

Parameterized AC^0 – Some upper and lower bounds

Yijia Chen
Fudan University

September 19th, 2017 @ Shonan

A family of Boolean circuits $(C_n)_{n \in \mathbb{N}}$ are AC^0 -circuits if for every $n \in \mathbb{N}$

- (i) C_n computes a Boolean function from $\{0, 1\}^n$ to $\{0, 1\}$;
- (ii) the depth of C_n is bounded by a fixed constant;
- (iii) the size of C_n is polynomially bounded in n .

Remark

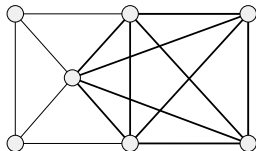
1. Without (ii), we get a family of polynomial-size circuits $(C_n)_{n \in \mathbb{N}}$, which decides a language in $P/poly$.
2. If C_n is computable by a TM in time $O(\log n)$, then $(C_n)_{n \in \mathbb{N}}$ is **dlogtime-uniform**, which corresponds to $FO(<, +, \times)$ [Barrington, Immerman, and Straubing, 1990].

The k -clique problem

Definition

Let G be a graph and $k \in \mathbb{N}$. Then a subset $C \subseteq V(G)$ is a k -clique if

- (i) for every two vertices $u, v \in V(G)$ either $u = v$ or $\{u, v\} \in E(G)$,
- (ii) and $|C| = k$.



A graph with a 5-clique.

k -clique by AC^0

Let $n \in \mathbb{N}$ and we encode a graph G with $V(G) = [n]$ as follows. For every $1 \leq i < j \leq n$ the **Boolean variable** $X_{\{i,j\}}$ is defined by

$$X_{\{i,j\}} = \begin{cases} 1 & \text{if there is an edge between } i \text{ and } j \\ 0 & \text{otherwise.} \end{cases}$$

Then the k -clique problem can be computed by circuits

$$C_{\binom{n}{2}} = \bigvee_{K \in \binom{[n]}{k}} \bigwedge_{\{i,j\} \in \binom{K}{2}} X_{\{i,j\}}.$$

- (i) $C_{\binom{n}{2}} : \{0, 1\}^{\binom{n}{2}} \rightarrow \{0, 1\}$.
- (ii) The depth of $C_{\binom{n}{2}}$ is 2.
- (iii) $C_{\binom{n}{2}}$ has size $n^{k+O(1)}$.

Rossman's Theorem

Theorem (Rossman, 2008)

Let $k \in \mathbb{N}$. There are no AC^0 -circuits $\left(C_{\binom{n}{2}}\right)_{n \in \mathbb{N}}$ of size $O(n^{k/4})$ such that for every n -vertex graph G

$$G \text{ has a } k\text{-clique} \iff C_{\binom{n}{2}}(G) = 1.$$

A uniform version

Corollary

There are no circuits $\left(C_{\binom{n}{2}, k} \right)_{n, k \in \mathbb{N}}$ which satisfy the following conditions.

- (i) The size of $C_{\binom{n}{2}, k}$ is bounded by $f(k) \cdot n^{k/4}$.
- (ii) The depth of $C_{\binom{n}{2}, k}$ is bounded by $g(k)$.
- (iii) Let G be an n -vertex graph G and $k \in \mathbb{N}$. Then

$$G \text{ has a } k\text{-clique} \iff C_{\binom{n}{2}}(G) = 1.$$

Remark

1. It is about the circuit complexity of the *parameterized clique problem*.
2. If true without (ii), then the parameterized clique problem is not fixed-parameter tractable. Thus it is an AC^0 version of $FPT \neq W[1]$.

Outline

1. Parameterized AC^0
2. Some lower bounds
 - ▶ for fpt-approximation of the clique problem.
3. Some upper bounds:
 - ▶ a descriptive characterizations of parameterized AC^0 ,
 - ▶ the color coding technique in parameterized AC^0 .

