

Due on November 10
In class, at the beginning of the lecture

The work you submit must be your own. You may discuss problems with each other; however, you should prepare written solutions alone. In particular, you should not leave with any written notes from such discussions. The style and clarity of your answers will be an important factor in the grade.

There are 5 questions, 20% each.

1. If C is a clause, let the *width* of C , $w(C)$ denote the number of literals in C . Extend this definition to a set of clauses \mathcal{C} in the obvious way: $w(\mathcal{C})$ is the largest width of all the clauses in \mathcal{C} . Also, if P is a resolution refutation, let $w(P)$ be the largest width of all the clauses in P . Finally, let $sw(\mathcal{C})$ be the smallest width of any resolution refutation of \mathcal{C} .
 - (a) Show that any tree-like resolution refutation of \mathcal{C} of size s can be converted to one of width bounded above by $(\lceil \log s \rceil + w(\mathcal{C}))$.
 - (b) Conclude that any tree-like resolution refutation of \mathcal{C} requires size

$$\Omega(2^{sw(\mathcal{C})-w(\mathcal{C})}).$$

2. Let $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be a function. We say that a propositional refutation system V is $f(n, s)$ -automatizable iff there exists an algorithm A_V which on input \mathcal{C} , $|\mathcal{C}| = n$, outputs a refutation P of \mathcal{C} in time at most $f(n, s)$ where s is the size of the shortest refutation of \mathcal{C} . (Note that we use \mathcal{C} , since we are thinking of clauses, but this definition is more general.) Show that for k -CNF formulas, tree resolution is $s^{O(\log n)}$ -automatizable.
3. Let $\alpha(\vec{p}, \vec{q}) \wedge \beta(\vec{p}, \vec{r})$ be an unsatisfiable CNF formula. (Letting $\vec{p} = p_1, p_2, \dots, p_n$.) A *Craig interpolant* (just *interpolant* from now on), is any function C such that given a value assignment \vec{p}_0 to \vec{p} :

$$C(\vec{p}_0) = \begin{cases} 0 & \alpha(\vec{p}_0, \vec{q}) \text{ is unsatisfiable} \\ 1 & \beta(\vec{p}_0, \vec{r}) \text{ is unsatisfiable} \end{cases}$$

Show the following: if for every unsatisfiable formula $\alpha(\vec{p}, \vec{q}) \wedge \beta(\vec{p}, \vec{r})$ there exists a polynomial time computable interpolant (i.e., there is a polytime algorithm for computing C), then $\mathbf{NP} \cap \mathbf{co-NP} \subseteq \mathbf{P/poly}^1$.

4. Let $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be a function. We say that a propositional refutation system V has $f(n, s)$ -*interpolation* iff given $\alpha(\vec{p}, \vec{q}) \wedge \beta(\vec{p}, \vec{r})$ with minimum refutation size s , there exists a circuit of size at most $f(s)$ computing the interpolant C for $\alpha(\vec{p}, \vec{q}) \wedge \beta(\vec{p}, \vec{r})$. We say that the interpolation is feasible if f is polytime, and monotone if whenever \vec{p} occur only positively in α (or only negatively in β) the circuit computing the interpolant is monotone. Show the following: if a refutation system V has feasible interpolation, and if \mathbf{NP} is not contained in $\mathbf{P/poly}$, then V is not polynomially bounded.

¹Note that the most prominent problem to be in $\mathbf{NP} \cap \mathbf{co-NP}$ is factoring. Strictly speaking, as it is not a decision problem, it is in \mathbf{TFNP} , the set of total functional \mathbf{NP} problems; see Papadimitriou, §10.3.

5. Razborov's theorem says that there exists an ε such that for sufficiently large n , and $m = \frac{n}{10}$, any monotone circuit which outputs a 1 on all m -cliques, and a 0 on all $(m - 1)$ -co-cliques, requires size 2^{n^ε} . This is a beautiful result presented in Papadimitriou in section 14.4 (albeit, with a slightly different statement). Assume this theorem for what follows.
- (a) Show that if V has monotone feasible interpolation, then V is not polynomially bounded. To do this question, consider the formula $\alpha(\vec{p}, \vec{q}) \wedge \beta(\vec{p}, \vec{r})$, where \vec{p} encodes an undirected graph G over n vertices, so you can think of \vec{p} as p_{ij} , $i, j \in [n]$. Show how to construct $\alpha(\vec{p}, \vec{q})$ which asserts that \vec{p} has a clique of size m , and $\beta(\vec{p}, \vec{r})$ asserts that \vec{p} has a co-clique of size $(m - 1)$. (Recall that a clique of size m is a subset of m vertices, which is fully connected, and a co-clique of size $(m - 1)$ is a partition of the vertices of the graph into $(m - 1)$ sets, so that all edges are between sets, and no edges within a set.) Give the specifics of α, β . Then, assume for the sake of contradiction that V has monotone feasible interpolation and that it is polybounded.
- (b) Show that resolution has monotone feasible interpolation, and draw the obvious conclusion. To do this question, assume that $\alpha(\vec{p}, \vec{q})$ and $\beta(\vec{p}, \vec{q})$ are two sets of clauses, and that $\alpha \cup \beta$ is unsatisfiable. Suppose we have a resolution refutation P of $\alpha \cup \beta$. Show how to compute an interpolant from P .