Hilbertsystemet (del 1)

- Axiomscheman och bevisregler
- Bevissystem i allmänt
- Hilbertsystemet

Ett (trivialt) exempel

Formella logiska bevis består normalt av en linjär följd av formler, där varje formel är en hypotes, ett axiom eller kan härledas av tidigare formler enligt bevissystemets regler.

Exempel: Vi vill visa att $\{A, A \to B, B \to C\} \models C$. Formlerna A, $A \to B$ och $B \to C$ är hypoteserna och vi vill komma fram till C. I bevissystemet som ska diskuteras här (nedan kallat Hilbertsystemet) ser beviset ungefär ut så här:

1.	A	(hypotes)
2.	$A \to B$	(hypotes)
3.	B	(fås av 1 och 2)
4.	$B \to C$	(hypotes)
5.	C	(fås av 3 och 4)

Ingredienser: Axiomscheman och bevisregler

- Axiomscheman är "mallar" för formler som innehåller platshållare. En platshållare står för en godtycklig wff. Ett exempel är

  $$\alpha_1 \to (\alpha_2 \to \alpha_1).$$

  Om förekomsterna av α_1 och α_2 ersätts med två godtyckliga wff:er fås ett axiom. Antalet axiom som schemat beskriver brukar alltså vara oändligt.

- Bevisregler skrivs vanligen som i det här exemplet, en berömd bevisregel:

  $$\frac{\alpha_1, \alpha_1 \to \alpha_2}{\alpha_2} \qquad \text{(modus ponens, MP).}$$

  MP användes i första exemplet. Regeln säger att om instanser av alla formler över strecket (premisserna) redan har härletts så får också motsvarande instans av formeln under strecket (konsekvensen) härledas. (Axiomscheman är egentligen ett specialfall där antalet formler över strecket är 0, vilket innebär att konsekvensen alltid får härledas.)

Uppgift 1

Om ett axiomschema innehåller mallen $(\alpha_1 \to (\alpha_2 \to \alpha_1))$, vilka av följande formler är då axiom?

$\varphi_1 = (A \to (B \to A))$

$\varphi_2 = ((A \to A) \to (A \to (A \to A)))$

$\varphi_3 = (A \to (A \to A))$

$\varphi_4 = (A \to (B \to (C \vee D)))$

Lösning 1

Formlerna φ_1, φ_2 och φ_3 är axiom (α_1 och α_2 kan bytas mot samma formel), men i φ_4 har skilda förekomster av α_1 ersatts med olika formler och det är inte tillåtet.

Uppgift 2

Vilka av följande resonemang är acceptabla tillämpningar av modus ponens?

$$\frac{\alpha_1, \alpha_1 \to \alpha_2}{\alpha_2}$$

1. A	(hypotes)	1. A	(hypotes)
2. $A \to B$	(hypotes)	2. $B \to C$	(hypotes)
3. B	(MP)	3. C	(MP)

Lösning 2

Det första resonmanget är korrekt, men i det andra stämmer inte premisserna överens; åter igen har skilda förekomster av α_1 ersatts med olika formler.

Bevissystem och bevis

Definition Ett bevissystem är ett par $\Gamma = (\mathbf{S}, \mathbf{R})$ bestående av ändliga mängder **S** och **R** av axiomscheman och bevisregler.

Ett bevis i Γ för en wff φ utifrån en mängd Φ av wff:er är en sekvens $\varphi_1, \ldots, \varphi_n$ av wff:er sådana att

- varje φ_i är
  - ett element i Φ,
  - en instans av ett axiomschema i **S** eller
  - konsekvensen av en instans av en regel i **R**, där varje premiss finns bland $\varphi_1, \ldots, \varphi_{i-1}$

  och
- $\varphi_n = \varphi$.

Notationen $\Phi \vdash_\Gamma \varphi$ uttrycker att det finns ett bevis av φ från Φ i Γ.

Ett bevisssystem av den klassiska Hilberttypen

Hilbertsystemet **H** har fått sitt namn efter David Hilbert, en av de mest framstående matematikerna i slutet av 1800- och början av 1900-talet, som kring 1920 initierade ett stort forskningsprogram vars mål var att fullständigt formalisera matematiken mha predikatlogik.

Systemet **H** är gjort för satslogiken med konnektiven $\neg$ och $\rightarrow$. Det består av axiomschemana

$$
\begin{aligned}
Ax_1 &= \alpha_1 \rightarrow (\alpha_2 \rightarrow \alpha_1) \\
Ax_2 &= (\alpha_1 \rightarrow (\alpha_2 \rightarrow \alpha_3)) \rightarrow ((\alpha_1 \rightarrow \alpha_2) \rightarrow (\alpha_1 \rightarrow \alpha_3)) \\
Ax_3 &= (\neg\alpha_1 \rightarrow \neg\alpha_2) \rightarrow (\alpha_2 \rightarrow \alpha_1)
\end{aligned}
$$

samt en enda bevisregel, nämligen modus ponens:

$$\frac{\alpha_1, \alpha_1 \rightarrow \alpha_2}{\alpha_2}$$

Ett enkelt formellt bevis

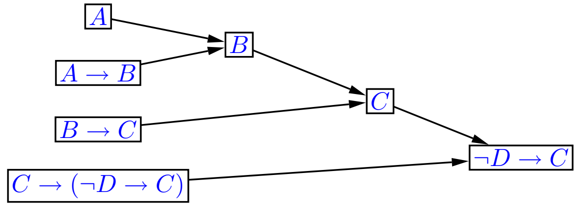
Vi vill visa att $\{A, A \rightarrow B, B \rightarrow C\} \models \neg D \rightarrow C$.

1.	A	(hypotes)
2.	$A \rightarrow B$	(hypotes)
3.	B	(modus ponens på 1 och 2)
4.	$B \rightarrow C$	(hypotes)
5.	C	(modus ponens på 3 och 4)
6.	$C \rightarrow (\neg D \rightarrow C)$	($Ax_1 = \alpha_1 \rightarrow (\alpha_2 \rightarrow \alpha_1)$ med $\alpha_1 = C$ och $\alpha_2 = \neg D$)
7.	$\neg D \rightarrow C$	(modus ponens på 5 och 6)

Observera att formlerna skulle också kunna härledas i en annan ordning. Man skulle t ex kunna börja med 6, 4, 2, 1 istället.

En grafisk representation av bevis

Beviset kan representeras som en dag – en riktad acyklisk graf (*directed acyclic graph*). Representationen är fördelaktig eftersom den gör beroendeförhållandena tydliga:



Varje linjärisering av grafen (dvs varje linjärt arrangemang av noderna som gör att kanterna pekar framåt) ger ett korrekt bevis.