U.C. Berkeley — CS278: Computational Complexity Handout N24
Professor Luca Trevisan 11/14/2002
Scribe: Manikandan Narayanan

Notes for Lecture 24

Today, we continue our study of the Resolution proof system. First we complete the discussion from last lecture, on how Resolution proof width approximates Resolution proof complexity. Next we establish lower bounds on Resolution Proof width of CNF formula having certain expansion properties, to prove results about their Resolution proof complexity.

Here is a quick recap of a few terms and notations. Let π be a Resolution proof (or in short, proof) deriving a clause D from a CNF formula φ. That is, π derives $(\varphi \rightarrow D)$. Then, the width of π denoted by $w(\pi)$ is the size of the longest clause in π, excepting those clauses that are also in φ. Note that the size of a clause is the number of literals in the clause. The length of π is simply the number of clauses in π (i.e., its cardinality $|\pi|$). We measure proof complexity of a derivation by the length of its shortest (minimum-length) proof. Throughout this material, we use φ to denote a CNF formula. Sometimes we interpret φ or a subformula of φ as a *set* of clauses and this interpretation should be clear from the context.

1 Width and Proof Complexity

1.1 The Main Theorem

In general, a derivation $(\varphi \rightarrow D)$ can have different proofs and by its width $w(\varphi \rightarrow D)$, we mean the width of its minimum-width proof. The following theorem is about $w(\varphi \rightarrow 0)$ (written sometimes as simply $w(\varphi)$), where 0 is the empty false clause and φ is unsatisfiable. A proof that derives $(\varphi \rightarrow 0)$ is called a refutation of φ.

Theorem 1 (Main Width-Length Theorem) *Let φ be a unsatisfiable k-CNF formula on n variables. Let L_T and L be the length of the shortest tree-like and shortest general refutation of φ respectively. Then, the width of the minimum-width refutation of φ, $w(\varphi)$ is related to L_T and L as:*

$$w(\varphi) \le log\, L_T + k \tag{1}$$

$$w(\varphi) \le O(\sqrt{n\, log\, L}) + k \tag{2}$$

This theorem is an attempt at simplifying the study of proof complexity [BSW01]. Instead of working directly with L_T and L, we work on proving linear lower bounds on $w(\varphi)$ to get exponential lower bounds on L_T and L. That is, if $w(\varphi) = \Omega(n)$ and $k = o(n)$, then by Relations (1) and (2), L_T and $L = 2^{\Omega(n)}$. If we replace n with n^{ϵ}, we can't say anything about L using the sub-linear lower bound on $w(\varphi)$, but we can still get a sub-exponential lower bound on L_T.

We proved Relation (1) last time, using a simple induction argument on the structure of the tree-like refutation. We can't mimic that proof for Relation (2) though, since a single clause in a general refutation can be used later in more than one derivation, leading to a *dag* structure. We prove Relation (2) using the following technical lemma.

Lemma 2 *Let π_d be the set of clauses of size strictly greater than d in a general refutation π, of a unsatisfiable k-CNF formula φ on n variables. If $|\pi_d| < (1 - \frac{d}{2n})^{-b}$ for some parameter b, then the width of π is atmost $d + b + k$.*

The clauses in π_d are in a sense the problematic clauses in π, but if there are not too many of them, we can safely bound the width of π. This lemma is true for any value of d and the proof of Relation (2) uses the value of d that optimizes this bound.

Proof: (of Relation (2) of Width-Length Theorem) Let π be the shortest general refutation of φ with length $|\pi| = L$. We obtain the result by using Lemma 2 on the trivial bound $|\pi_d| < L$.

$$\begin{aligned}
w(\varphi) &\leq w(\pi) \\
&\leq d + b + k && \text{(where b is from, } L = (1 - \tfrac{d}{2n})^{-b}) \\
&= d + log_{\frac{1}{1-\frac{d}{2n}}} L + k \\
&\leq d + log_{1+\frac{d}{2n}} L + k && \text{(using, } \tfrac{1}{1-\epsilon} \approx 1+\epsilon) \\
&\leq d + O(\tfrac{2n}{d}\, log\, L) + k && \text{(using, } log_{1+\epsilon} x \approx \tfrac{1}{\epsilon}\, log\, x) \\
&= d + O(\tfrac{n}{d}\, log\, L) + k
\end{aligned}$$

