# Some Lower Bounds in Parameterized $AC^0$*

**Yijia Chen[1] and Jörg Flum[2]**

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

**Abstract**

We demonstrate some lower bounds for parameterized problems via parameterized classes corresponding to the classical $AC^0$. Among others, we derive such a lower bound for all fpt-approximations of the parameterized clique problem and for a parameterized halting problem, which recently turned out to link problems of computational complexity, descriptive complexity, and proof theory. To show the first lower bound, we prove a strong $AC^0$ version of the planted clique conjecture: $AC^0$-circuits asymptotically almost surely can not distinguish between a random graph and this graph with a randomly planted clique of any size $\leq n^\xi$ (where $0 \leq \xi < 1$).

**1998 ACM Subject Classification** F.1.1 Unbounded-action devices, F.1.3 Complexity hierarchies, F.4.1 Computational logic

**Keywords and phrases** parameterized $AC^0$, lower bound, clique, halting problem

**Digital Object Identifier** 10.4230/LIPIcs.MFCS.2016.27

## 1 Introduction

For $k \in \mathbb{N}$ the $k$-clique problem asks, given a graph $G$, whether it contains a clique of size $k$. In [20], Rossman showed that the $k$-clique problem has no bounded-depth and unbounded-fan-in circuits of size $O(n^{k/4})$. Therefore, there doesn't exist a family $(\mathsf{C}_{n,k})_{n,k\in\mathbb{N}}$ of circuits such that for some functions $d, f : \mathbb{N} \to \mathbb{N}$,

- every $\mathsf{C}_{n,k}$ has depth at most $d(k)$ and size bounded by $f(k) \cdot n^{k/4}$,
- an $n$-vertex graph $G$ has a $k$-clique if and only if $\mathsf{C}_{n,k}(G) = 1$.

If the constraint on the depth of the circuits could be removed, then we would immediately obtain that the *parameterized clique problem*

| $p$-Clique | |
|---|---|
| *Instance:* | A graph $G$ and $k \in \mathbb{N}$. |
| *Parameter:* | $k$. |
| *Problem:* | Does $G$ contain a clique of size $k$? |

cannot be solved in time $f(k) \cdot n^{O(1)}$. Thus, $p$-Clique would not be fixed-parameter tractable and hence, FPT $\neq$ W[1] since $p$-Clique is in the parameterized class W[1]. Therefore, Rossman's result may be viewed as an $AC^0$ version of FPT $\neq$ W[1], an inequality conjectured by most experts in the field (recall that the complexity class $AC^0$ contains all problems that can be computed by bounded-depth and unbounded fan-in circuits of polynomial size).

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





In [11] Elberfeld et al. introduced the parameterized class para-$AC^0$ as the $AC^0$ analog of the class FPT: A problem is in para-$AC^0$ if it can be computed by *dlogtime-uniform* $AC^0$-circuits after an (arbitrarily complex) *precomputation* [12] on the parameter. Later in [3] it was shown that para-$AC^0$ contains the *parameterized vertex cover problem*, one of the archetypal fixed-parameter tractable problems. For various other problems the authors of [3] also proved their membership in para-$AC^0$. Concerning nonmembership, a result in [6] shows that the parameterized *st*-connectivity problem ($p$-stConn), i.e., the problem of deciding whether there is a path of length at most $k$ between vertices $s$ and $t$ in a graph $G$, parameterized by $k$, is not in para-$AC^0$. It is worth noting that *st*-connectivity is solvable in polynomial time, and hence, $p$-stConn $\in$ FPT.

The class $AC^0$ is one of the best understood classical complexity classes. Already in [1, 13] it was shown that Parity, the problem of deciding whether a binary string contains an even number of 1's, is not in $AC^0$. Since Parity has a very low complexity, for many other problems, including Vertex-Cover and Clique, the $AC^0$-lower bound can be easily derived by reductions from Parity. Similarly, as $p$-Clique $\notin$ para-$AC^0$, it is not very hard to see, using some appropriate weak parameterized reductions, that many other parameterized problems, including the dominating set problem, are not in para-$AC^0$.

It is well known that the class $AC^0$ is intimately connected to first-order logic (FO). In fact, the problems decidable by a dlogtime-uniform $AC^0$-family of circuits are precisely those definable in $\mathrm{FO}(<,+,\times)$, that is, in first-order logic for ordered structures with built-in predicates of addition and multiplication.

Now we can also study various parameterized classes based on fragments of $\mathrm{FO}(<,+,\times)$. Let us emphasize that this is not merely an academic exercise. Logic and parameterized complexity are surprisingly intertwined with each other, which, among others, is witnessed by various algorithmic meta-theorems (see e.g. [15]). Moreover, the problem whether there is a logic for PTIME, a central problem of descriptive complexity, turned out (see [9] for a thorough discussion) to be related to the complexity of the parameterized halting problem

| $p$-Halt | |
|---|---|
| *Instance:* | $n \in \mathbb{N}$ in *unary* and a nondeterministic Turing machine (NTM) $\mathbb{M}$. |
| *Parameter:* | $\lvert\mathbb{M}\rvert$, the size of the machine $\mathbb{M}$. |
| *Problem:* | Does $\mathbb{M}$ accept the empty input tape in at most $n$ steps? |

In fact, already in [19] it was shown that PTIME has a logic if $p$-Halt has an algorithm with running time $n^{f(|\mathbb{M}|)}$ for some function $f$. We get a family $(\mathsf{C}_{n,k})_{n,k\in\mathbb{N}}$ of circuits such that

- every $\mathsf{C}_{n,k}$ has depth 2 and size $g(k)\cdot n$ for some function $g:\mathbb{N}\to\mathbb{N}$,
- an NTM $\mathbb{M}$ accepts the empty input tape in at most $n$ steps if and only if $\mathsf{C}_{n,|\mathbb{M}|}(n,\mathbb{M})=1$

by hard-wiring into $\mathsf{C}_{n,k}$ the NTMs of size $k$ which halt on empty input in $\leq n$ steps. Therefore, $p$-Halt belongs to a *nonuniform* version of para-$AC^0$. The question arises whether $p$-Halt $\in$ para-$AC^0$. A positive answer will yield that $p$-Halt $\in$ FPT, which is considered to be highly unlikely [9]. Hence, the goal is to show *unconditionally* that $p$-Halt $\notin$ para-$AC^0$. To the best of our knowledge, all existing $AC^0$ lower bounds for natural problems apply to both uniform and nonuniform circuits. Perhaps, in order to settle the complexity of $p$-Halt with respect to para-$AC^0$, a better understanding of the uniformity conditions of circuits is really required.

## 1.1 Our work

In this paper, we investigate lower bounds in terms of para-$AC^0$. We show that a number of problems are not in this class or in some of its proper subclasses.

Following the framework proposed in [12], we first compare two possible definitions of para-$\mathrm{AC}^0$ depending on different ways to obtain parameterized classes from classical ones. We already mentioned the first one, in which an arbitrary precomputation can be performed on the parameter before a standard computation according to the corresponding classical class. The second approach requires the parameterized problem to be in the classical class if we restrict to instances where the parameter is far smaller than the size of the input. We show that both views lead to the same para-$\mathrm{AC}^0$.

