universität innsbruck

26W lecture 6



Computability Theory

Aart Middeldorp

Outline

1. **Summary of Previous Lecture**
2. **Recursive and Recursive Enumerable Sets**
3. **Diophantine Sets**
4. **Fibonacci Numbers**
5. **Summary**

Definition

$\varphi_e^n(x_1, \ldots, x_n) = \mathrm{u}((\mu\, y)\, (\mathrm{t}_n(e, x_1, \ldots, x_n, y) = 0))$

Lemma

φ_0^n, φ_1^n, φ_2^n, ... is computable enumeration of all n–ary partial recursive functions

Definition

predicate $P\colon \mathbb{N}^n \to \mathbb{B}$ is decidable if χ_P is recursive

Theorem

following problem is undecidable:

instance: natural number x

question: is $\varphi_x(x)$ defined ?

Kleene's s–m–n or Parameterization Theorem

$\forall\, m, n \geqslant 1 \quad \exists$ primitive recursive function $s_n^m \colon \mathbb{N}^{m+1} \to \mathbb{N} \quad \forall\, e \in \mathbb{N}$

$$\varphi_e^{m+n}(x_1, \ldots, x_m, y_1, \ldots, y_n) \simeq \varphi_{s_n^m(e, x_1, \ldots, x_m)}^n(y_1, \ldots, y_n)$$

Kleene's Fixed Point Theorem

$\forall$ recursive function $f \colon \mathbb{N} \to \mathbb{N} \quad \exists\, e \in \mathbb{N}$ such that $\varphi_e(x) \simeq \varphi_{f(e)}(x)$

Part I: Recursive Function Theory

Ackermann function, bounded minimization, bounded recursion, course–of–values recursion, diagonalization, diophantine sets, elementary functions, fixed point theorem, Fibonacci numbers, Gödel numbering, Gödel's β function, Grzegorczyk hierarchy, loop programs, minimization, normal form theorem, partial recursive functions, primitive recursion, recursive enumerability, recursive inseparability, s–m–n theorem, total recursive functions, undecidability, while programs

Part II: Combinatory Logic

abstraction, arithmetization, CL–representability, combinators, combinatorial completeness, Church numerals, Church–Rosser theorem, Curry–Howard isomorphism, fixed point theorem, intuitionistic propositional logic, normalization theorem, termination, typing, undecidability, Z property

Part I: Recursive Function Theory

Ackermann function, bounded minimization, bounded recursion, course–of–values recursion, diagonalization, diophantine sets, elementary functions, fixed point theorem, Fibonacci numbers, Gödel numbering, Gödel's β function, Grzegorczyk hierarchy, loop programs, minimization, normal form theorem, partial recursive functions, primitive recursion, recursive enumerability, recursive inseparability, s–m–n theorem, total recursive functions, undecidability, while programs

Part II: Combinatory Logic

abstraction, arithmetization, CL–representability, combinators, combinatorial completeness, Church numerals, Church–Rosser theorem, Curry–Howard isomorphism, fixed point theorem, intuitionistic propositional logic, normalization theorem, termination, typing, undecidability, Z property

Outline

1. Summary of Previous Lecture

2. **Recursive and Recursive Enumerable Sets**

3. Diophantine Sets

4. Fibonacci Numbers

5. Summary

Definitions

- set $A \subseteq \mathbb{N}$ is recursive if its characteristic function $\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$ is recursive

Definitions

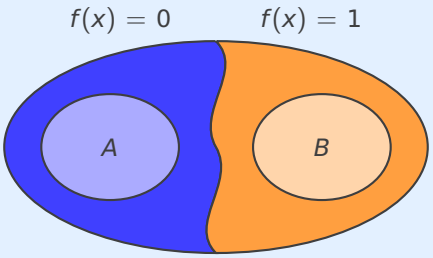
- set $A \subseteq \mathbb{N}$ is recursive if its characteristic function $\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$ is recursive
- disjoint sets $A, B \subseteq \mathbb{N}$ are recursively separable if $\exists$ recursive function $f\colon \mathbb{N} \to \{0, 1\}$ such that

$$x \in A \implies f(x) = 0 \qquad x \in B \implies f(x) = 1$$

Definitions

- set $A \subseteq \mathbb{N}$ is recursive if its characteristic function $\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$ is recursive
- disjoint sets $A, B \subseteq \mathbb{N}$ are recursively separable if $\exists$ recursive function $f\colon \mathbb{N} \to \{0,1\}$ such that

$$x \in A \implies f(x) = 0 \qquad x \in B \implies f(x) = 1$$



Lemma

if A and B are recursively inseparable then A and B are not recursive

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f \colon \mathbb{N} \to \{0, 1\}$ separating A and B

