The polynomial calculus (PC) and polynomial calculus resolution (PCR) are algebraic proof systems intended to model the use of algebraic reasoning in propositional logic. This paper studies the problem of obtaining lower bounds on the degree of PC and PCR proofs, and hence, by a result of Impagliazzo et al. [1], also on the size of proofs in these systems.

Alekhnovich and Razborov [2] established the fact that if the clause-variable incidence graph of a CNF formula F is a sufficiently good expander, then proving that F is unsatisfiable requires large PC/PCR degree. Their techniques are further developed to show that if the clauses and variables of a formula can be clustered in a way that respects the structure of the formula in a certain sense, then it is sufficient that the incidence graph of this clustered version is an expander. It is also shown how a weaker structural condition is sufficient to obtain lower bounds on the width of resolution proofs, and a unified treatment is given that highlights similarities and differences between resolution and polynomial calculus lower bounds.

As a corollary of the main technical theorem, it follows that the functional pigeonhole principle (FPHP) formulas require large degree in PC and PCR when restricted to constant-degree expander graphs. This answers an open question of Razborov [3], and also implies that the standard CNF encoding of the FPHP formulas require exponential proof size in PCR. Thus, while the functional and surjective pigeonhole principle (onto-FPHP) formulas are easy for polynomial calculus, as shown by Riis [4], both FPHP and onto-PHP formulas are hard even when restricted to bounded-degree expanders.

References

[1] R. G. Impagliazzo, P. Pudlák and J. Sgall, Lower bounds for the polynomial calculus and the Gröbner basis algorithm, Comput. Complexity **8** (1999), no. 2, 127–144; MR1724604

[2] M. Alekhnovich and A. A. Razborov, Lower bounds for polynomial calculus: the Non-binomial ideal case. Proc. Steklov Inst. Math. **2003**, no. 3(242), 18–35; translated from Tr. Mat. Inst. Steklova **242** (2003), 23–43; MR2054483

[3] A. A. Razborov, Proof complexity of pigeonhole principles, in *Developments in language theory (Vienna, 2001)*, 110–116, Lecture Notes in Comput. Sci., 2295, Springer, Berlin, ; MR1964164

[4] Søren Riis, Independence in Bounded Arithmetic. Ph.D. Dissertation, Oxford University, 1993.