Therefore, when $d = \frac{n}{d}\, log\, L$ (i.e., $d = \sqrt{n\, log\, L}$) in the relation above, we get the desired upper bound on $w(\varphi)$. $\square$

1.2 Proof of the technical lemmas

In this section, we prove two technical lemmas used in the proof of Width-Length theorem. Lemma 3 was used in proving Relation (1) last time and it will also be used in the proof of Lemma 2 this time. We need more notations before proceeding. For a variable x in φ, let x^1 and x^0 be aliases for the literals x and $\overline{x}$ respectively. Also, let $\varphi_{x=a}$ be the restriction of φ to $x{=}a$, for $a \in \{0, 1\}$. That is, $\varphi_{x=a}$ is the set of clauses obtained from φ after removing all clauses that have x^a in them and removing x^{1-a} from all clauses that have this literal. The restriction of a clause D to $x{=}a$, denoted by $D_{x=a}$, is obtained similarly.

Lemma 3 *If for $a \in \{0, 1\}$, $\varphi_{x=a}$ is a k-CNF formula,*

$$w(\varphi_{x=1-a}) \leq d - 1 \qquad \text{and} \qquad w(\varphi_{x=a}) \leq d,$$

then $w(\varphi) \leq max(d, k)$.

Proof: We will first prove the claim: If $w(\varphi_{x=1-a}) \leq d{-}1$, then $w(\varphi \to x^a) \leq d$. We assume $a{=}1$ for notational ease (the proof for general a extends easily). Let π be a refutation of $\varphi_{x=0}$ with width atmost $d{-}1$ and let ϕ denote the set of clauses in φ that have the literal x in them. Then $\phi' = \phi_{x=0} \cap \pi$ denotes the restricted clauses of ϕ that were used in the proof π. Obtain a new proof π' by copying all clauses in π, and adding x back to the clauses in ϕ'

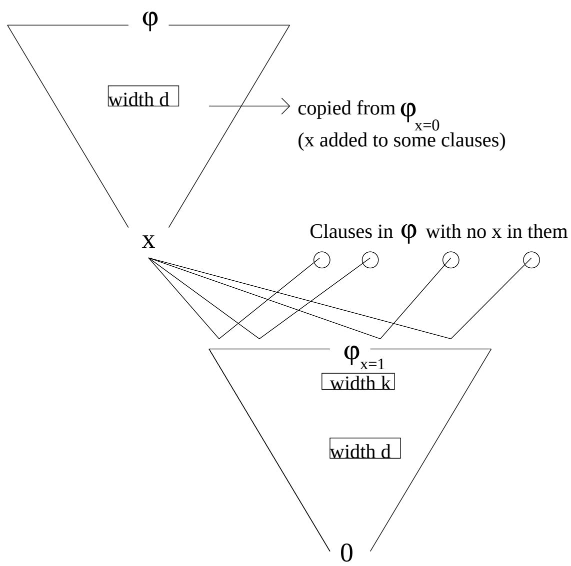

Figure 1: Composing $(\varphi \rightarrow x)$ with $(\varphi_{x=1} \rightarrow 0)$, to obtain a refutation for φ.

and its subsequent derivations (to preserve validity). The new proof π' derives x directly if ϕ' was not an empty set or indirectly via a weakening rule from the final 0 clause otherwise. Thus, π' is a valid proof of $(\varphi \rightarrow x)$ with width atmost $w(\pi) + 1 = d$.

Now we turn to the proof of the lemma, again assuming $a = 1$. We use the claim above to derive $(\varphi \rightarrow x)$. We then resolve this derived x with all clauses of φ that doesn't contain x, to obtain $\varphi_{x=1}$. This is finally fed into the refutation of $\varphi_{x=1}$. See Figure 1 for a depiction of this composition. Since $\varphi_{x=1}$ is a k-CNF and the width of both refutations used in the composition is atmost d, we get a refutation of φ with width atmost $max(d, k)$. □

We now give the proof of Lemma 2, which was used in proving Relation (2) of Width-Length theorem.

