# Slicewise Definability in First-Order Logic with Bounded Quantifier Rank*

**Yijia Chen[1], Jörg Flum[2], and Xuangui Huang[3]**

1 **School of Computer Science, Fudan University, Shanghai, China**
yijiachen@fudan.edu.cn
2 **Mathematisches Institut, Universität Freiburg, Germany**
joerg.flum@math.uni-freiburg.de
3 **Department of Computer Science, Shanghai Jiao Tong University, China**
stslxg@gmail.com

**Abstract**

For every $q \in \mathbb{N}$ let $\mathrm{FO}_q$ denote the class of sentences of first-order logic FO of quantifier rank at most $q$. If a graph property can be defined in $\mathrm{FO}_q$, then it can be decided in time $O(n^q)$. Thus, minimizing $q$ has favorable algorithmic consequences. Many graph properties amount to the existence of a certain set of vertices of size $k$. Usually this can only be expressed by a sentence of quantifier rank at least $k$. We use the color coding method to demonstrate that some (hyper)graph problems can be defined in $\mathrm{FO}_q$ where $q$ is independent of $k$. This property of a graph problem is equivalent to the question of whether the corresponding parameterized problem is in the class para-$\mathrm{AC}^0$.

It is crucial for our results that the FO-sentences have access to built-in addition and multiplication (and constants for an initial segment of natural numbers whose length depends only on $k$). It is known that then FO corresponds to the circuit complexity class uniform $\mathrm{AC}^0$. We explore the connection between the quantifier rank of FO-sentences and the depth of $\mathrm{AC}^0$-circuits, and prove that $\mathrm{FO}_q \subsetneq \mathrm{FO}_{q+1}$ for structures with built-in addition and multiplication.

**1998 ACM Subject Classification** F.1.1 [Models of Computation] Unbounded-Action Devices), F.1.3 [Complexity Measures and Classes] Complexity Hierarchies, F.4.1 [Mathematical Logic] Computational logic

**Keywords and phrases** first-order logic, quantifier rank, parameterized $\mathrm{AC}^0$, circuit depth

**Digital Object Identifier** 10.4230/LIPIcs.CSL.2017.19

## 1 Introduction

Many graph problems ask, given a graph $\mathcal{G}$ and a natural number $k$, for a set $C$ of vertices of $\mathcal{G}$ of size $k$ with a certain property. A well-known example is the *vertex cover problem* where the set $C$ is required to have the property that every edge in $\mathcal{G}$ has at least one end in $C$. The set $C$ is then called a *vertex cover* of $\mathcal{G}$ of size $k$. It is routine to show that the vertex cover problem is not in the complexity class $\mathrm{AC}^0$. However, its parameterized version $p$-Vertex-Cover, that is,

| $p$-Vertex-Cover | |
|---|---|
| *Input:* | A graph $\mathcal{G}$. |
| *Parameter:* | $k$. |
| *Question:* | Does $\mathcal{G}$ have a vertex cover of size $k$? |

* This research is partially supported by the Sino-German Center for Research Promotion (CDZ 996) and National Nature Science Foundation of China (Project 61373029).

is in the class para-$\mathrm{AC}^0$ [7], the parameterized version of $\mathrm{AC}^0$.

If in $p$-VERTEX-COVER we fix the parameter $k$, we get the *kth slice* of the problem. Clearly, the existence of a vertex cover of size $k$ can be expressed by the following sentence of first-order logic FO

$$\psi_k := \exists x_1 \cdots \exists x_k \Big( \bigwedge_{1 \le i < j \le k} x_i \ne x_j \wedge \forall u \forall v \big( Euv \to \bigvee_{i=1}^{k} (u = x_i \vee v = x_i) \big) \Big). \tag{1}$$

In other words, a graph $\mathcal{G}$ is in the $k$th slice of $p$-VERTEX-COVER if and only if $\mathcal{G}$ satisfies $\psi_k$. Observe that the quantifier rank $\mathrm{qr}(\psi_k)$ of $\psi_k$, the maximum nested depth of quantifiers in $\psi_k$, is $k+2$. Hence the naive algorithm derived from $\psi_k$ has running time $O(|\mathcal{G}|^{k+2})$. Clearly it is far worse than the existing linear time algorithms for deciding whether a graph contains a vertex cover of size $k$. An immediate question is whether the $k$th slice can be defined by a sentence of smaller quantifier rank.

For every $q \in \mathbb{N}$ denote by $\mathrm{FO}_q$ the set of sentences of quantifier rank at most $q$. There are only finitely pairwise nonequivalent sentences in $\mathrm{FO}_q$ (say in the language for graphs). Thus we see that there is no sequence $(\varphi_\ell)_{\ell \in \mathbb{N}}$ of bounded quantifier rank such that for every $k \in \mathbb{N}$ the sentence $\varphi_k$ is equivalent to $\psi_k$, that is, defines the $k$th slice of $p$-VERTEX-COVER. Nevertheless our first main result reads as follows:

▶ **Theorem 1.** *$p$-VERTEX-COVER is slicewise definable in* $\mathrm{FO}_{17}$.

So we have to explain what we mean by slicewise definable in Theorem 1 (the precise definition will be given in Definition 6).

It is well known that first-order logic FO captures the complexity class uniform $\mathrm{AC}^0$. This result crucially relies on the assumption that the input graphs (or more generally, the input structures) are equipped with built-in addition and multiplication. Our notion of slicewise definability assumes that the graphs have built-in addition and multiplication and furthermore, constants for an initial segment of natural numbers of a length depending only on the parameter.

The vertex cover problem is a special case of the *hitting set problem* on hypergraphs of bounded hyperedge size. For every $d \in \mathbb{N}$ a $d$-hypergraph is a hypergraph with hyperedges of size at most $d$. Then, the *parameterized $d$-hitting set problem* $p$-$d$-HITTING-SET asks whether an input $d$-hypergraph $\mathcal{G}$ contains a set of $k$ vertices that intersects with every hyperedge in $\mathcal{G}$. Thus $p$-VERTEX-COVER is basically the parameterized 2-hitting set problem. Extending Theorem 1 we prove that $p$-$d$-HITTING-SET is slicewise definable in $\mathrm{FO}_q$, where $q = O(d^2)$. The problem $p$-$d$-HITTING-SET can be Fagin-defined [8] by a FO-formula with a second-order variable which does not occur in the scope of an existential quantifier or negation symbol. We show that all problems Fagin-definable in this form are slicewise definable in some $\mathrm{FO}_q$.

What is the complexity of the class of parameterized problems that are slicewise definable in FO with bounded quantifier rank? We prove that it coincides with para-FO [6], the class of problems FO-definable after a precomputation on the parameter. Thus we obtain a descriptive characterization of the class para-FO, or equivalently of the parameterize circuit complexity class para-$\mathrm{AC}^0$ [7, 3, 6]. The equivalence between para-FO and para-$\mathrm{AC}^0$ is an easy consequence of the equivalence between FO and the classical circuit complexity class uniform $\mathrm{AC}^0$ mentioned above.

The main technical tool for proving Theorem 1 and the subsequent results, the *color coding* method [1], makes essential use of arithmetic. The counting quantifier $\exists^{\ge k} x$ in $\exists^{\ge k} x \varphi(x)$ is an abbreviation for the FO-sentence

$$\exists x_1 \cdots \exists x_k \Big( \bigwedge_{1 \le i < j \le k} x_i \neq x_j \wedge \bigwedge_{1 \le i \le k} \varphi(x_i) \Big)$$

expressing that there are at least $k$ many elements satisfying $\varphi$. Clearly, $\mathrm{qr}(\exists^{\ge k} x\varphi(x)) = k + \mathrm{qr}(\varphi(x))$, so the sequence $(\exists^{\ge k} x\varphi(x))_{k\in\mathbb{N}}$ has unbounded quantifier rank. Using the color coding method we get a sequence $(\chi^k)_{k\in\mathbb{N}}$ of bounded quantifier rank such that each $\chi^k$ is equivalent to $\exists^{\ge k} x\varphi(x)$. Note that the sentence in (1) is not of the form $\exists^{\ge k} x\varphi(x)$. We exploit the idea underlying Buss' kernilization in order to get an FO-sentence expressing the existence of a vertex cover of size $k$ in terms of counting quantifiers. Altogether, Theorem 1 (and its proof) exhibit the power of addition and multiplication, although on the face of it, the vertex cover problem has nothing to do with arithmetic operations.

In finite model theory there is consensus that inexpressibility results for FO and for fragments of FO are very hard to obtain in the presence of addition and multiplication. To get such a result we exploit the equivalence between FO and uniform $\mathrm{AC}^0$, more precisely, we analyze the connection between the quantifier rank of a sentence $\varphi$ and the depth of the corresponding $\mathrm{AC}^0$ circuits. Together with a theorem [11, 15] on a version of Sipser functions we show that the hierarchy $(\mathrm{FO}_q)_{q\in\mathbb{N}}$ is strict:

▶ **Theorem 2.** *Let $q \in \mathbb{N}$. Then there is a parameterized problem slicewise definable in $\mathrm{FO}_{q+1}$ but not in $\mathrm{FO}_q$.*

## 1.1 Organization of the paper

In Section 2 we prove Theorem 1, and then extend it to the hitting set problem in Section 3. We give a natural class of Fagin-definable problems that are slicewise definable in FO with bounded quantifier rank in Section 4. We prove the hierarchy theorem, i.e., Theorem 2, in Section 6. In the final section we conclude with some open problems. Due to space limitations we defer some proofs to the full version of the paper.