Then we derive a first set of lower bound results: We show that many natural W[1]-hard problems are not in para-$\mathrm{AC}^0$ by arguing that the corresponding reductions from $p$-Clique can be made in $\mathrm{AC}^0$. Among others, they include the weighted satisfiability problems for classes of propositional formulas, which define the W-hierarchy.

We present a modeltheoretic tool, based on the color-coding method, which allows to show membership in $\mathrm{AC}^0$ (similarly as done in [3] via circuits).

We generalize Rossman's result mentioned at the beginning of this introduction and show that any fpt-approximation of $p$-Clique is not in para-$\mathrm{AC}^0$. To get this result we prove that $\mathrm{AC}^0$-circuits asymptotically almost surely can not distinguish between a random graph and this graph with a randomly planted clique of any size $\leq n^\xi$ with $0 \leq \xi < 1$. Our first proof of the last two results used the sophisticated machinery in [20]. Here we outline a proof, suggested to us anonymously, which is directly built on Beame's *Clique Switching Lemma* [5]. The fpt-approximation lower bound of $p$-Clique again can be transferred to the weighted satisfiability problems, provided the propositional formulas are of odd depth.

Finally we turn to $p$-Halt. We are not able to show $p$-Halt $\notin$ para-$\mathrm{AC}^0$, however, using the decidability of Presburger's arithmetic we prove that $p$-Halt is not in para-$\mathrm{FO}(<,+)$, not even in $\mathrm{XFO}(<,+)$. On the other hand, $p$-Halt $\in$ nonuniform-para-$\mathrm{FO}(<,+)$.

Due to space limitations for some proofs we refer to the full version of the paper.

## 2 Preliminaries

By $\mathbb{N}$ we denote the set of nonnegative integers. For every $n \in \mathbb{N}$ we let $[n] := \{1, \dots, n\}$. Let $\mathbb{R}$ be the set of real numbers, $\mathbb{R}_+ := \{r \in \mathbb{R} \mid r > 0\}$, and $\mathbb{R}_{\geq 1} := \{r \in \mathbb{R} \mid r \geq 1\}$. For any set $A$ and $k \in \mathbb{N}$ we define $\binom{A}{k}$ as the class of $k$-element subsets of $A$, i.e., $\{S \subseteq A \mid |S| = k\}$.

A (simple) graph $G = (V(G), E(G))$ (for short, $G = (V, E)$) is undirected and has no loops and multiple edges. Here, $V(G)$ is the vertex set and $E(G)$ the edge set, respectively. A subset $C \subseteq V(G)$ is a *clique* of $G$ if for every $u, v \in C$ either $u = v$ or $\{u, v\} \in E(G)$. And $D \subseteq V(G)$ is a *dominating set* of $G$ if for every $v \in V(G)$ either $v \in D$ or there exists $u \in D$ with $\{u, v\} \in E(G)$.

### 2.1 Relational structures and first-order logic

A *vocabulary* $\tau$ is a finite set of relation symbols. Each relation symbol has an *arity*. A *structure* $\mathcal{A}$ of vocabulary $\tau$, or simply structure, consists of a finite set $A$ called the *universe*, and an interpretation $R^{\mathcal{A}} \subseteq A^r$ of each $r$-ary relation symbol $R \in \tau$. For example, a graph $G$ can be identified with a structure $\mathcal{A}(G)$ of vocabulary $\{E\}$ with binary relation symbol $E$ such that $A(G) := V(G)$ and $E^{\mathcal{A}(G)} := \{(u, v) \mid \{u, v\} \in E(G)\}$.

Formulas of first-order logic of vocabulary $\tau$ are built up from atomic formulas $x = y$ and $Rx_1 \dots x_r$, where $x, y, x_1, \dots, x_r$ are variables and $R \in \tau$ is of arity $r$, using the boolean connectives and existential and universal quantification. For example, for every $k \geq 1$ let

$$\mathit{clique}_k := \exists x_1 \dots \exists x_k \Big( \bigwedge_{1 \leq i < j \leq k} (\neg x_i = x_j \wedge E x_i x_j) \Big).$$

Then a graph $G$ has a $k$-clique if and only if $\mathcal{A}(G) \models \mathit{clique}_k$.

## 2.2 Parameterized complexity

We fix an alphabet $\Sigma := \{0,1\}$. A *parameterized problem* $(Q,\kappa)$ consists of a classical problem $Q \subseteq \Sigma^*$ and a function $\kappa : \Sigma^* \to \mathbb{N}$, the *parameterization*, computable in polynomial time. As an example, we have already seen $p$-Clique in the Introduction. A similar problem is the *parameterized dominating set problem*.

| $p$-Dominating-Set | |
|---|---|
| *Instance:* | A graph $G$ and $k \in \mathbb{N}$. |
| *Parameter:* | $k$. |
| *Problem:* | Does $G$ contain a dominating set of size $k$? |

Both, $p$-Clique and $p$-Dominating-Set, play an important role in parameterized complexity, mainly because they are complete for the classes W[1] and W[2], respectively. Recall that the classes of the W-hierarchy are defined by taking the closure under fpt-reductions of the following weighted satisfiability problem for suitable classes $\Gamma$ of propositional formulas.

| $p$-WSat($\Gamma$) | |
|---|---|
| *Instance:* | $\gamma \in \Gamma$ and $k \in \mathbb{N}$. |
| *Parameter:* | $k$. |
| *Problem:* | Does $\gamma$ have a satisfying assignment of Hamming weight $k$? |

▶ **Definition 1.** Let $(Q,\kappa)$ and $(Q',\kappa')$ be two parameterized problems. An *fpt-reduction* from $(Q,\kappa)$ to $(Q',\kappa')$ is a mapping $R : \Sigma^* \to \Sigma^*$ such that:

- For $x \in \Sigma^*$ we have $(x \in Q \iff R(x) \in Q')$.
- For $x \in \Sigma^*$, $R(x)$ is computable in time $f(\kappa(x)) \cdot |x|^{O(1)}$ for some computable $f : \mathbb{N} \to \mathbb{N}$.
- There is a computable function $g : \mathbb{N} \to \mathbb{N}$ such that $\kappa'(R(x)) \leq g(\kappa(x))$ for all $x \in \Sigma^*$.

If there is an fpt-reduction from $(Q,\kappa)$ to $(Q',\kappa')$, then we write $(Q,\kappa) \leq^{\mathrm{fpt}} (Q',\kappa')$.

