Boolean function complexity

Lecturer: *Nitin Saurabh* Meeting: 9
Scribe: *Nitin Saurabh* 19.06.2019

In this lecture we see Håstad's *switching lemma*. Since in the class we saw exactly the same presentation as in Beame's survey on switching lemmas. I attach the appropriate section from this survey as notes.

is that, whereas in the conditional probability argument the conditioning on the value of an arbitrary function being forced to 0 forces one to allow the number of unset variables to vary, in the counting argument it is actually advantageous to fix the number of unset variables.

In the following, we present the arguments for several switching lemmas for varied probability distributions, some of which require new variations on the structure of the counting argument. Razborov followed Håstad's original proof by showing that with high probability a DNF formula with short terms has only short maxterms after restriction.

In fact, Håstad's argument, as is the case with many of the switching lemma arguments mentioned above, more naturally proves a statement of the form that with high probability a DNF formula with short terms has a small height decision tree after restriction. This is a slightly stronger statement than the standard switching lemma phrasing since a small height decision tree allows one to obtain a short DNF formula for the negation of the formula which is essentially what is desired. This formulation of a switching lemma was first used by Cai [Cai86]. Several authors have subsequently noted that Håstad's argument also works in this fashion.

We modify Razborov's argument to prove results about decision trees, in part because it produces a more natural argument but also because in the case of the q-matching restrictions described in section 5 it is not clear how one could adapt Razborov's argument to the analogue of maxterms.

2 Decision tree version of the Håstad switching lemma

A *restriction* on a set of Boolean variables $\{x_i \mid i \in I\}$ is a map $\rho : I \to \{0, 1, *\}$. The result of its action on a Boolean function f is a Boolean function $f\lceil_\rho$ which is the result of substituting $\rho(i)$ for x_i for all places where $\rho(i) \neq *$. We say that all variables x_i such that $\rho(i) = *$ are *unset* and the resulting function becomes a function of the unset variables in the obvious way.

Define $\mathcal{R}_n^\ell$ to be the set of all restrictions ρ on a domain of n variables that have exactly ℓ unset variables. Håstad's switching lemma states that for any function f that is representable in disjunctive normal form (DNF) with short terms, then for almost all restrictions $\rho \in \mathcal{R}_n^\ell$, $f\lceil_\rho$ has a small height decision tree.

Fix some function f representable as a DNF formula F and assume that there is a total order on the terms of F as well as on the indices of the variables. A restriction ρ is applied to F in order, so that $F\lceil_\rho$ is the DNF formula whose terms consist of those terms of F that are not falsified by ρ, each shortened by removing any variables that are satisfied by ρ, and taken in the order of occurrence of the original terms on which they are based.

The *canonical decision tree for* F, $T(F)$ is defined inductively as follows:

1. If F is the constant function 0 or 1 (contains no terms or has an empty first term, respectively) then $T(F)$ consists of a single leaf node labelled by the appropriate constant value.
2. If the first term C_1 of F is not empty then let F' be the remainder of F so that $F = C_1 \vee F'$. Let K be the set of variables appearing in C_1. The tree $T(F)$ starts with a complete binary tree for K, which queries the variables in K in the order induced by the order on the indices. Each leaf v_σ in the tree is associated with a restriction σ which sets the variables of K according to the path from the root to v_σ. For each σ we replace the leaf node, v_σ, by the subtree $T(F\lceil_\sigma)$. (Note that for the unique σ which satisfies C_1 the leaf v_σ will remain a leaf and be labelled 1. For all other choices of σ, the tree that replaces v_σ is $T(F\lceil_\sigma) = T(F'\lceil_\sigma)$.)

We'll show that for any DNF formula F, for an appropriately chosen restriction ρ, the height of $T(F\lceil_\rho)$, $|T(F\lceil_\rho)|$, is small with high probability. This lemma is a switching lemma in the spirit of [Hås87] because it will allow us to obtain a DNF formula with short terms for $\neg F\lceil_\rho$ by taking the terms corresponding to the paths in $T(F\lceil_\rho)$ that have leaf labels 0. (We do not optimize the constants here. For improved constants see the discussion at the end of this section.)