## 1.2 Some logic preliminaries

A *vocabulary* $\tau$ is a finite set of relation symbols. Each relation symbol has an *arity*. A *structure* $\mathcal{A}$ of vocabulary $\tau$, or $\tau$*-structure*, consists of a nonempty set $A$ called the *universe* of $\mathcal{A}$, and of an interpretation $R^{\mathcal{A}} \subseteq A^r$ of each $r$-ary relation symbol $R \in \tau$. In this paper all structures have a finite universe. Occasionally we allow the use of constants: For a vocabulary $\tau$ we consider $(\tau \cup \{c_1, \ldots, c_s\})$-structures $\mathcal{A}$. Then $c_1^{\mathcal{A}}, \ldots, c_s^{\mathcal{A}}$, the interpretations of the constants $c_1, \ldots, c_s$, are elements of $\mathcal{A}$. However the letters $\tau$, $\tau'$, ... will always denote *relational* vocabularies (without constants). If $\tau$ contains a binary relation symbol $<$ and in the structure $\mathcal{A}$ the relation $<^{\mathcal{A}}$ is an order of the universe, then $\mathcal{A}$ is an *ordered structure*.

Let $\tau$ be a vocabulary and $C$ a set of constants. Formulas $\varphi$ of first-order logic of vocabulary $\tau \cup C$ are built up from atomic formulas $t_1 = t_2$ and $Rt_1 \ldots t_r$ where $t_1, t_2, \ldots, t_r$ are either variables or constants in $C$, and where $R \in \tau$ is of arity $r$, using the boolean connectives and existential and universal quantification. A formula $\varphi$ is a *sentence* if it has no free variables. The quantifier rank of $\varphi$ is defined inductively as:

$$\mathrm{qr}(\varphi) := 0 \ \text{ if } \varphi \text{ is atomic} \qquad \mathrm{qr}(\varphi_1 \wedge \varphi_2) = \mathrm{qr}(\varphi_1 \vee \varphi_2) := \max\{\mathrm{qr}(\varphi_1), \mathrm{qr}(\varphi_2)\}$$
$$\mathrm{qr}(\neg\varphi) := \mathrm{qr}(\varphi) \qquad \mathrm{qr}(\exists x\varphi) = \mathrm{qr}(\forall x\varphi) = 1 + \mathrm{qr}(\varphi).$$

## 2 Slicewise-definability in $\mathrm{FO}_q$ and the vertex cover problem

In this section we prove Theorem 1, i.e., $p$-VERTEX-COVER is slicewise definable in $\mathrm{FO}_{17}$. Our main tool is Theorem 4. It shows how we can express that there are $k$ elements having a first-order property by a number of quantifiers independent of $k$. We give further applications of this tool in this and the next section.

For $n \in \mathbb{N}$ let $[n] := \{0, 1, \dots, n-1\}$. Denote by $<^{[n]}$ the natural order on $[n]$. Clearly, if $\mathcal{A}$ is any ordered structure, then $(A, <^{\mathcal{A}})$ is isomorphic to $\big([|A|], <^{[|A|]}\big)$ and the isomorphism is unique. For ternary relation symbols $+$ and $\times$ we consider the ternary relations $+^{[n]}$ and $\times^{[n]}$ on $[n]$ that are the relations of addition and multiplication of $\mathbb{N}$ restricted to $[n]$. That is, $+^{[n]} := \{(a, b, c) \mid a, b, c \in [n] \text{ with } c = a + b\}$; $\times^{[n]} := \{(a, b, c) \mid a, b, c \in [n] \text{ with } c = a \cdot b\}$. Finally, for every $m \in \mathbb{N}$ let $C(m) := \{\bar{\ell} \mid \ell < m\}$ be a set of constants and set

$$\bar{\ell}^{[n]} := \ell, \text{ if } \ell < n \qquad \text{and} \qquad \bar{\ell}^{[n]} := n - 1, \text{ if } \ell \geq n.$$

The letters $\tau$, $\tau'$, ... will always denote *relational* vocabularies (without constants). Assume $\tau$ contains $<$, $+$, and $\times$. A $(\tau \cup C(m))$-structure $\mathcal{A}$ *has built-in* $<, +, \times, C(m)$ if its $\{<, +, \times, C(m)\}$-reduct is isomorphic to $\big([n], <^{[n]}, +^{[n]}, \times^{[n]}, (\bar{\ell}^{[n]})_{\ell<m}\big)$.

If $m = 0$, we briefly say that $\mathcal{A}$ *has built-in addition and multiplication.* We denote by $\mathrm{ARITHM}[\tau]$ the class of $\tau$-structures with built-in addition and multiplication. If $\mathcal{A} \in \mathrm{ARITHM}[\tau]$ and $m \in \mathbb{N}$, we denote by $\mathcal{A}_{C(m)}$ its unique expansion to a $(\tau \cup C(m))$-structure with built-in $<, +, \times, C(m)$.

In the proof of Theorem 4 we use Lemma 3, the color coding technique of Alon et al. [1] essentially in the form presented in [10, Claim 1 on page 349]. It will enable us to find in every sufficiently large structure with built-in arithmetic for each subset $X$ of cardinality $k$ an FO-definable function that one-to-one maps $X$ into the initial segment of length $k^2$.

▶ **Lemma 3.** *There is an $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, all $k \leq n$ and for every $k$-element subset $X$ of $[n]$, there exists a prime $p < k^2 \cdot \log_2 n$ and a $q < p$ such that the function $h_{p,q} : [n] \to \{0, \dots, k^2 - 1\}$ given by $h_{p,q}(m) := (q \cdot m \mod p) \mod k^2$ is injective on $X$.*

As already mentioned the following result allows to express the existence of $k$ elements satisfying a first-order property by a number of quantifiers independent of $k$.

▶ **Theorem 4.** *Let $\tau$ be a vocabulary containing $<$, $+$, $\times$. Then there is an algorithm that assigns to every $k \in \mathbb{N}$ and every $\mathrm{FO}[\tau]$-formula $\varphi(\bar{x}, y)$ an $\mathrm{FO}\big[\tau \cup C(k^2+1)\big]$-formula $\chi^k_\varphi(\bar{x})$ such that for every $\mathcal{A} \in \mathrm{ARITHM}[\tau]$ with $k^2 \leq |A|/\log |A|$ and $|A| \geq n_0$ and $\bar{u} \in A$,*

$$\mathcal{A}_{C(k^2)} \models \chi^k_\varphi(\bar{u}) \iff \text{there are pairwise distinct } v_0, \dots, v_{k-1} \in A \text{ with } \mathcal{A} \models \varphi(\bar{u}, v_i) \text{ for every } i \in [k]. \tag{2}$$

*By Lemma 3 we can take as $\chi^k_\varphi(\bar{x})$ a formula expressing*

$$\exists p \exists q \Big( \bigvee_{0 \leq i_0 < \cdots < i_{k-1} < k^2} \ \bigwedge_{j \in [k]} \exists y \big( \text{“}h_{p,q}(y) = i_j\text{”} \wedge \varphi(\bar{x}, y) \big) \Big).$$

*Furthermore,* $\mathrm{qr}\big(\chi^k_\varphi(\bar{x})\big) = \max\big\{12, \mathrm{qr}\big(\varphi(\bar{x}, y)\big) + 3\big\}$.

Note that the conditions “$k^2 \leq |A|/\log |A|$ and $|A| \geq n_0$” on $|A|$ are fulfilled if $|A| \geq \max\{2^{k^2}, n_0\}$, so we have a lower bound of $|A|$ in terms of $k$ (here $n_0$ is a natural number according to Lemma 3).

**Proof of Theorem 4.** Let $\mathcal{A}$ be as above, set $n := |A|$, and w.l.o.g. assume that $A := [n]$. In order to make formulas more readable, we introduce some abbreviations. Clearly, $x = (y \mod z)$ is an abbreviation for $\exists u(y = u \times z + x \wedge x < z)$, more precisely, as $+$ and $\times$ are relation symbols, an abbreviation for $\exists u \exists u'(u' = u \times z \wedge y = u' + x \wedge x < z)$. Now let

$$\chi_\varphi^k(\bar{x}) := \exists p \exists q \Big( \bigvee_{0 \le i_1 < \cdots < i_{k-1} < k^2} \bigwedge_{j \in [k]} \exists y (\text{“}h_{p,q}(y) = i_j\text{”} \wedge \varphi(\bar{x}, y)) \Big),$$

where

$$\text{“}h_{p,q}(y) = i_j\text{”} := (q \times (u \mod p) \mod p) \mod \overline{k^2} = \overline{i_j}.$$

We replaced $(q \times u \mod p)$ by $(q \times (u \mod p) \mod p)$, since $q \times u$ might exceed $|A|$. To count the quantifier rank note that “$h_{p,q}(y)$” $= \overline{i_j}$ means

$$\exists v \exists v' \exists \alpha \left( v' = v \times \overline{k^2} \wedge \alpha = v' + \overline{i_j} \wedge \overline{i_j} < \overline{k^2} \right),$$

where the intended meaning of $\alpha$ is $(q \times (u \mod p) \mod p)$. So $\alpha$ is the unique element satisfying

$$\exists w \exists w' \exists \beta (w' = w \times p \wedge \beta = w' + \alpha \wedge \alpha < p).$$

Here the intended meaning of $\beta$ is $q \times (u \mod p)$. Thus $\beta$ is the unique element satisfying

$$\exists \gamma (\beta = q \times \gamma \wedge \text{ “}\gamma = u \mod p\text{”}).$$

So we can replace “$\gamma = u \mod p$” by

$$\exists z \exists z' (z' = z \times p \wedge u = z' + \gamma \wedge \gamma < p).$$

Thus, $\mathrm{qr}(\text{“}h_{p,q}(y) = i_j\text{”}) = 9$ and hence, $\mathrm{qr}(\chi_\varphi^k(\bar{x})) = \max\{12, \mathrm{qr}(\varphi(\bar{x}, y)) + 3\}$. ◀

We use the previous result to show that two parameterized problems are slicewise definable in $\mathrm{FO}_q$ for some $q$, one is an easy application, the other the more intricate $p$-VERTEX-COVER. First we give the precise definitions of parameterized problem in our context and of slicewise definability.

