On the locality of arb-invariant first-order logic with modulo counting quantifiers

Frederik Harwath and Nicole Schweikardt

Institut für Informatik, Goethe-Universität Frankfurt, Germany
{harwath,schweika}@cs.uni-frankfurt.de

Abstract

We study Gaifman and Hanf locality of an extension of first-order logic with modulo p counting quantifiers (FO+MOD$_p$, for short) with arbitrary numerical predicates. We require that the validity of formulas is independent of the particular interpretation of the numerical predicates and refer to such formulas as arb-invariant formulas. This paper gives a detailed picture of locality and non-locality properties of arb-invariant FO+MOD$_p$. For example, on the class of all finite structures, for any $p \geqslant 2$, arb-invariant FO+MOD$_p$ is neither Hanf nor Gaifman local with respect to a sublinear locality radius. However, in case that p is an odd prime power, it is *weakly* Gaifman local with a polylogarithmic locality radius. And when restricting attention to the class of string structures, for odd prime powers p, arb-invariant FO+MOD$_p$ is both Hanf and Gaifman local with a polylogarithmic locality radius. Our negative results build on examples of order-invariant FO+MOD$_p$ formulas presented in Niemistö's PhD thesis. Our positive results make use of the close connection between FO+MOD$_p$ and Boolean circuits built from NOT-gates and AND-, OR-, and MOD$_p$-gates of arbitrary fan-in.

1998 ACM Subject Classification F.4.1 Mathematical Logic, H.2.3 Languages (Query Languages), F.1.3 Complexity Measures and Classes

Keywords and phrases finite model theory, Gaifman and Hanf locality, first-order logic with modulo counting quantifiers, order-invariant and arb-invariant formulas, lower bounds in circuit complexity

Digital Object Identifier 10.4230/LIPIcs.CSL.2013.363

1 Introduction

Expressibility of logics over finite structures plays an important role in various areas of computer science. In descriptive complexity, logics are used to characterise complexity classes, and concerning databases, common query languages have well-known logical equivalents. These applications have motivated a systematic study of the expressive powers of logics on finite structures. The classical inexpressibility arguments for logics over finite structures (i.e., back-and-forth systems or Ehrenfeucht-Fraïssé games; cf. [9]) often involve nontrivial combinatorics. Notions of *locality* have been proposed as an alternative that allows to contain much of the hard combinatorial work in generic results.

The two best known notions of locality are *Gaifman locality* and *Hanf locality*, introduced in [8, 6]. A k-ary query is called *Gaifman local with locality radius* $f(n)$ if in a structure of cardinality n, the question whether a given tuple satisfies the query only depends on the isomorphism type of the tuple's neighbourhood of radius $f(n)$. A Boolean query is *Hanf local with locality radius* $f(n)$ if the question whether a structure of size n satisfies the query only depends on the number of occurrences of isomorphism types of neighbourhoods of radius $f(n)$. If a given logic is capable of defining only Gaifman or Hanf local queries with a sublinear locality radius, then this logic cannot express "non-local" queries such as, e.g., the

Computer Science Logic 2013 (CSL'13).
Editor: Simona Ronchi Della Rocca; pp. 363–379
Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

query asking whether two nodes of a graph are connected by a path, or the query asking whether a graph is acyclic (cf., e.g., the textbook [9]). It is well-known that first-order logic FO, as well as extensions of FO by various kinds of counting quantifiers, are Gaifman local and Hanf local with a constant locality radius [8, 6]. Also, locality properties of extensions of FO by invariant uses of order and arithmetic have been considered [7, 1].

Order-invariant and arb-invariant logics[1] were introduced to capture the data independence principle in databases: An implementation of a database query may exploit the order in which the database elements are stored in memory, and thus identify the elements with natural numbers on which arithmetic can be performed. But the use of order and arithmetic should be restricted in such a way that the result of the query does not depend on the particular order in which the data is stored. *Arb-invariant* formulas are formulas that can make use, apart from the relations present in a given structure, also of a linear order $<$ and arithmetic predicates such as $+$ or $\times$ induced by $<$, but only in such a way that the answer is independent of the particular linear order on a structure chosen for $<$. Arb-invariant formulas that only use the linear order, but no further arithmetic predicates, are called *order-invariant*. In [7] it was shown that order-invariant FO can express only queries that are Gaifman local with a constant locality radius, and from [1] we know that arb-invariant FO can express only queries that are Gaifman local with a polylogarithmic locality radius. The proof of [1] relies on a reduction using strong lower bound results from circuit complexity, concerning AC^0-circuits. Similar lower bounds are known also for the extension of AC^0-circuits by modulo p counting gates, for a prime power p [13]. This naturally raises the question whether the locality results from [1] can be generalised to the extension of FO by modulo p counting quantifiers (FO+MOD$_p$, for short), which precisely corresponds to AC^0-circuits with modulo p counting gates [3]. This question was the starting point for the investigations carried out in the present paper. Our results give a detailed picture of the locality and non-locality properties of order-invariant and arb-invariant FO+MOD$_p$.

For every natural number $p \geqslant 2$, order-invariant FO+MOD$_p$ is neither Hanf nor Gaifman local with a sublinear locality radius (Section 4 and Proposition 3.2). For *even* numbers $p \geqslant 2$, order-invariant FO+MOD$_p$ is not even *weakly* Gaifman local with a sublinear locality radius (Proposition 3.4). Here, *weak* Gaifman locality is a relaxed notion of Gaifman locality referring only to tuples with disjoint neighbourhoods (cf., [9]). However, for *odd prime powers* p we can show that arb-invariant FO+MOD$_p$ is weakly Gaifman local with a polylogarithmic locality radius (Theorem 3.5). For showing the latter result, we introduce a new locality notion called *shift locality*, for which we can prove for all prime powers p that arb-invariant FO+MOD$_p$ is shift local with a polylogarithmic locality radius (Theorem 3.7). Our proof relies on Smolensky's circuit lower bound [13]. Generalising our result from prime powers p to arbitrary numbers p can be expected to be difficult, since it would solve long-standing open questions in circuit complexity (Remark 3.13). When restricting attention to the class of *string structures*, we obtain for odd prime powers p that arb-invariant FO+MOD$_p$ is both Hanf and Gaifman local with a polylogarithmic locality radius (Theorem 4.3 and Corollary 4.4). On the other hand, for even numbers $p \geqslant 2$, already order-invariant FO+MOD$_p$ on string structures is neither Gaifman nor Hanf local with a sublinear locality radius (Proposition 3.4 and Section 4). This, in particular, implies that order-invariant FO+MOD$_p$ is strictly more expressive on strings than FO+MOD$_p$, refuting a conjecture of Benedikt and Segoufin [4].

The remainder of this paper is structured as follows: Section 2 fixes the basic notation,

[1] Strictly speaking, arb-invariant first-order logic is a "logical system" rather than a "logic", as its syntax is undecidable.

introduces the notions of order-invariant and arb-invariant FO+MOD$_p$ and recalls two examples of order-invariant FO+MOD$_p$-formulas from Niemistö's PhD-thesis [11]. Section 3 presents our results concerning Gaifman locality, weak Gaifman locality, and shift locality. Section 4 deals with Hanf locality on finite structures, and with Gaifman and Hanf locality on string structures.

Several details had to be omitted from this paper due to lack of space. These can be found in the full version of this paper, available at the authors' websites.

2 Preliminaries

Basic notation. We write $\mathbb{N}$ for the set of non-negative integers and let $\mathbb{N}_{\geqslant 1} := \mathbb{N} \setminus \{0\}$. For $n \in \mathbb{N}_{\geqslant 1}$ we write $[n]$ for the set $\{i \in \mathbb{N} : 0 \leqslant i < n\}$, i.e., $[n] = \{0, \ldots, n{-}1\}$. For integers i, j, p with $p \geqslant 2$, we write $i \equiv j \bmod p$ (and say that i is congruent j modulo p) iff there exists an integer k such that $i = j + kp$. For integers i, i', the term $(i{+}i' \bmod p)$ denotes the number $j \in [p]$ such that $i{+}i' \equiv j \bmod p$. Two natural numbers i and j are *coprime* if their greatest common divisor is 1. A number p is called a *prime power* if $p = \hat{p}^i$ for a prime $\hat{p}$ and an integer $i \geqslant 1$, and p is called an *odd* prime power if p's prime factor is different from 2 (i.e., p is odd). A number $r \in \mathbb{N}_{\geqslant 1}$ is called a *factor* of a natural number s, if there is a $t \in \mathbb{N}$ such that $s = rt$. We write $\log n$ to denote the logarithm of a number n with respect to base 2, and we often simply write $\log n$ instead of $\lfloor \log n \rfloor$.

For a finite set A we write $|A|$ to denote the cardinality of A. By 2^A we denote the power set of A, i.e., the set $\{Y : Y \subseteq A\}$. The set of all non-empty finite strings built from symbols in A is denoted A^+. We write $|w|$ for the length of a string $w \in A^+$. For an $a \in A$ we write $|w|_a$ for the number of occurrences of the letter a in the string w.

Structures. A *signature* σ is a set of relation symbols R, each of them associated with a fixed arity $ar(R) \in \mathbb{N}_{\geqslant 1}$. Throughout this paper, σ will usually denote a fixed finite signature.

A *σ-structure* $\mathcal{A}$ consists of a non-empty set A called the *universe* of $\mathcal{A}$, and a relation $R^{\mathcal{A}} \subseteq A^{ar(R)}$ for each relation symbol $R \in \sigma$. The *cardinality* of a σ-structure $\mathcal{A}$ is the cardinality of its universe. *Finite* σ-structures are σ-structures of finite cardinality. For σ-structures $\mathcal{A}$ and $\mathcal{B}$ and tuples $\overline{a} = (a_1, \ldots, a_k) \in A^k$ and $\overline{b} = (b_1, \ldots, b_k) \in B^k$ we write $(\mathcal{A}, \overline{a}) \cong (\mathcal{B}, \overline{b})$ to indicate that there is an isomorphism π from $\mathcal{A}$ to $\mathcal{B}$ that maps $\overline{a}$ to $\overline{b}$ (i.e., $\pi(a_i) = b_i$ for each $i \leqslant k$).

We represent strings over a finite alphabet Σ by successor-based structures as follows: We choose $\sigma_\Sigma := \{E\} \cup \{P_a : a \in \Sigma\}$, where E is a binary relation symbol and P_a is a unary relation symbol, for each $a \in \Sigma$. We represent a non-empty string $w \in \Sigma^+$ by the σ_Σ-structure $\mathcal{S}_w$, where the universe of $\mathcal{S}_w$ is the set $\{1, \ldots, |w|\}$ of positions of w, the edge relation $E^{\mathcal{S}_w}$ is the successor relation, i.e., $E^{\mathcal{S}_w} = \{(i, i+1) : 1 \leqslant i < |w|\}$, and for each $a \in \Sigma$, the set $P_a^{\mathcal{S}_w}$ consists of all positions of w that carry the letter a. Structures of the form $\mathcal{S}_w$ (for a string w) are called *string structures*.

In this paper, all *classes* $\mathfrak{C}$ of finite σ-structures will be closed under isomorphism, i.e., if $\mathcal{A}$ and $\mathcal{B}$ are isomorphic σ-structures, then $\mathcal{A} \in \mathfrak{C}$ iff $\mathcal{B} \in \mathfrak{C}$. We will write Σ-*strings* to denote the class of all σ_Σ-structures that represent strings in Σ^+ (i.e., Σ-*strings* is the closure under isomorphisms of the set $\{\mathcal{S}_w : w \in \Sigma^+\}$).

