Notes for Lecture 12
Malka Rosenthal

1 Overview

Lemma 1 *Let* $S \subseteq \{0,1\}^m \neq \emptyset$.
Let $w_1, \ldots, w_m$ *be chosen independently from* $\{0,1\}^m$ *at random.*
Let $S_0 = S$
$S_i = \{v \in S : v \cdot w_1 = \ldots = v \cdot w_i = 0 \pmod 2\}$
Then, $Prob(\exists i \leq m : |S_i| = 1) \geq 1/4$

We will use this lemma to prove the following:

Theorem 2 *ACC* $\subseteq$ *deterministic depth 2 circuits with symmetric gate at the root and* $2^{\log^{O(1)} n} \wedge$ *gates with fan-in* $\log^{O(1)} n$ *at level 1.*

2 Proof of Theorem using Lemma

The lemma can be translated into the following circuit:

- Bottom level: nm gates computing $i \cdot w_j$ for $0 \leq i \leq n$ and $0 \leq j \leq m$, where $m = \log n$ and the number i is represented as a binary string of length $\log n$.
  To compute $i \cdot w_j$, use $\wedge$ gates in each position to multiply $\bmod 2$ and then a parity gate to add mod2.

- Note the following:
  $S \subseteq \{0,1\}^m, m = \log n$ so we can interpret S as a subset of $[n]$ by associating to each $i \in [n]$, its binary representation $\in \{0,1\}^m$. For $S \subseteq [n]$, associate a vector $\vec{x} \in \{0,1\}^n$ with $x_i = 1 \Leftrightarrow i \in S$.
  Second Level: $n(m+1)$ gates (one for each $(a,k) : 0 \leq a \leq n, 0 \leq k \leq m$) computing the value:

  $$(x_a = 1) \wedge a \cdot w_i = 0 \text{ for } i \leq k,$$

  i.e. check if $a \in S_k$

- Third level: $m+1$ parity gates, one for each $k, 0 \leq k \leq m$, to compute $|S_k| \pmod 2$

- Top level: The $\vee$ of the previous gates: i.e. check $\exists k, |S_k| \equiv 1 \pmod 2$

The lemma translates to the following:

$$x_1 \vee \ldots \vee x_n = 1 (i.e. S \neq \emptyset) \Rightarrow Prob(\text{Circuit outputs } 1) \geq 1/4$$

and clearly,

$$x_1 \vee \ldots \vee x_n = 0 \Rightarrow \text{Circuit outputs } 0 \text{ (with probability 1)}.$$

If we now take $O(\log n)$ independent copies of this circuit and put an $\vee$ gate on top, we will get

$$(x_1 \vee \ldots \vee x_n = 1) \Rightarrow Prob(\text{Circuit outputs } 1) \geq 1 \Leftrightarrow \frac{1}{n^l}$$

for some l.
We have thus built a 5-level circuit which replaces $\vee$ gates with $\wedge$ gates of small fan-in and parity gates; this circuit has the same error probability as the construction of Lecture 6 but with fewer probabilistic bits.
Total number of probabilistic bits:

$$(l \log n)((\log n) \log n) = O(\log^3 n)$$

.

To finish the proof of the Theorem (using the Lemma):

1. Remove all $\wedge$ gates; replace with $\vee, \oplus$ gates.

2. Remove all mod$m$ gates where $m = p_1^{a_1} \cdots p_r^{a_r}$ and replace with mod $p_1, \ldots,$ modp_r

3. Replace all $\vee$ gates with $\oplus$ and $\wedge$ gates of small fan-in using $\log^{O(1)} n$ probabilistic bits (as in the Lemma).

4. Make $2^{\log^{O(1)} n}$ copies of this circuit and put a MAJ (majority) gate at the root to eliminate the probabilistic bits.

5. Reorganize the circuit by merging mod$p$ gates which are near the root into a symmetric gate and moving all $\vee$ gates to lowest level.

3 Proof of Lemma

3.1 Preliminaries

Definition 3 *A* hyperplane *is a set of the form* $\{v : v \cdot w = 0\} =: H_w$ *for some* w. *If* $w \neq 0^m$, *then the hyperplane,* H_w *is half of* $\{0,1\}^m$.

• The intersection of two hyperplanes is a subspace and thus has size 2^j for some j.
If $w_1, \ldots, w_l$ are linearly independent then $H_{w_1} \cap \cdots \cap H_{w_l}$ is a subspace of size 2^{m-l}.

Definition 4 *The* rank *of a set S is the smallest number of vectors $w_1, \ldots, w_l$ such that $S \subseteq \{\Sigma b_i w_i, b_i \in \{0,1\}^m\}$. WLOG, $\{w_1, \ldots, w_l\} \subseteq S$. The rank of $\{0^m\}$ is 0.*

Fact 1 *For any set of rank k spanned by $\{w_1, \ldots, w_k\}$, there is an $m \times m$ matrix M such that $Mw_i = e_i$ where e_i is the i^{th} standard basis vector. M^{-1} is defined so M defines a permutation (i.e. M is a one-to-one, onto map).*

Fact 2 *Let $w_1, \ldots, w_{m-1}$ be chosen independently at random.*
Then Prob(all w_i's are linearly independent) $\geq 1/2$.

