FORMELLE SPROG OG FORMELLE BEVISER.

Anton Jensen
Matematisk Institut
Københavns Universitet

1. Matematiken som deduktiv videnskab par excellence.

Det er almindeligt accepteret at matematik som fag har en særlig karakter, der viser sig ved en speciel deduktiv fremstilling. Denne form stammer helt tilbage fra Euklid og går i princippet ud på at starte med en række alment acceptable og ret simple "sandheder" kaldet aksiomer, og derefter ud fra disse rent logisk udvikle alle matematiske resultater.

Metoden har uomtvisteligt haft stor succes, og den har naturligt nok også været forsøgt anvendt i andre fag. Dog må man vist konstatere, at når man f.eks. i fysik kan give en vellykket deduktiv fremstilling af visse teorier, som f.eks. termodynamik, rationel mekanik, relativitetsteori, etc. så drejer det sig i virkeligheden om matematiske resultater om bestemte matematiske modeller.

At en deduktiv fremstilling er vellykket betyder, at det er lykkedes at samle en mængde interessante og/eller nyttige udsagn på en sådan måde, at de alle kan deduceres fra et enkelt aksiomsystem, som vel at mærke ikke tillader deduktion af forkerte udsagn. Eller man skal måske snarere sige udsagn, der er så forkerte, at de er uanvendelige.

Nuvel, sagen er naturligvis den, at matematikere meget snildt har forstået at få matematik ud af alt hvad der på nogen måde egner sig til deduktiv fremstilling. Det gælder for geometri, hvor f.eks. Pythagoras læresætning oprindeligt var en erfaringssag; for aritmetik, hvor handelsregning var en særdeles konkret og praktisk ting; for mekanik, o.s.v. Det har ofte været en intellektuelt meget krævende proces

at opnå en tilfredsstillende rent matematisk version af disse forskellige discipliner. Et velkendt eksempel giver de reelle tal, som man først fik abstraheret fra den mere konkrete forestillig om punkter på en ret linie for godt hundrede år siden. Men man må vist konstatere, at med mængdeteorien har man et matematisk værktøj, der særdeles smidigt lader sig tilpasse stærkt varierende ønsker om deduktive teorier. (Og har haft så stor succes, at den også mange gange er forsøgt anvendt i situationer, hvor det deduktive eller matematiske indhold er af underordnet betydning).

2. Hvorledes er deduktion mulig ?

Dette gode gamle erkendelsesteoretiske spørgsmål er der i tidernes løb givet mange svar på. Det er f.eks. ikke ualmindeligt at deduktioner opfattes som en slags tankeeksperimenter. Eller som en mystisk fremgravning af latent viden. Vi vælger i det følgende en forklaring, der i hvert fald giver en nyttig angrebsvinkel for de problemer, vi skal beskæftige os med.

Den forklaring vi vælger går simpelt hen ud på, at deduktion er mulig, fordi visse sammensatte udsagn får deres betydning i kraft af, at de tillader visse logiske slutninger.

Det simpleste eksempel er konjunktionen $A \wedge B$ af to udsagn A og B. Her gælder, at har man sagt $A \wedge B$, så har man dermed hævdet et udsagn, der tillader slutning af både udsagnet A og udsagnet B. D.v.s. at $A \wedge B$ er mindst lige så kraftigt som A og B tilsammen. Omvendt kan man markere, at $A \wedge B$ ikke er kraftigere end A og B tilsammen ved at fastslå, at hvis man fra en samling udsagn $C_1, \ldots, C_n$ kan slutte både A og B, så har man også lov til fra $C_1, \ldots, C_n$ at slutte $A \wedge B$.

Det næstsimpleste eksempel vi kan give er implikationen $A \Rightarrow B$ af to udsagn A og B. Her gælder, at har man sagt $A \Rightarrow B$, så har man dermed hævdet et udsagn, der sammen med A tillader deduktion af B. D.v.s. at denne slutningsregel definitionsmæssigt angiver betydningen eller styrken af $A \Rightarrow B$.

Vi kan også omvendt markere, at $A \Rightarrow B$ ikke har større styrke ved at fastslå, at såfremt man fra en samling udsagn $C_1, \ldots, C_n$ sammen med A kan slutte B, så har man fra $C_1, \ldots, C_n$ alene lov at slutte $A \Rightarrow B$.

3. Hvad er beviser ?

Følger vi ovennævnte ideer, så starter et bevis med en række antagelser, hvorefter der ud fra disse antagelser deduceres en række konsekvenser. Hver af disse er antagelser eller tidligere deducerede konsekvenser eller udledes fra sådanne ved hjælp af de slutningsregler, der definerer de indgående udsagns betydning.

Vi tænker os fra starten givet et sprog $\mathcal{L}_0$, hvor de enkelte udsagn hævder indbyrdes uafhængige kendsgerninger. Sproget $\mathcal{L}_0$ udvides ved at udsagn D introduceres ved definitionssystemer

$$\Delta_D: \left\{ \begin{array}{l} A_{11}, A_{12}, \ldots, D \vdash B_1 \\ A_{21}, A_{22}, \ldots, D \vdash B_2 \\ \ldots\ldots \end{array} \right\},$$

der betyder, at D sammen med $A_{11}, A_{12}, \ldots$ skal medføre B_1, sammen med $A_{21}, A_{22}, \ldots$ skal medføre B_2, o.s.v. Her skal A-erne og B-erne naturligvis være udsagn fra $\mathcal{L}_0$ eller allerede introducerede udsagn. F.eks. er

$$\Delta_{A \wedge B}: \left\{ \begin{array}{l} A \wedge B \vdash A \\ A \wedge B \vdash B \end{array} \right\}$$

og

$$\Delta_{A \Rightarrow B}: \{ A, A \Rightarrow B \vdash B \}.$$

Et bevis starter med at antage en række udsagn, hvorefter der deduceres ved hjælp af reglerne fra udsagnenes definitionssystemer. D.v.s. at såfremt udsagnet D er introduceret som ovenfor, så kan det sammen med $A_{11}, A_{12}, \ldots$ benyttes til at slutte B_1, o.s.v. Endvidere kan D selv sluttes såfremt man fra de yderligere antagelser $A_{11}, A_{12}, \ldots$ kan slutte B_1 og fra de yderligere antagelser $A_{21}, A_{22}, \ldots$

kan slutte B_2 , o.s.v.

Et bevis har altså formen

$$[\![a_1, a_2, \ldots ; b_1, b_2, \ldots]\!] ,$$

hvor $a_1, a_2, \ldots$ er udsagn og $b_1, b_2, \ldots$ er udsagn eller beviser. Hvis b_i er et udsagn, skal det enten være en antagelse, et allerede bevist udsagn, eller følge af tidligere a-er og b-er ved hjælp af slutningsreglerne fra definitionssystemerne af formen Δ_D eller af den tilhørende omvendte slutningsregel, som vi vælger at skrive som

$$\Delta'_D: \{ [\![A_{11}, A_{12}, \ldots ; \ldots , B_1]\!], [\![A_{21}, A_{22}, \ldots ; \ldots , B_2]\!], \ldots \vdash D \} .$$

For $A \wedge B$ og $A \Rightarrow B$ bliver

$$\Delta'_{A \wedge B}: \{ [\![; \ldots , A]\!], [\![; \ldots , B]\!] \vdash A \wedge B \}$$

og

$$\Delta'_{A \Rightarrow B}: \{ [\![A ; \ldots , B]\!] \vdash A \Rightarrow B \} .$$

Medens $\Delta'_{A \Rightarrow B}$ er særdeles anvendelig, virker $\Delta'_{A \wedge B}$ lidt tung. Den erstattes naturligt af reglen

$$A , B \vdash A \wedge B ,$$

der kan bevises ved hjælp af $\Delta'_{A \wedge B}$ på følgende måde

$$[\![A , B ; [\![; A]\!] , [\![; B]\!] , A \wedge B]\!] .$$

Eksempelvis kan man slutte fra B til $A \Rightarrow B$ ved hjælp af beviset

$$[\![B ; [\![A ; B]\!] , A \Rightarrow B]\!] ,$$

der kunne have været opskrevet mere traditionelt som

(1)	<u>Antag</u>	B	
(2)		<u>Antag</u> A	
(3)		B ■ (2)	B er antaget i (1)
(4)		$A \Rightarrow B$ ■ (1)	$\Delta'_{A \Rightarrow B}$ og (2)-(3) .

Hvis vi var startet med $\mathcal{L}_o$ indeholdende A , B og C , og dernæst havde introduceret $A \Rightarrow B$, $A \Rightarrow C$, $B \Rightarrow C$ og $(A \Rightarrow B) \wedge (B \Rightarrow C)$, så kunne vi have sluttet fra $(A \Rightarrow B) \wedge (B \Rightarrow C)$ til $A \Rightarrow C$ på følgende måde

(1)	Antag	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	
(2)		$A \Rightarrow B$	$\Delta_{(A \Rightarrow B) \wedge (B \Rightarrow C)}$ og (1)
(3)		$B \Rightarrow C$	——————// ——————
(4)		Antag A	
(5)		B	$\Delta_{A \Rightarrow B}$ og (2) og (4)
(6)		C ■(4)	$\Delta_{B \Rightarrow C}$ og (3) og (5)
(7)		$A \Rightarrow C$ ■(1)	$\Delta'_{A \Rightarrow C}$ og (4)-(6) .