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f \colon \mathbb{N} \to \{0, 1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f \colon \mathbb{N} \to \{0, 1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f\colon \mathbb{N} \to \{0, 1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

$$f(e) = 0$$

$$f(e) = 1$$

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f\colon \mathbb{N} \to \{0,1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

$$f(e) = 0 \implies \varphi_e(e) = 1$$
$$f(e) = 1 \implies \varphi_e(e) = 0$$

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f\colon \mathbb{N} \to \{0,1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

$$f(e) = 0 \implies \varphi_e(e) = 1 \implies e \in B$$
$$f(e) = 1 \implies \varphi_e(e) = 0 \implies e \in A$$

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f\colon \mathbb{N} \to \{0,1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

$$f(e) = 0 \implies \varphi_e(e) = 1 \implies e \in B \implies f(e) = 1$$
$$f(e) = 1 \implies \varphi_e(e) = 0 \implies e \in A \implies f(e) = 0$$

Lemma

if A and B are recursively inseparable then A and B are not recursive

Theorem

sets $A = \{x \mid \varphi_x(x) = 0\}$ and $B = \{x \mid \varphi_x(x) = 1\}$ are recursively inseparable

Proof

- suppose $\exists$ recursive function $f\colon \mathbb{N} \to \{0,1\}$ separating A and B
- $g(x) = 1 \dot{-} f(x)$ is recursive
- $\exists\, e$ such that $g = \varphi_e$

$$f(e) = 0 \implies \varphi_e(e) = 1 \implies e \in B \implies f(e) = 1$$
$$f(e) = 1 \implies \varphi_e(e) = 0 \implies e \in A \implies f(e) = 0$$



Definition

set $A \subseteq \mathbb{N}$ is index set if

$$d \in A \wedge \varphi_e \simeq \varphi_d \quad \Longrightarrow \quad e \in A$$

for all $d, e \in \mathbb{N}$

Definition

set $A \subseteq \mathbb{N}$ is index set if

$$d \in A \wedge \varphi_e \simeq \varphi_d \quad \Longrightarrow \quad e \in A$$

for all $d, e \in \mathbb{N}$

Examples

- $\varnothing$ and $\mathbb{N}$ are (trivial) index sets

Definition

set $A \subseteq \mathbb{N}$ is index set if

$$d \in A \wedge \varphi_e \simeq \varphi_d \quad \Longrightarrow \quad e \in A$$

for all $d, e \in \mathbb{N}$

Examples

- $\varnothing$ and $\mathbb{N}$ are (trivial) index sets
- $\{e \mid \varphi_e$ is recursive function$\}$ is index set

Definition

set $A \subseteq \mathbb{N}$ is index set if

$$d \in A \wedge \varphi_e \simeq \varphi_d \quad \Longrightarrow \quad e \in A$$

for all $d, e \in \mathbb{N}$

Examples

- $\varnothing$ and $\mathbb{N}$ are (trivial) index sets
- $\{e \mid \varphi_e \text{ is recursive function}\}$ is index set
- $\{\langle 0\rangle, \langle 1\rangle\} \cup \{\langle 2, n, i\rangle \mid 1 \leqslant i \leqslant n\}$ is no index set

Definition

set $A \subseteq \mathbb{N}$ is index set if

$$d \in A \wedge \varphi_e \simeq \varphi_d \quad \Longrightarrow \quad e \in A$$

for all $d, e \in \mathbb{N}$

Examples

- $\varnothing$ and $\mathbb{N}$ are (trivial) index sets
- $\{e \mid \varphi_e$ is recursive function$\}$ is index set
- $\{\langle 0\rangle, \langle 1\rangle\} \cup \{\langle 2, n, i\rangle \mid 1 \leqslant i \leqslant n\}$ is no index set

Rice's Theorem

non–trivial index sets are not recursive

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive
- fixed point theorem $\implies$ $\exists\, a$ such that $\varphi_a \simeq \varphi_{f(a)}$

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive
- fixed point theorem $\implies$ $\exists\, a$ such that $\varphi_a \simeq \varphi_{f(a)}$

$a \in A$

$a \notin A$

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive
- fixed point theorem $\implies$ $\exists\, a$ such that $\varphi_a \simeq \varphi_{f(a)}$

$$a \in A \implies f(a) \in A$$
$$a \notin A \implies f(a) \notin A$$

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive
- fixed point theorem $\implies$ $\exists\, a$ such that $\varphi_a \simeq \varphi_{f(a)}$

$$a \in A \implies f(a) \in A \implies e \in A$$
$$a \notin A \implies f(a) \notin A \implies d \notin A$$

