BILL RECORD LECTURE!!!!

BILL RECORD LECTURE!!!

FINAL IS THURSDAY

May 15

10:30AM-12:30PM

FILL OUT COURSE EVALS for ALL YOUR COURSES!!!

Review for Final: Dec and Undec

Rules

1. **Begin** Final Thursday May 15, 10:30AM-12:30PM in IRB 1116 (unless you have contacted me to make other plans.)

Rules

1. **Begin** Final Thursday May 15, 10:30AM-12:30PM in IRB 1116 (unless you have contacted me to make other plans.)
2. **Resources** You can bring one sheet of notes and use both sides.

Rules

1. **Begin** Final Thursday May 15, 10:30AM-12:30PM in IRB 1116 (unless you have contacted me to make other plans.)
2. **Resources** You can bring one sheet of notes and use both sides.
3. **Warning** Cramming the entire course on to those pages does not work.

Rules

1. **Begin** Final Thursday May 15, 10:30AM-12:30PM in IRB 1116 (unless you have contacted me to make other plans.)
2. **Resources** You can bring one sheet of notes and use both sides.
3. **Warning** Cramming the entire course on to those pages does not work.
4. **Scope of the Exam:** My Slides and the HW.

Turing Machines

Turing Machines

1. For this review we omit definitions and conventions.

Turing Machines

1. For this review we omit definitions and conventions.
2. There is a JAVA program for function f iff there is a TM that computes f.

Turing Machines

1. For this review we omit definitions and conventions.
2. There is a JAVA program for function f iff there is a TM that computes f.
3. Everything computable can be done by a TM.

Decidable Sets

Def A set A is DECIDABLE if there is a Turing Machine M such that

Decidable Sets

Def A set A is DECIDABLE if there is a Turing Machine M such that

$$x \in A \to M(x) = Y$$

Decidable Sets

Def A set A is DECIDABLE if there is a Turing Machine M such that

$$x \in A \to M(x) = Y$$

$$x \notin A \to M(x) = N$$

What is a Theory

What is a Theory

1. All theories have the usual logical symbols, a domain of discourse for the quantifiers, and **Additional Symbols** .

What is a Theory

1. All theories have the usual logical symbols, a domain of discourse for the quantifiers, and **Additional Symbols** .
2. Sentences are combos of Atomic Fmls using $\wedge$, $\vee$, $\neg$, $\exists$ that have all variables quantified over.

What is a Theory

1. All theories have the usual logical symbols, a domain of discourse for the quantifiers, and **Additional Symbols** .
2. Sentences are combos of Atomic Fmls using $\wedge$, $\vee$, $\neg$, $\exists$ that have all variables quantified over.
3. Hence sentences are either TRUE or FALSE.

What is a Theory

1. All theories have the usual logical symbols, a domain of discourse for the quantifiers, and **Additional Symbols** .
2. Sentences are combos of Atomic Fmls using $\wedge$, $\vee$, $\neg$, $\exists$ that have all variables quantified over.
3. Hence sentences are either TRUE or FALSE.
4. Our main question will be **Is this theory decidable?**

WS1S Formulas and Sentences

WS1S Formulas and Sentences

1. Variables x, y, z range over $\mathbb{N}$, X, Y, Z range over finite subsets of $\mathbb{N}$.

WS1S Formulas and Sentences

1. Variables x, y, z range over $\mathbb{N}$, X, Y, Z range over finite subsets of $\mathbb{N}$.
2. Symbols: $<$, $\in$, $\equiv \pmod{}$ (usual meaning), S (meaning $S(x) = x + 1$), $=$ (for numbers and sets).

WS1S Formulas and Sentences

1. Variables x, y, z range over $\mathbb{N}$, X, Y, Z range over finite subsets of $\mathbb{N}$.
2. Symbols: $<$, $\in$, $\equiv \pmod{\ }$ (usual meaning), S (meaning $S(x) = x + 1$), $=$ (for numbers and sets).
3. Define atomic formulas, formulas, and sentences in the usual way.

TRUE Sets

Def If $\phi(x_1, \ldots, x_n, X_1, \ldots, X_m)$ is a WS1S Formula then $TRUE(\phi)$ is the set

TRUE Sets

Def If $\phi(x_1, \ldots, x_n, X_1, \ldots, X_m)$ is a WS1S Formula then $TRUE(\phi)$ is the set

$$\{(a_1, \ldots, a_n, A_1, \ldots, A_m) \mid \phi(a_1, \ldots, a_n, A_1, \ldots, A_m) = T\}$$

KEY THEOREM

Thm For all WS1S formulas ϕ the set $TRUE_\phi$ is regular.

KEY THEOREM

Thm For all WS1S formulas ϕ the set $TRUE_\phi$ is regular.

Need to clarify representation and the define stupid states to make all of this work.

KEY THEOREM

Thm For all WS1S formulas ϕ the set $TRUE_\phi$ is regular.

Need to clarify representation and the define stupid states to make all of this work.

We prove this by induction on the formation of a formula. If you prefer- induction on the LENGTH of a formula.

