University of Toronto CSC240
Midterm Test Solutions

1. [6 marks] Femat's conjecture says that it is impossible to write the n'th power of any positive integer as the sum of the n'th powers of two positive integers, when n is an integer greater than 2.
Note that when $n = 2$, it is possible. For example $3^2 + 4^2 = 5^2$.

   Give a literal translation of Fermat's conjecture as a predicate logic formula.
Then give a logically equivalent formula in prenex normal form.
Use the syntax from class and the online lectures.
Use parentheses and brackets when necessary to avoid ambiguity.
The only set you can use is $\mathbb{Z}^+$ and the only predicate that you can use is $eq : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \{\text{T,F}\}$, where $eq(x, y) = \text{T}$ if and only if x is equal to y.
However, you may define and then use any binary function from $\mathbb{Z}^+ \times \mathbb{Z}^+$ to $\mathbb{Z}^+$.

   Solution: Let $sum : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ denote the function such that $sum(x, y)$ is the sum of x and y.
Let $power : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ denote the function such that $power(x, n)$ is x^n, the n'th power of x.

   The following literally says that for all positive integers n, if n is not equal 1 or 2, then there does not exist positive integers x, y and z such that $x^n = y^n + z^n$.

$$\forall n \in \mathbb{Z}^+.[((\text{NOT } eq(n, 1)) \text{ AND } (\text{NOT } eq(n, 2))) \text{ IMPLIES}$$
$$\text{NOT } \exists x \in \mathbb{Z}^+.\exists y \in \mathbb{Z}^+.\exists z \in \mathbb{Z}^+.eq(power(x, n), sum(power(y, n), power(z, n)))]$$

   Converting this into prenex normal form gives:

$$\forall n \in \mathbb{Z}^+.\forall x \in \mathbb{Z}^+.\forall y \in \mathbb{Z}^+.\forall y \in \mathbb{Z}^+.[eq(n, 1) \text{ OR } eq(n, 2) \text{ OR NOT } eq(power(x, n), sum(power(y, n), power(z, n)))]$$

2. [10 marks] Let $\mathcal{F}$ denote the set of all functions from $\mathbb{N}$ to $\mathbb{R}^*$.
Recall that, for any function $f \in \mathcal{F}$,

$$O(f) = \{g \in \mathcal{F} \mid \exists b \in \mathbb{N}.\exists c \in \mathbb{R}^+.\forall n \in \mathbb{N}.[(n \geq b) \text{ IMPLIES } (g(n) \leq cf(n))].$$

   Give a formal proof that $n^2 \notin O(3n)$.
Number every line of your proof. Use proper indentation. Explicitly state when a proof technique is being applied and say which earlier lines it refers to.
You may not assume anything about O, except its definition.

   Solution:

   1. To obtain a contradiction, suppose that $n^2 \in O(3n)$.
   2. $\exists b \in \mathbb{N}.\exists c \in \mathbb{R}^+.\forall n \in \mathbb{N}.[(n \geq b) \text{ IMPLIES } (n^2 \leq c3n))]$, definition 1
   3. Let $b \in \mathbb{N}$ and $c \in \mathbb{R}^+$ be such that $\forall n \in \mathbb{N}.[(n \geq b) \text{ IMPLIES } (n^2 \leq 3cn)]$, instantiation 2
   4. Let $n = \max\{\lceil 3c + 1 \rceil, b\}$.
   5. $n \geq 3c + 1$, property of max and ceiling 4
   6. $n > 3c$, arithmetic 5
   7. $n^2 > 3cn$, arithmetic 6
   8. $n \geq b$, property of max 4
   9. $n \in \mathbb{N}$, by construction 4
   10. $(n \geq b)$ IMPLIES $(n^2 \leq c3n)$, specialization 3
   11. $n^2 \leq c3n$, modus ponens 9, 10
   12. $n^2 \notin O(3n)$, proof by contradiction 1,7,11

   Here's an alternative solution:

