Branching Program Complexity of Canonical Search Problems and Proof Complexity of Formulas[⋆]

Alexander Knop

University of California, San Diego
aknop@ucsd.edu

In 1991 Lovász et al. [8] defined a search problem Search_ϕ associated with an unsatisfiable CNF ϕ: given a substitution to all the variables of ϕ, find a falsified clause of ϕ. In the paper, they also mentioned an unpublished result of Chvátal and Szemerédi that says that the minimal size of a read-once branching program for Search_ϕ is equal to the minimal size of a regular resolution proof of ϕ. It is easy to see that the same equivalence holds for decision trees and tree-like resolution proofs and for ordered binary decision diagrams and ordered resolution proofs. The proof of this statement is made of two parts: "diagram to proof transformation" and "proof to diagram transformation".

The diagram to proof transformation: Chvátal and Szemerédi showed that it is possible to transform any read-once branching program for Search_ϕ (ϕ is an unsatisfiable CNF) into a regular resolution proof of ϕ. Moreover, if the diagram is a decision tree, then the resulting proof is a tree-like proof and if the diagram is ordered, then the resulting proof is also ordered. It is possible to note that any resolution proof of ϕ can be transformed into a branching program of the same size for Search_ϕ. Krajíček [7] generalized this approach and showed that a big class of proof systems (this class includes $\mathbf{CP}^*$) allows transformation to PLS games and, using the lower bound proven by Razborov [9], he proved lower bounds for these proof systems. Finally, recently Hrubesh, Pudlak, and Sokolov [5, 10] noticed that the same transformation can be done for **CP** and real communication games (generalization of PLS games to real communication).

The proof to diagram transformation: They also proved that any regular resolution proof can be transformed into a read-once branching program. Furthermore, if the proof is tree-like, the diagram is a decision tree and if the proof is ordered, then the diagram is also ordered. To construct this transformation Chvátal and Szemerédi showed that it is possible to annotate every node of a read-once branching program D for Search_ϕ with a clause, so that

- the source of the diagram is annotated by a constant false clause,
- every sink of the diagram is annotated by a clause of ϕ, and
- if some node u has children v and w, then clauses annotating u and w semantically imply the clause annotating v.

Note that these annotations form a semantic resolution proof. However, this construction does not work if the diagram is not read-once. Indeed, it is easy to see that for every unsatisfiable formula ϕ in CNF there is a branching program

[⋆] A preprint of this work was published on ECCC [6].

of polynomial size for Search_ϕ. In 1997 Krajíček [7] noticed that if instead of annotating the diagram we consider an already annotated diagram it is possible to drop the "read-once" constraint and prove lower bounds on size of such diagrams (using so-called "interpolation technique"), even if instead of clauses we consider functions of small communication complexity and instead of splitting by variables we allow to split by values of functions of small communication complexity.

However, the study of a relationship between the proof complexity of formulas and the complexity of not annotated and not read-once branching programs for corresponding search problems was stuck. Nothing was known for bigger classes of diagrams. I this research we revitalize the study of this problem in the light of **IPS**-like proof systems [2,4]. A $\mathcal{C}$-$\mathbf{PS}_a$ ($\mathcal{C}$ is a class of branching programs) proof of an unsatisfiable formula $\phi(x_1, \ldots, x_n) = \bigwedge_{i=1}^{m} C_i(\bar{x})$ is a $\mathcal{C}$ branching program D on the variables $x_1, \ldots, x_n, y_1, \ldots, y_m$, such that

- $D(x_1, \ldots, x_n, 1, \ldots, 1) = 1$,
- $D(x_1, \ldots, x_n, C_1(x_1, \ldots, x_n), \ldots, C_m(x_1, \ldots, x_n)) = 0$, and
- on any path in D, there are at most a nodes which query a variable from $y_1, \ldots, y_m$.

In the following we consider four types of branching programs: $\oplus$-OBDDs (branching programs with parity gates that read all the variables in some order), $(1, +b)$-BPs (in these branching programs there is no path which queries more than b variables more than once), $\oplus$-$(1, +b)$-BPs (the same as the previous one but with parity gates), and b-OBDDs (branching programs that read all the variables in some order b times).