Rice's Theorem

non–trivial index sets are not recursive

Proof

- let A be non–trivial index set and let $d \in A$ and $e \notin A$
- suppose A is recursive
- function f defined by $f(x) = \begin{cases} e & \text{if } x \in A \\ d & \text{if } x \notin A \end{cases}$ is recursive
- fixed point theorem $\implies$ $\exists\, a$ such that $\varphi_a \simeq \varphi_{f(a)}$

$$a \in A \implies f(a) \in A \implies e \in A$$
$$a \notin A \implies f(a) \notin A \implies d \notin A$$



Definition

set $A \subseteq \mathbb{N}$ is recursively enumerable if $A = \varnothing$ or A is range of unary recursive function

Definition

set $A \subseteq \mathbb{N}$ is recursively enumerable if $A = \varnothing$ or A is range of unary recursive function

Remark

other terminology: semi–decidable computably enumerable

Definition

set $A \subseteq \mathbb{N}$ is recursively enumerable if $A = \varnothing$ or A is range of unary recursive function

Remark

other terminology: semi–decidable computably enumerable

Lemma

set A is recursive if and only if A and $\mathbb{N} \setminus A$ are recursively enumerable

Definition

set $A \subseteq \mathbb{N}$ is recursively enumerable if $A = \varnothing$ or A is range of unary recursive function

Remark

other terminology: semi−decidable computably enumerable

Lemma

set A is recursive if and only if A and $\mathbb{N} \setminus A$ are recursively enumerable

Theorem

following statements are equivalent for any set $A \subseteq \mathbb{N}$:

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 1 $\Longrightarrow$ 3

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 1 $\Longrightarrow$ 3

- $A = \varnothing$ or A is range of unary recursive function

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 1 $\Longrightarrow$ 3

- $A = \varnothing$ or A is range of unary recursive function
- $\varnothing$ is domain of unary partial recursive function $f(x) = (\mu\, y)\,(x + 1 = 0)$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 1 $\Longrightarrow$ 3

- $A = \varnothing$ or A is range of unary recursive function f
- $\varnothing$ is domain of unary partial recursive function $f(x) = (\mu\, y)\,(x + 1 = 0)$
- define unary function $g(x) = (\mu\, y)\,(f(y) = x)$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 1 $\Longrightarrow$ 3

- $A = \varnothing$ or A is range of unary recursive function f
- $\varnothing$ is domain of unary partial recursive function $f(x) = (\mu\, y)\,(x + 1 = 0)$
- define unary function $g(x) = (\mu\, y)\,(f(y) = x)$
- g is partial recursive

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof (1 $\Longrightarrow$ 3)

- $A = \varnothing$ or A is range of unary recursive function f
- $\varnothing$ is domain of unary partial recursive function $f(x) = (\mu\, y)\,(x + 1 = 0)$
- define unary function $g(x) = (\mu\, y)\,(f(y) = x)$
- g is partial recursive
- domain of g is A

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 ⟹ 2

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e
- define unary function $f(x) = x + \mathsf{z}(\varphi_e(x))$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e
- define unary function $f(x) = x + \mathrm{z}(\varphi_e(x))$
- f is partial recursive

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e
- define unary function $f(x) = x + \mathsf{z}(\varphi_e(x))$
- f is partial recursive
- $\varphi_e(x)\downarrow \iff f(x)\downarrow$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e
- define unary function $f(x) = x + \mathsf{z}(\varphi_e(x))$
- f is partial recursive
- $\varphi_e(x)\downarrow \iff f(x)\downarrow \implies f(x) = x$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 3 $\Longrightarrow$ 2

- suppose A is domain of unary partial recursive function φ_e
- define unary function $f(x) = x + \mathsf{z}(\varphi_e(x))$
- f is partial recursive
- $\varphi_e(x)\downarrow \iff f(x)\downarrow \implies f(x) = x$
- range of f is A

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof (2 $\Longrightarrow$ 1)

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof (2 $\Longrightarrow$ 1)

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive
- claim: range of g is A

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof (2 $\Longrightarrow$ 1)

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive
- claim: range of g is A
- $z \in A \implies z = \varphi_e(x)$ for some x

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive
- claim: range of g is A
- $z \in A \implies z = \varphi_e(x)$ for some $x \implies \mathsf{T}_1(e,x,y)$ for some y