DECIDABILITY OF WS1S

Thm: WS1S is Decidable.
Proof:

1. Given a SENTENCE in WS1S put it into the form

   $$(Q_1X_1)\cdots(Q_nX_n)(Q_{n+1}x_1)\cdots(Q_{n+m}x_m)[\phi(x_1,\ldots,x_m,X_1,\ldots,X_n)]$$

2. Assume $Q_1 = \exists$. (If not then negate and negate answer.)
3. View as $(\exists X)[\phi(X)]$, a FORMULA with ONE free var.
4. Construct DFA M for $\{X \mid \phi(X) \text{ is true}\}$.
5. Test if $L(M) = \emptyset$.
6. If $L(M) \neq \emptyset$ then $(\exists X)[\phi(X)]$ is TRUE.
   If $L(M) = \emptyset$ then $(\exists X)[\phi(X)]$ is FALSE.

Undecidability

Notation

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.
$M_e(d)\downarrow$ means $M_e(d)$ halts.

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.
$M_e(d) \downarrow$ means $M_e(d)$ halts.
$M_e(d) \uparrow$ means $M_e(d)$ does not halts.

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.
$M_e(d)\downarrow$ means $M_e(d)$ halts.
$M_e(d)\uparrow$ means $M_e(d)$ does not halts.
$M_{e,s}(d)\downarrow$ means $M_e(d)$ halts within s steps.

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.
$M_e(d)\downarrow$ means $M_e(d)$ halts.
$M_e(d)\uparrow$ means $M_e(d)$ does not halts.
$M_{e,s}(d)\downarrow$ means $M_e(d)$ halts within s steps.
$M_{e,s}(d)\downarrow= z$ means $M_e(d)$ halts within s steps and outputs z.

Notation

Notation $M_{e,s}(d)$ is the result of running $M_e(d)$ for s steps.
$M_e(d)\downarrow$ means $M_e(d)$ halts.
$M_e(d)\uparrow$ means $M_e(d)$ does not halts.
$M_{e,s}(d)\downarrow$ means $M_e(d)$ halts within s steps.
$M_{e,s}(d)\downarrow= z$ means $M_e(d)$ halts within s steps and outputs z.
$M_{e,s}(d)\uparrow$ means $M_e(d)$ has not halted within s steps.

Noncomputable Sets

Are there any noncomputable sets?

1. Yes—ALL SETS: uncountable. DEC Sets: countable, hence there exists an uncountable number of noncomputable sets.
2. YES—HALT is undecidable, and once you have that you have many other sets undec.
3. YES—the problem of telling if a $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has an int solution is undecidable.

Noncomputable Sets

Are there any noncomputable sets?

1. Yes—ALL SETS: uncountable. DEC Sets: countable, hence there exists an uncountable number of noncomputable sets.
2. YES—HALT is undecidable, and once you have that you have many other sets undec.
3. YES—the problem of telling if a $p \in \mathbb{Z}[x_1, \ldots, x_n]$ has an int solution is undecidable. We will come back to this one later.
4. YES—there are other natural problems that are undecidable.

The HALTING Problem

Def The HALTING set is the set

$$HALT = \{(e, d) \mid M_e(d) \text{ halts } \}.$$

The HALTING Problem

Def The HALTING set is the set

$$HALT = \{(e, d) \mid M_e(d) \text{ halts } \}.$$

Thm HALT is not computable.

Def $A \in \Sigma_1$ if there exists decidable B such that

$$A = \{x : (\exists y)[(x, y) \in B]\}$$

Def $A \in \Sigma_1$ if there exists decidable B such that

$$A = \{x : (\exists y)[(x, y) \in B]\}$$

Similar to NP.

Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.

It was proven:

Hilbert's Tenth Problem

Hilbert's 10th problem (in modern language) Give an algorithm that will, given $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ determine if there exists $a_1, \ldots, a_n \in \mathbb{Z}$ such that $p(a_1, \ldots, a_n) = 0$.
It was proven:

Thm There is no such algorithm.

Beginning of the Proof that H10 is Undecidable

The proof consists of

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.
2. Show that HALT can be expressed using polynomials.

Beginning of the Proof that H10 is Undecidable

The proof consists of

1. Show that many sets can be expressed using polynomials.
2. Show that HALT can be expressed using polynomials.

We will discuss expressing sets using polynomials.

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

Diophantine Sets

Def A is **Diophantine (Dio)** if there exists a polynomial $p(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

$$a \in A \text{ iff } (\exists a_1, \ldots, a_n)[(a \geq 0) \wedge (p(a_1, \ldots, a_n, a) = 0)].$$

Examples of Dio Sets

For $a, m \in \mathbb{N}$.

$$\{x : x \equiv 4 \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - 4 = 0)]\}$$

Examples of Dio Sets

For $a, m \in \mathbb{N}$.

$$\{x : x \equiv 4 \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - 4 = 0)]\}$$

$$\{x : x \not\equiv a \pmod{m}\}.$$

Examples of Dio Sets

For $a, m \in \mathbb{N}$.

$$\{x : x \equiv 4 \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \land (x - 11y - 4 = 0)]\}$$

$\{x : x \not\equiv a \ (\text{mod}\ m)\}$.

$$\{x : x \not\equiv a \pmod{m}\} = \bigcup_{i=0, i\neq 4}^{10} \{x : x \equiv i \pmod{11}\}$$

Examples of Dio Sets

For $a, m \in \mathbb{N}$.