First-order logic with modulo counting quantifiers. We assume that the reader is familiar with basic concepts and notations concerning first-order logic and extensions thereof (cf., e.g., the textbooks [9, 5]). By *free*(φ) we denote the set of all free variables of a formula

φ. A *sentence* is a formula φ with *free*$(\varphi) = \emptyset$. We often write $\varphi(\overline{x})$, for $\overline{x} = (x_1, \ldots, x_k)$, to indicate that *free*$(\varphi) = \{x_1, \ldots, x_k\}$. If $\mathcal{A}$ is a σ-structure and $\overline{a} = (a_1, \ldots, a_k) \in A^k$, we write $\mathcal{A} \models \varphi[\overline{a}]$ to indicate that the formula $\varphi(\overline{x})$ is satisfied in $\mathcal{A}$ when interpreting the free occurrences of the variables $x_1, \ldots, x_k$ with the elements $a_1, \ldots, a_k$.

We write $\mathrm{FO}(\sigma)$ to denote the class of all first-order formulas of signature σ. In this paper, we consider the extension of $\mathrm{FO}(\sigma)$ by *modulo counting quantifiers*, defined as follows: Let p be a natural number with $p \geqslant 2$. A *modulo p counting quantifier* is of the form $\exists^{i \bmod p}$ for some $i \in [p]$. A formula of the form $\exists^{i \bmod p} x\, \varphi(x, \overline{y})$ is satisfied by a σ-structure $\mathcal{A}$ and an interpretation $\overline{b} \in A^k$ of the variables $\overline{y}$ iff the number of elements $a \in A$ such that $\mathcal{A} \models \varphi[a, \overline{b}]$ is congruent i modulo p.

For a fixed natural number $p \geqslant 2$ we write $\mathrm{FO{+}MOD}_p(\sigma)$ to denote the extension of $\mathrm{FO}(\sigma)$ by modulo p counting quantifiers. I.e., $\mathrm{FO{+}MOD}_p(\sigma)$ is built from atomic formulas of the form $x_1{=}x_2$ and $R(x_1, \ldots, x_{ar(R)})$, for $R \in \sigma$ and variables $x_1, x_2, \ldots, x_{ar(R)}$, and closed under Boolean connectives $\wedge$, $\vee$, $\neg$, existential and universal first-order quantifiers $\exists$, $\forall$, and modulo p counting quantifiers $\exists^{i \bmod p}$, for $i \in [p]$. This logic has been studied in depth, see e.g., [14, 8, 3]. Note that if m is a multiple of p, then $\mathrm{FO{+}MOD}_m$ can express modulo p counting quantifiers, since $\exists^{i \bmod p} x\ \varphi(x, \overline{y})$ is equivalent to $\bigvee_{0 \leqslant j < m/p} \exists^{jp+i \bmod m} x\ \varphi(x, \overline{y})$.

Arb-invariant logics. We can extend the expressive power of a logic by allowing formulas to use, apart from the relation symbols present in the signature σ, also a linear order $<$, arithmetic predicates such as $+$ or $\times$, or arbitrary numerical predicates. By definition, an r-ary *numerical predicate* $P^{\mathbb{N}}$ is an r-ary relation on $\mathbb{N}$ (i.e., $P^{\mathbb{N}} \subseteq \mathbb{N}^r$). Two examples of numerical predicates are the linear order $<^{\mathbb{N}}$ consisting of all tuples $(a, b) \in \mathbb{N}^2$ with $a < b$, and the addition predicate $+^{\mathbb{N}}$ consisting of all triples $(a, b, c) \in \mathbb{N}^3$ with $a + b = c$.

To allow formulas to use numerical predicates, we fix the following notation: For every $r \in \mathbb{N}_{\geqslant 1}$ and every r-ary numerical predicate $P^{\mathbb{N}}$, let P be a new relation symbol of arity r (“new” meaning that P does not belong to σ). We write η_{arb} to denote the set of all the relation symbols P obtained this way, and let $\sigma_{\mathrm{arb}} := \sigma \cup \eta_{\mathrm{arb}}$ (the subscript “arb” stands for “arbitrary numerical predicates”).

Next, we would like to allow $\mathrm{FO{+}MOD}_p(\sigma_{\mathrm{arb}})$-formulas to make meaningful statements about finite σ-structures. To this end, for a finite σ-structure $\mathcal{A}$, we consider embeddings ι of the universe of $\mathcal{A}$ into the initial segment of $\mathbb{N}$ of size $n = |A|$, i.e., the set $[n] = \{0, \ldots, n{-}1\}$.

▶ **Definition 2.1** (Embedding). Let $\mathcal{A}$ be a finite σ-structure, and let $n := |A|$.
An *embedding* ι of $\mathcal{A}$ is a bijection $\iota : A \to [n]$.

Given a finite σ-structure $\mathcal{A}$ and an embedding ι of $\mathcal{A}$, we can translate r-ary numerical predicates $P^{\mathbb{N}}$ into r-ary predicates on A as follows: $P^{\mathbb{N}}$ induces the r-ary predicate P^{ι} on A, consisting of all r-tuples $\overline{a} = (a_1, \ldots, a_r) \in A^r$ where $\iota(\overline{a}) = (\iota(a_1), \ldots, \iota(a_r)) \in P^{\mathbb{N}}$. In particular, the linear order $<^{\mathbb{N}}$ induces the linear order $<^{\iota}$ on A where for all $a, b \in A$ we have $a <^{\iota} b$ iff $\iota(a) < \iota(b)$.

The σ_{arb}-structure $\mathcal{A}^{\iota}$ associated with $\mathcal{A}$ and ι is the expansion of $\mathcal{A}$ by the predicates P^{ι} for all $P \in \eta_{\mathrm{arb}}$. I.e., $\mathcal{A}^{\iota}$ has the same universe as $\mathcal{A}$, all relation symbols $R \in \sigma$ are interpreted in $\mathcal{A}^{\iota}$ in the same way as in $\mathcal{A}$, and every numerical symbol $P \in \eta_{\mathrm{arb}}$ is interpreted by the relation P^{ι}.

To ensure that an $\mathrm{FO{+}MOD}_p(\sigma_{\mathrm{arb}})$-formula φ makes a meaningful statement about a σ-structure $\mathcal{A}$, we evaluate φ in $\mathcal{A}^{\iota}$, and we restrict attention to those formulas whose truth value is independent of the particular choice of the embedding ι. This is formalised by the following notion.

▶ **Definition 2.2** (Arb-invariance)**.** Let $\varphi(\overline{x})$ be an FO+MOD$_p(\sigma_{\text{arb}})$-formula with k free variables, and let $\mathcal{A}$ be a finite σ-structure. The formula $\varphi(\overline{x})$ is *arb-invariant on* $\mathcal{A}$ if for *all* embeddings ι_1 and ι_2 of $\mathcal{A}$ and for all tuples $\overline{a} \in A^k$ we have: $\mathcal{A}^{\iota_1} \models \varphi[\overline{a}] \iff \mathcal{A}^{\iota_2} \models \varphi[\overline{a}]$.

Let $\varphi(\overline{x})$ be arb-invariant on $\mathcal{A}$. We write $\mathcal{A} \models \varphi[\overline{a}]$, if $\mathcal{A}^{\iota} \models \varphi[\overline{a}]$ for some (and hence every) embedding ι of $\mathcal{A}$.

▶ **Definition 2.3** (arb-inv-FO+MOD$_p$)**.** An FO+MOD$_p(\sigma_{\text{arb}})$-formula $\varphi(\overline{x})$ is *arb-invariant on a class* $\mathfrak{C}$ of finite σ-structures, if $\varphi(\overline{x})$ is arb-invariant on every $\mathcal{A} \in \mathfrak{C}$. By arb-inv-FO+MOD$_p^{\mathfrak{C}}(\sigma)$ we denote the set of all FO+MOD$_p(\sigma_{\text{arb}})$-formulas that are arb-invariant on $\mathfrak{C}$.

$\varphi(\overline{x})$ is called *arb-invariant* if it is arb-invariant on the class of all finite σ-structures. We write arb-inv-FO+MOD$_p(\sigma)$ to denote the set of all arb-invariant FO+MOD$_p(\sigma_{\text{arb}})$-formulas.

▶ **Definition 2.4** (Order-invariance and <-inv-FO+MOD$_p$)**.**
An arb-invariant formula that only uses the numerical predicate $<^{\mathbb{N}}$ is called *order-invariant*. By <-inv-FO+MOD$_p(\sigma)$ we denote the set of all arb-invariant FO+MOD$_p(\sigma \cup \{<\})$-formulas.

Next, we present two examples of <-inv-FO+MOD$_p(\sigma)$-sentences that were developed by Niemistö in [11] and that will be used later on in this paper.

▶ **Example 2.5** (Niemistö (Proposition 6.22 in [11]))**.** Let $\sigma = \{E\}$ be the signature consisting of a binary relation symbol E. Proposition 6.22 of [11] presents an <-inv-FO+MOD$_2(\sigma)$-sentence $\varphi_{\textit{even cycles}}$ that is satisfied by exactly those finite σ-structures $\mathcal{A}$ that are disjoint unions of directed cycles where the number of cycles of even length is even.

▶ **Example 2.6** (Niemistö (Proposition 6.20 in [11]))**.** Let $\sigma = \{E_1, E_2\}$ be the signature consisting of two binary relation symbols E_1 and E_2 and let $h, w \in \mathbb{N}$ with $h, w \geqslant 2$. The *torus* $\mathcal{A}_{h,w}$ and the *twisted torus* $\mathcal{B}_{h,w}$ of height h and width w are the σ-structures defined as follows (illustrations can be found on the left and in the middle of Figure 1).
The *torus of height* h *and width* w is the σ-structure $\mathcal{A}_{h,w}$ with universe $[h] \times [w]$ and relations

$$\begin{aligned} E_1^{\mathcal{A}_{h,w}} &:= \{ \big((i,j),\, (i{+}1 \bmod h,\, j)\big) \ : \ i \in [h],\ \ j \in [w] \ \} \\ E_2^{\mathcal{A}_{h,w}} &:= F_{h,w} \ \cup \ \{ \big((i, w{-}1),\, (i,0)\big) \ : \ i \in [h] \ \} \end{aligned}$$

with $F_{h,w} := \{ \big((i,j),\, (i,j{+}1)\big) \ : \ i \in [h],\ j \in [w{-}1] \ \}$.
The *twisted torus of height* h *and width* w is the σ-structure $\mathcal{B}_{h,w}$ with universe $[h] \times [w]$ and relations

$$\begin{aligned} E_1^{\mathcal{B}_{h,w}} &:= E_1^{\mathcal{A}_{h,w}} \\ E_2^{\mathcal{B}_{h,w}} &:= F_{h,w} \ \cup \ \{ \big((i, w{-}1),\, (i{+}1 \bmod h,\, 0)\big) \ : \ i \in [h] \ \}. \end{aligned}$$

Proposition 6.20 in [11] presents, for every $h \in \mathbb{N}$ with $h \geqslant 2$, an <-inv-FO+MOD$_h(\sigma)$-sentence $\varphi_{h\text{-}torus}$ which, for every $w \in \mathbb{N}$ with $w \geqslant 2$, is satisfied by the torus $\mathcal{A}_{h,w}$, but not by the twisted torus $\mathcal{B}_{h,w}$.

