Lecture 3— Lower bounds based on resolution width

Massimo Lauria — lauria.massimo@gmail.com

Office 1107, Ookayama West 8th Building

Tuesday — October 27th, 2015 (This document was updated on June 21, 2017)

We discuss the complexity measure of resolution width, which will be the main proxy measure we use to get size lower bound. We show that short proofs can be made narrow, and we discuss the limits of this process. If time permits we prove new size lower bounds based on width lower bounds, using formulas that have certain expansion properties: random 3-CNF, Tseitin formulas, Pigeonhole principles on graphs, and so on.

Width of a resolution refutation

When we introduced resolution we defined the width of a clause/formula/proof as the largest number of literals included in one of its element. Remember that a refutation of width w is a refutation where each clause has at most w literals (and where one clause has width exactly w).

Exercise 1. Show that if a formula ϕ has refutations of width w, then it is possible to produce one such refutation in time $n^{O(w)}$. Such bound is tight, indeed there are 3-CNF formulas with n variables with resolution refutation width w and no refutation shorter than $n^{\Omega(w)}$, no matter the width.[1]

It turns out that the study of the width is a great way to get size lower bounds. The central result is the connection between size and width due to Ben-Sasson and Wigderson.[2]

Theorem 2 (Ben-Sasson and Wigderson, 2001)**.** *Consider a k-CNF formula ϕ of n variables that has a refutation of size S. Then ϕ has also a refutation of width at most*

$$k + O\left(\sqrt{n \ln S}\right).$$

In order to discuss the proof we need the following notation.

Definition 3 (Partial assignment)**.** *A partial assignment on a set of variables $x_1, x_2, \ldots x_n$ is a set $\{x_i = b_i\}_{i \in I}$ where $I \subseteq [n]$ and $b_i \in \{0,1\}$. We denote as $\mathrm{dom}(\rho)$ the set of assigned variables $\{x_i\}_{i \in I}$. Given a clause C, $C\restriction_\rho$ is $\top$ if there is some literal in C assigned to true by ρ, otherwise $C\restriction_\rho$ is the subclause of C obtained removing all literals assigned to false. The notation is extended to any CNF.*

Exercise 4. Consider a resolution derivation π of C from ϕ, where π. Show that there is a resolution derivation $\pi\restriction_\rho$ of $C\restriction_\rho$ from $\phi\restriction_\rho$ so that

- $\pi\restriction_\rho$ has at most the same length and width of π;
- each clause in $\pi\restriction_\rho$ is a subset of some clause $C_i\restriction_\rho$ where C_i is a clause in π which is not satisfied by ρ.

[1] Albert Atserias, Massimo Lauria, and Jakob Nordstrom. Narrow proofs may be maximally long. In *Computational Complexity (CCC), 2014 IEEE 29th Conference on*, pages 286–297. IEEE, 2014

[2] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001

Exercise 5. Observe that for every partial assignment ρ there is a unique minimal clause C_ρ that is falsified by ρ.[3]

Consider a resolution derivation π of a clause C from a restricted CNF formula $\phi\restriction_\rho$. Assume π has length ℓ and width w. Show that there is a resolution derivation from ϕ of some clause $C' \subseteq C \vee C_\rho$, which has length at most ℓ and width at most $w + |dom(\rho)|$.

Proof of Theorem 2. Proof in class. See the paper for reference. □

Corollary 6. *Consider a k-CNF formula ϕ of n variables. Let S the size of the smallest refutation of ϕ, and let W be the smallest width among the refutations of ϕ. Then it holds that*

$$S \geq \exp\left(\Omega\left(\frac{(W-k)^2}{n}\right)\right) .$$

In particular to prove a superpolynomial lower bound for the size of the refutation of a k-CNF, with $k = O(1)$, it is sufficient to show a width lower bound $\omega(\sqrt{n})$. We will see later some $\Omega(n)$ width lower bounds for $O(1)$-CNF formulas, which imply exponential lower bounds.

Exercise 7. Show that if a k-CNF ϕ has a tree-like refutation of size S_T, then it has also a (possibly non tree-like) refutation of width $k + \log(S_T)$.

The results in Theorem 2 and Corollary 6 raise two obvious questions.

1. In the proof of Theorem 2 the narrow proof we get is much larger that the proof we started with. Is this necessary? Can we make the proof narrow without blowing up the size?
2. To get a super polynomial lower bound we need $\omega(\sqrt{n})$ width lower bound. Can we improve the theorem and have lower bounds with weaker width lower bounds?

The answer to both questions is NO (at least in general). In a recent work Neil Thapen[4] proved that there are formulas with both small size and small width refutations, and but where we cannot keep both measures small simultaneously.

