Switching Lemma

Alexander Glazman

May 4, 2009

Contents

1 Introduction **1**

2 Definitions **1**

2.1 Matchings 1
2.2 Language L_n 2
2.3 Trees 2
2.4 Definition of $Code(r, s)$ 3

3 Proof **4**

3.1 Statement 4
3.2 Main idea 4
3.3 Bijection 5
3.4 Proof of Switching Lemma 7

1 Introduction

Sometimes we can represent $s-DNF$ as $r-CNF$. This is useful in proving lower bounds for proof in different proof systems. And Switching Lemma is the name for general statement concerning this problem. We will prove Switching Lemma in some particular case of Frege systems.

2 Definitions

2.1 Matchings

First of all we need some definitions. Let's begin with matchings.

- Let D, R be ordered subsets of S with all elements of D preceding elements of R and $D \cup R = S$. *A matching between D and R* is a set of mutually disjoint unordered pairs $\{i, j\}$, where $i \in D$, $j \in R$.
- A matching *covers a vertex i* if $\{i, j\}$ belongs to the matching for some vertex j. By $V(\pi)$ we will denote the vertices covered by π.
- If $X \subseteq S$, then $M(X)$ denotes the set of all matchings π such that π covers X, but no matching properly contained in π covers X.
- The set of matchings between D and R we shall denote by M_n.
- Two matchings π_1 and π_2 in M_n are *compatible* if $\pi_1 \cup \pi_2$ is also a matching. In this case we will denote there union by $\pi_1\pi_2$.
- If π is a matching then $S|\pi = S \setminus V(\pi)$.

2.2 Language L_n

Now some definitions concerning language L_n

- Let $|D| = n + 1$ and $|R| = n$. The language built from propositional variables P_{ij} and the constants 0 and 1 using the connectives $\vee$ and $\neg$ we shall refer to as L_n.
- A matching π determines a *restriction* ρ_π of the variables of L_n: if i or j is covered by π then $\rho_\pi(P_{ij}) = 1$ if $\{i, j\} \in \pi$, and $\rho_\pi(P_{ij}) = 0$ if $\{i, j\} \notin \pi$; otherwise $\rho_\pi(P_{i,j})$ is undefined.
- If F is formula of L_n, and $\pi \in M_n$, then we denote by $F|\pi$ the formula resulting from F by substituting for the variables in F the constants representing their value under π.

- Formula C is a *matching term* if:

$$C = \bigcap_{\{i,j\} \in \pi} P_{ij} = \wedge \pi$$

  where π is a matching.

- Formula F is a *matching disjunction* if $F = C_1 \vee \cdots \vee C_m$, where C_i is a matching term for every i. It is an *r-disjunction* if all the matching terms have size bounded by r.

2.3 Trees

Let $|D| = n + 1$ and $|R| = n$, where $S = D \cup R$ and $D \cap R = \varnothing$. *The full matching tree* for S over S is a tree T satisfying conditions:

1. nodes of T other than the leaves are labeled with vertices in S;

2. edges of T are labeled with pairs $\{i, j\}$, where $i \in D$ and $j \in R$;

3. if p is a node of T then the edge labels on the path from the root of T to p determine a matching $\pi(p)$ between D and R;

4. p is labeled with the first node i in X not covered by $\pi(p)$, and the set $\{\pi(q)|q\ a\ child\ of\ p\}$ consists of all matchings in S of the form $\pi(p) \cup \{\{i, j\}\}$ for $j \in S$;

Let $F = C_1 \vee \cdots \vee C_m$ be a matching disjunction over S. *The canonical matching decision tree* for F over S, $Tree_S(F)$, is defined inductively as follows:

1. If $F \equiv 0$ then $Tree_S(F)$ is a single node labeled 0; if $F \equiv 1$ then $Tree_S(F)$ is a single node labeled 1;

2. Let C be the first matching term in F such that $C \not\equiv 0$. Then $Tree_S(F)$ is constructed as follows:

   - Construct the full matching tree for $V(C)$ over S;
   - Replace each leaf ℓ of the fill matching tree for $V(C)$ by the canonical matching decision tree $Tree_{S|\pi(\ell)}(F|\pi(\ell))$.