3 Locality of queries

A *k-ary query* q is a mapping that associates with every finite σ-structure $\mathcal{A}$ a k-ary relation $q(\mathcal{A}) \subseteq A^k$, which is invariant under isomorphisms, i.e., if π is an isomorphism from a σ-structure $\mathcal{A}$ to a σ-structure $\mathcal{B}$, then for all $\overline{a} = (a_1, \ldots, a_k) \in A^k$ we have $\overline{a} \in q(\mathcal{A})$ iff $\pi(\overline{a}) = (\pi(a_1), \ldots, \pi(a_k)) \in q(\mathcal{B})$. If $\mathfrak{C}$ is a class of finite σ-structures, then every arb-inv-FO+MOD$_p^{\mathfrak{C}}(\sigma)$-formula $\varphi(\overline{x})$ with k free variables defines a k-ary query q_φ on $\mathfrak{C}$ via $q_\varphi(\mathcal{A}) = \{\overline{a} \in A^k \,:\, \mathcal{A} \models \varphi[\overline{a}]\}$, for every σ-structure $\mathcal{A} \in \mathfrak{C}$.

The *Gaifman graph* of a σ-structure $\mathcal{A}$ is the undirected graph $\mathcal{G}(\mathcal{A})$ with vertex set A, where for any $a, b \in A$ with $a \neq b$ there is an undirected edge between a and b iff there is an $R \in \sigma$ and a tuple $(a_1, \ldots, a_{ar(R)}) \in R^{\mathcal{A}}$ such that $a, b \in \{a_1, \ldots, a_{ar(R)}\}$. The *distance* $dist^{\mathcal{A}}(a,b)$ between two elements $a, b \in A$ is the length of a shortest path between a and b in $\mathcal{G}(\mathcal{A})$. The distance $dist^{\mathcal{A}}(b, \overline{a})$ between an element $b \in A$ and a tuple $\overline{a} = (a_1, \ldots, a_k) \in A^k$ is the the minimum of $dist^{\mathcal{A}}(b, a_i)$ for all $i \in \{1, \ldots, k\}$. For every $r \in \mathbb{N}$, the *r-ball* $N_r^{\mathcal{A}}(\overline{a})$ around a tuple $\overline{a} \in A^k$ is the set of all elements b with $dist^{\mathcal{A}}(b, \overline{a}) \leqslant r$. The *r-neighbourhood* of $\overline{a}$ is the induced substructure $\mathcal{N}_r^{\mathcal{A}}(\overline{a})$ of $\mathcal{A}$ on $N_r^{\mathcal{A}}(\overline{a})$.

3.1 Gaifman locality

The notion of *Gaifman locality* is a standard tool for showing that particular queries are not definable in certain logics (cf., e.g., the textbook [9] for an overview).

► **Definition 3.1** (Gaifman locality). Let $\mathfrak{C}$ be a class of finite σ-structures, $k \in \mathbb{N}_{\geqslant 1}$ and $f : \mathbb{N} \to \mathbb{N}$. A k-ary query q is *Gaifman $f(n)$-local on* $\mathfrak{C}$ if there is an $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ with $n \geqslant n_0$ and every σ-structure $\mathcal{A} \in \mathfrak{C}$ with $|A| = n$, the following is true for all k-tuples $\overline{a}, \overline{b} \in A^k$ with $(\mathcal{N}_{f(n)}^{\mathcal{A}}(\overline{a}), \overline{a}) \cong (\mathcal{N}_{f(n)}^{\mathcal{A}}(\overline{b}), \overline{b})$: $\quad \overline{a} \in q(\mathcal{A}) \iff \overline{b} \in q(\mathcal{A})$.
The query q is *Gaifman $f(n)$-local* if it is Gaifman $f(n)$-local on the class of all finite σ-structures.

I.e., in a σ-structure of cardinality n, a query that is Gaifman $f(n)$-local cannot distinguish between k-tuples of nodes whose neighbourhoods of radius $f(n)$ are isomorphic. The function $f(n)$ is called the *locality radius* of the query. It is well-known that queries definable in FO or FO+MOD$_p$ (for any $p \geqslant 2$) are Gaifman local with a constant locality radius [8]. The articles [7] and [1] generalised this to order-invariant FO (for constant locality radius) and arb-invariant FO (for polylogarithmic locality radius) in the following sense: Let $k \in \mathbb{N}_{\geqslant 1}$, and let q be a k-ary query. If q is definable in $<$-inv-FO(σ), then there is a $c \in \mathbb{N}$ such that q is Gaifman c-local. If q is definable in arb-inv-FO(σ), then there is a $c \in \mathbb{N}$ such that q is Gaifman $(\log n)^c$-local. However, for every $d \in \mathbb{N}$ there is a unary query q_d that is definable in arb-inv-FO($\{E\}$) and that is not Gaifman $(\log n)^d$-local.

Somewhat surprisingly, using Example 2.6 one obtains that the Gaifman locality result cannot be generalised to order- or arb-invariant FO+MOD$_p$. In fact, $<$-inv-FO+MOD$_p$ can define queries that are not even Gaifman local with locality radius as big as $(\frac{n}{h}-2)$, for the smallest prime divisor h of p:

► **Proposition 3.2.** *Let $h \in \mathbb{N}$ with $h \geqslant 2$, and let $\sigma = \{R, E_1, E_2\}$ be a signature consisting of a unary relation symbol R and two binary relation symbols E_1, E_2. There exists a unary query q that is not Gaifman $(\frac{n}{h}-2)$-local, but definable in* $<$-inv-FO+MOD$_p(\sigma)$, *for every multiple $p \geqslant 2$ of h.*

Proof. Recall the $\{E_1, E_2\}$-structures $\mathcal{A}_{h,w}$ and $\mathcal{B}_{h,w}$ from Example 2.6 called *torus* and *twisted torus*, and recall the definition of the relation $F_{h,w}$. For $w \in \mathbb{N}$ with $w \geqslant 2$, the *pre-torus of height h and width w* is the σ-structure $\mathcal{C}_{h,w}$ with universe $[h] \times [w]$ and relations $R^{\mathcal{C}_{h,w}} := \{\,(0, w{-}1)\,\}$, $E_1^{\mathcal{C}_{h,w}} := E_1^{\mathcal{A}_{h,w}}$, and $E_2^{\mathcal{C}_{h,w}} := F_{h,w}$ (see the rightmost part of Figure 1 for an illustration).

From Example 2.6 we obtain an $<$-inv-FO+MOD$_h(\{E_1, E_2\})$-sentence $\varphi_{h\text{-}torus}$ which, for every width $w \in \mathbb{N}$ with $w \geqslant 2$, is satisfied by $\mathcal{A}_{h,w}$, but not by $\mathcal{B}_{h,w}$. We modify $\varphi_{h\text{-}torus}$ in such a way that we obtain an $<$-inv-FO+MOD$_h(\sigma)$-formula $\psi(x)$ which, when evaluated

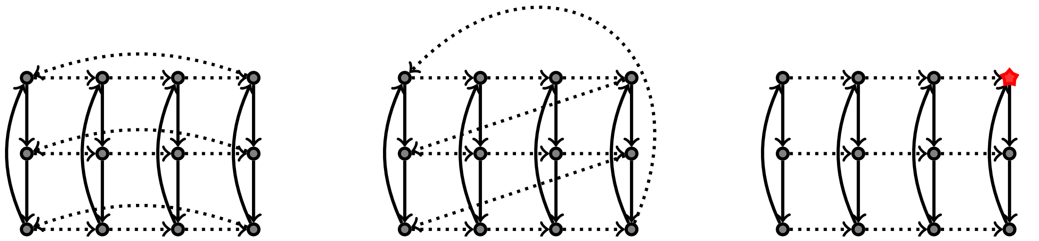

Figure 1 The torus $\mathcal{A}_{3,4}$ (left), the twisted torus $\mathcal{B}_{3,4}$ (middle), and the pre-torus $\mathcal{C}_{3,4}$ (right) of height 3 and width 4. The E_1- and E_2-edges are depicted by solid arcs and dotted arcs, respectively. The unique node in the relation $R^{\mathcal{C}_{3,4}}$ of the pre-torus is the rightmost node in the top row, depicted by a red star.

in the pre-torus $\mathcal{C}_{h,w}$ with x interpreted as the element $a := (0,0)$ (resp., as $b := (1,0)$), simulates $\varphi_{h\text{-}torus}$ evaluated on $\mathcal{A}_{h,w}$ (resp., on $\mathcal{B}_{h,w}$). To this end, we let $\psi(x)$ state that each of the following is satisfied:

- There is a unique element y_0 satisfying $R(y_0)$,
- there are elements $y_1, \ldots, y_{h-1}$ such that $E_1(y_i, y_{i+1 \bmod h})$ is true for all $i \in [h]$,
- there are elements $x_0, \ldots, x_{h-1}$ such that $x_0{=}x$ and $E_1(x_i, x_{i+1 \bmod h})$ is true for all $i \in [h]$,
- the formula φ' is satisfied, where φ' is obtained from $\varphi_{h\text{-}torus}$ by replacing every atom of the form $E_2(u,v)$ by the formula $\big(E_2(u,v) \ \vee\ \bigvee_{0\leqslant i<h} (u{=}y_i \ \wedge\ v{=}x_i)\big)$.

Clearly, $\mathcal{C}_{h,w} \models \psi[a]$ (since $\mathcal{A}_{h,w} \models \varphi_{h\text{-torus}}$), and $\mathcal{C}_{h,w} \not\models \psi[b]$ (since $\mathcal{B}_{h,w} \not\models \varphi_{h\text{-torus}}$). Thus, $a \in q_\psi(\mathcal{C}_{h,w})$ and $b \notin q_\psi(\mathcal{C}_{h,w})$. Note that the $(w{-}2)$-neighbourhoods of a and b in the pre-torus $\mathcal{C}_{h,w}$ are isomorphic, i.e., $(\mathcal{N}_{w-2}^{\mathcal{C}_{h,w}}(a), a) \cong (\mathcal{N}_{w-2}^{\mathcal{C}_{h,w}}(b), b)$. The cardinality of $\mathcal{C}_{h,w}$ is $n := hw$, and hence $w{-}2 = \frac{n}{h}{-}2$. Thus, the query defined by $\psi(x)$ is not Gaifman $(\frac{n}{h}{-}2)$-local.

By Example 2.6, $\varphi_{h\text{-}torus}$ is order-invariant on the class of all finite $\{E_1, E_2\}$-structures. Therefore, the formula $\psi(x)$ is order-invariant on the class of all finite σ-structures. Note that $\psi(x)$ is definable in $<$-inv-FO+MOD$_h(\sigma)$, and hence also in $<$-inv-FO+MOD$_p(\sigma)$, for every multiple p of h. ◀

3.2 Weak Gaifman locality

Weak Gaifman locality (cf., [9]) is a relaxed notion of Gaifman locality where "$\bar{a} \in q(\mathcal{A}) \iff \bar{b} \in q(\mathcal{A})$" needs to be true only for those tuples $\bar{a}$ and $\bar{b}$ whose $f(n)$-neighbourhoods are disjoint.