1. Let $c \in \mathbb{R}^+$ be arbitrary.
2. Let $b \in \mathbb{N}$ be arbitrary.
3. Let $n = \max\{\lceil 3c + 1 \rceil, b\}$.
4. $n \in \mathbb{N}$, by construction: 3
5. $n \geq b$, property of max: 3
6. $n \geq 3c + 1$, property of max and ceiling: 3
7. $n > 3c$, arithmetic: 6
8. $n^2 > 3cn$, arithmetic: 7
9. $(n \geq b)$ AND $(n^2 \leq c3n)$, proof of conjunction: 5,8
10. $\exists n \in \mathbb{N}.[(n \geq b)$ AND $(n^2 \leq c3n)]$, construction 3,4,9
11. $\forall b \in \mathbb{N}.\exists n \in \mathbb{N}.[(n > b)$ AND $(n^2 > 3cn)]$, generalization: 2,10
12. $\forall c \in \mathbb{R}^+.\forall b \in \mathbb{N}.\exists n \in \mathbb{N}.[(n > b)$ AND $(n^2 > 3cn)]$, generalization: 1, 11
13. NOT $\exists c \in \mathbb{R}^+.\exists b \in \mathbb{N}.\forall n \in \mathbb{N}.$NOT $[(n > b)$ AND $(n^2 > 3cn)]$, property of NOT: 12
14. NOT $[P$ AND $Q]$ IFF $[P$ IMPLIES NOT $(Q)]$, tautology
15. NOT $[(n > b)$ AND $(n^2 > 3cn)]$ IFF $[(n \geq b)$ IMPLIES $NOT(n^2 > c3n))]$, substitution, 14
16. NOT $(n^2 > c3n)$ IFF $(n^2 \leq c3n)$, arithmetic, 15
17. NOT $[(n > b)$ AND $(n^2 > 3cn)]$ IFF $[(n \geq b)$ IMPLIES $(n^2 \leq c3n)]$, substitution, 16
18. NOT $\exists c \in \mathbb{R}^+.\exists b \in \mathbb{N}.\forall n \in \mathbb{N}.[(n \geq b)$ IMPLIES $(n^2 \leq c3n)]$, substitution, 17
19. $n^2 \notin O(3n)$, by definition: 18

3. [10 marks] A set of connectives is *complete* if every propositional formula is logically equivalent to a propositional formula that only uses connectives from this set. Recall that {AND, OR, NOT} is a complete set of connectives.

   Let NOR be the binary connective such that P NOR Q has the following truth table:

P	Q	P NOR Q
T	T	F
T	F	F
F	T	F
F	F	T

   Use structural induction to prove that {NOR} is a complete set of connectives.

   (a) What set will you use for your structural induction? Give a recursive definition of this set.
   Solution: Let F = the set of all propositional formulas using the connectives {AND, OR, NOT}t.
   Base case: all propositional variables are in F.
   Constructor cases: if $f, g \in F$, then $(f$ AND $g) \in F$, $(f$ OR $g) \in F$, and (NOT $f) \in F$.

   (b) Prove that {NOR} is a complete set of connectives using structural induction.
   Solution:
   For $f \in F$, let $L(f)$ = "f is logically equivalent to a propositional formula that only uses the connective NOR ".
   Claim $\forall f \in F.L(f)$.
   Proof: Let $f \in F$ be arbitrary and suppose the claim is true for all subformulas of f.
   Case 1: f is a propositional variable. Then f is a propositional formula that only uses the connective NOR. Hence $L(f)$ is true.
   Case 2: $f =$ NOT g. By the induction hypothesis, $L(g)$ is true, so there exists a propositional formula g' that is logically equivalent to g and only uses the connective NOR. P NOR P is logically equivalent to NOT P. This can be verified by a truth table. Then, by substitution, f is logically equivalent to g' NOR g', which only uses the connective NOR. Thus, $L(f)$ is true.
   Case 3: $f = g$ OR h. By the induction hypothesis, $L(g)$ and $L(h)$ are true, i.e. there exist propositional formulas g' and h' that are logically equivalent to g and h and only use the connective

NOR.

NOT $(P$ NOR $Q)$ is logically equivalent to P OR Q. This can be verified by a truth table. Then, by substitution, f is logically equivalent to $(g'$ NOR $h')$ NOR $(g'$ NOR $h') \in F'$. This only uses the connective NOR. Thus, $L(f)$ is true.

Case 4: $f = g$ AND h. By the induction hypothesis, $L(g)$ and $L(h)$ are true,i.e. there exist propositional formulas g' and h' that are logically equivalent to g and h and only use the connective NOR.

(NOT P) NOR (NOT Q) is logically equivalent to P AND Q. This can be verified by a truth table. Then, by substitution, f is logically equivalent to $(g'$ NOR $g')$ NOR $(h'$ NOR $h') \in F'$. This only uses the connective NOR. Thus, $L(f)$ is true.

In all cases, $L(f)$ is true. It follows by structural induction that $\forall f \in F.L(f)$.