $\mathrm{qr}(\varphi) = r$. Let d and m be given by Theorem 3.4 for these r, n and f and choose $(d, m, \mathbf{D}_n)$-equivalent structures $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$. According to Theorem 3.4 we have $\mathbb{A} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}$; this is a contradiction because of the definition of φ.

Assume then that there are positive integers d and m such that $\mathcal{C}$ is closed under $(d, m, \mathbf{D}_n)$-equivalence. For every d-type τ there is a formula $\varphi_\tau(x)$ such that for every point a in a structure $\mathbb{A} \in \mathcal{C}$ we have $\mathbb{A} \models \varphi_\tau(a)$ if and only if a has d-type τ. Let $\varphi^{d,m}_{\mathbb{A}}$ be a sentence of $FO(\mathbf{D}_n)$ that tells for every d-type τ the number of points in $\mathbb{A}$ with type τ, or that there are at least m points with type τ and the number of such points modulo n. That is, if the number of points in $\mathbb{A}$ with d-type τ is $k < m$, this can be expressed in $\varphi^{d,m}_{\mathbb{A}}$ by the subformula $\exists^{=k} y\varphi_\tau(y)$, and if there are at least m and $k \pmod n$ points with d-type τ, this can be expressed by $\exists^{\ge m} y\varphi_\tau(y) \wedge \psi^{k,n}_{\varphi_\tau}$, where $\psi^{k,n}_{\varphi_\tau}$ is the sentence defined in Section 2.1. Since every point in any structure $\mathbb{A} \in \mathcal{C}$ has degree at most f, there are less than f^d points in each d-type occuring in a structure $\mathbb{A} \in \mathcal{C}$, and therefore there are only finitely many different d-types. Hence there are also only finitely many different formulas $\varphi_\tau(x)$ (up to logical equivalence) satisfiable in $\mathcal{C}$. Thus $\varphi^{d,m}_{\mathbb{A}}$ is a sentence of $FO(\mathbf{D}_n)$ whenever $\mathbb{A} \in \mathcal{C}$. By the same argument it also follows that there are only finitely many different formulas $\varphi^{d,m}_{\mathbb{A}}$ (up to logical equivalence), where $\mathbb{A} \in \mathcal{C}$. Let ψ_f be a sentence saying that every point has degree at most f. Now the sentence

$$\psi_f \wedge \bigvee_{\mathbb{A}\in\mathcal{C}} \varphi^{d,m}_{\mathbb{A}}$$

characterizes the class $\mathcal{C}$. Namely, obviously every $\mathbb{A} \in \mathcal{C}$ satisfies this sentence. On the other hand, if $\mathbb{B} \notin \mathcal{C}$ then either $\mathbb{B}$ has a point with degree more than f, or no structure $\mathbb{A} \in \mathcal{C}$ is $(d, m, \mathbf{D}_n)$-equivalent with $\mathbb{B}$. In the first case $\mathbb{B}$ does not satisfy ψ_f and in the second case $\mathbb{B}$ does not satisfy $\bigvee_{\mathbb{A}\in\mathcal{C}} \varphi_{\mathbb{A}}^{d,m}$. Hence $\mathcal{C}$ is definable in $FO(\mathbf{D}_n)$. $\square$

Note that in the case $n = 1$ this gives a characterization for first-order logic on classes of structures with points having a fixed bounded degree.

Suppose $\mathcal{C}$ is a class of finite structures. We say that $\mathcal{C}$ is *closed under disjoint unions*, if

$$\mathbb{A} \in \mathcal{C} \text{ and } \mathbb{B} \in \mathcal{C} \quad \text{implies} \quad \mathbb{A}\dot{\cup}\mathbb{B} \in \mathcal{C}.$$

The following observation is an easy consequence of the previous corollary. The notation $\overline{\mathcal{C}}$ is used for the class of σ-structures not in $\mathcal{C}$.

3.6. Corollary. *Let $\mathcal{C}$ be a class of finite σ-structures such that $\mathcal{C}$ and $\overline{\mathcal{C}}$ are closed under disjoint unions and every point in a structure $\mathbb{A} \in \mathcal{C}$ has degree at most f. If $\mathcal{C}$ is not definable in first-order logic, then $\mathcal{C}$ is not definable in $FO(\mathbf{D}_n)$, for any positive integer n.*

Proof. If $\mathcal{C}$ is not definable in first-order logic, according to Corollary 3.5 for every positive integers d and m there are (d, m)-equivalent structures $\mathbb{A} \in \mathcal{C}$ and $\mathbb{B} \notin \mathcal{C}$. For every d and m, choose $k \geq m$ divisible by n and consider structures obtained by taking k disjoint unions of $\mathbb{A}$ and $\mathbb{B}$

$$\mathbb{C} = \dot{\cup}_k \mathbb{A} \quad \text{and} \quad \mathbb{D} = \dot{\cup}_k \mathbb{B}.$$

For each d-type τ we have either $k_{\mathbb{C},\tau} = k_{\mathbb{D},\tau} = 0$ or $k_{\mathbb{C},\tau} \geq m$ and $k_{\mathbb{D},\tau} \geq m$ and

$$k_{\mathbb{C},\tau} \equiv 0 \pmod n \quad \text{and} \quad k_{\mathbb{D},\tau} \equiv 0 \pmod n.$$

Since $\mathcal{C}$ and $\overline{\mathcal{C}}$ are closed under disjoint unions, we have $\mathbb{C} \in \mathcal{C}$ and $\mathbb{D} \notin \mathcal{C}$. Hence for every d and m there are $(d, m, \mathbf{D}_n)$-equivalent structures $\mathbb{C} \in \mathcal{C}$ and $\mathbb{D} \notin \mathcal{C}$. The claim now follows from Corollary 3.5. $\square$

Hence in the case of any such class $\mathcal{C}$, undefinability in first-order logic gives undefinability also in $FO(\mathbf{D}_n)$. Subclasses, where every point has a bounded degree, of the class of planar graphs, of the class of 3-colorable graphs and the class of finite graphs that contain a cycle, are examples of such $\mathcal{C}$.

4. Weakness of counting modulo with linear order

Our main interest concerns inexpressibility results on ordered structures. We show that counting modulo quantifiers are not strong enough to compare cardinalities. Certain divisibility properties of word models and connectivity of ordered graphs are also proved not to be definable in $FO(\mathbf{D}_n)$.

When a linear order is present, in the Gaifman graph each point is adjacent to any other point. Therefore Theorems 3.1, 3.2 and 3.4 apply only in the trivial case, when the linearly ordered structures are isomorphic. In fact, Theorem 3.2 is based on bijective Ehrenfeucht-Fraïssé games introduced by Hella [13, 14], and these games cannot be applied to get non-definability results in the presence of a linear order. A similar phenomenon can also be seen in many other extensions of first-order Ehrenfeucht-Fraïssé games, such as the infinite pebble game for the infinitary logic $L^{\omega}_{\infty\omega}$ (see e.g. [8, Chapter 2]).

We solve this problem by requiring that in structures $\mathbb{A}^{\leqslant}$ all neighborhoods $N(d,a)$ are instead defined as neighborhoods in $\mathbb{A}$, i.e. the linear order $\leqslant$ is not taken into account in the definition of the neighborhoods.

First we consider disjoint union of ordered structures. Suppose that $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ are ordered σ-structures. Consider the ordered $\sigma\dot\cup\{F,L\}$-structure $\mathbb{C}^{\leqslant} = \mathbb{A}^{\leqslant} \triangleleft \mathbb{B}^{\leqslant}$ obtained as the disjoint union $\mathbb{A}^{\leqslant}\dot\cup\mathbb{B}^{\leqslant}$ with the natural ordering and the interpretations $F(\mathbb{C}^{\leqslant}) = A$ and $L(\mathbb{C}^{\leqslant}) = B$. First we show that taking disjoint unions preserves winning strategy of the duplicator in the $(r, \mathbf{D}_n)$-game.

