Math 481 Midterm Examination

October 21, 2011

Instructions:

1. Do not start until you are told.
2. Extinguish all cell phones and other noisemakers.
3. Except as noted below, headphones, computers, wireless devices, notebooks, textbooks, and other objects that is or *appears to be* capable of communication, comptuation, or storage must be stowed out of reach during the exam. (A watch may be used and a silent cellphone displaying the time and nothing else may be used.)
4. You may use both sides of one 4-by-6 inch index card for notes.
5. You have 50 minutes for this exam.
6. On all questions, there is exactly one right answer. Do not circle more than one offered answer. There is no penalty for guessing, so you may as well attempt every problem.
7. There are 23 problems.
8. Good Luck!

Ten people took the exam. The number of people getting each question right are as follows:

Questions 1–5	10,9,10,9,10
Questions 6–10	10,10,8,6,10
Questions 11–15	7,7,10,10,9
Questions 16–20	10,8,8,8,7
Questions 21–23	2,1,9

For whatever reason, questions 21 and 22 failed and will be thrown out. (The questions look ok taken out of context, but it's possible I said something misleading in class.) Scores ranged from 17 to 21 out of a possible 21.

Definitions and Reference

1. Except where indicated, we are permissive about parentheses. For example, $\mathbf{A} \wedge \mathbf{B} \wedge \mathbf{C}$ is a legitimate wff of length 5. Recall that formulas group to the right: $\alpha \to \beta \to \gamma$ is $\alpha \to (\beta \to \gamma)$. The connective $\neg$ has highest precedence, followed by $\wedge$ and $\vee$ with equal precedence, then $\to$ and $\leftrightarrow$ with equal precedence.

2. Formula ϕ tautologically implies formula ψ, written $\phi \models \psi$, if all truth assignments that satisfy ϕ also satisfy ϕ.

3. Formulas ϕ and ψ are tautologically equivalent, $\phi \models\!\dashv \psi$ means that, for all truth assignments v, v makes ϕ true iff v makes ψ true.

4. Formula ϕ is a tautology, $\models \phi$, if all truth assignments satisfy ϕ.

5. A formula is in Conjunctive Normal Form if it is the conjunction of any number of disjunctions any number of sentence symbols or the negations of sentence symbols.

6. A formula is in 3-CNF form if it is the conjunction of any number of 3-way disjunctions of sentence symbols or the negations of sentence symbols.

7. A protocol is *complete* if it accepts "YES" instances with high probability (or always).

8. A protocol is *sound* if it accepts "NO" instances with low probability (or never).

9. There are $n! = n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$ permutations on n items.

In Problems 1 through 17, circle TRUE or FALSE.

1. $\models \neg(\mathbf{A} \wedge \mathbf{B}) \leftrightarrow (\neg\mathbf{A}) \vee (\neg\mathbf{B})$

   [TRUE] FALSE

2. $\mathbf{A} \rightarrow (\mathbf{B} \rightarrow \mathbf{C}) \models (\mathbf{A} \wedge \mathbf{B}) \rightarrow \mathbf{C}$

   [TRUE] FALSE

3. $\models ((\mathbf{A} \rightarrow \mathbf{B}) \rightarrow \mathbf{A}$

   TRUE [FALSE]

4. $\models (((\mathbf{A} \rightarrow \mathbf{B}) \rightarrow \mathbf{A}) \rightarrow \mathbf{A})$

   [TRUE] FALSE

5. For all formulas ϕ, we have $\neg\phi$ is a tautology if and only if ϕ is unsatisfiable.

   [TRUE] FALSE

6. For all formulas α and β, if $\alpha \models \beta$, then $\models \beta$.

   TRUE [FALSE]

7. For all formulas α and β, if $\models \beta$, then $\alpha \models \beta$.

   [TRUE] FALSE

8. Formulas over $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, sentence symbols, and parentheses can be parsed uniquely even if all the parentheses are missing.

   TRUE [FALSE]

9. Given any Boolean function f on n inputs, there is a formula over $\{\rightarrow, \neg\}$ that realizes f.

   [TRUE] FALSE

10. Given any Boolean function f on n inputs, there is a formula over $\{\wedge, \vee, \neg\}$ *of length at most* $cn2^n$ *for some constant* c that realizes f.

    [TRUE] FALSE

11. One can express the function $g(\mathbf{A}) = \neg\mathbf{A}$ using connectives $\{\wedge, \vee, \#\}$, where $\#$, as a function, takes three of inputs and the output denotes the majority value of the inputs.

TRUE [FALSE]

12. Given formula ϕ, there is a *tautologically* equivalent formula ψ in 3-CNF form.

TRUE [FALSE]

13. Given formula ϕ, there is a *tautologically* equivalent formula ψ in Conjunctive Normal Form (not necessarily 3-CNF).

[TRUE] FALSE

14. Given an *expression* w over $\wedge, \vee, \neg, \rightarrow, \leftrightarrow$, sentence symbols, and parentheses, we can decide whether w is a well-formed formula.

