Quiz 1

Your name: ______________________________

DO NOT WRITE BELOW THIS LINE

Problem	Points	Grade	Grader
1	20		
2	20		
3	30		
4	30		
Total	100		

Problem 1 (20 points). We have explained that, given any proof-checking program for a sound proof system for arithmetic inequalities over the integers, we can construct a valid inequality which has no proof in the system. But Ben Bitdiddle (remember him from 6.001? `:-)` asks, "If the inequality has no proof, how can we possibly know it is valid?"

Provide a brief explanation to clear up Ben's confusion.

Problem 2 (20 points). We consider proofs using the standard equational proof rules (Table 1 in the Appendix) for terms over a signature with two symbols, f and g, both of arity 2, a single constant, c. The sole axiom is $f(x, y) = g(x, y)$.

Let F_0 be the term $f(c, c)$, and define $F_{n+1} ::= f(F_n, F_n)$; likewise for G_n. (That is, G_n is the same as F_n with all f's replaced by g's.)

(a) (5 points) Explain how to construct a *sequence-of-equations proof* of length $O(n)$ for the equation $F_n = G_n$.

(b) (15 points) Let $l(n)$ be the length of the *shortest substitution proof* of $F_n = G_n$. Prove that $2^n = O(l(n))$.

Problem 3 (30 points). As in Assignment 4, we consider terms with constants R, F, D and a binary operation symbol, $\circ$, with the model, $\mathcal{A}$, being the automorphisms of the square. That is, the domain of $\mathcal{A}$ is the eight automorphisms of the square, and the constants R, F, D mean 90^0 clockwise rotation, reflection about a vertical axis, and reflection about an upper-left/lower-right diagonal, respectively, and the operation symbol, $\circ$, means function composition.

Define another model, $\mathcal{A}'$, whose elements will be pairs (A, s), where A is an automorphism of the square and s is a binary string. The $\circ$ symbol in $\mathcal{A}'$ means the operation on pairs that composes the first coordinates and concatenates the second coordinates. For example,

$$(\text{vertical reflection}, 010) \circ_{\mathcal{A}'} (\text{diagonal reflection}, 11) ::= (90^o \text{ rotation}, 01011).$$

The meanings of the constants R, F, D in $\mathcal{A}'$ will be the pairs $(90^o \text{ rotation}, \lambda)$, $(\text{vertical reflection}, \lambda)$, and $(\text{diagonal reflection}, \lambda)$, respectively, where λ is the empty string.

Let $\mathcal{E}$ be the equational axioms

$$x \circ (y \circ z) = (x \circ y) \circ z, \qquad \text{(associativity)}$$
$$F^2 \circ x = x \qquad \text{(left identity)}$$
$$x \circ F^2 = x \qquad \text{(right identity)}$$

and *all* equations between variable-free terms that are true in $\mathcal{A}$, for example,

$$\begin{aligned} R^4 &= F^2, \\ R^4 &= D^2, \\ FR &= D, \\ R^3F &= D, \\ &\vdots \end{aligned}$$

(a) (5 points) Explain why $\mathcal{A}' \not\models x^5 = x$.

(b) (15 points) Explain why $\mathcal{A}' \models \mathcal{E}$.

(c) (10 points) Conclude that $\mathcal{E} \not\vdash x^5 = x$.

Problem 4 (30 points). Consider ae's extended to include applications

$$((\lambda(x)e)f)$$

A *free occurrence* of a variable x, in an ae, a, is an occurrence of x that is not in a subexpression of the form $(\lambda(x)\ldots)$. For example, we highlight in boldface all the free occurrences of variables in the ae

$$\begin{array}{l}([\lambda(y) \\ \quad (\ (\lambda(x)(x+y)) \\ \qquad ((y \cdot \mathbf{w}) \cdot \mathbf{x})\ )] \\ \ ((\mathbf{y} - ((\lambda(z)z)\ \mathbf{x})) \cdot ((\lambda(x)(x - \mathbf{y}))\ 7)))\end{array}$$

(We used square brackets],[instead of parentheses to make it easier to see the scope of $\lambda(y)$.)

The *free variables*, $\mathrm{FV}(e)$, of an ae, e, are those variables which have one or more free occurrences in e. For example, letting e_0 be the ae above, we have $\mathrm{FV}(e_0) = \{x, y, w\}$.

(a) (10 points) Define $\mathrm{FV}(e)$ recursively on the structure of e.

(b) (20 points) Prove that if V_1, V_2 are valuations such that

$$V_1(x) = V_2(x) \qquad \text{for all } x \in \mathrm{FV}(e),$$

then

$$[\![e]\!]V_1 = [\![e]\!]V_2. \tag{1}$$