

Undecidability in Logic -Part I

K. Subramani¹

¹Lane Department of Computer Science and Electrical Engineering
West Virginia University

Number Theory and Computation

Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - Sample Proof
 - Complete fragments of number theory

- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - Sample Proof
 - Complete fragments of number theory

- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - Sample Proof
 - Complete fragments of number theory
- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[(\text{mod}(x, y, z) \wedge \text{mod}(x, y, z')) \rightarrow (z = z')].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b).$

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b)$).

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((\text{mod } (x, y, z) \wedge \text{mod } (x, y, z')) \rightarrow (z = z'))].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b)$).

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[(\text{mod}(x, y, z) \wedge \text{mod}(x, y, z')) \rightarrow (z = z')].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b)$).

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[((x \bmod y = z) \wedge (x \bmod y = z')) \rightarrow (z = z')].$

A set of Axioms

Non-logical Axioms

NT1 $(\forall x)(\sigma(x) \neq 0).$

NT2 $(\forall x)(\forall y)[(\sigma(x) = \sigma(y)) \rightarrow (x = y)].$

NT3 $(\forall x)((x = 0) \vee (\exists y)(x = \sigma(y))).$

NT4 $(\forall x)(x + 0 = x).$

NT5 $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y)).$

NT6 $(\forall x)(x \times 0 = 0).$

NT7 $(\forall x)(\forall y)((x \times \sigma(y)) = (x \times y + x)).$

NT8 $(\forall x)(x \uparrow 0) = \sigma(0).$

NT9 $(\forall x)((x \uparrow \sigma(y)) = (x \uparrow y) \times x).$

NT10 $(\forall x)(x < \sigma(x)).$

NT11 $(\forall x)(\forall y)((x < y) \rightarrow (\sigma(x) \leq y)).$ ($a \leq b$ is an abbreviation for $(a < b) \vee (a = b)$).

NT12 $(\forall x)(\forall y)((\neg(x < y)) \leftrightarrow (y \leq x)).$

NT13 $(\forall x)(\forall y)(\forall z)[((x < y) \wedge (y < z)) \rightarrow (x < z)].$

NT14 $(\forall x)(\forall y)(\forall z)(\forall z')[(\text{mod}(x, y, z) \wedge \text{mod}(x, y, z')) \rightarrow (z = z')].$

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is both sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? **Apparently not!** For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$. In fact, no system of axioms exists for $\mathbf{N}$, that is **both** sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? **Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$.** In fact, no system of axioms exists for $\mathbf{N}$, that is **both** sound and complete.

A set of Axioms (contd.)

Notational convenience

- (i) $\text{mod}(x, y, z)$ is an abbreviation for $(\exists w)((x = y \times w + z) \wedge (z < y))$.
- (ii) $\text{div}(x, y, w)$ is an abbreviation for $(\exists z)((x = y \times w + z) \wedge (z < y))$.
- (iii) $\mathbf{NT} = \mathbf{NT}_1 \wedge \mathbf{NT}_2 \wedge \dots \mathbf{NT}_{14}$
- (iv) We use 1 for $\sigma(0)$, 2 for $\sigma(\sigma(0))$, 3 for $\sigma(\sigma(\sigma(0)))$ and so on.

Properties of Axiom set

- (i) Is it sound? Yes! If $\mathbf{NT} \vdash \phi$, then $\mathbf{N} \models \phi$. Use induction on the number of steps in the proof sequence of $\mathbf{NT} \vdash \phi$.
- (ii) Is it complete? i.e., if $\mathbf{N} \models \phi$, does $\mathbf{NT} \vdash \phi$? **Apparently not! For instance, there is no proof from $\mathbf{NT}$ of the valid sentence $(\forall x)(\forall y)[(x + y) = (y + x)]$.** In fact, no system of axioms exists for $\mathbf{N}$, that is **both** sound and complete.

Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - **Sample Proof**
 - Complete fragments of number theory
- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

Sample Proof

Example

Show that $\mathbf{NT} \vdash 1 < 1 + 1$.

Proof.

Consider the following proof sequence:

- (i) $(\forall x)(\forall y)((x + \sigma(y)) = \sigma(x + y))$, **NT5**.
- (ii) $(\forall x)((x + \sigma(0)) = \sigma(x + 0))$, (i), u.i. (setting $y = 0$).
- (iii) $(\forall x)((x + 1) = \sigma(x))$, **NT4**.
- (iv) $(\forall x)(\sigma(x) = x + 1)$, properties of equality.
- (v) $(\forall x)(x < \sigma(x))$, **NT10**.
- (vi) $1 < \sigma(1)$, (v), u.i. (setting $x = 1$).
- (vii) $\sigma(1) = 1 + 1$, (iv), u.i. (setting $x = 1$).
- (viii) $1 < 1 + 1$, (vi), (vii).



Outline

1 Axiomatizing Number Theory

- Non-logical Axioms
- Sample Proof
- Complete fragments of number theory

2 Complexity as a number-theoretic concept

- Representing Turing Machines as numbers
- Encoding sample

Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Variable-Free Sentences

Theorem

If ϕ is a variable-free sentence, then $\mathbf{N} \models \phi \Leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Any variable-free sentence is an arbitrary boolean combination of expressions of the form: $t = t'$ and $t < t'$.