The *depth* of a tree T is a maximum length of a branch in T.

2.4 Definition of $Code(r, s)$

Define $Code(r, s)$ to be the set of all tables $k \times r$ with elements just 0 and 1 such that there is no string with all 0, and the number of 1 in the whole table is s.
Given table A, define a map from $\{1, \ldots, s\}$ to $\{1, \ldots, r\} \times \{0, 1\}$ as follows:

1. Let the first 1 occur in the jth place. Then $f(1) = (j, 0)$.
2. Let the ith 1, where $i > 1$, occur in the jth place in the ℓth string for some ℓ. Then $f(i) = (j, b)$, where $b = 0$ if the previous 1 occurs in the same string, and $b = 1$ otherwise.

It is easy to see that this map uniquely determines a table $A \in Code(r, s)$. So we get the estimate for the cardinality of $Code(r, s)$:

$$|Code(r, s)| \leq (2r)^s.$$

Let $|D| = n + 1$ and $|R| = n$, $S = D \cup R$. For $\ell \leq n$ define M_n^ℓ:

$$M_n^\ell = \{\rho \in M_n : \#R|\rho = \ell\}.$$

For $s > 0$, F a matching disjunction over S:

$$Bad_n^\ell(F, s) = \{\rho \in M_n^\ell : |Tree_{S|\rho}(F|\rho)| \geq s\}.$$

3 Proof

3.1 Statement

Now we can formulate our main statement — Switching Lemma:

Theorem 1. *Let F be an r-disjunction over $D \cup R$, $|D| = n + 1$, $|R| = n$. Let $l \geq 10$. If $r \leq l$ and $l^4/n \leq 1/10$ then:*

$$\frac{|Bad_n^\ell(F, 2s)|}{|M_n^\ell|} \leq (11r\ell^4/n)^s.$$

3.2 Main idea

Now some words about proof of this fact. Note that:

$$\begin{aligned}
|M_n^\ell| &= \binom{n}{\ell}(n+1)^{\underline{n-l}} = \frac{n^{\underline{\ell}}(n+1)^{\underline{n-\ell}}}{\ell!} \\
\frac{|M_n^{\ell-j}|}{|M_n^\ell|} &= \frac{n^{\underline{\ell-j}}(n+1)^{\underline{n-\ell+j}}\ell!}{(\ell-j)!n^{\underline{\ell}}(n+\ell)^{\underline{n-\ell}}} = \frac{(\ell+1)^{\underline{j}}\ell!}{(\ell-j)!n^{\underline{\ell}}(n-\ell+j)^{\underline{j}}} = \\
&= \frac{(\ell+1)^{\underline{j}}\ell^{\underline{j}}}{(n-\ell+j)^{\underline{j}}} \leq \left(\frac{\ell(\ell+1)}{n-\ell}\right)^j
\end{aligned}$$

$$\begin{aligned}
&Bad_n^\ell(F,s) \to M_n^{\ell-j} \\
&Bad_n^\ell(F,s) \to \bigcup_{s/2\leq j\leq s} M_n^{\ell-j}
\end{aligned}$$

If we have one of these injections, we are home. But in fact we have another map.

