Hilbertsystemet (del 2)

- Metateorem i Hilbertsystemet
- Egenskaper av bevissystem
- Algoritmiska anmärkningar

Metateorem som förkortar bevis

- Betrakta ett bevissystem Γ (t ex Hilbertsystemet **H**) samt en mängd $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ av formelscheman och ett formelschema φ.
  Om det finns ett bevis $\Phi \vdash_\Gamma \varphi$ (där bevis av formelscheman är definierade på samma sätt som om det handlar om konkreta formler) så är varje konkret instans av beviset ett korrekt bevis.
- $\Phi \vdash_\Gamma \varphi$ är då ett metateorem som kan användas i senare bevis för att förkorta dem. Med andra ord, i bevis får man använda bevisregeln

$$\frac{\varphi_1, \ldots, \varphi_n}{\varphi}$$

- För att inse att den är korrekt, observera att man istället för den nya regelns tillämpning skulle kunna klistra in motsvarande konkret instans av beviset för $\Phi \vdash_\Gamma \varphi$.

Exempel 1: Bevis av ett metateorem

Vi vill bevisa metateorem 1: $\{\alpha_1 \to \alpha_2, \alpha_2 \to \alpha_3\} \vdash_{\mathbf{H}} \alpha_1 \to \alpha_3$.

Beviset går så här (där delformlerna som ersätter axiomschemanas platshållare är understrukna):

1.	$\alpha_2 \to \alpha_3$	(hypotes 2)
2.	$\underline{(\alpha_2 \to \alpha_3)} \to (\underline{\alpha_1} \to \underline{(\alpha_2 \to \alpha_3)})$	(Ax_1)
3.	$\alpha_1 \to (\alpha_2 \to \alpha_3)$	(MP på 1 och 2)
4.	$(\underline{\alpha_1} \to (\underline{\alpha_2} \to \underline{\alpha_3})) \to ((\underline{\alpha_1} \to \underline{\alpha_2}) \to (\underline{\alpha_1} \to \underline{\alpha_3}))$	(Ax_2)
5.	$(\alpha_1 \to \alpha_2) \to (\alpha_1 \to \alpha_3)$	(MP på 3 och 4)
6.	$\alpha_1 \to \alpha_2$	(hypotes 1)
7.	$\alpha_1 \to \alpha_3$	(MP på 6 och 5)

Exempel 2: Bevis av metateorem 2 mha metateorem 1

Metateorem 1 används för att bevisa metateorem 2: $\vdash_{\mathbf{H}} \neg\alpha_1 \to (\alpha_1 \to \alpha_2)$.

Beviset är ganska kort:

1.	$\underline{\neg\alpha_1} \to (\underline{\neg\alpha_2} \to \underline{\neg\alpha_1})$	(Ax_1)
2.	$(\underline{\neg\alpha_2} \to \underline{\neg\alpha_1}) \to (\underline{\alpha_1} \to \underline{\alpha_2})$	(Ax_3)
3.	$\neg\alpha_1 \to (\alpha_1 \to \alpha_2)$	(metateorem 1 på 1 och 2)

Om vi istället för rad 3 klistrar in motsvarande instans av beviset för metateorem 1 (där vi hänvisar till rad 1 och 2 istället för hypotes 1 och 2) får vi ett (längre) bevis utan metateorem.

Deduktionsteoremet

Deduktionsteoremet är en annan typ av metateorem. Det lyder så här:

$$\boxed{\Phi \cup \{\varphi\} \vdash_{\mathbf{H}} \varphi' \quad \text{om och endast om} \quad \Phi \vdash_{\mathbf{H}} \varphi \to \varphi'}$$

(där Φ är en ändlig mängd av wff:er och φ, φ' är wff:er). Teoremet kan bevisas via induktion över härledningens längd.

Intuitivt säger deduktionsteoremet att man, under vilka hypoteser Φ som helst, kan bevisa $\varphi \to \varphi'$ genom att betrakta φ som ytterligare en hypotes och sedan bevisa φ'.

