Math 262A Lecture Notes

Lecturer: Samuel Buss
Scribe: Udbhav Singh
Secondary Scribe: Radheshyam Balasundaram

November 13, 2013

Notations and conventions: We will be dealing with $\{\wedge, \vee, \neg\}$ formulas with the convention that the negations are pushed down to the leaves (variables).

We begin with the definition of restrictions

Definition 1 (Restrictions)**.** *A restriction p is a mapping $\{1, 2, \ldots, n\} \longrightarrow \{0, 1, *\}$. Given a function ϕ and a restriction p, the function ϕ restricted by p, denoted by $\phi|_p$, is defined as $\phi|_p(\vec{x}) = \phi(\vec{x})$ where*

$$x_i = \begin{cases} x_i \text{ if } p(i) = * \\ p(i) \text{ otherwise} \end{cases}$$

Such a restriction simplifies the formulas. We can also exploit the fact that the gates are either $\vee$ or $\wedge$.

Definition 2 (Constant Simplification)**.** *A **constant simplification** is one in which a single literal $Z = X_i$ or $\bar{X}_i$ is replaced by either a 0 or 1.*

Consider sub-formulas of the kind $Z \vee g$ and $Z \wedge g$. The following cases are possible

$$0 \wedge g \longrightarrow 0 \tag{1}$$
$$1 \wedge g \longrightarrow g \tag{2}$$
$$0 \vee g \longrightarrow g \tag{3}$$
$$1 \wedge g \longrightarrow 1 \tag{4}$$

We can exploit cases (1) and(4) to give further simplification.

The following fact leads to another kind of simplification.

Fact 1. *In a minimal size $\{\wedge, \vee, \neg\}$ formula, any sub-formula $Z \vee \psi$ or $Z \wedge \psi$ where Z is a literal (X_i or $\bar{X}_i$) has no occurrence of Z in ψ*

Proof. $Z \wedge \psi$ is equivalent to $Z \wedge \psi(Z|_1)$ and $Z \vee \psi$ is equivalent to $Z \vee \psi(Z|_0)$ where $\psi(Z|_i)$ is ψ restricted to $Z = i$ □

Definition 3 (One Variable Simplification)**.** *A **one variable simplification** of a formula ϕ is where all occurrences of sub-formulas of form $Z \wedge \psi$ are replaced by $Z \wedge \psi(Z|_1)$ and all sub-formulas of form $Z \vee \psi$ are replaced by $Z \vee \psi(Z|_0)$*

Question: By how much does a formula size decrease by constant simplification?

Theorem 1 (Subotovskaya's Theorem)**.** *Let ϕ be a $\{\wedge, \vee, \neg\}$ formula, then $\exists$ a literal Z such that the formula ϕ' on letting ϕ restricted by $Z = i$ (constant simplification) has leaf size bounded by*

$$leafsize(\phi') \leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} leafsize(\phi) \tag{5}$$

Proof. We choose X_i than appears more than $\frac{m}{n}$ times where m is $leafsize(\phi)$. Choose either X_i or $\bar{X}_i$ depending on which occurs more in the "Critical" cases which removes their neighboring sub-formulas. Without loss of generality, X_i and $\bar{X}_i$ do not occur in any neighborhood of these "critical occurrences" (by Fact 1.). Now apply the constant substitution that causes most collapse. Without loss of generality, assume it is $Z \longrightarrow 1$.
This removes $\frac{m}{n}$ gates where Z occurs. Another $\frac{m}{2n}$ gates are removed because half of these occurrences are critical and remove the neighbor as well and as the neighbor do not include Z, no over counting occurs. There may also be addition removals as constant simplifications can iterate, but there are at least $\frac{3m}{2n}$ removals. Thus we get

$$\begin{aligned} leafsize(\phi') &\leq m - \frac{3m}{2n} && (6)\\ &= \left(1 - \frac{3}{2n}\right) m && (7)\\ &\leq \left(1 - \frac{1}{n}\right)^{\frac{3}{2}} m && (8) \end{aligned}$$

□

We will call the exponent $\frac{3}{2}$, the shrinkage factor Γ.

We can now iterate this process which gives the following lemma

Lemma 1. *Let ϕ be as before. Let $k < n$, then one can choose $n - k$ variables $X_{i_1}, \ldots, X_{i_{n-k}}$ and values $a_1, \ldots, a_{n-k} \in 0, 1$ such that setting $X_{i_j} = a_j$ gives*

$$leafsize(\phi') \leq \left(\frac{k}{n}\right)^{\frac{3}{2}} leafsize(\phi) \tag{9}$$

where ϕ' is ϕ with constant simplification.

Proof. We can iterate the previous construction to get

$$leafsize(\phi') \leq \left(1-\frac{1}{n}\right)^{\frac{3}{2}}\left(1-\frac{1}{n-1}\right)^{\frac{3}{2}}\cdots\left(1-\frac{1}{k+1}\right)^{\frac{3}{2}} leafsize(\phi) \quad (10)$$

$$= \left(\frac{n-1}{n}\right)^{\frac{3}{2}}\left(\frac{n-2}{n-1}\right)^{\frac{3}{2}}\cdots\left(\frac{k}{k+1}\right)^{\frac{3}{2}} leafsize(\phi) \quad (11)$$

$$= \left(\frac{k}{n}\right)^{\frac{3}{2}} leafsize(\phi) \quad (12)$$

□

Another modification is possible when we choose the restrictions at random. Let R_k be the distribution on restrictions of the form where $\rho \in R_k$ has property $\rho(X_1,\ldots,X_n) \longrightarrow \{0,1,*\}$ and $|\rho^{-1}(*)| = k$ and we choose these restriction with equal probability (from a uniform distribution).

