The multi-switching lemma (lecture notes)

Course: Circuit Complexity, Autumn 2024, University of Chicago
Instructor: William Hoza (`williamhoza@uchicago.edu`)

---

1 The multi-switching lemma

In these lecture notes, we prove the "multi-switching lemma." This powerful lemma is a generalization of the switching lemma, and it turns out to be the key to proving the AC^0 Criticality Theorem that we discussed previously.

Lemma 1 (The Multi-Switching Lemma)**.** *Let $C_1, \dots, C_S$ be width-w DNF formulas, let $p \in (0,1)$ and let $D \in \mathbb{N}$. Sample $\rho \sim R_p$. Then except with probability $O(pw)^D$, there exist decision trees $T_{C_1,\rho}, \dots, T_{C_S,\rho}$ of depth at most $D - 1 + \log S$ computing $C_1|_\rho, \dots, C_S|_\rho$, such that the first $D-1$ queries made by $T_{C_i,\rho}$ do not depend on i.*

The standard switching lemma is the case $S = 1$. The failure probability bound is usually stated as $S \cdot O(pw)^D$, but we will prove the stronger bound $O(pw)^D$.

The proof of the multi-switching lemma builds on the proof of the standard switching lemma. Let $\mathsf{CDT}_{C_i,\rho}$ denote the canonical decision tree for $C_i|_\rho$ (see the switching lemma lecture notes). Let $q = \lfloor \log S \rfloor$, and let $i_* \in [S]$. Let A_ρ denote the following decision tree, which makes queries to $x \in \{0,1\}^n$ and outputs $\pi \in \{0,1,\star\}^n$:

1. Let $\pi^{(1)} = \rho$. For $t = 1, 2, 3, \dots$:
   (a) Let $i_t \in [S]$ maximize $d_t := \mathsf{Depth}(\mathsf{CDT}_{C_{i_t},\pi^{(t)}})$.
   (b) If $d_t \leq q$, then halt and output $\pi^{(t)}$. Otherwise:
   (c) Let Q_t be the set of variables queried on the first length-(d_t) path of $\mathsf{CDT}_{C_{i_t},\pi^{(t)}}$.
   (d) For every $j \in Q_t$, query x_j, and let

$$\pi_j^{(t+1)} = \begin{cases} \pi_j^{(t)} & \text{if } j \notin Q_t \\ x_j & \text{if } j \in Q_t. \end{cases}$$

The tree $T_{C_i,\rho}$ computes $\pi = A_\rho(x)$ and then simulates $\mathsf{CDT}_{C_i,\pi}$. To bound the depth of A_ρ, we will design a strategy for guessing many points in $\rho^{-1}(\star)$ given only a uniform random completion y of ρ. Let $d \in \mathbb{N}$, and let $\mathsf{StarGuesser}_{C_i,d}$ denote the strategy for guessing stars that we used when we proved the switching lemma (see the switching lemma lecture notes). Our new star guessing strategy, denoted $\mathsf{MultiStarGuesser}_d$, is as follows.

1. Pick $x \in \{0,1\}^n$ uniformly at random.
2. Pick a decomposition of d into positive integers, $d = \widehat{d}_1 + \widehat{d}_2 + \dots + \widehat{d}_r$, uniformly at random.
3. Initialize $z \leftarrow y$. For $t = 1, 2, \dots, r$:
   (a) Pick a term $\widehat{i}_t \in [S]$ uniformly at random.
   (b) Compute $\widehat{Q}_t = \mathsf{StarGuesser}_{C_{\widehat{i}_t},\widehat{d}_t}(z)$.
   (c) For every $j \in \widehat{Q}_t$, set $z_j \leftarrow x_j$.
4. Output $\widehat{Q}_1 \cup \dots \cup \widehat{Q}_r$.

We rely on the following fact about $\mathsf{StarGuesser}$.

Claim 1 (Correctness of $\mathsf{StarGuesser}$). *Let C be a width-w DNF, let $d \in \mathbb{N}$, let ρ be a restriction such that $\mathsf{Depth}(\mathsf{CDT}_{C,\rho}) = d$, and let Q be the set of variables queried on the first length-d path of $\mathsf{CDT}_{C,\rho}$. There exists a string $z^*_{C,\rho} \in \{0,1\}^Q$ such that for every completion z of ρ satisfying $z_Q = z^*_{C,\rho}$,*

$$\Pr[\mathsf{StarGuesser}_d(z) \text{ outputs } Q] \geq \frac{1}{O(w)^d},$$

where the probability is with respect to only the internal randomness of $\mathsf{StarGuesser}_d$.

