On Limitations of the Ehrenfeucht-Fraïssé-method in Descriptive Complexity

Yijia Chen
Shanghai Jiaotong University

June 10th, 2014 @ Algorithmic Randomness

Joint work with Jörg Flum (Freiburg)

Computability, complexity, and randomness

- This talk is all about complexity.
- Computability will appear several times.
- The last part of the talk is dominated by randomness.

The holy grail of complexity theory

Prove $\mathsf{P} \neq \mathsf{NP}$.

Why is P vs. NP so hard?

1. Diagonalization methods – relativization barrier [Baker, Gill, and Solovay, 1975]
2. Combinatorial methods – natural proof barrier [Razborov and Rudich, 1997]
3. Algebraic methods – algebrization barrier [Aaronson and Wigerson, 2009]

The only known viable approach in classical complexity is Geometric Complexity Theory (GCT) proposed by Mulmuley using algebraic geometry and representation theory.

Mulmuley believes that it might take hundreds of years before GCT can separate P and NP.

Understand computational problems by logic definability

Example

A graph G contains an independent set of size k if and only if

$$G \models \exists x_1 \ldots \exists x_k \left(\bigwedge_{1 \leqslant i < j \leqslant k} (x_i \neq x_j \wedge \neg E x_i x_j) \right).$$

Example

A graph G is 3-colorable if and only if

$$\begin{aligned} G \models \exists X_1 \exists X_2 \exists X_3 \Big(\forall x \bigvee_{1 \leqslant i \leqslant 3} X_i x \wedge \forall x \bigwedge_{1 \leqslant i < j \leqslant 3} (\neg X_i x \vee \neg X_j x) \\ \wedge \forall x \forall y \big(Exy \to \neg \bigvee_{1 \leqslant i \leqslant 3} (X_i x \wedge X_i y) \big) \Big) \end{aligned}$$

A model-theoretic approach to P vs. NP

Theorem (Immerman and Vardi, 1982)

A class of ordered graphs is decidable in polynomial time if and only if it can be defined by least fixed-point logic LFP.

Corollary

P $\neq$ NP *if and only if the class of 3-colorable ordered graphs is not definable in* LFP. *That is, there is no* LFP*-sentence* φ *such that for every ordered graph* $\mathcal{G}$

$$\mathcal{G} \text{ is 3-colorable} \quad \Longleftrightarrow \quad \mathcal{G} \models \varphi.$$

In classical model theory, the standard tool for proving inexpressiveness (for first-order logic FO) is the compactness theorem, which does not hold on the class $\mathscr{S}$ of all finite structures.

However, another tool of Ehrenfeucht-Fraïssé games survives on $\mathscr{S}$.

Ehrenfeucht-Fraïssé Games

Ehrenfeucht-Fraïssé games for FO

Let $\mathcal{G}$ and $\mathcal{H}$ be two ordered graphs and $m \in \mathbb{N}$. The Ehrenfeucht-Fraïssé game $G_m(\mathcal{G}, \mathcal{H})$ is played by two players, Spoiler and Duplicator, for m rounds:

(1) Spoiler chooses either $u_1 \in V(\mathcal{G})$ or $v_1 \in V(\mathcal{H})$.

(2) Duplicator answers by choosing either $v_1 \in V(\mathcal{H})$ or $u_1 \in V(\mathcal{G})$.

...

(2m) Spoiler chooses either $u_m \in V(\mathcal{G})$ or $v_m \in V(\mathcal{H})$.

(2m+1) Duplicator answers by choosing either $v_m \in V(\mathcal{H})$ or $u_m \in V(\mathcal{G})$.

Duplicator wins if by the mapping f with $f(u_i) = v_i$ for all $i \in [m]$

$$f : \mathcal{G}\big[\{a_1, \ldots, a_m\}\big] \cong \mathcal{H}\big[\{b_1, \ldots, b_m\}\big],$$

otherwise Spoiler wins.

