15-251: Great Theoretical Ideas In Computer Science

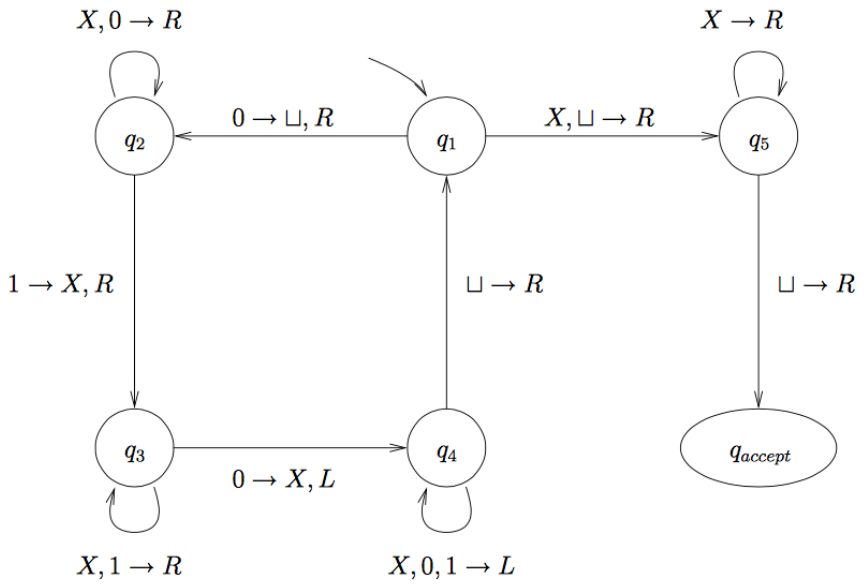
Recitation 12

November 17, 2014

1. Turing Machine

(a) Prove that $\{0^n1^n0^n \mid n \in \mathbb{N}\}$ is decidable.

Solution:



Medium level description:

1. Cross out the first 0 (with $\sqcup$), go to right and cross the first 1 (with X), go to right and cross the first 0 (with X).
2. Go to the left and stop at the first $\sqcup$, then repeat.

(b) Prove that $\{M \mid L(M) = 0^n1^n0^n\}$ is undecidable.

Solution:
AFSOC there exists a TM M that decides this language.
Consider a turing machine M'

1. On input w
2. Let P be any program/turing machine
3. Run P. If P halts, accept if $w \in \{0^n1^n0^n\}$, reject otherwise.

Therefore, $M(M')$ has to halt because M is a decider. However, its return value will imply whether P halts. This solves the halting problem, which is a contradiction.

2. More Turing Machine

Recall that a language L is decidable iff. there exists a TM such that

- Accept all $w \in L$
- Reject all $w \notin L$

Define a language L Turing-Acceptable iff. there exists a TM such that

- Accept all $w \in L$
- Rejct or loop forever on all $w \in L$

(a) Prove or disprove: The complement of a decidable language is decidable.

Solution: True. Consider a TM M for the language, we can construct M' from M with the accept/reject states swapped. M' decides the complement of the language.

(b) Prove or disprove: The complement of a Turing-Acceptable language is Turing-Acceptable.

Solution: False.
Consider the language that has a singleton alphabet $\Sigma = \{a\}$, possible words are $a^0, a^1, a^2, \cdots$.
Since turing machines have finite number of states, for a finite number of states, there is a finite configurations for transition functions, accepting states, etc. Therefore the set of all turing machines is countable. Let them be $M_1, M_2, M_3, \cdots$
Consider the two languages (diagonalization)

- $L = \{a^i \mid a^i \in L(M_i)\}$

- $\bar{L} = \{a^i \mid a^i \notin L(M_i)\}$

They are each other's complement, because every possible word is in exactly one of them. L is Turing-Acceptable, because we can first find out i, then simulate as if the a^i is running on M_i. $\bar{L}$ is not Turing-Acceptable, because it's different by at least one from all $L(M_i)$'s, which is all Turing-Acceptable TM.
Therefore $L, \bar{L}$ is a counterexample to the claim.

