Gödel Incompleteness Theorems: Solutions to sheet 1

Apologies for the lateness of this; I've been ill and everything is behind.

I do not people to do formal deductions in a system of first-order logic; I assume people know about the Completeness Theorem and are not afraid to use it.

A.

1. (Optional: have a go at this if you've not seen PA before.) Show that all of the following can be proved from PA.

(i) Every natural number is either even or odd (i.e. for all n, either there exists m such that $n = 2.m$, or there exists m such that $n = (2.m)^+$).

$0 = 2.0$, *so the statement is true for* 0.

Suppose that n *is either even or odd.*

If n *is even, then for some* m, $n = 2.m$, *so* $n^+ = (2.m)^+$, *so* n^+ *is odd.*

If n *is odd, then for some* m, $n = (2.m)^+$, *so* $n^+ = (2.m)^{++} = (2.m + 0)^{++} = ((2.m + 0^+)^+ = 2.m + 0^{++} = 2.m + 2 = 2.m^+$, *so* n^+ *is even.*

Hence n^+ *is even or odd.*

Now by induction, every natural number is either even or odd.

(Further exercise: prove that no natural number is both.)

(ii) Addition is associative.

We prove by induction on k *that, for all* m *and* n, $(m + (n + k)) = ((m + n) + k)$.

For $k = 0$, *it is straightforward:* $(m + (n + 0)) = m + n = (m + n) + 0$.

Now suppose the result true for k. *Then* $m+(n+k^+) = m+(n+k)^+ = (m+(n+k))^+$ *which is equal, by the inductive hypothesis, to* $((m + n) + k)^+ = (m + n) + k^+$.

(iii) Addition is commutative. (Hard.)

We first prove by induction on n *that* $0 + n = n$. *This is certainly true for* $n = 0$. *Now suppose that* $0 + n = n$. *Then* $0 + n^+ = (0 + n)^+ = n^+$ *as required.*

Now we prove by induction on n *that for all* m, $m + n^+ = m^+ + n$. *For* $n = 0$, *we prove this by induction on* m*: for* $m = 0$, *we have* $0 + 0^+ = 0^+ + 0$ *by the previous result. If* $m + 0^+ = m^+ + 0$, *then* $m^+ + 0^+ = (m^+ + 0)^+ = (0 + m^+)^+$ *by the previous result, which is equal to* $0 + m^{++}$, *which is equal to* $m^{++} + 0$ *by the previous result.*

Now we prove that if, for all m, $m + n = n + m$, *then for all* m, $m + n^+ = n^+ + m$. *For,* $m + n^+ = (m + n)^+ = (n + m)^+$ *by the inductive hypothesis, and this is equal to* $n + m^+$, *which is equal to* $n^+ + m$ *by the previous result.*

(iv) Multiplication is associative.

We prove by induction on k *that for all* m *and* n, $(m.n).k = m.(n.k)$.

For $k = 0$, $(m.n).0 = 0 = m.0 = m.(n.0)$.

If $(m.n).k = m.(n.k)$, *then* $(m.n).k^+ = (m.n).k+(m.n) = m.(n.k)+m.n = m.(n.k+n)$ *by distributivity on the left, which I should have put first, which is equal to* $m.(n.k^+)$.

(v) Multiplication is commutative. (Harder.)

We prove first that for all m, $0.m = 0$. *For,* $0.0 = 0$*; and if* $0.m = 0$, *then* $0.m^+ = 0.m + 0 = 0 + 0 = 0$.

Now for each m, *we prove by induction on* n *that* $m^+.n = m.n + n$.

For $n = 0$, $m^+.0 = 0 = 0 + 0 = m.0 + 0$.

Now suppose $m^+.n = m.n + n$. Then $m^+.n^+ = m^+.n + m^+ = (m.n + n) + m^+ = m.n + (n + m^+)$ since addition is associative, and this is equal to $m.n + (n^+ + m)$ by a lemma proved in part (iii), and this is equal to $m.n + (m + n^+)$ since addition is commutative, and this is equal by associativity of addition to $(m.n + m) + n^+$, which is in turn equal to $m.n^+ + n^+$ as required.

