Announcements

HW2 out by tonight

HW1, Test 1 will be returned next week

Review of Definitions

$\mathcal{L}_A = \{0, s, +, \cdot\, ; =\}$ Language of arithmetic

Φ_0 = all $\mathcal{L}_A$-sentences

$TA = \{A \in \Phi_0 \mid \mathbb{N} \models A\}$ True Arithmetic

A <u>theory</u> Σ is a set of sentences (over $\mathcal{L}_A$) closed under logical consequence

- We can specify a theory by a subset of sentences that logically implies all sentences in Σ

Σ is <u>consistent</u> iff $\Phi_0 \neq \Sigma$ (iff $\forall A \in \Phi_0$, either A or $\neg A$ Not in Σ)

Σ is <u>complete</u> iff Σ is consistent and $\forall A$ either A or $\neg A$ is in Σ

Σ is <u>sound</u> iff $\Sigma \subseteq TA$

Let $\mathfrak{M}$ be a model/structure over $\mathcal{L}_A$

$Th(\mathfrak{M}) = \{ A \in \Phi_0 \mid \mathfrak{M} \models A \}$

$Th(\mathfrak{M})$ is <u>complete</u> (for all structures $\mathfrak{M}$)

<u>Note</u> $TA = Th(\mathbb{N})$ is complete, consistent, & sound

$VALID = \{ A \in \Phi_0 \mid \models A \}$ ← smallest theory

Let Σ be a theory

Σ is <u>axiomatizable</u> if there exists a set $\Gamma \subseteq \Sigma$

such that ① Γ is recursive

② $\Sigma = \{ A \in \Phi_0 \mid \Gamma \models A \}$

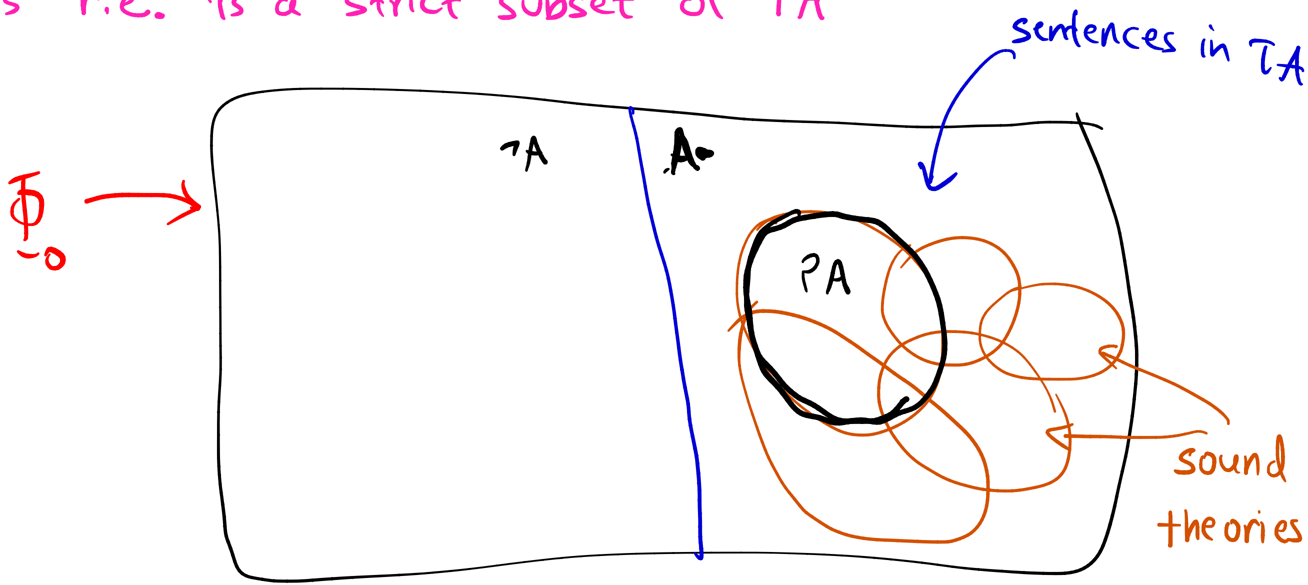
<u>Theorem</u> Σ is axiomatizable iff Σ is r.e.

