Kurt Gödel: úplnost a neúplnost

Vítězslav Švejdar

Karlova Univerzita v Praze, http://www.cuni.cz/~svejdar/

Hvězdárna a planetárium Brno, 9. března 2017

Obsah

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).
- Maturoval 1924 a odešel studovat do Vídně.

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).
- Maturoval 1924 a odešel studovat do Vídně.
- Volba rakouského občanství v roce 1929.

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).
- Maturoval 1924 a odešel studovat do Vídně.
- Volba rakouského občanství v roce 1929.
- Sňatek v září 1938.

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).
- Maturoval 1924 a odešel studovat do Vídně.
- Volba rakouského občanství v roce 1929.
- Sňatek v září 1938.
- Od roku 1934 několik pobytů v USA (Institute for Advanced Study, University of Notre Dame), naposledy v zimě 38–39.

Kurt Gödel: několik životopisných údajů

- Narozen 1906 (Wikipedia: Brün, Austria-Hungary).
- Maturoval 1924 a odešel studovat do Vídně.
- Volba rakouského občanství v roce 1929.
- Sňatek v září 1938.
- Od roku 1934 několik pobytů v USA (Institute for Advanced Study, University of Notre Dame), naposledy v zimě 38–39.
- Od března 1940, po dobrodružné cestě přes Sibiř, natrvalo v USA.

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení

pokud vyhraji, koupím si auto nebo pojedu do Chile

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení

pokud vyhraji, koupím si auto nebo pojedu do Chile

je $v \rightarrow (a \vee c)$.

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení
pokud vyhraji, koupím si auto nebo pojedu do Chile
je $v \rightarrow (a \vee c)$. Symboly $\vee$, $\rightarrow$, $\&$, $\neg$ jsou *logické spojky*.

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení
pokud vyhraji, koupím si auto nebo pojedu do Chile
je $v \rightarrow (a \vee c)$. Symboly $\vee$, $\rightarrow$, $\&$, $\neg$ jsou *logické spojky*.

Papadimitriou v [Pap94]:
everybody loves my baby,
my baby loves nobody but me:
$\forall x L(x, B) \ \& \ \forall y (L(B, y) \rightarrow y = M)$.

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení
pokud vyhraji, koupím si auto nebo pojedu do Chile
je $v \rightarrow (a \vee c)$. Symboly $\vee$, $\rightarrow$, $\&$, $\neg$ jsou *logické spojky*.

Papadimitriou v [Pap94]:
everybody loves my baby,
my baby loves nobody but me:
$\forall x L(x, B) \ \& \ \forall y (L(B, y) \rightarrow y = M)$.
Symboly $\forall$ a $\exists$ jsou *kvantifikátory*.

Symbolický zápis tvrzení (vlastností, podmínek)

Logická struktura tvrzení
pokud vyhraji, koupím si auto nebo pojedu do Chile
je $v \rightarrow (a \vee c)$. Symboly $\vee$, $\rightarrow$, $\&$, $\neg$ jsou *logické spojky*.

Papadimitriou v [Pap94]:
everybody loves my baby,
my baby loves nobody but me:
$\forall x L(x, B) \ \& \ \forall y (L(B, y) \rightarrow y = M)$.
Symboly $\forall$ a $\exists$ jsou *kvantifikátory*.

Zápis podmínky číslo x je prvočíslo:
$x \neq 1 \ \& \ \forall v (v \mid x \rightarrow v = 1 \vee v = x)$,
kde $v \neq 1$ je zkratka pro $\neg(v = 1)$, kdežto $v \mid x$ je zkratka pro $\exists u (u \cdot v = x)$ nebo pro $\mathrm{Mod}(x, v) = 0$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y (L(B, y) \rightarrow y = M)$ plyne :