▶ **Definition 3.3** (Weak Gaifman locality). Let $\mathfrak{C}$ be a class of finite σ-structures, $k \in \mathbb{N}_{\geqslant 1}$ and $f : \mathbb{N} \to \mathbb{N}$. A k-ary query q is *weakly Gaifman $f(n)$-local on $\mathfrak{C}$* if there is an $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ with $n \geqslant n_0$ and every σ-structure $\mathcal{A} \in \mathfrak{C}$ with $|A| = n$, the following is true for all k-tuples $\bar{a}, \bar{b} \in A^k$ with $(\mathcal{N}_{f(n)}^{\mathcal{A}}(\bar{a}), \bar{a}) \cong (\mathcal{N}_{f(n)}^{\mathcal{A}}(\bar{b}), \bar{b})$ and $N_{f(n)}^{\mathcal{A}}(\bar{a}) \cap N_{f(n)}^{\mathcal{A}}(\bar{b}) = \emptyset$: $\bar{a} \in q(\mathcal{A}) \iff \bar{b} \in q(\mathcal{A})$. The query q is *weakly Gaifman $f(n)$-local* if it is weakly Gaifman $f(n)$-local on the class of all finite σ-structures.

Note that the example presented in the proof of Proposition 3.2 does not provide a counter-example to *weak* Gaifman locality, since the elements a and b considered in the proof of Proposition 3.2 are of distance 1, and thus their $f(n)$-neighbourhoods are not disjoint. However, using Example 2.5, one obtains a counter-example to *weak* Gaifman locality for

$<$-inv-FO+MOD$_p$ for *even* numbers p; see Proposition 6.23 in [11]. Here, we present a refinement of Niemistö's proof which provides a counter-example to weak Gaifman locality already for the restricted case of string structures.

▶ **Proposition 3.4.** *Let $\Sigma := \{0,1\}$, and let $\sigma_\Sigma = \{E, P_0, P_1\}$ be the signature used for representing strings over Σ. There exists a unary query q that is not weakly Gaifman $(\frac{n}{4}-1)$-local on Σ-strings, but definable in* $<$-inv-FO+MOD$_p(\sigma_\Sigma)$*, for every even number $p \geqslant 2$.*

Proof. For every $\ell \in \mathbb{N}_{\geqslant 1}$, let $\mathcal{A}_\ell$ and $\mathcal{B}_\ell$ be $\{E\}$-structures whose universe consists of 2ℓ vertices, the edge relation of $\mathcal{A}_\ell$ consists of two directed cycles of length ℓ, and the edge relation of $\mathcal{B}_\ell$ consists of a single directed cycle of length 2ℓ. Furthermore, we choose w_ℓ to be the string $1^\ell\, 0^\ell\, 1^\ell\, 0^\ell$, and we let $a_\ell := \ell$ be the rightmost position of the first block of 1s, and $b_\ell := 3\ell$ the rightmost position of the second block of 1s.

From Example 2.5 we obtain an $<$-inv-FO+MOD$_2(\{E\})$-sentence $\varphi_{even\ cycles}$ that is satisfied by a finite $\{E\}$-structure $\mathcal{A}$ iff $\mathcal{A}$ is a disjoint union of directed cycles where the number of cycles of even length is even. Thus, for every $\ell \in \mathbb{N}_{\geqslant 1}$ we have: $\mathcal{A}_\ell \models \varphi_{even\ cycles}$ and $\mathcal{B}_\ell \not\models \varphi_{even\ cycles}$. We modify the formula $\varphi_{even\ cycles}$ in such a way that we obtain an $<$-inv-FO+MOD$_2(\sigma_\Sigma)$-formula $\psi(x)$ which, when evaluated in the σ_Σ-structure $\mathcal{S}_{w_\ell}$ representing the string w_ℓ with x interpreted as the position a_ℓ (respectively, the position b_ℓ), simulates $\varphi_{even\ cycles}$ evaluated on $\mathcal{A}_\ell$ (respectively, on $\mathcal{B}_\ell$). To this end, we let $\psi(x)$ be a formula stating that each of the following is satisfied:

- There is a unique position $x' \neq x$ that carries the letter 1 such that the position directly to the right of x' carries the letter 0.
- There is a unique position y of in-degree 0, and this position carries the letter 1. Furthermore, there is a unique position y' that carries the letter 1, such that the position directly to the left of y' carries the letter 0.
- The formula φ' is satisfied, where φ' is obtained from $\varphi_{even\ cycles}$ by relativisation of all quantifiers to positions that carry the letter 1, and by replacing every atom of the form $E(u,v)$ by the formula $\big(E(u,v) \vee (u{=}x \wedge v{=}y) \vee (u{=}x' \wedge v{=}y')\big)$.

Clearly, for every $\ell \in \mathbb{N}_{\geqslant 1}$ we have: $\mathcal{S}_{w_\ell} \models \psi[a_\ell]$ (since $\mathcal{A}_\ell \models \varphi_{even\ cycles}$), and $\mathcal{S}_{w_\ell} \not\models \psi[b_\ell]$ (since $\mathcal{B}_\ell \not\models \varphi_{even\ cycles}$). Thus, $a_\ell \in q_\psi(\mathcal{S}_{w_\ell})$ and $b_\ell \notin q_\psi(\mathcal{S}_{w_\ell})$. Note that the $(\ell{-}1)$-neighbourhoods of a_ℓ and b_ℓ in $\mathcal{S}_{w_\ell}$ are disjoint and isomorphic. The cardinality of $\mathcal{S}_{w_\ell}$ is $n := 4\ell$, and hence $\ell{-}1 = \frac{n}{4}{-}1$. Thus, the query defined by $\psi(x)$ is not weakly Gaifman $(\frac{n}{4}{-}1)$-local. Since $\varphi_{even\ cycles}$ is order-invariant on all finite $\{E\}$-structures, the formula $\psi(x)$ is order-invariant on the class of all finite σ_Σ-structures. Note that $\psi(x)$ is definable in $<$-inv-FO+MOD$_2(\sigma_\Sigma)$, and hence also in $<$-inv-FO+MOD$_p(\sigma_\Sigma)$, for every multiple p of 2. ◀

In light of Proposition 3.4 it is somewhat surprising that for *odd* numbers p, unary queries definable in $<$-inv-FO+MOD$_p$ are weakly Gaifman local with constant locality radius — this is a result obtained by Niemistö (see Corollary 6.37 in [11]). For *odd prime powers* p we can generalise this to k-ary queries definable in arb-inv-FO+MOD$_p$, when allowing polylogarithmic locality radius (note that we cannot hope for a smaller locality radius, since [1] provides, for every $d \in \mathbb{N}$, a unary query definable in arb-inv-FO$(\{E\})$ that is not weakly Gaifman $(\log n)^d$-local).

▶ **Theorem 3.5.** *Let $\mathfrak{C}$ be a class of finite σ-structures. Let $k \in \mathbb{N}_{\geqslant 1}$, let q be a k-ary query, and let p be an odd prime power. If q is definable in* arb-inv-FO+MOD$_p^{\mathfrak{C}}(\sigma)$ *on $\mathfrak{C}$, then there is a $c \in \mathbb{N}$ such that q is weakly Gaifman* $(\log n)^c$*-local on $\mathfrak{C}$.*

The proof of this theorem will be given in the next subsection, as an easy consequence of Theorem 3.7 below. A generalisation of Theorem 3.5 from odd prime powers to arbitrary odd numbers p would lead to new separations concerning circuit complexity classes and can therefore be expected to be rather difficult (see Remark 3.13).

3.3 Shift locality

The following notion of *shift locality* is a generalisation of the notion of *alternating Gaifman locality* introduced by Niemistö in [11].

▶ **Definition 3.6** (Shift locality)**.** Let $\mathfrak{C}$ be a class of finite σ-structures. Let $k, t \in \mathbb{N}_{\geqslant 1}$ with $t \geqslant 2$, and let $f : \mathbb{N} \to \mathbb{N}$. A kt-ary query q is *shift $f(n)$-local w.r.t. t on $\mathfrak{C}$* if there is an $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ with $n \geqslant n_0$ and every σ-structure $\mathcal{A} \in \mathfrak{C}$ with $|A| = n$, the following is true for all k-tuples $\overline{a}_0, \ldots, \overline{a}_{t-1} \in A^k$ with $(\mathcal{N}^{\mathcal{A}}_{f(n)}(\overline{a}_i), \overline{a}_i) \cong (\mathcal{N}^{\mathcal{A}}_{f(n)}(\overline{a}_j), \overline{a}_j)$ and $N^{\mathcal{A}}_{f(n)}(\overline{a}_i) \cap N^{\mathcal{A}}_{f(n)}(\overline{a}_j) = \emptyset$ for all $i, j \in [t]$ with $i \neq j$: $\quad (\overline{a}_0, \overline{a}_1 \ldots, \overline{a}_{t-1}) \in q(\mathcal{A}) \iff (\overline{a}_1, \ldots, \overline{a}_{t-1}, \overline{a}_0) \in q(\mathcal{A})$.
Query q is *shift $f(n)$-local w.r.t. t* if it is shift $f(n)$-local w.r.t. t on the class of all finite σ-structures.

In a technical lemma (Lemma 6.36 in [11]), Niemistö shows that for $k = 1$ and $p, t \in \mathbb{N}$ with $p, t \geqslant 2$ and p and t coprime, for every t-ary query q definable in $<$-inv-FO+MOD$_p(\sigma)$, there is a $c \in \mathbb{N}$ such that q is shift c-local w.r.t. t. Our next result deals with the general case of shift locality and the more expressive logic arb-inv-FO+MOD$_p(\sigma)$, when allowing polylogarithmic locality radius.

▶ **Theorem 3.7.** *Let $\mathfrak{C}$ be a class of finite σ-structures. Let $k, t \in \mathbb{N}_{\geqslant 1}$ with $t \geqslant 2$, let q be a kt-ary query, and let p be a prime power such that p and t are coprime. If q is definable in* arb-inv-FO+MOD$^{\mathfrak{C}}_p(\sigma)$ *on $\mathfrak{C}$, then there is a $c \in \mathbb{N}$ such that q is shift $(\log n)^c$-local w.r.t. t on $\mathfrak{C}$.*

Our proof of Theorem 3.7 relies on lower bounds achieved in circuit complexity. A generalisation of Theorem 3.7 from prime powers to arbitrary numbers $p \geqslant 2$ would lead to new separations of circuit complexity classes and can therefore be expected to be rather difficult (see Remark 3.13). Before giving the proof of Theorem 3.7, let us first point out that it immediately implies Theorem 3.5.

