Lecture 08

Earlier...

The following upper bound on discrepancy was used

1 Lemma (Discrepancy Bound). $f : X \times Y \to \{1, -1\}$, $\mu \sim X \times Y$.

$$\mathsf{Disc}_\mu(f)^2 \leq |X| \sum_{y,y' \in Y} \left| \sum_{x \in X} \mu(x, y)\mu(x, y')f(x, y)f(x, y') \right|$$

to prove:

2 Theorem (Degree/Discrepancy theorem). Let $\mathsf{deg}_\pm(f) = d \geq 1$. Let $N \geq n$, and define $F(x, S) = f(x|_S)$ with $x \in \{1, -1\}^N$ and $S \in \binom{N}{n}$. Then

$$\mathsf{Disc}_\mu(F) \leq \left(\frac{4en^2}{Nd}\right)^{d/2} \qquad (\leq 2^{-d/2} \text{ for } N \geq n^2/d).$$

Today we provide an AC^0 function with threshold-degree $\Omega(\sqrt{n})$.

Finishing up

To finish, we prove the following classical result:

3 Theorem (Minsky & Papert, 1967). The function

$$f(\bar{x}) = \bigwedge_{i\in[m]} \bigvee_{j\in[4m^2]} x_{i,j}$$

(is in AC^0, and) has $\mathsf{deg}_{\pm}(f) > m$.

Proof. Let $M = 4m^3$. First we observe that the function is very symmetrical. Indeed, consider the subgroup $G = (\mathbb{S}_{4m^2})^m \subset \mathbb{S}_M$ of permutations of i, j which leave the i fixed, i.e., if $\sigma \in G$, then $\sigma(i,j) = (i, \sigma_i(j))$ for some choice of $\sigma_1, \ldots, \sigma_m \in \mathbb{S}_{4m^2}$. Then f is invariant under G.

Now suppose that $\mathsf{deg}_{\pm}(f) \le d$; then

$$f(\bar{x}) = \left[\sum_{S\in\binom{M}{\le d}} \alpha_S \chi_S(\bar{x}) > 0\right]$$

Where $\chi_S(\bar{x})$ is the AND of the S-coordinates: $\bigwedge_{(i,j)\in S} x_{i,j} \in \{0,1\}$ (we could have picked any basis, this one will be the most convenient).

Let $X_i = \{x_{i,1}, \ldots, x_{i,4m^2}\}$, For a given $x \in \{0,1\}^M$, let $y_1(x), \ldots, y_m(x)$ be given by $y_i = |x \cap X_i|$. Now call $S, T \in \binom{M}{\le d}$ *equivalent* if $y_i(S) = y_i(T)$ for all i.[1] Split $\binom{M}{\le d}$ into equivalence classes $B_1, \ldots, B_K$. Then the B_k are generated by G (meaning that $G(S) = B_k$ for any $S \in B_k$).

It also happens that

$$\sum_{S\in B_k} \chi_S(\bar{x}) = \binom{y_1(x)}{y_1(B_k)} \cdots \binom{y_m(x)}{y_m(B_k)} = p_k(y_1(x), \ldots, y_m(x)).$$

Because $\sum_i y_i(B_k) \le d$ always, then p_k is a real polynomial on the variables $y_i(x)$, having *total* degree $\le d$.

Now, by the G-invariance of f,

$$f(\bar{x}) = \left[\sum_{\sigma\in G} \sum_{S\in\binom{M}{\le d}} \alpha_S \chi_S(\sigma(\bar{x})) > 0\right]$$

[1] Here we treat subsets of M as binary strings of length M (and vice-versa), with the 1s marking the positions belonging to the set, and 0s elsewhere.

$$= \left[\sum_{B_k} \sum_{\sigma \in G} \sum_{S \in B_k} \alpha_S \chi_{\sigma^{-1}(S)}(\bar{x}) > 0 \right]$$

Because σ is bijective on B,

$$f(\bar{x}) = \left[\sum_{B_k} \sum_{\sigma \in G} \sum_{S \in B_k} \alpha_{\sigma(S)} \chi_S(\bar{x}) > 0 \right] = \left[\sum_{B_k} \sum_{S \in B_k} \left(\sum_{\sigma \in G} \alpha_{\sigma(S)} \right) \chi_S(\bar{x}) > 0 \right];$$

Now, because $G(S) = G(T) = B_k$ for any $S, T \in B_k$, the innermost parenthesis is some value β_k depending only on B_k. Hence:

$$f(\bar{x}) = \left[\sum_{B_k} \beta_k \left(\sum_{S \in B_k} \chi_S(\bar{x}) \right) > 0 \right],$$

and we conclude that

$$f(\bar{x}) = \left[\sum_{B_k} \beta_k p_k(y_1(\bar{x}), \ldots, y_m(\bar{x})) > 0 \right].$$

Let $q(y_1, \ldots, y_m) = \sum_{B_k} \beta_k p_k$, and write $y_i = y_i(\bar{x})$. Then q has degree $\leq d$, and

$$q(y_1, \ldots, y_m) > 0 \iff f(\bar{x}) = 1 \iff y_i > 0 \text{ for all } i.$$

Now, for any $y \in [2m]$, we can find a $\bar{x}$ having $y_i = (t - (2i+1))^2$. Then $q(y_1, \ldots, y_i) = Q(t)$, for some single-variate polynomial Q of degree $\leq 2d$. Now notice that for even $t \in [2m]$, $y_i = 0$ for $i = t/2 - 1$; and for odd $t \in [2m]$, $0 < y_i \leq 4m^2$ for all i. This implies that Q has degree at least $2m$ (its derivative has $2m - 1$ zeroes), so $2d \geq 2m$, and we are done. ■

☞ The idea of the proof is the following: we first notice that the output is a function q of the number of 1s in each of the X_1 (of the $y_i(\bar{x})$). If q were a polynomial in the y_i's, it would need to have "total degree" $\geq d$, by the $(t - (2i+1))^2$ argument of the last paragraph. The rest of the proof establishes that if f had small threshold degree, then q is, indeed, a small-degree polynomial.