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne :
Když $\forall x L(x, B)$, pak i $L(B, B)$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne :
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$: Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k+67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x,B)$ a $\forall y(L(B,y) \rightarrow y=M)$ plyne $B=M$:
Když $\forall x L(x,B)$, pak i $L(B,B)$. Když $\forall y(L(B,y) \rightarrow y=M)$, pak i $L(B,B) \rightarrow B=M$. Tedy $B=M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a=3i+1$ nebo $a=3i+2$ pro vhodné i.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j. Když $a = 3i + 1$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 3j + 1$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y (L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y (L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b (3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j.
Když $a = 3i + 1$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 3j + 1$.
Když $a = 3i + 2$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 6j + 2$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j.
Když $a = 3i + 1$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 3j + 1$.
Když $a = 3i + 2$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 6j + 2$.
Když $a = 3i + 1$ a $b = 3j + 2$, pak $a \cdot b = 9ij + 6i + 3j + 2$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j.
Když $a = 3i + 1$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 3j + 1$.
Když $a = 3i + 2$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 6j + 2$.
Když $a = 3i + 1$ a $b = 3j + 2$, pak $a \cdot b = 9ij + 6i + 3j + 2$.
Když $a = 3i + 2$ a $b = 3j + 2$, pak $a \cdot b = 9ij + 6i + 6j + 3 + 1$.

Příklady argumentů (důkazů)

Příklad 1 Z předpokladu, že každé číslo tvaru $100k + 67$ je prvočíslo, plyne, že 67 je prvočíslo. Také, že 167, a také 267.

Příklad 2 Z $\forall x L(x, B)$ a $\forall y(L(B, y) \rightarrow y = M)$ plyne $B = M$:
Když $\forall x L(x, B)$, pak i $L(B, B)$. Když $\forall y(L(B, y) \rightarrow y = M)$, pak i $L(B, B) \rightarrow B = M$. Tedy $B = M$.

Příklad 3 $\forall a \forall b(3 \mid a \cdot b \rightarrow (3 \mid a \vee 3 \mid b))$:
Nechť jsou dána a a b taková, že $\neg(3 \mid a)$ a $\neg(3 \mid b)$. Pak a dává zbytek 1 nebo 2 při dělení třemi, čili $a = 3i + 1$ nebo $a = 3i + 2$ pro vhodné i. Analogicky, $b = 3j + 1$ nebo $b = 3j + 2$ pro vhodné j.
Když $a = 3i + 1$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 3j + 1$.
Když $a = 3i + 2$ a $b = 3j + 1$, pak $a \cdot b = 9ij + 3i + 6j + 2$.
Když $a = 3i + 1$ a $b = 3j + 2$, pak $a \cdot b = 9ij + 6i + 3j + 2$.
Když $a = 3i + 2$ a $b = 3j + 2$, pak $a \cdot b = 9ij + 6i + 6j + 3 + 1$.
Ve všech případech $\mathrm{Mod}(a \cdot b, 3) = 1$, čili 3 není dělitel čísla $a \cdot b$.

Analýza logických kroků v důkazech

Analýza logických kroků Ve všech důkazech se opakují stále tytéž logické kroky: specifikace čili konkretizace, modus ponens, rozbor případů (když $B \to A$ i $\neg B \to A$, pak A), generalizace. Logické kroky jsou definovány čistě syntakticky, takže o jejich správném použití může rozhodovat počítač.

Analýza logických kroků v důkazech

Analýza logických kroků Ve všech důkazech se opakují stále tytéž logické kroky: specifikace čili konkretizace, modus ponens, rozbor případů (když $B \to A$ i $\neg B \to A$, pak A), generalizace. Logické kroky jsou definovány čistě syntakticky, takže o jejich správném použití může rozhodovat počítač.

Kalkulus je soubor (soupis) takových kroků; obsahuje logické axiomy a odvozovací pravidla. Kalkuly se dnes uvažují hilbertovské, gentzenovské, ...

Analýza logických kroků v důkazech

Analýza logických kroků Ve všech důkazech se opakují stále tytéž logické kroky: specifikace čili konkretizace, modus ponens, rozbor případů (když $B \to A$ i $\neg B \to A$, pak A), generalizace. Logické kroky jsou definovány čistě syntakticky, takže o jejich správném použití může rozhodovat počítač.

Kalkulus je soubor (soupis) takových kroků; obsahuje logické axiomy a odvozovací pravidla. Kalkuly se dnes uvažují hilbertovské, gentzenovské, . . .
Věta o úplnosti pak tvrdí, že žádná další pravidla ani logické kroky nejsou potřeba: ty které máme, stačí ve všech (!) důkazech.
Kanonická citace: [Göd30].