Now we prove by induction on n that for all m, $m.n = n.m$.

If $n = 0$, then $m.0 = 0 = 0.m$ as proved above.

For the inductive step, assume that $m.n = n.m$ for all m. Then $m.n^+ = (m.n) + m = n.m + m = n^+.m$ by the previous result.

Hence addition is commutative.

(vi) Multiplication is distributive over addition.

We prove by induction on k that for all m and n, $m.(n + k) = m.n + m.k$.

For $k = 0$, we have $m.(n + 0) = m.n = m.n + 0 = m.n + m.0$.

For the inductive step, $m.(n+k^+) = m.(n+k)^+ = m.(n+k)+m = (m.n+m.k)+m = m.n + (m.k + m)$ by associativity of additon, which is equal to $m.n + m.k^+$ as required.

2. Describe informally a method by which it can be decided whether an expression of $\mathscr{L}_E$ is a term, a formula, or neither.

3. (i) Write down a true sentence in $\mathscr{L}_E$ containing exactly eight symbols, and write down its Gödel number according to the system given in lectures (write it in base 13 if you prefer).

For example, $\overline{0} \leq \overline{0}^{++++++}$; Gödel number $(1B100000)_{13}$.

(ii) Write down a true sentence in the language $\mathscr{L}_E$ containing $\neg$, $\rightarrow$ and $\forall$ that is not logically valid (ie. that is not true in every logical structure whatever), and give an informal argument to show that it is true.

For example, $\forall v \neg\forall v' \, (v \leq v' \rightarrow v = v')$, with the meaning "Every point has some other point strictly to the right", which cannot be true in any finite partially ordered set.

B.

4. (i) Show that the relation "x divides y" can be expressed in $\mathscr{L}_E$.

$\exists k \leq y \, (y = x.k)$ *which (even better) is Σ_0.*

(ii) Show that the property of being a power of 7 can be expressed in $\mathscr{L}_E$. Can it be expressed without using exponentiation?

7 divides n, and for all $k \leq n$, either $k = 1$, or 7 divides k. (This is Σ_0.)

(iii) Show that if A is a set and g is a (unary) function, and both A and g are definable in $\mathscr{L}_E$, then $g^{-1}(A)$ is also definable in $\mathscr{L}_E$.

If $\phi(x)$ expresses "$x \in A$" and $\psi(x, y)$ expresses "$g(x) = y$", then $\exists y \, (\psi(x, y) \wedge \phi(y))$ expresses "$x \in g^{-1}(A)$".

5. (i) Show that for any formula $F(v_i, v_j)$,

$$\text{PA} \vdash (\exists v_j \, \exists v_i \, F(v_i, v_j) \leftrightarrow \exists v_k \, (\exists v_j \leq v_k)(\exists v_i \leq v_k) F(v_i, v_j)).$$

We only need the axioms for a total order. We show that the result is true in any totally ordered set, and then note that total orders are first-order definable in our language.

In any total order, if $\exists v_j \, \exists v_i \, F(v_i, v_j)$ is true, then suppose this is witnessed by elements a_j and a_i of the structure, and let a_k be whichever is greater. Then a_k, a_j and a_i witness the truth of $\exists v_k \, \exists v_j \leq v_k \, \exists v_i \leq v_k F(v_i, v_j)$.

The other way round is similar but easier.

(ii) Show that for any formula $F(v_i, v_j)$,

$$\mathrm{PA} \vdash ((\forall v_j \leq v_k) \exists v_i \, F(v_i, v_j) \leftrightarrow \exists v_r (\forall v_j \leq v_k)(\exists v_i \leq v_r) F(v_i, v_j)).$$

Suppose that $\mathfrak{N}$ is a model of PA, and that for some $a_k \in \mathfrak{N}$, $\mathfrak{N} \models (\forall v_j \leq a_k) \, \exists v_i \, F(v_i, v_j)$.