(P. 76 of Notes)

Incompleteness Theorem

$\boxed{\text{Incompleteness Theorem of TA:}}$ TA is Not axiomatizable

In other words, any sound theory Σ (sound : $\Sigma \subseteq TA$) that is r.e. is a strict subset of TA



Representing a Relation by a Formula (in TA)

<u>Definition</u> Let $s_0 = 0$, $s_1 = S0$, $s_2 = SS0$, etc.

For $a \in \mathbb{N}$, Let $\tilde{a}$ be the term s_a corresponding to a.

Let $R(x)$ be a relation $R \subseteq \mathbb{N}^n$

Let $A(x)$ be an $\mathcal{L}_A$ formula, with free variable x

$A(x)$ **represents** R iff $\forall a \in \mathbb{N}$ $R(a)$ is true $\Leftrightarrow A(\tilde{a}) \in TA$

<u>Example</u> $R \subseteq \mathbb{N}$ $R = \{ a \in \mathbb{N} \mid a \text{ is even} \}$

$\exists y \leq x \, (y+y=x)$

$A(x) \stackrel{d}{=} \exists y \, (y+y=x)$

$R(3) = \text{false}$ and $\mathbb{N} \not\models A(SSS0) = \exists y \, (y+y=SSS0)$

$R(4) = \text{true}$, and $\mathbb{N} \models A(SSSS0) = \exists y \, (y+y=SSSS0)$

Representing a Relation by a Formula (in TA)

Definition Let $s_0 = 0$, $s_1 = S0$, $s_2 = SS0$, etc.
For $a \in \mathbb{N}$, Let $\tilde{a}$ be the term s_a corresponding to a.
Let $R(x)$ be a relation $R \subseteq \mathbb{N}^n$
Let $A(x)$ be an $\mathcal{L}_A$ formula, with free variable x

$A(x)$ **represents** R iff $\forall a \in \mathbb{N}$ $R(a)$ is true $\iff A(\tilde{a}) \in TA$

Defn A relation R is **arithmetical** iff there is a formula $A \in \mathcal{L}_A$ that represents R

(FIRST) INCOMPLETENESS THEOREM

EXISTS-DELTA THEOREM (pp 68-71):

Every r.e. predicate/language is arithmetical and therefore the complement of any r.e. language is arithmetical.

Example,

K is r.e. so by ↑ $K(x)$ is represented by some some formula $A(x)$.

$\therefore K^c$ is represented by $\neg A$

(FIRST) INCOMPLETENESS THEOREM

EXISTS-DELTA THEOREM (pp 68-71):

Every r.e. predicate/language is arithmetical, and therefore the complement of an r.e. language is arithmetical

Proof of Incompleteness from Exists-Delta Theorem

- If TA is axiomatizable, then TA is r.e.
- We will show that this implies that K^c is r.e. (to get a contradiction)
  - Assume TA is r.e. and let M be a TM s.t. $\mathcal{L}(M) = TA$
  - Since K^c is complement of an r.e. language, by Exists-Delta Thm there is a formula $F(x)$ such that $\forall a \in \mathbb{N}$:

    $F(\tilde{a}) \in TA$ iff $a \in K^c$, where $\tilde{a}$ is the term corresponding to a.
  - $\boxed{\text{TM for } K^c:}$ on input x, Run M on $F(\tilde{x})$ and accept iff $M(F(\tilde{x}))$ accepts

contradiction

$\exists\Delta_0$ Formulas

$t_1 \le t_2$ stands for $\exists w(t_1 + w = t_2)$

$$\left.\begin{array}{lll} \exists z \le t\ A & \text{stands for} & \exists z(z \le t \wedge A) \\ \forall z \le t\ A & \text{stands for} & \forall z(z \le t \supset A) \end{array}\right\} \text{Bounded Quantifiers}$$

