

Notes for Lecture 3
Martin Strauss

1 Preliminaries

Definition 1 A literal is a variable or the negation of a variable. A boolean expression ϕ is in disjunctive normal form if ϕ is the \vee of \wedge 's of literals, and conjunctive normal form if ϕ is the \wedge of \vee 's.

Definition 2 A leveled circuit is a circuit in which each path from input to output is the same length and consists of alternating \wedge - and \vee - gates.

Definition 3 A restriction of a set $\{x_1, \dots, x_n\}$ of variables is an assignment $\rho : \{1, \dots, n\} \rightarrow \{0, 1, *\}$. For a boolean formula ϕ and restriction ρ , let $\phi|_\rho$ denote ϕ with x_i instantiated by $\rho(i)$ if the latter is 0 or 1, and x_i free otherwise. Let R^l denote the set of restrictions leaving l variables free (the total number n of variables will be understood).

2 Switching Lemma

In this section give a proof of the Håstad Switching Lemma [1]. The proof is due to Razborov [3], expressed in terms of Kolmogorov complexity by Lance Fortnow, and published by Laplante [2].

We will prove a slightly different form of the switching lemma. We ultimately will prove statement C below, after showing that statement C implies statement B, and statement B implies the switching lemma H. The following statements all have the same form:

There exists a c such that for all $n, s, t \dots$ any leveled \wedge - \vee circuit with parameters c, n, s, t (suitably restricted) is equivalent to an \vee - \wedge circuit with small bottom fan-in.

- C There exists c such that for all n , all t and all n -ary $f = \bigwedge_i D_i$ where each D_i is the disjunct of at most t literals, for all $0 < s < l < n$, and all $\rho \in R^l$, if

$$K(\rho|f, l, s) > \log \binom{n}{l-s} + n - l + s \log 8t + c$$

then $f|_\rho = \bigvee_j C_j$, where each C_j is the conjunct of at most s literals.

- B There exists c such that for all n, t, m , all n -input leveled circuit families C_n of bottom fan-in at most t and at most m \wedge -gates at level 2, and all $0 < s < l$, if

$$K(\rho|C, l, s) > \log \binom{n}{l-s} + n - l + s \log 8t + \log m + c,$$

then each \wedge -gate on level 2 of C can be expressed as an \vee of \wedge 's of size at most s .

H There exists c such that for all n, t, m , all $0 < s < l$, with

$$\left(\frac{n-l+s}{8tl}\right)^s \geq 2^c m,$$

all Kolmogorov-random $\rho \in R^l$, and all n -input leveled circuits with bottom fan-in at most t and m \wedge -gates at level 2, each \wedge -gate in level 2 can be replaced by an \vee of \wedge 's, where each \wedge has fan-in at most s .

First we show that statement B implies the switching lemma. Suppose C, n, s, l, t satisfy the hypotheses of the switching lemma, and suppose

$$K(\rho|C, l, s, n, t) \geq \log |R^l|.$$

We need to show that the hypotheses of B are satisfied. We then have the conclusion of B which is the same as the conclusion of the switching lemma.

Lemma 4 *Statement B implies the switching lemma.*

Proof. We have

$$\begin{aligned} K(\rho|C, l, s, n, t) &\geq \log |R^l| \\ &= \log \left(\binom{n}{l} 2^{n-l} \right) \\ &\geq \log \left(\binom{n}{l-s} \left(\frac{n-l+s}{l} \right)^s 2^{n-l} \right) \quad (1) \\ &\geq \log \left(\binom{n}{l-s} \left(\frac{n-l+s}{8tl} \right)^s 2^{n-l} \right) + s \log 8t \\ &\geq \log \left(\binom{n}{l-s} cm 2^{n-l} \right) + s \log 8t \quad (2) \\ &\geq \log \binom{n}{l-s} + c' + \log m + (n-l) + s \log 8t \end{aligned}$$

Here in (1) we've used the identity

$$\frac{\binom{n}{l}}{\binom{n}{l-s}} = \frac{(n-l+s)!/(n-l)!}{l!/(l-s)!} \geq \left(\frac{n-l+s}{l} \right)^s,$$

and in (2) we've used the hypotheses of the switching lemma. ♣

Next we show that statement C implies statement B. Note that statement C concerns functions in normal form, whereas statement B concerns leveled circuits, and has a $\log m$ term in the hypotheses, where we recall m is the number of gates in the second level.

Lemma 5 *Statement C implies statement B.*

Proof. Let C be the circuit of statement B, and assume some second-level \wedge -gate in $C|_\rho$ is not expressible as an \vee of small \wedge 's. Let f be the function computed by that gate. Since C has at most m gates at level 2, we have

$$K(\rho|C, l, s) \leq K(\rho|f, l, s) + \log m + O(1).$$

(A few words are in order concerning the inequality

$$K(\rho|C, l, s) \leq K(\rho|f, l, s) + \log m + O(1).$$

Let $\bar{z}w$ be a description of ρ in terms of f, l, s . The description of ρ in terms of C, l, s is a string of the form $\bar{x}j\bar{z}w$, where \bar{x} is a self-delimiting string of instructions, saying to compute the number m' of AND gates in level 2 of C , and to consider the next $\log m'$ bits as a string $j \leq m$, and compute the truth-table corresponding to the function f computed at the j th AND gate in C . Then use $\bar{z}w$ to compute ρ from f, l, s . ♣

Now we prove statement C.