Parameterized AC^0

Parameterized problems

Definition

A **parameterized problem** (Q, κ) consists of a classical problem $Q \subseteq \Sigma^*$ and a function $\kappa : \Sigma^* \rightarrow \mathbb{N}$, the **parameterization**, computable in polynomial time.

Example

p -CLIQUE

Input: A graph G and $k \in \mathbb{N}$.
Parameter: k .
Problem: Does G contain a clique of size k ?

p -DOMINATING-SET

Input: A graph G and $k \in \mathbb{N}$.
Parameter: k .
Problem: Does G contain a dominating set of size k ?

Parameterized AC^0

Definition (Bannach, Stockhusen, and Tantau, 2015)

A parameterized problem (Q, κ) is in **para- AC^0** if there exists a family $(C_{n,k})_{n,k \in \mathbb{N}}$ of circuits such that:

1. The depth of every $C_{n,k}$ is bounded by a fixed constant.
2. $|C_{n,k}| \leq f(k) \cdot n^{O(1)}$ for every $n, k \in \mathbb{N}$.
3. Let $x \in \Sigma^*$. Then $(x \in Q \text{ if and only if } C_{|x|, \kappa(x)}(x) = 1)$.
4. There is a TM that on input $(1^n, 1^k)$ computes the circuit $C_{n,k}$ in time $g(k) + O(\log n)$.

Both $f, g : \mathbb{N} \rightarrow \mathbb{N}$ are computable functions.

Some equivalent characterizations

Proposition

Let (Q, κ) be a parameterized problem with κ computable by AC^0 -circuits. Then all the following are equivalent.

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

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

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

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

Some Lower Bounds

Theorem (Rossman, 2008)

p -CLIQUE \notin para-AC⁰.

By appropriate reductions, i.e., para-AC⁰-reductions:

Corollary

1. p -DOMINATING-SET \notin para-AC⁰, an AC⁰ version of FPT \neq W[2].
2. p -WSAT($\Gamma_{t,d}$) \notin para-AC⁰ for $t + d \geq 3$, an AC⁰ version of FPT \neq W[t].

Inapproximability of p -CLIQUE by para-AC⁰

A major open problem in parameterized complexity

Can we approximate p -CLIQUE in fpt time?

Approximation of p -CLIQUE

Let $\rho : \mathbb{N} \rightarrow \mathbb{R}_{\geq 1}$ be a computable function with nondecreasing and unbounded $k \mapsto k/\rho(k)$.

Definition

An algorithm \mathbb{A} is a **parameterized approximation for p -CLIQUE with approximation ratio ρ** 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 $|C| \geq k/\rho(k)$.

$\omega(G)$ is the size of a maximum clique of G .

Conjecture

p -CLIQUE *has no parameterized approximation for any ρ .*

Theorem (Chalermsook, Cygany, Kortsarz, Laekhanukit, Manurangsi, Nanongkai, and Trevisan, 2017)

*Under the **gap Exponential Time Hypothesis**, p -CLIQUE has no parameterized approximation for any ρ .*

Remark

*The gap Exponential Time Hypothesis might require the construction of **linear PCP**, which seems to be out of reach at this point.*

Approximation in para-AC^0

$p\text{-GAP}_\rho\text{-CLIQUE}$

Input: 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 $k \leq \omega(G)/\rho(\omega(G))$?

Lemma

If $p\text{-GAP}_\rho\text{-CLIQUE} \notin \text{FPT}$, then $p\text{-CLIQUE}$ has no parameterized approximation with ratio ρ .

Theorem (C. and Flum, 2016)

$p\text{-GAP}_\rho\text{-CLIQUE} \notin \text{para-AC}^0$ for any ρ .

The proof is based on an AC^0 version of the **planted clique conjecture** with respect to Erdős-Rényi random graphs.

Erdős-Rényi random graphs

Definition

Let $n \in \mathbb{N}$ and $p \in \mathbb{R}$ with $0 \leq p \leq 1$. Then $G \in \text{ER}(n, p)$ is the Erdős-Rényi random graph on vertex set $[n]$ constructed by adding every edge $e \in \binom{[n]}{2}$ independently with probability p .