Egenskaper av bevissystem

Låt Γ vara ett bevissystem.

Sundhet: Γ är sunt (*sound*) om $\vdash_\Gamma \varphi$ implicerar $\models \varphi$ för alla wff:er φ.

Med andra ord, bevissystemets bevis är pålitliga: $\vdash_\Gamma \varphi$ visar att φ är en tautologi. Bevissystem som inte är sunda är meningslösa.

Fullständighet: Γ är fullständigt (*complete*) om $\models \varphi$ implicerar $\vdash_\Gamma \varphi$ för alla wff:er φ.

Med andra ord, alla tautologier kan bevisas. Fullständighet är självklart önskvärd men inte lika viktig som sundhet. Ibland avstår man från fullständighet för att öka effektiviteten och ibland är det inte ens möjligt att skapa ett sunt bevissystem som både är sunt och fullständigt.

Bevissystemet **H** är både sunt och fullständigt.

Uppgift 1

Om **S** är ett satslogiskt bevissystem och det gäller att

$$\vdash_{\mathbf{S}} A$$

där A är en atom, är det då rimligt att tro att **S** är sunt?

Lösning 1

Om **S** är sunt så skulle

$$\vdash_{\mathbf{S}} A$$

innebära att

$$\models A \ ,$$

med andra ord att varje tolkning är en modell av A. Å andra sidan vet vi att det finns minst en tolkning v för vilken $v(A) = 0$, så vi kan dra slutsatsen att **S** inte är sunt.

Algoritmiska anmärkningar (1)

- En logik **L** är avgörbar om dess deduktionsproblem är avgörbart. Deduktionsproblemet frågar om $\models \varphi$ gäller (där $\varphi \in \mathrm{WF}(\mathbf{L})$).
- Satslogiken (dvs varje satslogik) är avgörbar. Är logiken i fråga ändlig så kan $\models \varphi$ avgöras genom att räkna ut $\overline{v}(\varphi)$ för varje tolkning v. Om logiken inte är ändlig kan φ trots allt endast innehålla ett ändligt antal atomer, vilket medför att man kan begränsa sig till dem.
- Algoritmen är väldigt ineffektiv. Från datavetenskapens synpunkt är en av de viktigaste anledningarna för att använda sig av bevissystem att man vill ha effektivare metoder för att lösa deduktionsproblemet.
- Bevissystemet **H** hjälper inte eftersom det inte innebär någon procedur för att välja rätt axiom. Modus ponens avbildar människans sätt att resonera, vilket medför att **H** kräver intuition och intelligens för att hitta bevis.

Algoritmiska anmärkningar (2)

Är det rimligt att endast betrakta frågan om $\models \varphi$, dvs om φ är en tautologi? Egentligen vill man snarare veta om $\Phi \models \varphi$ gäller, där Φ är en ändlig mängd hypoteser (se blockvärdsexemplet där Φ kan beskriva alla tillåtna världar)!

Låt $\Phi_\wedge$ vara konjunktionen av alla formler i Φ. Det är lätt att visa att följande ekvivalenser gäller

$$\begin{aligned} &\Phi \models \varphi \\ &\Leftrightarrow \Phi_\wedge \wedge \neg\varphi \text{ är osatisfierbar} \\ &\Leftrightarrow \neg(\Phi_\wedge \wedge \neg\varphi) \text{ är en tautologi.} \end{aligned}$$

Dessutom vet vi att $\neg(\Phi_\wedge \wedge \neg\varphi) \equiv \neg\Phi_\wedge \vee \varphi \equiv \Phi_\wedge \to \varphi$. Dvs om vi vill bevisa $\Phi \models \varphi$ kan vi istället bevisa det ekvivalenta påståendet $\models \Phi_\wedge \to \varphi$.
(Observera att det här är en semantisk version av deduktionsteoremet!)