Lemma 1: (Håstad Switching Lemma) Let F be a DNF formula in n variables with terms of length at most r. For $s \geq 0$, $\ell = pn$, and $p \leq 1/7$,

$$\frac{|\{\rho \in \mathcal{R}_n^\ell \ : \ |T(F\lceil_\rho)| \geq s\}|}{|\mathcal{R}_n^\ell|} < (7pr)^s.$$

The proof of this switching lemma is a small modification of Razborov's simplified proof of Håstad's switching lemma and uses a counting argument rather than complicated reasoning involving conditional probability. The property of the restriction family that is critical to the argument was clearly necessary in Håstad's argument but is implicit here: For any assignment of values to a set of variables and any s, it is exponentially more likely in s that a randomly chosen restriction agrees with the assignment than that it leaves s variables unset.

Before giving the proof of the switching lemma we give the following definition. Let $stars(r, s)$ to be the set of all sequences $\beta = (\beta_1, \ldots, \beta_k)$ such that for each j, $\beta_j \in \{*, -\}^r \setminus \{-\}^r$ and such that the total number of *'s in all the β_j is s. There is an easy bound of $|stars(r, s)| \leq 2^{s-1}r^s$ but we can also prove:

Lemma 2: $|stars(r, s)| < (r/\ln 2)^s$.

Proof For convenience in the proof we shall include the empty string in $stars(r,0)$ which would otherwise be empty. We shall show by induction on s that $|stars(r,s)| \leq \gamma^s$ for $(1+1/\gamma)^r = 2$; the statement of the lemma follows by using $1+x < e^x$ for $x \neq 0$.

The base case $s=0$ follows trivially. Now suppose that $s > 0$. It is easy to see from the definition that for any $\beta \in stars(r,s)$, if β_1 has $i \leq s$ *'s then $\beta = (\beta_1, \beta')$ where $\beta' \in stars(r, s-i)$. (For $i = s$ we have used our augmentation of $stars(r,0)$.) There are $\binom{r}{i}$ choices of β_1 so

$$\begin{aligned} |stars(r,s)| &= \sum_{i=1}^{\min(r,s)} \binom{r}{i} |stars(r, s-i)| \\ &\leq \sum_{i=1}^{r} \binom{r}{i} \gamma^{s-i} \\ &= \gamma^s \sum_{i=1}^{r} \binom{r}{i} (1/\gamma)^i \\ &= \gamma^s[(1+1/\gamma)^r - 1] \\ &= \gamma^s \end{aligned}$$

by the inductive hypothesis and the definition of γ. □

Proof (Håstad Switching Lemma) We only need to consider $s > 0$. Let $S \in \mathcal{R}_n^\ell$ be the set of restrictions ρ such that $|T(F\lceil_\rho)| \geq s$. As in Razborov's argument we obtain a bound on $|S|/|\mathcal{R}_n^\ell|$ by defining a 1-1 map from S to a small set. The proof is somewhat different because we are interested in the height of decision trees for $F\lceil_\rho$ rather than the length of maxterms of $F\lceil_\rho$.

We will define a 1-1 map

$$S \quad \longrightarrow \quad \mathcal{R}_n^{\ell-s} \times stars(r,s) \times 2^s.$$

Let $F = C_1 \vee C_2 \vee \ldots$. Suppose that $\rho \in S$ and let π be the restriction associated with the lexicographically first path in $T(F\lceil_\rho)$ that has length $\geq s$ (any way of canonically associated such a long path will do.) Trim the last few variables set in π along the path from the root so that $|\pi| = s$. We use the formula F and π to determine the image of ρ. The image of ρ is defined by following the path π in the canonical decision tree for $F\lceil_\rho$ and using the structure of that tree (see Figure 1.)