Ehrenfeucht-Fraïssé games for FO (cont'd)

Theorem

Duplicator has a winning strategy for $G_m(\mathcal{G}, \mathcal{H})$ if and only if $\mathcal{G}$ and $\mathcal{H}$ satisfy the same FO*-sentences of quantifier rank m,*

$$\mathcal{G} \equiv_{\mathsf{FO}_m} \mathcal{H}.$$

Theorem

Let K be a class of ordered graphs. K is not definable by FO *if and only if there is a sequence $(\mathcal{G}_m, \mathcal{H}_m)_{m \in \mathbb{N}}$ such that for all $m \in \mathbb{N}$ we have $\mathcal{G}_m \in K$, $\mathcal{H}_m \notin K$, and*

$$\mathcal{G}_m \equiv_{\mathsf{FO}_m} \mathcal{H}_m, \quad \text{i.e., Duplicator has a winning strategy in } G_m(\mathcal{G}_m, \mathcal{H}_m).$$

Evenness is not in FO

Let $m \in \mathbb{N}$. We construct an ordered graph $\mathcal{G}_m$ which is a path of length 2^m, and the second ordered graph $\mathcal{H}_m$ is a path of length $2^m + 1$.

In the i-th round, Duplicator ensures that for every $j < i$

1. $\mathrm{dist}^{\mathcal{G}_m}(u_i, u_j) = \mathrm{dist}^{\mathcal{H}_m}(v_i, v_j)$, or
2. $\mathrm{dist}^{\mathcal{G}_m}(u_i, u_j) > 2^{m-i}$ and $\mathrm{dist}^{\mathcal{H}_m}(v_i, v_j) > 2^{m-i}$.

Ehrenfeucht-Fraïssé games for LFP

Essentially we need to exhibit a sequence $(\mathcal{G}_m, \mathcal{H}_m)_{m \in \mathbb{N}}$ of pairs of ordered graphs such that

1. $\mathcal{G}_m$ is 3-colorable, while $\mathcal{H}_m$ is not.
2. $\mathcal{G}_m$ and $\mathcal{H}_m$ satisfy the same LFP-sentences of quantifier-rank/length at most m,

$$\mathcal{G}_m \equiv_{\mathsf{LFP}_m} \mathcal{H}_m.$$

Some successful highlights

1. Reachability in directed graphs is not expressible in monadic Σ^1_1 [Ajtai and Fagin, 1990].

2. There is a polynomial time property of structures not expressible in least fixed-point logic with counting [Cai, Fürer, and Immerman, 1992].

3. For ordered graphs connectivity is not expressible in monadic Σ^1_1 [T. Schwentick, 1994].

Why not P $\neq$ NP by Ehrenfeucht-Fraïssé games?

A quote from Fagin, Stockmeyer, and Vardi, 1995

It is known that $\Sigma^1_1 \neq \Pi^1_1$ [and hence NP $\neq$ coNP] if and only if such a separation can be proven via second-order Ehrenfeucht-Fraïssé games. Unfortunately, "playing" second-order Ehrenfeucht-Fraïssé games is very difficult, and the above promise is still largely unfulfilled; for example, the equivalence between the NP = coNP question and the $\Sigma^1_1 = \Pi^1_1$ has not so far led to any progress on either of these questions.

One way of attacking these difficult questions is to restrict the classes under consideration... The hope is that the restriction to the monadic classes will yield more tractable questions and will serve as a training ground for attacking the problems in their full generality.

EF-sequences

Theorem

P $\neq$ NP *if and only if there is a sequence* $(\mathcal{G}_m, \mathcal{H}_m)_{m \in \mathbb{N}}$ *of ordered graphs such that*

1. $\mathcal{G}_m$ *is 3-colorable and* $\mathcal{H}_m$ *is not.*
2. $\mathcal{G}_m \equiv_{\mathsf{LFP}_m} \mathcal{H}_m$.

Compared to other methods, we have some very concrete objects which must exist.

It is natural to ask for constructing $(\mathcal{G}_m, \mathcal{H}_m)$ efficiently.

Given a proof, one would expect to see a clear definition of $\mathcal{G}_m$ and $\mathcal{H}_m$ which might be turned into an efficient construction algorithm.

But what do we mean by "efficient construction?"

