

Decision Procedures for Verification

HOMEWORK 2

Problem 1

Prove the following replacement theorems:

- (a) If $X^{\mathcal{A}} = Y^{\mathcal{A}}$ then $[F(X)]^{\mathcal{A}} = [F(Y)]^{\mathcal{A}}$.
- (b) If $X \leftrightarrow Y$ is valid then $F(X) \leftrightarrow F(Y)$ is valid.

Prove (a) by structural induction, and use (a) to show (b).

Problem 2

Prove by simultaneous structural induction on F that:

- (a) If $F^{\mathcal{A}} = true$ and $F(p^+)$ and $\mathcal{B} = \mathcal{A} \circ \{p \leftarrow true\}$ then $F^{\mathcal{B}} = true$.
- (b) If $F^{\mathcal{A}} = false$ and $F(p^-)$ and $\mathcal{B} = \mathcal{A} \circ \{p \leftarrow true\}$ then $F^{\mathcal{B}} = false$.

Problem 3

Let ALG be an algorithm such that:

- ALG takes in input a propositional formula F
- ALG returns a propositional formula G
- F is satisfiable if and only if G is satisfiable
- G is in DNF
- ALG runs in polynomial time in the size of F

Show that if ALG exists then $\mathcal{P} = \mathcal{NP}$.