DD1350 Logik för dataloger

Fö 8 – Axiomatiseringar

Modeller och bevisbarhet

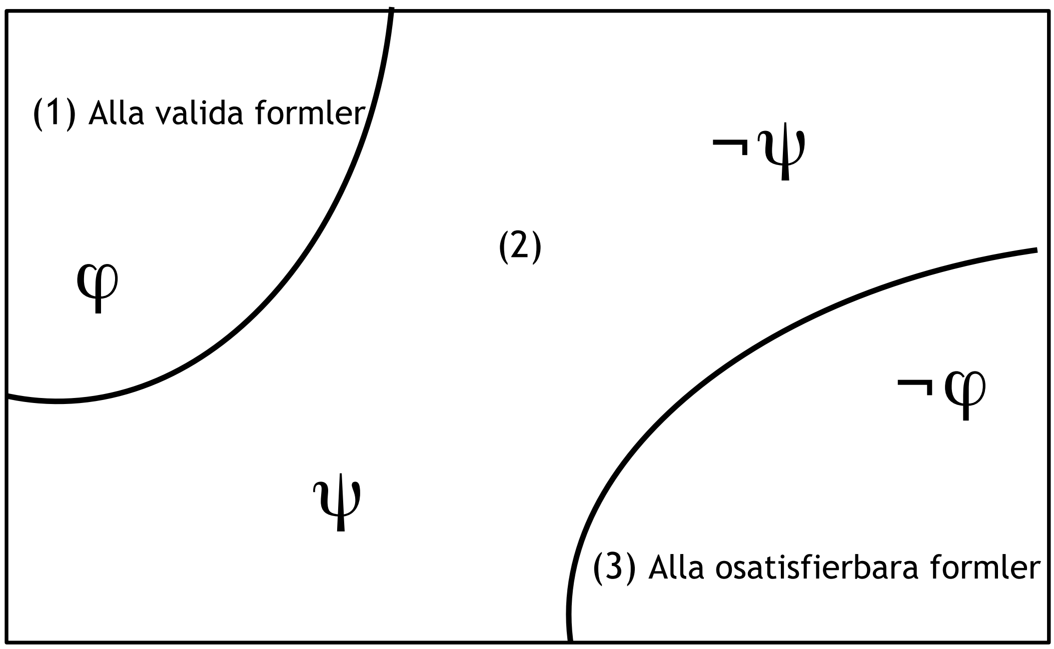
Sedan tidigare vet vi att:

Om en formel Φ är valid (sann i alla modeller) så finns det ett bevis för Φ i naturlig deduktion.

Men antag att vi bara är intresserad av huruvida Φ är sann i en viss modell?

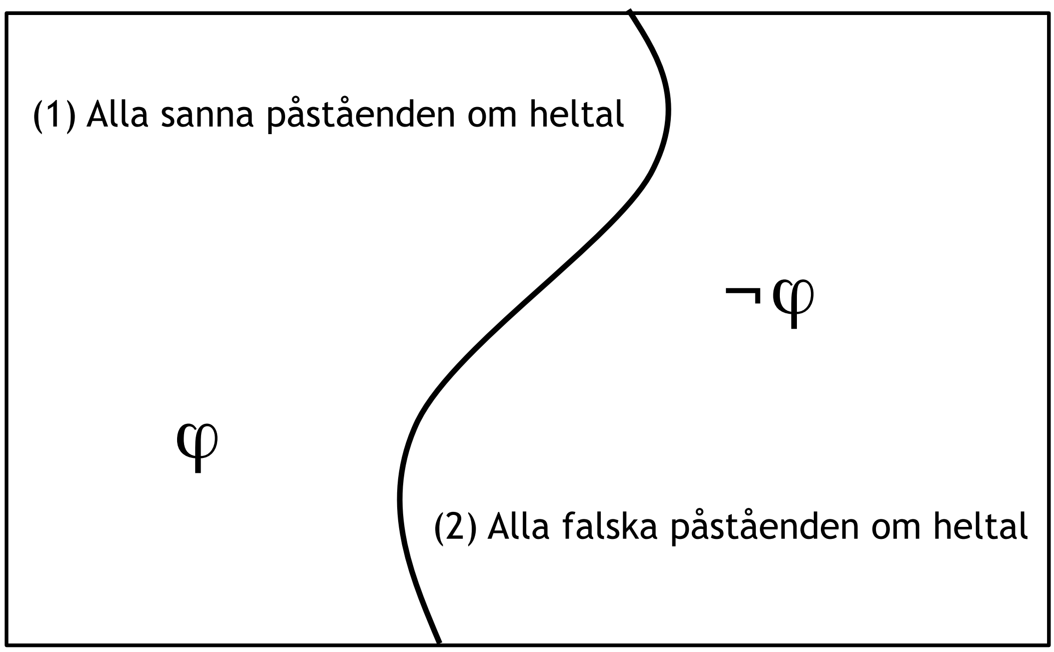
T.ex. en matematiker som vill visa att ett visst påstående är sant om heltalen, och är ointresserad av alla andra modeller?