4.1. Proposition. *Let n and r be positive integers. Suppose that the duplicator has a winning strategy in the $(r,\mathbf{D}_n)$-game over the ordered structures $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ and the structures $\mathbb{C}^{\leqslant}$ and $\mathbb{D}^{\leqslant}$. Then the duplicator has a winning strategy in the $(r,\mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant}$ and $\mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant}$. Especially $\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant}$.*

Proof. We show that the duplicator has a winning strategy in the $(r,\mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant}$ and $\mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant}$ by using the winning strategies ν_1 and ν_2 of the duplicator in the support $(r,\mathbf{D}_n)$-games over the structures $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ and the structures $\mathbb{C}^{\leqslant}$ and $\mathbb{D}^{\leqslant}$. Answers in ν_1 and ν_2 are used to build the desired answers of the duplicator in the $(r,\mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant}$ and $\mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant}$.

More precisely, assume as an induction hypothesis that after the round j, where $j \le r$, the duplicator has played according to his winning strategy and

$$\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant} \restriction \{x_1,\ldots,x_j\} \cong \mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant} \restriction \{y_1,\ldots,y_j\}.$$

Let the spoiler choose a subset $X \subseteq A\dot\cup C$. Consider the disjoint subsets $X \cap A$ and $X \cap C$. Let $Y_1 \subseteq B$ be given by ν_1, when in the $(r,\mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ the points $\{x_i \mid x_i \in A \text{ and } i \le j\}$ are chosen and the spoiler selects the subset $X \cap A$. Similarly, let $Y_2 \subseteq D$ be the subset given by ν_2 when the spoiler selects $X \cap C$. Now the duplicator can choose the subset $Y_1\dot\cup Y_2 \subseteq B\dot\cup D$. Since $|Y_1| \equiv |X \cap A| \pmod n$ and $|Y_2| \equiv |X \cap C| \pmod n$ and $Y_1 \cap Y_2 = \emptyset$, we have $|Y| \equiv |X| \pmod n$.

Let the spoiler choose $y_{j+1} \in B\dot\cup D$. Suppose $y_{j+1} \in B$. Then the duplicator can choose an element $x_{j+1} \in A$ given by the winning strategy ν_1, when the spoiler selects $y_{j+1} \in B$ in the support game. Similarly, if $y_{j+1} \in D$, the winning strategy ν_2 can be used to choose $x_{j+1} \in C$. According to the described strategy, we have $x_{j+1} \in X \iff y_{j+1} \in Y$ and

$$\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant} \restriction \{x_1,\ldots,x_{j+1}\} \cong \mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant} \restriction \{y_1,\ldots,y_{j+1}\}.$$

After the last round, we have

$$\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant} \restriction \{x_1,\ldots,x_r\} \cong \mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant} \restriction \{y_1,\ldots,y_r\}$$

and therefore the duplicator has a winning strategy in the $(r,\mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant} \triangleleft \mathbb{C}^{\leqslant}$ and $\mathbb{B}^{\leqslant} \triangleleft \mathbb{D}^{\leqslant}$. The second claim follows now from Theorem 2.2. □

Many of our counterexamples are sufficiently large linear orders with two unary predicates defined on them. When only unary predicates are present, for every positive integer

d we have $N(d,a) = \{a\}$. Thus no point b different from a belongs to $N(d,a)$, and moreover $N(d,a)$ and $N(d,b)$ are disjoint; this makes considerations easier. In the following we show that sufficiently large and of modulo n equal length linear orders cannot be distinguished in $FO(\mathbf{D}_n)$.

4.2. Proposition. *Let n and r be positive integers. There is a positive integer k such that the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over the linear orders $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ of length sk and tk, for every $s, t > 0$. Especially we have $\mathbb{A}^{\leqslant} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{B}^{\leqslant}$.*

Proof. Define $k = 2^r \cdot n^{r+1}$. Let $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ be the linear orders of length sk and tk, where $s, t > 0$. We show that the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$. Denote $A = [u_1, u_2]$ and $B = [v_1, v_2]$. We prove by induction, that after the round j, where $j \leq r$, when points $a_1, \ldots, a_j \in A$ and $b_1, \ldots, b_j \in B$ have been chosen and $h_j = 2^{r-j} \cdot n^{r-j+1}$, the following conditions $(*)_j$ hold:
for every i and i', where $1 \leq i, i' \leq j$,

- $a_i \leqslant a_{i'}$ if and only if $b_i \leqslant b_{i'}$;
- for $k = 1, 2$, $|a_i - u_k| = |b_i - v_k|$ or
$(|a_i - u_k| > h_j$ and $|b_i - v_k| > h_j$ and $|b_i - v_k| \equiv |a_i - u_k| \pmod{n^{r-j+1}})$;
- $|a_i - a_{i'}| = |b_i - b_{i'}|$ or
$(|a_i - a_{i'}| > h_j$ and $|b_i - b_{i'}| > h_j$ and $|b_i - b_{i'}| \equiv |a_i - a_{i'}| \pmod{n^{r-j+1}})$.

These conditions hold vacuously for $j = 0$. Suppose then they hold for $j < r$ and the spoiler decides to choose a subset $X \subseteq A_1$. We now describe a strategy for the duplicator to choose the set Y. Denote

$$N_{\mathbb{A}} = \{a_i \mid 1 \leq i \leq j\} \quad \text{and} \quad N_{\mathbb{B}} = \{b_i \mid 1 \leq i \leq j\}.$$

According to the conditions $(*)_j$,

$$\mathbb{A} \smallsetminus N_{\mathbb{A}} = \dot{\bigcup}_t [c_t, d_t] \quad \text{and} \quad \mathbb{B} \smallsetminus N_{\mathbb{B}} = \dot{\bigcup}_t [c'_t, d'_t]$$

such that for every t and $k = 1, 2$,

- $|d_t - c_t| = |d'_t - c'_t|$ or
$(|d_t - c_t| > h_j$ and $|d'_t - c'_t| > h_j$ and $|d'_t - c'_t| \equiv |d_t - c_t| \pmod{n^{r-j+1}})$;
- $|c_t - u_k| = |c'_t - v_k|$ or
$(|c_t - u_k| > h_j$ and $|c'_t - v_k| > h_j$ and $|c'_t - v_k| \equiv |c_t - u_k| \pmod{n^{r-j+1}})$;
- $|u_k - d_t| = |v_k - d'_t|$ or
$(|u_k - d_t| > h_j$ and $|v_k - d'_t| > h_j$ and $|v_k - d'_t| \equiv |u_k - d_t| \pmod{n^{r-j+1}})$.

If $[u, v]$ is an interval and h is a positive integer, we denote

$$C([u,v], h) = \{a \in [u,v] \mid |a - u| > h \text{ and } |v - a| > h\}.$$

For every t, there is a bijection

$$f_t : ([c_t, d_t] \smallsetminus C([c_t, d_t], h_{j+1})) \to ([c'_t, d'_t] \smallsetminus C([c'_t, d'_t], h_{j+1}))$$

that preserves the distances at the initial and final segments of the intervals $[c_t, d_t]$ and $[c'_t, d'_t]$. That is, for every $a \in [c_t, d_t]$, if $|a - c_t| \leq h_{j+1}$, then $f_t(a)$ is the unique $b \in [c'_t, d'_t]$ such that $|b - c'_t| = |a - c_t|$, and if $|d_t - a| \leq h_{j+1}$, $f_t(a)$ is the unique $b \in [c'_t, d'_t]$ such that $|d'_t - b| = |d_t - a|$.

For each t, define $X_t = \{a \in [c_t, d_t] \mid a \in X\}$. The set Y can now be defined as the union

$$\{b_i \mid a_i \in X\} \cup \dot{\cup}_t Y_t,$$

where the sets $Y_t \subseteq [c'_t, d'_t]$ are defined in the following way:

- For every $b \in [c'_t, d'_t] \smallsetminus C([c'_t, d'_t], h_{j+1})$, let $b \in Y_t$ if and only if $a \in X_t$ for the unique $a \in [c_t, d_t] \smallsetminus C([c_t, d_t], h_{j+1})$ such that $f_t(a) = b$.
- Suppose then $C([c_t, d_t], h_{j+1}) \neq \emptyset$ and $C([c'_t, d'_t], h_{j+1}) \neq \emptyset$. For every $k < n^{r-j}$,
  - if every $a \in C([c_t, d_t], h_{j+1})$ with $|a - c_t| \equiv k \pmod{n^{r-j}}$ belongs to X_t, then every $b \in C([c'_t, d'_t], h_{j+1})$ with $|b - c'_t| \equiv k \pmod{n^{r-j}}$ belongs to Y_t;
  - if no $a \in C([c_t, d_t], h_{j+1})$ with $|a - c_t| \equiv k \pmod{n^{r-j}}$ belongs to X_t, then no $b \in C([c'_t, d'_t], h_{j+1})$ with $|b - c'_t| \equiv k \pmod{n^{r-j}}$ belongs to Y_t;
  - otherwise, let $l \pmod{n}$ points $a \in C([c_t, d_t], h_{j+1})$ with $|a - c_t| \equiv k \pmod{n^{r-j}}$ belong to X_t. Then the duplicator selects $l \pmod{n}$ points $b \in C([c'_t, d'_t], h_{j+1})$ with $|b - c'_t| \equiv k \pmod{n^{r-j}}$ to the set Y_t.

