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 cannot 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 $(C_{n,k})_{n,k \in \mathbb{N}}$ of circuits such that for some functions $d, f : \mathbb{N} \rightarrow \mathbb{N}$,
- every $C_{n,k}$ 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 $C_{n,k}(G) = 1$.

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

\[
P\text{-CLIQUE}
\]

\begin{align*}
\text{Instance:} & \quad \text{A graph } G \text{ and } k \in \mathbb{N}. \\
\text{Parameter:} & \quad k. \\
\text{Problem:} & \quad \text{Does } G \text{ contain a clique of size } k?
\end{align*}

cannot be solved in time $f(k) \cdot n^{O(1)}$. Thus, $P\text{-CLIQUE}$ would not be fixed-parameter tractable and hence, $\text{FPT} \neq \text{W}[1]$ since $P\text{-CLIQUE}$ is in the parameterized class $\text{W}[1]$. Therefore, Rossman’s result may be viewed as an $AC^0$ version of $\text{FPT} \neq \text{W}[1]$, 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-AC⁰ as the AC⁰ analog of the class FPT: A problem is in para-AC⁰ if it can be computed by dlogtime-uniform AC⁰-circuits after an (arbitrarily complex) precomputation [12] on the parameter. Later in [3] it was shown that para-AC⁰ 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-AC⁰. 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-AC⁰. It is worth noting that st-connectivity is solvable in polynomial time, and hence, p-stConn ∈ FPT.

The class AC⁰ 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 AC⁰. Since PARITY has a very low complexity, for many other problems, including VERTEX-COVER and CLIQUE, the AC⁰-lower bound can be easily derived by reductions from PARITY. Similarly, as p-CLIQUE ∉ para-AC⁰, 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-AC⁰.

It is well known that the class AC⁰ is intimately connected to first-order logic (FO). In fact, the problems decidable by a dlogtime-uniform AC⁰-family of circuits are precisely those definable in FO(<, +, ×), 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 FO(<, +, ×). 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:

<table>
<thead>
<tr>
<th>p-HALT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance:</strong></td>
</tr>
<tr>
<td><strong>Parameter:</strong></td>
</tr>
<tr>
<td><strong>Problem:</strong></td>
</tr>
</tbody>
</table>

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

- every \( C_{n,k} \) has depth 2 and size \( g(k) \cdot n \) for some function \( g : \mathbb{N} \to \mathbb{N} \),
- an NTM M accepts the empty input tape in at most n steps if and only if \( C_{n,|M|}(n,M) = 1 \) by hard-wiring into \( C_{n,k} \) the NTMs of size k which halt on empty input in ≤ n steps.

Therefore, p-HALT belongs to a nonuniform version of para-AC⁰. The question arises whether p-HALT ∈ para-AC⁰. A positive answer will yield that p-HALT ∈ FPT, which is considered to be highly unlikely [9]. Hence, the goal is to show unconditionally that p-HALT ∉ para-AC⁰. To the best of our knowledge, all existing AC⁰ 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-AC⁰, 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-AC⁰. 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 \(\text{para-AC}^0\) 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 \(\text{para-AC}^0\).

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

We present a model-theoretic tool, based on the color-coding method, which allows to show membership in \(\text{AC}^0\) (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 \(p\)-\text{Clique} is not in \(\text{para-AC}^0\). To get this result we prove that \(\text{AC}^0\)-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 \textit{Clique Switching Lemma} [5].

The fpt-approximation lower bound of \(p\)-\text{Clique} again can be transferred to the weighted satisfiability problems, provided the propositional formulas are of odd depth.

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

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 \([n] := \{1, \ldots, n\}\).

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

Formulas of first-order logic of vocabulary \(\tau\) are built up from atomic formulas \(x = y\) and \(Rx_1 \ldots x_r\), where \(x, y, x_1, \ldots, x_r\) 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

\[
\text{clique}_k := \exists x_1 \ldots \exists x_k \left( \bigwedge_{1 \leq i < j \leq k} (\neg x_i = x_j \land E x_i x_j) \right).
\]
Then a graph $G$ has a $k$-clique if and only if $A(G) \models \text{clique}_k$.

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.

