The Schwartz-Zippel Lemma

Christopher Smith

April 15, 2024

Lemma 1 (Schwartz-Zippel). Let \( g \in F[x_1, \ldots, x_m] \) be an \( m \)-variate polynomial over a field \( F \) of total degree at most \( d \). Then, for any finite set \( S \subseteq F \),

\[
\Pr_{x \leftarrow S^m} [g(x) = 0] \leq \frac{d}{|S|}
\]

Proof. The proof is by induction on \( m \). Consider the base case \( m = 1 \) where \( g \in F[x] \), and let \( S \subseteq F \) be any finite set. We know \( g \) has at most \( d \) roots in \( F \), so \( S \) has at most \( d \) of these roots. Thus, \( \Pr_{x \leftarrow S}[g(x) = 0] \leq d/|S| \).

Now suppose the lemma is true for \( m - 1 \), and let \( g \in F[x_1, \ldots, x_m] \). The first trick is to rewrite \( g \) as

\[
g(x_1, \ldots, x_m) = \sum_{i=0}^{d} x_1^i g_i(x_2, \ldots, x_m)
\]

Because \( g \) is not identically zero, there must exist an \( i \) such that \( g_i(x_2, \ldots, x_m) \) is not identically zero. Let \( i^* \) be the largest such \( i \). Then \( \deg(x_1^i g_i(x_2, \ldots, x_m)) \leq d \), so \( \deg(g_i) \leq d - i^* \). By the induction hypothesis, we have that

\[
\Pr_{r_2,\ldots,r_m \leftarrow S_{m-1}} [g_i^*(r_2,\ldots,r_m) = 0] \leq \frac{d - i^*}{|S|}
\]

Consider the complementary case where \( g_i^*(r_2,\ldots,r_m) \neq 0 \). Notice that \( g(x_1, r_2, \ldots, r_m) \) is of degree \( i^* \), so applying the inductive hypothesis again we get

\[
\Pr_{r_1,\ldots,r_m \leftarrow S_m} [g(r_1,\ldots,r_m) = 0 \mid g_i^*(r_2,\ldots,r_m) \neq 0] \leq \frac{i^*}{|S|}
\]

Finally, using the total law of probability we get

\[
\Pr_{r_1,\ldots,r_m \leftarrow S_m} [g(r_1,\ldots,r_m) = 0] = \Pr[g(r_1,\ldots,r_m) = 0 \mid g_i^*(r_2,\ldots,r_m) = 0] \Pr[g_i^*(r_2,\ldots,r_m) = 0] + \\
\Pr[g(r_1,\ldots,r_m) = 0 \mid g_i^*(r_2,\ldots,r_m) \neq 0] \Pr[g_i^*(r_2,\ldots,r_m) \neq 0] \\
\leq \frac{d - i^*}{|S|} + \frac{i^*}{|S|} = \frac{d}{|S|}
\]

\( \Box \)