Gödel's Incompleteness Theorem

Part II: Arithmetical Definability

Computability and Logic

The Language of Arithmetic

- The language of arithmetic L_A contains the following four non-logical symbols:
  - **0**: constant symbol
  - **s**: 1-place function symbol
  - **+**: 2-place function symbol
  - **×**: 2-place function symbol
- An arithmetical formula is a FOL formula that uses L_A as its only non-logical symbols.

Standard Interpretation N

- N is the following (standard) interpretation of the language of Arithmetic:
  - Domain: natural numbers (0,1,2,3, etc)
  - N(**0**) = 0
  - N(**s**) = s, the successor function
  - N(**+**) = +, the addition function
  - N(**×**) = ×, the multiplication function
  - More technically, where $\mathbf{t_0}$, $\mathbf{t_1}$, and $\mathbf{t_2}$ are variable-free terms:
    - $N(\mathbf{s(t_0)}) = s(N(\mathbf{t_0}))$
    - $N(\mathbf{t_1 + t_2}) = N(\mathbf{t_1}) + N(\mathbf{t_2})$
    - $N(\mathbf{t_1 \times t_2}) = N(\mathbf{t_1}) \times N(\mathbf{t_2})$

Arithmetical Definability

- Let **n** = **s(s(…(0)…))** (n times)
- Remember that we write N ⊨ φ to say that under standard interpretation N, φ is a true statement.
- An arithmetical formula **φ(x)** *arithmetically defines* a set S iff for all natural numbers n: n ∈ S iff N ⊨ **φ(n)**.
- A set S of natural numbers is *arithmetically definable* if and only if there exists an arithmetical formula **φ(x)** that arithmetically defines S.

Arithmetical Definability of Relations and Functions

- An m-place relation R of natural numbers is *arithmetically definable* if and only if there exists an arithmetical formula $\boldsymbol{\varphi(x_1, \ldots, x_m)}$ such that for all natural numbers $n_1, \ldots, n_m$: $\langle n_1, \ldots, n_m \rangle \in R$ iff $N \vDash \boldsymbol{\varphi(n_1, \ldots, n_m)}$.
- An m-place function f as defined over natural numbers is *arithmetically definable* if and only if there exists an arithmetical formula $\boldsymbol{\varphi(x_1, \ldots, x_m, y)}$ such that for all natural numbers $n_1, \ldots, n_m$, n: $f(n_1, \ldots, n_m) = n$ iff $N \vDash \boldsymbol{\varphi(n_1, \ldots, n_m, n)}$.

Some Examples

- The x < y relationship is arithmetically defined by the formula **$\exists z\ x + s(z) = y$**
- The x ≤ y relationship is arithmetically defined by the formula **$\exists z\ x + z = y$**
- The modified predecessor function pred(x), where pred(0) = 0 and pred(x') = x, is defined by formula **$\varphi_{pred}(x, y)$** defined as **$(x = 0 \wedge y = 0) \vee x = s(y)$**
- The modified difference function diff(x,y), where diff(x,y) = 0 for x ≤ y, and diff(x,y) = x – y otherwise, is defined by formula **$\varphi_{diff}(x, y, z)$** defined as **$(x \leq y \wedge z = 0) \vee x = y + z$**

Quotient and Remainder

- The modified quotient function quo(x,y), where quo(x,y) = 0 for y = 0 and quo(x,y) = largest z such that $y \times z < x$, is defined by formula $\boldsymbol{\varphi_{quo}(x, y, z)}$ defined as $\boldsymbol{(y = 0 \wedge z = 0) \vee \exists w\, (w < y \wedge (y \times z) + w = x)}$
- The modified remainder function rem(x,y), where rem(x,y) = x for y = 0 and rem(x,y) = z such that $z < y$ and there is some w such that $y \times w + z = x$, is defined by formula $\boldsymbol{\varphi_{rem}(x, y, z)}$ defined as $\boldsymbol{(y = 0 \wedge z = x) \vee (z < y \wedge \exists w\, (y \times w) + z = x)}$ (we can also define φ_{rem} in terms of φ_{quo}: $\boldsymbol{\varphi_{rem}(x, y, z)} = \boldsymbol{\exists w\, (\varphi_{quo}(x, y, w) \wedge (y \times w) + z = x)}$)

Theorem: Every Recursive Function is Arithmetically Definable

- Proof: by induction over the formation of recursive functions.
- Base: Primitive functions:
  - z
  - s
  - Id
- Step: Operations:
  - Composition
  - Primitive Recursion
  - Minimization

All Primitive Functions are A.D.