4. Afledede slutningsregler.

I foregående paragraf har vi vist, hvorledes man kan slutte fra A , B til $A \wedge B$, og vi har skrevet resultatet som A , $B \vdash A \wedge B$. Et sådant resultat kaldes en afledet slutningsregel, og vi vil benytte sådanne afledede slutningsregler i beviser akkurat som om der var tale om regler af formen Δ_D og Δ'_D .

Dette betyder i realiteten blot at de beviser vi skriver op er forkortelser for beviser. Beviserne for de afledede slutningsregler angiver hvorledes beviset skal suppleres op.

5. Disjunktionen.

Disjunktionen $A \vee B$ kan ikke introduceres helt så enkelt som konjunktionen og implikationen. Det simpleste er

$$\Delta_{A \vee B}: \{ A \Rightarrow C \ , \ B \Rightarrow C \ , \ A \vee B \vdash C \quad \text{for alle} \quad C \in \mathcal{L}_o \}.$$

Vi kan ikke forlange $A \Rightarrow C$, $B \Rightarrow C$, $A \vee B \vdash C$ for alle $C \in \mathcal{L}$, hvor $\mathcal{L}$ er $\mathcal{L}_o$ suppleret op med alle introducerede udsagn, da udsagn skal kunne introduceres enkeltvis, og det jo ikke er sikkert, at $A \vee B$ introduceres til sidst. Det er imidlertid så heldigt, at

$$A \Rightarrow C \ , \ B \Rightarrow C \ , \ A \vee B \vdash C \quad \text{for alle} \quad C \in \mathcal{L}$$

automatisk bliver en gyldig afledet slutningsregel. Dette ses ved et induktionsbevis. Lad $\mathcal{M}$ være mængden af udsagn fra $\mathcal{L}$, som opfylder slutningsreglen ovenfor. Da gælder i det mindste $\mathcal{L}_o \subseteq \mathcal{M}$, og vi behøver blot at vise, at såfremt A_{ij}-erne og B_i-erne i

$$\Delta_D: \left\{ \begin{matrix} A_{11}, A_{12}, \ldots, D \vdash B_1 \\ A_{21}, A_{22}, \ldots, D \vdash B_2 \\ \ldots\ldots \end{matrix} \right\}$$

tilhører $\mathcal{M}$, så vil også D tilhøre $\mathcal{M}$. Men dette sidste kan indses ved følgende bevis (der anvender Δ_D og Δ'_D, men kun udnytter, at B_i-erne tilhører $\mathcal{M}$):

$[\![A \Rightarrow D , B \Rightarrow D , A \vee B ;$ -
$[\![A_{11}, A_{12}, \ldots; [\![A; D, B_1]\!] , A \Rightarrow B_1 , [\![B; D, B_1]\!] , B \Rightarrow B_1 , B_1]\!] ,$ -
$[\![A_{21}, A_{22}, \ldots; [\![A; D, B_2]\!] , A \Rightarrow B_2 , [\![B; D, B_2]\!] , B \Rightarrow B_2 , B_2]\!] ,$ -
$\ldots\ldots\ldots\ldots\ldots\ldots$, -
$D]\!]$.

Den omvendte slutningsregel

$$\Delta'_{A \vee B}: \{ [\![A \Rightarrow C , B \Rightarrow C ; \ldots , C]\!] \text{ for } C \in \mathcal{L}_0 \vdash A \vee B \}$$

er temmelig uhåndterlig, men den giver ved hjælp af beviserne

$$[\![A ; [\![A \Rightarrow C , B \Rightarrow C ; C]\!] \text{ for } C \in \mathcal{L}_0 , A \vee B]\!]$$

og

$$[\![B ; [\![A \Rightarrow C , B \Rightarrow C ; C]\!] \text{ for } C \in \mathcal{L}_0 , A \vee B]\!]$$

de bekvemme slutningsregler

$$A \vdash A \vee B \quad \text{og} \quad B \vdash A \vee B .$$

Andre nyttige afledede slutningsregler er de distrubutive love

$$A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C)$$
$$(A \vee B) \wedge (A \vee C) \vdash A \vee (B \wedge C)$$
$$A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$$
$$(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C) .$$

6. Negationen.

Negationen $\neg A$ kan naturligt introduceres som et udsagn, der kan udelukke A fra disjunktioner indeholdende A.

$$\Delta_{\neg A}: \{ A \vee C , \neg A \vdash C \text{ for } C \in \mathcal{L}_0 \} .$$

Analogt med hvad tilfældet var ved disjunktionen fås den afledede slutningsregel

$$A \vee C \ , \neg A \vdash C \quad \text{for alle} \quad C \in \mathcal{L} \ ,$$

der igen ved hjælp af $A \vdash A \vee C$ giver

$$A \ , \neg A \vdash C \quad \text{for alle} \quad C \in \mathcal{L} .$$

Det er nu ikke svært at indse, at man lige så godt kunne have introduceret negationen ved hjælp af det lidt simplere definitionssystem

$$\Delta_{\neg A}: \{ A \ , \neg A \vdash C \quad \text{for alle} \quad C \in \mathcal{L}_0 \} .$$

Den tilhørende omvendte slutningsregel $\Delta'_{\neg A}$ siger, at

$$[\![A \ ; \ \ldots \ C]\!] \text{ for alle } C \in \mathcal{L}_0 \vdash \neg A .$$

Imidlertid er det jo sådan, at såfremt man ved at antage A kan slutte ethvert $C \in \mathcal{L}_0$, så kan man også ved at antage A slutte ethvert $C \in \mathcal{L}$, altså specielt A. Da $A \ , \neg A \vdash C$ for alle $C \in \mathcal{L}_0$, kan ovenstående slutningsregel derfor forenkles til

$$[\![A \ ; \ \ldots \ \neg A]\!] \vdash \neg A .$$

Når man kan udvide $\mathcal{L}$ så det indeholder $\neg A$, så kan man naturligvis udvide yderligere, så det indeholder $\neg\neg A$ og $\neg\neg\neg A$. For disse udsagn gælder beviserne

$$[\![A \ ; \ [\![\neg A \ , \neg\neg A]\!] , \neg\neg A]\!] ,$$

der give den afledede slutningsregel

$$A \vdash \neg\neg A$$

og

$$[\![\neg\neg\neg A \ ; \ [\![A \ ; \ \neg\neg A \ , \ \neg A]\!] \ , \neg A]\!] ,$$

der giver den afledede slutningsregel

$$\neg\neg\neg A \vdash \neg A .$$

7. Kvantorer.

Vi har hidtil ikke antaget noget om nogen struktur på udsagnene i $\mathcal{L}_0$. Hvis disse er af formen $P(a)$ med dele, der kan udskiftes til b, c, ..., er der mulighed for at danne kvantificerede udsagn. Vi kan opfatte $\forall x P(x)$ og

$\exists x P(x)$ som "konjunktionen" og "disjunktionen"

$$P(a) \wedge P(b) \wedge P(c) \wedge \ldots \quad \text{og} \quad P(a) \vee P(b) \vee P(c) \vee \ldots \ .$$

D.v.s. som udsagn defineret ved

$$\Delta_{\forall x P(x)} : \{ \forall x P(x) \vdash P(y) \ , \ y = a, b, c, \ldots \}$$
$$\Delta_{\exists x P(x)} : \{ P(y) \Rightarrow C, \ y = a, b, c, \ldots , \exists x P(x) \vdash C \ \text{ for } C \in \mathcal{L}_0 \} .$$

8. Intuitionistisk logik og klassisk logik.

I det foregående er gennemgået, hvorledes et sprog med en deduktiv struktur kan tænkes opbygget trinvis, således at hvert nyt udsagn får sin mening gennem den måde den vekselvirker med de allerede givne udsagn, og sådan at tilføjelse af et nyt udsagn ikke ændrer den deduktive struktur hørende til de allerede givne udsagn.

Det er imidlertid bemærkelsesværdigt, at den ovennævnte naturlige deduktive struktur er svagere end den, der er knyttet til det, der almindeligvis kaldes klassisk logik. Dette kan man jo nok få en mistanke om, når man ser, at slutningsreglerne $A \vdash \neg\neg A$ og $\neg\neg\neg A \vdash \neg A$ kan retfærdiggøres, men at der tilsyneladende ikke gælder $\neg\neg A \vdash A$.

Afvigelsen fra den klassiske logik kommer simplest frem, hvis vi starter med et $\mathcal{L}_0$, der kun indeholder to udsagn A og B , og dernæst udvider med $A \Rightarrow B$ og $(A \Rightarrow B) \Rightarrow A$. Vi har så et sprog, der indeholder fire udsagn, og det er let at gøre rede for hvilke slutningsregler der gælder. Man ser, at det ikke er muligt at slutte fra $(A \Rightarrow B) \Rightarrow A$ til A . Dette er ikke desto mindre muligt i klassisk logik, hvilket ses ved at undersøge sandhedsværdierne for $(A \Rightarrow B) \Rightarrow A$ for de fire mulige kombinationer af sandhedsværdier for A og B .