Lemma 6 (Håstad) *Statement C of Håstad's switching lemma holds.*

Proof. Let f, l, s, n, t, ρ be as in the hypothesis. We'll show that if the disjunctive normal form of $f|_\rho$ contains a conjunct C_j with at least $s + 1$ literals then $K(\rho|f, l, s) \leq \binom{n}{l-s} + n - l + s \log 8t + c$.

The strategy is to construct $\rho' \in R^{l-s}$ extending ρ (i.e., fixing more variables), such that $K(\rho|\rho', f, l, s)$ is small compared to $K(\rho')$. Note that $K(\rho')$ is always small:

$$\begin{aligned} K(\rho') &\leq \log |R^{l-s}| + O(1) \\ &= \log \binom{n}{l-s} + n - l + s + O(1) \\ &\ll \log \binom{n}{l} + n - l \\ &= \log |R^l| \\ &\approx K(\rho) \end{aligned}$$

if $n + s \gg 3l$.

At first it seems that an extension ρ' of ρ ought to have *greater* complexity than ρ . The strategy succeeds since the positions of fewer $*$'s need to be specified in the extension.

For a restriction π , let $\text{Dom}(\pi)$ denote $\pi^{-1}(\{0, 1\})$, i.e., the variables set by π . For $S \subseteq \{1, \dots, n\}$, let $\pi|_S$ denote the restriction

$$\pi|_S(i) = \begin{cases} *, & i \notin S; \\ \pi(i) & i \in S \end{cases}$$

For a boolean expression ϕ , we will sometimes write $\pi(\phi)$ for $\phi|_\pi$.
 Suppose f is of the form $\bigwedge_i D_i$, and

$$f|_\rho = \bigvee_j C_j,$$

where some C_j has at least $s + 1$ literals. Then

$$f|_\rho = \bigwedge_i \rho(D_i) = \bigwedge_i D'_i,$$

where each D'_i is defined naturally and satisfies

$$D'_i \begin{cases} = 1 & \rho(D_i) = 1 \\ \subseteq D_i & \rho(D_i) = * \\ = 0 & \rho(D_i) = 0 \end{cases}$$

Let π be the unique minimal restriction satisfying C_j . Thus, in particular, π makes $f|_\rho = \bigvee_j C_j$ true, and since $f|_\rho = \bigwedge_i D'_i$, π makes each D'_i true, and $\pi\rho$ makes each D_i true, where $\pi\rho D_i$ means “set literals in D_i according to ρ , then set the remaining free literals according to π .”

Note there exists some i with $D'_i \neq 1$, since otherwise $f|_\rho = 1$, and hence $f|_\rho$ would have a DNF with all conjuncts smaller than $s + 1$. Let

$$i_1 = \min\{i : D'_i \neq 1\} = \min\{i : \rho D_i \neq 1\}.$$

Let

$$S_1 = D'_{i_1} \cap \text{Dom}(\pi) = (D_{i_1} \setminus \text{Dom}(\rho)) \cap \text{Dom}(\pi) \neq \emptyset.$$

This set is not empty since D_{i_1} is not determined by ρ but is determined by $\pi\rho$.

Let $\pi_1 = \pi|_{S_1}$. That is, π_1 is the part of the restriction $\pi\rho$ not contained in ρ . Thus $\pi_1\rho = \rho\pi_1$.

Define $\tilde{\pi}_1$ to “inflict maximum damage” to D_{i_1} :

$$\tilde{\pi}_1(i) = \begin{cases} * & i \notin S_1 \\ 1 & \text{“}\bar{x}_i\text{”} \in D_{i_1} \\ 0 & \text{“}x_i\text{”} \in D_{i_1} \end{cases}$$

Thus:

- $\text{Dom}(\pi_1) = \text{Dom}(\tilde{\pi}_1)$, and $\text{Dom}(\pi_1) \cap \text{Dom}(\rho) = \emptyset$.
- $\pi_1 \neq \tilde{\pi}_1$, since $\pi_1\rho(D_{i_1}) = 1$ and $\tilde{\pi}_1\rho(D_{i_1}) \neq 1$.
- $\rho(D_{i_1}) = *$.
- $\forall l < i_1 \rho(D_l) = 1$.

- $\forall l < i_1 \rho_{\tilde{\pi}_1}(D_l) = 1.$
- For any setting π' of the literals in $\text{Dom}(\pi) \setminus \text{Dom}(\tilde{\pi}_1)$, we have

$$\begin{cases} \rho_{\tilde{\pi}_1}\pi'(D_{i_1}) \in \{0, 1\} \\ \forall l < i_1 \rho_{\tilde{\pi}_1}\pi'(D_l) = 1. \end{cases}$$

⋮

■

References

- [1] J. Håstad. Almost optimal lower bounds for small depth circuits. In S. Micali, editor, *Randomness and Computation*, pages 143–170. JAI Press, 1989.
- [2] S. Laplante. A Kolmogorov complexity proof of Håstad’s switching lemma. Technical Report CS 94-03, University of Chicago, March 1994.
- [3] A. Razborov. Bounded arithmetic and lower bounds in boolean complexity. Manuscript.