Example

$\text{ER}(n, 1/2)$ is the **uniform distribution** on graphs with vertex set $[n]$.

Let $G \in \text{ER}(n, 1/2)$. Then the expected $\omega(G)$ is approximately $2 \cdot \log n$.

Erdős-Rényi random graphs with a planted clique

Definition

Let $n \in \mathbb{N}$ and $p \in \mathbb{R}$ with $0 \leq p \leq 1$. Moreover let $c \in [n]$. Then $(G + A) \in \text{ER}(n, p, c)$ is the distribution:

1. Pick $G \in \text{ER}(n, p)$.
2. Pick a uniformly random subset $A \subseteq [n]$ with $|A| = c$.
3. Plant in G a clique $C(A)$ on A , thus getting the graph $G + C(A)$.

Example

With high probability, the maximum clique in $G + C(A)$ with

$$(G + A) \in \text{ER}(n, 1/2, 4 \cdot \log n)$$

is the clique $C(A)$.

The planted clique conjecture

Conjecture (Jerrum, 1992; Kucera, 1995)

For every polynomial time algorithm \mathbb{A} and for all sufficiently large $n \in \mathbb{N}$

$$\Pr_{(G+A) \in \text{ER}(n, 1/2, 4 \cdot \log n)} \left[\mathbb{A}(G + C(A)) \neq A \right] > \frac{1}{2}.$$

That is, \mathbb{A} fails to find the planted clique with high probability.

An AC^0 version of the planted clique conjecture

Theorem (C. and Flum, 2016)

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 AC^0 -circuits $(C_n)_{n \in \mathbb{N}}$,

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

Let $(G, A) \in \text{ER}(n, n^{-1/k(n)}, c(n))$, then

$$\frac{\omega(G + C(A))}{\omega(G)}$$

can be arbitrarily large. Hence

Theorem (C. and Flum, 2016)

$p\text{-GAP}_\rho\text{-CLIQUE} \notin \text{para-}AC^0$.

Inapproximability of p -DOMINATING-SET by para-AC^0

Theorem (C. and Lin, 2017)

p -GAP $_{\rho}$ -DOMINATING-SET $\notin \text{para-AC}^0$ for

$$\rho(k) = \frac{\log k}{\omega(\log \log k)}.$$

$\text{FPT} \setminus \text{para-AC}^0 \neq \emptyset$

$p\text{-STCONN}$

Input: A graph G , $s, t \in V(G)$, and $k \in \mathbb{N}$.

Parameter: k .

Problem: Does G contain a path from s to t of length $\leq k$?

Theorem (Beame, Impagliazzo, and Pitassi, 1995)

$p\text{-STCONN}$ is not in parameterized AC^0 , *even on graphs of degree at most 2.*

Some Upper Bounds

p-VERTEX-COVER

Input: A graph G and $k \in \mathbb{N}$.

Parameter: k .

Problem: Does G contain a vertex cover of size k ?

Theorem (Bannach, Stockhusen, and Tantau, 2015)

p-VERTEX-COVER is in parameterized AC^0 .

Remark

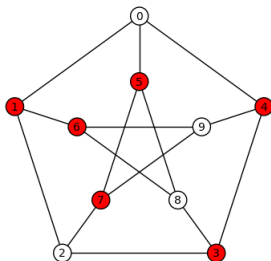
The proof of Bannach et al. is direct by circuits, which can be rephrased in first-order logic by a *descriptive characterization* of para- AC^0 .

The k -vertex-cover problem

Definition

Let G be a graph and $k \in \mathbb{N}$. Then a subset $C \subseteq V(G)$ is a k -vertex-cover if

- (i) for every edge $\{u, v\} \in E(G)$ either $u \in C$ or $v \in C$,
- (ii) and $|C| = k$.