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathsf{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive
- claim: range of g is A
- $z \in A \implies z = \varphi_e(x)$ for some $x \implies \mathsf{T}_1(e,x,y)$ for some y
- $f(x,s) = z$ for any $s > y$

1. A is recursively enumerable
2. A is range of unary partial recursive function
3. A is domain of unary partial recursive function

Proof 2 $\Longrightarrow$ 1

- suppose A is range of unary partial recursive function φ_e
- if $A = \varnothing$ then A is recursively enumerable suppose $A \neq \varnothing$ and let $a \in A$
- define $f(x,s) = \begin{cases} \varphi_e(x) & \text{if } (\exists\, y < s)\, \mathrm{T}_1(e,x,y) \\ a & \text{otherwise} \end{cases}$ and $g(x) = f(\pi_1(x), \pi_2(x))$
- f and g are recursive
- claim: range of g is A
- $z \in A \implies z = \varphi_e(x)$ for some $x \implies \mathrm{T}_1(e,x,y)$ for some y
- $f(x,s) = z$ for any $s > y \implies g(\pi(x,s)) = z$ for any $s > y$

Lemma

every non−empty recursively enumerable set $A \subseteq \mathbb{N}$ is range of primitive recursive function

Lemma

every non−empty recursively enumerable set $A \subseteq \mathbb{N}$ is range of primitive recursive function

Proof

- A is range of unary recursive function f

Lemma

every non−empty recursively enumerable set $A \subseteq \mathbb{N}$ is range of primitive recursive function

Proof

- A is range of unary recursive function f
- let e be index of f and let a be arbitrary element of A

Lemma

every non−empty recursively enumerable set $A \subseteq \mathbb{N}$ is range of primitive recursive function

Proof

- A is range of unary recursive function f
- let e be index of f and let a be arbitrary element of A
- function

$$g(x) = \begin{cases} \mathrm{u}((x)_1) & \text{if } \mathrm{T}_1(e, (x)_0, (x)_1) \\ a & \text{otherwise} \end{cases}$$

is primitive recursive

Lemma

every non−empty recursively enumerable set $A \subseteq \mathbb{N}$ is range of primitive recursive function

Proof

- A is range of unary recursive function f
- let e be index of f and let a be arbitrary element of A
- function

$$g(x) = \begin{cases} \mathrm{u}((x)_1) & \text{if } \mathrm{T}_1(e, (x)_0, (x)_1) \\ a & \text{otherwise} \end{cases}$$

  is primitive recursive
- range of g is A

Outline

1. Summary of Previous Lecture
2. Recursive and Recursive Enumerable Sets
3. **Diophantine Sets**
4. Fibonacci Numbers
5. Summary

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \quad \Longleftrightarrow \quad \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \quad \Longleftrightarrow \quad \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$ $\qquad P(x, y) = x - 2y$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$ $\qquad P(x, y) = x - 2y$
- $\{x^2 \mid x \in \mathbb{N}\}$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$ $\quad P(x, y) = x - 2y$
- $\{x^2 \mid x \in \mathbb{N}\}$ $\quad P(x, y) = x - y^2$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \quad \Longleftrightarrow \quad \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$ $\qquad P(x, y) = x - 2y$
- $\{x^2 \mid x \in \mathbb{N}\}$ $\qquad P(x, y) = x - y^2$
- $\qquad P(x, y, z) = x - (y + 2)(z + 2)$

Definition

set $A \subseteq \mathbb{N}$ is diophantine if $\exists$ polynomial $P(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \quad \Longleftrightarrow \quad \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0$$

Examples

- $\{x \mid x \text{ is even}\}$ $\qquad P(x, y) = x - 2y$
- $\{x^2 \mid x \in \mathbb{N}\}$ $\qquad P(x, y) = x - y^2$
- $\{x \geqslant 1 \mid x \text{ is composite}\}$ $\qquad P(x, y, z) = x - (y + 2)(z + 2)$

Lemma

diophantine sets are recursively enumerable

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set A

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$
- function $\varphi(x) = (\mu\, y)\, (P(x, (y)_1, \ldots, (y)_n)^2 = 0)$

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$
- function $\varphi(x) = (\mu\, y)\, (P(x, (y)_1, \ldots, (y)_n)^2 = 0)$ is partial recursive

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$
- function $\varphi(x) = (\mu\, y)\, (P(x, (y)_1, \ldots, (y)_n)^2 = 0)$ is partial recursive
- $x \in A \iff \varphi(x)\downarrow$