Proof. There are

$2^m \Leftrightarrow 1$ choices for w_1
$2^m \Leftrightarrow 2$ choices for w_2,
$\vdots$
$2^m \Leftrightarrow 2^{m-2}$ choices for w_{m-1}

$$\begin{aligned} Prob(\text{ all } w_i\text{'s are linearly independent }) &= \prod_{i=2}^{m}(1 \Leftrightarrow \frac{1}{2^i}) \\ &\geq 1 \Leftrightarrow \sum_{i=2}^{m} \frac{1}{2^i} \qquad (1) \\ &\geq 1 \Leftrightarrow 1/2 \\ &= 1/2 \end{aligned}$$

where (1) follows by induction. ∎

Fact 3 *Let $w_1, \ldots, w_m$ be chosen independently at random. Then with probability $\geq 1/4$, they are all linearly independent.*

Note: If $0^m \in S$,then with probability $\geq 1/4, w_1, \ldots, w_m$ are linearly independent, which implies that $H_{w_1} \cap \cdots \cap H_{w_m} = \{0^m\}$ and therefore $|S_m| = 1$.
The other (more interesting) case is:

Lemma 5 *Let S have rank $k, 0^m \notin S$. Let w be chosen at random. Then,*

$$Prob(S \cap H_w \neq \emptyset | S \not\subseteq H_w) \geq \frac{2^k \Leftrightarrow 2}{2^k \Leftrightarrow 1}$$

Proof. Let S be given and assume first that S is spanned by $\{e_1, \ldots, e_k\} \subseteq S$. Then

$$S \not\subseteq H_w \Leftrightarrow w \text{ has a 1 somewhere in the first } k \text{ positions}$$

This is trivial as

$$e_i \cdot w = 1 \text{ for some } i \leq k \Leftrightarrow w \notin 0^k\{0,1\}^{m-k}$$

.
Thus there are $2^m \Leftrightarrow 2^{m-k}$ strings w such that $S \not\subseteq H_w$.
OTOH, If $w \notin 1^k\{0,1\}^{m-k}$, then $\exists i; e_i \in S \cap H_w$ and therefore $S \cap H_w \neq \emptyset$.
Thus, there $2^m \Leftrightarrow 2 \cdot 2^{m-k}$ strings w *s.t.* $S \cap H_w \neq \emptyset$ and $S \not\subseteq H_w$.
Therefore,

$$Pr(S \cap H_w \neq \emptyset | S \not\subseteq H_w) \geq \frac{\frac{2^m - 2 \cdot 2^{m-k}}{2^m}}{\frac{2^m - 2^{m-k}}{2^m}} = \frac{2^{m-k}(2^k \Leftrightarrow 2)}{2^{m-k}(2^k \Leftrightarrow 1)}$$

as required.
If S is not spanned by $\{e_1, \ldots, e_k\}$ then by Fact 1, there is some matrix, M, that maps a spanning set of S,$\{w_1, \ldots, w_k\}$ to $\{e_1, \ldots, e_k\}$. Consider Mw and MS; M is a permutation and linear and as such preserves the probabilities and maintains the properties of inclusion in the hyperplane. ∎

Lemma 6 *Let $S \subseteq \{0,1\}^m \neq \emptyset, 0^m \notin S$. Randomly choose $w_1, w_2, w_3, \ldots$. Let*
$S_0 = S$
$S_i = S \cap H_{w_1} \cap \cdots \cap H_{w_i}$.
Then $Pr(\exists i \in \mathcal{N} : |S_i| = 1) \geq 1/2$.

Proof. By induction on $rank(S) = k$,

$$Pr(\exists i \in \mathcal{N} : |S_i| = 1) \geq \frac{2^{k-1}}{2^k \Leftrightarrow 1} (\text{ which is,of course } \geq 1/2.)$$

Base Case: $k = 0$ is impossible as $0^m \notin S$.
$k = 1 : |S_0| = 1$
Inductive Step With probability 1, some w_i is chosen such that $rank(S_i) < k = rank(S_0)$. Consider the first such i and note that w_i is linearly independent with $w_1, \ldots, w_{i-1}$.
We have $rank(S_{i-1}) = k$ and $S_{i-1} \not\subseteq H_{w_i}$

[else, $S_{i-1} \cap H_{w_i} = S_{i-1}$ but $rank(S_i) = rank(S_{i-1} \cap H_{w_i}) < rank(S_{i-1})$.]

Therefore, by Lemma 3.1,

$$Prob(S_i \neq \emptyset) \geq \frac{2^k \Leftrightarrow 2}{2^k \Leftrightarrow 1} \tag{2}$$

By induction,

$$Prob(\exists j \in \mathcal{N} : |S_i \cap H_{w_{i+1}} \cap \cdots \cap H_{w_j}| = 1) \geq \frac{2^{k-2}}{2^{k-1} \Leftrightarrow 1} \tag{3}$$

. Combining (2) and (3), we get:

$$Prob(\exists i \in \mathcal{N} : |S_i| = 1) \geq (\frac{2^k \Leftrightarrow 2}{2^k \Leftrightarrow 1})(\frac{2^{k-2}}{2^{k-1} \Leftrightarrow 1}) = \frac{2^{k-1}}{2^k \Leftrightarrow 1}$$

∎

3.2 Proof of Lemma

Note that with Probability $\geq 1/2, w_1, \ldots, w_{m-1}$ are linearly independent and then $|S_{m-1}| \leq 1$
and $Prob(\exists i \leq m \Leftrightarrow 1 : |S_i| = 1 \mid w_1, \ldots, w_{m-1}$ are lin. indept. $) \geq 1/2$.
Therefore, with probability $\geq 1/4, \exists i \leq m \Leftrightarrow 1$ s.t. $|S_i| = 1$.