According to the conditions above the sets

$$[c_t, d_t] \smallsetminus C([c_t, d_t], h_{j+1}) \quad \text{and} \quad [c'_t, d'_t] \smallsetminus C([c'_t, d'_t], h_{j+1})$$

are of the same cardinality and the sets $C([c_t, d_t], h_{j+1})$ and $C([c'_t, d'_t], h_{j+1})$ are of the same cardinality modulo n^{r-j+1}. Because $h_j = 2^{r-j} \cdot n^{r-j+1}$, we have furthermore

$$C([c_t, d_t], h_{j+1}) \neq \emptyset \quad \text{if and only if} \quad C([c'_t, d'_t], h_{j+1}) \neq \emptyset. \tag{2}$$

Therefore we can find the sets Y_t as described above. It follows from the construction of these sets that $|Y_t| \equiv |X_t| \pmod{n}$ and so $|Y| \equiv |X| \pmod{n}$.

Let the spoiler choose a point $b_{j+1} \in B$. If $b_{j+1} = b_i$ for some $1 \leq i \leq j$, then the duplicator can choose $a_{j+1} = a_i$. Suppose then that $b_{j+1} \in [c'_t, d'_t]$ for some t. If we have $b_{j+1} \in [c'_t, d'_t] \smallsetminus C([c'_t, d'_t], h_{j+1})$, the duplicator can choose the unique $a_{j+1} \in [c_t, d_t] \smallsetminus C([c_t, d_t], h_{j+1})$ that satisfies $f_t(a_{j+1}) = b_{j+1}$.

Suppose then $b_{j+1} \in C([c'_t, d'_t], h_{j+1})$. If $b_{j+1} \in Y$, the duplicator can choose a_{j+1} to be any point in $C([c_t, d_t], h_{j+1})$ with $|b_{j+1} - c'_t| \equiv |a_{j+1} - c_t| \pmod{n^{r-j}}$ such that $a_{j+1} \in X$. In the case $b_{j+1} \notin Y$, there is a point $a \in C([c_t, d_t], h_{j+1})$ with $|a - c_t| \equiv |b_{j+1} - c'_t| \pmod{n^{r-j}}$ such that $a \notin X$ and the duplicator can choose a_{j+1} to be such a point. In either case we have

$$a_{j+1} \in X \quad \text{if and only if} \quad b_{j+1} \in Y.$$

Since in the end $\mathbb{A}^{\leqslant}\lceil\{a_1,\ldots,a_r\} \cong \mathbb{B}^{\leqslant}\lceil\{b_1,\ldots,b_r\}$ under an isomorphism $a_i \mapsto b_i$, for $1 \le i \le r$, the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over the structures $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$. The second claim now follows from Theorem 2.2. □

We use a special notation for linear orders with two unary predicates defined on them. Let $\mathbb{A}^{\leqslant}$ be the linear order of length sk and $\mathbb{B}^{\leqslant}$ the linear order of length tk. We define $\mathbb{A}^{\leqslant}_{(s,t)k} = \mathbb{A}^{\leqslant} \triangleleft \mathbb{B}^{\leqslant}$. For our applications we state the following corollary.

4.3. Corollary. *Let n be a positive integer. Suppose that $\mathcal{C}^{\leqslant}$ is a class of ordered σ-structures, where $\sigma = \{P, S\}$ and P and S are unary. If for every positive integer k there are s_i and t_i, where $s_i, t_i > 0$ for $i = 1, 2$, such that $\mathbb{A}^{\leqslant}_{(s_1,t_1)k} \in \mathcal{C}^{\leqslant}$ and $\mathbb{A}^{\leqslant}_{(s_2,t_2)k} \notin \mathcal{C}^{\leqslant}$, then $\mathcal{C}^{\leqslant}$ is not definable in $FO(\mathbf{D}_n)$.*

Proof. Towards a contradiction, suppose that φ is a sentence of $FO(\mathbf{D}_n)$ that defines the class $\mathcal{C}^{\leqslant}$, possibly using the linear order $\leqslant$. Let $\mathrm{qr}(\varphi) = r$ and let k be given by Proposition 4.2 for these r and n. Suppose $\mathbb{A}^{\leqslant}_{(s_1,t_1)k} \in \mathcal{C}^{\leqslant}$ and $\mathbb{A}^{\leqslant}_{(s_2,t_2)k} \notin \mathcal{C}^{\leqslant}$ for some positive integers s_i and t_i, $i = 1, 2$. According to Proposition 4.2, the duplicator has a winning strategy over the linear orders $\mathbb{A}^{\leqslant}_1$ and $\mathbb{A}^{\leqslant}_2$ of length s_1k and s_2k and over the linear orders $\mathbb{B}^{\leqslant}_1$ and $\mathbb{B}^{\leqslant}_2$ of length t_1k and t_2k. Since $\mathbb{A}^{\leqslant}_{(s_i,t_i)k} = \mathbb{A}^{\leqslant}_i \triangleleft \mathbb{B}^{\leqslant}_i$, for $i = 1, 2$, we know by Proposition 4.1, that $\mathbb{A}^{\leqslant}_{(s_1,t_1)k} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{A}^{\leqslant}_{(s_2,t_2)k}$. This is a contradiction because of the definition of φ. □

Well-known unary quantifiers, which are not first-order definable, are the *Rescher quantifier*

$$\mathbf{R} = \{(A, P, S) \mid |P| \le |S|\}$$

and the *Härtig quantifier*

$$\mathbf{H} = \{(A, P, S) \mid |P| = |S|\}.$$

These quantifiers are considered as classes of structures $\mathbb{A}$ with universe A and two subsets $P, S \subseteq A$ on the universe. Hence with these quantifiers it is possible to compare cardinalities of sets, which increases considerably the expressive power of first-order logic. For more detailed discussion, see [16, 17, 22]. We show that these quantifiers are not definable in $FO(\mathbf{D}_n)$, for any positive integer n, even with built-in linear order.

4.4. Theorem. *The Rescher and the Härtig quantifiers are not definable in $FO(\mathbf{D}_n)$, for any n, even with built-in linear order.*

Proof. Suppose n and k are positive integers. Choose $\mathbb{A}^{\leqslant}_{\mathbf{R}} = \mathbb{A}^{\leqslant}_{(1,2)k}$ and $\mathbb{B}^{\leqslant}_{\mathbf{R}} = \mathbb{A}^{\leqslant}_{(2,1)k}$. Then $\mathbb{A}^{\leqslant}_{\mathbf{R}} \in \mathbf{R}$ but $\mathbb{B}^{\leqslant}_{\mathbf{R}} \notin \mathbf{R}$. The case for the Härtig quantifier can be proved similarly, with counterexamples $\mathbb{A}^{\leqslant}_{\mathbf{H}} = \mathbb{A}^{\leqslant}_{(1,1)k}$ and $\mathbb{B}^{\leqslant}_{\mathbf{H}} = \mathbb{A}^{\leqslant}_{(2,1)k}$. Undefinability of these quantifiers now follows from Corollary 4.3. □

4.1. Word models

Consider the alphabet $\{0,1\}$ and the vocabulary $\{P_0, P_1\}$, where P_0 and P_1 are unary. Recall that $\{0,1\}^+$ is the set of non-empty words over $\{0,1\}$ and for $w \in \{0,1\}^+$, $|w|$ is the length of w and w_i the i'th bit of w. The word model corresponding to the word w

is the ordered structure $\mathbb{A}_w^{\leqslant} = (A, P_0, P_1)$, where the cardinality of A equals the length of w, and for $i = 0, 1$,

$$P_i = \{a \in A \mid \text{ for some } j,\, a \text{ is the } j\text{'th element w.r.t. } \leqslant \text{ and } w_j = i\}.$$

Note that models in the previous subsection can be seen as word models.