Theorem 8 (Thapen, 2014)**.** *Fix a small constant $\varepsilon > 0$. Take any sufficiently large m such that both m and m^ε are powers of two. There is a CNF Φ_m with $\Theta(m^{1+2\varepsilon})$ variables and $\Theta(m^{1+3\varepsilon})$ clauses, of width $O(\log m)$, such that*

1. *Φ_m has a refutation of length $O(m^{1+3\varepsilon})$ and width $m + O(\log m)$;*
2. *Φ_m has a refutation of width $O(m^\varepsilon)$;*
3. *Φ_m has no subexponential length refutation of width strictly less than m.*

Using Theorem 2 and item 1 on Φ_m we get that the formula has a refutation of width $O(m^{1/2+\varepsilon} \log m)$. By item 3, though, when $\varepsilon < 1/2$ every such refutation requires exponential length.

[3] E.g. for the partial assignment $\rho = \{x = 0, y = 1\}$ we get $C_\rho = x \vee \bar{y}$.

[4] Neil Thapen. A trade-off between length and width in resolution. Technical Report TR14-137, Electronic Colloquium on Computational Complexity, 2014

Regarding the other question we refer to the work of Bonet and Galesi[5] where they build a formula with a small refutation which requires large width, but just not so large that Corollary 6 would kick in.

Theorem 9 (Bonet and Galesi, 2001)**.** *There exists a* 3*-CNF over* $O(m^2)$ *variables so that*

- *has* $O(m^3)$ *clauses;*
- *has a refutation of length* $m^{O(1)}$*;*
- *requires refutation width* $\Omega(m)$*.*

The formula is a variant of the Ordering principle. The unsatisfiable CNF encoding of this principle claims that a set of m elements can be partially ordered $\prec$ so that every element has at least one predecessor. Variable x_{ij} for $i \neq j$ and $i, j \in [m]$ encodes that the element $i \prec j$. The clauses of the ordering principle are.

$$\begin{aligned} &\bar{x}_{ij} \vee \bar{x}_{ji} && \text{for every distinct } i, j \in [m]; && (1)\\ &\bar{x}_{ij} \vee \bar{x}_{jk} \vee x_{ik} && \text{for every distinct } i, j, k \in [m]; && (2)\\ &\bigvee_{i \neq j} x_{ij} && \text{for every } j \in [m]. && (3) \end{aligned}$$

The clauses (1) and (2) ensure that the variables are encoding a partial order, while the clauses (3) ensure that each element has at least a predecessor. In (Bonet and Galesi, 2001) they actually prove a width $\Omega(m)$ lower bound for the 3-CNF version of this formula.

Exercise 10. Show that the ordering principle introduced before has a refutation of polynomial size and width $O(m)$. *(Hint: from the ordering principle of* m *elements, try to deduce the ordering principle of* $m - 1$ *elements.)*

Width lower bounds

We are going to see some exponential size lower bounds for resolution refutation based on width lower bounds. In particular we will get exponential lower bounds for

- random 3-CNFs;
- Tseitin formulas on expander graphs;
- sparse version of pigeonhole principle.

This section is based on (Ben-Sasson, Wigderson, 2001).[6] In all the lower bounds the strategy is essentially the same. We need to show that

1. there is a clause in the proof that is minimally implied by a large set of initial constraints;
2. the literals in that clause correspond to the "boundary" of those initial constraints, where the boundary is intended to arise from the graph structure of the formula;

[5] Maria Luisa Bonet and Nicola Galesi. Optimality of size-width tradeoffs for resolution. *Computational Complexity*, 10(4):261–276, 2001

[6] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001

3. if the graph is an expander, then the boundary must be large, and therefore the width of the clause is large as well;

4. we use Corollary 6 to get a size lower bound.

We need the following lemma to count literals in a clause, and then get width lower bounds.

Lemma 11. *Let $A_1, A_2, \ldots, A_\ell$ a set of clauses so that*

- *collectively, they logically implies a clause C;*
- *no strict subset of them logically implies;*

then C contains all variables that occur exactly once among clauses $A_1, \ldots, A_\ell$.

Proof sketch. Consider a variable x occurring only in A_i. Without loss of generality we assume x occurs positively. We want to show that literal x occurs in C. Since by minimality $\{A_1, \ldots, A_\ell\} \setminus \{A_i\}$ does not imply C, there is an assignment ρ that satisfies it, but simultaneously falsify C and (consequently) A_i. Therefore ρ sets x to false. We consider ρ' equal to ρ but with x set to true. The value of the clauses $\{A_1, \ldots, A_\ell\} \setminus \{A_i\}$ does not change, since they do not mention variable x. But now A_i is satisfied too and therefore ρ' must satisfy C. Clause C passed from false to true by only changing the value of variable x from false to true. Therefore C contains variable x. □

Random 3*-CNF*

We consider random 3-CNFs over n variables and $m = \Delta n$ clauses (Δ is called the clause density). The formula is sampled by sampling Δn times with repetition from the set of all $8\binom{n}{3}$ clauses.