- (i) t and t' are numbers - $t = t'$ is trivial to prove. $t < t'$ can be proved by using **NT10** to prove $t < \sigma(t)$, $\sigma(t) < \sigma(\sigma(t))$ and so on. Eventually, we can use **NT13** to establish the inequality.
- (ii) t and t' are general variable-free terms (e.g., $t = 2 \uparrow 3 + (4 \times 7) + 6$) - Both t and t' have values, say t_0 and t'_0 . We need to show that $\mathbf{NT} \vdash t = t_0$ and $\mathbf{NT} \vdash t' = t'_0$. Use induction on structure of t , by repeatedly applying the axioms **NT9**, **NT7** and **NT5**. Ultimately, the expression will be reduced to its value.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j]$, $0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots (x = n - 1) \rightarrow \psi)$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number.

Repeatedly apply **NT10** and **NT11** to conclude that

$\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction

$\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots \vee (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j], 0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \dots (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j]$, $0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Bounded Quantifiers

Notation

- (i) $(\forall x < t)\phi$ stands for $(\forall x)((x < t) \rightarrow \phi)$. Bounded prenex form.
- (ii) Bounded sentence.

Theorem

Suppose that ϕ is a bounded sentence. Then $\mathbf{N} \models \phi \leftrightarrow \mathbf{NT} \vdash \phi$.

Proof.

Since $\mathbf{NT}$ is sound, $\mathbf{NT} \vdash \phi \rightarrow \mathbf{N} \models \phi$. We use induction on the number of quantifiers to prove the converse.

- (i) ϕ has no quantifiers - Variable-Free sentence!
- (ii) $\phi = (\exists x)\psi$ - Since $\mathbf{N} \models \phi$, there is a specific integer n , such that $\mathbf{N} \models \psi[x \leftarrow n]$. By induction, $\mathbf{NT} \vdash \psi[x \leftarrow n]$ and hence $\mathbf{NT} \vdash \phi$.
- (iii) $\phi = (\forall x < t)\psi$ - Observe that t must be a variable-free term and hence a number. Repeatedly apply **NT10** and **NT11** to conclude that $\mathbf{NT} \vdash (\forall x)((x < n) \rightarrow ((x = 0) \vee (x = 1) \vee (x = 2) \vee \dots \vee (x = n - 1)))$. By induction $\mathbf{NT} \vdash \psi[x \leftarrow j]$, $0 \leq j < n$. Hence $\mathbf{NT} \vdash (\forall x)((x = 0) \vee (x = 1) \vee \dots \vee (x = n - 1)) \rightarrow \psi$. It follows that $\mathbf{NT} \vdash \phi = (\forall x < n)\psi$.



Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - Sample Proof
 - Complete fragments of number theory
- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{|\Sigma|, |\Sigma|+1, \dots, |\Sigma| + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) "yes" and "no" are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration

$C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{|\Sigma|, |\Sigma| + 1, \dots, |\Sigma| + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) "yes" and "no" are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration

$C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{\Sigma, \Sigma+1, \dots, \Sigma + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) "yes" and "no" are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration $C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{\Sigma, \Sigma+1, \dots, \Sigma + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) “yes” and “no” are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration $C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{\Sigma, \Sigma+1, \dots, \Sigma + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) “yes” and “no” are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration $C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Encoding Scheme

Procedure

Let $M = (K, \Sigma, \delta, s)$ denote a Turing Machine.

- (i) Represent the symbols in Σ using integers in $\{0, 1, \dots, |\Sigma| - 1\}$ and the symbols in K using integers in $\{\Sigma, \Sigma+1, \dots, \Sigma + |K| - 1\}$.
- (ii) s is always encoded as $|\Sigma|$ and 0 is always used to encode $\triangleright$.
- (iii) “yes” and “no” are encoded as $|\Sigma| + 1$ and $|\Sigma| + 2$ respectively.
- (iv) $\sqcup$ is encoded by 1.

Thus, all symbols can be encoded using $b = |\Sigma| + |K|$ integers. Consider the configuration $C = (q, w, u)$, where $q \in K$ and $w = w_1, w_2, \dots, w_m$ and $u = u_1, u_2, \dots, u_n \in \Sigma^*$. C can be thought of as the unique integer whose b -ary representation is

$$\sum_{i=1}^n w_i \cdot b^{m+n+1-i} + q \cdot b^n + \sum_{i=1}^n u_i \cdot b^{n-i}.$$

Outline

- 1 Axiomatizing Number Theory
 - Non-logical Axioms
 - Sample Proof
 - Complete fragments of number theory
- 2 Complexity as a number-theoretic concept
 - Representing Turing Machines as numbers
 - Encoding sample

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$\mathbf{N}_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$\mathbf{N}_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$\mathbf{N}_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$\mathbf{N}_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$N_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.

Example

$p \in K,$	$\sigma \in \Sigma$	$\delta(p, \sigma)$
s	a	$(s, a, \rightarrow)$
s	b	$(s, b, \rightarrow)$
s	$\sqcup$	$(q, \sqcup, \leftarrow)$
s	$\triangleright$	$(q, \triangleright, \rightarrow)$
q	a	$(q, \sqcup, \leftarrow)$
q	b	$(\text{"no"}, b, -)$
q	$\triangleright$	$(\text{"yes"}, \triangleright, \rightarrow)$

Table: A Turing Machine that accepts a^*

Characteristics

$|K| = |\Sigma| = 4$ and hence $b = 8$.

The configuration $(q, \triangleright aa, \sqcup \sqcup)$ is represented by the sequence $(0, 2, 2, 7, 1, 1)$ or by the integer 022711_8 or 9673_{10} .

Observation

The relation "yields in one step" over the configurations of M defines a relation $Y_M \subseteq \mathcal{N}^2$.

Goal

To formulate a first-order expression $yields_M(x, y)$ in number theory, over the free variables x and y , such that

$\mathbf{N}_{x=m, y=n} \models yields_M(x, y)$ iff $Y_M(m, n)$.