Exercises on Proof Complexity
CSCI 6114 Fall 2021

Joshua A. Grochow

October 7, 2021

A *Cook–Reckhow proof system* for a language L is a polynomial-time function P such that

1. For every $x \in L$, there exists a π such that $P(\pi) = x$; we call π a "P-proof" for x (or a P-proof that x is in L)
2. For every string π, $P(\pi) \in L$.

A proof system P is called polynomially bounded or p-bounded if for every x there exists a P-proof π for x such that $|\pi| \leq \mathrm{poly}(|x|)$.

1. Prove that for any language L, L has a p-bounded Cook–Reckhow proof system iff $L \in \mathsf{NP}$.
2. Let UNSAT denote the set of Boolean formulas that are unsatisfiable.
   (a) Show that UNSAT is coNP-complete. *Hint:* What is the complement of UNSAT?
   (b) Show that there is a p-bounded proof system for UNSAT iff $\mathsf{NP} = \mathsf{coNP}$.
3. When we think of Graph Isomorphism as a language, we consider it as the set of pairs $\{(G, H) : G \text{ is isomorphic to } H\}$.
   (a) Give a p-bounded Cook–Reckhow proof system for GI.
   (b) The k-dimensional Weisfeiler–Leman procedure (k-WL) to show two graphs G, H are non-isomorphic works as follows. It will iteratively color the k-tuples of vertices of G and H as follows. Two k-tuples $(u_1, \dots, u_k)$ and $(v_1, \dots, v_k)$ initially receive the same color iff $u_i = u_j \Leftrightarrow v_i = v_j$ for all $i \neq j$, and if the map $u_i \mapsto v_i$

induces an isomorphism on the corresponding induced subgraphs. At each iteration, the colors are refined similar to 2-WL: the new color of $(v_1, \ldots, v_k)$ consists of the tuple

$$(c_{t-1}, M_1, \ldots, M_k)$$

where c_{t-1} is the color of $(v_1, \ldots, v_k)$ at the previous time step $t-1$, and M_i is the multiset of colors of tuples of the form $(v_1, v_2, \ldots, v_{i-1}, *, v_{i+1}, \ldots, v_k)$. k-WL distinguishes G from H if at any point in this process, the multiset of all colors appearing in G differs from that in H. (The process stops when the partition of G^k is no longer refined.)

Reformulate Weisfeler–Leman (of arbitrary dimension) as a Cook–Reckhow proof system for coGI aka Graph Non-Isomorphism. Is it p-bounded?

4. Unsatisfiable formulas are also known as contradictions. Prove that any contradiction φ has a resolution refutation. Given an upper bound on the size of this refutation.

5. Show that unsatisfiable 2-CNF formulas variables have resolution refutations of polynomial size.

6. Show that resolution is p-simulated by sequent calculus where all cuts are on individual variables.

Resources

- Paul Beame lecture notes (notes by Ashish Sabharwal)
- Beame–Pitassi Bull. EATCS survey
- Pitassi–Tzameret survey on algebraic proof complexity
- Razborov SIGACT News survey
- Razborov 2009 course
- Nate Segerlind 2007 Bull. Symb. Logic survey
- Krajicek book