10.1 Aside about Countability and Uncountability

Georg Cantor considered the idea of how to measure the size (cardinality) of infinite sets. The following definition says that two sets – finite or infinite – have the same cardinality iff we can exactly count them off against each other.

Definition 10.1 [Cantor] Two sets, \( S, T \) have the same cardinality \( (S \sim T) \) iff there exists a 1:1 correspondence, \( f : S \rightarrow T \).

Cantor also defined a set, \( S \), to be countable iff \( S \) is finite, or \( S \sim \mathbb{N} \). Note that if \( f : \mathbb{N} \rightarrow S \) then we can count \( S \) as follows,

\[
S = \{ f(0), f(1), f(2), \ldots \}.
\]

Cantor proved the following:

Fact 10.2 (Cantor) The following sets are countable: \( \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \Sigma^* \), where \( \Sigma \) is any finite alphabet.

Notation 10.3 (Power Set) For any set, \( S \), the power set of \( S \) \( (\mathcal{P}(S)) \) is the set of all subsets of \( S \):

\[
\mathcal{P}(S) \overset{\text{def}}{=} \{ R \mid R \subseteq S \}.
\]

Fact 10.4 (Cantor) For all sets, \( S \), \( S \not\sim \mathcal{P}(S) \), i.e., the power set of \( S \) has strictly greater cardinality than \( S \). In particular, \( \mathbb{R} \not\sim \mathcal{P}(\mathbb{N}) \) is uncountable.

The standard proof of Thm 10.4 uses diagonalization. Turing used the same method to prove that \( \text{HALT} \), the complement of the halting problem, is not r.e., and thus \( \text{HALT} \) is not solvable.

10.2 Post’s Correspondence Problem (PCP)

Definition 10.5 [Post’s Correspondence Problem (PCP)] An instance of PCP, \( p = ((x_1, y_1), \ldots, (x_r, y_r)) \) is a finite sequence of pairs of binary strings. The instance \( p \) has a solution \( (p \in \text{PCP}) \) iff there exists a finite sequence of indices: \( i_1, \ldots, i_n \) from \( \{1, \ldots, r\} \) such that \( x_{i_1} x_{i_2} \cdots x_{i_n} = y_{i_1} y_{i_2} \cdots y_{i_n} \). The PCP Question is whether we can construct a pair of equal strings by repeatedly appending pairs from \( p \).

Example 10.6 \( p_0 = ((1, 101), (10, 00), (011, 11)) \) is a positive instance of the Post Correspondence Problem, i.e., \( p_0 \in \text{PCP} \). A solution is 1323. Note that,

\[
x_1 x_2 x_3 x_3 = 1 011 10 011 = 101 11 00 11 = y_1 y_3 y_2 y_3.
\]

PCP is a very simplified version of the Halting Problem in which Turing machine computations are encoded as binary strings. PCP has the same complexity at the halting problem, HALT:

Fact: [Post] PCP is r.e. complete. In particular, PCP is r.e. but not recursive.

10.3 Undecidability of FO Logic

Recall that FO-VALID is the set of all first-order formulas that are true in all appropriate structures. In his Ph.D. thesis in 1930, Gödel proved,
Theorem 10.7 [Gödel’s Completeness Thm] There is a complete recursive axiom system for FO Logic. That is, in this system, for all \( \varphi \in L(\Sigma) \), \( \varphi \) is a theorem iff \( \varphi \) is valid. In symbols,

\[
\vdash \varphi \iff \varphi \in \text{FO-VALID}.
\]

Corollary 10.8 (FO-VALID is r.e.) \( \text{FO-VALID} \in \text{r.e.} \)

In Gödel’s original proof, he showed that the axiomitization of FO Logic in Russel and Whitehead’s *Principia Mathematica* is complete. In Lecture 12, we will prove Thm 10.7 by showing that Resolution is complete for FO logic.

A year later, in 1931, Gödel proved that there is no recursive and complete axiom system for all of mathematics, or even for number theory. If there had been, then it would have meant that MATH and thus also FO-VALID and HALT would all be recursive.

Theorem 10.9 [Gödel’s Completeness Thm] There is no complete recursive axiom system for all of math, nor even for just \( \text{Theory}(\mathbb{N}) = \{ \varphi \in L(\Sigma_{\mathbb{N}}) \mid \mathbb{N} \models \varphi \} \).

10.4 Unsolvability of FO Logic

We now prove that FO-VALID is not solvable:

Theorem 10.10 (FO Logic is not Recursive) \( \text{FO-VALID} \) is r.e. complete.

Proof: We follow the proof in the text which shows that PCP \( \leq \) FO-VALID. In particular, we will show that there is a very easy-to-compute transformation, \( \tau \), which translates any PCP problem, \( p \), to an FO formula, \( \tau(p) \), such that

\[
P \in \text{PCP} \iff \tau(p) \in \text{FO-VALID}
\]  

(10.10)

Let \( \Sigma_{\text{PCP}} = (P^2; a, f^1_0, f^1_1) \). Let \( p = ((x_1, y_1), \ldots, (x_r, y_r)) \) be an arbitrary instance of PCP.