Chvátal and Szemerédi showed that with high probability a random 3-CNF sampled according to this distribution where Δ is a constant larger than $8 \ln 2$, is unsatisfiable and requires exponential size refutations.[7] The lower bound was extended to higher formula density in (Beame et al. 2002), and the proof has been simplified and rephrased later in term of width lower bound by (Ben-Sasson, Wigderson 2001).[8]

To study this formula we need to study the underlying bipartite graph structure.

Definition 12 (Bipartite matchability and expansion)**.** *Consider a bipartite graph $G = (V, U, E)$. For any $V' \subset V$ we define*

$$N(V') = \{u \in U | (v, u) \in E, v \in V'\} \qquad \textit{(neighborhood)} \qquad (4)$$

$$\partial V' = \{u \in U || N(u) \cap V'| = 1\} \qquad \textit{(boundary)}\ . \qquad (5)$$

A bipartite graph is a (r, ε)-boundary expander[9] *if for every V' of size between $r/2$ and r, $|\partial V'| \geq \frac{c|V'|}{2}$. A bipartite graph is matchable up to r vertices if for every V' with at most r vertices, $|N(V')| \geq |V'|$.*

[7] Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988

[8] Paul Beame, Richard M. Karp, Toniann Pitassi, and Michael E. Saks. The efficiency of resolution and davis–putnam procedures. *SIAM J. Comput.*, 31(4):1048–1075, 2002; and Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001

[9] There are several notions of boundary expansion in literature, they are similar but not entirely equivalent. In particular (Beame et al. 2002) use a different, but equivalent concept in their paper.

Exercise 13. Show that if the left side had degree 3, then

$$|\partial V'| \geq 2N(V') - 3|V'| \,. \tag{6}$$

We are going to consider the formula as a bipartite graphs. For a CNF $\phi = \bigwedge_{i=1}^{m} C_i$ over variables $x_1, x_2, \ldots, x_m$ we consider the biparite graph $G_\phi([m], [n], E)$ where $(j, i) \in E$ if clauses C_j contains either the literal x_i or the literal $\bar{x}_i$. A random 3-CNF formula induces a random bipartite graph of degree 3 on the left side. Such graph has good expansion and good matchability, accoding to the following claim that we don't prove.

Proposition 14 (Lemma 11 in Beame et at. 2002)**.** *For any $0 < \varepsilon < 1$ there is a constant $c_\varepsilon > 0$ so that for a random 3-CNF ϕ over n variables and $m = \Delta n \geq n$ clauses the following holds. If $r \leq c_\varepsilon n \cdot \Delta^{-\frac{2}{1-\varepsilon}}$ then with high probability in r the graph G_ϕ*

- *is a (r, ε)-boundary expander;*
- *is matchable up to r vertices.*

From these characteristic of the graph we get the width lower bound.

Theorem 15. *For any $0 < \varepsilon < 1$ there is a constant $c_\varepsilon > 0$ so that for a random 3-CNF ϕ over n variables and $m = \Delta n \geq n$ clauses the following holds. With high probability ϕ is unsatisfiable and requires a refutation of width $\Omega\big(n \cdot \Delta^{-\frac{2}{1-\varepsilon}}\big)$.*

Proof Sketch. Fix $r = c_\varepsilon n \cdot \Delta^{-\frac{2}{1-\varepsilon}}$ as in the statement of Proposition 14. For every clause C in the refutation we define a complexity measure μ, which is size of the smallest set of initial clauses of ϕ that implies C. Measure μ satisfies:

- $\mu(C) = 1$ when C is an initial clauses;
- subadditivity, namely if C is derived by A and B, then $\mu(C) \leq \mu(A) + \mu(B)$;
- $\mu(\bot) > r$ because G_ϕ is matchable up to r vertices on the left side, any set of r clauses are satisfiable.