Construction in time $m^{O(1)}$?

Theorem
$(\mathcal{G}_m, \mathcal{H}_m)$ cannot be constructed in time $m^{O(1)}$.

Consider the function

$$Q(m) := \min\Big\{ \max\{\|\mathcal{G}\|, \|\mathcal{H}\|\} \;\Big|\; \mathcal{G} \text{ and } \mathcal{H} \text{ are ordered graphs such that } \mathcal{G} \equiv_{\mathsf{LFP}_m} \mathcal{H},\ \mathcal{G} \text{ 3-colorable and } \mathcal{H} \text{ not}\Big\}.$$

Lemma
There is an $\varepsilon > 0$ such that for all $m \in \mathbb{N}$

$$Q(m) \geq 2^{\varepsilon m}.$$

The key observation is that an ordered graph can be characterized by sentences of logarithmic size.

The size of EF-sequences

Lemma

Assuming that the 3-colorability problem has no circuit of size $2^{o(n)}$ infinitely often, then for every $\varepsilon > 0$ and all sufficiently large $m \in \mathbb{N}$

$$Q(m) \leqslant 2^{(1+\varepsilon) m \log m}.$$

Recall: Evenness is not in FO

Let $m \in \mathbb{N}$. We construct an ordered graph $\mathcal{G}_m$ which is a path of length 2^m, and the second ordered graph $\mathcal{H}_m$ is a path of length $2^m + 1$.

The construction is done in time $\left(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|\right)^{O(1)}$.

Construction in time $\left(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|\right)^{O(1)}$?

Theorem

The EF-sequence $(\mathcal{G}_m, \mathcal{H}_m)_{m\in\mathbb{N}}$ cannot be constructed in time

$$\left(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|\right)^{O(1)}.$$

All successful applications of Ehrenfeucht-Fraïssé-method have corresponding structures constructed in such a time bound.

Proof sketch

1. Let $\mathbb{C}$ be an algorithm which constructs $(\mathcal{G}_m, \mathcal{H}_m)_{m\in\mathbb{N}}$ in time $(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|)^{O(1)}$.
2. We turn $\mathbb{C}$ into a polynomial time algorithm $\mathbb{D}$ such that for infinitely many $m \in \mathbb{N}$

$$\mathbb{D} \text{ accepts } \mathcal{G}_m \quad \text{and} \quad \mathbb{D} \text{ rejects } \mathcal{H}_m.$$

3. By Immerman-Vardi Theorem, there is an LFP-sentence $\varphi_{\mathbb{D}}$ such that for infinitely many $m \in \mathbb{N}$

$$\mathcal{G}_m \models \varphi_{\mathbb{D}} \quad \text{and} \quad \mathcal{H}_m \not\models \varphi_{\mathbb{D}}.$$

4. Choose m large enough such that $\varphi_{\mathbb{D}} \in \mathrm{LFP}_m$, and recall

$$\mathcal{G}_m \equiv_{\mathrm{LFP}_m} \mathcal{H}_m,$$

which contradicts to 3.

Ehrenfeucht-Fraïssé Games on Random Structures

Ehrenfeucht-Fraïssé games on random structures

Instead of constructing $(\mathcal{G}_m, \mathcal{H}_m)$ in deterministic time $(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|)^{O(1)}$, can we do it probabilistically?

Successful probabilistic constructions include [Ajtai and Fagin, 1990] and [Rossman, 2009].

A probabilistic algorithm $\mathbb{P}$ generates a random EF-sequence $(\mathcal{G}_m, \mathcal{H}_m)_{m\in\mathbb{N}}$ if:

(R1) For every $m \in \mathbb{N}$ the algorithm $\mathbb{P}$ first *deterministically* computes the vertex set $V(\mathcal{G}_m)$ and $V(\mathcal{H}_m)$, and then constructs the ordered graphs $\mathcal{G}_m$ and $\mathcal{H}_m$ probabilistically.