I matematik kommer disse vanskeligheder navnlig frem i forbindelse med indirekte beviser. Under negationen har vi omtalt slutningsreglen

$$[\![A \ ; \ \ldots \ , \neg A]\!] \vdash \neg A \ ,$$

der giver mulighed for en svag form for indirekte bevis, hvor $\neg A$ vises ved bevis for at A fører til modstrid. Reglen

$$[\![\neg A \; ; \; \ldots \; , \; A]\!] \vdash A \; ,$$

der giver mulighed for at vise A ved bevis for at $\neg A$ fører til modstrid, er der imidlertid ikke dækning for, og det er just denne form for indirekte beviser, der har givet anledning til mange uoverensstemmelser mellem matematikere.

Ved hjælp af den stærke form for indirekte beviser kan man f.eks. slutte fra $\neg\neg A$ til A således

$$[\![\neg\neg A \; ; [\![\neg A \; , \; A]\!] , \; A]\!] \; ,$$

og man kan slutte fra $(A \Rightarrow B) \Rightarrow A$ til A således

$$[\![(A \Rightarrow B) \Rightarrow A \; ; [\![\neg A \; ; \; [\![A \; ; \; B]\!] \; , \; A \Rightarrow B \; , \; A]\!] \; , \; A]\!] \; .$$

Den form for logik, vi blev ført til, kaldes normalt intuitionistisk logik, fordi den (ca. 1930) blev konstrueret ved formalisering af intuitionistisk matematik. Den klassiske logik blev derimod udviklet allerede i begyndelsen af århundredet. Det bevisbegreb vi har benyttet er en version af naturlig deduktion. Anvendelse af denne type beviser stammer også fra omkring 1930. Tidlige havde man udelukkende koncentreret sig om "lineære" beviser, hvor hvert udsagn følger af tidligere udsagn alene. Dette giver imidlertid komplicerede systemer af slutningsregler og logiske aksiomer, og særdeles "underligere" beviser.

Vi vil nu udskyde den videre diskussion af disse emner til vi mere præcist har fået defineret nogle formelle sprog, og dette kræver udvikling af teknik til behandling af sådanne sprog.

9. Symboler og symbolstrenge.

Vi vil ikke forsøge at forklare hvad symboler og symbolstrenge er, men i stedet udnytte den i §1 omtalte teknik til at "matematisere" emnet. Vi fastslår, at mængden af symbolstrenge $\mathcal{A}^\infty$ dannet ved hjælp af et sæt symboler $\mathcal{A}$ (alfabetet) udstyret med kompositionsreglen konkatenation (sammensætning af symbolstrenge) opfylder følgende aksiomer:

(1) Konkatenationen er associativ. D.v.s. at betegnes symbolstrengen a sammensat med symbolstrenge b med ab, så

gælder for alle a,b,c

$$(ab)c = a(bc) .$$

(2) $\mathcal{A}$ er et frit frembringersystem for $\mathcal{A}^\infty$. D.v.s. at ethvert element b i $\mathcal{A}^\infty$ entydigt lader sig skrive som (da kompositionen er associativ, er parenteser overflødige)

$$b = a_1 a_2 \dots a_n ,$$

hvor $a_1, a_2, \dots, a_n \in \mathcal{A}$.

Som sædvanligt med associative kompositioner får vi induceret en associativ komposition på potensmængden $\mathcal{P}(\mathcal{A}^\infty)$, der for $A,B \subseteq \mathcal{A}^\infty$ er defineret ved

$$AB = \{ ab \mid a \in A \text{ og } b \in B \}.$$

Bemærk, at aksiom (2) ikke gælder for denne komposition. Derimod gælder monotonisætningen

$$A \subseteq B \text{ medfører } AC \subseteq BC \text{ og } CA \subseteq CB \text{ for } A,B,C \in \mathcal{A}^\infty .$$

10. Semigruppen A^∞ frembragt af $A \subseteq \mathcal{A}^\infty$.

I denne paragraf skal vi vise en række sætninger, der ganske vist sagtens kan indses simplere, men hvor de metoder, vi bruger, er anvendelige i langt mere komplicerede tilfælde.

For ethvert $A \subseteq \mathcal{A}^\infty$ er funktionen

$$F(X) = A \cup AX$$

monotont voksende (d.v.s. $X_1 \subseteq X_2 \Rightarrow F(X_1) \subseteq F(X_2)$). Lad

$$\mathcal{M} = \{ X \subseteq \mathcal{A}^\infty \mid X \supseteq F(X) \} .$$

Da $\mathcal{A}^\infty \in \mathcal{M}$, er $\mathcal{M} \neq \emptyset$, og definitionen $X_0 = \bigcap \mathcal{M}$ har derfor en fornuftig mening. På grund af monotonien gælder

$$F(X_0) \subseteq F(X) \subseteq X \text{ for alle } X \in \mathcal{M} ,$$

hvoraf følger, at $X_0 \supseteq F(X_0)$, d.v.s. at der eksisterer en minimal løsning til inklusionen $X \supseteq F(X)$, og denne løsning er netop X_0. Endvidere kan man slutte

$$X_o = F(X_o),$$

fordi der som en simpel følge af monotonien gælder $F(X) \in \mathcal{M}$ for alle $X \in \mathcal{M}$. Den her fundne minimale løsning til ligningen $X = A \cup AX$ kaldes A^∞. (Bemærk at betegnelsen for mængden af symbolstrenge over alfabetet $\mathcal{A}$ harmonerer med denne definition af $\mathcal{A}^\infty$).

Vi vil nu vise, at A^∞ er afsluttet overfor konkatenation, d.v.s. at $(A^\infty)(A^\infty) \subseteq A^\infty$. Det sker ved hjælp af et typisk induktionsbevis, der baserer sig på, at A^∞ er den minimale løsning til inklusionen $X \supseteq A \cup AX$:

A er givet, og vi definerer

$$B = \{b \in A^\infty \mid \{b\}A^\infty \subseteq A^\infty\}.$$

Da $A^\infty = A \cup A\,A^\infty$ gælder oplagt $A \subseteq B$. Endvidere ses, at $b \in B$ medfører, at $(A\{b\})A^\infty = A(\{b\}A^\infty) \subseteq A\,A^\infty \subseteq A^\infty$. Heraf fås $AB \subseteq B$. Alt i alt ses, at $B \supseteq A \cup AB$, men dette giver $B \supseteq A^\infty$, fordi A^∞ er den minimale løsning til $X \supseteq A \cup AX$. For hvert $b \in A^\infty$ gælder altså $\{b\}A^\infty \subseteq A^\infty$, men dette medfører $A^\infty A^\infty \subseteq A^\infty$.

For ethvert $A \subseteq \mathcal{A}^\infty$ gælder altså, at konkatenationen er en associativ komposition på A^∞. Derimod behøver A ikke at være et frit frembringersystem for A^∞, hvad eksemplet $\{a,b,ab\}^\infty = \{a,b\}^\infty$ viser. Man ser let, at A kun er et frit frembringersystem for A^∞, når ethvert element i A enten tilhører A eller entydigt lader sig skrive som ab, hvor $a \in A$ og $b \in A^\infty$. D.v.s. at opspaltningen $A^\infty = A \cup AA^\infty$ er <u>entydig</u>.

Hvis den ovenfor omtalte entydighed gælder, vil der netop eksistere 1 funktion $n: A^\infty \rightsquigarrow \mathbb{N}$, så

$$(*) \quad \begin{cases} n(a) = 1 & \text{for } a \in A \\ n(ab) = 1 + n(b) & \text{for } a \in A \text{ og } b \in A^\infty. \end{cases}$$

Dette ses således: Lad

$$\mathcal{R} = \{R \subseteq A^\infty \times \mathbb{N} \mid A \times \{1\} \subseteq R \text{ og } (ab, 1+i) \in R \text{ for } a \in A,\ b \in A^\infty,\ (b,i) \in R\}.$$

Der gælder da $\mathcal{R} \neq \emptyset$, fordi $A^\infty \times \mathbb{N} \in \mathcal{R}$. Lad

$R_0 = \bigcap \mathcal{R}$ og $X_0 = \{b \in A^\infty \mid (b,i) \in R_0$ for netop 1 $i \in \mathbb{N}\}$. Man ser let, at $R_0 \in \mathcal{R}$, og at $A \subseteq X_0$, fordi $(a,i) \in R_0$, $i \neq 1$, ville medføre $R_0 \setminus \{(a,i)\} \in \mathcal{R}$ i modstrid med, at R_0 er det minimale element i $\mathcal{R}$. Endvidere gælder $AX_0 \subseteq X_0$, fordi $(b,i),(ab,j) \in R_0$, $a \in A$, $b \in X_0$ og $j \neq i+1$ medfører, at $R_0 \setminus \{(ab,j)\} \in \mathcal{R}$. Alt i alt haves $X_0 \supseteq A \cup AX_0$, der medfører, at $X_0 \supseteq A$. Hermed er vist, at relationen R_0 er en funktion, og man verificerer let rekursionsformlerne (*). Entydigheden følger af, at enhver anden funktion, der opfylder (*), også skulle tilhøre $\mathcal{R}$.

Ved hjælp af induktion kan nu vises, at funktionen n opfylder $n(bc) = n(b)+n(c)$ for alle $b,c \in A$:

Lad $B = \{b \in A^\infty \mid n(bc) = n(b)+n(c)$ for alle $c \in A^\infty\}$. Der gælder da oplagt $A \subseteq B$, og $AB \subseteq B$ følger af, at $a \in A$, $b \in B$, $c \in A^\infty$ medfører $n((ab)c) = n(a(bc)) = 1+n(bc) = 1+(n(b)+n(c)) = (1+n(b))+n(c) = n(ab)+n(c)$. Vi har altså $B \supseteq A \cup AB$, der medfører $B \supseteq A^\infty$.