For these reasons there must be in the proof a clause C with $\frac{r}{2} \leq \mu(C) \leq r$. Consider any such clause C and let be $V' \subseteq [m]$ the indices of the clauses that minimally imply C. The key step is to show that *clause C must contain one literal per edge in the boundary of V'*. By expansion we get that C has width $\varepsilon|V'| \geq \varepsilon r/2$. □

Corollary 16. *Consider any $0 < \gamma \leq 1/4$ and take a random 3-CNF ϕ over n variables and Δn clauses with $\Delta \approx n^{1/4-\gamma}$. With high probability ϕ requires a refutation of size at least*

$$\exp(\Omega(n^{\frac{4\gamma-\varepsilon}{1-\varepsilon}})) \tag{7}$$

for every $0 < \varepsilon < 4\gamma$.

Some observations on this results: for $\gamma > 0$ we can still get lower bound $\exp\left(n^{\Omega(1)}\right)$, and in particular for unsatisfiable random 3-CNF with $O(n)$ clauses resolution needs exponential size refutations with high probability.

This result implies that random 3-CNF with $n^{5/4-\gamma}$ clauses require super polynomial refutations. In (Ben-Sasson and Galesi, 2003)[10] they show a stronger bound for tree-like resolution which excludes no polynomial size refutations for $n^{2-\gamma}$ clauses which essentially matches a tree-like upper bound in (Beame et al. 2002). In Eli Ben-Sasson's PhD Thesis the results have been further improved. He shows stronger width lower bounds for random 3-CNF, and obtain consequently a superpolynomial size lower bound for resolution refutations of random 3-CNF with up to $n^{3/2-\gamma}$ clauses.[11].

Open Problem 17. *Does such lower bound hold for general resolution as well? Nothing excludes that random* 3*-CNF formulas may be hard for resolution even at $n^{2-\gamma}$ clauses.*

Interestingly enough around $n^{3/2}$ clauses it is possible to use spectral analysis and that can refute random 3-CNF in polynomial time with high probability. These techiques are definitely different from resolution.

Exercise 18. Use the statements in Exercise 7 and in Proposition 14 to prove that for any $0 < \gamma \leq 1/2$ and a random 3-CNF ϕ over n variables and Δn clauses with $\Delta \approx n^{1/2-\gamma}$ requires a refutation of size at least

$$\exp(n^{\Omega(1)}) \tag{8}$$

with high probability.

Graph Pigeonhole Principle

The graph pigeonhole principle is a variant of the pigeonhole principle formula. In this case each pigeon can only go in one among a restricted set of holes. The structure of this formula is naturally expressed as a bipartite graph $G = (P, H, E)$, so the that clauses are

$$\bigvee_{j \in N(i)} p_{i,j} \qquad \text{for every } i \in P; \tag{9}$$

$$\bar{p}_{i,j} \vee \bar{p}_{i',j} \qquad \text{for every distinct } i, i' \in P \text{ and } j \in N(i) \cap N(i'). \tag{10}$$

Theorem 19. *Assume that $\{G_n = (P, H, E)\}_{n \in \mathbb{N}}$ is a bipartite graph family such that*

- *$|P| = n + 1$ and $|H| = n$;*
- *each pigeon in P can go in at most $O(1)$ holes;*
- *G is matchable up to αn vertices, for some $\alpha > 0$;*
- *G is an $(\beta n, \Omega(1))$-boundary expander, for some $\beta \leq \alpha$.*[12]

[10] Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Struct. Algorithms*, 23(1):92–109, 2003

[11]

[12] In the original paper they use a different notion of expansion, but Definition 12 will do here.

The graph pigeohole principle formula over G is unsatisfiable but it requires resolution refutation of width $\Omega(n)$, and therefore exponential size refutations.

Proof. We will see the proof in class. □

Such graphs exist, and indeed these features hold with high probability in a random bipartite graph with left degree 3, $n+1$ vertices on the left and n vertices on the right.

Exercise 20. Use the previous result to give another proof of a $2^{\epsilon n}$ lower bound for the size of resolution refutations of the standard pigeonhole principle.

Exercise 21. Prove that the standard pigeonhole principle has a refutation of width $O(n)$. Deduce that it is not possible to get a refutation size lower bounds using Corollary 6 directly.

Tseitin formula

We start with a connected graph G in which each vertex is labeled by $\{0,1\}$ value. A labeling is *odd* if the sum of the values over all vertices is odd. A labeling is even otherwise. The Tseitin formula claims that it is possible to put a $\{0,1\}$ value on each edge of the graph so that the sum of the values on the edges incident to a vertex is equal (mod 2) to the value on the vertex.

