Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 96 (2010)

An Alternative Proof of The Schwartz-Zippel Lemma

Dana Moshkovitz *

July 8, 2010

Abstract

We show an alternative proof of the Schwartz-Zippel lemma. The lemma bounds the number of zeros of a multivariate low degree polynomial over a finite field.

1 Introduction

Let f be an m-variate polynomial of degree exactly d over a field $\mathbb{F}$, f is not identically zero. The Schwartz-Zippel lemma [Sch80, Zip79] in its commonly used form states that the number of zeros of f is at most $d \cdot |\mathbb{F}|^{m-1}$, or, alternatively,

$$\Pr_{x \in \mathbb{F}^m} [f(x) = 0] \leq \frac{d}{|\mathbb{F}|}.$$

For univariate polynomials, i.e., $m = 1$, this is a basic fact. The lemma works for any number of variables $m \geq 1$. The lemma is tight, as shown, e.g., by taking f to be a polynomial that depends on only one of its variables, and is zero for d different values of this variable.

The Schwartz-Zippel lemma is remarkably important to theoretical computer science: it is used for polynomial identity testing (e.g., to test whether a graph has a perfect matching), it establishes the distance property of the Reed-Muller code (the code that consists of truth tables of multivariate low degree polynomials), and it is used in proofs of hardness vs. randomness tradeoffs, as well as in algebraic constructions of Probabilistically Checkable Proofs.

The lemma has an inductive proof. In this note we present a different, more direct, proof. To the best of our knowledge, the proof we show was not known before.

We believe that there is a value – in general, and also here – to presenting alternative proofs for fundamental theorems. Such can shed new light on the statement being proven, introduce new arguments that can be useful elsewhere, or yield different generalizations and applications.

2 The Proof

Let us assume $m \geq 2$, $1 \leq d < |\mathbb{F}|$. The proof is by reduction to the case $m = 1$. Write $f = g + h$, where $g \not\equiv 0$ is homogeneous of degree d, and h contains only monomials of degree strictly smaller than d. Let[1] $y \neq \vec{0} \in \mathbb{F}^m$ be such that $g(y) \neq 0$. Note that $\mathbb{F}^m$ can be partitioned into $|\mathbb{F}|^{m-1}$ parallel lines, where each line is of the form $\{x + ty \mid t \in \mathbb{F}\}$ for some $x \in \mathbb{F}^m$. For

*dana.moshkovitz@gmail.com. School of Mathematics, The Institute for Advanced Study. Research supported by NSF Grant CCF-0832797.

[1] See Lemma 3.1.

ISSN 1433-8092

any $x \in \mathbb{F}^m$, the restriction $f(x+ty)$ is a univariate polynomial in t of degree at most d. Moreover, it is not identically 0! The reason is that the coefficient of t^d is $g(y)$. Thus, the number of zeros on each of the lines is at most d, and the total number of zeros of f is at most $d\,|\mathbb{F}|^{m-1}$.

3 A Lemma

Lemma 3.1. *If g is of degree $1 \leq d < |\mathbb{F}|$ and not identically zero, then there is $y \in \mathbb{F}^m$ such that $g(y) \neq 0$. Moreover, if g is homogeneous, then $y \neq \vec{0}$.*

Proof. Assume on way of contradiction that for every $y \in \mathbb{F}^m$, $g(y) = 0$. Then, there necessarily exist $1 \leq i \leq m$ and $a_1, \ldots, a_{i-1} \in \mathbb{F}$ such that $g(y_i, \ldots, y_m) \doteq f(a_1, \ldots, a_{i-1}, y_i, \ldots, y_m) \not\equiv 0$, but for every $a \in \mathbb{F}$ it holds that $g(a, y_{i+1}, \ldots, y_m) \equiv 0$. Note that g is of degree at most d. For every $a \in \mathbb{F}$, we have $(y_i - a)|g$, so g's degree is at least $|\mathbb{F}|$, which is a contradiction. Moreover, if g is homogeneous, then $g(\vec{0}) = 0$. □

4 Acknowledgments

The proof was devised for a mini-course on "Projection PCPs" given at Princeton University in spring 2009. It was concieved after hearing about the improvement of Noga Alon and Terry Tao to the solution of Zeev Dvir for the Kakeya problem in finite fields [Dvi09]. The author is thankful to Zeev Dvir and Noga Alon.

References

[Dvi09] Z. Dvir. On the size of kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22:1093–1097, 2009.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, 1980.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *In Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, pages 216–226, 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de