Bemærk, at A også kunne have været defineret som den minimale løsning til inklusionen $X \supseteq A \cup XA$ eller inklusionen $X \supseteq A \cup XX$. For den sidstnævnte inklusion gælder ikke entydighed, men dette forhindrer naturligvis ikke, at funktionen n kan defineres rekursivt ved

$$\begin{cases} n(a) = 1 & \text{for } a \in A \\ n(bc) = n(b) + n(c) & \text{for } b,c \in A \ . \end{cases}$$

Dog er det klart, at det er "farligt" at benytte rekursive definitioner, når der ikke gælder entydighed.

11. Backus-notationen.

Lad os antage, at

$$\mathcal{A} = \{[,], +, \cdot\} \cup V,$$

hvor V er en uendelig mængde $\{x_0, x_1, x_2, \ldots\}$ af symboler kaldet variable, er et alfabet, der frembringer en fri semigruppe ved hjælp af en associativ komposition, konkatenationen. Symbolerne "[", "]", "+", "·", samt x_0, x_1, x_2, ... er altså betegnelser for symboler i $\mathcal{A}$, ikke selve symbolerne.

Vi kigger på inklusionen

$$(*) \qquad X \supseteq V \cup \{[\}X\{+\}X\{]\} \cup \{[\}X\{\cdot\}X\{]\} \ .$$

Ved at bruge metoderne fra §10 kan man vise, at der netop findes 1 minimal løsning U, og at denne opfylder

$$U = V \cup \{[\}U\{+\}U\{]\} \cup \{[\}U\{\cdot\}U\{]\} \ .$$

Som eksempler på elementer i U kan nævnes

$$x_0,\ x_1,\ [x_0+x_1],\ [[x_0+x_1]\cdot x_2],\ \ldots$$

Endvidere gælder der entydighed, d.v.s. at ethvert element i U enten tilhører V eller entydigt kan skrives som $[u_1+u_2]$ eller som $[u_1\cdot u_2]$, hvor $u_1, u_2 \in U$. Den sidste påstand indses på følgende måde:

Funktionen $f: \mathcal{A}^\infty \to \mathbb{Z}$ defineres rekursivt ved

$$\begin{cases} f(a) = 1, \text{ hvis } a = [\\ f(a) = -1, \text{ hvis } a =] \\ f(a) = 0, \text{ hvis } a \in \mathcal{A} \setminus \{[,]\} \\ f(ab) = f(a) + f(b) \text{ for } a \in \mathcal{A} \text{ og } b \in \mathcal{A}^\infty. \end{cases}$$

Der gælder da $f(bc) = f(b)+f(c)$ for alle $b,c \in \mathcal{A}^\infty$. Ved induktion ses, at $f(u) = 0$ for alle $u \in U$, og at $f(b)<0$ og $f(c)>0$, såfremt $bc \in U$. Det fremgår heraf, at intet element u_1 i U kan være begyndelsessegment af et andet element u_2 i U. (D.v.s. at $u_2 = u_1 c$, hvor $c \in \mathcal{A}^\infty$). Dette giver oplagt entydigheden. Bemærk, at vi ikke har været så omhyggelige som i sidste paragraf, men dette skyldes at beviset så ville blive urimeligt omstændeligt.

Den ovenfor beviste entydighed medfører f.eks. at der for hver funktion $g: V \to \mathbb{R}$ findes netop 1 funktion $\hat{g}: U \to \mathbb{R}$, så

$$\begin{aligned} \hat{g}(v) &= g(v) \quad \text{for} \quad v \in V \\ \hat{g}([u_1+u_2]) &= \hat{g}(u_1)+\hat{g}(u_2) \quad \text{for} \quad u_1, u_2 \in U \\ \hat{g}([u_1\cdot u_2]) &= \hat{g}(u_1)\cdot\hat{g}(u_2) \quad \text{for} \quad u_1, u_2 \in U \end{aligned}$$

Man ser, at (*) definerer <u>syntaksen</u> hørende til en bestemt klasse symbolstrenge U, og at entydigheden af (*) gør det muligt at definere den tilhørende <u>semantik</u>, altså definere hvorledes udtrykkene i U skal fortolkes.

Der er tydeligt et vist overforbrug af parenteser i U.

Brugen af parenteser kan helt undgås ved anvendelse af polsk notation, hvor U_p defineres som minimalløsningen til

$$X \supseteq V \cup \{+\}XX \cup \{\cdot\}XX.$$

Her bevises entydigheden ved følgende rekursive definition af $f: \mathcal{A}^\infty \to \mathbb{Z}$

$$\begin{aligned} f(a) &= 1 \quad \text{for} \quad a \in \{+,\cdot\} \\ f(a) &= -1 \quad \text{for} \quad a \in V \\ f(a) &= 0 \quad \text{for} \quad a \in \mathcal{A} \setminus (V \cup \{+,\cdot\}) \\ f(ab) &= f(a) + f(b) \quad \text{for } a \in \mathcal{A},\ b \in \mathcal{A}^\infty . \end{aligned}$$

Ligesom før gælder $f(bc) = f(b)+f(c)$ for $b,c \in \mathcal{A}^\infty$, og ved induktion ses, at $f(u) = -1$ for alle $u \in U_p$, samt at $f(b) \geq 0$ og $f(c) < 0$ for $bc \in U_p$. Analogt med U gælder, at intet element u_1 i U_p kan være begyndelsessegment af et andet element u_2 i U_p, og dette giver umiddelbart entydigheden.

Polsk notation har imidlertid den ulempe, at udtrykkene (som f.eks. $+\cdot x_0 + x_1 x_0 x_2$) bliver temmelig uforståelige. Større betydning har omvendt polsk notation, hvor U'_p defineres som minimalløsningen til

$$X \supseteq V \cup XX\{+\} \cup XX\{\cdot\} .$$

Sådanne udtryk kan f.eks. umiddelbart tastes ind i mange lommeregnere, og det er meget almindeligt, at compilere "oversætter" udtryk til omvendt polsk notation, fordi operationerne + og $\cdot$, samt hvad man ellers har med, derved, læst fra venstre til højre, kommer i den rækkefølge de skal udføres.

Når det drejer sig om læselighed, er det naturligt at definere aritmetiske udtryk ved et mere kompliceret inklusionssystem, som f.eks.

$$\begin{aligned} U &\supseteq V \cup A \cup M \\ A &\supseteq A_1\{+\}A_2 \\ M &\supseteq M_1\{\cdot\}M_2 \\ A_1 &\supseteq V \cup A \cup M \\ A_2 &\supseteq V \cup \{(\}A\{)\} \cup M \\ M_1 &\supseteq V \cup \{(\}A\{)\} \cup M \\ M_2 &\supseteq V \cup \{(\}A\{)\} \cup \{(\}M\{)\} . \end{aligned}$$

Her fås en minimalløsning $(\overline{U},\overline{A},\overline{M},\overline{A}_1,\overline{A}_2,\overline{M}_1,\overline{M}_2)$, for hvilken der gælder

$$\begin{aligned}
\bar{U} &= V \cup \bar{A} \cup \bar{M} \\
\bar{A} &= \bar{A}_1 \{+\} \bar{A}_2 \\
\bar{M} &= \bar{M}_1 \{\cdot\} \bar{M}_2 \\
\bar{A}_1 &= V \cup \bar{A} \cup \bar{M} \quad (=\bar{U}) \\
\bar{A}_2 &= V \cup \{(\}\bar{A}\{)\} \cup \bar{M} \\
\bar{M}_1 &= V \cup \{(\}\bar{A}\{)\} \cup \bar{M} \quad (=\bar{A}_2) \\
\bar{M}_2 &= V \cup \{(\}\bar{A}\{)\} \cup \{(\}\bar{M}\{)\} .
\end{aligned}$$

Sådanne systemer opgives normalt ved hjælp af Backus notationen (fra Report on the algorithmic language ALGOL-60), hvor foreningsmængdesymbolet $\cup$ skrives som | og b skrives som b for b $\in \mathcal{A}^{\infty}$. Endvidere benyttes normalt udtryk af formen <et navn> som konstanter eller variable, og i stedet for = eller $\supseteq$ skrives ::= . Systemet ovenfor bliver altså f.eks. til

<aritmetisk udtryk>::=<variabel>|<sum>|<produkt>
<sum>::=<venstre addend>+<højre addend>
<produkt>::=<venstre faktor>·<højre faktor>
<venstre addend>::=<variabel>|<sum>|<produkt>
<højre addend>::=<variabel>|(<sum>)|<produkt>
<venstre faktor>::=<variabel>|(<sum>)|(<produkt>)

Kaldes et + eller · frit, såfremt det ikke er lukket inde mellem samhørende parenteser, ses at elementerne i $\bar{A}$ er karakteriseret ved mindst et frit +, og at det længst til højre forekommende frie + entydigt deler i et element fra $\bar{A}_1$ og et element fra $\bar{A}_2$. Elementerne fra $\bar{M}$ er karakteriseret ved mindst et frit · og ingen frie +, og opspaltningen i et element fra $\bar{M}_1$ og et element fra $\bar{M}_2$ sker analogt ved det sidst forekommende frie · . Inklusionssystemet er altså entydigt.

