Problem set 1 — Proof systems and Resolution

Massimo Lauria — lauria.massimo@gmail.com
Office 1107, Ookayama West 8th Building

(This document was updated on June 21, 2017)

Due: Friday, November 6th, 2015 at 10:45. Submit your solutions as a PDF file by e-mail to lauria.massimo@gmail.com with the subject line

`Problem set : ⟨your full name⟩`

Name the PDF file `PS1⟨YourFullName⟩.pdf` (with your name coded in ASCII without national characters and no spaces), and also state your name (in both national and latin character) and e-mail address at the top of the first page. Solutions should be written in LaTeX or some other math-aware typesetting system. Please try to be precise and to the point in your solutions and refrain from vague statements. If you are not confident with English please limit yourself to simple, short and clear sentences. Nevertheless the solutions needs to be explained in reasonable precision. *Write so that a fellow student of yours can read, understand, and verify your solutions.*

Collaboration: Discussions of ideas in groups of two people are allowed—and indeed, encouraged—but you should write down your own solution individually and understand all aspects of it fully. You should also acknowledge any collaboration. State at the beginning of the problem set if you have been collaborating with someone and if so with whom.

Reference material: Some of the problems are "classic" and hence it might be easy to find solutions on the Internet, in textbooks or in research papers. **Please don't do that.**

☺ You can use and refer to anything said during the lectures or written in the lecture notes.

☹ You cannot use textbooks/internet/papers to find the answer to the problems in the set.

☺ You can refer to research papers/textbooks/internet for those proofs that we saw in class, either because they are missing from the lecture notes or because you feel the lecture notes are not clear enough.

☹ The previous permission does not apply to missing pieces of those proofs that the lecturer explicitly asked you to prove as an exercise.

It is hard to pin down 100% formal rules on what all this means—when in doubt, ask the lecturer. Obviously these rules are designed with honest students in mind. I am confident that there is no need to develop rules against malicious students.

Assessment of the final grade: Some of the problems are meant to be quite challenging and you are not necessarily expected to solve all of them. As a general guideline, **a total score of 80 should be sufficient to pass**. Partial score may be given for partial solutions and for partially (but mostly) correct solutions. Please refrain from providing answers if you are not confident of their correctness. The tentative plan it to have three problem sets, published:

- at the 3rd lecture;
- at the 6th or 7th lecture;
- at the 10th lecture.

Passing three problem sets is sufficient to pass the course. If a student fails to pass one problem set by a small amount of points, he/she could still pass the course if he/she has a good score (well above pass) at the other two problem sets. How good depends on how far for the threshold the student was in the failed problem set.

The total points and the passing thresholds of the three problem sets may be different. Beware that the each passing threshold may be lowered (but never increased!) during the grading.

Problem 1 (15 points)**.** *Prove that for any propositional formula $\Psi(\vec{x})$ over connectives $\{\neg, \vee, \wedge, \rightarrow\}$ there exists a CNF $\phi(\vec{x}, \vec{y})$ such that Ψ is a tautology if and only if ϕ is unsatisfiable, and ϕ has length at most linear in the length of Ψ.*

Problem 2 (10 points)**.** *Prove the equivalence of the two definition of proof systems given in the first lecture. Namely show that any proof system according to the classic definition can be transformed in a proof system according to the verifier definition, and vice versa, so that the length of proofs has at most a polynomial increase.*

Problem 3 (15 points)**.** *Prove that any resolution derivation of C from ϕ that uses weakening rule can be transformed into a resolution derivation of some $C' \subseteq C$ that does not use the weakening rule and has width and length no larger than the original derivation. In particular this shows that the weakening rule is not necessary for resolution refutations.*

For the next exercise we recall the definition of decision-tree.

Definition. *A decision tree for a CNF ϕ is a rooted binary tree where each internal node is labeled by a variable of ϕ and has two outgoing edges labeled by 0 and 1, respectively, and where no variable labels two nodes on any root-to-leaf path. For any node q in the tree we associate an assignment ρ_q as follows: if q is the root then $\rho_q = \emptyset$; if q has parent p then $\rho_q = \rho_p \cup \{x = b\}$ where x is the variable labeling node p and $b \in \{0,1\}$ is the value associated to the edge from p to q.*

If ρ_q neither satisfy nor falsify ϕ then q must be an internal node. When in instead q is a leaf node, its label is either

- *the value $\top$ when ρ_q satisfies formula ϕ; or*
- *a clause of ϕ that is falsified by ρ_q.*