For $t \geq 0$ and $d \geq 1$ we inductively define the classes $\Gamma_{t,d}$ and $\Delta_{t,d}$ of propositional formulas: $\Gamma_{0,d}$ and $\Delta_{0,d}$ are the class of conjunctions of at most $d$ literals and the class of disjunctions of at most $d$ literals, respectively.

$$\Gamma_{t+1,d} := \Big\{ \bigwedge_{i \in I} \delta_i \mid I \text{ finite and } \delta_i \in \Delta_{t,d} \text{ for all } i \in I \Big\},$$

$$\Delta_{t+1,d} := \Big\{ \bigvee_{i \in I} \gamma_i \mid I \text{ finite and } \gamma_i \in \Gamma_{t,d} \text{ for all } i \in I \Big\}.$$

▶ **Definition 2.** Let $t \geq 1$. The class W[$t$] of the W-*hierarchy* is defined by

$$\mathrm{W}[t] := \bigcup_{d \geq 1} \big\{ (Q,\kappa) \mid (Q,\kappa) \leq^{\mathrm{fpt}} p\text{-WSat}(\Gamma_{t,d}) \big\}.$$

## Circuit Complexity

A circuit $\mathsf{C}$ with $n$ input gates is a directed acyclic graph in which every node (i.e., gate) is labelled by $\bigwedge$, $\bigvee$, $\neg$, or by one of the variables, or by $0, 1$. All $\bigwedge$ and $\bigvee$ gates may have arbitrarily many inputs, i.e., $\mathsf{C}$ is of *unbounded fan-in*. The *depth* of $\mathsf{C}$ is the length of a longest directed path in $\mathsf{C}$. The *size* of $\mathsf{C}$, denoted by $|\mathsf{C}|$, is the number of gates in $\mathsf{C}$. We

often tacitly identify $\mathsf{C}$ with the function $\mathsf{C} : \{0,1\}^n \to \{0,1\}^m$ it computes. Here, $n$ is the number of variables of $\mathsf{C}$ and $m$ the number of its *output gates*.

$\mathrm{AC}^0$ is the class of problems that can be computed by circuits of bounded-depth and polynomial size. More precisely:

▶ **Definition 3.** Let $Q \subseteq \Sigma^*$. We say that $Q \in \mathrm{AC}^0$ if there exists a family of boolean circuits $(\mathsf{C}_n)_{n\in\mathbb{N}}$ such that:

**(A1)** The depth of every $\mathsf{C}_n$ is bounded by a fixed constant.

**(A2)** $|\mathsf{C}_n| = n^{O(1)}$.

**(A3)** Let $x \in \Sigma^*$. Then ($x \in Q$ if and only if $C_{|x|}(x) = 1$). In particular, every $\mathsf{C}_n$ has $n$ input gates.

**(A4)** $(\mathsf{C}_n)_{n\in\mathbb{N}}$ is *dlogtime-uniform*, that is: there is a *deterministic logtime Turing machine* $\mathbb{M}$ which on input $1^n$ outputs the circuit $\mathsf{C}_n$. More precisely, $\mathbb{M}$ recognizes the language $\{(b, i, 1^n) \mid \text{the } i\text{th bit of the binary encoding of } C_n \text{ is } b\}$ (cf. Section 6 of [4]).

Often, $(\mathsf{C}_n)_{n\in\mathbb{N}}$ are called $\mathrm{AC}^0$*-circuits*.

We remark that most lower bounds in our paper still hold without the requirement (A4). Therefore, (A4) is irrelevant for most of our results. However, with this uniformity condition, $\mathrm{AC}^0$ characterizes precisely the class of problems that are definable in $\mathrm{FO}(<, +, \times)$ [4].

## 3 The class para-$\mathrm{AC}^0$ and some natural examples

▶ **Definition 4** ([3])**.** Let $(Q, \kappa)$ be a parameterized problem. Then $(Q, \kappa)$ is in para-$\mathrm{AC}^0$ if there exists a family $(\mathsf{C}_{n,k})_{n,k\in\mathbb{N}}$ of circuits such that:

**(P1)** The depth of every $\mathsf{C}_{n,k}$ is bounded by a fixed constant.

**(P2)** $|\mathsf{C}_{n,k}| \leq f(k) \cdot n^{O(1)}$ for every $n, k \in \mathbb{N}$, where $f : \mathbb{N} \to \mathbb{N}$ is a computable function.

**(P3)** Let $x \in \Sigma^*$. Then ($x \in Q$ if and only if $\mathsf{C}_{|x|,\kappa(x)}(x) = 1$).

**(P4)** There is a deterministic Turing machine that on input $(1^n, 1^k)$ computes the circuit $\mathsf{C}_{n,k}$ in time $g(k) + O(\log n)$, where $g : \mathbb{N} \to \mathbb{N}$ is a computable function.

For future reference, we restate Rossman's main result [20] as follows.

▶ **Theorem 5.** *Let $k \in \mathbb{N}$. Then there is no family $(\mathsf{C}_n)_{n\in\mathbb{N}}$ of circuits such that:*

- *The depth of every $\mathsf{C}_n$ is bounded by a fixed constant.*
- *The size of $\mathsf{C}_n$ is $n^{O(k/4)}$.*
- *Let $G$ be a graph and $n := |V(G)|$. Then $G$ has a $k$-clique if and only if $\mathsf{C}_n(G) = 1$.*

*In particular, $p$-Clique $\notin$ para-$\mathrm{AC}^0$.*

▶ Remark. Recall that Chen et al. [7] showed that $p$-Clique has no algorithms of running time $f(k) \cdot |n|^{o(k)}$ unless the Exponential Time Hypothesis (ETH) fails. ETH is apparently stronger than FPT $\neq$ W[1]. Theorem 5 establishes an $\mathrm{AC}^0$ version of FPT $\neq$ W[1].

Next, we give two equivalent characterizations of para-$\mathrm{AC}^0$ (for a proof see the full version). The first one (i.e., between (i) and (ii)) was already mentioned in [11]. Note that in [11] it is required that a problem in para-$\mathrm{AC}^0$ has an $\mathrm{AC}^0$ computable parameterization.

▶ **Proposition 6.** *Let $(Q, \kappa)$ be a parameterized problem. Consider the following statements.*

**(i)** $(Q, \kappa) \in$ para-$\mathrm{AC}^0$.

**(ii)** *There is a computable function $pre : \mathbb{N} \to \Sigma^*$ (i.e., a precomputation) and $\mathrm{AC}^0$-circuits $(\mathsf{C}_n)_{n\in\mathbb{N}}$ such that for $x \in \Sigma^*$,*

$$x \in Q \iff \mathsf{C}_{|(x,pre(\kappa(x)))|}(x, pre(\kappa(x))) = 1.$$

**(iii)** *$Q$ is decidable and there is a computable function, $h : \mathbb{N} \to \mathbb{N}$ and $\mathrm{AC}^0$-circuits $\left(\mathsf{C}_n\right)_{n\in\mathbb{N}}$ such that for every $x \in \Sigma^*$ with $|x| \geq h(\kappa(x))$,*

$$x \in Q \iff C_{|x|}(x) = 1.$$

*Then (iii) ⇒ (i) ⇔ (ii). If, in addition, the parameterization $\kappa$ can be computed by $\mathrm{AC}^0$-circuits, then (i) ⇒ (iii), i.e., they are all equivalent.*

In order to use Theorem 5 to show para-AC$^0$ lower bounds for other problems, we introduce a more restricted form of fpt-reductions.