Det er klart, at entydighedsbeviser kan blive ganske komplicerede. Og i den oprindelige ALGOL-rapport, hvor sproget blev defineret ved hjælp af over 150 "ligninger" var entydigheden da heller ikke helt i orden.

12. Chomsky's grammatik'er.

De klasser af symbolstrenge, som kan defineres ved hjælp

af Backus-notationen var faktisk allerede karakteriseret nogle år tidligere i sprogteoretiske undersøgelser af Noam Chomsky.

En kontekstfri grammatik $\mathcal{G}$ er givet ved hjælp af to disjunkte mængder $\mathcal{A}$ og $\mathcal{V}$ af symboler, en mængde

$$\mathcal{P} \subseteq \mathcal{V} \times (\mathcal{A} \cup \mathcal{V})^{\infty}$$

af produktioner, samt et specielt udpeget symbol i $\mathcal{V}$ kaldet sætningssymbolet. Elementerne i $\mathcal{A}$ kaldes terminale symboler, og elementerne i $\mathcal{V}$ kaldes ikke-terminale symboler. En produktion (v,b) skrives normalt v->b .

Vi vedtager at udvide $(\mathcal{A} \cup \mathcal{V})^{\infty}$ med et neutralt element ε , kaldet den tomme symbolstreng, således at $\varepsilon b = b\varepsilon = b$ for alle $b \in (\mathcal{A} \cup \mathcal{V})^{\infty} \cup \{\varepsilon\}$. Dette berører ikke gyldigheden af den associative lov, men aksiom (2) på side 10 må naturligvis modificeres en smule.

Hvis v->b er en produktion, $c=c_1 v c_2$ og $d=d_1 b d_2$, hvor $c_1, c_2, d_1, d_2 \in (\mathcal{A} \cup \mathcal{V})^{\infty} \cup \{\varepsilon\}$, siges d at kunne umiddelbart udledes af c. En symbolstreng d siges at kunne udledes af en symbolstreng c, såfremt der findes en endelig følge af symbolstrenge $e_0, e_1, \ldots, e_n$, så $c=e_0$, $d=e_n$ og e_i er en umiddelbar følge af e_{i-1} for i=1, ... ,n.

Det kontekstfrie sprog defineret ved hjælp af grammatik'en $\mathcal{G}$ er mængden af symbolstrenge i $\mathcal{A}^{\infty}$, der kan udledes af sætningssymbolet.

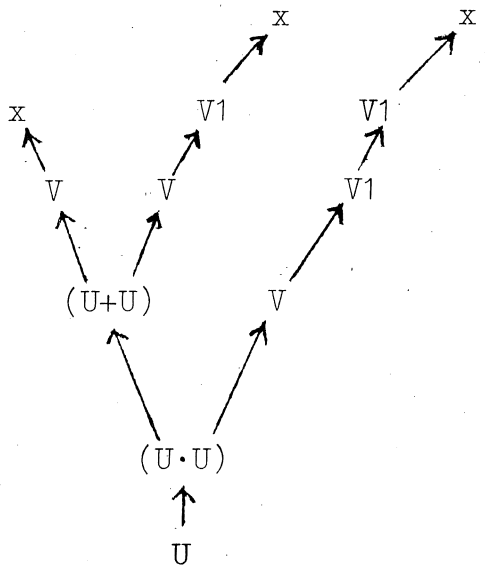
Lad f.eks. $\mathcal{A}$ være {+,·,(,),x,1} ,lad $\mathcal{V}$ være {V,U} , lad $\mathcal{P}$ bestå af produktionerne (sammenlign med (*) på side 13)

V -> x
V -> V1
U -> V
U ->(U+U)
U ->(U·U)

og lad U være sætningssymbolet. Da kan symbolstrengen ((x+x1)·x11) udledes således:

U=>(U·U)=>((U+U)·U)=>((V+U)·U)=>((V+V)·U)=>((V+V)·V)=>
((x+V)·V)=>((x+V1)·V)=>((x+x1)·V)=>((x+x1)·V1)=>((x+x1)·V11)=>
((x+x1)·x11)

Denne udledelse kan mere overskueligt opstilles i et træ



hvor resultatet kan læses ved at følge træet rundt fra venstre mod højre og registre de terminale symboler.

Et eksempel fra de naturlige sprogs verden fås ved hjælp af en grammatik med følgende produtioner (hvor S er sætningssymbolet og de ikke-terminale symboler N_G,V_G,T,N og V betyder nominalgruppe, verbalgruppe, artikel, substantiv og verbum)

$$S \rightarrow N_G V_G$$
$$N_G \rightarrow TN$$
$$V_G \rightarrow VN_G$$
$$T \rightarrow \text{the}$$
$$N \rightarrow \text{man}$$
$$N \rightarrow \text{ball}$$
$$V \rightarrow \text{hit}$$
$$V \rightarrow \text{took}$$

der tillader udledelse af sætninger som "the man hit the ball" og "the ball took the man".

Man kan spørge sig selv, om alle mængder af symbolstrenge kan defineres som kontekstfrie sprog. Svaret er benægtende. F.eks. gælder for $\Sigma = \{a,b\}$, at

$$\{a^n b^n a^n \mid n \in \mathbb{N}\}$$

ikke kan defineres som et kontekstfrit sprog, medens f.eks. $\{a^n b^n \mid n \in \mathbb{N}\}$ kan defineres ved hjælp af produktionerne

S -> ab
S -> aSb .

Chomsky's undersøgelser viser, at de naturlige sprog er for komplicerede til at kunne beskrives ved hjælp af kontekstfrie grammatik'er, og han har derfor konstrueret mere komplicerede transformationsgrammatik'er , hvor sætningers dybdestruktur kan defineres ved hjælp af kontekstfrie grammatik'er, medens overfladestrukturen fremkommer ved transformationsregler anvendt på dybdestrukturen. Disse transformationsregler anvender bl.a. kontekstsensitive produktioner b->c , hvor venstresiden ikke blot består af et enkelt ikke-terminalt symbol.

Det er også værd at nævne, at Chomsky har gjort sig til talsmand for det synspunkt, at man for at forklare menneskets overraskende evne til hurtigt at tilegne sig et sprog må antage, at vi arveligt er forsynet med en vis universalgrammatik. Denne skulle sætte os i stand til udfra kendskab til relativt få eksempler på sætninger i et sprog at konstruere sprogets grammatik og ved hjælp af denne danne uendelig mange korrekte sætninger. Det er nærliggende at antage at kendskabet til en sådan sprogevne også ville kunne belyse vor evne til at oversætte intuitiv indsigt til logiske ræsonementer og vor evne til at "forstå" sådanne ræsonementer. Desværre synes undersøgelserne langt fra at være på et stade, hvor noget sådant kan lade sig gøre.

13. Formel klassisk udsagnslogik.

Vi tænker os nu givet en fri semigruppe $\mathcal{S}^\infty$ med frembringersystem

$$\mathcal{S} = \{\wedge, \Rightarrow, \vee, \neg, (,)\} \cup A ,$$

hvor A = <atomisk udsagn> er en tællelig mængde af symboler.

Mængden af udsagn U = <udsagn> kan da i Backus-notationen defineres på følgende måde

<udsagn>::=<atomisk udsagn>|<implikation>|<konjunktion>|
<disjunktion>|<negation>
<implikation>::=<udsagn$_1$> $\Rightarrow$ <udsagn>
<disjunktion>::=<udsagn$_1$> $\vee$ <udsagn$_2$>
<konjunktion>::=<udsagn$_2$> $\wedge$ <udsagn$_3$>
<negation>::= $\neg$ <udsagn$_3$>
<udsagn$_1$>::=<atomisk udsagn>|<negation>|<konjunktion>|
<disjunktion>|(<implikation>)
<udsagn$_2$>::=<atomisk udsagn>|<negation>|<konjunktion>|
(<disjunktion>)|(<implikation>)
<udsagn$_3$>::=<atomisk udsagn>|<negation>|(<konjunktion>)|
(<disjunktion>)|(<implikation>)

Kaldes et tegn frit, hvis det ikke forekommer mellem samhørende parenteser, ses at entydigheden fremgår af, at et udsagn deles ved det længst til venstre forekommende $\Rightarrow$, hvis der er frie implikationstegn, ved det længst til højre forekommende $\vee$, hvis der er frie disjunktionstegn, men ikke frie implikationstegn, o.s.v.

Lad $f_\Rightarrow, f_\vee, f_\wedge$:<udsagn> $\times$ <udsagn> $\rightsquigarrow$ <udsagn> og $f_\neg$:<udsagn> $\rightsquigarrow$ <udsagn> være defineret ved

$$f_\Rightarrow(u,v) = \begin{cases} u \Rightarrow v \text{ , hvis } u \in \langle\text{udsagn}_1\rangle \text{ og } v \in \langle\text{udsagn}\rangle \\ (u) \Rightarrow v \text{ , hvis } u \in \langle\text{udsagn}\rangle \setminus \langle\text{udsagn}_1\rangle \text{ og } v \in \langle\text{udsagn}\rangle \end{cases}$$

- - - - - - - - - - - - - - -

$$f_\neg(u) = \begin{cases} \neg u \text{ , hvis } u \in \langle\text{udsagn}_3\rangle \\ \neg(u) \text{ , hvis } u \in \langle\text{udsagn}\rangle \setminus \langle\text{udsagn}_3\rangle \text{ .} \end{cases}$$

Da er $f_\Rightarrow, f_\vee, f_\wedge$ og $f_\neg$ injektive funktioner med disjunkte billedmængder, hvis foreningsmængde er mængden af ikke-atomiske udsagn. I det følgende lader vi $u \Rightarrow v$, $u \vee v$, $u \wedge v$ og $\neg u$ betyde $f_\Rightarrow(u,v)$, $f_\vee(u,v)$, $f_\wedge(u,v)$ og $f_\neg(u)$, når u og v er variable eller udtryk, der betegner elementer i <udsagn>.