Problem (Optional for self-study, do not submit this)**.** *Build a decision tree for the following satisfiable 2-CNF.*

$$p_{11} \vee p_{12} \tag{1}$$
$$p_{21} \vee p_{22} \tag{2}$$
$$p_{31} \vee p_{32} \tag{3}$$
$$\bar{p}_{11} \vee \bar{p}_{21} \tag{4}$$
$$\bar{p}_{11} \vee \bar{p}_{21} \tag{5}$$
$$\bar{p}_{21} \vee \bar{p}_{31} \tag{6}$$
$$\bar{p}_{12} \vee \bar{p}_{22} \tag{7}$$
$$\bar{p}_{12} \vee \bar{p}_{32}\ . \tag{8}$$

Now build a decision tree for the unsatisfiable CNF which contains the same clauses as before, plus the clause

$$\bar{p}_{22} \vee \bar{p}_{32}\ . \tag{9}$$

Problem 4 (15 points)**.** *Show that an unsatisfiable CNF formula ϕ has a decision tree with at most S nodes if and only if it has a tree-like resolution refutation of length at most S.*

Problem 5 (5 points)**.** *Using the previous result, prove that any unsatisfiable ϕ has a resolution refutation.*

Recall the definition of the pigeonhole principle from Lecture 2.

Problem 6 (15 points)**.** *Find a pigeohole principle resolution refutation of size $2^{O(n \log n)}$.*
(Hint: build a decision tree of size roughly $O(n!)$, which is $2^{O(n \log n)}$.)

Problem (Optional for self-study, this maybe hard)**.** *Find a pigeohole principle resolution refutation of size $2^{O(n)}$.*

Recall the definition of Prosecutor/Defendant from Lecture 2.

Problem 7 (15 points)**.** *Show that from any Prosecutor strategy there is a corresponding resolution refutation of essentially the same size (a linear factor blow up is fine). Furthermore, if the Prosecutor never deletes infomation from the record, then the refutation can be made tree-like.*

Problem 8 (10 points)**.** *Consider a resolution derivation π of C from ϕ, where $\pi = (C_1, C_2, \ldots, C_\ell)$. Build a resolution derivation (denoted by $\pi\restriction_\rho$) that derives $C\restriction_\rho$ from $\phi\restriction_\rho$, using at most the same length and width of the original derivation π, and according to the following observation regarding the list of restricted formulas $(C_1\restriction_\rho, C_2\restriction_\rho, \ldots, C_\ell\restriction_\rho)$.*[1]

- *A resolution step which resolve on variables x can be turned into a weakening step in x is assigned by ρ;*
- *all occurrences of formula $\top$ can be removed from the derivation.*

[1] Not all these formulas are proper clauses. The ones satiafied by ρ are occurrences of the true formula $\top$.

Problem 9 (10 points)**.** *Observe that for every partial assignment ρ there is a unique minimal clause C_ρ that is falsified by ρ.*

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 $w + |dom(\rho)|$.

Problem 10 (30 points)**.** *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 $k + \log(S_T)$.*

Problem (Optional for self-study, do not submit this)**.** *Show that if a formula ϕ has refutations of width w, then it is possible to produce one such refutation in time $n^{O(w)}$.*

Problem 11 (20 points)**.** *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.)

Problem 12 (5 points)**.** *Show that in a bipartite graph $G = (V, U, E)$, if the left side had degree 3, then*

$$|\partial V'| \geq 2N(V') - 3|V'| \tag{10}$$

for all $V' \subseteq V$.

Problem 13 (15 points)**.** *Use the statements in Exercise 10 and in Proposition 13 in lecture 3 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*

$$\exp\left(n^{\Omega(1)}\right) \tag{11}$$

with high probability.

Problem 14 (10 points)**.** *Use the width lower bound for pigeonhole principle over bipartite graphs to give another proof of the $2^{\varepsilon n}$ lower bound for the size of resolution refutations of the standard pigeonhole principle.*

Problem 15 (5 points)**.** *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 in lecture 3 directly.*

Problem 16 (15 points)**.** *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.*

Problem (Optional for self-study, do not submit this)**.** *Fix any $b \in \{0,1\}$. Prove that the equation*

$$x_1 + x_2 + \cdots + x_d = b \pmod 2 \tag{12}$$

over boolean variables $x_1, x_2, \ldots, x_d$ can be represented as 2^{d-1} clauses. Essentially you need to show that there are 2^{d-1} clauses over $x_1, x_2, \ldots, x_d$ that are satisfied by an assignment if and only if the assignment satisfies the equation.

References