The peterson graph with a 6-vertex-cover.

k -vertex-cover by FO

G has a k -vertex-cover $\iff G \models \psi_k$

where $\psi_k = \exists x_1 \cdots \exists x_k \left(\bigwedge_{1 \leq i < j \leq k} x_i \neq x_j \right.$

$\left. \wedge \forall u \forall v (Euv \rightarrow \bigvee_{i \in [k]} (u = x_i \vee v = x_i)) \right)$.

Can we do better?

Better in what sense?

The **quantifier rank** of

$$\psi_k = \exists x_1 \cdots \exists x_k \left(\bigwedge_{1 \leq i < j \leq k} x_i \neq x_j \right. \\ \left. \wedge \forall u \forall v (Eu v \rightarrow \bigvee_{i \in [k]} (u = x_i \vee v = x_i)) \right)$$

is $\text{qr}(\psi_k) = k + 2$.

There is an algorithm which checks whether

$$\mathcal{A} \models \varphi$$

in time $O(|\varphi| \cdot \|\mathcal{A}\|^{\text{qr}(\varphi)})$.

Definition

Let $q \in \mathbb{N}$. Then FO_q is the fragment of FO consisting of all formulas of quantifier rank at most q .

By simple Ehrenfeucht-Fraïssé games

Theorem

There is no $\varphi \in \text{FO}_{k-1}$ such that for every graph G

$$G \text{ has a } k\text{-vertex cover} \iff G \models \varphi.$$

With arithmetics

Theorem (C. , Flum, and Huang, 2017)

For every $k \in \mathbb{N}$ there is a $\psi_k \in \text{FO}_{17}$ such that for every graph G

$$G \text{ has a } k\text{-vertex cover} \iff (G, <, +, \times, \mathbf{0}, \dots, \mathbf{k}') \models \psi_k.$$

Moreover, the mapping is

$$k \mapsto \psi_k$$

is computable (hence, so is $k \mapsto k'$).

The slicewise definability of the vertex cover problem

Theorem

p -VERTEX-COVER is *slicewise definable* in FO_{17} . That is, for every $k \in \mathbb{N}$, the k th slice of VERTEX-COVER i.e., the k -vertex-cover problem, is definable by some $\psi_k \in \text{FO}_{17}$.

Moreover, $k \mapsto \psi_k$ is computable.

The descriptive characterization of para-AC^0

Theorem (C. , Flum, and Huang, 2017)

Let (Q, κ) be a parameterized problem. Then (Q, κ) is slicewise definable in FO_q for some $q \in \mathbb{N}$ if and only if $(Q, \kappa) \in \text{para-AC}^0$.

The main theorem

Theorem

p -VERTEX-COVER is *slicewise definable* in FO_{17} .

The proof strategy

1. There is a polynomial time algorithm \mathbb{K} which for every graph G and $k \in \mathbb{N}$ computes a graph G' and k' such that
 - 1.1 G has k -vertex-cover if and only if G' has a k' -vertex-cover.
 - 1.2 $|V(G')| \leq k^2 + k$ and $k' \leq k$.

\mathbb{K} is known as **Buss' kernelization** of VERTEX-COVER.

2. We show that \mathbb{K} can be implemented in FO_{17} .
3. Any class of graphs with at most $k^2 + k$ vertices can be defined in FO_0 with the constants $0, \dots, k^2 + k$.

Buss' kernelization

1. If v is a vertex of degree at least $k + 1$, then v must be in every k -vertex cover. Thus we can remove all such v and decrease k accordingly.
2. Remove all isolated vertices.
3. Let G' and k' be the resulting instance. If

$$|V(G')| > k^2 + k \geq k'(k + 1),$$

then G' , and hence also G , is a no instance.

Implementing Buss' kernelization in FO_{17} ?

The main difficulty is how to count in FO_{17} , e.g. how to identify a vertex v with degree at least $k + 1$.

$$\exists x_1 \cdots \exists x_{k+1} \left(\bigwedge_{1 \leq i < j \leq k+1} x_i \neq x_j \wedge \bigwedge_{i \in [k]} E v x_i \right)$$

would not work.