”Logikerns världsbild”



(1) + (2) + (3) = Alla predikatlogiska formler som finns
(1) + (2) = Alla satisfierbara formler

”Matematikerns världsbild”



Notera: Vi kommer strax att definiera exakt vad vi menar med ”ett påstående om heltal”.

Aritmetiska formler

Vi kommer vara mest intresserade av att prata om addition och multiplikation av heltal. Därför kommer vi anta att våra formler bara innehåller:

- funktionssymbolerna + och •
- siffror
- relationssymbolen =
- logiska symboler (kvantifierare, konnektiv, variabler, parenteser)

<u>T. ex.</u> $\forall x \forall y \forall z(x \cdot (y+z) = (x \cdot y)+(x \cdot z))$

Aritmetikens standardmodell

Aritmetikens standardmodell $\mathcal{ASM}$ har de naturliga talen som universum, och tolkar '+' som addition,
'•' som multiplikation, och sifferstängar som tal.

$$\forall x \forall y \forall z(x \cdot (y+z) = (x \cdot y)+(x \cdot z))$$

Ovanstående formel är alltså sann i $\mathcal{ASM}$.

Axiom och teorier

Ett sätt att specificera en viss modell är att skriva ned en mängd **axiom** för den modell *M* vi vill prata om.

”Axiom” är helt enkelt utsagor som är sanna i *M*.

Givet ett mängd Γ med axiom, så är **teorin för** Γ = mängden av alla formler som kan bevisas från Γ.

T.ex. om Γ innehåller

$$\forall x \forall y \forall z(x\cdot(y+z) = (x\cdot y)+(x\cdot z))$$

så finns t.ex. följande formler i teorin för Γ:

$$1\cdot(2+3) = (1\cdot 2)+(1\cdot 3))$$

$$\forall x \, (x\cdot(12+14) = (x\cdot 12)+(x\cdot 14))$$

Axiomatisering

Vad vi vill göra är att skriva ned axiom Γ för + och • som vi kan använda som premisser närhelst vi vill bevisa något om heltal.

Om axiomen i Γ är sanna i ASM, så är allt som kan bevisas från Γ också sant i ASM (pga sundheten hos naturlig deduktion).

Helst vill vi uppnå följande:

- **ingen redundans**: inget axiom i Γ kan härledas från de övriga
- **negations-fullständighet**: för varje formel Φ gäller att $\Gamma \vdash \Phi$ eller $\Gamma \vdash \neg\Phi$.

Peanos axiom

Guiseppe Peano föreslog 1889 följande axiom för $\mathbb{N}$:

a. 0 är ett naturligt tal
b. Om x är ett naturligt tal så är x+1 ett naturligt tal

1. 0 är inte x+1 för något x
2. För alla x,y: Om x+1=y+1 så x=y.
3. För varje egenskap P, om P(0) är sann, och om P(n) implicerar P(n+1), så är P(x) sann för alla x. (**induktionsprincipen**)

Efterföljar-funktionen

Eftersom Peanos axiom inte använder generell addition utan bara ”+1”, kan vi använda **efterföljar-funktionen** $s(x)$ (dvs $s(x) = x+1$).

1. $\forall x\ (\neg(\ 0 = s(x)))$
2. $\forall x\ \forall y\ (s(x)=s(y) \rightarrow x=y)$
3. Kan skrivas som en bevisregel:

$$\dfrac{\Phi[0/x] \quad \boxed{\begin{array}{ll} x_0 & \Phi[x_0/x] \\ & \dots \\ & \Phi[s(x_0)/x] \end{array}}}{\forall x\ \Phi}$$

Addition

Om vi lägger till + och 1 så kan vi ta bort s:

1. $\forall x\ (\neg(0 = x+1))$
2. $\forall x\ \forall y\ (x+1=y+1 \ \rightarrow x=y)$
3. $(\Phi[0/x]\ /\backslash\ \forall x_0\ (\Phi[x_0/x] \rightarrow \Phi[x_0+1/x])) \rightarrow \forall x\ \Phi$
4. $\forall x\ (\ x+0 = x\ )$
5. $\forall x\ \forall y\ (\ x+(y+1) = (x+y)+1\ )$

Detta är axiomen i sk **Presburger-aritmetik.**

Presburger-aritmetik

Presburger-aritmetik är en **negations-fullständig teori**,

dvs om Φ är en formel vi kan konstruera med +, siffror och logiska symboler,

och om *Presburger* är axiomen 1-5 på föregående bild, så gäller att:

$$\textit{Presburger} \vdash \Phi \text{ eller } \textit{Presburger} \vdash \neg\Phi$$

Detta visade Mojżesz Presburger år 1929.