▶ **Definition 7.** Let $(Q, \kappa)$ and $(Q', \kappa')$ be two parameterized problems. A *para-$\mathrm{AC}^0$-reduction* from $(Q, \kappa)$ to $(Q', \kappa')$ is a mapping $R : \Sigma^* \to \Sigma^*$ such that:

**(R1)** For all $x \in \Sigma^*$ we have $(x \in Q \iff R(x) \in Q')$.

**(R2)** There is a family $(\mathsf{C}_{n,k})_{n,k\in\mathbb{N}}$ of circuits, whose depth is bounded by a fixed constant, such that

1. for all $x \in \Sigma^*$, $\mathsf{C}_{|x|,\kappa(x)}(x)$ outputs $R(x)$;
2. every $|\mathsf{C}_{n,k}| \leq f(k) \cdot |x|^{O(1)}$ for a computable function $f : \mathbb{N} \to \mathbb{N}$;
3. there is a deterministic Turing machine that on input $(1^n, 1^k)$ computes the circuit $\mathsf{C}_{n,k}$ in time $g(k) + O(\log\ n)$, where $g : \mathbb{N} \to \mathbb{N}$ is a computable function.

**(R3)** There is a computable function $h : \mathbb{N} \to \mathbb{N}$ such that $\kappa'(R(x)) \leq h(\kappa(x))$ for all $x \in \Sigma^*$.

If there is a para-AC$^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$, then we write $(Q, \kappa) \leq^{\mathrm{pac}} (Q', \kappa')$.

However, in general para-AC$^0$ is *not* closed under para-AC$^0$-reductions:

▶ **Example 8.** Define $Q := \left\{(x, b) \;\middle|\; x \in \{0,1\}^* \text{ and } b = \sum_{i\in[|x|]} x_i \mod 2\right\}$. Clearly, $Q$ is equivalent to the classical Parity problem of deciding whether there is an even number of 1's in $x$. Thus $Q \notin \mathrm{AC}^0$. We define polynomial time computable parameterizations of $Q$ by $\kappa_1(x, b) := 0$ and $\kappa_2(x, b) := \sum_{i\in[|x|]} x_i \mod 2$. Then it is easy to see that $(Q, \kappa_1) \notin$ para-AC$^0$ and $(Q, \kappa_2) \in$ para-AC$^0$; yet $(Q, \kappa_1) \leq^{\mathrm{pac}} (Q, \kappa_2)$ by the identity mapping $R(x, b) = (x, b)$.

Note $(Q, \kappa_2)$ also serves as a counterexample for the direction from (i) to (iii) in Proposition 6.

Therefore we need a further requirement on pac-reductions. The previous example suggests to require the AC$^0$-computability of the parameterization (as done in [11]). In fact, para-AC$^0$ is closed under those reductions. However, we choose another requirement, which is simpler to verify and is satisfied by almost all natural reductions.

▶ **Definition 9.** Let $(Q, \kappa)$ and $(Q', \kappa')$ be two parameterized problems. A *weak para-$\mathrm{AC}^0$-reduction* from $(Q, \kappa)$ to $(Q', \kappa')$ is a *para-$\mathrm{AC}^0$-reduction* which satisfies:

**(R3')** There is a computable function $h : \mathbb{N} \to \mathbb{N}$ such that $\kappa'(R(x)) = h(\kappa(x))$ for all $x \in \Sigma^*$.

$(Q, \kappa) \leq^{\mathrm{pwac}} (Q', \kappa')$ means that there is a weak para-AC$^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$.

It is straightforward to verify that para-AC$^0$ is closed under weak para-AC$^0$-reductions.

▶ **Lemma 10.** *Let $(Q, \kappa)$ and $(Q', \kappa')$ be parameterized problems with $(Q, \kappa) \leq^{pwac} (Q', \kappa')$. If $(Q', \kappa') \in$ para-AC$^0$, then $(Q, \kappa) \in$ para-AC$^0$, too.*

It is well known that $p$-Clique is fpt-reducible to $p$-Dominating-Set. The reduction presented in the full version of this paper is a weak para-AC$^0$-reduction. Thus, by Theorem 5 and Lemma 10:

▶ **Proposition 11.** $p$-Dominating-Set $\notin$ para-AC$^0$.

▶ **Corollary 12.** *Let $t, d \geq 1$ with $t + d \geq 3$. Then $p$-WSat$(\Gamma_{t,d}) \notin$ para-AC$^0$.*

**Proof.** For every graph $G = (V, E)$ we define a propositional formula

$$\delta_G := \bigwedge_{\substack{u,v \in V \text{ with} \\ u \neq v \text{ and } \{u,v\} \notin E}} \neg X_u \vee \neg X_v.$$

Clearly, for every $k \in \mathbb{N}$,

$$G \text{ has a } k\text{-clique} \iff \delta_G \text{ has a satisfying assignment of weight } k \tag{1}$$

This gives a weak para-AC$^0$-reduction from $p$-Clique to $p$-WSat$(\Gamma_{1,2})$, or $p$-WSat$(\Gamma_{t,1})$ in case $t \geq 2$. ◀

Similarly, one can show that basic problems like $p$-Subgraph-Isomorphism, $p$-Hom, $p$-Emb, and $p$-MC$(\Sigma_1^1)$ are not in para-AC$^0$ (we use the notations of [12]).

In view of Corollary 12 the reader might wonder about the status of $p$-WSat$(\Gamma_{1,1})$. Using the color-coding technique as in [3], one can show that the problem is in fact solvable in para-AC$^0$. We present a more logic-oriented technique for such proofs. It is based on Proposition 13. It uses FO$(<, +, \times)$ instead of dlogtime-uniform AC$^0$. We defer the proofs of this proposition and of Proposition 14 to the full version of the paper.

For $n \in \mathbb{N}$ denote by $<^{[n]}$ the natural ordering on $[n]$. If $\mathcal{A}$ is any ordered structure, then $(A, <^{\mathcal{A}})$ is isomorphic to $([|A|], <^{[|A|]})$ 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 underlying the addition and the multiplication of $\mathbb{N}$ restricted to $[n]$. That is,

$$+^{[n]} := \{(a, b, c) \mid a, b, c \in [n],\ c = a + b\}, \quad \times^{[n]} := \{(a, b, c) \mid a, b, c \in [n],\ c = a \cdot b\}.$$

Let $\tau$ be a vocabulary which does not contain $<, +, \times$ and set $\tau_{<,+,\times} := \tau \cup \{<, +, \times\}$. We say that a $\tau_{<,+,\times}$-structure $\mathcal{A}$ *has built-in addition and built-in multiplication* if $(A, <^{\mathcal{A}}, +^{\mathcal{A}}, \times^{\mathcal{A}})$ is isomorphic to $([|A|], <^{[|A|]}, +^{[|A|]}, \times^{[|A|]})$. Sometimes we write $\varphi \in$ FO$(<, +, \times)$ to emphasize that $\varphi$ is a first-order formula in a vocabulary containing the symbols $<, +, \times$.