We implicitly proved Claim 1 in the lecture notes on the switching lemma. Now let us use Claim 1 to prove the correctness of $\mathsf{MultiStarGuesser}_d$.

Claim 2 (Correctness of $\mathsf{MultiStarGuesser}_d$). *Let $\mathsf{MultiWin}_d$ denote the event that $\mathsf{MultiStarGuesser}_d(y)$ outputs d distinct points, each of which is in $\rho^{-1}(\star)$. Then*

$$\Pr[\mathsf{MultiWin}_d \mid \mathsf{Depth}(\mathsf{A}_\rho) = d] \geq \frac{1}{O(w)^d}.$$

(The probability above is with respect to the random choices of ρ and y and the internal randomness of $\mathsf{MultiStarGuesser}_d$.)

Proof. Fix any choice of ρ such that $\mathsf{Depth}(\mathsf{A}_\rho) = d$. With probability at least 2^{-d+1}, the strategy $\mathsf{MultiStarGuesser}_d$ picks an input $x \in \{0,1\}^n$ on which A_ρ makes d queries. Fix any such x. Let $i_1, i_2, \dots, i_r \in [S]$ be the DNFs visited by A_ρ on x, let $Q_1, Q_2, \dots, Q_r$ be the sets of variables queried when visiting those DNFs, and let $\rho = \pi^{(1)}, \pi^{(2)}, \dots, \pi^{(r)}$ be the restrictions used to define the canonical decision tree in those iterations.

With probability 2^{-d+1}, the strategy $\mathsf{MultiStarGuesser}_d$ chooses $\widehat{d}_t = |Q_t|$ for every $t \in [r]$. Assume this occurs. With probability 2^{-d}, we choose a completion y of ρ such that for every $t \in [r]$, we have $y_{Q_t} = z^*_{C_{i_t}, \pi^{(i_t)}}$, where $z^*_{C_{i_t}, \pi^{(i_t)}}$ is the string from Claim 1. Assume that this occurs.

With probability $1/S^r$, the strategy $\mathsf{MultiStarGuesser}_d$ chooses $\widehat{i}_t = i_t$ for every $t \in [r]$. Assume that this occurs. Then, with respect to the internal randomness of $\mathsf{StarGuesser}_{\widehat{d}_t}$, with probability at least $1/O(w)^d$, we get $\widehat{Q}_t = Q_t$ for every t, and hence $\mathsf{MultiWin}_d$ occurs.

The tree A_ρ makes at least q queries in each iteration, so $r \leq d/q$. Therefore, our overall success probability is at least

$$\frac{1}{2^d} \cdot \frac{1}{2^d} \cdot \frac{1}{2^d} \cdot \frac{1}{S^{d/q}} \cdot \frac{1}{O(w)^d} = \frac{1}{O(w \cdot S^{1/q})^d}.$$

Finally, recall that $q = \lfloor \log S \rfloor$, so $S^{1/q} \leq 2$. □

Proof of the Multi-Switching Lemma (Lemma 1). For each $d \in \mathbb{N}$, we have

$$\frac{1}{O(w)^d} \leq \Pr[\mathsf{MultiWin}_d \mid \mathsf{Depth}(\mathsf{A}_\rho) = d] \leq \frac{\Pr[\mathsf{MultiWin}_d]}{\Pr[\mathsf{Depth}(\mathsf{A}_\rho) = d]} \leq \frac{p^d}{\Pr[\mathsf{Depth}(\mathsf{A}_\rho) = d]},$$

where the last step uses the fact that the output of $\mathsf{MultiStarGuesser}_d$ is independent of $\rho^{-1}(\star)$. Rearranging, we get $\Pr[\mathsf{Depth}(\mathsf{A}_\rho) = d] \leq O(pw)^d$. Therefore,

$$\Pr[\mathsf{Depth}(\mathsf{A}_\rho) \geq D] \leq \sum_{d=D}^{\infty} \Pr[\mathsf{Depth}(\mathsf{A}_\rho) = d] \leq \sum_{d=D}^{\infty} O(pw)^d \leq O(pw)^D.$$ □