Proof of Theorem 3.5 (using Theorem 3.7). Let $\varphi(\overline{x})$ be an arb-inv-FO+MOD$^{\mathfrak{C}}_p(\sigma)$-formula with k free variables $\overline{x} = (x_1, \ldots, x_k)$, defining a k-ary query q_φ on $\mathfrak{C}$. Let $\overline{y} = (y_1, \ldots, y_k)$ be k variables different from the variables in $\overline{x}$. Then, $\psi(\overline{x}, \overline{y}) := \big(\varphi(\overline{x}) \wedge \bigwedge_{1 \leqslant i \leqslant k} y_i{=}y_i\big)$ is an arb-inv-FO+MOD$^{\mathfrak{C}}_p(\sigma)$-formula that defines a $2k$-ary query q_ψ. By Theorem 3.7, there exists a $c \in \mathbb{N}$ such that q_ψ is shift $(\log n)^c$-local w.r.t. $t := 2$ on $\mathfrak{C}$. It is straightforward to see that the shift $(\log n)^c$-locality of q_ψ w.r.t. $t = 2$ implies that the query q_φ is weakly Gaifman $(\log n)^c$-local. ◀

The remainder of this subsection is devoted to the proof of Theorem 3.7. We follow the overall method of [1] for the case of disjoint neighbourhoods (see [12] for an overview) and make use of the connection between arb-inv-FO+MOD$_p$ and MOD$_p$-circuits [3], along with a circuit lower bound by Smolensky [13].

We assume that the reader is familiar with basic notions and results in circuit complexity (cf., e.g., the textbook [2]). A MOD$_p$-gate returns the value 1 iff the number of ones at its inputs is congruent 0 modulo p. We consider Boolean MOD$_p$-*circuits* consisting of AND-, OR-, and MOD_p-gates of unbounded fan-in, input gates, negated input gates, and constant gates **0** and **1**. More precisely, a *MOD_p-circuit with m input bits* is a directed acyclic graph whose vertices without ingoing edges are called *input gates* and are labelled with either **0**, **1**, w_ν, or $\neg w_\nu$ for $\nu \in \{1, \dots, m\}$, whose internal nodes are called *gates* and are labelled either AND or OR or MOD_p, and which has a distinguished vertex without outgoing edges called the *output gate.* A MOD_p-circuit C with m input bits naturally defines a function from $\{0,1\}^m$ to $\{0,1\}$. For an input string $w \in \{0,1\}^m$ we say that C *accepts* w if $C(w) = 1$. Accordingly, C *rejects* w if $C(w) = 0$. The *size* of a circuit is the number of gates it contains, and the *depth* is the length of the longest path from the output gate to one of the input gates.

Our proof of Theorem 3.7 relies on Smolensky's following circuit lower bound.

▶ **Theorem 3.8** (Smolensky [13] (see also [14])). *Let p be a prime power. There exist numbers $\varepsilon, \ell > 0$ such that for every $d \in \mathbb{N}_{\geqslant 1}$ there is an $m_d \in \mathbb{N}_{\geqslant 1}$ such that for every $m \in \mathbb{N}$ with $m \geqslant m_d$ the following is true for every number r that has a prime factor different from p's prime factor: No MOD_p-circuit of depth d and size at most $2^{\varepsilon \sqrt[\ell d]{m}}$ accepts exactly those bitstrings $w \in \{0,1\}^m$ that contain a number of ones congruent 0 modulo r.*

In the literature, Smolensky's theorem is usually stated only for primes p. Note, however, that (for each fixed $k \in \mathbb{N}_{\geqslant 1}$) MOD_{p^k}-gates can easily be simulated by MOD_p-circuits of constant depth and polynomial size (cf., [14]), and hence Smolensky's theorem also holds for prime powers p, as stated in Theorem 3.8. It is still open whether an analogous result also holds for numbers p composed of more than one prime factor (see Chapter VIII of [14] and Chapter 14.4 of [2] for discussions on this).

To establish the connection between MOD_p-circuits and arb-inv-FO+$\mathrm{MOD}_p(\sigma)$, we need to represent σ-structures $\mathcal{A}$ and K-tuples $\overline{a} \in A^K$ (for $K \in \mathbb{N}$) by bitstrings. This is done in a straightforward way: Let $\sigma = \{R_1, \dots, R_{|\sigma|}\}$ and let $r_i := ar(R_i)$ for each $i \leqslant |\sigma|$. Consider a finite σ-structure $\mathcal{A}$ with $|A| = n$. Let ι be an embedding of $\mathcal{A}$ into $[n]$. For each $R_i \in \sigma$ we let $\mathrm{Rep}^\iota(R_i^{\mathcal{A}})$ be the bitstring of length n^{r_i} whose j-th bit is 1 iff the j-th smallest element in A^{r_i} w.r.t. the lexicographic order associated with $<^\iota$ belongs to the relation $R_i^{\mathcal{A}}$. Similarly, for each component a_i of a K-tuple $\overline{a} = (a_1, \dots, a_K) \in A^K$ we let $\mathrm{Rep}^\iota(a_i)$ be the bitstring of length n whose j-th bit is 1 iff a_i is the j-th smallest element of A w.r.t. $<^\iota$. Finally, we let

$$\mathrm{Rep}^\iota(\mathcal{A}, \overline{a}) \ := \ \ \mathrm{Rep}^\iota(R_1^{\mathcal{A}}) \ \cdots \ \mathrm{Rep}^\iota(R_{|\sigma|}^{\mathcal{A}}) \ \mathrm{Rep}^\iota(a_1) \ \cdots \ \mathrm{Rep}^\iota(a_K)$$

be the *binary representation of $(\mathcal{A}, \overline{a})$ w.r.t. ι.* Note that, independently of ι, the length of the bitstring $\mathrm{Rep}^\iota(\mathcal{A}, \overline{a})$ is $\lambda_K^\sigma(n) := \sum_{i=1}^{|\sigma|} n^{r_i} + Kn$.

The connection between FO+$\mathrm{MOD}_p(\sigma_{\mathrm{arb}})$ and MOD_p-circuits is obtained by the following result.

▶ **Theorem 3.9** (implicit in [3] (see also [14])). *Let σ be a finite relational signature, let $K \in \mathbb{N}$, and let $p \in \mathbb{N}$ with $p \geqslant 2$. For every FO+$\mathrm{MOD}_p(\sigma_{arb})$-formula $\varphi(\overline{x})$ with K free variables there exist numbers $d, s \in \mathbb{N}$ such that for every $n \in \mathbb{N}_{\geqslant 1}$ there is a MOD_p-circuit C_n with $\lambda_K^\sigma(n)$ input bits, depth d, and size n^s such that the following is true for all σ-structures $\mathcal{A}$ with $|A| = n$, all $\overline{a} \in A^K$, and all embeddings ι of $\mathcal{A}$ into $[n]$: C_n accepts $\mathrm{Rep}^\iota(\mathcal{A}, \overline{a})$ $\iff$ $\mathcal{A}^\iota \models \varphi[\overline{a}]$.*

Our proof of Theorem 3.7 uses the next two technical lemmas. To simplify notation, let $\vec{a}^{(0)} := (\overline{a}_0, \overline{a}_1, \dots, \overline{a}_{t-1})$ and $\vec{a}^{(i)} := (\overline{a}_i, \overline{a}_{i+1}, \dots, \overline{a}_{t-1}, \overline{a}_0, \overline{a}_1, \dots, \overline{a}_{i-1})$, for all $i \in [t]$ with $i \geqslant 1$.

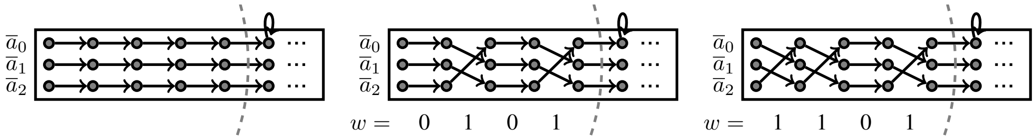

Figure 2 Illustration of a structure $\mathcal{A}$ (left) and structures $\mathcal{A}_w$ for two different bitstrings w.

▶ **Lemma 3.10.** *Let $m, k, t \in \mathbb{N}_{\geqslant 1}$ with $t \geqslant 2$. Let $\mathcal{A}$ be a finite σ-structure with $n := |A|$. For each $i \in [t]$ let $\overline{a}_i \in A^k$ such that for all $i, j \in [t]$ with $i \neq j$ we have $(\mathcal{N}_m^{\mathcal{A}}(\overline{a}_i), \overline{a}_i) \cong (\mathcal{N}_m^{\mathcal{A}}(\overline{a}_j), \overline{a}_j)$ and $N_m^{\mathcal{A}}(\overline{a}_i) \cap N_m^{\mathcal{A}}(\overline{a}_j) = \emptyset$. Let $p \in \mathbb{N}$ with $p \geqslant 2$. Let C be a MOD_p-circuit with $\lambda_{kt}^{\sigma}(n)$ input bits such that: (a) C accepts $\mathrm{Rep}^{\iota_1}(\mathcal{A}, \vec{a}^{(i)})$ iff it accepts $\mathrm{Rep}^{\iota_2}(\mathcal{A}, \vec{a}^{(i)})$, for all embeddings ι_1 and ι_2 of $\mathcal{A}$ and for every $i \in [t]$, and (b) C accepts $\mathrm{Rep}^{\iota}(\mathcal{A}, \vec{a}^{(0)})$ and rejects $\mathrm{Rep}^{\iota}(\mathcal{A}, \vec{a}^{(1)})$, for every embedding ι of $\mathcal{A}$.*

There exists a MOD_p-circuit $\tilde{C}$ with m input bits, such that: (c) $\tilde{C}$ has the same depth and size as C, (d) for all $w, w' \in \{0,1\}^m$ with $|w|_1 \equiv |w'|_1 \bmod t$, $\tilde{C}$ accepts w iff it accepts w', and (e) $\tilde{C}$ accepts all $w \in \{0,1\}^m$ with $|w|_1 \equiv 0 \bmod t$ and rejects all $w \in \{0,1\}^m$ with $|w|_1 \equiv 1 \bmod t$.

Proof. Let $I \subset [t]$ be the set containing $i \in [t]$ iff C accepts $\mathrm{Rep}^{\iota_1}(\mathcal{A}, \vec{a}^{(i)})$ for some (i.e., due to property (a) of C, *every*) embedding ι_1 of $\mathcal{A}$. By property (b) of C, we know that $0 \in I$ and $1 \notin I$.

For the remainder of this proof, fix an embedding ι of $\mathcal{A}$ into $[n]$. Note that ι is also an embedding of any other σ-structure that has the same universe as $\mathcal{A}$. For every $w \in \{0,1\}^m$, we will define a σ-structure $\mathcal{A}_w$ with the same universe as $\mathcal{A}$, which has the following property for every $i \in [t]$:

$$\text{If} \quad |w|_1 \equiv i \bmod t, \quad \text{then} \quad (\mathcal{A}_w, \vec{a}^{(0)}) \ \cong \ (\mathcal{A}, \vec{a}^{(i)}). \tag{1}$$

Note that if $(\mathcal{A}_w, \vec{a}^{(0)}) \cong (\mathcal{A}, \vec{a}^{(i)})$, then there is an embedding ι_1 such that $\mathrm{Rep}^{\iota_1}(\mathcal{A}, \vec{a}^{(i)}) = \mathrm{Rep}^{\iota}(\mathcal{A}_w, \vec{a}^{(0)})$. Hence, due to property (a), C accepts $\mathrm{Rep}^{\iota}(\mathcal{A}_w, \vec{a}^{(0)})$ iff it accepts $\mathrm{Rep}^{\iota}(\mathcal{A}, \vec{a}^{(i)})$.