▶ **Proposition 13.** *There is a computable function which associates every $k \in \mathbb{N}$ with a structure $\mathcal{C}(k)$ and every* FO*-formula $\varphi(x)$ with an* FO$(<, +, \times)$*-sentence $\chi_\varphi$ such that for every structure $\mathcal{A}$,*

$$[\mathcal{A} : \mathcal{C}(k)] \models \chi_\varphi \iff \text{there are pairwise distinct } x_1, \ldots, x_k \in A \text{ with } \mathcal{A} \models \varphi(x_i) \text{ for every } i \in [k]. \tag{2}$$

*Here, $[\mathcal{A} : \mathcal{C}(k)] := \mathcal{B} = \big(\mathcal{A} \dot\cup \mathcal{C}(k), U^{\mathcal{B}}, <^{\mathcal{B}}, +^{\mathcal{B}}, \times^{\mathcal{B}}\big)$ is defined as follows.*

- *$\mathcal{A} \dot\cup \mathcal{C}(k)$ is the disjoint union of $\mathcal{A}$ and $\mathcal{C}(k)$ (see the full version of the paper for the definition of the disjoint union of structures).*
- *$U^{\mathcal{B}} := A$ and $<^{\mathcal{B}}$ is an ordering of $B$ and every element of $A$ precedes all elements of $C(k)$. Furthermore $<^{\mathcal{B}}$ extends the ordering $\prec^{\mathcal{C}(k)}$ given in $\mathcal{C}(k)$.*
- *$\mathcal{B}$ has built-in addition and multiplication.*

▶ **Proposition 14.** *$p$-WSat$(\Gamma_{1,1}) \in$ para-AC$^0$.*

## 4 Inapproximability of $p$-Clique by para-AC$^0$

We recall the notion of fpt approximation introduced in [10]. We present the definition for $p$-Clique, the problem which interests us. It can easily be generalized to any maximization problem.

If not stated otherwise, $\rho : \mathbb{N} \to \mathbb{R}_{\geq 1}$ is always a computable function such that the mapping $k \mapsto k/\rho(k)$ is nondecreasing and unbounded.

▶ **Definition 15.** An algorithm $\mathbb{A}$ is a *parameterized approximation for* $p$-Clique *with approximation ratio* $\rho$ if for every graph $G$ and $k \in \mathbb{N}$ with $\omega(G) \geq k$ the algorithm $\mathbb{A}$ computes a clique $C$ of $G$ such that $|C| \geq k/\rho(k)$. Here the clique number $\omega(G)$ is the size of a maximum clique of $G$. If the running time of $\mathbb{A}$ is bounded by $f(k) \cdot |G|^{O(1)}$ where $f : \mathbb{N} \to \mathbb{N}$ is computable, then $\mathbb{A}$ is an *fpt approximation algorithm*.

We tend to believe that $p$-Clique has no fpt approximation algorithm for any ratio $\rho$. Since para-AC$^0$ is a class of decision problems, in order to prove a lower bound it is more convenient to deal with decision algorithms instead of algorithms computing a clique.

▶ **Definition 16** ([10])**.** A decision algorithm $\mathbb{A}$ is a *parameterized cost approximation for* $p$-Clique *with approximation ratio* $\rho$ if for every graph $G$ and $k \in \mathbb{N}$,

- if $k \leq \omega(G)/\rho(\omega(G))$, then $\mathbb{A}$ accepts $(G, k)$;
- if $k > \omega(G)$, then $\mathbb{A}$ rejects $(G, k)$.

In other words, $\mathbb{A}$ decides the *promise* problem:

| $p$-Gap$_\rho$-Clique | |
|---|---|
| *Instance:* | A graph $G$ and $k \in \mathbb{N}$ such that either $k \leq \omega(G)/\rho(\omega(G))$ or $k > \omega(G)$. |
| *Parameter:* | $k$. |
| *Problem:* | Is $k \leq \omega(G)/\rho(\omega(G))$? |

The intuition behind this definition: If $G$ contains a clique far bigger than $k$, detecting a $k$-clique might become easier. It is straightforward to verify that if $p$-Clique has no fpt cost approximation of ratio $\rho$, then it has no fpt approximation of ratio $\rho$ either [10].

▶ **Theorem 17.** $p$-Gap$_\rho$-Clique $\notin$ para-AC$^0$.

Our original proof of this result was based on a generalization of the machinery developed in [20], a generalization we first used to prove that AC$^0$ circuits are not sensitive to planted cliques of a reasonable size, see Theorem 21. The much simpler proof of Theorem 21 we present here is based on Beame's Clique Switching Lemma [5] (see Section 4.1) and was suggested to us anonymously. In the full version of the paper we apply Theorem 21 to derive Theorem 17.

First we prove a consequence of Theorem 17. For $t \geq 0$, $d \geq 1$ we denote by $\Gamma^-_{t,d}$ the subset of subformulas of $\Gamma_{t,d}$ with only negative literals. Clearly, if $\gamma \in \Gamma^-_{t,d}$ has a satisfying assignment of Hamming weight $k$, then it has one of weight $k'$ for every $k' < k$. Denote by $\omega(\gamma)$ the maximum Hamming weight of assignments satisfying $\gamma$. Then $p$-Gap$_\rho$-Wsat$(\Gamma^-_{t,d})$ can be defined similarly as $p$-Gap$_\rho$-Clique.

▶ **Proposition 18.** *Let* $t, d \geq 1$ *with* $t + d \geq 3$. *Then* $p$-Gap$_\rho$-Wsat$(\Gamma^-_{t,d}) \notin$ para-AC$^0$.

**Proof.** Consider the reduction from $p$-Clique to $p$-Gap$_\rho$-Wsat$(\Gamma_{t,d})$ in the proof of Corollary 12. Clearly $\delta_G \in \Gamma^-_{t,d}$ and $\delta_G$ is independent of $k$. Thus, the equivalence (1) preserves the approximation ratio. The result then follows immediately. ◀

## 4.1 Beame's Clique Switching Lemma

Let $n \in \mathbb{N}$. We consider graphs with vertex set $[n]$. To represent functions on those graphs, every potential edge $e \in \binom{[n]}{2}$ is encoded by a boolean variable $X_e$. We set

$$\mathcal{X}_n := \left\{ X_e \;\middle|\; e \in \binom{[n]}{2} \right\}.$$

In particular, $X_e = 1$ means that $e$ is present in the given graph, otherwise $X_e = 0$. Sometimes, it is convenient to understand $e$ as a natural number with $e \in \left[\binom{n}{2}\right]$. Then, $e$ is the $e$th potential edge in an $n$-vertex graph, and $X_e$ is the $e$th variable in $\mathcal{X}_n$.

For every $\ell \in [n]$ and $q \in \mathbb{R}$ with $0 \le q \le 1$ let $\mu \in \mathcal{C}_n^{\ell,q}$ be a *random restriction*, $\mu : \mathcal{X}_n \to \{0, 1, \star\}$ generated as follows:

- Choose $U \in \binom{[n]}{\ell}$ uniformly at random and then set $\mu(X_e) := \star$ for every $e \in \binom{U}{2}$.
- For $e \notin \binom{U}{2}$ we set $\mu(X_e) := 1$ with probability $q$ and $\mu(X_e) := 0$ with probability $1 - q$.

Let $F$ be a boolean function defined on the set of assignments from $\mathcal{X}_n$ to $\{0, 1\}$ and $\mu \in \mathcal{C}_n^{\ell,q}$. The function $F{\restriction_\mu}$ is defined on the set of assignments from $\mu^{-1}(\star)$ to $\{0, 1\}$ by: For $S : \mu^{-1}(\star) \to \{0, 1\}$, we set $F{\restriction_\mu}(S) := F(S \cup \mu)$, where $S \cup \mu : \mathcal{X}_n \to \{0, 1\}$ is the assignment:

$$(S \cup \mu)(X_e) := S(X_e), \text{ if } X_e \in \mu^{-1}(\star) \quad \text{and} \quad (S \cup \mu)(X_e) := \mu(X_e), \text{ otherwise.}$$

Recall that a rooted binary tree is a *decision tree* on some variable set $\mathcal{X} \subseteq \mathcal{X}_n$ if every leaf is labeled either 0 or 1, every internal node is labelled by a variable of $\mathcal{X}$, and the edges between an internal node and its two children are labelled 0 and 1. The *vertex height* of a path $P$ in $T$ is the number of distinct vertices occurring in edges $e$ such that the corresponding $X_e$ appears in $P$. The *vertex height* $|T|_v$ of $T$ is the maximum vertex height of a path in $T$.