In this work we show that for the proof systems based on $(1, +b)$-BPs and b-OBDDs the size of the smallest proof of a formula ϕ is equal to the smallest size of a $(1, +b)$-BP diagrma and a b-OBDD diagram for Search_ϕ, respectively. As a corollary, using the result of Chvátal and Szemerédi [8] it is possible to show that OBDD-$\mathbf{PS}_1$ and 1-BP-$\mathbf{PS}_1$ are equivalent to ordered resolution and regular resolution, respectively. Additionally, in this project we prove that $\oplus$-OBDD-$\mathbf{PS}_1$ p-simulates b-OBDD-$\mathbf{PS}_1$ for any constant $b > 0$. We show that every b-round protocol for the search problem corresponding to some Tseitin formula has cost at least $n^{1/2b}$. Since lower bounds on b-round communication complexity imply lower bounds on OBDD complexity, we prove a $2^{\Omega\left(n^{1/2b}\right)}$ lower bound for size of b-OBDD-$\mathbf{PS}_1$ proofs of Tseitin formulas. We also show that this lower bound for OBDD complexity is almost tight and as a result, we show that resolution (**Res**) does not p-simulate b-OBDD-$\mathbf{PS}_1$ for $b \geq 2$. Additionally, we prove a polynomial upper bound for the size of $\oplus$-OBDD-$\mathbf{PS}_1$ proofs of Tseitin formulas and prove that b-OBDD-$\mathbf{PS}_1$ does not p-simulate $\oplus$-OBDD-$\mathbf{PS}_1$. Besides, we notice that for b-OBDD-$\mathbf{PS}_1$ and $(1, +b)$-BP-$\mathbf{PS}_1$ proof systems, composition of a simple formula with a small gadget is also simple. As a result, we show that **CP** does not p-simulate 2-OBDD-$\mathbf{PS}_1$ and that **Res** does not p-simulate $(1, +6)$-BP-$\mathbf{PS}_1$. The lower bounds for **CP** and **Res** follow from a result of Garg et al. [3] and an unpublished result of Alekhnovich and Razborov [1], respectively. Finally, in this project we prove that extended Frege p-simulates b-OBDD-$\mathbf{PS}_1$.

References

1. Eli Ben-Sasson. Size space tradeoffs for resolution. In John H Reif, editor, *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*, pages 457–464. ACM, 2002.
2. Michael A. Forbes, Amir Shpilka, Iddo Tzameret, and Avi Wigderson. Proof complexity lower bounds from algebraic circuit complexity. In *31st Conference on Computational Complexity, CCC 2016, May 29 to June 1, 2016, Tokyo, Japan*, pages 32:1–32:17, 2016.
3. Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone Circuit Lower Bounds from Resolution. *Electronic Colloquium on Computational Complexity (ECCC)*, 175, 2017.
4. Joshua A. Grochow and Toniann Pitassi. Circuit complexity, proof complexity, and polynomial identity testing. *55th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2014, Philadelphia, PA, USA, October 18-21, 2014*, pages 110–119, 2014.
5. Pavel Hrubes and Pavel Pudlák. Random formulas, monotone circuits, and interpolation. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:42, 2017.
6. Alexander Knop. IPS-like Proof Systems Based on Binary Decision Diagrams. *Electronic Colloquium on Computational Complexity (ECCC)*, 24:179, 2017.
7. Jan Krajiček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *Journal of Symbolic Logic*, 62(2):457–486, 1997.
8. László Lovász, Moni Naor, Ilan Newman, and Avi Wigderson. Search problems in the decision tree model. *SIAM Journal on Discrete Mathematics*, 8(1):119–132, 1995.
9. Alexander A. Razborov. Lower Bounds for Propositional Proofs and Independence Results in Bounded Arithmetic (Abstract). In *Mathematical Foundations of Computer Science 1995, 20th International Symposium, MFCS'95, Prague, Czech Republic, August 28 - September 1, 1995, Proceedings*, page 105, 1995.
10. Dmitry Sokolov. Dag-like communication and its applications. In Pascal Weil, editor, *Computer Science - Theory and Applications - 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12, 2017, Proceedings*, volume 10304 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2017.