<table>
<thead>
<tr>
<th>$\mathsf{p}$-DOMINATING-SET</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance:</strong> A graph $G$ and $k \in \mathbb{N}$.</td>
</tr>
<tr>
<td><strong>Parameter:</strong> $k$.</td>
</tr>
<tr>
<td><strong>Problem:</strong> Does $G$ contain a dominating set of size $k$?</td>
</tr>
</tbody>
</table>

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 $\mathsf{fpt}$-reductions of the following weighted satisfiability problem for suitable classes $\Gamma$ of propositional formulas.

<table>
<thead>
<tr>
<th>$\mathsf{p}$-WSAT($\Gamma$)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Instance:</strong> $\gamma \in \Gamma$ and $k \in \mathbb{N}$.</td>
</tr>
<tr>
<td><strong>Parameter:</strong> $k$.</td>
</tr>
<tr>
<td><strong>Problem:</strong> Does $\gamma$ have a satisfying assignment of Hamming weight $k$?</td>
</tr>
</tbody>
</table>

**Definition 1.** Let $(Q, \kappa)$ and $(Q', \kappa')$ be two parameterized problems. An $\mathsf{fpt}$-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 $\mathsf{fpt}$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$, then we write $(Q, \kappa) \leq_{\mathsf{fpt}} (Q', \kappa')$.

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.

\[
\Gamma_{t+1,d} := \left\{ \bigwedge_{i \in I} \delta_i \mid \text{I finite and } \delta_i \in \Delta_{t,d} \text{ for all } i \in I \right\},
\]

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

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

\[
W[t] := \bigcup_{d \geq 1} \{(Q, \kappa) \mid (Q, \kappa) \leq_{\mathsf{fpt}} p$-WSAT($\Gamma_{t,d}$)\}.
\]

**Circuit Complexity**

A circuit $C$ with $n$ input gates is a directed acyclic graph in which every node (i.e., gate) is labelled by $\land$, $\lor$, $\neg$, or by one of the variables, or by $0,1$. All $\land$ and $\lor$ gates may have arbitrarily many inputs, i.e., $C$ is of unbounded fan-in. The depth of $C$ is the length of a longest directed path in $C$. The size of $C$, denoted by $|C|$, is the number of gates in $C$. We
often tacitly identify $C$ with the function $C : \{0,1\}^n \to \{0,1\}^m$ it computes. Here, $n$ is the number of variables of $C$ and $m$ the number of its output gates.

$AC^0$ 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 $Q \in AC^0$ if there exists a family of boolean circuits $(C_n)_{n \in \mathbb{N}}$ such that:

- **(A1)** The depth of every $C_n$ is bounded by a fixed constant.
- **(A2)** $|C_n| = n^{O(1)}$.
- **(A3)** Let $x \in \Sigma^*$. Then $(x \in Q \text{ if and only if } C_{|x|}(x) = 1)$. In particular, every $C_n$ has $n$ input gates.
- **(A4)** $(C_n)_{n \in \mathbb{N}}$ is $dlogtime$-uniform, that is: there is a deterministic logtime Turing machine $M$ which on input $1^n$ outputs the circuit $C_n$. More precisely, $M$ 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, $(C_n)_{n \in \mathbb{N}}$ are called $AC^0$-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, $AC^0$ characterizes precisely the class of problems that are definable in $FO(<,+,,\times)$ [4].

### 3 The class para-$AC^0$ and some natural examples

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

- **(P1)** The depth of every $C_{n,k}$ is bounded by a fixed constant.
- **(P2)** $|C_{n,k}| \leq f(k) \cdot n^{O(1)}$ for every $n,k \in \mathbb{N}$, where $f : \mathbb{N} \to \mathbb{N}$ is a computable function.
- **(P3)** Let $x \in \Sigma^*$. Then $(x \in Q \text{ if and only if } C_{|x|,\kappa(x)}(x) = 1)$. (i.e., a precomputation)
- **(P4)** There is a deterministic Turing machine that on input $(1^n, 1^k)$ computes the circuit $C_{n,k}$ 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 $(C_n)_{n \in \mathbb{N}}$ of circuits such that:

- The depth of every $C_n$ is bounded by a fixed constant.
- The size of $C_n$ is $n^{O(k/4)}$.
- Let $G$ be a graph and $n := |V(G)|$. Then $G$ has a $k$-clique if and only if $C_n(G) = 1$. In particular, $p$-$\text{CLIQUE} \notin$ para-$AC^0$.