For any boolean function $F$ as above, we set

$$\mathrm{DTdepth}_{\mathrm{vertex}}(F) = \min\{|T|_v \mid T \text{ a decision tree computing } F\}.$$

The following lemma is the imbalanced version of [5, Lemma 3] mentioned in the first paragraph of page 12 of that paper. The *vertex length* of a clause is the number of distinct vertices in edges $e$ with $X_e$ appearing in this clause.

▶ **Lemma 19** ([5]). *Let $n, r \in \mathbb{N}$ and $0 \le q \le 1/2$. Moreover, let $F$ be a* DNF*-formula of variable set $\mathcal{X}_n$ with conjunctive clauses of vertex length at most $r$. For $s, \ell \in \mathbb{N}$ with $\ell := pn$, where $s \ge 0$ and $\ell := pn$ with $p \le 1/(r(2/q)^{(r+s)/2})$, we have*

$$\Pr_{\mu \in \mathcal{C}_n^{\ell,q}} \left[ \mathrm{DTdepth}_{\mathrm{vertex}}\big(F{\restriction_\mu}\big) > s \right] < \frac{8\big((2/q)^{(s+r-1)/2} pr\big)^s}{3}.$$

In the full version of the paper we apply Lemma 19 inductively on bounded-depth circuits and show

▶ **Lemma 20.** *Assume*

- *$k : \mathbb{N} \to \mathbb{R}_+$ with $k(n) \le \log_2 n$ for all sufficiently large $n$ and $\lim_{n\to\infty} k(n) = \infty$,*
- *$S, d : \mathbb{N} \to \mathbb{N}$ with $S(n) \ge n$.*

*Define $q : \mathbb{N} \to \mathbb{R}_+$ and $s : \mathbb{N} \to \mathbb{N}$ by*

$$q(n) := n^{-1/k(n)} \quad \text{and} \quad s(n) := \left\lfloor \sqrt{k(n)(\log_n S(n)d(n))} \right\rfloor, \tag{3}$$

*and* $\ell_i : \mathbb{N} \to \mathbb{N}$ *inductively by*

$$\ell_0(n) := n \quad \textit{and} \quad \ell_{i+1}(n) := \left\lfloor \frac{\ell_i(n)}{n^{5s(n)/k(n)}} \right\rfloor. \tag{4}$$

*Then,* $\ell_{d(n)}(n) = n^{1-\Theta\left(5d(n)\sqrt{(\log_n S(n)d(n))/k(n)}\right)}$ *and for every circuit* $\mathsf{C}$ *with variable set* $\mathcal{X}_n$*, size bounded by* $S(n)$*, and depth bounded by* $d(n)$*,*

$$\Pr_{\mu \in \mathcal{C}_n^{\ell_{d(n)}(n),q(n)}} \left[ \mathsf{C}\restriction_\mu \textit{ is constant} \right] = 1 - o(1).$$

## 4.2 A strong AC$^0$ version of the planted clique conjecture

In the standard planted clique problem, we are given a graph $G$ whose edges are generated by starting with a random graph with universe $[n]$ and edge probability $1/2$, then "planting" (adding edges to make) a random clique on $k$ vertices; the problem asks for efficient algorithms finding such a clique of size $k$. The problem was addressed in [17, 18, 2], among many others. It is conjectured that no such algorithm exists. Here, as a consequence of Lemma 20, we prove a statement considerably stronger than the AC$^0$ version of this conjecture.

Let us be more precise. The Erdős-Rényi probability space $\mathrm{ER}(n,p)$, where $n \in \mathbb{N}$ and $0 \leq p \leq 1$, is obtained as follows. We start with the set $[n]$ of vertices. Then we choose every $e \in \binom{[n]}{2}$ as an edge of $G$ with probability $p$, independently of the choices of other edges.

For $G \in \mathrm{ER}(n, 1/2)$ the expected size of a maximum clique is approximately $2 \log\ n$. Therefore $G$ almost surely has no clique of size, say, $4 \log\ n$. For any graph $G$ with vertex set $[n]$ and any $A \subseteq [n]$ we denote by $G + C(A)$ the graph obtained from $G$ by adding edges such that the subgraph induced on $A$ is a clique. For $n, c \in \mathbb{N}$ with $c \in [n]$ and $p \in \mathbb{R}$ with $0 \leq p \leq 1$ we consider a second distribution $\mathrm{ER}(n,p,c)$: Pick a random graph $G \in \mathrm{ER}(n,p)$ and a uniformly random subset $A$ of $[n]$ of size $c$ and plant in $G$ a clique on $A$, thus getting the graph $G + C(A)$. The notation $(G,A) \in \mathrm{ER}(n,p,c)$ should give the information that the random graph was $G$ and that the random subset of $[n]$ of size $c$ was $A$.

▶ **Theorem 21.** *Let* $k : \mathbb{N} \to \mathbb{R}^+$ *with* $\lim_{n\to\infty} k(n) = \infty$*, and* $c : \mathbb{N} \to \mathbb{N}$ *with* $c(n) \leq n^\xi$ *for some* $0 \leq \xi < 1$*. Then for all* AC$^0$ *circuits* $(\mathsf{C}_n)_{n\in\mathbb{N}}$*,*

$$\lim_{n\to\infty} \Pr_{(G,A)\in \mathrm{ER}(n, n^{-1/k(n)},\ c(n))} \left[ \mathsf{C}_n(G) = \mathsf{C}_n(G + C(A)) \right] = 1.$$

**Proof.** We assume that $k(n) \leq \log_2\ n$ for all sufficiently large $n$. The general case can be reduced to it by standard techniques from probability theory.

Let $(\mathsf{C}_n)_{n\in\mathbb{N}}$ be a family of circuits such that for some $\bar{d}, t \in \mathbb{N}$ every $\mathsf{C}_n$ has depth at most $\bar{d}$ and size bounded by $n^t$. In order to apply Lemma 20, we set for $n \in \mathbb{N}$,

$$S(n) = n^t \text{ and } d(n) = \bar{d}. \tag{5}$$

By Lemma 20, it follows that (recall that $q(n) = n^{-1/k(n)}$)

$$\Pr_{\mu \in \mathcal{C}_n^{\ell_{\bar{d}}(n),q(n)}} \left[ \mathsf{C}_n\restriction_\mu \text{ is constant} \right] = 1 - o(1). \tag{6}$$

Furthermore, $\ell_{\bar{d}}(n) = n^{1-\Theta\left(5d(n)\sqrt{(\log_n S(n)d(n))/k(n)}\right)} = n^{1-o(1)}$; the first equality holds by Lemma 20 and the second by (5). The key step consists of the following random process, which generates $(G,A) \in \mathrm{ER}(n, n^{-1/k(n)},\ c(n))$ from $\mu \in \mathcal{C}_n^{\ell_{\bar{d}}(n),q(n)}$.

