

Towards an Understanding of Polynomial Calculus: New Separations and Lower Bounds

Yuval Filmus¹, Massimo Lauria², Mladen Mikša², Jakob Nordström², and
Marc Vinyals²

¹ Institute for Advanced Study, Princeton, NJ 08540, USA

² KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden

Abstract. Recently, an active line of research has been into the space complexity of proofs. We prove that if a formula requires large resolution width, then making XOR substitution yields a formula requiring large PC space. This yields formulas that exhibiting a degree-space separation similar to what is known for resolution. Using related ideas, we show that Tseitin formulas over random 4-regular graphs almost surely require space at least $\Omega(\sqrt{n})$.

Our proofs use techniques from [Bonacina-Galesi '13]. Our final contribution, however, is to show that these techniques cannot yield non-constant space lower bounds for the functional pigeonhole principle, which is conjectured to be hard for PC space. This talk is based on [FLMN '13].

One motivation for proof complexity is the connection to applied SAT solving, as upper and lower bounds provide information about the potential and limitations of SAT solvers. Two major concerns in SAT solving are running time and memory consumption. In proof complexity, these two resources are modelled by *proof size* and *proof space*. In the context of applied SAT solving, we focus on simpler proof systems that can be used as a basis for SAT solvers, for instance resolution and polynomial calculus.

Most state-of-the-art SAT solvers are based on *resolution*. Besides size and space, Ben-Sasson and Wigderson [4] identified width (i.e., the size of clauses in the proof) as a crucial resource for this proof system. They proved that strong lower bounds on width imply strong lower bounds on size. Atserias and Dalmau [2] showed that space is lower-bounded by width, and a strong space-width separation was obtained in [3].

This talk focuses on the more powerful *polynomial calculus (PC)* proof system introduced by Clegg et al. and extended by Alekhnovich et al. [1, 6]. In a PC proof, clauses are interpreted as multilinear polynomials (expanded out to sums of monomials), and one derives contradiction by showing that these polynomials have no common root. The analogues of resolution size and space are defined for PC by counting the number of monomials instead of clauses, while the degree of polynomials can be viewed as the analogue of width in resolution.

Impagliazzo et al. [8] showed that strong degree lower bounds imply strong size lower bounds which is analogous to the length-width relation in [4]. Hence, it is a natural question whether this parallel between width and degree can be

extended to PC space. However, the question whether degree is a lower bound for space remains open and also it has been unknown whether there are formulas of low degree complexity requiring high space.

We present results on the relation of space and degree in PC, as well as some results on PC space lower bounds, which were originally published in [7].

1. By using results from [5] and [2] we show that if the resolution width of refuting a CNF formula F is w , then by substituting each variable by an exclusive or of two new variables we get a new formula $F[\oplus]$ requiring PC space $\Omega(w)$.
2. From this result an essentially optimal separation between degree and space follows. Namely, for expander graphs with double copies of edges Tseitin formulas have proofs in degree $O(1)$ but require space $\Theta(n)$ in PC.
3. Using related ideas, we prove PC space lower bounds for Tseitin formulas over graphs whose edges can be partitioned into small cycles. In particular, for Tseitin formulas over random 4-regular graphs we establish that an $\Omega(\sqrt{n})$ PC space lower bound holds asymptotically almost surely.
4. On the negative side, we show that the techniques in [5] cannot prove any non-constant PC space lower bounds for functional pigeonhole principle (FPHP) formulas. That is, although it seems that these formulas are hard with respect to space, current machinery cannot establish such lower bounds.

References

1. Alekhovich, M., Ben-Sasson, E., Razborov, A.A., Wigderson, A.: Space complexity in propositional calculus. In: Proc. 32nd Symposium on Theory of Computing (STOC '00). pp. 358–367 (May 2000)
2. Atserias, A., Dalmau, V.: A combinatorial characterization of resolution width. In: Proc. 18th IEEE Annual Conference on Computational Complexity (CCC '03). pp. 239–247 (Jul 2003)
3. Ben-Sasson, E., Nordström, J.: Short proofs may be spacious: An optimal separation of space and length in resolution. In: Proc. 49th Symposium on Foundations of Computer Science (FOCS '08). pp. 709–718 (Oct 2008)
4. Ben-Sasson, E., Wigderson, A.: Short proofs are narrow—resolution made simple. In: Proc. 31st Symposium on Theory of Computing (STOC '99). pp. 517–526 (May 1999)
5. Bonacina, I., Galesi, N.: Pseudo-partitions, transversality and locality: A combinatorial characterization for the space measure in algebraic proof systems. In: Proc. 4th Innovations in Theoretical Computer Science Conference (ITCS '13) (Jan 2013)
6. Clegg, M., Edmonds, J., Impagliazzo, R.: Using the Groebner basis algorithm to find proofs of unsatisfiability. In: Proc. 28th Symposium on Theory of Computing (STOC '96). pp. 174–183 (May 1996)
7. Filmus, Y., Lauria, M., Mikša, M., Nordström, J., Vinyals, M.: Towards an understanding of polynomial calculus: New separations and lower bounds (extended abstract). In: Proc. 40th International Colloquium on Automata, Languages and Programming (ICALP '13). Lecture Notes in Computer Science, vol. 7965, pp. 437–448. Springer (Jul 2013)
8. Impagliazzo, R., Pudlák, P., Sgall, J.: Lower bounds for the polynomial calculus and the Gröbner basis algorithm. Computational Complexity 8(2), 127–144 (1999)