▶ **Definition 5.** A parameterized problems is a subclass $Q$ of $\mathrm{ARITHM}[\tau] \times \mathbb{N}$ for some vocabulary $\tau$, where for each $k \in \mathbb{N}$ the class $Q_k := \{\mathcal{A} \in \mathrm{ARITHM}[\tau] \mid (\mathcal{A}, k) \in Q\}$ is closed under isomorphism. The class $Q_k$ is the *kth slice of Q*.

Every pair $(\mathcal{A}, k) \in \mathrm{ARITHM}[\tau] \times \mathbb{N}$ is an *instance* of $Q$, $\mathcal{A}$ its *input* and $k$ its *parameter*.

▶ **Definition 6.** $Q$ is *slicewise definable in* FO *with bounded quantifier rank*, briefly $Q \in \mathrm{XFO_{qr}}$, if there is a $q \in \mathbb{N}$ and computable functions $h : \mathbb{N} \to \mathbb{N}$ and $f : \mathbb{N} \to \mathrm{FO}_q[\tau \cup C(h(k))]$ such that for all $(\mathcal{A}, k) \in \mathrm{ARITHM}[\tau] \times \mathbb{N}$,

$$(\mathcal{A}, k) \in Q \iff \mathcal{A}_{C(h(k))} \models f(k).$$

That is, if $m_k := h(k)$ and $\varphi_k := f(k)$, then

$$(\mathcal{A}, k) \in Q \iff \mathcal{A}_{C(m_k)} \models \varphi_k.$$

We then say that $Q$ *is slicewise definable in* $\mathrm{FO}_q$ and write $Q \in \mathrm{XFO}_q$.

Using the constants in $C(m)$ we can characterize arithmetical structures with less that $m$ elements by a quantifier free sentence, more precisely:

▶ **Lemma 7.** *Assume that* $\mathcal{A} \in \mathrm{ARITHM}[\tau]$ *and that* $|A| < m$. *Then there is a quantifier free* $\mathrm{FO}[\tau \cup C(m)]$*-sentence* $\varphi_{\mathcal{A}_{C(m)}}$ *(that is,* $\varphi_{\mathcal{A}_{C(m)}} \in \mathrm{FO}_0[\tau \cup C(m)]$*) such that for all structures* $\mathcal{B} \in \mathrm{ARITHM}[\tau]$ *we have*

$$\mathcal{B}_{C(m)} \models \varphi_{\mathcal{A}_{C(m)}} \iff \mathcal{A} \cong \mathcal{B}.$$

Using this lemma we get the following simple but useful observation.

▶ **Proposition 8.** *Let* $Q \in \mathrm{ARITHM}[\tau] \times \mathbb{N}$ *be a decidable parameterized problem and* $q \in \mathbb{N}$. *Assume that* $Q$ *is* eventually slicewise definable in $\mathrm{FO}_q$*, that is, there are computable functions* $k \mapsto m_k$ *with* $m_k \in \mathbb{N}$ *and* $k \mapsto \varphi_k$ *with* $\varphi_k \in \mathrm{FO}_q\big[\tau \cup C(m_k)\big]$ *and a computable and increasing function* $g : \mathbb{N} \to \mathbb{N}$ *such that for all* $(\mathcal{A}, k) \in \mathrm{ARITHM}[\tau] \times \mathbb{N}$ *with* $|A| \geq g(k)$*,*

$$(\mathcal{A}, k) \in Q \iff \mathcal{A}_{C(m_k)} \models \varphi_k.$$

*Then* $Q$ *is slicewise definable in* $\mathrm{FO}_q$*.*

We now turn to our first application of Theorem 4.

▶ **Theorem 9.** *The parameterized problem*

| *p-deg*-Independent-Set | |
|---|---|
| *Input:* | A graph $\mathcal{G}$. |
| *Parameter:* | $k \in \mathbb{N}$. |
| *Question:* | Is $k \geq \deg(\mathcal{G})$ and does $\mathcal{G}$ have an independent set of $k - \deg(\mathcal{G})$ elements? |

*is slicewise definable in* $\mathrm{FO}_{13}$*.*

Let $\tau_{\mathrm{GRAPH}} := \{E, +, <, \times\}$ with binary $E$. More formally, in our context we mean by *p-deg*-Independent-Set the following class:

$$\Big\{(\mathcal{G}, k) \in \mathrm{ARITHM}[\tau_{\mathrm{GRAPH}}] \times \mathbb{N} \;\Big|\; k \geq \deg(\mathcal{G}) \text{ and } \text{(the } \{E\}\text{-reduct of) } \mathcal{G} \text{ has an independent set of size } \ell := k - \deg(\mathcal{G})\Big\}.$$ [1]

**Proof.** An easy induction on $\ell := k - \deg(\mathcal{G})$ shows that every graph $\mathcal{G}$ with at least $(\deg(\mathcal{G}) + 1) \cdot \ell$ vertices has an independent set of size $\ell$. Hence, for $(\mathcal{G}, k) \in \mathrm{ARITHM}[\tau]$, where the graph $\mathcal{G}$ has at least $(k + 1) \cdot k$ vertices, we have

$$(\mathcal{G}, k) \in \mathrm{ARITHM}[\tau_{\mathrm{GRAPH}}] \in p\text{-}deg\text{-}\mathrm{INDEPENDENT\text{-}SET} \iff k \geq \deg(\mathcal{G}). \tag{3}$$

We use this fact to prove that *p-deg*-Independent-Set is eventually slicewise definable in $\mathrm{FO}_{13}$, which yields our claim by Proposition 8.

Let $d \in \mathbb{N}$ and $\varphi := Euy$. Then, by Theorem 4, we have for every graph $\mathcal{G}$ with at least $h(k)$ vertices for some computable $h : \mathbb{N} \to \mathbb{N}$ and every vertex $u$ of $\mathcal{G}$,

$$\mathcal{G} \models \chi^d_\varphi(u) \iff \text{the degree of } u \text{ in } \mathcal{G} \text{ is} \geq d.$$

[1] In the following we will present parameterized graph problems in the more liberal form as given by the box above.

Thus, for $k \in \mathbb{N}$ and every graph $\mathcal{G} \in \text{ARITHM}[\tau_{\text{GRAPH}}]$ with at least $\max\{h(k), (k+1)\cdot k\}$ vertices, by (3),

$$(\mathcal{G}, k) \in p\text{-}deg\text{-INDEPENDENT-SET} \iff \mathcal{G} \models \neg\exists u \chi_{\varphi}^{k+1}(u).$$

As $\text{qr}(\varphi) = 0$, Theorem 4 and the previous equivalence show that $p$-*deg*-INDEPENDENT-SET is eventually in $\text{XFO}_{13}$ (and hence in $\text{XFO}_{13}$ by Proposition 8). ◀

Now we are ready to show the slicewise definability of $p$-VERTEX-COVER in $\text{FO}_{17}$.

**Proof of Theorem 1.** Recall the main ingredient of Buss' kernelization for an instance $(\mathcal{G}, k)$ of the vertex cover problem.

1. If a vertex $v$ has degree $\geq k+1$ in $\mathcal{G}$, then $v$ must be in every vertex cover of size $k$. We remove all $v$ of degree $\geq k+1$ in $\mathcal{G}$, say $\ell$ many, and decrease $k$ to $k' := k - \ell$.
2. Remove all isolated vertices.
3. Let $\mathcal{G}'$ be the resulting induced graph. If $k' < 0$ or $\mathcal{G}'$ has $> k' \cdot (k+1)$ vertices, then $(\mathcal{G}', k')$, and hence also $(\mathcal{G}, k)$, is a NO instance of $p$-VERTEX-COVER.

