HOMEWORK 8, CPSC 421/501, FALL 2019

JOEL FRIEDMAN

Please note:

(1) You must justify all answers; no credit is given for a correct answer without justification.
(2) Proofs should be written out formally.
(3) Homework that is difficult to read may not be graded.
(4) You may work together on homework, **but you must write up your own solutions individually.** You must acknowledge with whom you worked. You must also acknowledge any sources you have used beyond the textbook and two articles on the class website.

---

(1) Consider the Boolean variables $x_{ij\gamma}$, y_{ij}, and z_{iq} to describe the configuration of a non-deterministic Turing machine at step i as in class to prove that SAT and 3SAT are NP-complete (see notes of November 1, 4, and 6).[1]
   (a) What is the meaning of the formula
   $$(x_{i,j,\sigma} = true) \wedge (y_{i,j} = true) \wedge (z_{i,q} = true)$$
   ($\wedge$ means AND) in terms of the Turing machine configuration at step i?
   (b) Explain why the formula in part (a) has the same true/false values as
   $$x_{i,j,\sigma} \wedge y_{i,j} \wedge z_{i,q}$$
   (c) Explain the meaning of the formula
   $$x_{i,j,\sigma} \wedge y_{i,j} \wedge z_{i,q} \Rightarrow \bigl(x_{i,j',\sigma'} = x_{i+1,j',\sigma'}\bigr)$$
   and why part of our proof of the Cook-Levin theorem (i.e., that SAT and 3SAT are NP-complete) involves formulas like this.
   (d) Show that the Boolean formula $u_4 = u_5$ is equivalent to the formula
   $$(\neg u_4 \vee u_5) \wedge (u_4 \vee \neg u_5)$$

Research supported in part by an NSERC grant.

[1] So $x_{ij\gamma}$ is true iff at step i and cell j the symbol γ appears there; y_{ij} is true iff at step i the tape head is over cell j; and z_{iq} is true iff at step i the configuration is in state q.

(e) Use the fact that $p \Rightarrow q$ is equivalent to $\neg p \vee q$ ($\vee$ is OR) to write
$$u_1 \wedge u_2 \wedge u_3 \Rightarrow (u_4 = u_5).$$
using just $\neg, \vee, \wedge$ and the $u_1, \ldots, u_5$.

(f) Write a 3CNF formula that is satisfiable iff the variables $u_1, \ldots, u_5$ satisfy
$$u_1 \wedge u_2 \wedge u_3 \Rightarrow (u_4 = u_5).$$

(g) How are parts (c) and (f) involved in our proof (in class) that 3SAT is NP-complete?

(2) In view of Problem (1), explain the meaning of the formula
$$x_{i,j,\sigma} \wedge y_{i,j} \wedge z_{i,q} \Rightarrow \Big(\big(x_{i+1,j,\sigma'} \wedge y_{i+1,j+1} \wedge z_{i+1,q'}\big) \vee \big(x_{i+1,j,\sigma''} \wedge y_{i+1,j-1} \wedge z_{i+1,q''}\big) \Big).$$
For which value of $\delta(q,\sigma)$ would you use a formula like this (where δ is the non-deterministic Turing machine transition function)?

(3) Show that if SAT can be decided in polynomial time, then there is a Turing machine that in polynomial time takes as input a Boolean formula $f(x_1, \ldots, x_n)$ and gives you true/false values for $x_1, \ldots, x_n$ for which $f(x_1, \ldots, x_n)$ is true, provided that f is satisfiable. [Hint: as a first step, notice that if $f(x_1, \ldots, x_n)$ is satisfiable, then either $f(true, x_2, \ldots, x_n)$ is satisfiable or $f(false, x_2, \ldots, x_n)$ is satisfiable.]

(4) Using your answer to Question 2, show that if SAT can be decided in polynomial time, then there is a Turing machine that in polynomial time takes as input a graph and returns a 3-colouring of the graph if the graph can be 3-coloured.

(5) Using your answer to Question 2, show that if SAT can be decided in polynomial time, then there is a Turing machine that in polynomial time takes as input a positive integer and returns a non-trivial factorization of the integer (i.e., as the product of two smaller positive integers) if one exists.

Department of Computer Science, University of British Columbia, Vancouver, BC V6T 1Z4, CANADA.
E-mail address: `jf@cs.ubc.ca`
URL: `http://www.cs.ubc.ca/~jf`