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

Next, we give two equivalent characterizations of para-$AC^0$ (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-$AC^0$ has an $AC^0$ computable parameterization.

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

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

$$x \in Q \iff C_{|x|,\text{pre}(\kappa(x))}(x, \text{pre}(\kappa(x))) = 1.$$
Some lower bounds in parameterized $\text{AC}^0$

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

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

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

In order to use Theorem 5 to show para-$\text{AC}^0$ 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-$\text{AC}^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$ is a mapping $R : \Sigma^* \to \Sigma^*$ such that:

1. For all $x \in \Sigma^*$ we have $(x \in Q) \iff (R(x) \in Q')$.  
2. There is a family $(C_{n,k})_{n,k \in \mathbb{N}}$ of circuits, whose depth is bounded by a fixed constant, such that:
   1. for all $x \in \Sigma^*$, $C_{|x|, \kappa(x)}(x)$ outputs $R(x)$;
   2. every $C_{n,k}$ outputs $\mathbb{N} \to \mathbb{N}$ such that $f \in \text{AC}^0$ 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 $C_{n,k}$ in time $g(k) + O(\log n)$, where $g : \mathbb{N} \to \mathbb{N}$ is a computable function.

3. 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-$\text{AC}^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$, then we write $(Q, \kappa) \preceq_{\text{fpt}} (Q', \kappa')$.

However, in general para-$\text{AC}^0$ is not closed under para-$\text{AC}^0$-reductions:

**Example 8.** Define $Q := \{(x, b) \mid x \in \{0,1\}^* \text{ and } b = \sum_{i \in \{0\}^{|x|}} x_i \mod 2\}$. Clearly, $Q$ is equivalent to the classical PARITY problem of deciding whether there is an even number of 1’s in $x$. Thus $Q \notin \text{AC}^0$. We define polynomial time computable parameterizations of $Q$ by $\kappa_1(x, b) := 0$ and $\kappa_2(x, b) := \sum_{i \in \{0\}^{|x|}} x_i \mod 2$. Then it is easy to see that $(Q, \kappa_1) \notin \text{para-AC}^0$ and $(Q, \kappa_2) \in \text{para-AC}^0$; yet $(Q, \kappa_1) \preceq_{\text{fpt}} (Q, \kappa_2)$ 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 fpt-reductions. The previous example suggests to require the $\text{AC}^0$-computability of the parameterization (as done in [11]). In fact, para-$\text{AC}^0$ 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-$\text{AC}^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$ is a para-$\text{AC}^0$-reduction which satisfies:

3. There is a computable function $h : \mathbb{N} \to \mathbb{N}$ such that $\kappa'(R(x)) = h(\kappa(x))$ for all $x \in \Sigma^*$. $(Q, \kappa) \preceq_{\text{fpt}} (Q', \kappa')$ means that there is a weak para-$\text{AC}^0$-reduction from $(Q, \kappa)$ to $(Q', \kappa')$.

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

**Lemma 10.** Let $(Q, \kappa)$ and $(Q', \kappa')$ be parameterized problems with $(Q, \kappa) \preceq_{\text{fpt}} (Q', \kappa')$. If $(Q', \kappa') \in \text{para-AC}^0$, then $(Q, \kappa) \in \text{para-AC}^0$, 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-$\text{AC}^0$-reduction. Thus, by Theorem 5 and Lemma 10:

**Proposition 11.** $p$-DOMINATING-SET $\notin$ para-$\text{AC}^0$. 

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

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

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

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

$G$ has a $k$-clique $\iff \delta_G$ has a satisfying assignment of weight $k$ \hspace{1cm} (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 $\text{FO}(\cdot,+,\times)$ 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 $A$ is any ordered structure, then $(A,<^A)$ 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,

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

Let $\tau$ be a vocabulary which does not contain $<,+,\times$ and set $\tau_{<,+\times} := \tau \cup \{<,+,\times\}$. We say that a $\tau_{<,+\times}$-structure $A$ has built-in addition and built-in multiplication if $(A,<^A,+,^A,\times^A)$ is isomorphic to $(|A|,<_{|A|},+^{|A|},\times^{|A|})$. Sometimes we write $\varphi \in \text{FO}(\cdot,+,\times)$ 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 $C(k)$ and every $\text{FO}$-formula $\varphi(x)$ with an $\text{FO}(\cdot,+,\times)$-sentence $\chi_\varphi$ such that for every structure $A$,

$$[A : C(k)] \models \chi_\varphi \iff \text{there are pairwise distinct } x_1,\ldots,x_k \in A \text{ with } A \models \varphi(x_i) \text{ for every } i \in [k].$$ \hspace{1cm} (2)

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

$A \cup C(k)$ is the disjoint union of $A$ and $C(k)$ (see the full version of the paper for the definition of the disjoint union of structures).