Avgörbarhet

Alla negations-fullständiga teorier är **avgörbara**.

Vi kan helt enkelt leta efter ett bevis för Φ och ett bevis för $\neg\Phi$ parallellt.

Om teorin är negations-fullständig kommer vi hitta det ena eller det andra i ändlig tid.

Multiplikation

Vi behöver också lägga till axiom för multiplikation:

1. $\forall x\ (\neg(0 = x+1))$
2. $\forall x\ \forall y\ (x+1=y+1 \ \rightarrow x=y)$
3. $(\Phi[0/x] \ /\backslash\ \forall x_0\ (\Phi[x_0/x] \rightarrow \Phi[x_0+1/x])) \rightarrow \forall x\ \Phi$
4. $\forall x\ (\ x+0 = x\ )$
5. $\forall x\ \forall y\ (\ x+(y+1) = (x+y)+1\ )$
6. $\forall x\ (\ x \cdot 1 = x\ )$
7. $\forall x\ \forall y\ (\ x \cdot (y+1) = (x \cdot y)+x\ )$

Detta är axiomen i sk **Peano-aritmetik**.

Peano-aritmetik

Underligt nog är Peano-aritmetik allt vi behöver för att kunna uttrycka alla beräkningsbara funktioner.

dvs om det finns ett datorprogram som implementerar $f : \mathrm{N} \rightarrow \mathrm{N}$, och

om *Peano* är axiom 1-7 på föregående bild,

så finns det en formel Φ med två fria variabler *x*, *y* sådan att

$f(m)=n$ om och endast om $Peano \vdash \Phi[m/x][n/y]$.

Gödels ofullständighetssats

Kurt Gödel visade 1931 att Peano-aritmetik **inte** är negationsfullständigt.

Mer specifikt lyckades han konstruera en formel *G* som man kan inse är **sann,** men sådan att $Peano \nvdash G$ och $Peano \nvdash \neg G$.

Beviset är gjort så att för **varje tänkbar uppsättning axiom** för heltalen kan vi konstruera en sådan formel *G*. Alltså **går det inte att axiomatisera aritmetiken.**

Detta är **Gödels** berömda **första ofullständighetssats.**

Gödels bevis på 2 bilder (1)

Insikt 1: Formler och bevis kan kodas som tal.

Insikt 2: Eftersom Peano-aritmetik kan representera alla beräkningsbara funktioner, och beviskontroll är beräkningsbart, så finns det en aritmetisk formel $Prf(x,y)$ som är sann exakt när y (kodat som ett tal) är ett bevis för x (kodat som ett tal).

(x är ett mycket stort tal, y är ännu mycket större.)

Formeln $\neg\exists y(\ Prf(n,y))$ uttrycker då att ”det finns inget bevis för formeln med koden n”.

Gödels bevis på 2 bilder (2)

Formeln $\neg\exists y(\ Prf(n,y))$ uttrycker att ”det finns inget bevis för formeln med koden n”.

Gödel lyckades nu konstruera en formel G med kod m och som han kunde bevisa var ekvivalent med $\neg\exists y(\ Prf(m,y))$. Det betyder att G säger ”jag är inte bevisbar”.

Om nu G är falsk, så är det också falskt att G inte är bevisbar, dvs vi kan bevisa något falskt utifrån våra axiom. Då måste axiomen vara falska eller innehålla en motsägelse, men vi vet att axiomen är sanna i ASM.

Alltså är G sann men inte bevisbar. Underbart!

Mängdlära och ZF-axiomen

Ännu har man inte funnit någon sann men icke bevisbar formel som uttrycker något ”naturligt” samband mellan naturliga tal.

Annat är det i mängdläran, där flera viktiga utsagor har visat sig vara oberoende av de sk **Zermelo-Fraenkel-axiomen.**

T.ex. både **kontinuumhypotesen** (se Fö 6) och dess negation är bägge konsistenta med axiomen.