Color coding

Lemma (Alon, Yuster, and Zwick, 1995)

For every sufficiently large $n \in \mathbb{N}$, it holds that for all $k \leq n$ and for every k -element subset X of $[n]$, there exists a prime $p < k^2 \cdot \log_2 n$ and $q < p$ such that the function $h_{p,q} : [n] \rightarrow \{0, \dots, k^2 - 1\}$ given by

$$h_{p,q}(m) := (q \cdot m \bmod p) \bmod k^2$$

is injective on X .

Color coding in FO_q

Corollary

Let $k \in \mathbb{N}$ and $\varphi(\bar{x}, y)$ be an FO-formula. Then there exists an FO-formula $\chi_{\varphi, k}(\bar{x})$ of the form

$$\rho \vee \exists p \exists q \left(\bigvee_{0 \leq i_1 < \dots < i_k < k^2} \bigwedge_{j \in [k]} \exists y ("h_{p,q}(y) = i_j" \wedge \varphi(\bar{x}, y)) \right),$$

such that

1. for every graph G and $\bar{u} \in V(G)^{|\bar{x}|}$ there are k vertices v in G satisfying $\varphi(\bar{u}, v)$ if and only if

$$(G, <, +, \times, \mathbf{0}, \dots, \mathbf{k}^3) \models \chi_{\varphi, k}(\bar{u}),$$

2. and $\text{qr}(\chi_{\varphi, k}) = \max \{12, \text{qr}(\varphi) + 3\}$.

Degree constraints by color coding

Let

$$\varphi(x, y) = E_{xy}.$$

Then for every $k \in \mathbb{N}$, every graph G and $v \in V(G)$

$$(G, <, +, \times, \mathbf{0}, \dots, \mathbf{k}^3) \models \chi_{\varphi, k}(v) \iff \text{the degree of } v \text{ in } G \text{ is at least } k.$$

Moreover, $\text{qr}(\chi_{\varphi, k}) = 12$.

Recall Buss' kernelization

1. If v is a vertex of degree $\geq k + 1$, then v must be in every k -vertex cover. Thus we can remove all such v and decrease k accordingly.
2. Remove all isolated vertices.
3. Let G' and k' be the resulting instance. If $|V(G')| > k^2 + k \geq k'(k + 1)$, then G' , and hence also G , is a no instance.

Corollary

For every $k \in \mathbb{N}$ and $k' \leq k$ there are

$$\varphi_{\text{vertex}}(x), \varphi_{\text{edge}}(x, y), \varphi_{\text{kernel}} \in \text{FO}_{17},$$

such that for every graph G if we define G' with

$$V(G') := \{v \in V(G) \mid G \models \varphi_{\text{vertex}}(v)\},$$

$$E(G') := \{\{u, v\} \mid u, v \in V(G'), u \neq v, \text{ and } G \models \varphi_{\text{edge}}(u, v)\},$$

then

G has a k -vertex-cover

$$\iff (G, <, +, \times, \mathbf{0}, \dots) \models \varphi_{\text{kernel}} \text{ and } G' \text{ has a } k'\text{-vertex-cover.}$$

Moreover, $|V(G')| \leq k^2 + k$ if $(G, <, +, \times, \mathbf{0}, \dots) \models \varphi_{\text{kernel}}$.

The final step

Lemma

Let H be a graph with $|V(H)| = k$. Then there is an FO_0 -sentence φ_H such that for every graph G

$$G \text{ and } H \text{ are isomorphic} \iff (G, \mathbf{0}, \dots, \mathbf{k}) \models \varphi_H.$$

Corollary

Let K be a *finite* class of graphs closed under isomorphisms. Then there is an FO_0 -sentence φ_K such that for every graph G

$$G \in K \iff (G, \mathbf{0}, \dots) \models \varphi_K.$$

Recall:

Corollary

For every $k \in \mathbb{N}$ and $k' \leq k$ there are $\varphi_{\text{vertex}}(x), \varphi_{\text{edge}}(x, y), \varphi_{\text{kernel}} \in \text{FO}_{17}$, such that for every graph G if we define G' with

$$\begin{aligned} V(G') &:= \{v \in V(G) \mid G \models \varphi_{\text{vertex}}(v)\}, \\ E(G') &:= \{\{u, v\} \mid u, v \in V(G'), u \neq v, \text{ and } G \models \varphi_{\text{edge}}(u, v)\}, \end{aligned}$$

then

G has a k -vertex-cover $\iff G \models \varphi_{\text{kernel}}$ and G' has a k' -vertex-cover

Moreover, $|V(G')| \leq k^2 + k$ if $G \models \varphi_{\text{kernel}}$.

But how to define $0, 1, \dots$ of G' in G ?

Final step by color-coding

What we really need to define a finite graph is to say, e.g.,

there is an edge between the first and the twelfth vertices.

So if we know the subgraph G' of G constructed by Buss' kernelization, and its size ℓ , then for some p and q , and $0 \leq i_1 < \dots < i_\ell < \ell^2$ we have

$$h_{p,q}(V(G')) = \{i_1, \dots, i_\ell\}.$$

Thus we can say, the first, the second, \dots , vertices in G' in FO_{17} .

Hitting set problems with bounded hyperedge size

d -HITTING-SET

Input: A hypergraph H in which every hyperedge has size at most d and $k \in \mathbb{N}$.

Problem: Does G contain a vertex set of size at most k such that it intersects every hyperedge?

Theorem

Let $d \in \mathbb{N}$. Then d -HITTING-SET is slicewise definable in FO_q with $q = O(d^2)$.

What makes vertex-cover/ d -hitting-set slicewise definable?

Let X be a **set variable**. Then p -VERTEX-COVER is **Fagin-defined** by

$$\varphi(X) := \forall x \forall y (\neg E_{xy} \vee Xx \vee Xy).$$

More precisely, for every graph G and $S \subseteq V(G)$

$$S \text{ is a vertex cover of } G \iff G \models \varphi(S).$$

p -CLIQUE is Fagin-defined by

$$\forall x \forall y (x = y \vee E_{xy} \vee \neg Xx \vee \neg Xy).$$

It is not slicewise definable in any FO_q [Rossman, 2008].

p -DOMINATING-SET is Fagin-defined by

$$\forall x \exists y (Xy \wedge (x = y \vee E_{xy})).$$

It is not slicewise definable in any FO_q [C. and Flum, 2016].

A meta-theorem

Theorem (C. , Flum, and Huang, 2017)

*Let $\varphi(X)$ be a formula in which **the set variable X does not occur in the scope of an existential quantifier or negation symbol**. Then the problem Fagin-defined by $\varphi(X)$ is slicewise definable in FO_q , where q only depends on φ .*

Another meta-theorem

Theorem (C. and Flum, 2017)

Let \mathbf{K} be a class of graphs of *bounded tree depth*. Then

$p\text{-MC}(\mathbf{K}, \text{MSO})$

Input: A graph $G \in \mathbf{K}$ and $\varphi \in \text{MSO}$.

Parameter: $|\varphi|$.

Problem: Decide whether $G \models \varphi$.

is in para-AC^0 .

If \mathbf{K} has unbounded tree depth, and is *closed under subgraphs*, then $p\text{-MC}(\mathbf{K}, \text{FO}) \notin \text{para-AC}^0$.

Some lower bounds

Building on [Håstad, 1988],

Theorem (C. , Flum, and Huang, 1988)

Let $q \in \mathbb{N}$. Then there is a problem slicewise definable in FO_{q+1} but not in FO_q .

Conclusions

1. As in classical AC^0 -complexity, we can prove many unconditional para- AC^0 lower bounds. They might increase our confidence in those parameterized complexity assumptions.
2. Proving classical AC^0 -lower bounds likely leads to lower bounds for para- AC^0 . Conversely, proving lower bounds for para- AC^0 might require proving optimal AC^0 -lower bounds.
3. Can we go beyond AC^0 , e.g., circuits with **modular counting gates**?