- z:
  - for $\varphi(x, y)$ we can pick: $\mathbf{y = 0}$
- s:
  - $\varphi(x, y)$: $\mathbf{y = s(x)}$
- id^n_i:
  - $\varphi(x_1, \ldots, x_n, y)$: $\mathbf{y = x_i}$

Composition

- Inductive step: Assuming that k-place function f and m-place functions $g_1, \ldots, g_k$ are A.D., show that $h = Cn[f, g_1, \ldots, g_k]$ is A.D.
- Proof: Given that f, $g_1, \ldots, g_k$ are all A.D., we know that we have formulas $\boldsymbol{\varphi_f(x_1, \ldots, x_k, y)}$ and $\boldsymbol{\varphi_{g1}(x_1, \ldots, x_m, y)}$ … $\boldsymbol{\varphi_{gk}(x_1, \ldots, x_m, y)}$ that arithmetically define f, $g_1, \ldots, g_k$.
- Well, then the formula $\boldsymbol{\varphi_h(x_1, \ldots, x_m, y)} = \boldsymbol{\exists y_1 \ldots \exists y_k\, \varphi_{g1}(x_1, \ldots, x_m, y_1) \wedge \ldots \wedge \varphi_{gk}(x_1, \ldots, x_m, y_k) \wedge \varphi_f(y_1, \ldots, y_k, y)}$ will arithmetically define h.

Primitive Recursion

- Inductive step: If functions f and g are A.D. (for simplicity we stick to 1-place function f, but proof trivially generalizes), show that h = Pr[f,g] is A.D.
- Remember: h(x,0) = f(x); h(x, s(y)) = g(x, y, h(x,y)).
- So, we know that h(a,b) = c iff there exists a sequence of numbers a_0, …, a_b such that:
  - a_0 = h(a,0) = f(a)
  - $a_{s(i)}$ = h(a, s(i)) = g(a,i,a_i) for all i < b
  - a_b = h(a,b) = c
- So, we want to encode a sequence of integers of some finite, but arbitrary length. Consider this to be n_1 … n_k (this will make it clear what we mean by "i-th entry", and also simplify the proof in small ways). How do we encode such a sequence?

Encoding Sequences

- We know that we can encode any sequence of numbers of arbitrary length using a single number using the prime factors encoding.
- This, however, requires an exponential function, and we don't have a function symbol for that in our language (of course, we could just add one, but that would weaken the ultimate result).
- So, instead, we'll show that we can encode any sequence of natural numbers using two numbers s and t, such that the function ent(i,s,t) = i-th entry of sequence encoded by s and t, is A.D.

Chinese Remainder Theorem

- Take any numbers t_1, …, t_k, no two of which have a common prime factor (i.e. any two of which are co-prime, or relatively prime, or have a greatest common divisor of 1).
- Now take any numbers a_1, …, a_k such that $a_i < t_i$ for all i.
- The Chinese Remainder Theorem now says that there is a number s such that for all i: $rem(s,t_i) = a_i$.

Example (and Inspiration for Theorem and its Proof)

- Let k = 2.
- Consider $t_1 = 2$ and $t_2 = 3$ (which are co-prime)
- Consider $a_1 = 1$ and $a_2 = 2$ (so $a_i < t_i$)
- Again, the claim is that there exists a number s such that rem(s,2) = 1 and rem(s,3) = 2.
- Let's look for such a number.

s	rem(s,2)	rem(s,3)
0	0	0
1	1	1
2	0	2
3	1	0
4	0	1
5	1	2

Not only do we find such a number (s = 5), but we notice that all pairs (rem(s,2),rem(s,3)) are different between 0 and 2×3.

Indeed, we can prove that this holds in general, and from that the Chinese Remainder Theorem immediately follows!

Proof of Chinese Remainder Theorem

- Again, we have numbers $t_1, \ldots, t_k$ (that are all relatively prime) and $a_1, \ldots, a_k$ such that $a_i < t_i$ for all i.
- The key observation is that when you consider all numbers $s < t_1 \times \ldots \times t_k$, and all associated tuples $(rem(s,t_1), \ldots rem(s,t_k))$, then all tuples are different.
- So, since there are exactly $t_1 \times \ldots \times t_k$ possible tuples of numbers $<b_1, \ldots, b_k>$ such that $b_i < t_i$ for all i, that means that one of these tuples is the $<a_0, \ldots, a_n>$ tuple we are looking for, meaning that indeed there is a number s such that for all i: $rem(s,t_i) = a_i$.