Definition A formula is a Δ_0-formula if it has the form

$$\underbrace{\forall z_1 \le t_1\ \exists z_2 \le t_2\ \forall z_3 \le t_3 \ldots \exists z_k \le t_k}_{\text{Bounded Quantifiers}}\ \underbrace{A(\vec{x}, \vec{z})}_{\text{No quantifiers}}$$

Definition A relation $R(\vec{x})$ is a Δ_0-relation iff some Δ_0-formula represents it

$\exists\Delta_0$ Formulas

$t_1 \le t_2$ stands for $\exists w(t_1 + w = t_2)$

$\exists z \le t\ A$ stands for $\exists z\,(z \le t \wedge A)$
$\forall z \le t\ A$ stands for $\forall z\,(z \le t \supset A)$

} Bounded Quantifiers

Definition A formula is a Δ_0-formula if it has the form $\forall z_1 \le t_1\ \exists z_2 \le t_2\ \forall z_3 \le t_3 \ldots \exists z_k \le t_k\ A(\vec{x}, \vec{z})$

Definition A $\exists\Delta_0$ formula has the form $\exists \vec{y}\, \underbrace{B(\vec{x}, \vec{y}, \vec{z})}_{\Delta_0 \text{ formula}}$

Definition A relation $R(\vec{x})$ is a Δ_0-relation iff some Δ_0-formula represents it

Definition $R(\vec{x})$ is a $\exists\Delta_0$-relation iff some $\exists\Delta_0$-formula represents it

$\exists\Delta_0$ Formulas

Example $\mathrm{Prime} = \{ x \in \mathbb{N} \mid x \text{ is prime} \}$ is a Δ_0-relation, represented by the following Δ_0-formula:

$$A(x) \overset{d}{=} S0 < x \wedge \forall z_1 \leq x \, \forall z_2 \leq x \, (x = z_1 \cdot z_2 \supset (z_1 = 1 \vee z_1 = x))$$

$$\forall z_1 \leq x \, \forall z_2 \leq x \left((S0 < x) \wedge (x = z_1 \cdot z_2 \supset (z_1 = 1 \vee z_1 = x)) \right)$$

$\exists\Delta_0$ Formulas

Lemma Every Δ_0 relation is recursive

Lemma Every $\exists\Delta_0$ relation is r.e.

$\exists\Delta_0$ (Exists-Delta) Theorem every r.e. relation is represented by a $\exists\Delta_0$ formula

---

Example:

$K = \{ x \mid \{x\} \text{ halts on } x \}$ is r.e.

$A_K : \exists y \left[\begin{array}{l} y \text{ describes tableaux of } \{x\} \text{ on input } x \text{ and final line of tableaux} \\ \text{halts} \end{array} \right]$

$\exists\Delta_0$ Theorem

Main Lemma Let $f : \mathbb{N}^n \to \mathbb{N}$ be a total computable function.

Let $R_f = \{ (\vec{x}, y) \in \mathbb{N}^{n+1} \mid f(\vec{x}) = y \}$ ← also called graph(f)

Then R_f is a $\exists\Delta_0$-relation.

$\exists\Delta_0$

any r.e. relation is arithmetical

Main Lemma Let $f: \mathbb{N}^n \to \mathbb{N}$ be total, computable

Then $\text{graph}(f) = R_f = \{(\vec{x}, y) \mid f(\vec{x}) = y\}$ is a $\exists\Delta_0$ relation

Proof of $\exists\Delta_0$ Theorem from Main Lemma

Let $R(\vec{x})$ be an r.e. relation [example $K(x)$]

Then $R(\vec{x}) = \exists y\, S(\vec{x}, y)$ where S is recursive $\quad K(x) = \exists y\, S(x, y)$