We may prove by induction on n the (first order) statement: there exists m such that for all $k < n$, if $k \leq a_k$ also, then there exists $v_i \leq m$ such that $F(v_i, k)$ holds.

The base case is vacuous, and for the inductive step, if $n > a_k$ then nothing need be done, while if $n \leq a_k$, then the value of m appropriate for $n+1$ is the maximum of the value of m appropriate for n and a witness of the statement $\exists v_i \, F(v_i, n)$.

Thus $\mathfrak{N} \models \exists v_r (\forall v_j \leq v_k)(\exists v_i \leq v_r) F(v_i, v_j)$; for the appropriate value of v_r is m_{n+1}.

The reverse implication is easier.

6. (i) Show that the function

$$p(m, n) = \tfrac{1}{2}(m + n + 1)(m + n) + m$$

is a pairing function on the natural numbers, that is, it is a bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$; and show that it is Σ_0 (that is, the statement "$k = [m, n]$" is provably Σ_0).

The fact that $p(m, n)$ is one-to-one and onto follows from the fact that $\sum_{i \leq k} i = \frac{1}{2}(k+1)k$; $\frac{1}{2}(k+1)k \leq p(m, n) < \frac{1}{2}(k+1)k$ if and only if $m + n = k$, and then $m = p(m, n) - \frac{1}{2}(k+1)k$.

It is clearly Σ_0.

(ii) Show that there are two one-place Σ_0-functions p_l and p_r such that $p_l(p(m, n)) = m$ and $p_r(p(m, n)) = n$.

$m = p_l(p)$ if and only if $\exists n \leq p \, 2.p = (m + n + 1)(m + n) + m$, and $n = p_r(p)$ if and only if $\exists m \leq p \, 2.p = (m + n + 1)(m + n) + m$; both statements are Σ_0.

C.

7. Show that

(i) for $n > 0$, formulae provably Σ_n with respect to PA are closed under existential quantification, and formulae provably Π_n with respect to PA are closed under universal quantification,

By question 5.(i), $\exists v_i \, \exists v_j \, \phi$ is equivalent to $\exists v_k \, \exists v_i \leq v_k \, \exists v_j \leq v_k \, \phi$. We now need to argue that if ϕ is Π_{n-1}, where $n > 0$ (for $n = 0$ it's obvious) then $\exists v_i \leq v_k \, \exists v_j \leq v_k \, \phi$ is provably Π_{n-1}. But this follows from (an easy adaptation of) question 5.(ii).

(ii) formulae provably equivalent Σ_n with respect to PA are closed under conjunction and disjunction, and formulae provably Π_n with respect to PA are closed under conjunction and disjunction, *We first note that if v_j is not free in $\phi(v_i)$, then $\forall v_i, \phi(v_i)$ is provably equivalent to $\forall v_j\, \phi(v_j)$. So, given two different statements beginning with a quantifier, we can assume the quantified variables are different or the same as it suits us.*

Now $\exists v_i\, \phi \vee \exists v_i\, \psi$ is equivalent to $\exists v_i\, (\phi \vee \psi)$.

$\exists v_i\, \phi \wedge \exists v_j\, \psi$ is equivalent to $\exists v_i\, \exists v_j\, (\phi \wedge \psi)$ if $i \neq j$.

$\forall v_i\, \phi \wedge \forall v_i\, \psi$ is equivalent to $\forall v_i\, (\phi \wedge \psi)$.

$\forall v_i\, \phi \wedge \forall v_j\, \psi$ is equivalent to $\forall v_i\, \forall v_j\, (\phi \vee \psi)$ if $i \neq j$.

We apply the previous part, or 5.(i), to replace two $\exists$ or two $\forall$ by one.

(iii) formulae that are provably Δ_n with respect to PA are closed under conjunction and disjunction.

Now obvious.