Let C_{ν_1} be the first term of F that is not set to 0 by ρ. Then $C_{\nu_1}\lceil_\rho$ will be the first term in $F\lceil_\rho$. Since $|\pi| > 0$, such a term must exist and will not be the empty term. Let K be the set of variables in $C_{\nu_1}\lceil_\rho$ and let σ_1 be the unique restriction of the variables in K that satisfies $C_{\nu_1}\lceil_\rho$. Let π_1 be the portion of π that sets the variables in K. We have two cases based on whether or not $\pi_1 = \pi$.

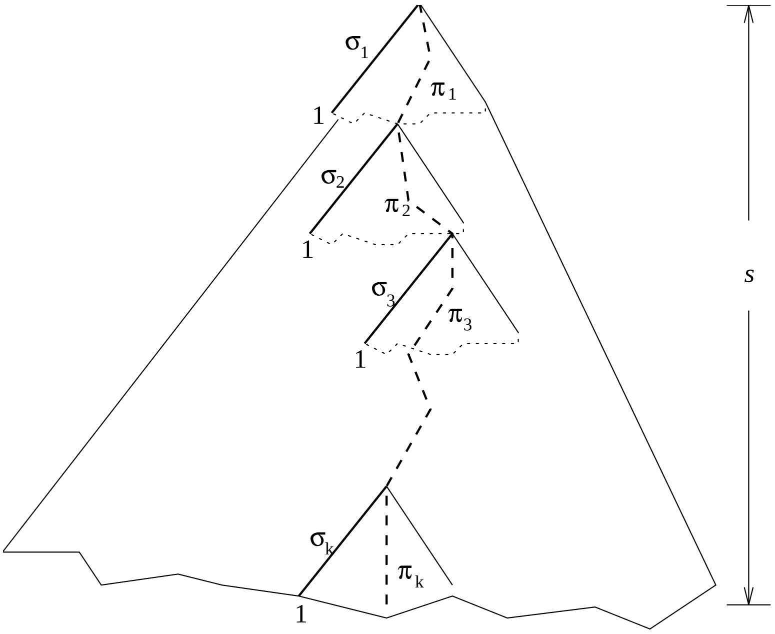

Figure 1: Canonical decision tree $T(F\lceil_\rho)$

1: If $\pi_1 \neq \pi$ then by the construction of π, π_1 sets all the variables in K. Note also that $C_{\nu_1}\lceil_{\rho\sigma_1}= 1$ but since $\pi_1 \neq \pi$, $\pi_1 \neq \sigma_1$, and thus $C_{\nu_1}\lceil_{\rho\pi_1}= 0$.

2: If $\pi_1 = \pi$ then it is possible that π does not set all of the variables in K. In this case we shorten σ_1 to the variables in K that appear in π_1. Now all we know is that $C_{\nu_1}\lceil_{\rho\sigma_1}\neq 0$.

Define $\beta_1 \in \{*, -\}^k$ based on the fixed ordering of the variables in term C_{ν_1} by letting the j-th component of β_1 be $*$ if and only if the j-th variable in C_{ν_1} is set by σ_1. Note that since $C_{\nu_1}\lceil_\rho$ is not the empty term there is at least one $*$ in β_1. From C_{ν_1} and β_1 we can reconstruct σ_1.

Now, by the definition of $T(F\lceil_\rho)$, $\pi \setminus \pi_1$ labels a path in the canonical tree $T(F\lceil_{\rho\pi_1})$. If $\pi_1 \neq \pi$, we repeat the above argument, with $\pi \setminus \pi_1$ in place of π, $\rho\pi_1$ in place of ρ and find a term C_{ν_2} which is the first term of F not set to 0 by $\rho\pi_1$. Based on this we generate π_2, σ_2, and β_2 as before. We repeat this process until the round k in which $\pi_1\pi_2...\pi_k = \pi$.

Let $\sigma = \sigma_1\sigma_2...\sigma_k$. We finally define $\delta \in \{0, 1\}^s$ to be a vector that indicates for each variable set by π (which are the same as those set by σ) whether it is set to the same value as σ sets it.