**(a)** Let $V(G) := [n]$.
**(b)** Add edges $e \in \binom{[n]}{2}$ with $\mu(e) = 1$ to $E(G)$.
**(c)** Recall that $\mu^{-1}(\star) = \binom{U}{2}$, where $U \in \binom{[n]}{\ell_{\bar{d}}(n)}$ was chosen uniformly at random. For every $e \in \binom{U}{2}$, add $e$ to $E(G)$ with probability $q(n)$.
**(d)** Choose $A \in \binom{U}{c(n)}$ uniformly at random. Note that this is possible as $|U| = \ell_{\bar{d}}(n) = n^{1-o(1)} > n^{\xi} \geq c(n)$ for sufficiently large $n$.

By (b)–(d), $G$ and $G + C(A)$ contain the same edges from $\binom{[n]}{2} \setminus \mu^{-1}(\star)$. Thus, by (6), $\mathsf{C}_n(G) = \mathsf{C}_n(G + C(A))$ with high probability. By (c) and (d), $A$ can be viewed as being chosen in $\binom{[n]}{c(n)}$ uniformly at random. ◀

## 5 The complexity of $p$-Halt

We already mentioned in the abstract of this article that the complexity of the parameterized halting problem $p$-Halt is linked to open problems in computational complexity, descriptive complexity, and proof theory [9]. For example, $p$-Halt $\in$ XP is equivalent to the existence of an almost optimal algorithm for the set of tautologies of propositional logic, or to the fact that a certain logic, presented in [16], is a logic for PTIME. Both statements are conjectured to be false. The origin of our interest in para-$\mathrm{AC}^0$ was our hope to get a lower bound on the complexity of $p$-Halt in terms of para-$\mathrm{AC}^0$, that is, to show $p$-Halt $\notin$ para-$\mathrm{AC}^0$. But also this problem remains open. We know that $\mathrm{AC}^0$ corresponds to $\mathrm{FO}(<, +, \times)$, first-order logic with an ordering relation and built-in addition and multiplication. In this section we prove that $p$-Halt $\notin$ para-$\mathrm{FO}(<, +)$, even $p$-Halt $\notin$ $\mathrm{XFO}(<, +)$, hold unconditionally, to our knowledge the best known lower bound for the complexity of $p$-Halt.

Recall that in the paragraph preceding Proposition 13 we defined the natural ordering $<^{[n]}$ on $[n]$ and the ternary relations $+^{[n]}$ and $\times^{[n]}$ of addition and multiplication, respectively, on $[n]$. Now we address the definition of $\mathrm{XFO}(<, +, \times)$. For this purpose we view inputs to parameterized problems as structures.

Any string $x \in \Sigma^*$ with $|x| = n$ can be identified with the $\{<, +, \times, \mathit{One}\}$-structure $\langle x\rangle^{<,+,\times} := ([n], <^{[n]}, +^{[n]}, \times^{[n]}, \mathit{One}^{[n]})$. Here $i \in [n]$ is in $\mathit{One}^{[n]}$, the interpretation of the unary relation symbol $\mathit{One}$, if and only if the $i$th bit of $x$ is a '1'. The structures $\langle x\rangle^{<,+}$ and $\langle x\rangle^{<}$ are reducts of $\langle x\rangle^{<,+,\times}$ over the vocabularies $\{<, +, \mathit{One}\}$ and $\{<, \mathit{One}\}$, respectively.

▶ **Definition 22.** Let $(Q, \kappa)$ be a parameterized problem. Then $(Q, \kappa) \in \mathrm{XFO}(<, +, \times)$ if there is a computable function that assigns to every $k \in \mathbb{N}$ a first-order sentence $\varphi_k$ such that for every instance $x$ of $(Q, \kappa)$ we have $\big(x \in Q \iff \langle x\rangle^{<,+,\times} \models \varphi_{\kappa(x)}\big)$. Analogously, the class $\mathrm{XFO}(<, +)$ is defined.

▶ **Theorem 23.** $p$-Halt $\notin$ $\mathrm{XFO}(<, +)$.

**Proof.** For a contradiction we assume that $p$-Halt $\in$ $\mathrm{XFO}(<, +)$ and show that then the halting problem for Turing machines would be decidable.

Assume that there is a computable function that assigns to every $k \in \mathbb{N}$ a first-order sentence $\varphi_k$ such that $\big((1^n, \mathbb{M}) \in p\text{-Halt} \iff \langle(1^n, \mathbb{M})\rangle^{<,+} \models \varphi_{|\mathbb{M}|}\big)$ for every instance $(1^n, \mathbb{M})$. Fix $\mathbb{M}$. There is a first-order interpretation $I$ that for every $n \in \mathbb{N}$ defines an isomorphic copy of $\langle(1^n, \mathbb{M})\rangle^{<,+}$ in $([n], <^{[n]}, +^{[n]})$: Let $c(n) := |(1^n, \mathbb{M})|$ be the length of the string $(1^n, \mathbb{M})$. We define the interpretation stepwise. As $\mathbb{M}$ is fixed, it is easy to see that we can define in $([n], <^{[n]}, +^{[n]})$ a subset $S$ of $c(n)$ elements of $[n]^s$ for suitable $s$, the universe of the structure defined by the intended interpretation. We order $S$ by the lexicographical

order on $s$-tuples with respect to $<^{[n]}$. Now it is easy to define, using $+^{[n]}$, the corresponding built-in addition.

Then, from $\mathbb{M}$ we can compute $\varphi_{|\mathbb{M}|}$ and $\varphi^I_{|\mathbb{M}|}$ such that $(1^n, \mathbb{M})^{<,+} \models \varphi_{|\mathbb{M}|}$ if and only if $([n], <^{[n]}, +^{[n]}) \models \varphi^I_{|\mathbb{M}|}$, and thus,

$$(1^n, \mathbb{M}) \in p\text{-HALT} \iff \big([n], <^{[n]}, +^{[n]}\big) \models \varphi^I_{|\mathbb{M}|}. \tag{7}$$

By the Ginsburg-Spanier [14] improvement of Presburger's Theorem we know that for $\varphi^I_{|\mathbb{M}|}$ we may compute $n_0, p_0 \in \mathbb{N}$ such that for all $n \geq n_0$ we have $\big([n], <^{[n]}, +^{[n]}\big) \models \varphi^I_{\mathbb{M}}$ if and only if $\big([n+p_0], <^{[n+p_0]}, +^{[n+p_0]}\big) \models \varphi^I_{\mathbb{M}}$. By this equivalence and (7) we see that

$$\mathbb{M} \text{ does not hold on empty input tape} \iff \big([n_0], <^{[n_0]}, +^{[n_0]}\big) \models \neg\varphi^I_{\mathbb{M}}.$$

We can decide the halting problem by checking whether $\big([n_0], <^{[n_0]}, +^{[n_0]}\big) \models \neg\varphi^I_{\mathbb{M}}$. ◀

For the proof it was essential that the function assigning to every $k \in \mathbb{N}$ the FO$(<,+)$-sentence $\varphi_k$ is *computable*. The class obtained if we drop the requirement of computability is called nonuniform-XFO$(<,+)$. We will see that $p$-HALT $\in$ nonuniform-XFO$(<,+)$ by the even stronger statement of part 1 of Proposition 24, a proposition we prove in the full version of the paper.

