CSCE 235H – Advanced Topics

Advanced Set Theory

1. "Naïve" Set Theory
   - Uses *natural language* to define sets, not at all formal
   - We've already seen problems when attempting to reconcile natural language with logic (implication law, definition of "if" versus xor)
   - Created by Georg Cantor (late 19th Century)
   - Dominant foundation of "sets" prior to the early 20th century
   - Assumed that any operation could be used to define a set: any definable collection is a set
   - Still used as a "first step" in introducing basic concepts (ordinals, numbers, relations, functions)
   -
2. Russell's Paradox (Bertrand Russell)
   - Bertrand Russell (1901)
   - Caused by the axiom of "Unrestricted Comprehension" (ie unrestricted definition)
   - Even if it is an unrestricted predicate
   - Forall w_1, …, w_n exists B forall x (x in B iff phi(x, w_1, …, w_n))
   - Problem: let phi be the predicate (x not in x), that is:
   - R = { x | x not in x} then R in R iff R not in R (contradiction)
   - Argument: let R be in R, then by the definition of R, R cannot be contained in itself; let R not in R then R is in R!
   - Similar Paradoxes
     - Liar Paradox (this sentence is false)
     - Kleen-Rosser Paradox
     - Curry's paradox
3. Zermelo-Fraenkel Set Theory
   - Ernst Zermelo, Abraham Fraenkel (1908 - 1922)
   - 9 Axioms
   - Competing systems
     - Peano Axioms (weaker, regarding the natural numbers: 0 exists; every natural number has a successor; except 0; distinctness; etc.)
     - Neumann-Bernays-Godel (NBG), "equivalent" to ZFC
     - Morse-Kelley (MK)
     - New Foundations (Willard Von Orman Quine, 1937)
   - Leads to Independence of some statements: some statements can be proven true (or false) in ZFC, while proven false (true) in another (ZF)

4. Cantor's Diagonalization
   - N, Z, Q are all countable: infinite, but enumerable
   - R, C are uncountable: no enumeration possible
   - Formally: A countable iff exists a bijective function between N and A
   - Informally: graphical enumeration (or functional)
   - R is not countable: Cantor's diagonalization proof (1874)
     - Intuition: "more reals" than integers
     - But there are just as many integers as rationals!
   - Not all infinities are equal: aleph null, aleph 1, etc.
   - Controversial at the time: theological implications and philosophy of mathematics (Poincare), rejection of non-constructive proofs (Kronecker)
5. Independence: Continuum Hypothesis
   - Does there exists a set S of intermediate cardinality between aleph0, aleph1? (asked Cantor) prior to axiomatic set theory, so unresolved
   - Hilbert's 1st problem (1900)
   - Godel showed that it cannot be disproven in ZFC (1940)
   - Paul Cohen showed that it cannot be proven in ZFC either (1963)
   - Both assume that ZFC is consistent (not known, but believed)
   - Other results shown to be independent of ZFC:
     - Consistency of ZFC within itself (Godel)
     - Whitehead problem (extensions of Abelian Groups)
6. Godel's Incompleteness Theorem (1931)
   - Metamathematics: math talking about math (axioms can be formalized as objects themselves)
   - An axiomatic system is *consistent* if it lacks contradiction (some statement can be proved and disproved)
   - An axiom is called *independent* if it cannot be derived from other axioms; a system is independent if all of its axioms are.
   - A system is *complete* if for every statement, either it or its negation can be derived
   - First Incompleteness theorem: no consistent system of axioms whose results can be enumerated by an algorithm is capable of proving all truths about the relations of natural numbers; there will always be true statements about N that are not provable by a Turing machine
     - Since we start with a finite number of axioms, all statements can be built via an enumeration algorithm
   - Second Incompleteness Theorem: Such a system cannot prove its own consistency (if you can prove its consistency, then it is inconsistent)
   - A system is either consistent or complete, but not both (enumerable systems that is)
   - A statement is independent if it can neither be proven nor disproven in a system
   - Intuition: No formula phi(x) can be shown from the axioms of ZF to have the property that the collection of all x satisfying phi(x) form a model for ZF