Proof: (of Lemma 2) The proof is by induction on b and n. When $b = 0$, $|\pi_d| < 1$ and the lemma is trivially true for any value of n. Similarly for $n = 1$, the lemma is trivially true for any value of b, as there are only two literals in the formula. For the induction step, we need a literal that hits many clauses in π_d and we will indeed have such a literal by the Pigeon Hole Principle (on viewing the $2n$ literals as holes and the sum-total of the sizes of all clauses in π_d as the number of pigeons). Specifically, there must be a literal, say x wlog, that occurs in atleast $\frac{d}{2n} |\pi_d|$ clauses in π_d (another way to look at this result is to pick one out of the $2n$ literals in random and see the expected number of clauses in π_d that this literal hits).

Using this x, we obtain valid refutations of $\varphi_{x=0}$ and $\varphi_{x=1}$ by restricting π to $x = 0$ and $x = 1$. The induction step then follows from applying Lemma 3 on these new refutations. By induction on n, we already have $w(\varphi_{x=0}) \leq b + d + k$. So, we just need to prove that $w(\varphi_{x=1}) \leq b + d + k - 1$. Here, we are rescued by the fact that x appears in many clauses in π_d and hence the set of clauses that are still wider than d in the restricted refutation $\varphi_{x=1}$

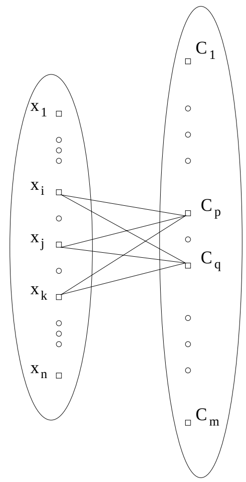

Figure 2: Graph G_φ associated with a formula φ. Clause C_p could be $x_i \vee x_j \vee x_k$ and C_q could be $\overline{x_i} \vee x_j \vee \overline{x_k}$.

(call this set π'_d) is small enough:

$$\begin{aligned} \left|\pi'_d\right| &\leq (1 - \tfrac{d}{2n})\ |\pi_d| \\ &< (1 - \tfrac{d}{2n})^{-(b-1)} \qquad\qquad \text{(substituting for } \pi_d\text{)} \end{aligned}$$

Since the parameter is now $(b-1)$, $w(\varphi_{x=1}) \leq b-1+d+k$ by induction on b and we are done with the proof. □

2 Width Lower Bounds

2.1 The Setting

We establish lower bounds on width by relating it to some natural combinatorial property. In our case, we will use the expansion property of the bipartite graph associated with a CNF formula. We first define this expansion property and state the main theorem relating width and expansion. Next we use this theorem to show that random k-CNFs require exponential-length refutations (whp, due to their expansion properties).

Definition 1 (Graph associated with a formula) *Let φ be a CNF formula on m clauses $C_1, C_2, \ldots, C_m$ and n variables $x_1, x_2, \ldots, x_n$. The graph associated with φ (see Figure 2) is the undirected bipartite graph $G_\varphi = (L, R, E)$, defined by*

$$\begin{aligned} L &= \{x_1, x_2, \ldots, x_n\}\,, \\ R &= \{C_1, C_2, \ldots, C_m\} \ \textit{and} \\ E &= \{(x_i, C_j) \mid \textit{clause } C_j \textit{ contains one of the literals } x_i \textit{ or } \overline{x_i}\}\,. \end{aligned}$$

Definition 2 (Bipartite Expansion) *A CNF formula φ on m clauses $C_1, C_2, \ldots, C_m$ is (r, c)-expanding if and only if*

$$\forall S \subseteq \{C_1, C_2, \ldots, C_m\} \text{ and } |S| \leq r, \quad |N(S)| \geq (1 + c)\, r$$

where $N(S)$ refers to the neighbourhood of S in G_φ.

Theorem 4 (Main Width-LB (LowerBound) Theorem) *For positive r and c, if φ is (r,c)-expanding and unsatisfiable, then*

$$w(\varphi) \geq \frac{rc}{2}.$$

The proof of this theorem is quite interesting and is given in the next two sections. The application of this theorem lies in the context of Width-Length theorem (Theorem 1), since a linear lower bound on rc is now enough to show a exponential lower bound on the length of any refutation of φ. Infact, the next theorem gives such a lower bound for random k-CNFs.