The *majority language* is defined as

$$maj = \{w \in \{0,1\}^+ \mid \sum_{i=0}^{|w|-1} w_i \geq \frac{|w|}{2}\}.$$

This language has been of great interest in the research of low level complexity classes. Barrington [3] conjectured that maj is not in ACC; this conjecture, if true, would imply that $ACC \neq NC^1$.

We show in this paper that maj is not definable in $FO(\mathbf{D}_n)$, for any n; i.e. we show that $\mathcal{C}_{maj}^{\leqslant} = \{\mathbb{A}_w^{\leqslant} \mid w \in maj\}$ is not definable in $FO(\mathbf{D}_n)$.

4.5. Theorem. *The majority language maj is not definable in $FO(\mathbf{D}_n)$ for any positive integer n.*

Proof. Suppose n and k are positive integers. Consider words $w, w' \in \{0,1\}^+$, where $|w| = 2k$ and $|w'| = 3k$ and

$$w_i = \begin{cases} 1 & \text{for } i < k, \\ 0 & \text{for } i \geq k; \end{cases}$$

and

$$w'_i = \begin{cases} 1 & \text{for } i < k, \\ 0 & \text{for } i \geq k. \end{cases}$$

Then $w \in maj$ but $w' \notin maj$ and therefore $\mathbb{A}_w^{\leqslant} \in \mathcal{C}_{maj}^{\leqslant}$ and $\mathbb{A}_{w'}^{\leqslant} \notin \mathcal{C}_{maj}^{\leqslant}$. Since $\mathbb{A}_w^{\leqslant} = \mathbb{A}_{(1,1)k}^{\leqslant}$ and $\mathbb{A}_{w'}^{\leqslant} = \mathbb{A}_{(1,2)k}^{\leqslant}$, the claim now follows from Corollary 4.3. □

Similarly we can consider classes where the input sums and the lengths are congruent to 0 modulo p:

$$length(p) = \{w \in \{0,1\}^+ \mid |w| \equiv 0 \pmod{p}\} \quad \text{and}$$

$$sum(p) = \{w \in \{0,1\}^+ \mid \textstyle\sum_{i=0}^{|w|-1} w_i \equiv 0 \pmod{p}\}.$$

Compton and Straubing [6] were interested in the class $sum(p)$ and its definability in FO with extra predicates, without using the results of Ajtai [2] and Furst, Saxe and Sipser [10]. Proposition 4.2 gives the following answer (in the presence of linear order).

4.6. Theorem. *Suppose p and n are positive integers and $n > 1$. If p has a prime factor that does not divide n, then*

- *$sum(p)$ is not definable in $FO(\mathbf{D}_n)$;*
- *$length(p)$ is not definable in $FO(\mathbf{D}_n)$.*

Proof. Suppose on the contrary that a sentence φ of $FO(\mathbf{D}_n)$ defines the class $sum(p)$, possibly using the order $\leqslant$, and $\mathrm{qr}(\varphi) = r$. Let k be the multiple of n given by Proposition 4.2 for these r and n, and let q be a prime factor of p that does not divide n. Define

$$l = \min\{t \geq k \mid t \equiv 0 \pmod{k} \text{ and } \gcd(t, q) = 1\}.$$

Consider then words $w, w' \in \{0,1\}^+$ of length lp and l, where $w_i = 1$ for $i < lp$ and $w'_i = 1$ for $i < l$. Obviously $w \in sum(p)$ but since $\gcd(l, q) = 1$, $w' \notin sum(p)$. Since l is a multiple of k, $\mathbb{A}_w^{\leqslant} \equiv^r_{FO(\mathbf{D}_n)} \mathbb{A}_{w'}^{\leqslant}$ by Proposition 4.2. This a contradiction because of the definition of φ. Hence $sum(p)$ is not definable in $FO(\mathbf{D}_n)$. The proof of the second claim is verbatim the same with $sum(p)$ replaced by $length(p)$. □

4.7. Remark. Since languages definable in $FO(\mathbf{D}_n)$ are known to be regular, the undefinability of the majority language, as well as the undefinability of the Rescher and Härtig quantifiers, can be easily verified also by a pumping lemma argument. However, note that for languages $sum(p)$ and $length(p)$ the pumping lemma argument does not apply, since these languages are regular.

This result enables us to prove a characterization, when the logic $FO(\mathbf{D}_n)$ is at most as strong as the logic $FO(\mathbf{D}_m)$ on ordered structures, where n and m are positive integers. First notice that the following observation holds even without order.

4.8. Lemma. *If* $\gcd(n, m) = 1$*, then* $FO(\mathbf{D}_n, \mathbf{D}_m) \equiv FO(\mathbf{D}_{nm})$.

Proof. Suppose $\varphi(x)$ is a formula. If $\gcd(n, m) = 1$, the number of points that satisfy φ is divisible by nm if and only if the number of such points is divisible by both n and m. But then $\mathbf{D}_n x\varphi(x) \wedge \mathbf{D}_m x\varphi(x)$ expresses that there are $0 \pmod{nm}$ points that satisfy φ. The converse direction is already established in Section 2.1. □

On ordered structures the logic $FO(\mathbf{D}_n)$ is as strong as the logic $FO(\mathbf{D}_{n^i})$.

4.9. Proposition. *Let* n*,* i *and* j *be positive integers. On ordered structures we have* $FO(\mathbf{D}_n) \equiv FO(\mathbf{D}_{n^i})$*, and especially* $FO(\mathbf{D}_{n^i}) \equiv FO(\mathbf{D}_{n^j})$.

Proof. According to Theorem 2.1, we know that even without built-in linear order, $FO(\mathbf{D}_n) \leq FO(\mathbf{D}_{n^i})$. We show by induction that on ordered structures also the converse holds.

The claim is obvious for $k = 1$. Suppose then it holds for $k < i$ and let $\varphi(x)$ be a formula. Consider the following sentence ψ:

$$\psi = \mathbf{D}_n x\varphi(x) \wedge \mathbf{D}_{n^k} x\left(\varphi(x) \wedge \mathbf{D}_n y(y \leqslant x \wedge \varphi(y))\right).$$

Then ψ holds if and only if the number of points that satisfy φ is divisible by n^{k+1}. According to the induction hypothesis, ψ is equivalent to a sentence of $FO(\mathbf{D}_n)$. Especially for every positive integers i and j, we have

$$FO(\mathbf{D}_{n^i}) \equiv FO(\mathbf{D}_n) \equiv FO(\mathbf{D}_{n^j}).$$

□

We can now prove the following characterization[1].

[1] This characterization was shown to me by Kerkko Luosto.

4.10. Theorem. *Let n and m be positive integers. Then $FO(\mathbf{D}_n) \leq FO(\mathbf{D}_m)$ if and only if the prime factors of n are also the prime factors of m.*

Proof. Suppose n has a prime factor that is not a prime factor of m. According to Theorem 4.6, $length(n)$ is not definable in $FO(\mathbf{D}_m)$ whereas $length(n)$ is obviously definable in $FO(\mathbf{D}_n)$. Therefore $FO(\mathbf{D}_n) \not\leq FO(\mathbf{D}_m)$.

Let P_n be the set of prime factors of n and P_m the set of prime factors of m, and suppose $P_n \subseteq P_m$. Since for every $p, q \in P_n$ we have $\gcd(p,q) = 1$, then on ordered structures $FO(\mathbf{D}_n) \equiv FO(\mathcal{D}_n)$ by Propositions 4.8 and 4.9, where $\mathcal{D}_n = \{\mathbf{D}_p \mid p \in P_n\}$. Correspondingly, $FO(\mathbf{D}_m) \equiv FO(\mathcal{D}_m)$, where $\mathcal{D}_m = \{\mathbf{D}_p \mid p \in P_m\}$. Because on ordered structures $FO(\mathbf{D}_{p^i}) \equiv FO(\mathbf{D}_{p^j})$ for positive integers i and j, thus $FO(\mathbf{D}_n) \leq FO(\mathbf{D}_m)$. □

4.2. Connectivity of graphs

Recall that connectivity of graphs is not definable in first-order logic even with built-in linear order. Gurevich [11] proved this by showing that the class of linear orders of even length is not definable in *FO* and reducing the connectivity of ordered graphs to this problem. We can get a similar result for $FO(\mathbf{D}_n)$ by modifying this proof.