Again let $\varphi(x, y) := Exy$. Then, by Theorem 4, for every instance $(\mathcal{G}, k)$ of $p$-VERTEX-COVER, where the vertex set $G$ of $\mathcal{G}$ is sufficiently large compared with $k$ and every vertex $v \in G$,

$$\mathcal{G} \models \chi_{\varphi}^{k+1}(v) \iff v \text{ has degree} \geq k+1.$$

Therefore, applying again Theorem 4 we get for $\ell \in \mathbb{N}$,

$$\mathcal{G} \models \left(\chi^{\ell}_{\chi_{\varphi}^{k+1}} \wedge \neg\chi^{\ell+1}_{\chi_{\varphi}^{k+1}}\right) \iff \mathcal{G} \text{ has exactly } \ell \text{ vertices of degree} \geq k+1.$$

For every vertex $v$ of $\mathcal{G}$ we have

$$\mathcal{G} \models uni(v) \iff v \text{ is a vertex of } \mathcal{G}',$$

where

$$uni(x) := \left(\neg\chi_{\varphi}^{k+1}(x) \wedge \neg\forall y\big(Exy \to \chi_{\varphi}^{k+1}(y)\big)\right).$$

Then,

$$\begin{aligned}
&(\mathcal{G},k) \in p\text{-VERTEX-COVER}\\
&\quad\iff \text{for some } \ell \text{ with } 0 \leq \ell \leq k,\ \mathcal{G} \text{ has exactly } \ell \text{ vertices of degree} \geq k+1 \text{ and}\\
&\qquad\qquad \text{there is a } j \leq (k-\ell)\cdot(k+1) \text{ such that } \mathcal{G}' \text{ has } j \text{ vertices and}\\
&\qquad\qquad (\mathcal{G}', k-\ell) \text{ is a YES instance of } p\text{-VERTEX-COVER}\\
&\quad\iff \mathcal{G} \models \bigvee_{0\leq\ell\leq k}\Big(\chi^{\ell}_{\chi_{\varphi}^{k+1}} \wedge \neg\chi^{\ell+1}_{\chi_{\varphi}^{k+1}} \wedge \bigvee_{0\leq j\leq(k-\ell)\cdot(k+1)} (\chi^{j}_{uni} \wedge \neg\chi^{j+1}_{uni} \wedge \rho_j)\Big). \qquad (4)
\end{aligned}$$

Here the formula $\rho_j$, a formula expressing (in $\mathcal{G}$ with an $\mathcal{G}'$ with exactly $j$ vertices) that $\mathcal{G}'$ has a vertex cover of size $k-\ell$, still has to be defined. We do that by saying that $\mathcal{G}'$ is isomorphic to one of the graphs with $j$ vertices that has a vertex cover of size $k-\ell$. For this we have to be able to define an order of $\mathcal{G}'$ by a formula of quantifier rank bounded by a constant number independent of $k$. Again this is done (using built-in arithmetics) with the color coding method: We find $p$ and $q$, and $0 \leq i_0 < \cdots < i_{j-1} < j^2$ with

$$h_{p,q}(G') = \{i_0, \ldots, i_{j-1}\}.$$

Then, we can speak of the first, the second ,..., vertex in $\mathcal{G}'$. Thus as $\rho_j$ we can take the sentence

$$\exists p \exists q \Big( \bigvee_{0 \le i_0 < \ldots < i_{j-1} < j^2} \Big( \bigwedge_{s \in [j]} \exists y (\text{“}h_{p,q}(y) = i_s\text{”} \wedge uni(y)) \wedge \bigvee_{\substack{(\mathcal{H}, k-\ell) \in p\text{-VERTEX-COVER} \\ H = [j]}} \rho'_{\mathcal{H}} \Big)\Big),$$

where

$$\rho'_{\mathcal{H}} := \bigwedge_{\substack{s,t \in [j] \\ E^{\mathcal{H}} st}} \exists y \exists z \big( uni(y) \wedge uni(z) \wedge \text{“}h_{p,q}(y) = i_s\text{”} \wedge \text{“}h_{p,q}(z) = i_t\text{”} \wedge Eyz \big)$$
$$\wedge \bigwedge_{\substack{s,t \in [j] \\ \neg E^{\mathcal{H}} st}} \exists y \exists z \big( uni(y) \wedge uni(z) \wedge \text{“}h_{p,q}(y) = i_s\text{”} \wedge \text{“}h_{p,q}(z) = i_t\text{”} \wedge \neg Eyz \big).$$

As $\mathrm{qr}(\chi_\varphi^{k+1}) \le 12$, we have $\mathrm{qr}(uni(x)) \le 13$. Thus, $\mathrm{qr}(\chi_{uni}^j) \le 16$ and $\mathrm{qr}(\rho_j) \le 17$. As the remaining formulas in (4) have at most quantifier rank 16, we get $p$-VERTEX-COVER $\in$ $\mathrm{XFO}_{17}$. ◀

## 3 The hitting set problems with bounded hyperedge size

We consider the parameterized problem

| $p$-$d$-HITTING-SET | |
|---|---|
| *Input:* | A hypergraph $\mathcal{G}$ with edges of size at most $d$. |
| *Parameter:* | $k \in \mathbb{N}$. |
| *Question:* | Does $\mathcal{G}$ have a hitting set of size $k$? |

Here a *hypergraph* $\mathcal{G}$ is a pair $(V, E)$, where $V$ is a set, the set of *vertices of* $\mathcal{G}$, and every element of $E$ is a *hyperedge*, that is, a nonempty subset of $V$. A *hitting set* in $\mathcal{G}$ is a set $H$ that intersects each hyperedge (that is, $H \cap e \neq \emptyset$ for all $e \in E$).

The goal of this section is to show:

▶ **Theorem 10.** *Let $d \ge 1$. Then $p$-$d$-HITTING-SET is slicewise definable in* FO *with bounded quantifier rank; more precisely, $p$-$d$-HITTING-SET $\in \mathrm{XFO}_q$ with $q = O(d^2)$.*

The following lemma can be viewed as a generalization of part of Buss' kernelization algorithm for $p$-VERTEX-COVER to $p$-$d$-HITTING-SET. The case for $p$-3-HITTING-SET was first shown in [13].

▶ **Lemma 11.** *Let $(\mathcal{G}, k)$ with $\mathcal{G} = (V, E)$ be an instance of $p$-$d$-HITTING-SET. Let $1 < \ell \le d$ and assume that every $\ell$-set (i.e., set with exactly $\ell$ elements) of vertices has at most $k^{d-\ell}$ extensions in $E$.*

*If $v_1, \ldots, v_{\ell-1}$ are pairwise distinct vertices such that there is a hitting set $H$ of size $\le k$ that contains none of these vertices, then $\{v_1, \ldots, v_{\ell-1}\}$ has at most $k^{d-(\ell-1)}$ extensions in $E$.*

**Proof.** Every hyperedge that extends $\{v_1, \ldots, v_{\ell-1}\}$ must contain a vertex $u$ of the hitting set $H$. By the assumptions, $u$ is distinct from the $v_i$'s and therefore, the set $\{v_1, \ldots, v_{\ell-1}, u\}$ has at most $k^{d-\ell}$ extensions in $E$. As $|H| \le k$, we see that there are at most $k \cdot k^{d-\ell}$ $\big(= k^{d-(\ell-1)}\big)$ extensions in $E$. ◀

Let $(\mathcal{G}, k)$ and $1 < \ell \leq d$ satisfy the hypotheses of the lemma, that is, $(\mathcal{G}, k)$ with $\mathcal{G} = (V, E)$ is an instance of $p$-$d$-HITTING-SET and every $\ell$-set has at most $k^{d-\ell}$ extensions in $E$. For every pairwise distinct vertices $v_1, \ldots, v_{\ell-1}$ such that $\{v_1, \ldots, v_{\ell-1}\}$ has more than $k^{d-(\ell-1)}$ extensions in $E$, we delete from $E$ all hyperedges extending $\{v_1, \ldots, v_{\ell-1}\}$ and add the hyperedge $\{v_1, \ldots, v_{\ell-1}\}$. Let $\mathcal{G}^\ell = (V, E^\ell)$ be the resulting hypergraph. Then:

**(a)** For every pairwise distinct vertices $v_1, \ldots, v_{\ell-1}$ there are at most $k^{d-(\ell-1)}$ hyperedges in $E^\ell$ extending $\{v_1, \ldots, v_{\ell-1}\}$.

**(b)** If $H$ is a subset of $V$ and $|H| \leq k$, then

$$H \text{ is a hitting set of } \mathcal{G} \iff H \text{ is a hitting set of } \mathcal{G}^\ell,$$

in particular,

$$(\mathcal{G}, k) \in p\text{-}d\text{-HITTING-SET} \iff (\mathcal{G}^\ell, k) \in p\text{-}d\text{-HITTING-SET}.$$

Let $(\mathcal{G}, k)$ be an instance of $p$-$d$-HITTING-SET. For $\ell := d$ the hypothesis of Lemma 11 is fulfilled: Every $d$-set of vertices has at most one extension in $E$, namely at most, itself. Hence, applying the above procedure for $\ell = d$ we get the hypergraph $\mathcal{G}^\ell$, which satisfies the hypotheses of Lemma 11 for $\ell := d - 1$. So we get, again by the above procedure the hypergraph $(\mathcal{G}^\ell)^{\ell-1}$, which we denote by $\mathcal{G}^{\ell,\ell-1}$. Following this way, we finally obtain the hypergraph $\mathcal{G}^{\ell,\ell-1,\ldots,2}$, which we denote by $\mathcal{G}'$. Note that $\mathcal{G}' = (V, E')$ for some $E'$. From (a) and (b) we get (a') and (b').

**(a')** For every vertex $v$ there are at most $k^{d-1}$ hyperedges in $E'$ containing $v$.

**(b')** If $H$ is a subset of $V$ and $|H| \leq k$, then

$$H \text{ is a hitting set of } \mathcal{G} \iff H \text{ is a hitting set of } \mathcal{G}',$$

Moreover,

**(c')** If $(\mathcal{G}, k) \in p$-$d$-HITTING-SET, then $|E'| \leq k^d$ and $|V'| \leq d \cdot k^d$, where $V' := \{v \in V \mid \text{there is an } e \in E' \text{ with } v \text{ in } e\}$ is the set of non-isolated vertices of $\mathcal{G}'$.