Definitions and Theorems from the Gödel Lecture

Soundness: A logic is sound if every theorem is true. Intuitively, it means, *if I can prove something, then it must be true.*

Completeness: A logic is complete if for every sentence S, either S or $\neg S$ is a theorem. Intuitively, it means, *I can prove everything that is true.*

Consistency: A logic is consistent if for every sentence S, at least one of S or $\neg S$ is not a theorem. Intuitively, it means, *I cant prove contradictions!*

Gödels Completeness Theorem: There exists an axiomatic system with computable axioms whose theorems are precisely the set of valid sentences in first-order logic.

Gödel's First Incompleteness Theorem: Any mathematical proof system which can define Turing Machines and has computable axioms cannot be both complete and sound.

Gödels Second Incompleteness Theorem: Any mathematical proof system which can define Turing Machines and has computable axioms cannot be both complete and consistent.

Corollary: If ZFC is consistent, then ZFC is incomplete and it cannot prove the statement "ZFC is consistent."

3. Löbs Theorem

Löbs theorem states that if ZFC (or any sufficiently expressive system) can prove its own soundness, then it is inconsistent. This is rather surprising, since it basically means that we cannot prove that our proofs are correct!

To prove Löbs theorem, we will define the following:

- Let S be an arbitrary statement (i.e. $2 + 2 = 4$, P = N P , etc.)
- Let A be the statement "There is a proof of S within ZFC."
- Let T be the statement "$A \rightarrow S$", i.e. ZFC is sound.

To prove Löbs Theorem, consider the axiomatic system Z^*, which is ZFC with the axiom $\neg S$.

For the rest of the proof, **assume that there is a ZFC proof of T.**

(a) Show that in Z^*, it is possible to prove $\neg A$.

Solution: Z^* contains ZFC, so by our assumption, Z^* can prove T, i.e., $A \to S$. Z^* can also of course prove $\neg S$, since thats an axiom in Z^*. Hence it can also prove $\neg A$ (by contrapositive).

(b) Show that in Z^*, it is possible to prove that ZFC is consistent.

Solution:
We just showed that in Z^* its possible to prove "there is no proof of S within ZFC." In particular, this implies that not both S and $\neg S$ have proofs in ZFC, i.e. ZFC is consistent.

(c) Show that in Z^*, it is possible to prove that Z^* is consistent.

Solution:
Z^* is just ZFC and $\neg S$. We just showed that Z^* proves ZFC is consistent. The only way adding $\neg S$ can make it inconsistent is if ZFC can prove S; i.e. if A is true. But by part (a), Z^* proves $\neg A$.

(d) Deduce that there is a ZFC proof of S.

Solution:
By Gödels 2nd Incompleteness Theorem, Z^* must be inconsistent, since part (c) says it proves its own consistency. Thus, Z^* can prove T and $\neg T$. What does the proof of T look like in Z^*? It is just a sequence of valid deductions, which use ZFC axioms as well as the axiom $\neg S$. Now, take this proof, and whenever you have a line L which depends on the axiom $\neg S$, replace it with the line $\neg S \to L$. Do this for all the lines. At the end, what youve got is a ZFC proof of the statement $\neg S \to T$. Similarly, you can convert the Z^* proof of $\neg T$ into a ZFC proof of $\neg S \to T$. So now ZFC proves

$$(\neg S \to T) \wedge (\neg S \to \neg T) \ .$$

Hence, ZFC proves $\neg S \to (T \wedge \neg T)$, i.e. it proves S (this is a proof by contradiction).

(e) Prove Löbs theorem.

Solution: We have just shown that if there is a ZFC proof of T, then there is a ZFC proof of S. In other words, if we have a ZFC proof that ZFC is sound, then ZFC can prove any statement S, which would mean that ZFC is inconsistent (by definition).