Since S is recursive, $f_S(\vec{x}, y) = \begin{cases} 1 & \text{if } (\vec{x}, y) \in S \\ 0 & \text{otherwise} \end{cases}$

is total computable

By main lemma R_{f_S} is represented by a $\exists\Delta_0$ relation

So $R(\vec{x}) = \exists y\, \underbrace{\exists z\, B}_{R_{f_S}}$ is represented by a $\exists\Delta_0$ relation

Let $K = \{x \mid \{x\} \text{ halts on input } x\}$

We will represent K by the formula:

$$A_K = \exists y \underbrace{A(x,y)}_{\exists \bar{z}\, \underbrace{F(x,y,\bar{z})}_{\Delta_0}}$$

where A is a recursive relation that accepts iff y is the tableaux of TM $\{x\}$, when run on input x and last configuration of y is halting

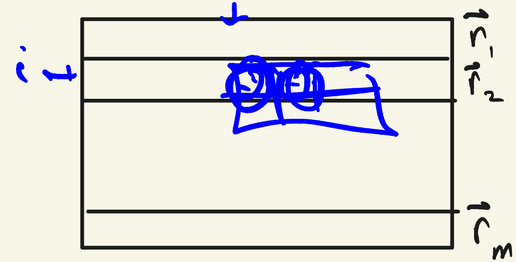
A is recursive so by main Lemma, A is represented by an $\exists \Delta_0$ formula

$\therefore$ K is represented by a $\exists \Delta_0$ formula

Proof of Main Lemma: MAIN IDEA

Let $f : \mathbb{N} \to \mathbb{N}$ be unary, total computable function, & let M_f be TM computing f

$R(x, y)$ will be a $\exists\Delta_0$ relation saying: $\exists m, c, d$ such that:



(1) c, d encode an m-by-m tableaux (described by $\vec{r}_1, \ldots, \vec{r}_m$):

(2) $\vec{r}_1$ encodes start config of M_f on x

(3) $\vec{r}_m$ encodes last config, that halts and outputs y

(4) For all other configs, state is not q_2.

(5) all 2×3 local cells are consistent with transition function of M_f

Proof of Main Lemma: MAIN IDEA

Let $f: \mathbb{N} \to \mathbb{N}$ be unary, total computable function, + let M_f be TM computing f

$R(\vec{x}, y)$ will be a $\exists\Delta_0$ relation saying:

$A(x,y)$ formula

$\exists m, c, d$ such that

(1) c, d describe the tableaux given by $r_1 \ldots r_m \ldots r_{m^2}$

(2) $r_1 .. r_m$ encode start config of M_f on x

(3) last m numbers $r_{(m-1)m} .. r_{m^2}$ encode last config, containing y in first cells then B, and state is q_z

(4) For all other configs, state is not q_z.

(5) all 2×3 local cells are consistent with transition function of M_f

- Need to encode an arbitrarily long sequences (of Numbers/strings) by a few (3) numbers (m, c, d)
- Need formulas that can talk about the i^{th} number in the sequence

Proof of Main Lemma: MAIN IDEA

- Need to encode an arbitrarily long sequences (of Numbers/strings) by a few (3) numbers (m, c, d)
- Need formulas that can talk about the i^{th} number in the sequence
- WARMUP: if exponentiation fxn x^y were in $\mathcal{L}_A$, this would be easier.

encode 57, 3009, 205, 4, 5 by

$$2^{57} \cdot 3^{3009} \cdot 5^{205} \cdot 7^{4} \cdot 11^{5}$$

(ie i^{th} number x sequence encoded by p_i^{x}, where $p_i = i^{th}$ smallest prime number)

Proof of Main Lemma: MAIN IDEA

- Need to encode an arbitrarily long sequences (of Numbers/strings) by a few (3) numbers (m, c, d)
- Need formulas that can talk about the i^{th} number in the sequence
- WARMUP: if exponentiation fxn x^y were in $\mathcal{L}_A$, this would be easier.