The circuit $\tilde{C}$ will be constructed so that on input $w \in \{0,1\}^m$ it does the same as circuit C does on input $\mathrm{Rep}^{\iota}(\mathcal{A}_w, \vec{a}^{(0)})$. Thus, the following is true for every $w \in \{0,1\}^m$ and the particular number $i \in [t]$ such that $|w|_1 \equiv i \bmod t$:

$$\tilde{C} \text{ accepts } w \iff C \text{ accepts } \mathrm{Rep}^{\iota}(\mathcal{A}_w, \vec{a}^{(0)}) \iff C \text{ accepts } \mathrm{Rep}^{\iota}(\mathcal{A}, \vec{a}^{(i)}) \iff i \in I.$$

This immediately implies that $\tilde{C}$ satisfies property (d); and since $0 \in I$ and $1 \notin I$, the circuit $\tilde{C}$ also satisfies property (e).

Definition of $\mathcal{A}_w$: For each $j \in [t]$, we partition $N_m^{\mathcal{A}}(\overline{a}_j)$ into *shells* $S_\nu(\overline{a}_j) := \{x \in A : \mathit{dist}^{\mathcal{A}}(x, \overline{a}_j) = \nu\}$, for all $\nu \in \{0, \ldots, m\}$. We write S_ν for the set $S_\nu(\overline{a}_0) \cup \cdots \cup S_\nu(\overline{a}_{t-1})$. For each $j \in [t]$ let π_j be an isomorphism from $(\mathcal{N}_m^{\mathcal{A}}(\overline{a}_j), \overline{a}_j)$ to $(\mathcal{N}_m^{\mathcal{A}}(\overline{a}_{(j+1 \bmod t)}), \overline{a}_{(j+1 \bmod t)})$. Note that $\pi_j(S_\nu(\overline{a}_j)) = S_\nu(\overline{a}_{(j+1 \bmod t)})$ for each $j \in [t]$ and each $\nu \leqslant m$.

For a bitstring $w = w_1 \cdots w_m \in \{0,1\}^m$ the structure $\mathcal{A}_w$ has the same universe as $\mathcal{A}$. For each $R \in \sigma$ of arity r, the relation $R^{\mathcal{A}_w}$ is obtained from $R^{\mathcal{A}}$ as follows: We start with $R^{\mathcal{A}_w} := \emptyset$, and then for each tuple $\overline{c} \in R^{\mathcal{A}}$ we insert the tuple $\overline{c}_w$ into $R^{\mathcal{A}_w}$, where $\overline{c}_w$ is defined as follows:

- If $\overline{c} \notin (S_{\nu-1} \cup S_\nu)^r$ for any $\nu \leqslant m$, or $\overline{c} \in S_\nu^r$ for some $\nu \leqslant m$, then $\overline{c}_w := \overline{c}$.
- Otherwise, if $\overline{c} \in (S_{\nu-1} \cup S_\nu)^r$ for some $\nu \leqslant m$, then note that (since $\overline{c} \in R^{\mathcal{A}}$), there is a unique $j \in [t]$ such that $\overline{c} \in (S_{\nu-1}(\overline{a}_j) \cup S_\nu(\overline{a}_j))^r$ (since $N_m^{\mathcal{A}}(\overline{a}_j) \cap N_m^{\mathcal{A}}(\overline{a}_{j'}) = \emptyset$, for all

$j, j' \in [t]$ with $j \neq j'$). To keep the notation simple, assume that $\overline{c} = (\overline{c}_{\nu-1}, \overline{c}_\nu)$, where all elements of $\overline{c}_{\nu-1}$ belong to $S_{\nu-1}(\overline{a}_j)$ and all elements of $\overline{c}_\nu$ belong to $S_\nu(\overline{a}_j)$. We define $\overline{c}_w$ depending on the ν-th bit w_ν of w: If $w_\nu = 0$, then $\overline{c}_w := \overline{c}$. If $w_\nu = 1$, then $\overline{c}_w := (\overline{c}_{\nu-1}, \pi_j(\overline{c}_\nu))$.

Note that for every $\nu \in \{1, \dots, m\}$ with $w_\nu = 1$, this construction enforces that the role that was formerly played by shell $S_\nu(\overline{a}_j)$ is afterwards played by shell $S_\nu(\overline{a}_{(j+1 \bmod t)})$; see Figure 2 for an illustration. It is easy to verify that if $|w|_1 \equiv i \bmod t$, then $(\mathcal{A}_w, \vec{a}^{(0)}) \cong (\mathcal{A}, \vec{a}^{(i)})$.

Construction of $\tilde{C}$: The circuit $\tilde{C}$ is obtained from C by replacing the input gates of C in a way that mirrors the construction of $\mathcal{A}_w$ above, in the same way as done in [1]: Each input gate g of C is replaced either by a constant gate **0** or **1** or by a new input gate w_ν or its negation $\neg w_\nu$. In particular, $\tilde{C}$ has the same depth as C, and the size of $\tilde{C}$ is smaller than or equal to the size of C. ◀

▶ **Lemma 3.11.** *Let $m, d, M, t, p \in \mathbb{N}_{\geqslant 1}$ with $m > 9$ and $p, t \geqslant 2$ such that p and t are coprime. Let $\tilde{C}$ be a MOD_p-circuit of depth d and size M which has the property that for all words $w, w' \in \{0,1\}^m$ with $|w|_1 \equiv |w'|_1 \bmod t$, it accepts w iff it accepts w'. Furthermore, let $\tilde{C}$ accept all $w \in \{0,1\}^m$ with $|w|_1 \equiv 0 \bmod t$, and reject all $w \in \{0,1\}^m$ with $|w|_1 \equiv 1 \bmod t$.*

There is a MOD_p-circuit $\hat{C}$ of depth $(d{+}6)$ and size $(tM{+}2m^t)$ which, for some factor $r \geqslant 2$ of t, accepts exactly those bitstrings $w \in \{0,1\}^m$ where $|w|_1 \equiv 0 \bmod r$.

Proof. We let $b = b_0 b_1 \cdots b_{t-1}$ be the bitstring of length t where, for every $j \in [t]$ we have $b_j = 1$ iff $\tilde{C}$ accepts bitstrings $w \in \{0,1\}^m$ with $|w|_1 \equiv j \bmod t$.

For a bitstring $w \in \{0,1\}^m$ with $|w|_0 \geqslant t{-}1$, we let $\mathit{pattern}(w) = a_0 a_1 \cdots a_{t-1} \in \{0,1\}^t$ with $a_j = 1$ iff $\tilde{C}$ accepts the bitstring obtained from w by replacing the first j zeros with ones. Note that if $|w|_1 \equiv i \bmod t$, then $\mathit{pattern}(w) = b_i b_{i+1} \cdots b_{t-1} b_0 \cdots b_{i-1}$.

▶ **Claim.** *There is a factor $r \geqslant 2$ of t such that for all $w \in \{0,1\}^m$ with $|w|_0 \geqslant t{-}1$ we have: $\mathit{pattern}(w) = b \iff |w|_1 \equiv 0 \bmod r$.*

Proof. In case that $\mathit{pattern}(w) = b$ iff $|w|_1 \equiv 0 \bmod t$, we are done by choosing $r := t$. In case that there is a w with $\mathit{pattern}(w) = b$ and $|w|_1 \equiv i \bmod t$ for an $i \in \{1, \dots, t{-}1\}$, we know that $b_0 b_1 \cdots b_{t-1} = b_i b_{i+1} \cdots b_{t-1} b_0 \cdots b_{i-1}$. Thus, for $x := b_0 \cdots b_{i-1}$ and $y := b_i \cdots b_{t-1}$ we have $b = xy = yx$, and $x, y \in \{0,1\}^+$.

A basic result in word combinatorics (see Proposition 1.3.2 in [10]) states that two words $x, y \in \{0,1\}^+$ commute (i.e., $xy = yx$) iff they are powers of the same word (i.e., there is a $z \in \{0,1\}^+$ and $\nu, \mu \in \mathbb{N}_{\geqslant 1}$ such that $x = z^\nu$ and $y = z^\mu$). We choose $z \in \{0,1\}^+$ of minimal length such that $b = z^s$ for some $s \in \mathbb{N}$. Clearly, $|z| \geqslant 2$, since by assumption we have $b_0 b_1 = 10$.

Since z is of minimal length, it is straightforward to see that for every $w \in \{0,1\}^m$ with $|w|_0 \geqslant t{-}1$ we have: $\mathit{pattern}(w) = z^s \iff |w|_1 \equiv 0 \bmod |z|$. ◀

We choose r according to the claim. Obviously, the following is true for every $w \in \{0,1\}^m$:

$$|w|_1 \equiv 0 \bmod r \iff \begin{cases} (1) & |w|_0 \geqslant t{-}1 \ \text{ and } \ \mathit{pattern}(w) = b, \ \text{ or} \\ (2) & \text{there is a } j \in [t{-}1] \text{ with } m{-}j \equiv 0 \bmod r \text{ such that } |w|_0 = j. \end{cases}$$

To complete the proof of Lemma 3.11, it therefore suffices to construct circuits $C_{(1)}$ and $C_{(2)}$ testing for (1) and (2), respectively, and to let $\hat{C}$ be the disjunction of $C_{(1)}$ and $C_{(2)}$. It is an easy exercise to construct these circuits, using the given circuit $\tilde{C}$, in such a way that the resulting circuit $\hat{C}$ has depth $\leqslant (d{+}6)$ and size $\leqslant (tM + 2m^t)$. ◀

We are now ready for the proof of Theorem 3.7.

Proof of Theorem 3.7. Let q be a kt-ary query defined on $\mathfrak{C}$ by an arb-inv-FO+MOD$_p^{\mathfrak{C}}(\sigma)$-formula $\varphi(\overline{x}_0,\dots,\overline{x}_{t-1})$, where $\overline{x}_i$ is a k-tuple of variables, for each $i \in [t]$. By Theorem 3.9, there exist numbers $d, s \in \mathbb{N}$ such that for every $n \in \mathbb{N}_{\geqslant 1}$ there is a MOD$_p$-circuit C_n with $\lambda^{\sigma}_{kt}(n)$ input bits, depth d, and size n^s such that the following is true for all σ-structures $\mathcal{A} \in \mathfrak{C}$ with $|A| = n$, all k-tuples $\overline{a}_0,\dots,\overline{a}_{t-1} \in A^k$, and all embeddings ι of $\mathcal{A}$ into $[n]$:

$$C_n \text{ accepts } \mathrm{Rep}^{\iota}(\mathcal{A},\overline{a}_0,\dots,\overline{a}_{t-1}) \iff \mathcal{A}^{\iota} \models \varphi[\overline{a}_0,\dots,\overline{a}_{t-1}] \iff \mathcal{A} \models \varphi[\overline{a}_0,\dots,\overline{a}_{t-1}].$$

For contradiction, assume that for every $c \in \mathbb{N}$ the query q is *not* shift $(\log n)^c$-local w.r.t. t on $\mathfrak{C}$. Thus, in particular for $c := 2\ell(d{+}6)$ (with ℓ chosen as in Theorem 3.8), we obtain that for all $n_0 \in \mathbb{N}$ there is an $n \geqslant n_0$, and a σ-structure $\mathcal{A} \in \mathfrak{C}$ with $|A| = n$, and k-tuples $\overline{a}_0,\dots,\overline{a}_{t-1} \in A^k$ such that for $m := (\log n)^c = (\log n)^{2\ell(d+6)}$ we have:

- $(\mathcal{N}^{\mathcal{A}}_m(\overline{a}_i),\overline{a}_i) \cong (\mathcal{N}^{\mathcal{A}}_m(\overline{a}_j),\overline{a}_j)$ and $N^{\mathcal{A}}_m(\overline{a}_i) \cap N^{\mathcal{A}}_m(\overline{a}_j) = \emptyset$ for all $i, j \in [t]$ with $i \neq j$, and
- $\mathcal{A} \models \varphi[\overline{a}_0,\overline{a}_1,\dots,\overline{a}_{t-1}]$ and $\mathcal{A} \not\models \varphi[\overline{a}_1,\dots,\overline{a}_{t-1},\overline{a}_0]$.