$U^B := A$ and $<^B$ is an ordering of $B$ and every element of $A$ precedes all elements of $C(k)$. Furthermore $<^B$ extends the ordering $<_C(k)$ given in $C(k)$.

$B$ has built-in addition and multiplication.

Proposition 14. $p$-WSAT$(\Gamma_{1,1}) \in \text{para-AC}^0$. 
4 Inapproximability of $p$-Clique by para-$AC^0$

We recall the notion of fpt approximation introduced in [10]. We present the definition for $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETH}

Definition 16 ([10]). A decision algorithm $A$ 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 $A$ accepts $(G, k)$;

- if $k > \omega(G)$, then $A$ rejects $(G, k)$.

In other words, $A$ decides the promise problem:

$p$-$\text{Gap}_{\rho}^p$-$\text{Clique}$

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 $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETHEOREM 17. We tend to believe that $p$-CLIQUETH}

Theorem 17. $p$-$\text{Gap}_{\rho}^p$-$\text{Clique} \notin \text{para-AC}^0$.

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 $\Gamma^t_{t,d}$ the subset of subformulas of $\Gamma_{t,d}$ with only negative literals. Clearly, if $\gamma \in \Gamma^t_{t,d}$ 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 $p$-$\text{Gap}_{\rho}^p$-$\text{Wsat}(\Gamma^t_{t,d})$ can be defined similarly as $p$-$\text{Gap}_{\rho}^p$-$\text{Clique}$.

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

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

\end{document}
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

\[
X_n := \left\{ X_e \mid e \in \binom{[n]}{2} \right\}.
\]

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 \( e \in \binom{[n]}{2} \). Then, \( e \) is the \( e \)th potential edge in an \( n \)-vertex graph, and \( X_e \) is the \( e \)th variable in \( X_n \).

For every \( \ell \in [n] \) and \( q \in \mathbb{R} \) with \( 0 \leq q \leq 1 \) let \( \mu \in \mathcal{E}_{n}^{q} \) be a random restriction, \( \mu : X_n \to \{0, 1, \ast\} \) generated as follows:

- Choose \( U \in \binom{[n]}{\ell} \) uniformly at random and then set \( \mu(X_e) := \ast \) for every \( e \in \binom{U}{2} \).
- For \( e \not\in \binom{U}{2} \) 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 \( X_n \) to \([0, 1]\) and \( \mu \in \mathcal{E}_{n}^{q} \). The function \( F|_{\mu} \) is defined on the set of assignments from \( \mu^{-1}(\ast) \) to \([0, 1]\) by:

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

Recall that a rooted binary tree is a decision tree on some variable set \( \mathcal{X} \subseteq X_n \) if every leaf is labeled either 0 or 1, every internal node is labeled 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

\[
\text{DTdepth}_{\text{vertex}}(F) = \min\{|T|_{v} \mid T \text{ a decision tree computing } F\}.
\]

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 \( 0 \leq q \leq 1/2 \). Moreover, let \( F \) be a DNF-formula of variable set \( X_n \) with conjunctive clauses of vertex length at most \( r \). For \( s, \ell \in \mathbb{N} \) with \( \ell := pn \), where \( s \geq 0 \) and \( \ell := pn \) with \( p \leq 1/(r(2/q)^{(r+s)/2}) \), we have

\[
\Pr_{\mu \in \mathcal{E}_{n}^{q}} \left[ \text{DTdepth}_{\text{vertex}}(F|_{\mu}) > s \right] < \frac{8((2/q)^{(s+r-1)/2}pr)^s}{3}.
\]

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 \( k(n) \leq \log_2 n \) for all sufficiently large \( n \) and \( \lim_{n \to \infty} k(n) = \infty \),
- \( S, d : \mathbb{N} \to \mathbb{N} \) with \( S(n) \geq n \).