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$
- function $\varphi(x) = (\mu\, y)\, (P(x, (y)_1, \ldots, (y)_n)^2 = 0)$ is partial recursive
- $x \in A \iff \varphi(x)\downarrow$

Theorem (Matiyasevich 1970)

recursively enumerable sets are diophantine

Lemma

diophantine sets are recursively enumerable

Proof

- arbitrary diophantine set $A = \{x \mid \exists\, y_1 \cdots \exists\, y_n\, P(x, y_1, \ldots, y_n) = 0\}$
- function $\varphi(x) = (\mu\, y)\, (P(x, (y)_1, \ldots, (y)_n)^2 = 0)$ is partial recursive
- $x \in A \iff \varphi(x)\downarrow$

Theorem (Matiyasevich 1970)

recursively enumerable sets are diophantine

Corollary (MRDP Theorem)

Hilbert's 10th problem is unsolvable

Breaking News (OpenAI, 24 September 2026)

Hilbert's 10th problem over $\mathbb{Q}$ is unsolvable

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists x_1 \cdots \exists x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists y_1 \cdots \exists y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

define $P(x, y_1, \ldots, y_n) = x - (x+1)\,(Q(x, y_1, \ldots, y_n))^2$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

define $P(x, y_1, \ldots, y_n) = x - (x+1)\,(Q(x, y_1, \ldots, y_n))^2$

$$\{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } P(x, y_1, \ldots, y_n) \geqslant 0\}$$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

define $P(x, y_1, \ldots, y_n) = x - (x+1)\,(Q(x, y_1, \ldots, y_n))^2$

$$\{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } P(x, y_1, \ldots, y_n) \geqslant 0\}$$
$$= \{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } Q(x, y_1, \ldots, y_n) = 0\}$$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

define $P(x, y_1, \ldots, y_n) = x - (x+1)\,(Q(x, y_1, \ldots, y_n))^2$

$$\begin{aligned} &\{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } P(x, y_1, \ldots, y_n) \geqslant 0\} \\ &= \{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } Q(x, y_1, \ldots, y_n) = 0\} \\ &= \{x \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } Q(x, y_1, \ldots, y_n) = 0\} \end{aligned}$$

Lemma

A is recursively enumerable $\iff$ $A = \{P(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{N} \text{ and } P(x_1, \ldots, x_n) \geqslant 0\}$ for some polynomial $P(x_1, \ldots, x_n)$ with integer coefficients

Proof

$\Longleftarrow$ $x \in A \iff \exists\, x_1 \cdots \exists\, x_n \quad P(x_1, \ldots, x_n) - x = 0$

$\Longrightarrow$ $\exists$ polynomial $Q(x, y_1, \ldots, y_n)$ with integer coefficients such that

$$x \in A \iff \exists\, y_1 \cdots \exists\, y_n \quad Q(x, y_1, \ldots, y_n) = 0$$

define $P(x, y_1, \ldots, y_n) = x - (x+1)\,(Q(x, y_1, \ldots, y_n))^2$

$$\begin{aligned} &\{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } P(x, y_1, \ldots, y_n) \geqslant 0\} \\ &= \{P(x, y_1, \ldots, y_n) \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } Q(x, y_1, \ldots, y_n) = 0\} \\ &= \{x \mid x, y_1, \ldots, y_n \in \mathbb{N} \text{ and } Q(x, y_1, \ldots, y_n) = 0\} \;=\; A \end{aligned}$$

Example

polynomial $P(a, b, \ldots, z)$:

$$
\begin{aligned}
(k+2)\Big(1 &- (wz+h+j-q)^2 - \big((gk+2g+k+1)(h+j)+h-z\big)^2 \\
&- (2n+p+q+z-e)^2 - \big((a^2-1)y^2+1-x^2\big)^2 \\
&- \big(16(k+1)^3(k+2)(n+1)^2+1-f^2\big)^2 - (n+l+v-y)^2 \\
&- \big(16r^2y^4(a^2-1)+1-u^2\big)^2 - (e^3(e+2)(a+1)^2+1-o^2)^2 \\
&- \big(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2\big)^2 \\
&- \big((a^2-1)l^2+1-m^2\big)^2 - (ai+k+1-l-i)^2 \\
&- \big(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\big)^2 \\
&- \big(z+pl(a-p)+t(2ap-p^2-1)-pm\big)^2 \\
&- \big(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\big)^2\Big)
\end{aligned}
$$