First of all, we observe that the class of linear orders of length divisible by $n+1$ is not definable in $FO(\mathbf{D}_n)$ (a slightly more general result will be proved in the next section). Denote the class of such linear orders by

$$\mathcal{C}^{\leqslant}_{n+1} = \{\mathbb{A}^{\leqslant} \mid |A| \equiv 0 \pmod{(n+1)}\}.$$

Since for every positive integer n, $n+1$ has a prime factor that does not divide n, the following lemma is a restatement of Theorem 4.6 for $length(n+1)$.

4.11. Lemma. *The class of linear orders of length divisible by $n+1$ is not definable in $FO(\mathbf{D}_n)$.*

Connectivity of graphs can now be reduced to this problem by modifying the proof in [11].

4.12. Theorem. *Connectivity of graphs is not definable in $FO(\mathbf{D}_n)$ even with built-in linear order.*

Proof. Suppose on the contrary, that a sentence φ of $FO(\mathbf{D}_n)$ with linear order $\leqslant$ defines the class $\mathcal{C}^{\leqslant} = \{\mathbb{B}^{\leqslant} \mid \mathbb{B} = (B, E)$ is a connected graph $\}$. Consider the sentence ψ obtained when every occurrence of xEy in φ is replaced by

'y is the $(n+1)$'th successor of x, or
x is the first element and y is the second element, or
x is the second element and y is the third element, or $\ldots$,or
x is the $(n-1)$'th element and y is the n'th element, or
x is the last element and y is the first element.'

The ordered graph $\mathbb{B}^{\leqslant}$ in a linear order $\mathbb{A}^{\leqslant}$ defined in this way consists of $n+1$ paths and the first elements of the first $n-1$ paths are connected to the first element of the next path. Since the last element is connected to the first element, the last path is connected to the other paths if and only if $\mathbb{A}^{\leqslant}$ has length divisible by $n+1$. Hence $\mathbb{B}^{\leqslant}$ is connected if and only if $\mathbb{A}^{\leqslant} \in \mathcal{C}^{\leqslant}_{n+1}$. Therefore ψ is a sentence of $FO(\mathbf{D}_n)$ which with the linear order $\leqslant$ defines the class $\mathcal{C}^{\leqslant}_{n+1}$. This is a contradiction according to Lemma 4.11. □

5. Complete trees

Consider the logic $FO(\mathbf{D}_n)$ with built-in linear order augmented with the extra predicate $y = nx$. We show that this logic is not strong enough to express that the cardinality of a model is divisible by $n+1$. This solves the conjecture of Niwiński and Stolboushkin [19].

Consider first an ordered complete n-ary tree $\mathbb{A}^{\leqslant} = (A, E)$, where E denotes the usual edge relation. The *height* $h(a)$ of a point $a \in A$ is its distance from the root, that is, the root has height 0, its direct descendants have height 1, and so on. Since $\mathbb{A}^{\leqslant}$ is complete, each leaf has the same height. The *depth* $d(a)$ of a is the least distance of a from a leaf. The linear order $\leqslant$ orders nodes of A starting from the root, and going from left to right within nodes of the same height, and from the root to leaves.

Recall from the previous section that in structures $\mathbb{A}^{\leqslant}$ the neighborhoods $N(e,a)$ are defined as neigborhoods in $\mathbb{A}$. Observe that for every positive integer e and for every e-type τ, $T_{\mathbb{A}^{\leqslant},\tau} = [u,v]$ for some $u, v \in A$. This is because all points with the same height have the same e-type and moreover, all points $a \in \mathbb{A}$ such that $N(e,a)$ contains neither the root nor leaves, have the same e-type.

For every positive integer e and for every point $a \in A$ with e-type τ, we have $N(e,a) = \dot\bigcup_{i=1}^{t_\tau}[a_i, a'_i]$ such that $a_1 = a'_1$, and $h(a_i) = h(a'_i)$ for $1 \le i \le t_\tau$, and $h(a_{i+1}) = h(a_i)+1$ and $a'_i < a_{i+1}$ for $i < t_\tau$, and if $b \in A$ also has e-type τ, then $N(e,a) = \dot\bigcup_{i=1}^{t_\tau}[b_i, b'_i]$ such that for every $i \le t_\tau$, $|a'_i - a_i| = |b'_i - b_i|$.

Suppose that $a \in A$ has e-type τ and $b \in A$ has e-type π and $N(e,a) \cap N(e,b) = \emptyset$. Consider the set

$$L = \{i \mid \exists x \in [b_i, b'_i] \text{ such that } a'_j \leqslant x \leqslant a_{j+1} \text{ for some } j < t_\tau\}.$$

We say that a and b *k-match*, if $L \neq \emptyset$ and $k = |L|+1$; if $L = \emptyset$, then a and b do not match (or 0-match). If $a \leqslant b$ ($b \leqslant a$) and a and b k-match, then *a k-matches b from left (right)*. Note that if $N(e,a)$ and $N(e,b)$ contain neither the root nor leaves and $a \leqslant b$, then a t_τ-matches b from left, if $h(b) = h(a)$, or $h(b) = h(a)+1$ and for every $j \le t_\tau$ and $j' \le t_\pi = t_\tau$, if $h(a_j) = h(b_{j'})$, then $b'_{j'} \leqslant a_j$. If we play the $(r, \mathbf{D}_n)$-game over complete n-ary trees of different height, the duplicator cannot restrict himself to moves with the corresponding height as the spoiler's moves to win the game; otherwise the spoiler has an easy winning strategy. The concept of k-matching of points allows the duplicator play points with different heights.

For any $X \subseteq A$, we denote by $\mathbb{A}\lceil X$ the unordered substructure of $\mathbb{A}^{\leqslant}$ and the ordered substructure by $\mathbb{A}^{\leqslant}\lceil X$. Especially, for τ an e-type of a point $a \in A$, we define the *$e^{\leqslant}$-type* $\tau^{\leqslant}$ of the point a to be the isomorphism type of the ordered substructure $(\mathbb{A}^{\leqslant}\lceil N(e,a), a)$. For any points $a, b \in A$ such that $N(e,a)$ and $N(e,b)$ contain the root, a and b have the same $e^{\leqslant}$-type if and only if $a = b$. For the points, where $N(e,a)$ contains neither the root nor leaves, $e^{\leqslant}$-types behave periodically: a and b have the same $e^{\leqslant}$-type if and only if $|a-b| \equiv 0 \pmod{n^{e-1}}$. This is because the least point in $N(e,a)$ w.r.t $\leqslant$ is within distance $e-1$ from a and $(\mathbb{A}^{\leqslant}\restriction N(e,a), a)$ is determined by the information about the path, how a can be reached from this point. Similarly, for points a, where $N(e,a)$ contains a leaf, a point b with $h(b)=h(a)$ has the same $e^{\leqslant}$-type as a has if and only if $|a-b| \equiv 0 \pmod{n^{e-1}}$. Note also that if a and b have the same $e^{\leqslant}$-type and $f \leq e$, then a and b also have the same $f^{\leqslant}$-type.

We are now in the position to show that the height of complete n-ary trees is not expressible in $FO(\mathbf{D}_n)$.

5.1. Proposition. *Assume that n and r are positive integers. There is a positive integer k such that complete n-ary trees $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ of height at least k satisfy $\mathbb{A}^{\leqslant} \equiv^{r}_{FO(\mathbf{D}_n)} \mathbb{B}^{\leqslant}$.*

Proof. We again show that the duplicator has a winning strategy in the $(r,\mathbf{D}_n)$-game over $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$. Let $e=3^r$ and choose $k=4e$. Let $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ be complete n-ary trees of height at least k.

