KTH Computer Science
and Communication

Current Research in Proof Complexity: Problem Set 2

Due: January 8, 2012. Submit as a PDF-file by e-mail to `jakobn at kth dot se` with the subject line `Problem set 2: ⟨your name⟩`. 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. In addition to what is stated below, the general rules stated on the course webpage always apply.

Hints: For most or all problems, "hints" can be purchased at a cost of 5–10 points. In this way, you can configure yourself whether you want the problems to be more creative and open-ended, where sometimes a lot can depend on finding the right idea, or whether you want them to be more of guided exercises providing a useful work-out on the concepts of proof complexity. If you do not solve a problem, there is no charge for the hint (i.e., it is not deducted from the score on other problems).

Collaboration: Discussions of ideas in groups of two to three people are allowed—and indeed, encouraged—but you should write down your own solution individually and understand all aspects of it fully. For each problem, state at the beginning of your solution with whom you have been collaborating. Everybody collaborating on a certain problem is considered to have purchased a hint if one of the collaborators has done so.

Reference material: Some of the problems below are "classic" and hence their solutions can probably be found on the Internet or in research papers. It is not allowed to use such solutions in any way unless explicitly stated otherwise. Anything said during the lectures on in the lecture notes should be fair game, though, unless you are specifically asked to show something that we claimed without proof in class. It is hard to pin down 100% formal rules on what all this means—when in doubt, ask the lecturer.

About the problems: Some of these 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 around 120 points on this problem set should be enough to get a pass. Any corrections or clarifications will be posted on the course webpage `www.csc.kth.se/~jakobn/teaching/proofcplx11`.

1 (10 p) In class, we defined the canonical "3-CNF version" $\widetilde{F}$ of a CNF formula F and claimed somewhat handwavingly that $\widetilde{F}$ is equivalent to F. We want to make this claim more formal.

1a Prove that $\widetilde{F}$ is unsatisfiable if and only if F is unsatisfiable.

1b Prove that $\widetilde{F}$ is minimally unsatisfiable if and only if F is minimally unsatisfiable.

2 (10 p) Prove that polynomial calculus resolution (PCR) can polynomially simulate resolution by showing that given any resolution refutation $\pi : F \vdash \bot$, PCR can simulate this refutation line by line in almost the same length, size and space (where we assume that the field is finite so that coefficients do not matter, and where the space measures compared are clause space for resolution and monomial space for PCR). Making clear what "almost" means is part of the problem, but any increase should be small.

3 (10 p) Prove that $Deg_{\mathcal{PC}}(F \vdash \bot) = Deg_{\mathcal{PCR}}(F \vdash \bot)$ for any unsatisfiable CNF formula F.

4 (30 p) Decide whether the CNF formulas in the formula families below are minimally unsatisfiable or not. If you claim that formulas in a family are minimally unsatisfiable, a formal proof of this is needed that works for any formula in the family. If you claim that formulas are not necessarily minimally unsatisfiable, just one counter-example is needed together with a proof that this formula is not minimally unsatisfiable.

4a Pigeonhole principle formulas PHP_n^{n+1}.

4b Tseitin formulas $Ts(G, f)$ for any connected undirected graph G and any odd-weight function f, and with the encoding described in class and in the scribe notes. (If you wish, you may focus on graphs with at most three edges incident to any vertex for simplicity and still get full credit.)

4c Partial ordering principle formulas POP_n.

4d Linear ordering principle formulas LOP_n.

5 (30 p) What is the smallest length of a refutation of $\widetilde{POP}_n$ that you can find based on what was outlined in class, and what is the clause space of this refutation (expressed in terms of the parameter n, say)? Can you prove that it is not possible to do better? For full credit, a refutation in asymptotically optimal length and clause space is needed (ignoring constant factors hidden in the big-oh notation) plus a proof that this refutation is asymptotically optimal.

6 (50 p) Prove that if a CNF formula F of size n is refutable in resolution in constant total space, then it is refutable in constant total space and length polynomial in n simultaneously. That is, in formal notation, if $TotSp(F \vdash \bot) = O(1)$, then there is a resolution refutation $\pi : F \vdash \bot$ with $L(\pi) = \mathrm{poly}(n)$ and $TotSp(\pi) = O(1)$. Does the same claim hold for clause space instead of total space? Prove that the answer is yes or explain why it seems hard to generalize the proof for total space.

7 (60 p) Define the *negative width* $W^-(C)$ of a clause C to be the number of negated literals in C. Let the negative width of a resolution refutation π be $W^-(\pi) = \max_{C \in \pi}\{W^-(C)\}$ and let $W^-(F \vdash \bot)$ be the minimal negative width of any resolution refutation of F.

7a Prove that resolution refutations in negative width $O(1)$ can be efficiently simulated line by line by polynomial calculus (PC) refutations.

7b Prove that for any unsatisfiable k-CNF formula F, it holds that $W^-(F \vdash \bot) \leq k$.

Hint: Use induction over the number of variables.

7c Using the facts proven above, show that any k-CNF formula in size n can be refuted in PC in simultaneous size $\exp(O(n))$ and monomial space $O(n)$, where the constants hidden in the asymptotic notation depend on k.

8 (60 p) Define a new proof system *binary implicational resolution (BIR)* to be a sequential proof system where proof lines are disjunctive clauses, just as in resolution, but where the inference rule is that any clause D that is *semantically implied* by two clauses C_1, C_2 in the current clause configuration $\mathbb{C}$ can be derived in one step. Let $L_{\mathcal{BIR}}(F \vdash \bot)$ and $Sp_{\mathcal{BIR}}(F \vdash \bot)$ denote the minimal length and clause space of refuting the formula F in binary implicational resolution.

Define *full implicational resolution (FIR)* to be a sequential proof system with disjunctive clauses as proof lines where the inference rule is that any clause D that is *semantically implied* by the full current clause configuration $\mathbb{C}$ can be derived in one step, and let $L_{\mathcal{FIR}}(F \vdash \bot)$ and $Sp_{\mathcal{FIR}}(F \vdash \bot)$ denote the minimal length and clause space of refuting the formula F.

8a What is the relation of $L_{\mathcal{BIR}}(F \vdash \bot)$ and $Sp_{\mathcal{BIR}}(F \vdash \bot)$ to the corresponding measures $L_{\mathcal{R}}(F \vdash \bot)$ and $Sp_{\mathcal{R}}(F \vdash \bot)$ in standard resolution? Does length increase or decrease? By how much? Does clause space increase or decrease? By how much? Is BIR a propositional proof system in the sense defined in lecture 1?

8b What is the relation of $L_{\mathcal{FIR}}(F \vdash \bot)$ and $Sp_{\mathcal{FIR}}(F \vdash \bot)$ to $L_{\mathcal{R}}(F \vdash \bot)$ and $Sp_{\mathcal{R}}(F \vdash \bot)$? Does length and/or clause space increase or decrease? By how much? Is FIR a propositional proof system in the sense defined in lecture 1?

Getting the answers to the questions above about length and space right to within constant factors (that can be hidden in the asymptotic notation) is sufficient for full credit.