Example (Jones, Sato, Wada, Wiens 1976)

polynomial $P(a, b, \ldots, z)$:

$$
\begin{aligned}
(k+2)\Big(1 &- (wz+h+j-q)^2 - \big((gk+2g+k+1)(h+j)+h-z\big)^2 \\
&- (2n+p+q+z-e)^2 - \big((a^2-1)y^2+1-x^2\big)^2 \\
&- \big(16(k+1)^3(k+2)(n+1)^2+1-f^2\big)^2 - (n+l+v-y)^2 \\
&- \big(16r^2y^4(a^2-1)+1-u^2\big)^2 - (e^3(e+2)(a+1)^2+1-o^2)^2 \\
&- \big(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2\big)^2 \\
&- \big((a^2-1)l^2+1-m^2\big)^2 - (ai+k+1-l-i)^2 \\
&- \big(p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m\big)^2 \\
&- \big(z+pl(a-p)+t(2ap-p^2-1)-pm\big)^2 \\
&- \big(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\big)^2\Big)
\end{aligned}
$$

generates all prime numbers

Examples (Prime Generating Functions)

- $\left\lfloor \frac{n! \bmod (n+1)}{n} \right\rfloor (n-1) + 2$

Examples (Prime Generating Functions)

- $\left\lfloor \frac{n! \bmod (n+1)}{n} \right\rfloor (n-1) + 2$
- $1 + \sum_{i=1}^{2^n} \left\lfloor \left(\frac{n}{\sum_{j=1}^{i} \left\lfloor \cos^2 \left(\frac{(j-1)!+1}{j} \pi \right) \right\rfloor} \right)^{1/n} \right\rfloor$

Outline

1. Summary of Previous Lecture
2. Recursive and Recursive Enumerable Sets
3. Diophantine Sets
4. **Fibonacci Numbers**
5. Summary

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Theorem (Jones 1975)

$P(x, y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Theorem (Jones 1975)

$P(x, y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

demo

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0$
- $i = 1$
- $i > 1$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0$
- $i = 1$
- $i > 1$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1$
- $i > 1$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1$
- $i > 1$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (F_{i-1} + F_i)^2 - (F_{i-1} + F_i) F_i - F_i^2$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (F_{i-1} + F_i)^2 - (F_{i-1} + F_i) F_i - F_i^2 = -F_i^2 + F_{i-1}^2 + F_i F_{i-1}$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (F_{i-1} + F_i)^2 - (F_{i-1} + F_i) F_i - F_i^2 = -F_i^2 + F_{i-1}^2 + F_i F_{i-1}$
  $= -(F_i^2 - F_i F_{i-1} - F_{i-1}^2)$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (F_{i-1} + F_i)^2 - (F_{i-1} + F_i) F_i - F_i^2 = -F_i^2 + F_{i-1}^2 + F_i F_{i-1}$
  $= -(F_i^2 - F_i F_{i-1} - F_{i-1}^2) = -(-1)^{i-1}$

Definition (Fibonacci numbers)

$$F_0 = 0 \qquad F_1 = 1 \qquad F_{n+2} = F_n + F_{n+1}$$

Lemma 1

$F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (-1)^i$ for all $i \geqslant 0$

Proof

induction on i

- $i = 0 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 0 - 0 = 1 = (-1)^0$
- $i = 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = 1 - 1 - 1 = -1 = (-1)^1$
- $i > 1 \implies F_{i+1}^2 - F_{i+1} F_i - F_i^2 = (F_{i-1} + F_i)^2 - (F_{i-1} + F_i) F_i - F_i^2 = -F_i^2 + F_{i-1}^2 + F_i F_{i-1}$
  $= -(F_i^2 - F_i F_{i-1} - F_{i-1}^2) = -(-1)^{i-1} = (-1)^i$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \quad \Longrightarrow \quad x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0$
- $x > 0$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1$
- $x > 0$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \quad \Longrightarrow \quad x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \quad \Longrightarrow \quad y = 1 \quad \Longrightarrow \quad i = 0$
- $x > 0$

Lemma ❷

$y^2 - yx - x^2 = 1 \ \wedge \ x, y \geqslant 0 \quad \Longrightarrow \quad x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \quad \Longrightarrow \quad y = 1 \quad \Longrightarrow \quad i = 0$
- $x > 0 \quad \Longrightarrow \quad yx + x^2 > y$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

$(x+1)^2 = x^2 + 2x + 1$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

$(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

$y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

  $b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

  $b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - yx - x^2 = 1$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

  $b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - yx - x^2 = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ by induction hypothesis