Analýza logických kroků v důkazech

Analýza logických kroků Ve všech důkazech se opakují stále tytéž logické kroky: specifikace čili konkretizace, modus ponens, rozbor případů (když $B \to A$ i $\neg B \to A$, pak A), generalizace. Logické kroky jsou definovány čistě syntakticky, takže o jejich správném použití může rozhodovat počítač.

Kalkulus je soubor (soupis) takových kroků; obsahuje logické axiomy a odvozovací pravidla. Kalkuly se dnes uvažují hilbertovské, gentzenovské, ...
Věta o úplnosti pak tvrdí, že žádná další pravidla ani logické kroky nejsou potřeba: ty které máme, stačí ve všech (!) důkazech. Kanonická citace: [Göd30].

Algoritmický aspekt Korektnost důkazu lze verifikovat *algoritmem*. Leibniz rozlišoval mezi *ars inveniendi* a *ars iudicandi*.

Analýza předpokladů použitých v důkazech

Jazyk V Příkladu 3 hraje roli jazyk $\{+, \cdot, 0, 1\}$ obsahující symboly pro sčítání i násobení.

Analýza předpokladů použitých v důkazech

Jazyk V Příkladu 3 hraje roli jazyk $\{+, \cdot, 0, 1\}$ obsahující symboly pro sčítání i násobení.

Matematické předpoklady V tomtéž příkladu je například použita distributivita násobení vůči sčítání, jednoznačnost dělení se zbytkem, ...

Analýza předpokladů použitých v důkazech

Jazyk V Příkladu 3 hraje roli jazyk $\{+, \cdot, 0, 1\}$ obsahující symboly pro sčítání i násobení.

Matematické předpoklady V tomtéž příkladu je například použita distributivita násobení vůči sčítání, jednoznačnost dělení se zbytkem, ...

Axiomatická teorie má jazyk a množinu axiomů. Například *Peanova aritmetika* PA má (může mít) axiomy postulující asociativitu a komutativitu obou operací, distributivitu násobení vůči sčítání atd. Lze ji chápat jako vážný pokus o axiomatizaci struktury přirozených čísel, tj. struktury $\mathbb{N} = \langle \mathrm{N}, +, \cdot, 0, 1 \rangle$.

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg(y < x))$,
$\forall x \forall y (x < y \vee x = y \vee y < x)$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \to x < z)$,
$\forall x \forall y (x < y \to \neg (y < x))$,
$\forall x \forall y (x < y \vee x = y \vee y < x)$,
$\exists x \forall y \neg (y < x)$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,

$\forall x \forall y (x < y \rightarrow \neg(y < x))$,

$\forall x \forall y (x < y \vee x = y \vee y < x)$,

$\exists x \forall y \neg(y < x)$,

$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \;\&\; y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg(y < x))$,
$\forall x \forall y (x < y \vee x = y \vee y < x)$,
$\exists x \forall y \neg(y < x)$,
$\forall x \exists y (x < y \;\&\; \neg \exists v (x < v \;\&\; v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \;\&\; \neg \exists v (z < v \;\&\; v < x)))$.

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg (y < x))$,
$\forall x \forall y (x < y \lor x = y \lor y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:
$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg (y < x))$,
$\forall x \forall y (x < y \vee x = y \vee y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg (y < x))$,
$\forall x \forall y (x < y \vee x = y \vee y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R}, +, 0 \rangle$,

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg (y < x))$,
$\forall x \forall y (x < y \lor x = y \lor y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R}, +, 0 \rangle$, $\mathbb{R} = \langle \mathrm{R}, +, \cdot, 0, 1 \rangle$.

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z (x < y \ \& \ y < z \rightarrow x < z)$,
$\forall x \forall y (x < y \rightarrow \neg (y < x))$,
$\forall x \forall y (x < y \lor x = y \lor y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \rightarrow \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R}, +, 0 \rangle$, $\mathbb{R} = \langle \mathrm{R}, +, \cdot, 0, 1 \rangle$.