(R2) There is a polynomial time algorithm $\mathbb{C}$:

- For any $(\mathcal{G}, \mathcal{H})$, if $\mathbb{C}$ accepts $(\mathcal{G}, \mathcal{H})$, then $\mathcal{G}$ is 3-colorable and $\mathcal{H}$ is not.
- For sufficiently large $m \in \mathbb{N}$,

$$\Pr\left[\mathbb{C} \text{ accepts } (\mathcal{G}_m, \mathcal{H}_m)\right] \geq \frac{4}{5}.$$

(R3) There is an algorithm $\mathbb{E}$:

- For any $(\mathcal{G}, \mathcal{H})$ and all $m \in \mathbb{N}$, if $\mathbb{E}$ accepts $(\mathcal{G}, \mathcal{H}, m)$, then $\mathcal{G} \equiv_{\mathsf{LFP}_m} \mathcal{H}$.
- For sufficiently large $m \in \mathbb{N}$,

$$\Pr\left[\mathbb{E} \text{ accepts } (\mathcal{G}_m, \mathcal{H}_m, m)\right] \geq \frac{4}{5}.$$

- The running time of $\mathbb{E}(\mathcal{G}, \mathcal{H}, m)$ is bounded by $f(m) \cdot (\|\mathcal{G}\| + \|\mathcal{H}\|)^{O(1)}$ for a computable function $f : \mathbb{N} \to \mathbb{N}$.

Justifications

(R1) Clear.

(R2) Similar to (R3).

(R3) There is an algorithm $\mathbb{E}$:

- For any $(\mathcal{G}, \mathcal{H})$ and all $m \in \mathbb{N}$, if $\mathbb{E}$ accepts $(\mathcal{G}, \mathcal{H}, m)$, then $\mathcal{G} \equiv_{\mathrm{LFP}_m} \mathcal{H}$.
- For sufficiently large $m \in \mathbb{N}$,

$$\Pr\left[\mathbb{E} \text{ accepts } (\mathcal{G}_m, \mathcal{H}_m, m)\right] \geq \frac{4}{5}.$$

- The running time of $\mathbb{E}(\mathcal{G}, \mathcal{H}, m)$ is bounded by $f(m) \cdot (\|\mathcal{G}\| + \|\mathcal{H}\|)^{O(1)}$ for a computable function $f : \mathbb{N} \to \mathbb{N}$.

That is, $\mathbb{E}$ provides an algorithmic proof of with high probability $\mathcal{G}_m \equiv_{\mathrm{LFP}_m} \mathcal{H}_m$. The running time of $f(m) \cdot (\|\mathcal{G}\| + \|\mathcal{H}\|)^{O(1)}$ can be used to explain why Ehrenfeucht-Fraïssé-method has been particularly successful with respect to monadic second-order logic where one can apply Courcelle's Theorem.

Theorem
Assume that

there is a function in E *which has no circuit of size* $2^{o(n)}$ *infinitely often*. $(\star)$

Then there is no probabilistic algorithm that generates a random EF-sequence $(\mathcal{G}_m, \mathcal{H}_m)_{m\in\mathbb{N}}$ *in time* $(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|)^{O(1)}$.

Remark
The assumption $(\star)$ *is widely believed in complexity theory, which implies* $\mathsf{P} = \mathsf{BPP}$ [Impagliazzo and Wigderson, 1997].

Is Ehrenfeucht-Fraïssé-method really hopeless?

The Planted Clique Conjecture

The Erdős-Rényi random graph

Definition

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

Lemma

The expected size of a maximum clique in $\mathcal{G} \in \mathrm{ER}(n, 1/2)$ is approximately $2 \log n$, thus $\mathcal{G}$ almost surely has no clique of size $4 \log n$.

We consider a second distribution $\mathcal{G} + A$ with $A \in K(n, 4 \log n)$:

Definition

Let $n, k \in \mathbb{N}$. Then $K(n, k)$ is the uniform distribution over all cliques of size k on the vertex set $[n]$.