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

$(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

$y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

$b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - yx - x^2 = 1$

$a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ by induction hypothesis

$x = a + b$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

$(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

$y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

$b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - yx - x^2 = 1$

$a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ by induction hypothesis

$x = a + b$ and $y = b + x$

Lemma ❷

$y^2 - yx - x^2 = 1 \wedge x, y \geqslant 0 \implies x = F_{2i}$ and $y = F_{2i+1}$ for some $i \geqslant 0$

Proof

induction on x

- $x = 0 \implies y = 1 \implies i = 0$
- $x > 0 \implies yx + x^2 > y \implies 1 = y^2 - (yx + x^2) < y^2 - y \implies y \geqslant 2$

  $(x+1)^2 = x^2 + 2x + 1 \leqslant x^2 + yx + 1 = y^2 \implies y > x$

  $y^2 = yx + x^2 + 1 \leqslant yx + x^2 + x = yx + (x+1)x \leqslant yx + yx = 2yx \implies y \leqslant 2x$

  let $a = 2x - y$ and $b = y - x \implies 0 \leqslant a < x$ and $0 < b$

  $b^2 - ba - a^2 = (y-x)^2 - (y-x)(2x-y) - (2x-y)^2 = y^2 - yx - x^2 = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ by induction hypothesis

  $x = a + b$ and $y = b + x \implies x = F_{2(i+1)}$ and $y = F_{2(i+1)+1}$

Lemma ❸

$y^2 - yx - x^2 = -1 \;\wedge\; x \geqslant 0 \;\wedge\; y > 0 \quad \Longrightarrow \quad x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

- $y < x$

Lemma ❸

$y^2 - yx - x^2 = -1 \;\wedge\; x \geqslant 0 \;\wedge\; y > 0 \quad\Longrightarrow\quad x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y - x) - (y - x)^2$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$ and $y = a + x = F_{2i+2}$

- $y < x$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$ and $y = a + x = F_{2i+2}$

- $y < x \implies yx = y^2 - x^2 + 1 \leqslant 0$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$ and $y = a + x = F_{2i+2}$

- $y < x \implies yx = y^2 - x^2 + 1 \leqslant 0 \implies yx = 0$

Lemma 3

$y^2 - yx - x^2 = -1 \;\wedge\; x \geqslant 0 \;\wedge\; y > 0 \quad\Longrightarrow\quad x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$ and $y = a + x = F_{2i+2}$

- $y < x \quad\Longrightarrow\quad yx = y^2 - x^2 + 1 \leqslant 0 \quad\Longrightarrow\quad yx = 0 \quad\Longrightarrow\quad x = 0$

Lemma 3

$y^2 - yx - x^2 = -1 \wedge x \geqslant 0 \wedge y > 0 \implies x = F_{2i+1}$ and $y = F_{2i+2}$ for some $i \geqslant 0$

Proof

case analysis

- $x \leqslant y$

  let $a = y - x$ and $b = x$

  $a \geqslant 0$ and $b \geqslant 0$

  $b^2 - ba - a^2 = x^2 - x(y-x) - (y-x)^2 = -(y^2 - yx - x^2) = 1$

  $a = F_{2i}$ and $b = F_{2i+1}$ for some $i \geqslant 0$ according to lemma 2

  $x = F_{2i+1}$ and $y = a + x = F_{2i+2}$

- $y < x \implies yx = y^2 - x^2 + 1 \leqslant 0 \implies yx = 0 \implies x = 0$ ↯

Corollary 1

$\{x \geqslant 0 \mid y^2 - yx - x^2 = \pm 1 \text{ for some } y > 0\}$ is set of Fibonacci numbers

Corollary 1

$\{x \geqslant 0 \mid y^2 - yx - x^2 = \pm 1 \text{ for some } y > 0\}$ is set of Fibonacci numbers

Corollary 2

$\{x \geqslant 0 \mid (y^2 - yx - x^2)^2 - 1 = 0 \text{ for some } y > 0\}$ is set of Fibonacci numbers

Corollary 1

$\{x \geqslant 0 \mid y^2 - yx - x^2 = \pm 1 \text{ for some } y > 0\}$ is set of Fibonacci numbers

Corollary 2

$\{x \geqslant 0 \mid (y^2 - yx - x^2)^2 - 1 = 0 \text{ for some } y \geqslant 0\}$ is set of Fibonacci numbers

