Circuit Complexity Notes

Bob Chen

Fall 2013

1 October 30 - Exponential lower bounds for Constant Depth Circuits for Parity — the Switching Lemma

Definition 1.1. Let $k \geq 1$. A k-CNF is a CNF formula where each conjunct is a disjunt of at most k literals. A k-DNF is defined dually.

Remark 1.2. Let $p \in [0,1]$. We can choose a random restriction $\rho : \{x_1, \ldots, x_m\} \to \{0, 1, \star\}$ by letting

$$\rho(x_i) = \begin{cases} \star & \text{probability } p \\ 1 & \text{probability } \frac{1-p}{2} \\ 0 & \text{probability } \frac{1-p}{2}. \end{cases}$$

Lemma 1.3. *(Switching; Hastad, 1984) Let F be a t-DNF. Let $p \in [0, \frac{1}{7}]$ and let ρ be chosen as above at random. Then with probability at least $1 - (5pt)^s$, $F \restriction \rho$ can be expressed as an s-CNF.*

Remark 1.4. The big picture: to get a lower bound on Parity, we're going to look at the bottom level of a constant depth circuit. Say it's an AND of ORs. If everything is small enough, then hit the bottom with the switching lemma, then collapse upwards. Eventually we'll get a contradiction, so in fact the circuit can't be too small.

Remark 1.5. Given $f(x_1, \ldots, x_n)$ and $l \leq n$, let R^l be the set of restrictions ρ for which $\rho(x_i) = \star$ for exactly l indices i. Hence the domain of ρ has size $n - l$. Let $p = \frac{l}{n}$.

Note that $|R^l| = \binom{n}{l} 2^{n-l}$ (note of course that it also depends on n).

Definition 1.6. A *minterm* for f is a restriction ρ such that $f \restriction \rho$ is the constant function 1, but for which no subrestriction $\rho' \subsetneq \rho$ has $f \restriction \rho' \equiv 1$. (Often we write a minterm as a conjunction of literals that are set to 1 in ρ, e.g. $x_1 \wedge \overline{x_4} \wedge x_6$ is the minterm that sets x_1, x_6 to 1 and x_4 to 0.)

We define $min(f)$ = the maximum *size* of a minterm of f (the size of a restriction is the size of the domain).

Remark 1.7. Observe that

$$f \equiv \bigvee \{\tau \mid \tau \text{ is a minterm of } f\}.$$

Also, f is expressible by a s-DNF if and only if $min(f) \leq s$.

Lemma 1.8. *(Switching, version 2.) (Proof due to Razborov, see also* [1]*)*
Let f be a t-CNF Let $\rho \in R^l$ be chosen at random with $p = \frac{l}{n}$ (assume $p < \frac{1}{2}$). Then the probability that $min(f \restriction \rho) > s$ is at most $(16pt)^s$; hence f is an s-DNF with probability at least $1 - (16pt)^s$.

Definition 1.9. $BAD_f(l, s)$ is the set of $\rho \in R^l$ such that $\min(f \restriction \rho) > s$.

Lemma 1.10. *(Bad.)* $|BAD_f(l, s)| \leq |R^{l-s}|(4t)^s$.

Proof. Express f as $F_1 \wedge F_2 \wedge \cdots$, where each F_i is a disjunction of at most t literals.

We'll construct an injective mapping

$$CODE : BAD_f(l, s) \to R^{l-s} \times S$$

where $|S| \leq (4t)^s$.

Suppose $\rho \in BAD_f(l, s)$. Fix a minterm π of $f \restriction \rho$ of size bigger than s. We know that $f \restriction \rho\pi \equiv 1$, but we also know that $f \restriction \rho \not\equiv 1$ (because π has nonzero size).

What do $F_i \restriction \rho, \rho\pi$ look like? We must have $F_i \restriction \rho\pi \equiv 1$ because some $x \in F_i$ is 1 under ρ or π. On the other hand, $F_i \restriction \rho$ is never all 0s.

Choose a clause C_1 to be the first F_i for which $F_i \restriction \rho \not\equiv 1$ (such a clause must exist). Let π_1 be π restricted to the variables in C_1. (This is nonempty since $\pi(x) = 1$ for some $x \in C_1$.)

Now let $\overline{\pi_1}$ be π_1 modified to send all of its (possibly negated) literals to 0. Let $a_1 \in \{0, 1\}^t$ be the indicator vector of which of the t variables $x \in C_1$ are in the domain of π.

Repeat this with $\rho\pi_1$ in place of ρ and $\pi \setminus \pi_1$ in place of π. Pick C_2 to be the next F_i such that blah blah is true (as before). Repeat $k \leq s$ times until the domain of $\pi_1 \cdots \pi_k$ has size s. (Make sure π_k is truncated so that the domain is exactly s.)

Let $b \in \{0, 1\}^s$ give the value of $\prod \pi_i$ on the s members of its domain. Now all we have to do is define

$$CODE(\rho) := (\rho\overline{\pi_1} \cdots \overline{\pi_k}, a_1, \ldots, a_k, b).$$

Note that C_1 is now the first F_i for which

$$F_i \restriction \rho\overline{\pi_1} \cdots \overline{\pi_k} \equiv 0.$$

[1] Håstad, Johan (1987), Computational limitations of small depth circuits, Ph.D. thesis, Massachusetts Institute of Technology.

Razborov, Alexander A. (1993), "An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic", Arithmetic, proof theory and computational complexity 23: 247277.

Beame, Paul (1994), "A Switching Lemma Primer", Unpublished manuscript.

Using a_1 and C_1 we can determine the domain of π_1, and b tells us what this value needs to be. Hence we can back out ρ from $CODE(\rho)$, so that $CODE$ is injective.

It remains to show that $|S| \leq (4t)^s$, where S is the set of possible values for a_i and b. There are 2^s many bs. Each a_i has s_i many 1s, and $\sum s_i = s$. There are

$$\prod_{i=1}^{k} \binom{t}{s_i} \leq \prod t^{s_i} = t^s$$

many ways to choose various combinations of a_i (for a fixed $k, \{s_i\}$). But we can code the choices of s_i as the string

$$10^{s_1-1}10^{s_2-1}\cdots \in \{0,1\}^s .$$

Hence there are 2^{s-1} ways to choose these parameters.

Altogether we have $|S| \leq 2^s 2^{s-1} t^s \leq (4t)^s$, as desired. □

Proof. (Of the Switching Lemma v2.) The probability in question is just

$$\begin{aligned}
P[\min(f \restriction \rho) > s] &= \frac{|BAD_f(l,s)|}{|R^l|} \\
&= \frac{|R^{l-s}|(4t)^s}{|R^l|} \\
&= \frac{\binom{n}{l-s}2^{n-l+s}(4t)^s}{\binom{n}{l}2^{n-l}} \\
&= \frac{(n-l)!}{(n-l+s)!}\binom{l!}{(l-s)!}2^s 4^s t^s \\
&\leq \left(\frac{l}{n-l}\right)^s (8t)^s \\
&= \left(\frac{p}{1-p}8t\right)^s \\
&\leq (16pt)^s,
\end{aligned}$$

as desired. □