Lecture 18:
PIT algorithm

Valentine Kabanets

November 25, 2016

1 Proof of the Schwartz-Zippel Lemma

We will prove the following.

Theorem 1 (Schwartz-Zippel Lemma)**.** *Let $p(x_1, ..., x_n)$ be any non-zero polynomial of total degree at most d. Let S be any finite set (of integers). Then $\mathbf{Pr}[p(r_1, ..., r_n) = 0] \leq d/|S|$, where the probability is over the independently randomly chosen values $r_1 \in S$, $r_2 \in S$,..., $r_n \in S$.*

Proof. The proof is a simple argument by induction on the number n of variables. The base case of univariate polynomials is easy. The inductive step uses the trick of viewing the polynomial in $(i + 1)$ variables $x_1, ..., x_{i+1}$ as the polynomial in the variable x_1 whose coefficients are themselves polynomials in the remaining variables $x_2, ..., x_{i+1}$. Let d_1 be the max degree of x_1 in this representation, and let $f_1(x_2, ..., x_{i+1})$ be the coefficient of x_1. Note that the degree of f_1 is at most $d - d_1$.

Consider the random event: $r_2, ..., r_{i+1}$ are such that $f_1(r_2, ..., r_{i+1}) = 0$. Call this event E. We have

$$\mathbf{Pr}[p(r_1, ..., r_{i+1}) = 0] = \mathbf{Pr}[p(r_1, ..., r_{i+1}) = 0 \mid E] \cdot \mathbf{Pr}[E] + \mathbf{Pr}[p(r_1, ..., r_{i+1}) = 0 \mid \text{ not } E] \cdot \mathbf{Pr}[\text{ not } E].$$

We upperbound the first term by $\mathbf{Pr}[E]$, which is, by Inductive Hypothesis, at most $(d-d_1)/|S|$. We upper bound the second term by $\mathbf{Pr}[p(r_1, ..., r_{i+1}) = 0 \mid \text{ not } E]$. Assume that $r_2, ..., r_{i+1}$ are chosen so that E doesn't hold. This means that $f_1(r_2, ..., r_{i+1}) \neq 0$. So, once $r_2, ..., r_{i+1}$ are chosen, we get that p is a univariate polynomial in x_1, of degree d_1 (since the coefficient of $x_1^{d_1}$ is non-zero). But then by the base case, we know that the probability this univariate polynomial is zero on a random $r_1 \in S$ is at most $d_1/|S|$.

Overall, the probability of $p(r_1, ..., r_{i+1}) = 0$ is at most $(d - d_1)/|S| + d_1/|S| = d/|S|$, as required. $\square$