3.3 Bijection

Theorem 2. *Let $F = C_1 \vee \cdots \vee C_m$ be an r-disjunction over S. Then there is a bijection from $Bad_n^l(F,s)$ into*

$$\bigcup_{s/2\leq j\leq s} M_n^{l-j} \times Code(r,j) \times [2l+1]^s.$$

Proof. Let $\rho \in Bad_n^l(F,s)$; choose π to be matching determined by the leftmost path originating in the root of $Tree_{S|\rho}(F|\rho)$ that has length s. Define three sequences by induction:

1. $D_1, \ldots, D_k$, a subsequence of $C_1, \ldots, C_m$;
2. $\sigma_1, \ldots, \sigma_k$, a sequence of restrictions $\sigma_i \subseteq \delta_i$, where $D_i = \wedge\delta_i$, and $\rho\sigma_1 \ldots \sigma_i \in M_n$;
3. $\pi_1, \ldots, \pi_k$, a partition of π, where each π_i, $i < k$, satisfies the conditions:

- $\pi_i \in M(V(\sigma_i))$;
- the restriction $\rho\pi_1 \dots \pi_i$ labels a path in $Tree_S(F)$, ending in a boundary node.

We have $\pi_{i-1}, D_{i-1}, \sigma_{i-1}$ and $\pi_1 \dots \pi_{i-1} \neq \pi$. Since $\pi_1 \dots \pi_{i-1}$ labels a path ending in a boundary node, it follows that there must be a term D in F so that $D|\rho\pi_1 \dots \pi_{i-1} \not\equiv 0$ and $D|\rho\pi_1 \dots \pi_{i-1} \not\equiv 1$, for otherwise the path labeled by π would end at that node.

1. Define D_i be the first such term in F;
2. then define σ_i to be the unique minimal matching so that $D|\rho\pi_1 \dots \pi_{i-1}\sigma_i \equiv 1$ (at the end here $\not\equiv 0$);
3. let π_i be the set of pairs in π that cover vertices in $V(\sigma_i)$.

It is easy to verify that $\rho\sigma_1 \dots \sigma_i \in M_n$, moreover $\rho\pi_1 \dots \pi_{i-1}\sigma_i \dots \sigma_k \in M_n$. It is convenient to introduce a special ordering of the $2l+1$ vertices unset by the restriction ρ. To avoid confusion between the original ordering and the new ordering, we shall refer to the original ordering as *ordering by size.* and the new order as *ordering by index.*
Let $\sigma = \sigma_1 \dots \sigma_k$. The index ordering is defined as follows:

- The vertices set by σ are listed:
  1. first according to the order $V(\sigma_1) < \dots < V(\sigma_k)$
  2. then by size
- The remaining vertices unset by $\rho\sigma$ are listed by size, in the index positions $2j+1, \dots, 2l+1$, where $j = |\sigma|$.

The map $G(\rho) = \langle G_1(\rho), G_2(\rho), G_3(\rho) \rangle$ is now defined as follows:

1. $G_1(\rho) = \rho\sigma$;
2. For $i = 1, \dots, k$ and $j = 1, \dots, r$ let $G_2(\rho)_{ij}$ be 1 if σ_i sets the jth variable of D_i, and let it be 0, otherwise
3. The list $G_3(\rho) \in [2l+1]^s$ is defined as follows:

- List the elements of π according to the index ordering, where for each pair in π the element with lower index determines the position of the pair;
- From the ordered list of the pairs in π, create a new list by recording for each pair the index of the element in the pair with the higher index. This new list is $G_3(\rho)$.

It is easy to see that $G(\rho) \in M_n^{l-j} \times Code(r, j) \times [2l+1]^s$, where $j = |\sigma|$. For $i < k$, $\pi_i \in M(V(\sigma_i))$, so that $|\sigma_i| \leq |\pi_i| \leq 2|\sigma_i|$, while for $i = k$, $|\sigma_i| = |\pi_i|$ holds by construction. Thus $|\pi|/2 \leq |\sigma| \leq |\pi|$, that is, $s/2 \leq j \leq s$. So it remains to show that G is a bijection.
How to reconstruct ρ from $G(\rho)$:

1. We know $G(\rho)$ and the r-disjunction F;
2. the set of vertices unset by $\rho\sigma$;
3. Induction by i. We know $D_1, \ldots, D_{i-1}$, $\pi_1, \ldots, \pi_{i-1}$, $\sigma_1, \ldots, \sigma_{i-1}$ and $\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k$.
4. If C_j occurs earlier in F than D_i, then $C_j|\rho\pi_1 \ldots \pi_{i-1} \equiv 0$. Hence:
$$C_j|\rho\pi_1 \ldots \pi_{i-1}\sigma_i, \ldots, \sigma_k \equiv 0$$
5. If $i < k$ then $D|\rho\pi_1 \ldots \pi_{i-1}\sigma_i \equiv 1$ while $D|\rho\pi_1 \ldots \pi_{k-1}\sigma_k \not\equiv 0$. Thus in either case:
$$D_i|\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k \not\equiv 0$$
6. We know D_i — this is the first term in F not set 0 by the restriction $\rho\pi_1 \ldots \pi_{i-1}\sigma_i \ldots \sigma_k$.
7. Using D_i and $G_2(\rho)$ we can find σ_i.
8. We know indices of the vertices in $V(\sigma_i)$.
9. Every pair in π_i contains at least one vertex in $V(\sigma_i)$, hence for every such pair we can find the vertex with lower index.
10. Using $G_3(\rho)$ we can find π_i.
11. By replacing σ_i by π_i we can find restriction $\rho\pi_1 \ldots \pi_i\sigma_{i+1} \ldots \sigma_k$.

12. Having found all of $\sigma_1, \ldots, \sigma_k$, we can find ρ by removing all of the pairs in $\sigma_1 \ldots \sigma_k$ from $\rho\sigma_1 \ldots \sigma_k$.

$\square$

3.4 Proof of Switching Lemma

Now we are close to proof of Switching Lemma.

Theorem 3. *Let F be an r-disjunction over $D \cup R$, $|D| = n+1$, $|R| = n$. Let $\ell \geq 10$. If $r \leq \ell$ and $\ell^4/n \leq 1/10$ then:*

$$\frac{|Bad_n^\ell(F, 2s)|}{|M_n^\ell|} \leq (11r\ell^4/n)^s.$$

Proof. By the previous theorem we should bound the ratio:

$$\frac{\bigcup_{s \leq j \leq 2s} M_n^{\ell-j} \times Code(r,j) \times [2\ell+1]^s}{|M_n^\ell|}$$

And we know, that:

$$\frac{|M_n^{\ell-j}|}{|M_n^\ell|} \leq \left(\frac{\ell(\ell+1)}{n-\ell}\right)^j$$

Using this and the estimate $|Code(r,j)| \leq (2r)^j$ we can bound our ratio by the sum:

$$\sum_{s \leq j \leq 2s} \left(\frac{\ell(\ell+1)}{n-\ell}\right)^j (2r)^j (2\ell+1)^{2s} = (2\ell+1)^{2s} \sum_{s \leq j \leq 2s} \left(\frac{2\ell(\ell+1)r}{n-\ell}\right)^j$$

Using the inequalities $r \leq \ell$, $\ell^4/n \leq 1/10$ and $\ell \geq 10$, we can prove that:

$$\frac{2\ell(\ell+1)r}{n-\ell} < 0.0221.$$

So the geometrical progression which we have is less than 1.03 times its largest term. This provides the estimate:

$$\frac{|Bad_n^\ell(F, 2s)|}{|M_n^\ell|} \leq 1.03 \left(\frac{2(2\ell+1)^2\ell(\ell+1)r}{n-\ell}\right)^s$$

Now we can estimate the right side:

$$\left(\frac{2(2\ell+1)^2\ell(\ell+1)r}{n-\ell}\right) \leq \frac{10.65\ell^4 r}{n}$$

This inequality yields the bound:

$$\frac{|Bad_n^\ell(F,2s)|}{|M_n^\ell|} \leq 1.03(10.65r\ell^4/n)^s < (11r\ell^4/n)^s.$$

$\square$

References

[1] Alasdair Urquhart, Xudong Fu Simplified lower bounds for propositional proofs