Define \( q : \mathbb{N} \to \mathbb{R}^{+} \) and \( s : \mathbb{N} \to \mathbb{N} \) by

\[
q(n) := n^{-1/k(n)} \quad \text{and} \quad s(n) := \left\lfloor \sqrt{k(n)(\log S(n)d(n))} \right\rfloor,
\]

(3)
and \( \ell_i : \mathbb{N} \rightarrow \mathbb{N} \) inductively by \[
\ell_0(n) := n \quad \text{and} \quad \ell_{i+1}(n) := \left\lfloor \frac{\ell_i(n)}{n^{5\ell(n)/k(n)}} \right\rfloor.
\tag{4}
\]

Then, \( \ell_d(n) = n^{1-\Theta\left(5d(n)\sqrt{\log n S(n)/d(n)}\right)} \) and for every circuit \( C \) with variable set \( X_n \), size bounded by \( S(n) \), and depth bounded by \( d(n) \), \[
\Pr_{\mu \in \mathcal{C}_n^{d(n), q(n)}}[C_{\mu} \text{ is constant}] = 1 - o(1).
\]

### 4.2 A strong \( \text{AC}^0 \) 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 \( \text{AC}^0 \) version of this conjecture.

Let us be more precise. The Erdős-Rényi probability space \( \text{ER}(n, p) \), 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 edge \( e \in \binom{[n]}{2} \) as an edge of \( G \) with probability \( p \), independently of the choices of other edges.

For \( G \in \text{ER}(n, 1/2) \) 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 \( \text{ER}(n, p, c) \): Pick a random graph \( G \in \text{ER}(n, p) \) 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 \( (G, A) \in \text{ER}(n, p, c) \) 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 \( k : \mathbb{N} \rightarrow \mathbb{R}^+ \) with \( \lim_{n \rightarrow \infty} k(n) = \infty \), and \( c : \mathbb{N} \rightarrow \mathbb{N} \) with \( c(n) \leq n^\xi \) for some \( 0 \leq \xi < 1 \). Then for all \( \text{AC}^0 \) circuits \( (C_n)_{n \in \mathbb{N}} \),
\[
\lim_{n \rightarrow \infty} \Pr_{(G, A) \in \text{ER}(n, n^{-1/k(n)}, c(n))} [C_n(G) = C_n(G + C(A))] = 1.
\]

**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 \( (C_n)_{n \in \mathbb{N}} \) be a family of circuits such that for some \( \bar{d}, \bar{t} \in \mathbb{N} \) every \( C_n \) has depth at most \( \bar{d} \) and size bounded by \( n^\bar{t} \). In order to apply Lemma 20, we set for \( n \in \mathbb{N} \),
\[
S(n) = n^\ell \quad \text{and} \quad d(n) = \bar{d}.
\tag{5}
\]

By Lemma 20, it follows that (recall that \( q(n) = n^{-1/k(n)} \))
\[
\Pr_{\mu \in \mathcal{C}_n^{d(n), q(n)}}[C_n|_{\mu} \text{ is constant}] = 1 - o(1).
\tag{6}
\]

Furthermore, \( \ell_d(n) = n^{1-\Theta\left(5d(n)\sqrt{\log n S(n)/d(n)}\right)} = n^{1-o(1)} \); the first equality holds by Lemma 20 and the second by (5). The key step consists of the following random process, which generates \( (G, A) \in \text{ER}(n, n^{-1/k(n)}, c(n)) \) from \( \mu \in \mathcal{C}_n^{d(n), q(n)} \).
We already mentioned in the abstract of this article that the complexity of the parameterized problems as structures.

Recall that in the paragraph preceding Proposition 13 we defined the natural ordering $<_n$ on $[n]$. Any string $x \in \Sigma^*$ with $|x| = n$ can be identified with the $\{<,+,\times, One\}$-structure $\langle x \rangle <,+,\times := ([n], <_n, +_n, \times_n, One_n)$. Here $i \in [n]$ is in $One_n$, the interpretation of the unary relation symbol $One$, if and only if the $i$th bit of $x$ is a ‘1’. The structures $\langle x \rangle ^<,+,\times$ and $\langle x \rangle ^<$ are reducts of $\langle x \rangle ^<,+,\times$ over the vocabularies $\{<,+,One\}$ and $\{<,One\}$, respectively.