Example 22. Consider a triangle graph on vertices u, v, w, labeled respectively by $1, 0, 0$, respectively, and edges e_{uv}, e_{vw}, e_{wu}. The formula has one variable per edge, and it claims that the following linear system is satisfiable.

$$\begin{aligned} e_{uv} + e_{wu} &= 1 \pmod 2 \\ e_{uv} + e_{vw} &= 0 \pmod 2 \\ e_{vw} + e_{wu} &= 0 \pmod 2 \,. \end{aligned}$$

Any parity constraint over d variable can be encoded with 2^{d-1} clauses, therefore the final CNF is

$$\begin{aligned} & e_{uv} \lor e_{wu} \\ & \bar{e}_{uv} \lor \bar{e}_{wu} \\ & \bar{e}_{uv} \lor e_{vw} \\ & e_{uv} \lor \bar{e}_{vw} \\ & \bar{e}_{vw} \lor e_{wu} \\ & e_{vw} \lor \bar{e}_{wu} \,. \end{aligned}$$

Exercise 23. Prove that for every connected graph G, the Tseitin formula is satisfiable if and only if the sum of the labels on all vertices is even. Show that when it is not satisfiable, it is always possible to satisfy any set of $|V(G)| - 1$ parity constraints.

For the sake of this result we will use a different notion of expansion over graphs.

Definition 24 (Graph edge expansion)**.** *Consider a graph $G = (V, E)$. For any $S \subseteq V$ we define the edge boundary of a set of vertices as*

$$e(S, \bar{S}) = \{\{u, v\} \in E | u \in S, v \in \bar{S}\}, \tag{11}$$

and we define the edge expansion $e(G)$ of a graph as the minimum, among all subsets S of vertices with $\frac{1}{3}|V| \leq |S| \leq \frac{2}{3}|V|$, of

$$\frac{e(S, \bar{S})}{|S|} . \tag{12}$$

A graph is an edge expander if $e(G) = \Omega(1)$.

In literature it is possible to find connected d-regular graph with constant edge expansion, for $d \geq 3$ (See the survey on expander graphs [13]). Any such graph then induced an exponentially hard formula for resolution, as proved originally in (Urquhart, 1987).[14].

Theorem 25. *Consider a d-regular edge expander graph G over n vertices, and pick any odd labeling of its vertices. The corresponding Tseitin formula ϕ is unsatisfiable and any refutation requires $\Omega(n)$ width.*

Proof sketch. For every clause C in the refutation we define a complexity measure μ, which is size of the smallest set of initial *parity constraints* of ϕ that implies C. Measure μ satisfies:

- $\mu(C) = 1$ when C is an initial clauses;
- subadditivity, namely if C is derived by A and B, then $\mu(C) \leq \mu(A) + \mu(B)$;
- $\mu(\perp) = n$ because all sets of $n - 1$ parity constraints are satisfiable.

For these reasons there must be in the proof a clause C with $\frac{n}{3} \leq \mu(C) \leq \frac{2}{3}n$. Consider any such clause C and let be $S \subseteq V(G)$ the set of vertices which parities minimally imply C. The key step is to show that *clause C must contain one literal per edge in in $E(S, \bar{S})$*. By expansion we get that C has width $\Omega(|S|) = \Omega(n)$. □

References

[ALN14] Albert Atserias, Massimo Lauria, and Jakob Nordstrom. Narrow proofs may be maximally long. In *Computational Complexity (CCC), 2014 IEEE 29th Conference on*, pages 286–297. IEEE, 2014.

[BG01] Maria Luisa Bonet and Nicola Galesi. Optimality of size-width tradeoffs for resolution. *Computational Complexity*, 10(4):261–276, 2001.

[BKPS02] Paul Beame, Richard M. Karp, Toniann Pitassi, and Michael E. Saks. The efficiency of resolution and davis–putnam procedures. *SIAM J. Comput.*, 31(4):1048–1075, 2002.

[13] Shlomo Hoory, Nati Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43(4):439–561, 2006

[14] A. Urquhart. Hard examples for resolution. *Journal of the ACM (JACM)*, 34(1):209–219, 1987

[BSG03] Eli Ben-Sasson and Nicola Galesi. Space complexity of random formulae in resolution. *Random Struct. Algorithms*, 23(1):92–109, 2003.

[BSW01] Eli Ben-Sasson and Avi Wigderson. Short proofs are narrow - resolution made simple. *J. ACM*, 48(2):149–169, 2001.

[CS88] Vašek Chvátal and Endre Szemerédi. Many hard examples for resolution. *J. ACM*, 35(4):759–768, 1988.

[HLW06] Shlomo Hoory, Nati Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc.*, 43(4):439–561, 2006.

[Tha14] Neil Thapen. A trade-off between length and width in resolution. Technical Report TR14-137, Electronic Colloquium on Computational Complexity, 2014.

[Urq87] A. Urquhart. Hard examples for resolution. *Journal of the ACM (JACM)*, 34(1):209–219, 1987.