Corollary

set of Fibonacci numbers is diophantine

Lemma 4

$$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0$
- $x > 0$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

$$4(y^2 - yx - x^2) = (2y - x)^2 - 5x^2$$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

$$4(y^2 - yx - x^2) = (2y - x)^2 - 5x^2$$

$$(2y - x)^2 - 5x^2 = 0 \quad \Longrightarrow \quad \sqrt{5} = \frac{|2y - x|}{x}$$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

$$4(y^2 - yx - x^2) = (2y - x)^2 - 5x^2$$

$$(2y - x)^2 - 5x^2 = 0 \quad \Longrightarrow \quad \sqrt{5} = \frac{|2y - x|}{x}$$



Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

$4(y^2 - yx - x^2) = (2y - x)^2 - 5x^2$

$(2y - x)^2 - 5x^2 = 0 \quad \Longrightarrow \quad \sqrt{5} = \dfrac{|2y - x|}{x}$ ↯

$(2y - x)^2 - 5x^2 \neq 0$

Lemma 4

$y > 0 \wedge x \geqslant 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$

Proof

case analysis

- $x = 0 \quad \Longrightarrow \quad y^2 - yx - x^2 = y^2 > 0$
- $x > 0$

$$4(y^2 - yx - x^2) = (2y - x)^2 - 5x^2$$

$$(2y - x)^2 - 5x^2 = 0 \quad \Longrightarrow \quad \sqrt{5} = \frac{|2y - x|}{x}$$ ↯

$$(2y - x)^2 - 5x^2 \neq 0 \quad \Longrightarrow \quad y^2 - yx - x^2 \neq 0$$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Proof

two directions

- x is Fibonacci number

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1}$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1}$ $\implies$ $(y^2 - yx - x^2)^2 = 1$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x, y) = x(2 - (y^2 - yx - x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2 - yx - x^2)^2 = 1 \implies 2 - (y^2 - yx - x^2)^2 = 1$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

$y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x, y \geqslant 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0$
  - $y > 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4)$
  - $y > 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1$
  - $y > 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4 $\implies 0 < (y^2-yx-x^2)^2$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4 $\implies 0 < (y^2-yx-x^2)^2 < 2$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4 $\implies 0 < (y^2-yx-x^2)^2 < 2$

    $(y^2-yx-x^2)^2 = 1$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4 $\implies 0 < (y^2-yx-x^2)^2 < 2$

    $(y^2-yx-x^2)^2 = 1 \implies z = x$

Theorem

set of Fibonacci numbers equals non−negative values of $P(x,y) = x(2-(y^2-yx-x^2)^2)$

Proof

two directions

- x is Fibonacci number $\implies$ $x = F_i$ for some $i \geqslant 0$

  $y = F_{i+1} \implies (y^2-yx-x^2)^2 = 1 \implies 2-(y^2-yx-x^2)^2 = 1 \implies P(x,y) = x$

- $z = P(x,y) > 0$ for some $x,y \geqslant 0 \implies z = x(2-(y^2-yx-x^2)^2)$

  two cases

  - $y = 0 \implies z = x(2-x^4) \implies x = 1 \implies z = x$ is Fibonacci number
  - $y > 0 \implies y^2-yx-x^2 \neq 0$ by lemma 4 $\implies 0 < (y^2-yx-x^2)^2 < 2$

    $(y^2-yx-x^2)^2 = 1 \implies z = x \implies z$ is Fibonacci number by corollary 2

Theorem (Jones 1975)

$P(x, y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

Theorem (Jones 1975)

$P(x,y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

Proof

$$2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x = x(2 - (y^2 - yx - x^2)^2)$$

Theorem (Jones 1975)

$P(x,y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

Proof

$$2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x = x(2 - (y^2 - yx - x^2)^2)$$

Remark

$P(2,2) = -28$

Theorem (Jones 1975)

$P(x, y) = 2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x$ generates set of Fibonacci numbers

Proof

$2x + 2y^3x^2 + y^2x^3 - 2yx^4 - x^5 - y^4x = x(2 - (y^2 - yx - x^2)^2)$

Remark

$P(2, 2) = -28$

Theorem

there exists no polynomial $Q(x_1, \ldots, x_n)$ such that

$$\{Q(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \geqslant 0\}$$

is set of all Fibonacci numbers

Outline

1. Summary of Previous Lecture
2. Recursive and Recursive Enumerable Sets
3. Diophantine Sets
4. Fibonacci Numbers
5. **Summary**

Important Concepts

- diophantine set
- Fibonacci numbers
- index set
- recursive set
- recursive enumerable set
- recursive separable sets

Important Concepts

- diophantine set
- Fibonacci numbers
- index set
- recursive set
- recursive enumerable set
- recursive separable sets

homework for November 30