We show by induction, that after the round j, where $j \leq r$, when points $a_1,\ldots,a_j \in A$ and $b_1,\ldots,b_j \in B$ have been chosen, and $e_j = 3^{r-j}$ and $l_j = 2^{r-j}\cdot n^{e_j-1}$, the following conditions $(*)_j$ hold: for every i, i', where $1 \leq i, i' \leq j$,

(*i*) $\theta_j : \mathbb{A}^{\leqslant}\restriction \bigcup_{i\leq j} N(e_j,a_i) \cong \mathbb{B}^{\leqslant}\restriction \bigcup_{i\leq j} N(e_j,b_i)$,
where θ_j is an isomorphism mapping a_i to b_i;

(*ii*) for every $a \in N(e_j,a_i)$ and $a' \in N(e_j,a_{i'})$, $|a-a'| = |\theta_j(a)-\theta_j(a')|$ or $(|a-a'|>l_j$ and $|\theta_j(a)-\theta_j(a')|>l_j)$;

(*iii*)
- a_i and b_i have the same height or both have height at least $2e_j$;
- a_i and b_i have the same depth or both have depth at least $2e_j$;

(*iv*) for every $k \leq 2e_j-1$, a_i k-matches $a_{i'}$ from left (right) if and only if b_i k-matches $b_{i'}$ from left (right);

(*v*) for τ an e_j-type such that $T_{\mathbb{A}^{\leqslant},\tau}=[u,v]$ and $T_{\mathbb{B}^{\leqslant},\tau}=[u',v']$, and for $j<r$

$$N_{\mathbb{A}} = \bigcup_{i\leq j} N(2\cdot e_{j+1},a_i) \quad \text{and} \quad N_{\mathbb{B}} = \bigcup_{i\leq j} N(2\cdot e_{j+1},b_i),$$

if

$$T_{\mathbb{A}^{\leqslant},\tau} \setminus N_{\mathbb{A}} = \dot{\bigcup}_t [u_t,v_t] \quad \text{and} \quad T_{\mathbb{B}^{\leqslant},\tau} \setminus N_{\mathbb{B}} = \dot{\bigcup}_t [u'_t,v'_t],$$

then for every t,

- $|v_t-u_t| = |v'_t-u'_t|$ or
- $|v_t-u_t|>l_j$ and $|v'_t-u'_t|>l_j$ and $|v'_t-u'_t| \equiv |v_t-u_t| \pmod{n}$.

Observe that it follows from the first condition that $a_i \leqslant a_{i'}$ if and only if $b_i \leqslant b_{i'}$ for every $1 \leq i, i' \leq j$. Obviously these conditions hold for $j=0$. Suppose then the conditions $(*)_j$ hold for $j<r$. Let the spoiler choose a subset $X = \dot{\bigcup}_{\tau^{\leqslant}} X_{\tau^{\leqslant}} \subseteq A$, where $X_{\tau^{\leqslant}} = T^{X}_{\mathbb{A}^{\leqslant},\tau^{\leqslant}}$. We describe a strategy for the duplicator to choose the set Y. Let $Y_{\tau^{\leqslant}} = \theta_j[X_{\tau^{\leqslant}} \cap N_{\mathbb{A}}] \cup Z_{\tau^{\leqslant}}$, where $Z_{\tau^{\leqslant}}$ is defined as follows:

Let $T_{\mathbb{A}^{\leqslant},\tau} = [u,v]$ and $T_{\mathbb{B}^{\leqslant},\tau} = [u',v']$ and

$$T_{\mathbb{A}^{\leqslant},\tau} \smallsetminus N_{\mathbb{A}} = \dot{\bigcup}_t [u_t, v_t] \quad \text{and} \quad T_{\mathbb{B}^{\leqslant},\tau} \smallsetminus N_{\mathbb{B}} = \dot{\bigcup}_t [u'_t, v'_t].$$

For $[c,d]$ an interval and l a positive integer, we denote

$$C([c,d],l) = \{x \in [c,d] \mid |x-c| > l \text{ and } |d-x| > l\}.$$

Let for every t

$$C_t = C([u_t,v_t], l_{j+1}) \quad \text{and} \quad C'_t = C([u'_t,v'_t], l_{j+1}).$$

For each t, there is a bijection

$$f_t : ([u_t,v_t] \smallsetminus C_t) \to ([u'_t,v'_t] \smallsetminus C'_t)$$

that preserves the distances at the initial and final segments of the intervals $[u_t,v_t]$ and $[u'_t,v'_t]$. More precisely, for every $a \in [u_t,v_t]$, if $|a-u_t| \le l_{j+1}$ then $f_t(a)$ is the unique $b \in [u'_t,v'_t]$ such that $|b-u'_t| = |a-u_t|$, and similarly, if $|v_t - a| \le l_{j+1}$, $f_t(a)$ is the unique $b \in [u'_t,v'_t]$ such that $|d'_t - b| = |d_t - a|$.

We say that $a \in A$ and $b \in B$ are *similar* for the positive integers e_{j+1} and l_{j+1} and the points $a_1,\dots,a_j \in A$ and $b_1,\dots,b_j \in B$, if a and b have the same $e^{\leqslant}_{j+1}$-type and for every $i \le j$ and $k \le 2e_{j+1}-1$, a k-matches a_i from left (right) if and only if b k-matches b_i from left (right) and for every $c \in N(e_{j+1},a)$ and $d \in N(e_{j+1},a_i)$, and for the corresponding points $c' \in B$, given by the isomorphism $\mathbb{A}^{\leqslant}\lceil N(e_{j+1},a) \cong \mathbb{B}^{\leqslant}\lceil N(e_{j+1},b)$, and $d' \in B$, where $d' = \theta_j(d)$, we have $|c-d| = |c'-d'|$ or ($|c-d| > l_{j+1}$ and $|c'-d'| > l_{j+1}$).

- For every $b \in [u'_t,v'_t] \smallsetminus C'_t$, let $b \in Z_{\tau^{\leqslant}}$ if and only if $a \in X_{\tau^{\leqslant}}$ for the unique $a \in [u_t,v_t] \smallsetminus C_t$ such that $f_t(a) = b$.
- Suppose then $C_t \neq \emptyset$ and $C'_t \neq \emptyset$.
  - If $T^{C_t}_{\mathbb{A}^{\leqslant},\tau^{\leqslant}} = X_{\tau^{\leqslant}} \cap C_t$, then $b \in Z_{\tau^{\leqslant}}$ for every $b \in T^{C'_t}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$.
  - If $X_{\tau^{\leqslant}} \cap C_t = \emptyset$, then no $b \in T^{C'_t}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ belongs to $Z_{\tau^{\leqslant}}$.
  - Otherwise, let $|X_{\tau^{\leqslant}} \cap C_t| \equiv l \pmod n$ and choose l distinct $b'_1,\dots b'_l \in T^{C'_t}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ such that for each i, where $1 \le i \le l$, b'_i and some $a \in X_{\tau^{\leqslant}} \cap C_t$ are similar for l_{j+1} and e_{j+1} and points $a_1,\dots,a_j$ and $b_1,\dots,b_j$; let $Z_{\tau^{\leqslant}} \cap C'_t = \{b'_1,\dots,b'_l\}$.
- If $h(b) < 2e_{j+1}$, then it also required that $h(a) = h(b)$, and if $d(b) < 2e_{j+1}$, then we also require that $d(a) = d(b)$.

Define $Y = \dot{\bigcup}_\tau Y_{\tau^{\leqslant}}$, where the union is taken over every $e^{\leqslant}_{j+1}$-type $\tau^{\leqslant}$.

According to the induction hypothesis, for every t the sets $[u_t,v_t] \smallsetminus C_t$ and $[u'_t,v'_t] \smallsetminus C'_t$ are of the same cardinality and the sets C_t and C'_t are of the same cardinality modulo n. Since $l_j = 2^{r-j} \cdot n^{e_j - 1}$, we have furthermore

$$C_t \neq \emptyset \quad \text{if and only if} \quad C'_t \neq \emptyset. \tag{3}$$

Since points with the same $e_j^{\leqslant}$-type have the same $e_{j+1}^{\leqslant}$-type and $e_{j+1}^{\leqslant}$-types behave periodically, it also follows from the conditions $(*)_j$, that every $a \in [u_t, v_t] \setminus C_t$ and $b \in [u_t', v_t'] \setminus C_t'$ have the same $e_{j+1}^{\leqslant}$-type. In the sets C_t and C_t' $e_{j+1}^{\leqslant}$-types behave again periodically, with period $n^{e_{j+1}-1}$.