Lad nu $\varphi_\Rightarrow, \varphi_\vee, \varphi_\wedge : \{0,1\} \times \{0,1\} \rightsquigarrow \{0,1\}$ og $\varphi_\neg : \{0,1\} \rightsquigarrow \{0,1\}$ være defineret ved (0 fortolkes som

"falsk" og 1 som "sand"):

$\varphi_{\Rightarrow}$	0	1
0	1	1
1	0	1

$\varphi_{\vee}$	0	1
0	0	1
1	1	1

$\varphi_{\wedge}$	0	1
0	0	0
1	0	1

$\varphi_{\neg}$	
0	1
1	0

I det følgende lader vi $i \Rightarrow j$, $i \vee j$, $i \wedge j$ og $\neg i$ betyde $\varphi_{\Rightarrow}(i,j)$, $\varphi_{\vee}(i,j)$, $\varphi_{\wedge}(i,j)$ og $\varphi_{\neg}(i)$, når $i,j \in \{0,1\}$.

Enhver funktion g:<atomisk udsagn>$\rightsquigarrow\{0,1\}$ vil da entydigt inducere en funktion $\hat{g}$:<udsagn>$\rightsquigarrow\{0,1\}$, således at (jvf. nederst side 13)

$$\begin{cases} \hat{g}(u) = g(u), \text{ hvis } u \in \langle\text{atomisk udsagn}\rangle \\ \hat{g}(u \Rightarrow v) = \hat{g}(u) \Rightarrow \hat{g}(v) \quad \text{for } u,v \in \langle\text{udsagn}\rangle \\ \hat{g}(u \vee v) = \hat{g}(u) \vee \hat{g}(v) \quad \text{———} \\ \hat{g}(u \wedge v) = \hat{g}(u) \wedge \hat{g}(v) \quad \text{———} \\ \hat{g}(\neg u) = \neg \hat{g}(u) \quad \text{for } u \in \langle\text{udsagn}\rangle \end{cases}$$

Når $\Gamma \subseteq$<udsagn> og $u \in$<udsagn> siges u at være en <u>konsekvens</u> af Γ (dette skrives $\Gamma \models u$), såfremt der for alle g: <atomisk udsagn>$\rightsquigarrow\{0,1\}$ gælder, at $\hat{g}(u)=1$, når $\hat{g}(v)=1$ for alle $v \in \Gamma$. I stedet for $\{u_1, \ldots, u_n\} \models u$ skrives blot $u_1, \ldots, u_n \models u$.

Vi skal nu definere mængden af beviser. Mængden af korrekte beviser kan strengt taget ikke defineres som et kontekstfrit sprog; vi vælger at definere en større mængde af symbolstrenge som <bevis> og en endnu større mængde som <bevisstreng>. Dette kan gøres ved hjælp af Backus-notationen. Dernæst defineres, hvornår et udsagn u kan deduceres fra en mængde Γ af udsagn. Dette skrives som $\Gamma \vdash u$. Tilbage har vi det interessante spørgsmål om $\Gamma \vdash u$ er ensbetydende med $\Gamma \models u$.

Vi får kun brug for beviser med 1 antagelse og kan derfor forenkle opbygningen af beviser til $[\![A_0 A_1 \ldots A_n]\!]$, hvor A_0 er antagelsen. Vi antager at alfabetet $\mathcal{A}$ yderligere indeholder symbolerne $[\![$ og $]\!]$, og har da det entydige system (bemærk at <bevisstreng>=(<udsagn>$\cup$ <bevis>)$^{\infty}$):

<bevisstreng>::=<udsagn>|<bevis>|<bevisstreng><udsagn>|
<bevisstreng><bevis>

<bevis>::= $[\![$<udsagn><bevisstreng>$]\!]$

I det følgende lader vi a og b betegne elementer i <udsagn>, og s og t betegne elementer i <bevisstreng>$\cup \{\varepsilon\}$, hvor ε er den tomme symbolstreng (se side 16). Endvidere betegner Γ delmængder af <udsagn>, og Δ delmængder af <udsagn>$\cup$<bevis>.

Et udsagn u kaldes en <u>umiddelbar følge</u> af Δ såfremt en af følgende betingelser er opfyldt:

(0) $u \in \Delta$

(1) $a, a \Rightarrow u \in \Delta$ — (1)' u er $a \Rightarrow b$ og $[\![asb]\!] \in \Delta$

(2) $a \wedge u \in \Delta$ eller $u \wedge a \in \Delta$ — (2)' u er $a \wedge b$ og $a, b \in \Delta$

(3) $[\![asu]\!], [\![bsu]\!], a \vee b \in \Delta$ — (3)' u er $a \vee b$, og $a \in \Delta$ eller $b \in \Delta$

(4) $a, \neg a \in \Delta$ — (4)' $[\![\neg usu]\!] \in \Delta$.

Mængden af <u>elementer</u> i en bevisstreng defineres rekursivt ved

$$E(\varepsilon) = \emptyset$$
$$E(sa) = E(s) \cup \{a\}$$
$$E(s[\![at]\!]) = E(s) \cup \{[\![at]\!]\},$$

og korrektheden af en bevisstreng defineres rekursivt ved

$$\varkappa(\Gamma, \varepsilon) = 1$$

$$\varkappa(\Gamma, sa) = \begin{cases} 1, \text{ hvis } \varkappa(\Gamma, s) = 1, \text{ og a er element i } \Gamma \text{ eller en umiddelbar følge af } E(s) \\ 0 \text{ ellers} \end{cases}$$

$$\varkappa(\Gamma, s[\![at]\!]) = \begin{cases} 1, \text{ hvis } \varkappa(\Gamma, s) = 1 \text{ og } \varkappa(\Gamma \cup \{a\}, sat) = 1 \\ 0 \text{ ellers} \end{cases}$$

Den sidste definition kræver den kommentar, at når man har defineret $\varkappa(\Gamma, s)$ for alle Γ og alle s kortere end t, så giver definitionen værdien af $\varkappa(\Gamma, t)$ for alle Γ.

Vi definerer nu, at $\Gamma \vdash u$ såfremt $\Gamma \subseteq$ <udsagn> og der findes et s, så $\varkappa(\Gamma, su) = 1$. Hvis $\Gamma = \{u_1, \ldots, u_n\}$ er dette ensbetydende med, at der findes et bevis t lig

$$[\![u_1 \wedge u_2 \wedge \ldots \wedge u_n \quad s \quad u]\!],$$

så $(\emptyset, t) = 1$.

For ethvert g:<atomisk udsagn>$\rightsquigarrow \{0,1\}$ udvider vi $\hat{g}$:<udsagn>$\rightsquigarrow \{0,1\}$ til <bevisstreng>$\cup \{\varepsilon\}$ ved følgende definitioner

$$\begin{cases} \hat{g}(\varepsilon) = 1 \\ \hat{g}(sa) = \hat{g}(s) \wedge \hat{g}(a) \\ \hat{g}(s[\![at]\!]) = \hat{g}(s) \wedge (\hat{g}(a) \Rightarrow \hat{g}(t)) \end{cases}$$

Ved induktion ses da let, at $\hat{g}(x)=1$ for alle $x \in \Gamma$ sammen med $\varkappa(\Gamma,s)=1$ medfører $\hat{g}(s)=1$, men dette giver umiddelbart, at $\Gamma \vdash u$ medfører $\Gamma \models u$.

Det er meget vanskeligere at vise, at $\Gamma \models u$ medfører $\Gamma \vdash u$. Det bevis vi giver er et typisk ikke-intuitionistisk-gyldigt bevis, idet vi viser, at non $\Gamma \vdash u$ medfører non $\Gamma \models u$. D.v.s. vi benyttet at $\neg b \Rightarrow \neg a \vdash a \Rightarrow b$. Denne afledede slutningsregel kan vises ved hjælp af den stærke form for indirekte bevis (4)', samt (4),(1) og (1)', på følgende måde

$$[\![\neg b \Rightarrow \neg a [\![a [\![\neg b \quad \neg a \; b]\!] \; b]\!] \; a \Rightarrow b]\!] .$$

Vi antager altså, at $\Gamma \subseteq$ <udsagn>, og at der ikke findes nogen bevisstreng s, så $\varkappa(\Gamma,su)=1$. Vi skal vise, at der findes en funktion $g:$<atomisk udsagn>$\to \{0,1\}$, så $\hat{g}(a)=1$ for alle $a \in \Gamma$ og $\hat{g}(u)=0$.