In fact, let $H$ be a hitting set with $|H| = k$ of $\mathcal{G}$ and hence, by (b') of $\mathcal{G}'$. As every hyperedge must contain a vertex of $H$, we get $|E'| \leq k^d$ from (a'). As every hyperedge $e \in E'$ contains at most $d$ vertices, we have $|V'| \leq d \cdot k^d$.

We fix $k$ and look at the $k$th slice of $p$-$d$-HITTING-SET. In the proof of Theorem 10 which will be presented in the full paper we will see that for hypergraphs $\mathcal{G}$ sufficiently large compared with $k$ we can FO-define $\mathcal{G}'$ in $\mathcal{G}$. By (b') and (c'), we know that $(\mathcal{G}, k) \in p$-$d$-HITTING-SET implies $|E'| \leq k^d$. By Theorem 4, we can express $|E'| \leq k^d$ in first-order logic with a bounded number of quantifiers if we add built-in addition and multiplication. Essentially this shows that $p$-$d$-HITTING-SET is eventually slicewise definable in FO with bounded quantifier rank and thus, $p$-$d$-HITTING-SET $\in$ XFO$_{\text{qr}}$ (by Proposition 8).

A part of an FO-interpretation $I$ is an FO-formula $\varphi^I_{uni}(x_1, \ldots, x_s)$ defining the universe of the defined structure, that is: if $I$ is an interpretation of $\sigma$-structures in a class $\mathbf{K}$ of $\tau$-structures, then for every structure $\mathcal{A} \in \mathbf{K}$ the set

$$(\varphi^I_{uni})^{\mathcal{A}} := \{(a_1, \ldots, a_s) \in A^s \mid \mathcal{A} \models \varphi(a_1, \ldots, a_s)\}$$

is the universe of the $\sigma$-structure $I(\mathcal{A})$ defined by $I$ in $\mathcal{A}$.

Assume that $\sigma$ does not contain the relation symbols $<, +, \times$, but that the structures in $\mathbf{K}$ are structures with built-in addition and multiplication, i.e., $\mathbf{K} \subseteq$ ARITHM$[\tau]$. In general, we can not extend the interpretation $I$ to an FO-interpretation $J$ such that

$$J(\mathcal{A}) = \left(I(\mathcal{A}), <^{J(\mathcal{A})}, +^{J(\mathcal{A})}, \times^{J(\mathcal{A})}\right)$$

has built-in addition and multiplication (that is, so that $J(\mathcal{A})$ is $I(\mathcal{A})$ together with an order and the corresponding addition and multiplication).

For example, for $\tau = \{P, <, +, \times\}$ with unary $P$ let $\mathbf{K}$ be the class of $\tau$-structures $\mathcal{A}$ with $P^{\mathcal{A}} \neq \emptyset$. Let $\sigma$ be the empty vocabulary and consider the interpretation $I$ yielding in $\mathcal{A}$ the $\sigma$-structure with universe $P^{\mathcal{A}}$ (take $\varphi^I_{uni}(x) := Px$). If we could extend $I$ to an interpretation $J$ such that $J(\mathcal{A}) := (P^{\mathcal{A}}, <^{\mathcal{A}}, +^{\mathcal{A}}, \times^{\mathcal{A}})$ has built-in addition and multiplication, then we could express in $J(\mathcal{A})$, and thus in $\mathcal{A}$, that "$P^{\mathcal{A}}$ is even," i.e., the parity problem, which is well known to be impossible.

The next result (proven in [4, Lemma 10.5], see also [12, Exercise 1.33]) shows that the situation is different if for $\varphi^I_{uni}(x_1, \dots, x_s)$ we have $(\varphi^I_{uni})^{\mathcal{A}} = A^s$.

▶ **Proposition 12.** *Let $\tau$ contain $<, +, \times$ and assume that none of these symbols is in $\sigma$. Let $\mathbf{K} \subseteq$ ARITHM$[\tau]$ and let $I$ be an* FO*-interpretation of $\sigma$-structures in the structures in $\mathbf{K}$ with $\varphi^I_{uni} = \varphi^I_{uni}(x_1, \dots, x_s)$. If for all $\mathcal{A} \in \mathbf{K}$, $(\varphi^I_{uni})^{\mathcal{A}} = A^s$, then $I$ can be extended to an* FO*-interpretation of $\sigma \cup \{<, +, \times\}$ such that $J(\mathcal{A}) = (I(\mathcal{A}), <^{J(\mathcal{A})}, +^{J(\mathcal{A})}, \times^{J(\mathcal{A})})$ has built-in addition and multiplication for all $\mathcal{A} \in \mathbf{K}$.*

## 4 Fagin definability

Let $\varphi(X)$ be an FO$[\tau]$-formula which for a, say $r$-ary, second-order variable $X$ may contain atomic formulas of the form $Xx_1 \dots x_r$ . Then the *parameterized problem* $\mathrm{FD}_{\varphi(X)}$ *Fagin-defined by* $\varphi(X)$ is the problem

| $\mathrm{FD}_{\varphi(X)}$ | |
|---|---|
| *Input:* | A $\tau$-structure $\mathcal{A}$. |
| *Parameter:* | $k \in \mathbb{N}$. |
| *Question:* | Decide whether there is an $S \subseteq A^r$ with $\lvert S\rvert = k$ and $\mathcal{A} \models \varphi(S)$. |

The following metatheorem improves [9, Theorem 4.4].

▶ **Theorem 13.** *Let $\varphi(X)$ be an* FO$[\tau]$*-formula without first-order variables occurring free and in which $X$ does not occur in the scope of an existential quantifier or negation symbol. Then $\mathrm{FD}_{\varphi(X)} \in \mathrm{XFO}_{\mathrm{qr}}$ that is, $\mathrm{FD}_{\varphi(X)}$ is slicewise definable with bounded quantifier rank.*

We view a hypergraph $\mathcal{G} := (V, E)$ as an $\{E_0, \epsilon\}$-structure $(V \cup E, E_0^{\mathcal{G}}, \epsilon^{\mathcal{G}})$, where $E_0$ is a unary relation symbol and $\epsilon$ is a binary relation symbol and

$$E_0^{\mathcal{G}} := E \quad \text{and} \quad \epsilon^{\mathcal{G}} := \big\{(v, e) \bigm| v \in V,\ e \in E \text{ and } v \in e\big\}.$$

Fix $d \in \mathbb{N}$. For $k \in \mathbb{N}$ we have (assuming $\lvert V\rvert \geq k$)

$$(\mathcal{G}, k) \in p\text{-}d\text{-}\textsc{Hitting-Set} \iff \text{for some } S \text{ with } \lvert S\rvert = k \text{ we have } (V \cup E, E_0^{\mathcal{G}}, \epsilon^{\mathcal{G}}) \models \varphi(S),$$

where $\varphi(x) := \forall e\Big(E_0 e \to \forall x_1 \dots \forall x_d\big((\forall x(x \,\epsilon\, e \leftrightarrow \bigvee_{i=1}^{d} x_i = x) \to (Xx_1 \vee \dots \vee Xx_d)\big)\Big)$. By Theorem 13 we know that $\mathrm{FD}_{\varphi(X)} \in \mathrm{XFO}_{\mathrm{qr}}$. Hence, $p$-$d$-Hitting-Set $\in \mathrm{XFO}_{\mathrm{qr}}$, so we get the result of the previous section. However here, to prove Theorem 13 we use the result of the previous section.

**Proof of Theorem 13.** For simplicity, let us assume that $X$ is unary. Without loss of generality we can assume that

$$\phi(X) = \forall y_1 \dots \forall y_\ell \bigwedge_{i=1}^{m} \bigvee_{j=1}^{p} \psi_{ij},$$

where each $\psi_{ij}$ either is $Xy_q$ for some $q \in \{1,\dots,\ell\}$, or a first-order formula with free variables in $\{y_1,\dots,y_\ell\}$ in which $X$ does not occur.

Let $(\mathcal{A},k)$ be an instance of $\mathrm{FD}_{\varphi(X)}$. We construct an instance $(\mathcal{G}(\mathcal{A}),k)$ of $p$-$\ell$-Hitting-Set such that

$$(\mathcal{A},k) \in \mathrm{FD}_{\varphi(X)} \iff (\mathcal{G}(\mathcal{A}),k) \in p\text{-}\ell\text{-}\textsc{Hitting-Set}. \tag{5}$$

As $(\mathcal{G}(\mathcal{A}),k)$ we take the hypergraph $(V,E)$ with $V=A$ and where $E$ contains the following hyperedges. Let $\bar{a} \in A^\ell$ and $i \in \{1,\dots,m\}$. If

$$\mathcal{A} \models \neg \bigvee_{\substack{j\in\{1,\dots,p\}\\ X \text{ does not occur in } \psi_{ij}}} \psi_{ij}(\bar{a}).$$

then $E$ contains the hyperedge $\{a_{s_1},\dots,a_{s_t}\}$ where $Xy_{s_1},\dots,Xy_{s_t}$ are exactly the disjuncts of the form $Xy_{\dots}$ in $\bigvee_{j=1}^{p}\psi_{ij}$. If $t=0$ (for some $\bar{a}\in A^\ell$), we take as $\mathcal{G}(\mathcal{A})$ a fixed hypergraph chosen in advance such that $(\mathcal{G}(\mathcal{A}),k)$ is a no instance of $p$-$\ell$-Hitting-Set.