We fix $n \in \mathbb{N}$ sufficiently large such that, for $\hat{d} := (d{+}6)$ and ε and $m_{\hat{d}}$ chosen as in Theorem 3.8, we have for $m = (\log n)^c$ that $m > 9$, $m \geqslant m_{\hat{d}}$, and $n^{\varepsilon \log n} > tn^s + 2(\log n)^{ct}$.

Clearly, C_n is a MOD$_p$-circuit with $\lambda^{\sigma}_{kt}(n)$ input bits which, for every $i \in [t]$ and all embeddings ι_1 and ι_2 of $\mathcal{A}$ accepts $\mathrm{Rep}^{\iota_1}(\mathcal{A},\vec{a}^{(i)})$ iff it accepts $\mathrm{Rep}^{\iota_2}(\mathcal{A},\vec{a}^{(i)})$. Furthermore, C_n accepts $\mathrm{Rep}^{\iota}(\mathcal{A},\vec{a}^{(0)})$ and rejects $\mathrm{Rep}^{\iota}(\mathcal{A},\vec{a}^{(1)})$, for every embedding ι of $\mathcal{A}$. Thus, from Lemma 3.10 we obtain a MOD$_p$-circuit $\tilde{C}$ on m input bits, with depth d and size n^s, such that $\tilde{C}$ has the property that for all words $w, w' \in \{0,1\}^m$ with $|w|_1 \equiv |w'|_1 \bmod t$, it accepts w iff it accepts w'. Furthermore, $\tilde{C}$ accepts all $w \in \{0,1\}^m$ with $|w| \equiv 0 \bmod t$ and rejects all $w \in \{0,1\}^m$ with $|w| \equiv 1 \bmod t$. From Lemma 3.11, we therefore obtain a MOD$_p$-circuit $\hat{C}$ of depth $\hat{d} := (d{+}6)$ and size $(tn^s + 2m^t) = (tn^s + 2(\log n)^{ct})$ which, for some factor $r \geqslant 2$ of t, accepts exactly those bitstrings $w \in \{0,1\}^m$ where $|w|_1 \equiv 0 \bmod r$.

Since p and t are coprime by assumption, and $r \geqslant 2$ is a factor of t, we know that r has a prime factor different from p's prime factor. Thus, from Theorem 3.8 (for $\varepsilon, \ell, m_{\hat{d}}$ chosen as in Theorem 3.8, and for $m \geqslant m_{\hat{d}}$) we know that the size $(tn^s + 2(\log n)^{ct})$ of $\hat{C}$ must be bigger than $2^{\varepsilon \sqrt[\ell\hat{d}]{m}}$. However, we chose $m = (\log n)^c = (\log n)^{2\ell\hat{d}}$, and hence $2^{\varepsilon \sqrt[\ell\hat{d}]{m}} = 2^{\varepsilon\cdot(\log n)^2} = n^{\varepsilon\cdot\log n} > tn^s + 2(\log n)^{ct}$ for all sufficiently large n — a contradiction! Thus, the proof of Theorem 3.7 is complete. ◀

3.4 Applications

In the same way as Gaifman locality (cf., e.g., [9]), also shift locality can be used for showing that certain queries are not expressible in particular logics. The first example query we consider here is the reachability query *reach* which associates, with every finite directed graph $\mathcal{A} = (A, E^{\mathcal{A}})$, the relation

$$\mathit{reach}(\mathcal{A}) := \{(a,b) \,:\, \mathcal{A} \text{ contains a directed path from node } a \text{ to node } b\}.$$

▶ **Proposition 3.12.** *Let $\sigma = \{E\}$ consist of a binary relation symbol E. Let $p, t \in \mathbb{N}$ with $p, t \geqslant 2$ be chosen such that every t-ary query q definable in* arb-inv-FO+MOD$_p(\sigma)$ *is shift $f_q(n)$-local w.r.t. t, for a function $f_q : \mathbb{N} \to \mathbb{N}$ where $f_q(n) \leqslant (\frac{n}{2t} - \frac{1}{2})$ for all sufficiently large n. Then, the reachability query is not definable in* arb-inv-FO+MOD$_p(\sigma)$.

Proof. Assume, for contradiction, that *reach* is definable by an arb-inv-FO+MOD$_p(\sigma)$-formula $\varrho(x,y)$. Then, $\psi(x_0,\dots,x_{t-1}) := \varrho(x_0,x_1) \wedge \varrho(x_1,x_2) \wedge \cdots \wedge \varrho(x_{t-2},x_{t-1})$ is an arb-inv-FO+MOD$_p(\sigma)$-formula expressing in a finite graph $\mathcal{A}$, that there is a directed path from node x_i to node x_{i+1}, for every $i \in [t{-}1]$. Let q be the t-ary query defined by $\psi(x_0,\ldots,x_{t-1})$. By assumption, this query is shift $f_q(n)$-local w.r.t. t, for a function f_q with $f_q(n) \leqslant \frac{n}{2t}-\frac{1}{2}$ for all sufficiently large n.

Now, consider for each $\ell \in \mathbb{N}_{\geqslant 1}$ the graph $\mathcal{A}_\ell$ consisting of a single directed path $v_1 \to v_2 \to \cdots \to v_{t(2\ell+1)}$ on $t{\cdot}(2\ell{+}1)$ nodes. For each $i \in [t]$ let $a_i := v_{i(2\ell+1)+(\ell+1)}$. Then, the ℓ-neighbourhoods of the a_i, for $i \in [t]$, are pairwise disjoint and isomorphic. The cardinality of $\mathcal{A}_\ell$ is $n := t{\cdot}(2\ell{+}1)$, and thus $\ell = \frac{n}{2t}-\frac{1}{2} \geqslant f_q(n)$. Since q is shift $f_q(n)$-local w.r.t. t, we obtain that $\mathcal{A}_\ell \models \psi[a_0,a_1,\ldots,a_{t-1}] \iff \mathcal{A}_\ell \models \psi[a_1,\ldots,a_{t-1},a_0]$. But in $\mathcal{A}_\ell$ there is a directed path from a_i to a_{i+1} for every $i \in [t{-}1]$, but there is no directed path from a_{t-1} to a_0. Due to the choice of ψ, we have that $\mathcal{A}_\ell \models \psi[a_0,a_1,\ldots,a_{t-1}]$ but $\mathcal{A}_\ell \not\models \psi[a_1,\ldots,a_{t-1},a_0]$ — a contradiction! ◀

As an immediate consequence of Proposition 3.12 and Theorem 3.7 we obtain (the known fact) that the reachability query is not definable in arb-inv-FO+MOD$_p(\{E\})$, for any prime power p. Using similar constructions, it is an easy exercise to show that none of the following queries is definable in arb-inv-FO+MOD$_p(\{E\})$, for any prime power p:

- $\mathit{cycle}(\mathcal{A}) := \{a \in A \,:\, a \text{ is a node that lies on a cycle of the graph } \mathcal{A} = (A, E^{\mathcal{A}})\}$,
- $\mathit{triangle\text{-}reach}(\mathcal{A}) := \{a \in A \,:\, a \text{ is reachable from a triangle in the graph } \mathcal{A} = (A, E^{\mathcal{A}})\}$,
- $\mathit{same\text{-}distance}(\mathcal{A}) := \{(a,b,c) \in A^3 \,:\, \mathit{dist}^{\mathcal{A}}(a,c) = \mathit{dist}^{\mathcal{A}}(b,c)\}$.

We close with a remark explaining why it can be expected to be difficult to generalise Theorem 3.5 and Theorem 3.7 from prime powers p to arbitrary numbers $p \geqslant 2$.

▶ **Remark 3.13.** Assume, we could generalise Theorem 3.7 from prime powers p to arbitrary numbers $p \geqslant 2$. By Proposition 3.12, we would then obtain that the reachability query is not definable in arb-inv-FO+MOD$_p(\{E\})$, for any $p \in \mathbb{N}$ with $p \geqslant 2$. The “opposite direction” of Theorem 3.9, obtained in [3], would then tell us that the reachability query is not computable in ACC^0. Here, ACC$^0 = \bigcup_{p\geqslant 2}$ AC$^0[p]$, where AC$^0[p]$ is the class of all problems computable by a family of constant depth, polynomial size MOD$_p$-circuits. Since the reachability query can be computed in nondeterministic logarithmic space, we would thus obtain that NLOGSPACE $\not\subseteq$ ACC^0. This would constitute a major breakthrough in computational complexity: The current state-of-the-art (see [15] for a recent survey) states that NEXP $\not\subseteq$ ACC^0, but does not know a problem in PTIME that provably does not belong to ACC^0.

Similarly, a generalisation of Theorem 3.5 to all odd numbers p would imply that the reachability query is not definable in AC$^0[p]$, for any odd number p. Also this is currently not known.

4 Hanf locality and locality on string structures

For giving the precise definition of Hanf locality, we need the following notation: As in [9], for σ-structures $\mathcal{A}$ and $\mathcal{B}$, for k-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$, and for an $r \in \mathbb{N}$, we write $(\mathcal{A},\overline{a}) \leftrightarrows_r (\mathcal{B},\overline{b})$ (or simply $\mathcal{A} \leftrightarrows_r \mathcal{B}$ in case that $k{=}0$) if there is a bijection $\beta : A \to B$ such that $(\mathcal{N}_r^{\mathcal{A}}(\overline{a}c), \overline{a}c) \cong (\mathcal{N}_r^{\mathcal{B}}(\overline{b}\beta(c)), \overline{b}\beta(c))$ is true for every $c \in A$.

▶ **Definition 4.1** (Hanf locality). Let $\mathfrak{C}$ be a class of finite σ-structures, $k \in \mathbb{N}$, and $f : \mathbb{N} \to \mathbb{N}$. A k-ary query q is *Hanf $f(n)$-local on* $\mathfrak{C}$ if there is an $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}$ with $n \geqslant n_0$ and all σ-structures $\mathcal{A}, \mathcal{B} \in \mathfrak{C}$ with $|A| = |B| = n$, the following is true for all k-tuples $\overline{a} \in A^k$ and $\overline{b} \in B^k$ with $(\mathcal{A},\overline{a}) \leftrightarrows_{f(n)} (\mathcal{B},\overline{b})$: $\quad \overline{a} \in q(\mathcal{A}) \iff \overline{b} \in q(\mathcal{B})$.

The query q is called *Hanf* $f(n)$*-local* if it is Hanf $f(n)$-local on the class of all finite σ-structures.