(I). Numerér elementerne i <udsagn> $u_1, u_2, u_3, \ldots$ og lad $\Gamma_i, i \in \mathbb{N}_0$ være defineret rekursivt ved

$$\Gamma_0 = \Gamma$$

$$\Gamma_{i+1} = \begin{cases} \Gamma_i \cup \{u_{i+1}\}, \text{ hvis non } \Gamma_i \cup \{u_{i+1}\} \vdash u \\ \Gamma_i \quad \text{ellers} \end{cases}$$

Der gælder da, at $\Gamma = \Gamma_0 \subseteq \Gamma_1 \subseteq \Gamma_2 \subseteq \ldots$. Lad $\Gamma_\infty = \bigcup_{i=0}^{\infty} \Gamma_i$. Da en bevisstreng kun kan indeholde endelig mange udsagn, gælder non $\Gamma_\infty \vdash u$. Endvidere vil for ethvert udsagn u_i gælde netop én af mulighederne $u_i \in \Gamma_\infty$ og $\neg u_i \in \Gamma_\infty$. At $u_i, \neg u_i \in \Gamma_\infty$ er umuligt, da (4) ville medføre $\Gamma_\infty \vdash u$. Også $u_i, \neg u_i \notin \Gamma_\infty$ er umuligt, da det ville medføre $\Gamma_\infty \cup \{u_i\} \vdash u$ og $\Gamma_\infty \cup \{\neg u_i\} \vdash u$, d.v.s. at der fandtes bevisstrenge s og t, så $\varkappa(\Gamma_\infty \cup \{u_i\}, su)=1$ og $\varkappa(\Gamma_\infty \cup \{\neg u_i\}, tu)=1$. Men da gælder

$$\varkappa(\Gamma_\infty, [\![\neg u [\![\neg u_i t u u_i]\!] \; u_i s u]\!] \; u) = 1,$$

som medfører $\Gamma_\infty \vdash u$.

(II). Af (I) fås

$a \Rightarrow b \in \Gamma_\infty$ hvis og kun hvis $a \notin \Gamma_\infty$ eller $b \in \Gamma_\infty$
$a \wedge b \in \Gamma_\infty$ ——— // ——— $a \in \Gamma_\infty$ og $b \in \Gamma_\infty$
$a \vee b \in \Gamma_\infty$ ——— // ——— $a \in \Gamma_\infty$ eller $b \in \Gamma_\infty$
$\neg a \in \Gamma_\infty$ ——— // ——— $a \notin \Gamma_\infty$

F.eks. kan der ikke gælde $a \vee b \in \Gamma_\infty$ samtidig med $a \notin \Gamma_\infty$ og $b \notin \Gamma_\infty$, da $\neg a, \neg b, a \vee b \vdash u$, hvilket fremgår af bevisstrengen

$$\neg a \ \neg b \ a \vee b \ [\![a \ u]\!] \ [\![b \ u]\!] \ u \ .$$

(III). Vi definerer nu g:<atomisk udsagn>$\rightsquigarrow\{0,1\}$ ved

$$g(a) = \begin{cases} 1, & \text{hvis } a \in \Gamma_\infty \\ 0 & \text{ellers} \end{cases}$$

Udnyttes (II) i et induktionsbevis fås at der for alle udsagn a gælder

$$\hat{g}(a) = \begin{cases} 1, & \text{hvis } a \in \Gamma_\infty \\ 0 & \text{ellers} \ . \end{cases}$$

Da $\hat{g}(u)=0$ er vi hermed færdig.

14. Formel klassisk 1.ordens logik.

I første omgang begrænser vi os til det system, der senere skal benyttes til talteori. Det er iøvrigt let at se, hvorledes andre systemer kan defineres analogt.

Vi udvider alfabetet med symbolerne

$$= \quad + \quad \cdot \quad 0 \quad 1 \quad \forall \quad \exists$$

samt en tællelig mængde variable <variable>$= x_0, x_1, \ldots$. Til gengæld fjernes mængden af atomiske udsagn fra alfabetet, og systemet der definerer mængden af udsagn udvides med

<konstant>::=0|1
<kvantor>::=$\forall$|$\exists$
<term>::=<konstant>|<variabel>|<produkt>|<sum>
<sum>::=<term>+<term$_1$>
<produkt>::=<term$_1$>$\cdot$<term$_2$>

<$term_1$>::=<konstant>|<variabel>|<produkt>|(<sum>)
<$term_2$>::=<konstant>|<variabel>|(<produkt>)|(<sum>)
<atomisk udsagn>::=<term>=<term>|
<kvantor><variabel><udsagn$_3$>

I det følgende opfattes + og · som de naturligt definerede injektive funktioner fra <term> × <term> over i <term>. Analogt med kvantorerne.

Funktionen

$$F: \langle term\rangle \cup \langle udsagn\rangle \rightsquigarrow \mathcal{P}\langle variabel\rangle,$$

der til termer og udsagn knytter mængden af <u>frie variable</u>, defineres rekursivt ved

$F(k) = \emptyset$ for $k \in \{0,1\}$

$F(v) = \{v\}$ for $v \in$ <variabel>
$F(t_1+t_2) = F(t_1) \cup F(t_2)$ for $t_1, t_2 \in$ <variabel>
$F(t_1 \cdot t_2) = F(t_1) \cup F(t_2)$ ——— // ———
$F(t_1=t_2) = F(t_1) \cup F(t_2)$ ——— // ———
$F(a \Rightarrow b) = F(a) \cup F(b)$ for $a,b \in$ <udsagn>
$F(a \vee b) = F(a) \cup F(b)$ ——— // ———
$F(a \wedge b) = F(a) \cup F(b)$ ——— // ———
$F(\neg a) = F(a)$ for $a \in$ <udsagn>
$F(\forall va) = F(a) \setminus \{v\}$ for $v \in$ <variabel> og $a \in$ <udsagn>
$F(\exists va) = F(a) \setminus \{v\}$ ——— // ———

For alle $v \in$ <variabel> og $t \in$ <term> defineres funktionen

$$S_t^v: \langle term\rangle \cup \langle udsagn\rangle \rightsquigarrow \langle term\rangle \cup \langle udsagn\rangle ,$$

der i termer og udsagn <u>substituerer</u> termen t i stedet for variablen v, rekursivt på følgende måde:

$S_t^v(k) = k$ for $k \in \{0,1\}$

$$S_t^v(x) = \begin{cases} t & \text{for } x=v \\ x & \text{for } x \in \langle variabel\rangle \setminus \{v\} \end{cases}$$

$S_t^v(t_1+t_2) = S_t^v(t_1)+S_t^v(t_2)$ for $t_1, t_2 \in$ <term>
$S_t^v(t_1 \cdot t_2) = S_t^v(t_1) \cdot S_t^v(t_2)$ ——— // ———
$S_t^v(t_1=t_2) = S_t^v(t_1)=S_t^v(t_2)$ ——— // ———
$S_t^v(a \Rightarrow b) = S_t^v(a) \Rightarrow S_t^v(b)$ for $a,b \in$ <udsagn>

$S_t^v(a \vee b) = S_t^v(a) \vee S_t^v(b)$ for $a,b \in$ <udsagn>

$S_t^\forall(a \wedge b) = S_t^\forall(a) \wedge S_t^\forall(b)$ ——— ———

$S_t^\forall(\neg a) = \neg S_t^v(a)$ for $a \in$ <udsagn>

For $K \in \{\forall,\exists\}$, $x \in$ <variabel> og $a \in$ <udsagn> gælder

$$S_t^v(Kxa) = \begin{cases} Kxa & \text{for } x=v \\ KxS_t^v(a) & \text{for } x \notin \{v\} \cup F(t) \\ S_t^v(KyS_y^x(a)), & \text{hvor y er første variabel for hvilken } y \in \{v\} \cup F(t) \cup F(a), \text{ når } x \in F(t) \setminus \{v\}. \end{cases}$$

Den sidste lidt komplicerede regel er nødvendig for at udregne f.eks. $S^{x_1}_{x_1+x_2}(\exists x_2 x_1=x_2+x_2)$. Resultatet bliver $\exists x_3 x_1+x_2=x_3+x_3$, ikke $\exists x_2 x_1+x_2=x_2+x_2$.

Man fremhæver ofte en enkelt fri variabel x i et udsagn ved at skrive dette som $a(x)$, og $S_t^x(a(x))$ skrives da blot som $a(t)$.

Da $\forall x a(x)$ og $\exists x a(x)$ skal opfattes som en slags ubegrænsede konjunktioner og disjunktioner

$$a(t_1) \wedge a(t_2) \wedge \ldots \quad \text{og} \quad a(t_1) \vee a(t_2) \vee \ldots$$

er det naturligt at udvide definitionen af at u er en umiddelbar følge af Δ på side 21 til også at omfatte følgende tilfælde

(5) $\forall x a \in \Delta$ og u er $S_t^x(a)$ (5)' u er $\forall x a, a \in \Delta$ og x er vilk.

(6) $[\![$asu$]\!], \exists x a \in \Delta$ og x er vilkårlig (6)' u er $\exists x a$ og $S_t^x(a) \in \Delta$.

Her betyder forudsætningen om at x skal være vilkårlig, at når (5)' eller (6) benyttes til påvisning af at $\varkappa(\Gamma, sa)=1$, så må x ikke være fri i noget element i Γ. Denne vilkårlighed sikrer, at enhver term kunne have været substitueret i stedet for x, og at man derfor i virkeligheden har uendelig mange forudsætninger.