Čím je struktura $\mathbb{N} = \langle \mathrm{N}, +, \cdot, 0, 1 \rangle$ jiná?

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:

$\forall x \forall y \forall z(x < y \;\&\; y < z \rightarrow x < z)$,
$\forall x \forall y(x < y \rightarrow \neg(y < x))$,
$\forall x \forall y(x < y \vee x = y \vee y < x)$,
$\exists x \forall y \neg(y < x)$,
$\forall x \exists y(x < y \;\&\; \neg \exists v(x < v \;\&\; v < y))$,
$\forall x \forall y(y < x \rightarrow \exists z(z < x \;\&\; \neg \exists v(z < v \;\&\; v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R}, +, 0 \rangle$, $\mathbb{R} = \langle \mathrm{R}, +, \cdot, 0, 1 \rangle$.

Čím je struktura $\mathbb{N} = \langle \mathrm{N}, +, \cdot, 0, 1 \rangle$ jiná? Může se pro určitou formuli $\varphi(x)$ stát, že všechny instance $\varphi(0)$, $\varphi(1)$, $\varphi(2)$, ... v PA dokazatelné jsou, ale $\forall x \varphi(x)$ není?

Lze určitou strukturu úplně axiomatizovat?

Přirozená čísla pouze s uspořádáním Uvažujme například, co platí ve struktuře $\langle \mathrm{N}, < \rangle$:
$\forall x \forall y \forall z (x < y \ \& \ y < z \to x < z)$,
$\forall x \forall y (x < y \to \neg (y < x))$,
$\forall x \forall y (x < y \lor x = y \lor y < x)$,
$\exists x \forall y \neg (y < x)$,
$\forall x \exists y (x < y \ \& \ \neg \exists v (x < v \ \& \ v < y))$,
$\forall x \forall y (y < x \to \exists z (z < x \ \& \ \neg \exists v (z < v \ \& \ v < x)))$.

Jiné struktury Analogicky to dopadne také se strukturami $\langle \mathrm{N}, +, 0 \rangle$, $\langle \mathrm{R}, < \rangle$, $\langle \mathrm{R}, +, 0 \rangle$, $\mathbb{R} = \langle \mathrm{R}, +, \cdot, 0, 1 \rangle$.

Čím je struktura $\mathbb{N} = \langle \mathrm{N}, +, \cdot, 0, 1 \rangle$ jiná? Může se pro určitou formuli $\varphi(x)$ stát, že všechny instance $\varphi(0)$, $\varphi(1)$, $\varphi(2)$, … v PA dokazatelné jsou, ale $\forall x \varphi(x)$ není? Příklad 3 naznačuje sentenci když x je prvočíslo, pak kdykoliv x dělí součin $a \cdot b$, dělí i a nebo b. Ta tuto vlastnost ale nemá.

Rekurzívní a rekurzívně spočetné množiny

Definice Množina A (přirozených čísel nebo slov v nějaké abecedě) je *rekurzívní*, jestliže existuje algoritmus, který rozhoduje o náležení do A.

Rekurzívní a rekurzívně spočetné množiny

Definice Množina A (přirozených čísel nebo slov v nějaké abecedě) je *rekurzívní*, jestliže existuje algoritmus, který rozhoduje o náležení do A.

Definice Množina A je *rekurzívně spočetná* (*RE*), jestliže existuje procedura (algoritmus, který nevyžaduje žádný vstup), která, je-li spuštěna, postupně vygeneruje všechny prvky množin A.

Rekurzívní a rekurzívně spočetné množiny

Definice Množina A (přirozených čísel nebo slov v nějaké abecedě) je *rekurzívní*, jestliže existuje algoritmus, který rozhoduje o náležení do A.

Definice Množina A je *rekurzívně spočetná* (RE), jestliže existuje procedura (algoritmus, který nevyžaduje žádný vstup), která, je-li spuštěna, postupně vygeneruje všechny prvky množin A.

Definice (alternativní) A je RE, jestliže existuje rekurzívní relace R taková, že $\forall x(x \in A \Leftrightarrow \exists y R(x, y))$.

Rekurzívní a rekurzívně spočetné množiny

Definice Množina A (přirozených čísel nebo slov v nějaké abecedě) je *rekurzívní*, jestliže existuje algoritmus, který rozhoduje o náležení do A.