Hanf locality is an even stronger locality notion than Gaifman locality:

▶ **Theorem 4.2** (Hella, Libkin, Nurmonen [8]). *Let* $\mathfrak{C}$ *be a class of finite* σ*-structures and let* $f : \mathbb{N} \to \mathbb{N}$*. Let* $k \in \mathbb{N}_{\geqslant 1}$ *and let* q *be a* k*-ary query. If* q *is Hanf* $f(n)$*-local on* $\mathfrak{C}$*, then* q *is Gaifman* $(3f(n){+}1)$*-local on* $\mathfrak{C}$*.*

It is well-known that queries definable in FO or FO+MOD$_p$ (for any $p \geqslant 2$) are Hanf local with a constant locality radius [6, 8]. For order-invariant or arb-invariant FO it is still open whether they are Hanf local with respect to any sublinear locality radius. As an immediate consequence of Proposition 3.2 and Theorem 4.2 one obtains for every $p \in \mathbb{N}$ with $p \geqslant 2$ that order-invariant FO+MOD$_p$ is *not* Hanf local with respect to any sublinear locality radius.

For the restricted case of string structures, Benedikt and Segoufin [4] have shown that on Σ-*strings* order-invariant FO has the same expressive power as FO and thus is Hanf local with constant locality radius (in fact, [4] obtains the same result also for finite labelled ranked trees). In [1] it was shown that every query definable in arb-invariant FO on Σ-*strings* is Hanf local with polylogarithmic locality radius, and that in the worst case the locality radius can indeed be of polylogarithmic size. As an immediate consequence of Proposition 3.4 and Theorem 4.2 we obtain that for $\Sigma := \{0, 1\}$ there is a unary query q that is *not* Hanf $(\frac{n}{4}{-}1)$-local on Σ-*strings*, but definable in $<$-inv-FO+MOD$_p(\sigma_\Sigma)$ for every *even* number $p \geqslant 2$. A modification of the proof of Proposition 3.4 also leads to an example of a *Boolean* query (i.e., a 0-ary query) that is not Hanf $(\frac{n-1}{8})$-local on Σ-*strings* for $\Sigma := \{0, 1, 2\}$. Together with the Hanf locality of FO+MOD$_p$, this implies that the result of Benedikt and Segoufin [4] cannot be lifted from order-invariant FO to order-invariant FO+MOD$_p$ on Σ-*strings*, for even numbers $p \geqslant 2$, thus refuting a conjecture of [4].

From Niemistö's Corollary 7.25 in [11] it follows that for *odd* numbers p, order-invariant FO+MOD$_p(\sigma_\Sigma)$ on Σ-*strings* has exactly the same expressive power as FO+MOD$_{\mathrm{PFC}(p)}(\sigma_\Sigma)$, where PFC$(p)$ is the set of all numbers whose prime factors are prime factors of p, and FO+MOD$_{\mathrm{PFC}(p)}$ is first-order logic with modulo m counting quantifiers for all $m \in \mathrm{PFC}(p)$.

The present section's main result shows that for *odd prime powers* p, the Hanf locality result of [1] can be generalised from arb-invariant FO to arb-invariant FO+MOD$_p$ on Σ-*strings*:

▶ **Theorem 4.3.** *Let* Σ *be a finite alphabet. Let* $k \in \mathbb{N}$*, let* q *be a* k*-ary query, and let* p *be an odd prime power. If* q *is definable in* arb-inv-FO+MOD$_p^{\Sigma\text{-}strings}(\sigma_\Sigma)$ *on* Σ*-strings, then there is a* $c \in \mathbb{N}$ *such that* q *is Hanf* $(\log n)^c$*-local on* Σ*-strings.*

Together with Theorem 4.2 this implies (general instead of weak) Gaifman locality on Σ-*strings*:

▶ **Corollary 4.4.** *Let* Σ *be a finite alphabet. Let* $k \in \mathbb{N}_{\geqslant 1}$*, let* q *be a* k*-ary query, and let* p *be an odd prime power. If* q *is definable in* arb-inv-FO+MOD$_p^{\Sigma\text{-}strings}(\sigma_\Sigma)$ *on* Σ*-strings, then there is a* $c \in \mathbb{N}$ *such that* q *is Gaifman* $(\log n)^c$*-local on* Σ*-strings.*

Note that this corollary does not contradict the non-locality result of Proposition 3.2, as the counter-example given in the proof of that proposition is not a string structure.

The remainder of this section is devoted to the proof of Theorem 4.3. We follow the overall approach of [1]. The crucial step is to prove Theorem 4.3 for queries q of arity $k = 0$; the case for queries of arity $k \geqslant 1$ can easily be reduced to the case for queries of arity 0 by adding k extra symbols to the alphabet (see Section 5.3 in [1] for details).

Note that a 0-ary query q defines the string-language $L_q := \{w \in \Sigma^+ : () \in q(\mathcal{S}_w)\}$, where () denotes the unique tuple of arity 0. The language L_q is called *Hanf $f(n)$-local* iff q is Hanf $f(n)$-local on Σ*-strings*. For proving Theorem 4.3 for the case $k = 0$, we consider the following notion.

▶ **Definition 4.5** (Disjoint swaps [1]). Let $r \in \mathbb{N}$ and let $w \in \Sigma^+$ be a string over a finite alphabet Σ. A string $w' \in \Sigma^+$ is obtained from w by a *disjoint r-swap operation* if there exist strings $\mathtt{x}, \mathtt{u}, \mathtt{y}, \mathtt{v}, \mathtt{z}$ such that $w = \mathtt{xuyvz}$ and $w' = \mathtt{xvyuz}$, and for the positions i, j, i', j' of w just before $\mathtt{u}, \mathtt{y}, \mathtt{v}, \mathtt{z}$ the following is true: The neighbourhoods $N_r^{\mathcal{S}_w}(i)$, $N_r^{\mathcal{S}_w}(j)$, $N_r^{\mathcal{S}_w}(i')$, $N_r^{\mathcal{S}_w}(j')$ are pairwise disjoint, and $(\mathcal{N}_r^{\mathcal{S}_w}(i), i) \cong (\mathcal{N}_r^{\mathcal{S}_w}(i'), i')$ and $(\mathcal{N}_r^{\mathcal{S}_w}(j), j) \cong (\mathcal{N}_r^{\mathcal{S}_w}(j'), j')$.

Let $f : \mathbb{N} \to \mathbb{N}$. A string-language $L \subseteq \Sigma^+$ is *closed under disjoint $f(n)$-swaps* if there exists an $n_0 \in \mathbb{N}$ such that for every $n \in \mathbb{N}_{\geqslant 1}$ with $n \geqslant n_0$, all strings $w \in \Sigma^+$ of length n, and all strings w' obtained from w by a disjoint $f(n)$-swap operation, we have: $w \in L \iff w' \in L$.

It was shown in [1] (see Proposition 5.7, Lemma 5.2, and the proof of Theorem 5.1 in [1]) that if a language $L \subseteq \Sigma^+$ is closed under disjoint $(\log n)^d$-swaps, for some $d \in \mathbb{N}$, then it is Hanf $(\log n)^c$-local on Σ*-strings*, for some $c > d$. Hence, the following lemma immediately implies Theorem 4.3 for the case $k = 0$.

▶ **Lemma 4.6.** *Let Σ be a finite alphabet, let $L \subseteq \Sigma^+$, and let p be an odd prime power. If L is definable, on Σ-strings, by an* arb-inv-FO+MOD$_p^{\Sigma\text{-}strings}(\sigma_\Sigma)$*-sentence, then there exists a constant $d \in \mathbb{N}$ such that L is closed under disjoint* $(\log n)^d$*-swaps.*

Proof sketch. We proceed in the same way as in the proof of Proposition 5.5 in [1], which obtained the analogue of Lemma 4.6 for arb-inv-FO$^{\Sigma\text{-}strings}(\sigma_\Sigma)$-sentences. By contradiction, assume that there does not exist any $d \in \mathbb{N}$ such that the language L is closed under disjoint $(\log n)^d$-swaps. Then, for any choice of $d, n_0 \in \mathbb{N}$ there exist strings w and w' of length $n \geqslant n_0$ which witness the violation of the “closure under disjoint $(\log n)^d$-swaps” property.

The proof of [1] then proceeds as follows: Choose an appropriate extension $\tilde{\sigma}$ of the signature σ_Σ, define a suitable $\tilde{\sigma}$-structure $\mathcal{A}_w$, and modify the sentence φ defining L to obtain a formula $\psi(\overline{x})$, so that for suitably chosen tuples $\overline{a}$ and $\overline{a}'$ of elements in A_w, the following is true: On $\mathcal{A}_w$, the formula $\psi(\overline{x})$ simulates the evaluation of φ in $\mathcal{S}_w$ (resp., $\mathcal{S}_{w'}$) when assigning the values $\overline{a}$ (resp., $\overline{a}'$) to the variables $\overline{x}$. In [1], $\psi(\overline{x})$ and $\mathcal{A}_w$ are constructed in such a way that $\overline{a}$ and $\overline{a}'$ witness a violation of the Gaifman locality (with a polylogarithmic locality radius) of arb-invariant FO($\tilde{\sigma}$).

However, in the present case we consider arb-invariant FO+MOD$_p(\tilde{\sigma})$, and thus we only have available the *weak* Gaifman locality result stated in Theorem 3.5. Therefore, we have to choose $\mathcal{A}_w$ and $\psi(\overline{x})$ more carefully, so that we can conclude by using only *weak* Gaifman locality. ◀

References

1 M. Anderson, D. van Melkebeek, N. Schweikardt, and L. Segoufin. Locality from circuit lower bounds. *SIAM Journal on Computing*, 41(6):1481–1523, 2012.

2 S. Arora and B. Barak. *Computational Complexity: A Modern Approach.* Cambridge Univ. Press, 2009.

3 D. A. M. Barrington, N. Immerman, and H. Straubing. On uniformity within NC^1. *J. Comput. Syst. Sci.*, 41(3):274–306, 1990.

4 M. Benedikt and L. Segoufin. Towards a characterization of order-invariant queries over tame structures. *Journal of Symbolic Logic*, 74(1):168–186, 2009.

5 H.-D. Ebbinghaus and J. Flum. *Finite model theory.* Springer, 1999.

6 R. Fagin, L. J. Stockmeyer, and M. Y. Vardi. On Monadic NP vs. Monadic co-NP. *Information and Computation*, 120(1):78–92, 1995.

7 M. Grohe and T. Schwentick. Locality of order-invariant first-order formulas. *ACM Transactions on Computational Logic*, 1(1):112–130, 2000.

8 L. Hella, L. Libkin, and J. Nurmonen. Notions of locality and their logical characterizations over finite models. *Journal of Symbolic Logic*, 64(4):1751–1773, 1999.

9 L. Libkin. *Elements of Finite Model Theory.* Springer, 2004.

10 M. Lothaire. *Combinatorics on words.* Cambridge University Press, 1984.

11 H. Niemistö. *Locality and Order-Invariant Logics.* PhD thesis, Department of Mathematics and Statistics, University of Helsinki, 2007.

12 N. Schweikardt. A short tutorial on order-invariant first-order logic. In *Proc. 8th Int'l Computer Science Symposium in Russia (CSR'13)*, pages 112–126, 2013.

13 R. Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proc. STOC'87*, pages 77–82, 1987.

14 H. Straubing. *Finite Automata, Formal Logic, and Circuit Complexity.* Birkhäuser, 1994.

15 R. Williams. Guest column: A casual tour around a circuit complexity bound. *SIGACT News*, 42(3):54–76, 2011.