Zippel's Lemma or the Sparse Zeros Lemma

Frank R. Kschischang

November 7, 2009

Let $f \in F[x_1, \ldots, x_n]$ be a polynomial in n variables over an arbitrary field F, in which the degree of f as a polynomial in x_i is at most d, for $1 \leq i \leq n$. We say that f has "degree bounded by d."

Proposition: Let $f \in F[x_1, \ldots, x_n]$ have degree bounded by d and let $S \subset F$ be a set of $d+1$ distinct elements of F. If $f(s_1, \ldots, s_n) = 0$ for all n-tuples $(s_1, \ldots, s_n)$ in S^n, then $f \equiv 0$, i.e., f is identically the zero polynomial.

Proof: We proceed by induction on n, the number of variables. Recall that a univariate polynomial of degree at most d over F can have at most d zeros; this establishes the truth of the proposition for $n = 1$.

Suppose, for some $n \geq 1$, that the proposition is true for all polynomials of degree bounded by d in $F[x_1, \ldots, x_n]$. Let $f \in F[x_1, \ldots, x_{n+1}]$ have degree bounded by d, written as

$$f(x_1, \ldots, x_{n+1}) = \sum_{i=0}^{d} f_i(x_1, \ldots, x_n) x_{n+1}^i,$$

where $f_i \in F[x_1, \ldots, x_n]$ are polynomials of degree bounded by d. Suppose that $f(s_1, \ldots, s_{n+1}) = 0$ for all $(s_1, \ldots, s_{n+1}) \in S^{n+1}$. Then, in particular, each polynomial $f(s_1, \ldots, s_n, x_{n+1})$ in x_{n+1} (fixing $(s_1, \ldots, s_n)$) has at least $d+1$ zeros, and hence must identically be the zero polynomial. This implies that $f_i(x_1, \ldots, x_n) = 0$ for all $(s_1, \ldots, s_n) \in S^n$. By assumption, each such f_i must be identically the zero polynomial, which implies that f is identically the zero polynomial.

Thus if the proposition is true for $n \geq 1$ variables, it is also true for $n+1$ variables. Since the proposition is true if $n = 1$, by induction it follows that the proposition is true for all $n \geq 1$. ∎

Corollary: Let $f \in F[x_1, \ldots, x_n]$ be a polynomial of degree bounded by d. If f is not identically the zero polynomial, and if F has more than d elements, then $f(s_1, \ldots, s_n) \neq 0$ for some $(s_1, \ldots, s_n) \in F^n$.

In particular, if F is a finite field of q elements, then f must evaluate to a nonzero value in F_{q^m}, where m is the smallest value such that $q^m > d$.

Notes: The corollary is referred to as the "Sparse Zeros Lemma" in [1], in which the authors cite [2], [3] (see also [4]), and [5]. The terminology "Zippel's Lemma" follows from [6], where a version of the proposition (first?) appeared.

References

[1] C. Fragouli and E. Soljanin, "Network Coding Fundamentals," *Foundations and Trends in Networking*, volume 2, Issue 1, 2007.

[2] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, "Network Coding Theory: A Tutorial," *Foundations and Trends in Communications and Information Theory*, volume 2, 2006.

[3] N. J. A. Harvey, "Deterministic Network Coding by Matrix Completion," MS Thesis, 2005.

[4] N. J. A. Harvey, D. R. Karger, and K. Murota, "Deterministic Network Coding by Matrix Completion," *Proc. 16th Annual ACM-SIAM Symp. on Discrete Algorithms (SODA05)*, Vancouver, B.C., pp. 489–498, 2005.

[5] J. T. Schwartz, "Fast Probabilistic Algorithms for Verification of Polynomial Identities," *J. of the ACM*, vol. 27, pp. 701–717, 1980.

[6] R. E. Zippel, "Probabilistic Algorithms for Sparse Polynomials," *Lecture Notes in Computer Science*, vol. 72, pp. 216–226, Springer-Verlag, 1979.