Definice Množina A je *rekurzívně spočetná* (*RE*), jestliže existuje procedura (algoritmus, který nevyžaduje žádný vstup), která, je-li spuštěna, postupně vygeneruje všechny prvky množin A.

Definice (alternativní) A je *RE*, jestliže existuje rekurzívní relace R taková, že $\forall x(x \in A \Leftrightarrow \exists y R(x, y))$.

Příklad Když T je teorie s rekurzívní množinou axiomů (*rekurzívně axiomatizovatelná* teorie), pak relace $R(x, y)$ definovaná podmínkou $R(x, y) \Leftrightarrow x$ je sentence a y je její důkaz v T je rekurzívní. Množina $\mathrm{Thm}(T)$ všech sentencí dokazatelných v T je *RE*.

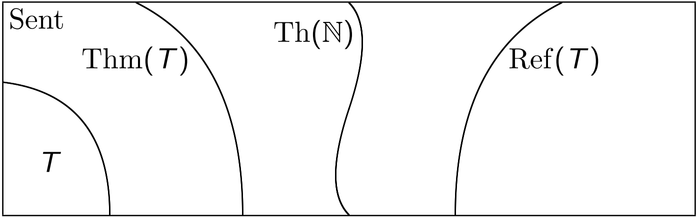
Rekurzívní a *RE* množiny (pokračování)

Platí (a) Každá rekurzívní A je RE, ale opačná inkluze neplatí.
(b) Komplement $-A$ rekurzívní množiny A je opět rekurzívní množina.
(c) Komplement $-A$ množiny A, která je RE, je rekurzívní pouze tehdy, když A je dokonce rekurzívní.

Rekurzívní a *RE* množiny (pokračování)

Platí (a) Každá rekurzívní A je RE, ale opačná inkluze neplatí.
(b) Komplement $-A$ rekurzívní množiny A je opět rekurzívní množina.
(c) Komplement $-A$ množiny A, která je RE, je rekurzívní pouze tehdy, když A je dokonce rekurzívní.

Aplikace v logice



Věty o neúplnosti

Platí (a) Když T je rekurzívně axiomatizovatelná teorie v aritmetickém jazyce, jejíž všechny axiomy platí v $\mathbb{N}$, pak existuje formule $\varphi(x)$ taková, že všechny instance $\varphi(0)$, $\varphi(1)$, $\varphi(2)$, ... jsou v T dokazatelné, ale $\forall x \varphi(x)$ dokazatelná není.

Věty o neúplnosti

Platí (a) Když T je rekurzívně axiomatizovatelná teorie v aritmetickém jazyce, jejíž všechny axiomy platí v $\mathbb{N}$, pak existuje formule $\varphi(x)$ taková, že všechny instance $\varphi(0)$, $\varphi(1)$, $\varphi(2)$, ... jsou v T dokazatelné, ale $\forall x \varphi(x)$ dokazatelná není.
(b) Je-li T navíc rozšíření Peanovy aritmetiky, v T lze formalizovat logickou syntax, a za $\varphi(x)$ pak lze vzít formuli číslo x není důkazem (není numerickým kódem důkazu) sporu v T.

Dodatky

Cvičení Napište v aritmetickém jazyce formuli, která vyjadřuje, že číslo x je mocninou dvojky.

Když p je prvočíslo a $p \mid a \cdot b$, pak $p \mid a$ nebo $p \mid b$

Nechť p není dělitelem čísla a. V tom případě, protože p je prvočíslo, čísla a a p jsou spolu nesoudělná. Dle Bezoutovy věty existují čísla x a y taková, že $ax - py = 1$. Z toho máme $abx - pby = b$. Číslo p je dělitelem jak čísla abx, tak čísla pby. Tedy $p \mid b$.

Literatura

- K. Gödel. Die Vollständigkeit der Axiome des logischen Funktionenkalküls. *Monatsh. Math. Phys.*, 37:349–360, 1930.
- K. Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38:173–198, 1931.
- J. Malina a J. Novotný, editoři. *Kurt Gödel*. Georgetown, Nauma, Brno, 1996.
- C. H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.