The planted clique conjecture (PCC)

Conjecture

There is no polynomial time algorithm to distinguish $\mathrm{ER}(n, 1/2)$ *and* $\mathrm{ER}(n, 1/2) + K(n, 4 \log n)$*. For every polynomial time algorithm* $\mathbb{A}$

$$\left| \Pr_{\mathcal{G} \in \mathrm{ER}(n,1/2)} \Big[\mathbb{A} \text{ accepts } \mathcal{G} \Big] - \Pr_{\substack{\mathcal{G} \in \mathrm{ER}(n,1/2), \\ A \in K(n, 4 \log n)}} \Big[\mathbb{A} \text{ accepts } (\mathcal{G} + A) \Big] \right| \leqslant 1/5$$

for all sufficiently large $n \in \mathbb{N}$*.*

The logic version of the planted clique conjecture (LPCC)

Conjecture

There is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that for every $m \in \mathbb{N}$

$$\Pr_{\substack{\mathcal{G} \in \mathrm{ER}(f(m),1/2),\\ A \in K(f(m),4\log f(m))}} \Big[G \equiv_{\mathrm{LFP}_m} (\mathcal{G} + A) \Big] \geq 4/5.$$

Theorem

LPCC *implies* PCC.

Remark

The converse is open.

LPCC and randomized EF-sequences

Theorem

Assume LPCC*. Then there is a probabilistic algorithm* $\mathbb{A}$ *which for every* $m \in \mathbb{N}$ *generates* $(\mathcal{G}_m, \mathcal{H}_m)$ *in time* $\left(\|\mathcal{G}_m\| + \|\mathcal{H}_m\|\right)^{O(1)}$ *such that with high probability*

1. $\mathcal{G}_m$ *is not 3-colorable, while* $\mathcal{H}_m$ *is;*
2. $\mathcal{G}_m \equiv_{\mathsf{LFP}_m} \mathcal{H}_m$.

Proof.

Finding a clique of size $4 \log n$ is in NP, and 3-colorability is NP-complete. $\square$

How plausible is LPCC?

PCC, hence also LPCC, implies P $\neq$ NP.

However we can prove unconditionally an FO version of LPCC:

Theorem

There is a computable function $f : \mathbb{N} \to \mathbb{N}$ such that for every $m \in \mathbb{N}$

$$\Pr_{\substack{\mathcal{G} \in \mathrm{ER}(f(m),1/2),\\ A \in K(f(m),4\log f(m))}} \left[\mathcal{G} \equiv_{\mathrm{FO}_m} (\mathcal{G} + A)\right] \geq 4/5.$$

The proof uses a very tricky machinery developed by Rossman in his 2008 proof that the k-clique problem requires AC^0-circuits of size $\omega(n^{k/4})$, whose core is Håstad's Switching Lemma.

Generalized PCC and Parameterized Complexity

Generalized PCC

Let computable $g : \mathbb{N} \to \mathbb{N}$ be non-decreasing and unbounded with $g(n) \geq 1/\log n$. Then the expected size of a maximum clique in $G \in \mathrm{ER}\left(n, n^{2/g(n)}\right)$ is approximately $g(n)$.

Conjecture

There is no polynomial time algorithm to distinguish $\mathrm{ER}\left(n, n^{2/g(n)}\right)$ *and* $\mathrm{ER}\left(n, n^{2/g(n)}\right) + K(n, 2g(n))$.

Theorem

There is a computable function $f : \mathbb{N} \to \mathbb{N}$ *such that for every* $m \in \mathbb{N}$

$$\Pr_{\substack{\mathcal{G} \in \mathrm{ER}(f(m), f(m)^{2/g(f(m))}),\\ A \in K(f(m), 2g(f(m)))}} \left[\mathcal{G} \equiv_{\mathrm{FO}_m} (\mathcal{G} + A)\right] \geq 4/5.$$

Theorem

The parameterized clique problem has no fpt-approximation algorithm with constant approximation ratio, unless the generalized PCC fails.

Conclusions

1. It would be difficult to prove P $\neq$ NP using the Ehrenfeucht-Fraïssé-method, but probably not impossible.
2. Ehrenfeucht-Fraïssé games on random graphs are more powerful than deterministic games.
3. LPCC has applications not only in Ehrenfeucht-Fraïssé games, but also parameterized complexity as well.

Thank You!