We note in passing that by standard modeltheoretic techniques one can show that the parameterized vertex cover problem, a fixed-parameter tractable problem, is not in the subclass nonuniform-XFO$(<)$ of nonuniform-XFO$(<,+)$. Thus we get a lower bound for the parameterized complexity of this problem.

We come back to our claim $p$-HALT $\in$ nonuniform-XFO$(<,+)$. We even show $p$-HALT $\in$ nonuniform-para-FO$(<,+)$. By definition, a parameterized probelm $(Q,\kappa)$ belongs to nonuniform-para-FO$(<,+)$ (to para-FO$(<,+)$) if there are a sentence $\varphi \in$ FO$(<,+)$ and a (computable) function $pre : \mathbb{N} \to \Sigma^*$ such that for all $x$,

$$x \in Q \iff \langle (x, pre(\kappa(x))\rangle^{<,+} \models \varphi.$$

So, in the nonuniform version we allow noncomputable precomputations. Note that para-FO$(<,+) \subseteq$ XFO$(<,+)$ as the role of the precomputation $\big($in the definition of para-FO$(<,+)\big)$ can be taken over by the sentences $\varphi_k$ $\big($in the definition of XFO$(<,+)\big)$.

▶ **Proposition 24.** *1.* $p$-HALT $\in$ nonuniform-para-FO$(<,+)$.
*2.* $p$-HALT $\notin$ nonuniform-para-FO$(<)$.

Let $\tau$ be a vocabulary which does not contain the reation symbols $<,+,\times$ and set $\tau_{<,+,\times} := \tau \cup \{<,+,\times\}$. Recall that a $\tau_{<,+,\times}$-structure $\mathcal{A}$ *has built-in addition and built-in multiplication* if $(A, <^{\mathcal{A}}, +^{\mathcal{A}}, \times^{\mathcal{A}})$ is isomorphic to $([|A|], <^{[|A|]}, +^{[|A|]}, \times^{[|A|]})$.

A first-order sentence $\varphi$ of vocabulary $\tau_{<,+,\times}$, shortly $\varphi \in$ FO$(<,+,\times)$, is *invariant* (more precisely, $<$*-invariant*) if for every $\tau$-structure $\mathcal{A}$ and any expansions $(\mathcal{A}, <_1, +_1, \times_1)$ and $(\mathcal{A}, <_2, +_2, \times_2)$ of $\mathcal{A}$ to structures with built-in addition and multiplication, we have:

$$(\mathcal{A}, <_1, +_1, \times_1) \models \varphi \iff (\mathcal{A}, <_2, +_2, \times_2) \models \varphi.$$

It should be clear what we mean if we say that a $\varphi \in$ FO$(<,+)$ or a $\varphi \in$ FO$(<)$ is *invariant*.

Along the lines of [8, Theorem 10] one can show:

▶ **Proposition 25.** *Assume that* $p$-HALT $\in$ XFO$(<,+,\times)$. *Let* $\tau$ *be any vocabulary not containing the symbols* $<$, $+$, *and* $\times$. *Then there is a computable function* $F$ *defined on the class of* FO$(<,+,\times)$*-sentences of vocabulary* $\tau \cup \{<,+,\times\}$ *such that*

- *for every* $\varphi \in \mathrm{FO}(<,+,\times)$ *the sentence* $F(\varphi)$ *is invariant;*
- *if* $\varphi$ *is an invariant* $\mathrm{FO}(<,+,\times)$*-sentence, then* $\varphi$ *and* $F(\varphi)$ *are equivalent.*

*Thus,* $\{F(\varphi) \mid \varphi$ *an invariant* $\mathrm{FO}(<,+,\times)\}$ *is the class of sentences of vocabulary* $\tau$ *of a logic for the invariant fragment of* $\mathrm{FO}(<,+,\times)$.

In view of Theorem 23, we tried, without success, to show that for $\mathrm{FO}(<,+)$ there is no computable function $F$ with the properties mentioned in the preceding result for $\mathrm{FO}(<,+,\times)$, or even to show that there is no effective enumeration of the invariant sentences of $\mathrm{FO}(<,+,\times)$.

## References


1 M. Ajtai. $\Sigma^1_1$ formulae on finite structures. *Annals of Pure and Applied Logic*, 24(3):1–48, 1983.

2 N. Alon, M. Krivelevich, and B. Sudakov. Finding a large hidden clique in a random graph. *Random Struct. Algorithms*, 13(3-4):457–466, 1998.

3 M. Bannach, C. Stockhusen, and T. Tantau. Fast parallel fixed-parameter algorithms via color coding. In *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 P. Beame. *A Switching Lemma Primer*. Technical Report, University of Washington, 1984.

6 P. Beame, R. Impagliazzo, and T. Pitassi. Improved depth lower bounds for small distance connectivity. *Computational Complexity*, 7(4):325–345, 1998.

7 J. Chen, X. Huang, I. A. Kanj, and G. Xia. Linear FPT reductions and computational lower bounds. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing, Chicago, STOC 2004, IL, USA, June 13-16, 2004*, pages 212–221, 2004.

8 Y. Chen and J. Flum. A logic for PTIME and a parameterized halting problem. In *Proceedings of the 24th Annual IEEE Symposium on Logic in Computer Science, LICS 2009, 11-14 August 2009, Los Angeles, CA, USA*, pages 397–406, 2009.

9 Y. Chen and J. Flum. From almost optimal algorithms to logics for complexity classes via listings and a halting problem. *Journal of the ACM*, 59(4):17, 2012.

10 Y. Chen, M. Grohe, and M. Grüber. On parameterized approximability. *Electronic Colloquium on Computational Complexity (ECCC)*, 14(106), 2007.

11 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.

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

13 M. L. Furst, J. B. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17(1):13–27, 1984.

14 S. Ginsburg and E.H. Spanier. Semigroups, Presburger fomulas, and languages. *Pacific Journal of Mathematics*, 16:285–296, 1966.

15 M. Grohe, S. Kreutzer, and S. Siebertz. Deciding first-order properties of nowhere dense graphs. In *Proceedings of the 46th Annual ACM Symposium on the Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 89–98, 2014.

16 Y. Gurevich. Logic and the challenge of computer science. In *Current trends in Theoetical computer Science*, Computer Science Press, pages 1–57, 1988.

17 M. Jerrum. Large cliques elude the metropolis process. *Random Structures and Algorithms*, 3(4):347–360, 1992.

18 L. Kučera. Expected complexity of graph partitioning problems. *Discrete Applied Mathematics*, 57(2-3):193–212, 1995.

**19** A. Nash, J. B. Remmel, and V. Vianu. PTIME queries revisited. In *Database Theory - ICDT 2005, 10th International Conference, Edinburgh, UK, January 5-7, 2005, Proceedings*, volume 3363 of *Lecture Notes in Computer Science*, pages 274–288. Springer, 2005.

**20** 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.