- But we need to encode sequences using <u>only</u> $+, \cdot, s$

  ⋆ gödel's β function does this using magic of chinese remainder theorem

Proof of Main Lemma (see pp 70-71)

Main idea: is a way of representing sequences of numbers by numbers using $\exists\Delta_0$ formulas

Note: Prime power decomposition not useful here since we only have $s, +, \cdot$
(ie. represent (a_1, a_2, a_3, a_4) by $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4}$)

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1)$$

where $rm(x, y) = x \bmod y$

$$x = q \cdot y + r$$

Proof of Main Lemma ($R_f = \text{graph}(f)$ is an $\exists\Delta_0$ relation)

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1) \quad \text{where } rm(x, y) = x \bmod y$$

Lemma 0. $\forall n, r_0, r_1, \ldots, r_n \;\; \exists c, d$ such that $\forall i \le n \;\; \beta(c, d, i) = r_i$

the pair (c, d) represents the sequence $\underbrace{r_0\, r_1, \ldots r_n}_{\text{entire tableaux of TM configuration}}$ using β

Corollary of Chinese Remainder Theorem

Proof of Main Lemma (R_f = graph(f) is an r.e. relation)

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1) \quad \text{where } rm(x, y) = x \bmod y$$

Lemma 0. $\forall n, r_0, r_1, \ldots, r_n \ \exists c, d$ such that $\forall i \le n \ \beta(c, d, i) = r_i$

the pair (c, d) represents the sequence $\underbrace{r_0 r_1, \ldots r_n}_{\text{entire tableaux of TM configuration}}$ using β

Lemma 1 graph(β) is a Δ_0 relation

Lemma 0

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1) \quad \text{where } rm(x, y) = x \bmod y$$

Lemma 0: $\forall n, r_0, r_1, \ldots, r_n \ \exists c, d$ such that

$$\beta(c, d, i) = r_i \quad \forall i, \ 0 \leq i \leq n$$

CRT (Chinese Remainder Theorem)

Let $r_0, \ldots, r_n$, $m_0, \ldots, m_n$ be such that
$0 \leq r_i \leq m_i \quad \forall i, \ 0 \leq i \leq n$ and $\gcd(m_i, m_j) = 1 \ \forall i, j$

Then $\exists r$ such that $rm(r, m_i) = r_i \quad \forall i, \ 0 \leq i \leq n$

CRT (Chinese Remainder Theorem)

Let $r_0, \ldots, r_n$, $m_0, \ldots, m_n$ be such that:

(1) $0 \le r_i \le m_i \quad 0 \le i \le n$

(2) $\gcd(m_i, m_j) = 1 \quad \forall i,j, \; i \neq j$

Then $\exists r$ such that $rm(r, m_i) = r_i \quad \forall i, \; 0 \le i \le n$

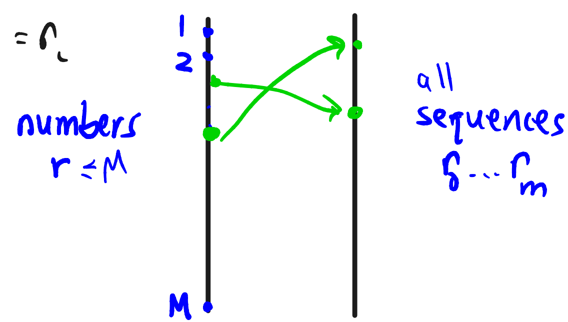
Proof (counting Argument: we will show $\exists r \le M$, where $M = m_0 \cdot m_1 \cdots m_n$)

- The number of sequences $r_0 \ldots r_n$ such that (1) holds is $M = m_0 \cdot m_1 \cdot \ldots \cdot m_n$
- Each r, $0 \le r \le M$ corresponds to a different sequence:

  I.e. If $\forall i \; rm(r, m_i) = r_i$ and $\forall i \; rm(s, m_i) = r_i$

  Then $r = s$ (mapping is 1-1)