The image of ρ under the 1-1 map we define is a triple, $\langle \rho\sigma_1...\sigma_k, (\beta_1, ..., \beta_k), \delta\rangle$. Clearly $\rho\sigma = \rho\sigma_1...\sigma_k \in \mathcal{R}_n^{\ell-s}$ and $(\beta_1, ..., \beta_k) \in stars(r, s)$ so the map is as required.

It remains to show that the map we have just defined is indeed 1-1. To do this, as in Razborov's argument, we show how to recover ρ from its image. The reconstruction is iterative. In the general stage of the reconstruction we will have recovered $\pi_1, ..., \pi_{i-1}$, $\sigma_1, ..., \sigma_{i-1}$, and will have constructed $\rho\pi_1...\pi_{i-1}\sigma_i...\sigma_k$. Recall that for $i < k$, $C_{\nu_i}\lceil_{\rho\pi_1...\pi_{i-1}\sigma_i} = 1$ and $C_j\lceil_{\rho\pi_1...\pi_{i-1}\sigma_i} = 0$ for all $j < \nu_i$. This clearly also holds when we append $\sigma_{i+1}...\sigma_k$ to the restriction. When $i = k$, something similar occurs except the only guarantee is that $C_{\nu_i}\lceil_{\rho\pi_1...\pi_{k-1}\sigma_k} \neq 0$. Thus we can recover ν_i as the index of the first term of F that is not set to 0 by $\rho\pi_1...\pi_{i-1}\sigma_i...\sigma_k$.

Now, based on C_{ν_i} and β_i we can determine σ_i. Since we know $\sigma_1, ..., \sigma_i$, using the vector δ we can determine π_i. We can now change $\rho\pi_1...\pi_{i-1}\sigma_i...\sigma_k$ to $\rho\pi_1...\pi_{i-1}\pi_i\sigma_{i+1}...\sigma_k$ using the knowledge of π_i and σ_i. Finally, given all the values of the π_i we can reconstruct ρ.

Now we compute the value $|S|/|\mathcal{R}_n^\ell|$:

$|\mathcal{R}_n^\ell| = \binom{n}{\ell}2^{n-\ell}$ so

$$\frac{|\mathcal{R}_n^{\ell-s}|}{|\mathcal{R}_n^\ell|} = \frac{\ell^{(s)}}{(n-\ell+s)^{(s)}} \cdot 2^s \leq \frac{(2\ell)^s}{(n-\ell)^s}.$$

Applying the bounds we obtain

$$\begin{aligned} \frac{|S|}{|\mathcal{R}_n^\ell|} &\leq \frac{|\mathcal{R}_n^{\ell-s}|}{|\mathcal{R}_n^\ell|} \cdot |stars(r,s)| \cdot 2^s \\ &\leq \left(\frac{4\ell r}{(n-\ell)\ln 2}\right)^s \\ &= (\frac{4pr}{(1-p)\ln 2})^s \end{aligned}$$

for $\ell = pn$. For $p < 1/7$ this is at most $(7pr)^s$. □

It is worth noting that in avoiding conditional probability we do not obtain bounds that are quite as strong as those obtained by Håstad. It is possible to obtain somewhat better bounds than described above by combining the information in $stars(r, s)$ and δ since, except for $i = k$, $\sigma_i \neq \pi_i$ and thus δ must contain at least one 1 in the seqment associated with each σ_i. In fact, by choosing without loss of generality a long branch π that does not have a leaf labelled 1, this is true even in the case that $i = k$. In that case we can replace Lemma 2 by a similar argument that produces a bound of α^s on the number of different encodings of both $stars(r, s)$ and δ where α is the solution of $(1 + 2/\alpha)^r - (1 + 1/\alpha)^r = 1$. This produces a final result very close to Håstad's bounds but it has a $1-p$ in the denominator as opposed to a $1+p$. The gap here seems to depend on the fact that we have fixed the number of stars as opposed to allowing it to vary. We chose to separate $stars(r, s)$ from δ in our argument above since $stars(r, s)$ is useful in the other switching lemma proofs.