[TRUE] FALSE

15. There is a finite set Σ of formulas whose consequences, $\{\tau : \Sigma \vDash \tau\}$, is undecidable.

TRUE [FALSE]

16. Let Σ be an infinite set of formulas and let τ be a formula such that any truth assignment that satisfies τ makes some $\sigma \in \Sigma$ false. Then there is some finite subset $\{\sigma_1, \sigma_2, \ldots, \sigma_n\} \subseteq \Sigma$ such that

$$\neg(\sigma_1 \wedge \sigma_2 \ldots \wedge \sigma_n \wedge \tau)$$

is a tautology.

[TRUE] FALSE

17. Let $\Sigma = \{\mathbf{A}_1 \vee \neg\mathbf{A}_1, \mathbf{A}_2 \vee \neg\mathbf{A}_2, \ldots\}$. Then $\{\tau : \Sigma \vDash \tau\}$ is undecidable.

TRUE [FALSE]

Two graphs G and G' (which we assume to have the same number of vertices) are said to be *isomorphic*, $G \approx G'$, if there is some relabeling of the vertices of G, with edges following, that turns G into G'. For example, see Figure 1.

Problems 18 through 23, concern GRAPH NON-ISOMORPHISM: Given two graphs, G and G', are they *non*-isomorphic? We will consider protocols with which Peggy may want to prove to Victor that two graphs, seen by both parties, are *non*-isomorphic. (So a pair (G, G') of graphs is a YES instance if they are *non*-isomorphic, and (G, G') is a NO instance if they are isomorphic.)

Consider the protocol in Algorithm 1. In each of the following problems, we will make modifications to Algorithm 1. The modifications do *not* accumulate between problems. Circle the best answer.

18. If the number t of repetitions is set to $t = 2^n$ instead of $t = n$, which will suffer significantly?

    1. Soundness only
    2. Completeness only
    3. [Efficiency only]
    4. Zero Knowledge only
    5. None of the above.
    6. Two or more of the above.

19. Suppose Victor chooses G with probability 2/3 and G' with probability 1/3, but increases t from n to $2n$. Which will suffer significantly? (Note: an increase in computation time or communication by the factor 2 is *not* considered "significant" here. But check all ways in which efficiency may suffer.)

    1. Soundness only
    2. Completeness only
    3. Efficiency only
    4. Zero Knowledge only
    5. [None of the above.]
    6. Two or more of the above.

20. Suppose Victor always rejects (ignoring any input).

    1. Soundness only
    2. [Completeness only]
    3. Efficiency only
    4. Zero Knowledge only
    5. None of the above.

6. Two or more of the above.

21. Suppose Victor does not interact with Peggy but instead checks whether his random π is an isomorphism from G to G'. Then, following the rest of the protocol, he repeatedly tries $t = n$ random π's, rejects if any is an isomorphism, and accepts at the end if he has not already rejected. Which will suffer significantly?

    1. [Soundness only]
    2. Completeness only
    3. Efficiency only
    4. Zero Knowledge only
    5. None of the above.
    6. Two or more of the above.

22. Suppose Victor does not interact with Peggy but instead checks whether his random π is an isomorphism from G to G'. Then, following the rest of the protocol, he repeatedly tries $t = n \cdot n!$ random π's, rejects if any is an isomorphism, and accepts at the end if he has not already rejected. Which will suffer significantly? (Note this question is identical to the previous except for the number t of repetitions.)

    1. Soundness only
    2. Completeness only
    3. [Efficiency only]
    4. Zero Knowledge only
    5. None of the above.
    6. Two or more of the above.

23. Suppose Victor fails to sort the vertices of H, but instead sends the vertices of H in an order that (somehow) completely leaks to Peggy whether Victor chose G or G'. Which will suffer significantly?

    1. [Soundness only]
    2. Completeness only
    3. Efficiency only
    4. Zero Knowledge only
    5. None of the above.
    6. Two or more of the above.

Figure 1: Two graphs, isomorphic under the mapping $1 \to B, 2 \to C, 3 \to D, 4 \to A$.

Algorithm 1 Zero-Knowledge protocol for Graph Non-Isomorphism. Comments are introduced by //.

Input is pair (G, G') of graphs.
Protocol accepts if $G \not\approx G'$ and rejects otherwise (small probability of error.)

$t = n$
for $i = 1$ to t **do**
  Victor chooses one of G and G' at random; call it G''
  Victor chooses a random permutation π of $\{1, \ldots, n\}$
  Victor forms H by letting $u \sim_H v$ iff $\pi(u) \sim_{G''} \pi(v)$
    // That is, u and v are adjacent in the new graph H
    // iff $\pi(u)$ and $\pi(v)$ were adjacent in the old graph G''
  Victor sends Peggy a sorted list of pairs of vertices that are adjacent in H
  Peggy responds that $H \approx G$ or $H \approx G'$, appropriately
    // If $G \not\approx G'$, then $H \approx G''$ is isomorphic to exactly one of G and G'.
    // If $G \approx G'$, then $G \approx H \approx G'' \approx G'$;
    // Victor could have chosen G or G'.
  if Peggy is incorrect **then**
    return Victor rejects
  end if
end for
return Victor accepts