According to the induction hypothesis, points a_i and $a_{i'}$, where $1 \leq i, i' \leq j$, k-match from left (right) for $k \leq 2e_j - 1$, if and only if b_i and $b_{i'}$ k-match from left (right). Therefore we know that if $a \in T^{C_t}_{\mathbb{A}^{\leqslant},\tau^{\leqslant}}$ k-matches from left (right) with some a_i, where $1 \leq i \leq j$ and $k \leq 2e_{j+1} - 1$, there is $b \in T^{C_t'}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ that k-matches from left (right) with b_i. If $a \in T^{C_t}_{\mathbb{A}^{\leqslant},\tau^{\leqslant}}$ does not k-match with any a_i, for $k \leq 2e_{j+1} - 1$ and $1 \leq i \leq j$, then there are a_i and $a_{i'}$, $1 \leq i, i' \leq j$, such that $a_i < a < a_{i'}$ and a_i and $a_{i'}$ do not k-match for any $k \leq 2e_j - 1$ and thus b_i and $b_{i'}$ do not k-match for any $k \leq 2e_j - 1$. Hence there is $b \in T^{C_t'}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ that does not k-match with any b_i, for $k \leq 2e_{j+1} - 1$ and $1 \leq i \leq j$. Similarly, if in the neighborhood $N(e_{j+1}, a)$ of a point $a \in T^{C_t}_{\mathbb{A}^{\leqslant},\tau^{\leqslant}}$ there is a point within distance at most l_{j+1} (w.r.t $\leqslant$) to a point in the neighborhood $N(e_{j+1}, a_i)$ of some point a_i, where $1 \leq i \leq j$, it follows from the induction hypothesis that there is $b \in T^{C_t'}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ such that the corresponding point in the neighborhood $N(e_{j+1}, b)$ is equally near the corresponding point in the neighborhood $N(e_{j+1}, b_i)$. And if there is no point in $N(e_{j+1}, a)$ within distance at most l_{j+1} to any point in $N(e_{j+1}, a_i)$, for every $1 \leq i \leq j$, there is b such that the same holds for $N(e_{j+1}, b)$ and $N(e_{j+1}, b_i)$. Hence for every $a \in C_t$ there is $b \in C_t'$ such that a and b are similar for l_{j+1} and e_{j+1} and points $a_1, \ldots, a_j$ and $b_1, \ldots, b_j$, and correspondingly, for every $b \in C_t'$ there is $a \in C_t$ such that a and b are similar. Because $e_{j+1}^{\leqslant}$-types behave periodically with period $n^{e_{j+1}-1}$, if $|X_{\tau^{\leqslant}} \cap C_t| \equiv l \pmod n$, there are l distinct $b_1', \ldots, b_l' \in T^{C_t'}_{\mathbb{B}^{\leqslant},\tau^{\leqslant}}$ such that each b_i' and some $a \in X_{\tau^{\leqslant}} \cap C_t$ are similar. Since for every $e_{j+1}^{\leqslant}$-type $\tau^{\leqslant}$ we have $|Z_{\tau^{\leqslant}}| \equiv |X_{\tau^{\leqslant}} \setminus N_{\mathbb{A}}| \pmod n$, also $|Y_{\tau^{\leqslant}}| \equiv |X_{\tau^{\leqslant}}| \pmod n$ and so $|Y| \equiv |X| \pmod n$. Finally, since for every a_i and b_i, where $1 \leq i \leq j$, $d(a_i) = d(b_i)$ ($h(a_i) = h(b_i)$) or both have depth (height) at least $2e_j$, for points b with $d(b) < 2e_{j+1}$ (or $h(b) < 2e_{j+1}$), the consideration above can be restricted to points a with $d(a) = d(b)$ ($h(a) = h(b)$).

Let the spoiler choose $b_{j+1} \in B$ and assume b_{j+1} has $e_{j+1}^{\leqslant}$-type $\tau^{\leqslant}$. If $b_{j+1} \in N_{\mathbb{B}}$, then

$$N(e_{j+1}, b_{j+1}) \subseteq \bigcup_{i \leq j} N(e_j, b_i)$$

and the duplicator can choose $a_{j+1} \in A$ such that $\theta_j(a_{j+1}) = b_{j+1}$. It is obvious that the conditions $(*)_{j+1}$ hold.

Suppose then $b_{j+1} \notin N_{\mathbb{B}}$. Let

$$T_{\mathbb{A}^{\leqslant},\tau} \setminus N_{\mathbb{A}} = \dot{\cup}_t [u_t, v_t] \quad \text{and} \quad T_{\mathbb{B}^{\leqslant},\tau} \setminus N_{\mathbb{B}} = \dot{\cup}_t [u_t', v_t']$$

and let $b_{j+1} \in [u_t', v_t']$ for some t. If $b_{j+1} \in [u_t', v_t'] \setminus C_t'$, the duplicator can choose $a_{j+1} \in [u_t, v_t] \setminus C_t$ with $f_t(a_{j+1}) = b_{j+1}$. Suppose then $b_{j+1} \in C_t'$. If $b_{j+1} \in Y$, then $X \cap C_t \neq \emptyset$ and the duplicator can choose a_{j+1} to be any point $a \in C_t$ such that a and b_{j+1} are similar for l_{j+1} and e_{j+1} and points $a_1, \ldots, a_j$ and $b_1, \ldots, b_j$. If $b_{j+1} \notin Y$, according to the condition (3) and the induction hypothesis there is $a \in C_t$ such that a and b_{j+1} are similar and $a \notin X$. In either case we have

$$a_{j+1} \in X \quad \text{if and only if} \quad b_{j+1} \in Y.$$

Since a_{j+1} and b_{j+1} are similar for l_{j+1} and e_{j+1} and points a_i and b_i, where $i \leq j$, the conditions (ii) and (iv) in the induction hypothesis $(*)_{j+1}$ hold. If $b_{j+1} \notin N_{\mathbb{B}}$, then $\mathbb{B} \restriction N(e_{j+1}, b_{j+1})$ contains no point adjacent to any point in $\mathbb{B} \restriction \bigcup_{i \leq j} N(e_{j+1}, b_i)$, and similarly in $\mathbb{A}$. Hence also the first condition in $(*)_{j+1}$ holds. Because both a_{j+1} and b_{j+1} have either the same height (depth), or heigth (depth) at least $2e_{j+1}$, also the condition (iii) holds. Since a_{j+1} and b_{j+1} are the corresponding points of $[u_t, v_t] \smallsetminus C_t$ and $[u'_t, v'_t] \smallsetminus C'_t$ or both are in C_t and C'_t and have the same $e^{\leqslant}_{j+1}$-type, there are equally many intervals in $T_{\mathbb{A}^{\leqslant}, \tau} \smallsetminus N_{\mathbb{A}}$ and $T_{\mathbb{B}^{\leqslant}, \tau} \smallsetminus N_{\mathbb{B}}$, for every e_{j+1}-type τ, and these intervals are either of equal or modulo n equal length. Therefore we can conclude that the conditions $(*)_{j+1}$ hold.

Since in the end $\mathbb{A}^{\leqslant} \restriction \{a_1, \ldots a_r\} \cong \mathbb{B}^{\leqslant} \restriction \{b_1, \ldots b_r\}$ under an isomorphism $a_i \mapsto b_i$, for $1 \leq i \leq r$, the duplicator has a winning strategy in the $(r, \mathbf{D}_n)$-game over $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$. The claim now follows from Theorem 2.2. □

With this proposition we can give an easy proof for our main result. We prove that for every positive integer $n \geq 2$, the predicate $y = (n+1)x$ is not definable with built-in linear order, the predicate $y = nx$ and the counting modulo quantifier $\mathbf{D}_n$.

Let S and S_i, where $1 \leq i \leq n$, be relation symbols with interpretations

$$S(x, y) \iff y = nx \quad \text{and} \quad S_i(x, y) \iff y = nx + i$$

(for convenience, we use the same notation for a relation symbol and its interpretation). It is easy to see, that the structure $\mathbb{T}^n_k$ over the vocabulary $\{S_i \mid 1 \leq i \leq n\}$ and with the universe $T^n_k = \{0, \ldots, \frac{1-n^{k+1}}{1-n} - 1\}$ can be considered as the complete n-ary tree (T^n_k, E) of height k, where

$$E(x, y) \quad \text{if and only if} \quad S_i(x, y) \text{ for some } i.$$

Here 0 is thought of as the root of the tree and direct descendants of a point $x \in T^n_k$ are the elements $nx + 1, \ldots, nx + n$, if $nx < \frac{1-n^{k+1}}{1-n} - 1$; otherwise x is a leaf. (A similar construction was used in [19].)