Since $\mathcal{G}(\mathcal{A})$ can be defined from $\mathcal{A}$ by an FO-interpretation and $p$-$\ell$-Hitting-Set $\in \mathrm{XFO}_{\mathrm{qr}}$, we get $\mathrm{FD}_{\varphi(X)} \in \mathrm{XFO}_{\mathrm{qr}}$. ◀

Some parameterized problems can be shown to be in para-FO by a simple application of this theorem, e.g., for every $\ell \geq 1$, the problem $p$-WSat$(\Gamma^{+}_{1,\ell})$, the restriction of $p$-Dominating-Set to graphs of degree $\ell$, and the problem $p$-$\ell$-Matrix-Domination, the restriction to matrices with at most $\ell$ ones in every row and column in $p$-Matrix-Domination.

## 5 para-$\mathrm{AC}^0$ = $\mathrm{XFO}_{\mathrm{qr}}$

The importance of the class $\mathrm{XFO}_{\mathrm{qr}}$ from the point of view of complexity theory stems from the fact that it coincides with the class para-$\mathrm{AC}^0$, the class of parameterized problems that are in dlogtime-uniform $\mathrm{AC}^0$ after a precomputation. As dlogtime-uniform $\mathrm{AC}^0$ contains precisely the class of parameterized problems definable in first-order logic, the class para-$\mathrm{AC}^0$ corresponds to the class para-FO of parameterized problems definable in first-order logic after a precomputation on the parameter (see [7, 6]). We deal here with the class para-FO and thus in this section aim to show para-FO = $\mathrm{XFO}_{\mathrm{qr}}$.

To define the class para-FO we need a notion of union of two arithmetical structures.

▶ **Definition 14.** Assume $\mathcal{A} \in \mathrm{ARITHM}[\tau]$ and $\mathcal{A}' \in \mathrm{ARITHM}[\tau']$ satisfy

$$A \cap A' = \emptyset \quad \text{and} \quad \tau \cap \tau' = \{<,+,\times\}.$$

Let $U$ be a new unary relation symbol. We set $\tau \uplus \tau' := \tau \cup \tau' \cup \{U\}$. Then $\mathcal{A} \uplus \mathcal{A}'$ is the structure $\mathcal{B} \in \mathrm{ARITHM}(\tau \uplus \tau')$ with

- $B := A \cup A'$;
- $U^{\mathcal{B}} = A'$;
- $<^{\mathcal{B}} := <^{\mathcal{A}} \cup <^{\mathcal{A}'} \cup \big\{(a,a') \bigm| a \in A \text{ and } a' \in A'\big\}$, that is, the order $<^{\mathcal{B}}$ extends the orders $<^{\mathcal{A}}$ and $<^{\mathcal{A}'}$, and in $<^{\mathcal{B}}$ every element of $A$ precedes every element of $A'$;
- $R^{\mathcal{B}} := R^{\mathcal{A}}$ for $R \in \tau$ and $R^{\mathcal{B}} := R^{\mathcal{A}'}$ for $R \in \tau'$.

As we require $\mathcal{B} \in \mathrm{ARITHM}(\tau \uplus \tau')$ we do not need to define $+^{\mathcal{B}}$ and $\times^{\mathcal{B}}$ explicitly. If $A \cap A' \neq \emptyset$, then we pass to isomorphic structures with disjoint universes before defining $\mathcal{A} \uplus \mathcal{A}'$.

▶ **Definition 15.** Let $Q \subseteq \text{ARITHM}[\tau] \times \mathbb{N}$ be a parameterized problem. $Q$ is *first-order definable after a precomputation*, in symbols $Q \in \text{para-FO}$, if for some vocabulary $\tau'$ there is a computable function $\mathit{pre} : \mathbb{N} \to \text{ARITHM}[\tau']$, a *precomputation*, and a sentence $\varphi \in \text{FO}\big[\tau \uplus \tau'\big]$ such that for all $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$,

$$(\mathcal{A}, k) \in Q \iff \mathcal{A} \uplus \mathit{pre}(k) \models \varphi.$$

The main result of this section reads as follows. It is the modeltheoretic analogue of the equivalence between (i) and (ii) of [6, Proposition 6].[2]

▶ **Theorem 16.** $\text{para-FO} = \text{XFO}_{\text{qr}}$.

**Proof.** We sketch a proof, details will be given in the full version of this paper. Assume that $Q \in \text{para-FO}$. Hence, for some vocabulary $\tau'$ there is a computable function $\mathit{pre} : \mathbb{N} \to \text{ARITHM}[\tau']$ and a sentence $\varphi \in \text{FO}[\tau \uplus \tau']$ such that for all $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$,

$$(\mathcal{A}, k) \in Q \iff \mathcal{A} \uplus \mathit{pre}(k) \models \varphi.$$

Clearly, then $Q$ is decidable. Therefore, by Proposition 8, it suffices to show that for some $q \in \mathbb{N}$ the problem $Q$ is eventually slicewise definable in $\text{FO}_q$, that is, that there are an increasing and computable function $g : \mathbb{N} \to \mathbb{N}$ and computable functions $k \mapsto m_k$ and $k \mapsto \psi_k \in \text{FO}_q[\tau \cup C(m_k)]$ such that for all $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$ with $|A| \geq g(k)$,

$$\mathcal{A} \uplus \mathit{pre}(k) \models \varphi \iff \mathcal{A}_{C(m_k)} \models \psi_k. \tag{6}$$

The main idea: As the precomputation $\mathit{pre}$ is computable, for $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$ with sufficiently large $|A|$ compared with $|\mathit{pre}(k)|$, we can FO-define $\mathit{pre}(k)$ in $\mathcal{A}_{C(k+1)}$. Furthermore, from $\mathcal{A}$ and from this FO-defined $\mathit{pre}(k)$ in $\mathcal{A}_{C(k+1)}$ we get (an isomorphic copy of) $\mathcal{A} \uplus \mathit{pre}(k)$ in $\mathcal{A}_{C(k+1)}$ by an FO-interpretation. Summing up, we can FO-interpret $\mathcal{A} \uplus \mathit{pre}(k)$ in $\mathcal{A}_{C(k+1)}$. This FO-interpretation yields the desired $\psi_k$ satisfying (6).

Now assume that $Q \in \text{FO}_{\text{qr}}$. Then there is a $q \in \mathbb{N}$ and computable functions $k \mapsto m_k$ with $m_k \in \mathbb{N}$ and $k \mapsto \varphi_k$ with $\varphi_k \in \text{FO}_q\big[\tau \cup C(m_k)\big]$ such that for all $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$,

$$(\mathcal{A}, k) \in Q \iff \mathcal{A}_{C(m_k)} \models \varphi_k.$$

We have to find a precomputation $\mathit{pre} : \mathbb{N} \to \text{ARITHM}[\tau']$ and an $\text{FO}[\tau \uplus \tau']$-sentence $\varphi$ such that for all $(\mathcal{A}, k) \in \text{ARITHM}[\tau] \times \mathbb{N}$,

$$\mathcal{A}_{C(m_k)} \models \varphi_k \iff \mathcal{A} \uplus \mathit{pre}(k) \models \varphi.$$

Essentially $\mathit{pre}(k)$ is the parse tree of $\varphi_k$ and the sentence $\varphi$ expresses that $\mathcal{A}_{C(m_k)}$ satisfies the sentence given by this parse tree, that is, the sentence $\varphi_k$. ◀

▶ **Corollary 17.** *For every $d \in \mathbb{N}$, $p$-$d$-*HITTING-SET *is in* para-FO *(and hence in* $\text{para-AC}^0$*).*

---

[2] Proposition 6 in [6] contains a third statement equivalent to (i) and (ii). The corresponding modeltheoretic analogue *decidable and eventually in* FO also characterizes $\text{XFO}_{\text{qr}}$.

## 6 The hierarchy $(\mathrm{FO}_q)_{q\in\mathbb{N}}$ on arithmetical structures

Let $\tau_0 := \{<, +, \times\}$ and let $\tau$ be a vocabulary with $\tau_0 \subseteq \tau$. For $q \in \mathbb{N}$ by $\mathrm{FO}_q[\tau] \subsetneq \mathrm{FO}_{q+1}[\tau]$ *on arithmetical structures* we mean that there is an $\mathrm{FO}_{q+1}[\tau]$-sentence which is not equivalent to any $\mathrm{FO}_q[\tau]$-sentence on all finite $\tau$-structures with built-in addition and multiplication. We say that *the hierarchy* $(\mathrm{FO}_q)_{q\in\mathbb{N}}$ *is strict on arithmetical structures* if there is a vocabulary $\tau \supsetneq \tau_0$ such that $\mathrm{FO}_q[\tau] \subsetneq \mathrm{FO}_{q+1}[\tau]$ on arithmetical structures for every $q \in \mathbb{N}$.