Theorem 5 *Let φ be a random k-CNF formula on n variables and Δn clauses, constructed by picking each clause with k variables independently at random, from all possible $\binom{n}{k} 2^k$ clauses with repetition. Then, whp φ is $\left(\frac{n}{\Delta^{\frac{1}{k-2+\epsilon}}}, \epsilon\right)$-expanding, where the clause density Δ and the parameter ϵ with $0 \leq \epsilon \leq \frac{1}{2}$ are constants.*

The proof of this theorem follows from counting arguments and is left as an exercise. For a specific value of ϵ, say $\frac{1}{2}$, we see that random k-CNFs are $(\Omega(n), \frac{1}{2})$-expanding and hence by Width-LB and Width-Length theorem, they require exponential-length refutations whp (note that they are also unsatisfiable whp for proper choice of Δ and k).

2.2 Matching and Satisfiability

This section prepares us for the proof of Width-LB theorem. Consider a subformula S of φ. If we have a matching of S in G_φ, then we can satisfy S by assigning proper truth values to the unique non-conflicting variable that each of its clauses is matched to. This simple observation along with Hall's Matching theorem, leads to an interesting result called the Tarsi's theorem. We look at Hall's theorem first.

Theorem 6 (Hall's Matching Theorem) *For a bipartite graph $G = (L, R, E)$, there exists a matching of vertices $R' \subseteq R$, if and only if*

$$\forall R'' \subseteq R', \ \left|N(R'')\right| \geq \left|R''\right|$$

where $N(R'')$ refers to the neighbourhood of R'' in G.

If there is a matching of vertices in R', then the condition in the theorem is clearly true. But the theorem's strength lies in the sufficiency of the condition, inspite of possible overlaps between the neighbourhood of different R''s. Sufficiency of the condition leads to the following two corollaries of Hall's theorem. The first corollary follows from the absence of a matching (in G_φ) of the entire formula φ. The second one follows from the presence of a matching (in G_φ) of a subformula of size atmost r (by virtue of φ's bipartite expansion property).

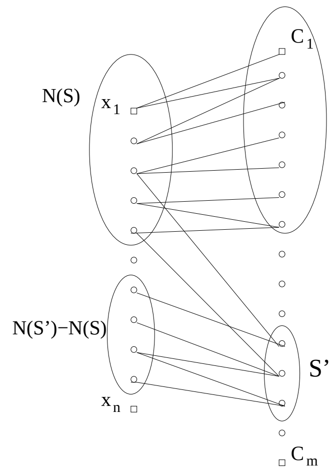

Figure 3: S' is an arbitrary subset of $\{C_1, C_2, \ldots, C_m\} - S$ in the proof of Tarsi's theorem. $|S'| < |N(S') - N(S)|$, because otherwise we could add S' to the already maximal S, resulting in a contradiction.

Corollary 7 *If φ is unsatisfiable, then there exists a subset S of the clauses of φ for which $|S| > |N(S)|$.*

Corollary 8 *For a positive r and c, if φ is (r, c)-expanding, then every subformula of φ having atmost r clauses is satisfiable.*

We now present Tarsi's theorem and its corollary, which will be used in the proof of Width-LB theorem in the next section.

Theorem 9 (Tarsi's theorem) *For a minimally unsatisfiable CNF formula φ on m clauses and n variables,*

$$m > n.$$

(Note that minimal unsatisfiability refers to minimality w.r.t inclusion of clauses. That is, if we we take away any clause from φ, it becomes satisfiable).