Every S_i, where $1 \leq i \leq n$, can be defined by the following first-order formula, using the relation S and the linear order:

$$\begin{aligned} S_i(x, y) \iff \exists u_0 \ldots \exists u_i \; (\; & S(x, u_0) \wedge (u_i = y) \wedge \bigwedge_{j=0}^{i-1} (u_j < u_{j+1}) \wedge \\ & \forall v (v < u_0 \vee \bigvee_{j=0}^{i} (v = u_j) \vee u_i < v)) \end{aligned}$$

(as usually, $u < v$ denotes $u \leqslant v$ and $u \neq v$). Thus we can (w.l.o.g) consider ordered structures $\mathbb{T}^n_k$ over the vocabulary $\{S_i \mid 1 \leq i \leq n\}$, instead of ordered $\{S\}$-structures. And as mentioned above, structures $\mathbb{T}^n_k$ can be thought of as complete n-trees.

According to Proposition 5.1, for each quantifier rank r, there are complete n-trees $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ (or $\mathbb{T}^n_k$ and $\mathbb{T}^n_{k+1}$ for some k) such that $\mathbb{A}^{\leqslant}$ has odd height and $\mathbb{B}^{\leqslant}$ has even height, but $\mathbb{A}^{\leqslant}$ and $\mathbb{B}^{\leqslant}$ are equivalent up to the quantifier rank r. Furthermore, note that the partial isomorphisms in the proof of Proposition 5.1 preserve the relations S and S_i. Since $(1 - n^{k+1})/(1 - n)$ is divisible by $n + 1$ if and only if k is odd, the cardinality of $\mathbb{A}^{\leqslant}$ is divisible by $n + 1$ and the cardinality of $\mathbb{B}^{\leqslant}$ is not divisible by $n + 1$.

5.2. Theorem. *No formula of $FO(\mathbf{D}_n)$ using a linear order and the predicate $y = nx$ can define the property that the size of a model is divisible by $n + 1$.*

For $n = 2$, this solves the conjecture of Niwiński and Stolboushkin [19].

6. Conclusion

We showed that $FO(\mathbf{D}_n)$, first-order logic with counting modulo n quantifiers, fails to express many properties which are not definable in first-order logic, either (even with built-in linear order). We focused the consideration to properties like comparing cardinalities and expressing divisibility by $n + 1$.

We gave a combinatorial method for proving elementary equivalence of structures up to a certain quantifier rank with respect to $FO(\mathbf{D}_n)$. Often rather complicated Ehrenfeucht-Fraïssé type game theoretical methods can be replaced by the combinatorial argument. The method was based on counting the number of isomorphism types of a fixed radius of points. In that sense, this paper can be seen as a continuation of [9, 12, 20].

Inexpressibility results with built-in linear order were also considered. We showed that sufficiently large linear orders of modulo n equal length cannot be distinguished in $FO(\mathbf{D}_n)$. With this observation we showed that the majority language as well as the languages $sum(p)$ and $length(p)$ are not definable in $FO(\mathbf{D}_n)$, whenever p has a prime factor that does not divide n. A characterization, when the logic $FO(\mathbf{D}_n)$ is at most as strong as the logic $FO(\mathbf{D}_m)$ on ordered structures, was also given. By modifying the proof of Gurevich [11] that connectivity is not expressible in FO with linear order, we can extend this result to $FO(\mathbf{D}_n)$. Also the Rescher and Härtig quantifiers can be easily seen not to be expressible in $FO(\mathbf{D}_n)$. All the given counterexamples are finite structures.

The weakness of this logic augmented with other predicates was also established. We showed that for any positive integer $n \geq 2$, there is no formula of $FO(\mathbf{D}_n)$, which with a linear order $\leqslant$ and the predicate $y = nx$, expresses that the size of a model is divisible by $n + 1$. Therefore, the predicate $y = (n + 1)x$ is not definable with $y = nx$ and $\leqslant$. The proof used structures with cardinalities $(1 - n^{k+1})/(1 - n)$, that can be considered as complete n-trees. In the proof we showed that no formula of $FO(\mathbf{D}_n)$ with linear order can distinguish two such trees, if they are deep enough.

Our result can be seen as a possible step towards solving the well-known open problem in circuit complexity theory, whether $ACC = NC^1$. An interesting question for further consideration is whether our results hold in the presence of the BIT-predicate (for more details, see e.g. [4, 5, 21]).

Acknowledgement

I want to thank my advisor Lauri Hella for suggesting me this subject and for his helpful comments. I also thank Kerkko Luosto for careful reading the manuscript of this paper and many useful suggestions and improvements.

References

[1] S. Abiteboul and V. Vianu. Fixpoint extensions of first-order logic and Datalog-like languages. In *Proc. 4th IEEE Symp. on Logic in Computer Science*, pages 71–79, 1989.

[2] M. Ajtai. Σ_1^1 formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.

[3] D. A. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1. *Journal of Computer and System Sciences*, 38(1):150–164, 1989.

[4] D. A. M. Barrington, K. Compton, H. Straubing, and D. Thérien. Regular languages in NC^1. *Journal of Computer and System Sciences*, 44:478–499, 1992.

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

[6] K. Compton and H. Straubing. Characterizations of regular languages in low level complexity classes. In *Bulletin of the EATCS*, pages 134–142, October 1992.

[7] L. J. Corredor. El reticulo de las logicas de primer orden con cuantificadores cardinales identification. *Revista Colombiana de Mathemáticas*, 20:1–26, 1986.

[8] H.-D. Ebbinghaus and J. Flum. *Finite Model Theory.* Perspectives in Mathematical Logic. Springer, Berlin, 1995.

[9] R. Fagin, L. Stockmeyer, and M. Vardi. On monadic NP vs. monadic co-NP. *Information and Computation*, 120(1):78–92, July 1995.

[10] M. Furst, J.B. Saxe, and M. Sipser. Parity, circuits and the polynomial time hierarchy. *Mathematical System Theory*, 17:13–27, 1984.

[11] Y. Gurevich. Toward logic tailored for computational complexity. In M. M. Ricther et al., editor, *Computation and Proof Theory, Lecture Notes in Mathematics 1104*, pages 175–216. Springer-Verlag, 1984.

[12] W. Hanf. Model-theoretic methods in the study of elementary logic. In J. Addison, L. Henkin, and A. Tarski, editors, *The Theory of Models*, pages 132–145. North Holland, 1965.

[13] L. Hella. Definability hierarchies of generalized quantifiers. *Annals of Pure and Applied Logic*, 43:235–271, 1989.

[14] L. Hella. Logical hierarchies in PTIME. In *Proc. 7th IEEE Symp. on Logic in Computer Science*, pages 360–368, 1992. Full version to appear in, *Information and Computation.*

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

[16] Ph. G. Kolaitis and J. A. Väänänen. Generalized quantifiers and pebble games on finite structures. *Annals of Pure and Applied Logic*, 74(1):23–75, June 1995.

[17] K. Luosto. Hierarchies of monadic generalized quantifiers. Manuscript, 1996.

[18] R. McNaughton and S. Papert. *Counter-Free Automata.* MIT Press, Cambridge, 1971.

[19] D. Niwiński and A. Stolboushkin. $y = 2x$ vs. $y = 3x$. In *Proc. 8th IEEE Symp. on Logic in Computer Science*, pages 172–178, 1993.

[20] J. Nurmonen. On winning strategies with unary quantifiers. *Journal of Logic and Computation*, 1996. To appear.

[21] H. Straubing, D. Thérien, and W. Thomas. Regular languages defined with generalized quantifiers. In *Proc. 15th International Colloq. on Automata, Languages, and Programming*, pages 561–575, 1988.

[22] J. Väänänen. Unary quantifiers on finite models. Preprint 101, Reports of the Department of Mathematics, University of Helsinki, January 1996.

[23] M. Vardi. The complexity of relational query languages. In *Proceedings, 14th ACM Symposium on Theory of Computing*, pages 137–146, 1982.