$\therefore$ for every sequene $r_0 \ldots r_m$, some $r \le M$ maps to it



Lemma 0

Lemma 0 $\forall n, r_0, r_1, \ldots, r_n$ $\exists c, d$ such that
$\beta(c,d,i) = r_i \quad \forall i, \; 0 \le i \le n$

$$\beta(c,d,i) = rm(c, d(i+1)+1)$$
$$= c \bmod d(i+1)+1$$

Chinese Remainder Theorem

Let $r_0, \ldots, r_n$, $m_0, \ldots, m_n$ be such that $0 \le r_i \le m_i$ and $\gcd(m_i, m_j) = 1$. Then $\exists r$ $rm(r, m_i) = r_i \;\; \forall i$

Proof of Lemma 0

Let $d = (n + r_0 + \ldots + r_n + 1)!$

Let $m_i = d(i+1)+1$

Claim $\forall i,j$ $\gcd(m_i\, m_j) = 1$ (proof next page)

By CRT $\exists r = c$ so that $\beta(c,d,i) = rm(c, m_i) = r_i \;\; \forall i \in [n]$

$$\beta(c,d,i) \stackrel{d}{=} c \bmod \underbrace{d(i+1)+1}_{m_i}$$

<u>Claim</u> Let $d = (n + r_0 + r_1 + \dots + r_n + 1)!$, $m_i = d(i+1) + 1$

then $\forall i \neq j \leq n$ $\gcd(m_i, m_j) = 1$

<u>Pf</u> Suppose p is a prime, and $p \mid \underbrace{d(i+1)+1}_{m_i}$, $p \mid \underbrace{d(j+1)+1}_{m_j}$

Then $p \mid \underbrace{[d(j+1)+1]}_{m_j} - \underbrace{[d(i+1)+1]}_{m_i}$ (assume $j > i$)

so $p \mid d(j-i)$

But p cannot divide both d and $d(i+1)+1$ so $p \mid j-i$

But then $p \leq j-i < n$ so $p \mid d$ #

$d(i+1)+1 \bmod p = 1$ $\quad$ $p \mid d(j-i)$

Proof of Main Lemma (R_f = graph(f) is an r.e. relation)

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1) \quad \text{where } rm(x, y) = x \bmod y$$

Lemma 0. $\forall n, r_0, r_1, \ldots, r_n \ \exists c, d$ such that $\forall i \leq n \ \beta(c, d, i) = r_i$

the pair (c, d) represents the sequence $\underbrace{r_0 r_1, \ldots r_n}_{\text{entire tableaux of TM configuration}}$ using β

Lemma 1 graph(β) is a Δ_0 relation

Proof of Main Lemma (see pp 70-71)

Lemma 0 $\forall n, r_0, r_1, \ldots, r_n \ \exists c, d$ such that $\beta(c,d,i) = r_i \quad \forall i, 0 \le i \le n$

Lemma 1 graph(β) is a Δ_0 relation

Proof We want a Δ_0 formula $A(c,d,i,y)$ such that A is true on input (c,d,i,y) iff $\beta(c,d,i) = y$.

$c \bmod x = y$
$c = x \cdot q + y$
$y < x$

$$y = \beta(c,d,i) \iff c \bmod d(i+1)+1 = y$$
$$\iff c = [\underbrace{d(i+1)+1}]q + y, \quad \text{where } y < d(i+1)+1$$

$\therefore$

$$y = \beta(c,d,i) \iff \underbrace{[\exists q \le c\,(c = q(d(i+1)+1)+y) \wedge y < d(i+1)+1]}_{A_\beta(c,d,i,y)}$$

Proof of Main Lemma (R_f = graph(f) is an r.e. relation)

Definition β-function

$$\beta(c, d, i) = rm(c, d(i+1)+1) \quad \text{where } rm(x, y) = x \bmod y$$

Lemma 0. $\forall n, r_0, r_1, \ldots, r_n \ \exists c, d$ such that $\forall i \le n \ \beta(c,d,i) = r_i$

the pair (c,d) represents the sequence $\underbrace{r_0 r_1, \ldots r_n}_{\text{entire tableaux of TM configuration}}$ using β