Theorem 2 (Subotovskaya)**.** *Let ϕ, k and n be as above and $\rho_k \in R_k$ is chosen at random, then*

$$\mathbb{E}[leafsize(\phi')] \leq \left(\frac{k}{n}\right)^{\frac{3}{2}} leafsize(\phi) \quad (13)$$

and thus

$$\mathbb{P}\left[leafsize(\phi') \geq 4\left(\frac{k}{n}\right)^{\frac{3}{2}} leafsize(\phi)\right] \leq \frac{1}{4} \quad [\textit{by Markov's Inequality}] \quad (14)$$

Proof. Same as above except numbers are replaced by expectations everywhere. □

Thus from Subotovskaya, we have the shrinkage exponent $\Gamma = \frac{3}{2}$. Using the shrinkage factors allows us to get a lower bound on the formula size of functions. Progressive improvements on the shrinkage factor have been made by using one variable simplification in addition to constant simplification. *Impagliazzo-Nisan* gave a shrinkage exponent of 1.55. *Paterson-Zande* gave a value 1.65 and *Hastad* gave a value of 2 for the shrinkage factor.
Using the shrinkage factor, Andreev gave a much better lower bound of $\frac{5}{2}$ (almost) using $\Gamma = \frac{3}{2}$ and a bound of 3 (almost) using $\Gamma = 2$

We will now prove Andreev's lower bound result.

Let u_{ij} be new variable for $i = 1,\ldots,k$ and $j = 1,\ldots,n/k$. Define the function $f(y_0,\ldots,y_{m-1},u_{11},\ldots,u_{k,\frac{n}{k}}) = SA_n(\vec{y},\oplus_{j=1}^{n/k}u_{1j},\ldots,\oplus_{j=1}^{n/k}u_{kj})$. Here SA_n is the storage access function as defined in the last class.

Claim 1. *There are constants $\{a_0,\ldots,a_{m-1}\}$ such that $SA_n(a_0,\ldots,a_{m-1},z_1,\ldots,z_k) = SA_n^{\vec{a}}(z_1,\ldots,z_k)$ requires formula size greater than $\frac{1}{2}\frac{2^k}{\log k}$*

Proof. Immediate by Riordon-Shannon Theorem □

Now let's fix such a value of $\vec{a}$. Let $g(\vec{u}) = f(\vec{a}, \vec{u})$

Claim 2. *If ρ is a restriction such that $\forall i = 1, \ldots, k$ there is a j such that $\rho(u_{ij}) = *$, then $g|_\rho$ requires formulas of leaf size greater than $\frac{2^{k-1}}{\log k}$*

Proof. $g = SA_n(\vec{y}, \oplus_{j=1}^{n/k} u_{1j}, \ldots, \oplus_{j=1}^{n/k} u_{kj})$. Now consider a restriction $\rho' \supseteq \rho$ such that ρ' sets exactly one u_{ij} equal to * for each i. Then $g|_{\rho'} = g$ because we can flip the free variables in $g|_{\rho'}$ to get any value of g we want (possibly with some variables negated). □

Consider R_s, the set of restrictions which leave exactly s literals unset, where $s = k \ln(4k)$.

Claim 3. *If $\rho \in R_s$ chosen at random, then $\mathbb{P}[\forall i \, \exists j \, \rho(u_{ij} = *)] > \frac{3}{4}$*

Proof. Each $u_{ij} = *$ with probability $\frac{s}{n} = \frac{k \ln(4k)}{n}$. So for fixed i, we have

$$\mathbb{P}[\exists j \, \rho(u_{ij}) \neq *] \leq \left(1 - \frac{s}{n}\right)^{\frac{k}{n}} \tag{15}$$

$$= \left(1 - \frac{k \ln(4k)}{n}\right)^{\frac{k}{n}} \tag{16}$$

$$\leq e^{-\ln(4k)} = \frac{1}{4k} \tag{17}$$

$$\implies \mathbb{P}[\forall i \, \exists j \, \rho(u_{ij} \neq *)] < k \frac{1}{4k} = \frac{1}{4} \tag{18}$$

□

From Subotovskaya (Theorem 2) we have

$$\mathbb{P}\left[leafsize(g|_\rho) \leq 4\left(\frac{s}{n}\right)^{\frac{3}{2}} leafsize(g)\right] \geq \frac{3}{4}$$

There is at least one $\rho \in R_s$ such that $g_|\rho$ requires formula of leaf size greater than $\frac{2^{k-1}}{\log k}$ and $g|_\rho$ has leafsize less than $4\left(\frac{s}{n}\right)^{\frac{3}{2}} leafsize(g)$. Thus

$$leafsize(g) \geq \frac{1}{4}\left(\frac{n}{s}\right)^{\frac{3}{2}} \frac{2^{k-1}}{\log k} = \Omega\left(\frac{n^{\frac{5}{2}}}{(\log n)^{\frac{3}{2}} (\log \log n)^3}\right) \tag{19}$$

$$= \Omega(n^{\frac{5}{2} - o(1)}) \tag{20}$$

Thus we have proved Andreev's lower bound.

Corollary 1 (Andreev's Theorem)**.** *For $\{\wedge, \vee, \neg\}$ basis, size of any fomula f is greater than $n^{\frac{5}{2} - o(1)}$*

Proof. If f has smaller size then g does too which is not possible. □

Using Hastad's value of 2 for the shrinkage exponent, it is possible to show that

$$L_{\{\wedge,\vee,\neg\}} = \Omega\left(\frac{n^3}{(\log n)^{\frac{3}{2}}(\log\log n)^3}\right)$$

This lower bound is tight as there are examples that achieve this bound.