▶ **Theorem 18.** *The hierarchy* $\big(\mathrm{FO}_q\big)_{q\in\mathbb{N}}$ *is strict on arithmetical structures.*

Some preparations are in order. First, we recall how structures are represented by strings. Let $\tau$ be a relational vocabulary and $n \in \mathbb{N}$. We encode a $\tau$-structure $\mathcal{A}$ with $A = [n]$ by a binary string $\mathrm{enc}(\mathcal{A})$ of length $\ell_{\tau,n} := \sum_{R\in\tau} n^{\mathrm{arity}(R)}$. For instance, assume $\tau = \{E, P\}$ with binary $E$ and unary $P$, then $\mathrm{enc}(A) = i_0 i_1 \cdots i_{n^2-1}\, j_0 j_1 \cdots j_{n-1}$ where for every $a, b \in [n]$, $\big(i_{a+b\cdot n} = 1 \iff (a,b) \in E^{\mathcal{A}}\big)$ and $\big(j_a = 1 \iff a \in P^{\mathcal{A}}\big)$.

Let $\mathbf{K}$ be a class of $\tau$-structures. A family of circuits $(\mathsf{C}_n)_{n\in\mathbb{N}}$ *decides* $\mathbf{K}$ if

1. every $\mathsf{C}_n$ has $\ell_{\tau,n}$ inputs,
2. for $n \in \mathbb{N}$ and every $\tau$-structure $\mathcal{A}$ with $A = [n]$, $(\mathcal{A} \in \mathbf{K} \iff \mathsf{C}_n(\mathrm{enc}(\mathcal{A})) = 1)$.

Recall that for $n \in \mathbb{N}$ the classes $\Sigma_n$ and $\Pi_n$ of formulas are defined as follows: $\Sigma_0$ and $\Pi_0$ are the class of quantifier free formulas. The class $\Sigma_{n+1}$ (the class $\Pi_{n+1}$) is the class of formulas of the form $\exists x_1 \ldots \exists x_k \varphi$ with $\varphi \in \Pi_n$ and arbitrary $k$ (of the form $\forall x_1 \ldots \forall x_k \varphi$ with $\varphi \in \Sigma_n$ and arbitrary $k$). The proof of the following fact is simple.

▶ **Lemma 19.** *Every* FO*-formula of quantifier rank $q$ is logically equivalent to a $\Sigma_{q+1}$-formula and to a $\Pi_{q+1}$-formula.*

▶ **Lemma 20.** *Let $q \in \mathbb{N}$. Then for every sentence $\varphi \in \mathrm{FO}_q$ there is a family of circuits $(\mathsf{C}_n)_{n\in\mathbb{N}}$ of depth $\le q+2$ and size $n^{O(1)}$ which decides* $\mathrm{Mod}(\varphi) = \{\mathcal{A} \mid \mathcal{A} \models \varphi\}$*. Moreover, the output of $\mathsf{C}_n$ is an* OR *gate, and the bottom layer of gates in $\mathsf{C}_n$ has fan-in bounded by a constant which only depends on $\varphi$.*

**Proof.** For notational simplicity we assume $q = 3$. By Lemma 19 the sentence $\varphi$ is equivalent to a $\Sigma_4$-sentence

$$\psi = \exists x_{1,1} \cdots \exists x_{1,i_1} \forall x_{2,1} \cdots \forall x_{2,i_2} \exists x_{3,1} \cdots \exists x_{3,i_3} \forall x_{4,1} \cdots \forall x_{4,i_4} \bigwedge_{p\in I_\wedge} \bigvee_{q\in I_\vee} \chi_{pq},$$

where $I_\wedge$ and $I_\vee$ are index sets and every $\chi_{pq}$ is a literal.

For $n \in \mathbb{N}$ we construct the desired circuit $\mathsf{C} = \mathsf{C}_n$ using the standard translation from FO-sentences to $\mathrm{AC}^0$-circuits. That is, every existential (universal) quantifier corresponds to a $\bigvee$ ($\bigwedge$) gate with fan-in $n$; the conjunction is translated to a $\bigwedge$ gate with fan-in $|I_\wedge|$ and the disjunctions to $\bigvee$ gates with fan-in $|I_\vee|$. Next we merge consecutive layers of gates that are all $\bigwedge$, or that are all $\bigvee$. The resulting circuit $\mathsf{C}_n$ is of depth $q+2$. It has an OR as output gate and bottom fan-in bounded by $|I_\vee|$. ◀

Key to our proof of Theorem 18 are the following boolean functions called *Sipser functions*.

▶ **Definition 21** ([16, 5])**.** Let $d \ge 1$ and $m_1, \ldots, m_d \in \mathbb{N}$. For every $i_1 \in [m_1]$, $i_2 \in [m_2]$, $\ldots$, $i_d \in [m_d]$ we introduce a boolean variable $X_{i_1,\ldots,i_d}$. Define

$$f_d^{m_1,\ldots,m_d} := \bigwedge_{i_1\in[m_1]} \bigvee_{i_2\in[m_2]} \cdots \bigodot_{i_d\in[m_d]} X_{i_1,\ldots,i_d}, \qquad (7)$$

where $\bigodot$ is $\bigvee$ if $d$ is even, and $\bigwedge$ otherwise. For every $d \geq 2$ and $m \geq 1$ we set

$$\text{Sipser}_d^m := f_d^{m_1,\dots,m_d}$$

with $m_1 = \left\lceil \sqrt{m/\log\, m} \right\rceil$, $m_2 = \cdots m_{d-1} = m$, and $m_d = \left\lceil \sqrt{d/2 \cdot m \cdot \log\, m} \right\rceil$.

Observe that the size of $\text{Sipser}_d^m$ is bounded by $m^{O(d)}$.

The following lower bound for $\text{Sipser}_d^m$ is proved in [11]. We use the version presented as Theorem 4.2 in [15].

▶ **Theorem 22.** *Let $d \geq 2$. Then there exists a constant $\beta_d > 0$ so that if a depth $d+1$, bottom fan-in $k$ circuit with an* OR *gate as the output and at most $S$ gates in levels* 1 *through $d$ computes $\text{Sipser}_d^m$, then either $S \geq 2^{m^{\beta_d}}$ or $k \geq m^{\beta_d}$.*

**Proof of Theorem 18.** $\text{FO}_0 \subsetneq \text{FO}_1$ is trivial by considering the sentence $\exists x\, Ux$ where $U$ is a unary relation symbol. We still need to show that for an appropriate vocabulary $\tau \supseteq \tau_0$ it holds $\text{FO}_q[\tau] \subsetneq \text{FO}_{q+1}[\tau]$ on arithmetical structures for every $q \geq 1$.

Let $d, m \in \mathbb{N}$. We identify the function $\text{Sipser}_d^m$ with the circuit in (7) which computes it. Let $E$ be a binary relation symbol and $U$ a unary relation symbol. Then we view the underlying (directed) graph of $\text{Sipser}_d^m$ as a $\{E, U\}$-structure $\mathcal{A}_{d,m}$ with

$$A_{d,m} := \{v_g \mid g \text{ a gate in } \text{Sipser}_d^m\}, \qquad E^{\mathcal{A}_{d,m}} := \{(v_{g'}, v_g) \mid g' \text{ is an input to } g\},$$
$$U^{\mathcal{A}_{d,m}} := \{v_g \mid g \text{ is an input to the output gate}\}.$$

Let $P$ be a unary relation symbol. Every assignment $B$ of (truth values to the input nodes of) $\text{Sipser}_d^m$ can be identified with $P^{\mathcal{A}_{d,m}} := \{g \mid g \text{ an input gate assigned to } \textsc{true} \text{ by } B\}$. For $\tau' := \{E, U, P\}$ we define an $\text{FO}[\tau']$-sentence $\varphi_d$ such that for all $m$,

$$\text{Sipser}_d^m(P^{\mathcal{A}_{d,m}}) = \textsc{true} \iff (\mathcal{A}_{d,m}, P^{\mathcal{A}_{d,m}}) \models \varphi_d. \tag{8}$$

Fix $q \geq 1$. Assume $q$ is even and set $d := q+1$ (the case of odd $q$ is treated similarly). We define inductively $\text{FO}[\tau']$-formulas $\psi_\ell(x)$ by

$$\psi_0(x) := Px, \qquad \text{and} \qquad \psi_{\ell+1}(x) := \begin{cases} \forall y\big(Eyx \to \psi_\ell(y)\big) & \text{if } \ell \text{ is even,} \\ \exists y\big(Eyx \wedge \psi_\ell(y)\big) & \text{if } \ell \text{ is odd.} \end{cases}$$

We set (recall the definition of $U^{\mathcal{A}_{d,m}}$)

$$\varphi_{q+1} := \forall x(Ux \to \psi_q(x)).$$

It is straightforward to verify that $\text{qr}(\varphi_{q+1}) = q+1$ and that $\varphi_{q+1}$ satisfies (8) (for $d = q+1$).

Let $\tau := \tau' \cup \{<, +, \times\} = \{E, U, P, <, +, \times\}$. We define

$$\textsc{Sipser}_{q+1} := \big\{\mathcal{A} \in \text{ARITHM}[\tau] \;\big|\; \mathcal{A} \models \varphi_{q+1}\big\}.$$

By definition the class $\textsc{Sipser}_{q+1}$ is axiomatizable in $\text{FO}_{q+1}[\tau]$. We show that $\textsc{Sipser}_{q+1}$ is not axiomatizable in $\text{FO}_q[\tau]$. For a contradiction, assume that $\textsc{Sipser}_{q+1} = \text{Mod}(\varphi)$ for some $\varphi \in \text{FO}_q[\tau]$. Then by Lemma 20 there exists a family of circuits $\big(\mathsf{C}_n\big)_{n\in\mathbb{N}}$ such that the following conditions are satisfied.