$\{x : x \equiv 4 \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - 4 = 0)]\}$

$\{x : x \not\equiv a \ (\text{mod } m)\}$.

$$\{x : x \not\equiv a \pmod{m}\} = \bigcup_{i=0, i \neq 4}^{10} \{x : x \equiv i \pmod{11}\}$$

$\{x : x \equiv i \ (\text{mod } 11)\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - i = 0)]\}$

Examples of Dio Sets

For $a, m \in \mathbb{N}$.

$$\{x : x \equiv 4 \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - 4 = 0)]\}$$

$\{x : x \not\equiv a \pmod{m}\}$.

$$\{x : x \not\equiv a \pmod{m}\} = \bigcup_{i=0, i\neq 4}^{10} \{x : x \equiv i \pmod{11}\}$$

$\{x : x \equiv i \pmod{11}\} = \{x : (\exists y)[(x \geq 0) \wedge (x - 11y - i = 0)]\}$
Use MULT for OR $\{x : x \not\equiv a \pmod{m}\} =$
$\{x : (\exists y_1, y_2, y_3, y_5, y_6, y_7, y_8, y_9, y_{10})[\prod_{i=0,\neq 4}^{10}(x - 11y - i) = 0]$.

Dio Sets are Closed Under Union

Let A, B be Dio Sets.

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

Dio Sets are Closed Under Union

Let A, B be Dio Sets.
$A = \{x : (\exists y_1, \ldots, y_n)[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) = 0)]\}$
$B = \{x : (\exists z_1, \ldots, z_n)[(x \geq 0) \wedge (p_B(z_1, \ldots, z_n, x) = 0)]\}$

$$\{x : (\exists y_1, \ldots, y_n, z_1, \ldots, z_n)$$

$$[(x \geq 0) \wedge (p_A(y_1, \ldots, y_n, x) p_B(z_1, \ldots, z_n, x) = 0)]\}.$$

Beyond Σ_1

Def B is always a decidable set.

Beyond Σ_1

Def B is always a decidable set.
$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x, y_1, y_2) \in B]\}$.

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x,y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x,y_1,y_2) \in B]\}$.

$A \in \Pi_2$ if $A = \{x : (\forall y_1)(\exists y_2)[(x,y_1,y_2) \in B]\}$.

$\vdots$

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x, y_1, y_2) \in B]\}$.

$A \in \Pi_2$ if $A = \{x : (\forall y_1)(\exists y_2)[(x, y_1, y_2) \in B]\}$.

$\vdots$

$TOT = \{x : (\forall y)(\exists s)[M_{x,s}(y) \downarrow]\} \in \Pi_2$.

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x, y_1, y_2) \in B]\}$.

$A \in \Pi_2$ if $A = \{x : (\forall y_1)(\exists y_2)[(x, y_1, y_2) \in B]\}$.

$\vdots$

$TOT = \{x : (\forall y)(\exists s)[M_{x,s}(y) \downarrow]\} \in \Pi_2$.

Known: $TOT \notin \Sigma_1 \cup \Pi_1$.

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x, y_1, y_2) \in B]\}$.

$A \in \Pi_2$ if $A = \{x : (\forall y_1)(\exists y_2)[(x, y_1, y_2) \in B]\}$.

$\vdots$

$TOT = \{x : (\forall y)(\exists s)[M_{x,s}(y) \downarrow]\} \in \Pi_2$.

Known: $TOT \notin \Sigma_1 \cup \Pi_1$.

Known:

$\Sigma_1 \subset \Sigma_2 \subset \Sigma_3 \cdots$

$\Pi_1 \subset \Pi_2 \subset \Pi_3 \cdots$

Beyond Σ_1

Def B is always a decidable set.

$A \in \Pi_1$ if $A = \{x : (\forall y)[(x, y) \in B]\}$.

$A \in \Sigma_2$ if $A = \{x : (\exists y_1)(\forall y_2)[(x, y_1, y_2) \in B]\}$.

$A \in \Pi_2$ if $A = \{x : (\forall y_1)(\exists y_2)[(x, y_1, y_2) \in B]\}$.

$\vdots$

$TOT = \{x : (\forall y)(\exists s)[M_{x,s}(y) \downarrow]\} \in \Pi_2$.

Known: $TOT \notin \Sigma_1 \cup \Pi_1$.

Known:

$\Sigma_1 \subset \Sigma_2 \subset \Sigma_3 \cdots$

$\Pi_1 \subset \Pi_2 \subset \Pi_3 \cdots$

TOT is **harder** than HALT.