Proof of Key Claim

- Proof by Contradiction!
- Suppose that two different numbers $u < v < t_1 \times \ldots \times t_k$ give same tuples, i.e. $rem(u,t_i) = rem(v,t_i)$ for all i.
- Then consider $q = v - u$.
- That means that $rem(q,t_i) = 0$ for all i. So q is multiple of $t_1 \times \ldots \times t_k$.
- But: $q > 0$ and $q < t_1 \times \ldots \times t_k$.
- Contradiction!

OK, so what?

- OK, so I encode (a sequence of) numbers $a_1, \ldots, a_k$ with a single number s, … but I haven't told you what this number is.
- Even worse, I need numbers $t_1, \ldots, t_k$ in order to recover (decode) $a_1, \ldots, a_k$! So, I am encoding and decoding k numbers using k+1 numbers … How is this at all an improvement?!?
- Well, we'll see that numbers $t_1, \ldots, t_k$ can be coded using a single number t, together with index i.
- Hence, we are down to 2 numbers: s and t.
- OK, but what is t?

Finishing Up

- Let $t = n!$, where $n = \max\{k, a_1, \ldots, a_k\}$.
- Let $t_i = t \times i + 1$
- Then: for any $0 < i < j \leq k$: t_i and t_j are co-prime
  - Proof: Suppose t_i and t_j are not. Then there is some prime number p that divides both $t \times i + 1$ and $t \times j + 1$. This means that p also divides the difference, i.e. p divides $t \times (j - i) = n! \times (j - i)$. If p divides n!, then $p \leq n$. If p divides j - i, then $p < k \leq n$. So, either way, $p \leq n$, meaning that p divides n!, and therefore p divides $n! \times i$. but that means that p divides $t_i - 1$ as well as t_i. Contradiction!
- Also, for all i: $a_i < t_i$
- So, we can apply the Chinese Remainder Theorem, i.e. there is an s such that for all i: $a_i = rem(s,t_i)$
- This also means that $\boldsymbol{\varphi_{ent}(i, s, t, y)} = \boldsymbol{\varphi_{rem}(s, (t \times i) + s(0), y)}$ arithmetically defines function ent(i,s,t).

The Formula

- OK, but we still don't have a formula that arithmetically defines h=Pr[f,g]. Again, for simplicity sake assume f is a 1-place function f(x) and assume $\varphi_f(x, y)$ defines f(x). Also, assume $\varphi_g(x, y, z, w)$ defines function g(x, y, z).
- Then the following formula defines h(x,y): $\boldsymbol{\varphi_h(x, y, z)}$ =

  ∃s ∃t (/*we have two numbers s and t that encode a sequence such that */

  $\boldsymbol{\exists u\ (\varphi_{ent}(s(0), s, t, u) \wedge \varphi_f(x, u))}$ /* first entry is f(x) */

  $\boldsymbol{\wedge\ \forall w\ ((0 < w \wedge w \leq y) \rightarrow}$

  $\boldsymbol{\exists u\ \exists v\ (\varphi_{ent}(w, s, t, u) \wedge \varphi_{ent}(s(w), s, t, v) \wedge \varphi_g(x, w, u, v))}$ /* subsequent entries are obtained by applying g */

  $\boldsymbol{\wedge\ \varphi_{ent}(s(y), s, t, z)}$ /* last entry (i.e. (y+1)-th entry) is answer */ **)**

Minimization

- Inductive Step: Assuming f is a n+1-place function $f(x_1, \ldots, x_n, y)$ that is arithmetically defined by $\varphi_f(x_1, \ldots, x_n, y, z)$, show that $h = Mn[f](x_1, \ldots, x_k)$ is arithmetically definable.
- Remember, $h(x_1, \ldots, x_k) = y$ if y is the smallest number for which $f(x_1, \ldots, x_n, y) = 0$, and where for all $w < y$: $f(x_1, \ldots, x_n, w)$ is defined. Otherwise, $h(x_1, \ldots, x_k)$ is undefined.
- This function is defined by the following formula: $\boldsymbol{\varphi_h(x_1, \ldots, x_k, y) = \varphi_f(x_1, \ldots, x_n, y, 0) \wedge \forall w\, (w < y \rightarrow \exists z\, (\varphi_f(x_1, \ldots, x_n, y, z) \wedge \neg\, z = 0))}$