**(C1)** Every $\mathsf{C}_n$ has $\ell_{\tau,n}$ inputs, depth $q+2$, and size $\ell_{\tau,n}^{O(1)}$.

**(C2)** The output of $\mathsf{C}_n$ is an OR gate, and its bottom fan-in is bounded by a constant.

**(C3)** For every $n \in \mathbb{N}$ and every $\tau$-structure $\mathcal{A}$ with $A = [n]$

$$\mathcal{A} \in \textsc{Sipser}_{q+1} \iff \mathsf{C}_n(\text{enc}(\mathcal{A})) = 1.$$

Let $m \in \mathbb{N}$ and let $n$ be the number of variables in $\text{Sipser}_{q+1}^m$, i.e.,

$$n = \left\lceil \sqrt{m/\log m} \right\rceil \cdot m^{q-1} \cdot \left\lceil \sqrt{(q+1)/2 \cdot m \cdot \log m} \right\rceil.$$

Consider the structure $\mathcal{A}_{q+1,m}$ associated with $\text{Sipser}_{q+1}^m$ and expand it with $<, +, \times$. Thus for any assignment of the $n$ inputs, identified with the unary relation $P^{\mathcal{A}_{q+1,m}}$, we have

$$\begin{aligned} \text{Sipser}_{q+1}^m(P^{\mathcal{A}_{q+1,m}}) = 1 \quad &\iff \quad \left(\mathcal{A}_{q+1,m}, <, +, \times, P^{\mathcal{A}_{q+1,m}}\right) \models \varphi \\ &\iff \quad \mathsf{C}_n\Big(\text{enc}\left(\mathcal{A}_{q+1,m}, <, +, \times, P^{\mathcal{A}_{q+1,m}}\right)\Big) = 1. \end{aligned}$$

Here is the crucial observation. In the string $\text{enc}(\mathcal{A}_{q+1,m}, <, +, \times, P^{\mathcal{A}_{q+1,m}})$ only the last $n$ bits depend on the assignment, that is, on $P^{\mathcal{A}_{q+1,m}}$. These are precisely the $n$ input bits for the $\text{Sipser}_{q+1}^m$ function. Thus we can simplify the circuit $\mathsf{C}_n$ by fixing the values of the first $\ell_{\tau,n} - n$ inputs according to $(\mathcal{A}_{q+1,m}, <, +, \times)$. Let $\mathsf{C}_n^*$ be the resulting circuit. We have

$$\text{Sipser}_{q+1}^m(P^{\mathcal{A}_{q+1,m}}) = 1 \quad \iff \quad \mathsf{C}_n^*(P^{\mathcal{A}_{q+1,m}}) = 1.$$

By (C1), $\mathsf{C}_n^*$ has depth $q+2$ and size $n^{O(1)}$ (as $\ell_{\tau,n} = n^{O(1)}$). By (C2) its output is an OR gate, and its bottom fan-in is bounded by a constant. As $m \in \mathbb{N}$ is arbitrary, this clearly contradicts Theorem 22. ◀

**Proof of Theorem 2.** Let $q \in \mathbb{N}$. By Theorem 18 we know that there is a vocabulary $\tau$ and an $\text{FO}_{q+1}[\tau]$-sentence $\varphi$ which is not equivalent to any $\text{FO}_q[\tau]$-sentences on arithmetical structures. We claim that

$$Q := \left\{(\mathcal{A}, 0) \;\middle|\; \mathcal{A} \in \text{ARITHM}[\tau] \text{ and } \mathcal{A} \models \varphi\right\}$$

is not slicewise definable in $\text{FO}_q$. As $Q$ is slicewise definable in $\text{FO}_{q+1}$, this would give us the desired separation.

Assume otherwise, then, by Definition 6, there is a constant $m_0 \in \mathbb{N}$ and a sentence $\psi$ in $\text{FO}_q[\tau \cup C(m_0)]$ such that for every $\mathcal{A} \in \text{ARITHM}[\tau]$

$$\mathcal{A} \models \varphi \quad \iff \quad \mathcal{A}_{C(m_0)} \models \psi.$$

This does not give us a contradiction immediately, since $\psi$ might contain constants in $C(m_0)$. But it is easy to see that Lemma 19 and Lemma 20 both survive in the presence of constants. Thus almost the same proof of Theorem 18 shows that $\psi \in \text{FO}_q[\tau \cup C(m_0)]$ cannot exist. ◀

## 7 Conclusions

We have shown that a few parameterized problems are slicewise definable in first-order logic with bounded quantifier rank. In particular, the $k$-vertex-cover problem, i.e., the $k$th slice of $p$-VERTEX-COVER, is definable in $\text{FO}_{17}$ for every $k \in \mathbb{N}$. One natural follow-up question is whether this is optimal. Or can we show at least that $p$-VERTEX-COVER $\notin \text{XFO}_2$? Such a question is reminiscent of the recent quest for optimal algorithms for natural polynomial time solvable problems (see e.g., [2]). In our result $p$-$d$-HITTING-SET $\in \text{XFO}_q$ we have $q = O(d^2)$, and we conjecture that there is no universal constant $q$ which works for every $p$-$d$-HITTING-SET. But so far, we do not know how to prove such a result.

It turns out that the class $\text{XFO}_{\text{qr}}$ coincides with the parameterized circuit complexity class para-$\text{AC}^0$ which has been intensively studied in [3, 6]. Similar to [3], it seems that all the non-trivial examples in $\text{XFO}_{\text{qr}}$ require the color coding technique. It would be interesting to see whether other tools from parameterized complexity can be used to show membership in $\text{XFO}_{\text{qr}}$.

We have also established the strictness of $\left(\mathrm{XFO}_q\right)_{q\in\mathbb{N}}$ by proving that $\mathrm{FO}_q \subsetneq \mathrm{FO}_{q+1}$ on arithmetical structures for every $q \in \mathbb{N}$. Our proof is built on a strict $\mathrm{AC}^0$-hierarchy on Sipser functions. We conjecture that the sentence

$$\exists x_1 \cdots \exists x_{q+1} \bigwedge_{1\leq i<j\leq q+1} E_{x_i x_j},$$

which characterizes the existence of a $(q+1)$-clique, witnesses $\mathrm{FO}_q \subsetneq \mathrm{FO}_{q+1}$ on graphs with built-in addition and multiplication. Rossman [14] has shown that $(q+1)$-clique cannot be expressed in arithmetical structures with $\lfloor (q+1)/4 \rfloor$ variables and hence not in $\mathrm{FO}_{\lfloor (q+1)/4\rfloor}$. This already shows that the hierarchy $(\mathrm{FO}_q)_{q\in\mathbb{N}}$ does not collapse.

## References


1 N. Alon, R. Yuster, and U. Zwick. Color-coding. *Journal of the ACM*, 42(4):844–856, 1995.

2 A. Backurs and P. Indyk. Edit distance cannot be computed in strongly subquadratic time (unless SETH is false). In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing, STOC 2015, Portland, OR, USA, June 14-17, 2015*, pages 51–58, 2015.

3 M. Bannach, C. Stockhusen, and T. Tantau. Fast parallel fixed-parameter algorithms via color coding. In *Proceedings of the 10th International Symposium on Parameterized and Exact Computation, IPEC 2015, September 16-18, 2015, Patras, Greece*, pages 224–235, 2015.

4 D. A. Mix Barrington, N. Immerman, and H. Straubing. On uniformity within $\mathrm{NC}^1$. *Journal of Computer and System Sciences*, 41(3):274–306, 1990.

5 R. B. Boppana and M. Sipser. The complexity of finite functions. In *Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity (A)*, pages 757–804. MIT Press, 1990.

6 Y. Chen and J. Flum. Some lower bounds in parameterized $\mathrm{AC}^0$. In *Proceedings of the 41st International Symposium on Mathematical Foundations of Computer Science, MFCS 2016, August 22-26, 2016 – Kraków, Poland*, pages 27:1–27:14, 2016.

7 M. Elberfeld, C. Stockhusen, and T. Tantau. On the space and circuit complexity of parameterized problems: Classes and completeness. *Algorithmica*, 71(3):661–701, 2015.

8 J. Flum and M. Grohe. Fixed-parameter tractability, definability, and model-checking. *SIAM Journal on Computing*, 31(1):113–145, 2001.

9 J. Flum and M. Grohe. Describing parameterized complexity classes. *Information and Computation*, 187(2):291–319, 2003.

10 J. Flum and M. Grohe. *Parameterized Complexity Theory.* Springer, 2006.

11 J. Håstad. Almost optimal lower bounds for small depth circuits. In *Randomness and Computation*, pages 6–20. JAI Press, 1989.

12 N. Immerman. *Descriptive Complexity.* Graduate Texts in Computer Science. Springer, 1999.

13 R. Niedermeier and P. Rossmanith. An efficient fixed-parameter algorithm for 3-hitting set. *Journal of Discrete Algorithms*, 1(1):89–102, 2003.

14 B. Rossman. On the constant-depth complexity of $k$-clique. In *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, Victoria, British Columbia, Canada*, pages 721–730, 2008.

15 N. Segerlind, S. R. Buss, and R. Impagliazzo. A switching lemma for small restrictions and lower bounds for k-DNF resolution. *SIAM Journal on Computing*, 33(5):1171–1200, 2004.

16 M. Sipser. Borel sets and circuit complexity. In *Proceedings of the 15th Annual ACM Symposium on Theory of Computing, 25-27 April, 1983, Boston, Massachusetts, USA*, pages 61–69, 1983.