Notation 10.11 (Schöning)

\[
f_{j,s-1} \cdots j_1 (x) \leftrightarrow f_{j_1}(f_{j_2}(\cdots(f_{j_{s-1}}(f_{j_s}(x)))\cdots))
\]

For example, \( f_{110}(x) = f_0(f_1(f_1(x))) \).

We now construct \( \tau(p) = \alpha_p \land \beta_p \rightarrow \gamma_p \) so that Eqn 10.10 holds.

\[
\alpha_p \overset{\text{def}}{=} \bigwedge_{i=1}^r P(f_{x_i}(a), f_{y_i}(a))
\]

\[
\beta_p \overset{\text{def}}{=} \varphi_2 = \forall uv \ (P(u, v) \rightarrow \bigwedge_{i=1}^r P(f_{x_i}(u), f_{y_i}(v)))
\]

\[
\gamma_p \overset{\text{def}}{=} \exists z \ P(z, z)
\]

The intuitive idea behind these formulas is that they mean, “If we start with some pair from \( p \), \( (\alpha_p) \), and we continue to add any pairs from \( p \) any number of times, \( (\beta_p) \), then we can eventually reach a situation where the two strings are equal, \( (\gamma_p) \).”
More explicitly, $a$ is the starting point, e.g., the empty string, and we are not given that $P(a, a)$ holds.

The formula $\alpha_p$ says that we may start with any of the pairs $(x_1, y_1)$, through $(x_r, y_r)$. For the example of $p_0$ (Ex. 10.6),

$$\alpha_{p_0} \overset{\text{def}}{=} P(f_1(a), f_{101}(a)) \land P(f_{10}(a), f_{00}(a)) \land P(f_{011}(a), f_{11}(a))$$

The formula $\beta_p$ says that for any position $(u, v)$, that we have reached, we may start with any of the pairs $(x_1, y_1)$, through $(x_r, y_r)$. Continuing the example $p_0$,

$$\beta_{p_0} \overset{\text{def}}{=} \forall uv (P(u, v) \rightarrow (P(f_1(u), f_{101}(v)) \land P(f_{10}(u), f_{00}(v)) \land P(f_{011}(u), f_{11}(v))))$$

We now prove Eqn 10.10

**Assume** $p \in \text{PCP}$. Let $\mathcal{A} \in \text{STRUC}[\Sigma_{\text{PCP}}]$ be arbitrary. We will show that $\mathcal{A} \models \alpha_p \land \beta_p \rightarrow \gamma_p$.

If $\mathcal{A} \not\models \alpha_p \land \beta_p$, then $\mathcal{A} \models \tau(p)$, so we may assume that $\mathcal{A} \models \alpha_p \land \beta_p$.

Consider the example of $p_0$ (Ex. 10.6) whose solution is 1323. Since $\mathcal{A} \models \alpha_{p_0}$, we have that $\mathcal{A} \models P(f_1(a), f_{101}(a))$. Since $\mathcal{A} \models \beta_{p_0}$, we can conclude that $\mathcal{A} \models P(f_{1011}(a), f_{10111}(b))$. Applying $\beta_{p_0}$ again, we have that $\mathcal{A} \models P(f_{101110}(a), f_{1011100}(b))$. Applying $\beta_{p_0}$ a third time we get, $\mathcal{A} \models P(f_{101110011}(a), f_{101110011}(b))$.

Now, we have won because $\mathcal{A} \models \gamma_{p_0}$. The witness is $z = f_{101110011}(a)$. Thus, since $p \in \text{PCP}$, $\mathcal{A} \models \tau(p)$. Since $\mathcal{A}$ was arbitrary, it follows that $\tau(p) \in \text{FO-VALID}$.

Conversely, assume $\tau(p) \in \text{FO-VALID}$. We construct the standard model we have in mind, $S \in \text{STRUC}[\Sigma_{\text{PCP}}]$:

$$|S| = \{0, 1\}^*$$

$$P^S = \{(u, v) \in (\{0, 1\}^*)^2 \mid \exists i_1, \ldots, i_n (u = f_{x_{i_1} \cdots x_{i_n}}(a) \land v = f_{y_{i_1} \cdots y_{i_n}}(a))\}$$

$$a = \epsilon$$

$$f_0^S = \{(w, w0) \mid w \in \{0, 1\}^*\}$$

$$f_1^S = \{(w, w1) \mid w \in \{0, 1\}^*\}$$

Note that by construction, $S \models \alpha_p \land \beta_p$. Thus, $S \models \gamma_p$. But, again by the construction of $S$, this means that the $z$ asserted to exists in $\gamma_p$ is a winning position for the PCP problem of $p$, i.e., $p \in \text{PCP}$. 

\[\square\]