Outline of Fall 1993 Lectures

1. (Fri, 9/10) Administration, course overview. Informal discussion: what do we mean when we say two programs are "the same" or are "different"? Grammar of **IMP**.
2. (Mon, 9/13) Definition of kernel Scheme.
3. (Wed, 9/15) Extended Scheme vs. kernel Scheme: syntactic sugar.
4. (Fri, 9/17) The substitution model of kernel Scheme; rewrite rules.
5. (Mon, 9/20) The substitution model continued.
6. (Wed, 9/22) Definition of syntactic substitution. Declaratioun contexts and referential transparency.
7. (Fri, 9/24) Final lecture on the substitution model: evaluation contexts, deterministic evaluation.
8. (Mon, 9/27) Inductive definition of rules.
9. (Wed, 9/29) Proofs by induction.
10. (Fri, 10/1) What is a good inductive definition? What is a well-defined function?
11. (Mon, 10/4) Functional equations with no, many, unique, unique least solutions. Mention least fixed points.
12. (Wed, 10/6) Evaluation assertions for **IMP**. Functionality of arithmetic exp's by structural ind.
13. (Fri, 10/8) ADD DATE. Derivations in **IMP**. Example: Euclid's algorithm. Proofs by induction on derivations.

    (Mon, 10/11) COLUMBUS DAY.
14. (Wed, 10/13) What is the "meaning" of an **IMP** program?
15. (Fri, 10/15) QUIZ 1.
16. (Mon, 10/18) Compositionality of meaning, observational congruence, and full abstraction.
17. (Wed, 10/20) Proof of compositionality.
18. (Fri, 10/22) Introduction to Hoare logic. Partial correctness assertions. Rules of Hoare logic for **IMP**. Soundness.
19. (Mon, 10/25) Hoare logic rule for assignments. While-loop invariants.
20. (Wed, 10/27) Proof of correctness for Euclid's algorithm.
21. (Fri, 10/29) Language of assertions. Using assertions to encode primes and prime-powers.
22. (Mon, 11/1) Express "$i = k^n$" in **Assn** using base-p concatenation.
23. (Wed, 11/3) **IMP**-computable functions, predicates, and sets. Closure properties of **IMP**-decidable sets. "Computable" implies "expressible".
24. (Fri, 11/5) Expressibility of **IMP** input/output relations.
25. (Mon, 11/8) Checkable, decidable, and expressible sets.

    (Tue, 11/9, evening) QUIZ 2.

26. (Wed, 11/10) All **IMP**-computable functions are expressible. Dynamic assertions. Weakest preconditions. Expressing partial correctness assertions as dynamic assertions.

27. (Fri, 11/12) Relative completeness of Hoare logic for **IMP**. Closure properties of expressible sets.

28. (Mon, 11/15) More on closure properties of decidable and expressibile sets. Checkable sets. A set is decidable if and only if it is checkable and co-checkable.

29. (Wed, 11/17) Relative computability/expressibility. The halting problem. $\overline{H}$ is not checkable, and H is not decidable.

30. (Fri, 11/19) DROP DATE. $\bar{H}_0$ is not checkable. Many-one reducibility ($\leq_m$). Gödel encoding of commands.

31. (Mon, 11/22) H is checkable. $\overline{\text{True}}$ is not checkable. True is not checkable. Definition of provable; Peano arithmetic.

32. (Wed, 11/24) General definition of proof system as a decidable relation, $\vdash$, between a countable set, D, of derivations and an **Assn**. Theorem: for any proof system, $\vdash$, let $\mathbf{Provable} = \{\, A \mid d \vdash A \,\}$. Then **Provable** is checkable. Corollary (Incompleteness): for sound proof systems, **Provable** $\subsetneq$ **Valid**. Statement of Rice's Theorem.

    (Fri, 11/26) THANKSGIVING HOLIDAY.

33. (Mon, 11/29) Proof of Rice's Theorem. Examples of checkable, not decidable sets; $2H \cup 2H + 1$ is expressible but not checkable, not co-checkable. Statement of Theorem: **Validity** is not expressible.

34. (Wed, 12/1) Proof of Theorem: **Validity** is not expressible. Turing-reducibility ($\leq_T$). The Arithmetic Hierarchy and Hilbert's 10^{th} Problem.

35. (Fri, 12/3) More on Hilbert's 10^{th} Problem. The Diophantine sets = the checkable sets. Hilbert's 10^{th} is undecidable, in fact uncheckable. Corollary: $\{\, b \in \mathbf{Bexp} \mid \models b \,\}$ is uncheckable. Corollary: it is uncheckable whether two **while**-free commands are equivalent.

36. (Mon, 12/6) Theorem: $\{\, (a_1, a_2) \in \mathbf{Aexp} \times \mathbf{Aexp} \mid \models a_1 = a_2 \,\}$ is decidable and completely axiomatizable (by transformation to canonical form).

37. (Wed, 12/8) Further courses: 6.821 Programming Languages; 6.830 Program Semantics and Verification; 6.826 Principles of Systems; 18.505 Mathematical Logic. Further Topics: Undecidable problems in grammars, geometry, algebra, program schemes; logic programming; semantics of concurrency; denotational semantics of first-class functions; types in programming and constructive logic; formal logic, predicate calculus and completeness.

    (Wed, 12/15, 1:30–4:30 PM, room 24–115) FINAL EXAM.