Proof: Since φ is a unsatisfiable formula (on clauses $C_1, C_2, \ldots, C_m$ and variables $x_1, \ldots, x_n$), by Corollary 7 of Hall's theorem, we have a subset of clauses S for which $|S| > |N(S)|$. Let's make sure that S is the maximal such set. If S is the entire formula, we are done with the proof as $|S| = m$ and $|N(S)| = n$. So, let's assume otherwise (i.e., $|S| < m$) and let S' be an arbitrary subset of $\{C_1, C_2, \ldots, C_m\} - S$. By maximality of S, we have $|S'| < |N(S') - N(S)|$ (see Figure 3). By Hall's theorem, this result basically translates to a matching in G_φ (and hence satisfiability), of all the clauses in $\{C_1, C_2, \ldots, C_m\} - S$ using only the variables in $\{x_1, \ldots, x_n\} - N(S)$. Since φ is minimally unsatisfiable, S can also be satisfied (ofcourse using only the variables in $N(S)$), leading to the satisfiability of the entire formula φ. The only way to resolve this contradiction requires S to be the entire formula, the case that we have already proved. □

Corollary 10 *If a CNF formula φ on m clauses and n variables, minimally implies a clause D of size k, then*

$$m > n - k \quad \textit{or equivalently,} \quad k > n - m.$$

(Note that "minimally implies" again refers to minimality w.r.t inclusion of clauses. That is, D can be derived from φ but not from any subformula of φ).

PROOF: Recall that x^1 and x^0 are aliases for x and $\overline{x}$ respectively. If D is $(x_1^{a_1} \vee \ldots \vee x_k^{a_k})$, the unique assignment that contradicts D is then $(x_1 = 1 - a_1, \ldots, x_k = 1 - a_k)$. Restricting φ to this assignment should yield a unsatisfiable formula $\varphi_{(x_1=1-a_1,\ldots,x_k=1-a_k)}$ on $(n-k)$ variables and atmost m clauses. It is also minimally unsatisfiable because φ minimally implied D in the first place. We obtain the result by direct application of Tarsi's theorem. $\Box$

2.3 Putting them together

Equipped with the tools of last section, we are ready for the proof of Width-LB theorem (Theorem 4). Intuitively, φ can't be refuted using only r of its clauses and we should be able to find a clause that can be derived from a "fairly big" but not "too big" subformula of φ. The proof follows from arguing about the size of such a clause in the minimum-width refutation.

PROOF: (of Width-LB Theorem) Let π be the minimum-width refutation of φ, a (r, c)-expanding formula on m clauses. Define a measure μ (a number between 1 and m) for all clauses $D \in \pi$ as:

$$\mu(D) = |\text{ smallest subformula of } \varphi \text{ that minimally implies } D\ |.$$

This measure has the following easily verifiable properties.

1. For any clause C in π that is also in φ, $\mu(C) = 1$.
2. For the final 0 clause in π, $\mu(0) \geq r$. (from Corollary 8 of Hall's theorem).
3. For a clause D derived from D' and D'' in π, $\mu(D) \leq \mu(D') + \mu(D'')$. In other words, μ is a sub-additive measure.

The above properties suggest that there exists a clause in π (say D^*), whose measure is such that $r/2 \leq \mu(D^*) \leq r$. To see this, start from the final 0 clause and pick the higher measure clause of the two clauses from which it is derived. The measure of the picked clause is atleast $r/2$ and if it is also atmost r stop; Otherwise continue this process recursively. Since $\mu(C) = 1$ for a clause C in φ, we will ultimately succeed due to sub-additivity of the measure.

Now, let S be the smallest subformula of φ that minimally implies D^*. Then using the fact that $r/2 \leq |S| \leq r$ and the corollary of Tarsi's theorem, we get: (note how we use the fact that S is "fairly big" but not "too big")

$$\begin{aligned} w(\varphi) &\geq \text{Size of } D^* \\ &\geq |N(S)| - |S| && \text{(by Corollary 10 of Tarsi's theorem)} \\ &\geq (1+c)\,|S| - |S| && \text{(by expansion property of } \varphi\text{, since } |S| \leq r) \\ &= c\,|S| \\ &\geq rc/2. \end{aligned}$$

□

References

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow: Resolution made simple. *Journal of the ACM*, 48(2), 2001.

Exercises

1. Prove Theorem 5 on the expansion property of random k-CNFs.
2. Show that Relation (1) of Width-Length theorem (proved last time) and Lemma 2, can be proven by induction on n alone. (The current proofs use induction on two variables).
3. Provide a family of examples, for which the upper bound on $w(\varphi)$ in Lemma 3 becomes tight. (Note that a tighter bound is $min(d+1, max(d,k))$ because there is a composition slightly different from the one in Figure 1, that yields a bound of $d+1$ on $w(\varphi)$).