Definition 22. Let $(Q, \kappa)$ be a parameterized problem. Then $(Q, \kappa) \in \text{XFO}(<,+)$ 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 $(x \in Q \iff \langle x \rangle ^<,+,\times \models \varphi_{\kappa(x)})$. Analogously, the class $\text{XFO}(<,+)$ is defined.

Theorem 23. $p\text{-HALT} \notin \text{XFO}(<,+)$.

Proof. For a contradiction we assume that $p\text{-HALT} \in \text{XFO}(<,+)$ 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 $((1^n, M) \in p\text{-HALT} \iff \langle (1^n, M) \rangle ^<,+,\times \models \varphi_{|M|})$ for every instance $(1^n, M)$. Fix $M$. There is a first-order interpretation $I$ that for every $n \in \mathbb{N}$ defines an isomorphic copy of $\langle (1^n, M) \rangle ^<,+,\times$. Let $c(n)$ := $[1^n, M]$ be the length of the string $[1^n, M]$. We define the interpretation stepwise. As $M$ 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
Some lower bounds in parameterized \(\text{AC}^0\)

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

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

\[
(1^n, M) \in p\text{-HALT} \iff ([n], <^{[n]}, +^{[n]}) \models \varphi_{[M]}^f.
\]

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

\[
\text{M does not hold on empty input tape} \iff ([n_0], <^{[n_0]}, +^{[n_0]}) \models \neg \varphi_{[M]}^f.
\]

We can decide the halting problem by checking whether \(([n_0], <^{[n_0]}, +^{[n_0]}) \models \neg \varphi_{[M]}^f\).

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-\(\text{XFO}(<,+)>\). We will see that \(p\text{-HALT} \in \text{nonuniform-\(\text{XFO}(<,+>\)}\) 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-\(\text{XFO}(<>)\) of nonuniform-\(\text{XFO}(<,+>)\). Thus we get a lower bound for the parameterized complexity of this problem.

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

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

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

\[\text{Proposition 24.}\]

1. \(p\text{-HALT} \in \text{nonuniform-para-\(\text{FO}(<,+>)\)}\).
2. \(p\text{-HALT} \not\in \text{nonuniform-para-\(\text{FO}(<>)\)}\).

Let \(\tau\) be a vocabulary which does not contain the relation 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 \((\mathcal{A}, <^{\mathcal{A}}, +^{\mathcal{A}}, \times^{\mathcal{A}})\) is isomorphic to \((\langle [\mathcal{A}] \rangle, <^{[\mathcal{A}]}, +^{[\mathcal{A}]}, \times^{[\mathcal{A}]}\rangle\).

A first-order sentence \(\varphi\) of vocabulary \(\tau_{<,+,,\times}\), written \(\varphi \in \text{FO}(<,+,,\times)\), is **invariant** (more precisely, \(<\text{-invariant}\)) if for every \(\tau\)-structure \(\mathcal{A}\) and any expansions \((\mathcal{A}, <_{1,1}, +_{1,1}, \times_1)\) and \((\mathcal{A}, <_{2,2}, +_{2,2}, \times_2)\) of \(\mathcal{A}\) to structures with built-in addition and multiplication, we have:

\[
(\mathcal{A}, <_{1,1}, +_{1,1}, \times_1) \models \varphi \iff (\mathcal{A}, <_{2,2}, +_{2,2}, \times_2) \models \varphi.
\]

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

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

\[\text{Proposition 25.}\]

Assume that \(p\text{-HALT} \in \text{XFO}(<,+,,\times)\). Let \(\tau\) be any vocabulary not containing the symbols \(<,+,,\times\). Then there is a computable function \(F\) defined on the class of \(\text{FO}(<,+,,\times)\)-sentences of vocabulary \(\tau \cup \{<,+,,\times\}\) such that
for every $\varphi \in \text{FO}(\prec, +, \times)$ the sentence $F(\varphi)$ is invariant;
if $\varphi$ is an invariant FO$(\prec, +, \times)$-sentence, then $\varphi$ and $F(\varphi)$ are equivalent.
Thus, $\{ F(\varphi) \mid \varphi \text{ an invariant FO}(\prec, +, \times) \}$ is the class of sentences of vocabulary $\tau$ of a logic for the invariant fragment of FO$(\prec, +, \times)$.

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

References

Some lower bounds in parameterized AC$^0$