Lemma 1 graph(β) is a Δ_0 relation

Recap: we wanted to prove

$\exists\Delta_0$ (Exists-Delta) Theorem every r.e. relation is represented by a $\exists\Delta_0$ formula

which followed by **Main Lemma**:

f total, computable $\Rightarrow R_f$ is a $\exists\Delta_0$ relation

Recap: First Incompleteness Theorem

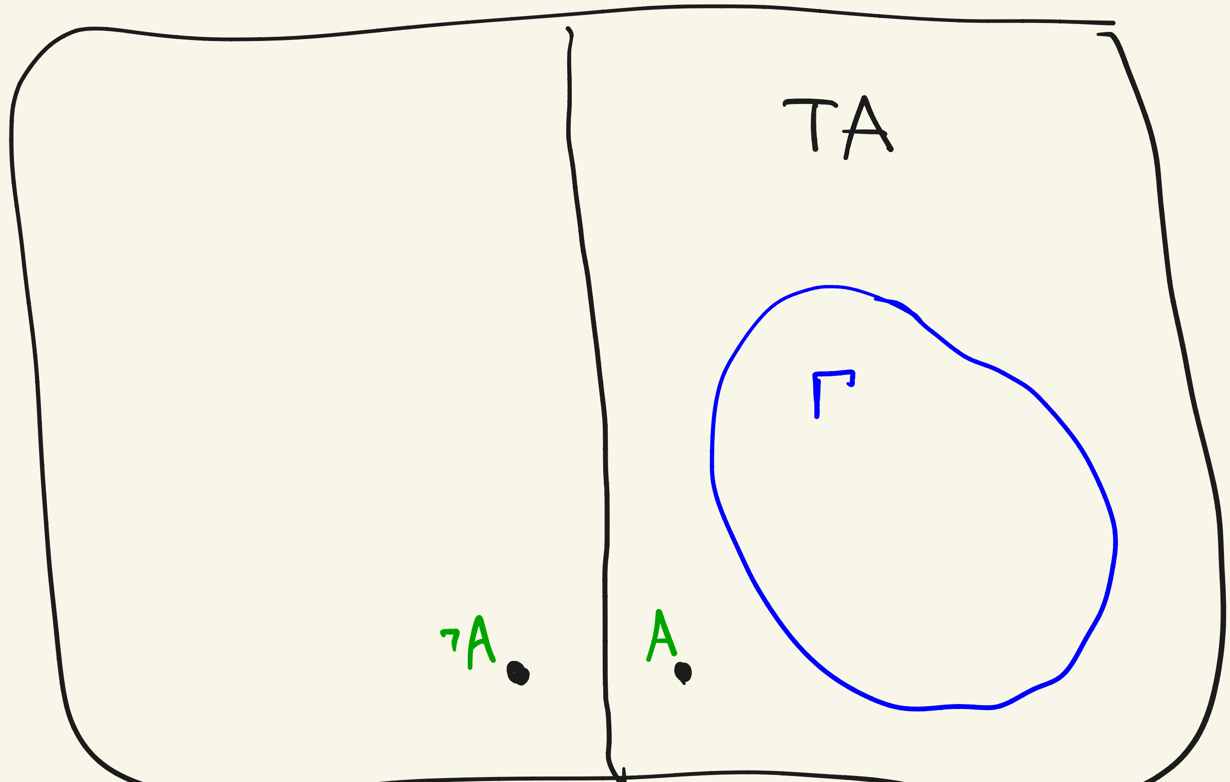
1st Incompleteness Theorem: TA is not axiomatizable

That is, any sound, axiomatizable theory is incomplete.

→ PA is axiomatizable. So assuming PA is sound, it is incomplete (so there are sentences A such that neither A or $\neg A$ is provable from axioms of PA.)

$$K^c = \{ \underbrace{\tilde{x} \mid \{x\}(x) \text{ doesn't halt}}_{F(\tilde{x})} \} \qquad K$$

Φ_0: all $\mathcal{L}_A$ sentences



Γ sound and axiomatizable $\Rightarrow \exists A, \neg A \notin \Gamma$