Linear Gaps Between Degrees for the Polynomial Calculus Modulo Distinct Primes
Abstract[1]

Sam Buss[2,3]
Department of Mathematics
Univ. of Calif., San Diego
La Jolla, CA 92093-0112
sbuss@ucsd.edu

Dima Grigoriev
IMR Universite Rennes-1
Beaulieu 35042
Rennes, France
dima@maths.univ-rennes1.fr

Russell Impagliazzo[2,4]
Computer Science and Engineering
Univ. of Calif., San Diego
La Jolla, CA 92093-0114
russell@cs.ucsd.edu

Toniann Pitassi[2,5]
Computer Science
University of Arizona
Tucson, AZ 85721-0077
toni@cs.arizona.edu

Two important algebraic proof systems are the Nullstellensatz system [1] and the polynomial calculus [2] (also called the Gröbner system). The Nullstellensatz system is a propositional proof system based on Hilbert's Nullstellensatz, and the polynomial calculus (PC) is a proof system which allows derivations of polynomials, over some £eld. The *complexity* of a proof in these systems is measured in terms of the degree of the polynomials used in the proof.

The mod p counting principle can be formulated as a set MOD_p^n of constant-degree polynomials expressing the negation of the counting principle. The Tseitin mod p principles, $TS_n(p)$, are translations of the MOD_p^n into the Fourier basis [3].

The present paper gives linear lower bounds on the degree of polynomial calculus refutations of MOD_p^n over £elds of characteristic $q \neq p$ and over rings Z_q with q, p relatively prime. These are the £rst linear lower bounds for the polynomial calculus. As it is well-known to be easy to give constant degree polynomial calculus (and even Nullstellensatz) refutations of the MOD_p^n polynomials over F_p, our results imply that the MOD_p^n polynomials have a linear gap between proof complexity for the polynomial calculus over F_p and over F_q. We also obtain a linear gap for the polynomial calculus over rings Z_p and Z_q where p, q do not have identical prime factors.

Theorem 1 *Let F be a £eld of characteristic q, and let G_n be an r-regular graph with expansion ϵ. Then, for all $d < \epsilon n/8$, there is no degree d PC refutation of $TS_n(p)$ over F.*

Theorem 2 *Let $q \geq 2$ be a prime such that $q \nmid p$ and let F be a £eld of characteristic q. Any PC-refutation of the MOD_p^n polynomials requires degree $> \delta n$, for some constant $\delta > 0$.*

References

[1] P. Beame, R. Impagliazzo, J. Krajíček, T. Pitassi, and P. Pudlák. Lower bounds on Hilbert's Nullstellensatz and propositional proofs. *Proceedings of the London Mathematical Society*, 73:1–26, 1996.

[2] M. Clegg, J. Edmonds, and R. Impagliazzo. Using the Groebner basis algorithm to £nd proofs of unsatis£ability. In *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing*, pages 174–183, 1996.

[3] D. Grigoriev. Nullstellensatz lower bounds for Tseitin tautologies. In *Proceedings of the 39th Annual IEEE Symposium on Foundations of Computer Science*, pages 648–652. IEEE Computer Society Press, 1998.

[1]This paper was presented jointly to the 14th Annual IEEE Conference on Computational Complexity and the 31st Annual ACM Symposium on Theory of Computer Science. The complete version is in the latter's proceedings volume.

[2]Supported in part by international grant INT-9600919/ME-103 from the NSF (USA) and the MŠMT (Czech republic)

[3]Supported in part by NSF grant DMS-9803515

[4]Supported in part by NSF grant CCR-9734911, Sloan Research Fellowship BR-3311, and US-Israel BSF grant 97-00188.

[5]Supported in part by NSF grant CCR-9457783 and US-Israel BSF grant 95-00238.