F.eks. kan følgende fire bevisstrenge bruges til at eftervise, at $\forall x a(x) \vdash \neg\exists y \neg a(y), \neg\exists y \neg a(y) \vdash \forall x a(x)$, $\exists x a(x) \vdash \neg\forall y \neg a(y)$ og $\neg\forall y \neg a(y) \vdash \exists x a(x)$. Nummeret på den benyttede slutningsregel er anført forneden til højre for udsagnene. Nummeret (4)'' angiver den svage form for indirekte bevis, der kan begrundes med, at hvis

$\varkappa(\Gamma,[\![us\neg u]\!])=1$, så gælder også $\varkappa(\Gamma,[\![\neg\neg u[\![\neg uu]\!]us\neg u]\!]\neg u)=1$.

$$\forall xa(x)[\![\exists y\neg a(y)\,[\![\neg a(y)\;a(y)_{(5)}\;\neg\exists y\neg a(y)_{(4)}]\!]\;\neg\exists y\neg a(y)_{(6)}]\!]\;\neg\exists y\neg a(y)_{(4)}\text{''}$$

$$\neg\exists y\neg a(y)\,[\![\neg a(x)\;\exists y\neg a(y)_{(6)}\text{'},a(x)_{(4)}]\!]\;a(x)_{(4)}\text{'},\quad \forall xa(x)_{(5)}\text{'}$$

$$\exists xa(x)\,[\![\forall y\neg a(y)[\![a(x)\;\neg a(x)_{(5)}\;\neg\forall y\neg a(y)_{(4)}]\!]\;\neg\forall y\neg a(y)_{(6)}]\!]\;\neg\forall y\neg a(y)_{(4)}\text{''}$$

$$\neg\forall y\neg a(y)[\![\neg\exists xa(x)[\![a(y)\;\exists xa(x)_{(6)}\text{'}\;\neg a(y)_{(4)}]\!]\;a(y)_{(4)}\text{''}\;\forall y\neg a(y)_{(5)}\text{'}\;\exists xa(x)_{(4)}]\!]\exists xa(x)_{(4)}\text{'}$$

Bemærk at man altså i den klassiske logik kan definere eksistenskvantoren ved hjælp af alkvantoren og omvendt, men at dette ikke gælder i den intuitionistiske logik. En analog bemærkning gælder selvfølgelig for disjunktionen og konjunktionen.

Vi vil ikke diskutere i detailler hvorledes konsekvensrelationen $\models$ kan defineres for 1.ordens logikken, men blot bemærke, at hver gang der er givet en mængde med elementer 0 og 1 og to kompositioner $+$ og $\cdot$, så får hvert afsluttet udsagn (d.v.s. uden frie variable) værdien "sand" eller "falsk", og $\Gamma\models u$ skal for afsluttede udsagn betyde, at u altid er sand, når alle udsagn fra Γ er sande. Da bliver $\Gamma\models u$ ensbetydende med $\Gamma\cup A\vdash u$, hvor A består af de 5 logiske aksiomer

$$\forall x_0\; x_0=x_0$$
$$\forall x_0\forall x_1\;(x_0=x_1\Rightarrow x_1=x_0)$$
$$\forall x_0\;\forall x_1\;\forall x_2(x_0=x_1\wedge x_1=x_2\Rightarrow x_0=x_2)$$
$$\forall x_0\;\forall x_1\;\forall x_2\;\forall x_3(x_0=x_1\wedge x_2=x_3\Rightarrow x_0+x_2=x_1+x_3)$$
$$\forall x_0\;\forall x_1\;\forall x_2\;\forall x_3(x_0=x_1\wedge x_2=x_3\Rightarrow x_0\cdot x_2=x_1\cdot x_3)$$

Det er sædvane at indbygge disse logiske aksiomer for lighedstegnet i følgerelationen $\vdash$, således at $\Gamma\vdash u$ betyder $\Gamma\cup A\vdash u$. D.v.s. at de logiske aksiomer uden videre kan anvendes i beviser.

15. Aksiomatisk talteori.

Vi supplerer nu vort formelle system bestående af slutningsreglerne (0)-(6),(1)'-(6)' og lighedsaksiomerne L1-L5 fra side 26 med aksiomerne

S1 $0+1=1$

S2 $\forall x_0 \neg\, x_0+1=0$

S3 $\forall x_0 \forall x_1 (x_0+1=x_1+1 \quad x_0=x_1)$

A1 $\forall x_0 \; x_0+0=x_0$

A2 $\forall x_0 \forall x_1 \; x_0+(x_1+1)=x_0+x_1+1$

M1 $\forall x_0 \; x_0 \cdot 0=0$

M2 $\forall x_0 \forall x_1 \; x_0 \cdot (x_1+1)=x_0 \cdot x_1+x_0$,

samt de uendelig mange induktionsaksiomer, der fremkommer ved at man for hvert udsagn $a(x_i)$ danner udsagnet

$$I_{a,i} \quad [a(0) \wedge \forall x_i (a(x_i) \Rightarrow a(x_i+1)) \Rightarrow \forall x_i a(x_i)] ,$$

hvor parenteserne [ ] angiver, at eventuelle frie variable skal bindes af alkvantorer, således at f.eks. $[\exists x_2 x_1+x_2=x_3]$ er $\forall x_1 \forall x_3 \exists x_2 \; x_1+x_2=x_3$.

I dette system kan man f.eks. bevise $\neg\, 0=1$ med følgende bevisstreng, der benytter aksiomerne S1 og S2:

1	$\forall x_0 \neg\, x_0+1=0$	S2
2	$\neg\, 0+1=0$	1(5)
3	$0+1=1$	S1
4	Antag $0=1$	
5	$\forall x_0 \forall x_1 (x_0=x_1 \quad x_1=x_0)$	L3
6	$\forall x_1 (0=x_1 \quad x_1=0)$	5(5)
7	$0=1 \Rightarrow 1=0$	6(5)
8	$1=0$	4,7(1)
9	$0+1=1 \wedge 1=0$	3,8(2)'
10	$\forall x_0 \forall x_1 \forall x_2 (x_0=x_1 \wedge x_1=x_2 \Rightarrow x_0=x_2)$	L3
11	$\forall x_1 \forall x_2 (0+1=x_1 \wedge x_1=x_2 \Rightarrow 0+1=x_2)$	10(5)
12	$\forall x_2 (0+1=1 \wedge 1=x_2 \Rightarrow 0+1=x_2)$	11(5)
13	$0+1=1 \wedge 1=0 \Rightarrow 0+1=0$	12(5)
14	$0+1=0$	9,13(1)'
15	$\neg\, 0=1$ ■	3,14(4)
16	$\neg\, 0=1$	4-15(4)"

Man ser at anvendelsen af lighedsaksiomerne kræver ret mange enkeltskridt. Disse vil vi udelade i de følgende bevisstrenge og kun markere dem som om der er brugt en enkelt slutningsregel L. Endvidere vil gentagen anvendelse af slutningsregel (5) blive markeret som en enkelt anvendelse.

Udsagnet $0\cdot 1=0$ kan bevises på følgende måde:

1	$0+1=1$	S1
2	$0+0=0$	A1(5)
3	$0\cdot 0=0$	M1(5)
4	$0\cdot(0+1)=0\cdot 0+0$	M2(5)
5	$0\cdot 1=0$	1,2,3,4L

Udsagnet x_0 $0+x_0=x_0$ kan kun bevises ved hjælp af et af induktionsaksiomerne:

1	$0+0=0 \wedge \forall x_0(0+x_0=x_0 \Rightarrow 0+(x_0+1)=x_0+1) \Rightarrow \forall x_0\ 0+x_0=x_0$	
2	$0+0=0$	A1(5)
3	Antag $0+x_0=x_0$	
4	$0+(x_0+1)=0+x_0+1$	A2(5)
5	$0+(x_0+1)=x_0+1$ ■	3,4L
6	$0+x_0=x_0 \Rightarrow 0+(x_0+1)=x_0+1$	3-4(1)'
7	$\forall x_0(0+x_0=x_0 \Rightarrow 0+(x_0+1)=x_0+1)$	6(5)'
8	$0+0=0 \wedge \forall x_0(0+x_0=x_0 \Rightarrow 0+(x_0+1)=x_0+1)$	2,7(2)'
9	$\forall x_0\ 0+x_0=x_0$	1,8(1)

Vi vil ikke her opskrive flere bevisstrenge, idet man lærer mest af selv at opskrive dem eller følge en gennemgang. En oplagt øvelse er at bevise de nedenfor givne udsagn, hvor vi for nemheds skyld har skrevet x,y,z,u,v i stedet for x_0,x_1,x_2,x_3,x_4. Rækkefølgen er væsentlig, da man mange gange skal benytte allerede beviste udsagn.

$\forall x\ 0\cdot x=x$

$\forall x(x=0 \vee \exists y\ x=y+1)$

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

$\forall x\ x+1=1+x$

$\forall x\forall y\ x+y=y+x$

$$\forall x \forall y \exists z (x+z=y \vee y+z=x)$$

Definer nu $t_1 \leq t_2$, hvor t_1 og t_2 er termer, som en forkortelse for $\exists v\ t_1+v=t_2$, hvor v er første variabel der ikke forekommer i hverken t_1 eller t_2.

$$\forall x(x \leq 0 \Rightarrow x=0)$$
$$\forall x \forall y(x \leq y+1 \Rightarrow x \leq y \vee x=y+1)$$
$$\forall x \forall y(\neg\, y=0 \Rightarrow x \leq x \cdot y)$$
$$\forall x \forall y \forall z\ x \cdot (y+z)=x \cdot y+x \cdot z$$
$$\forall x \forall y \forall z\ x \cdot y \cdot z=x \cdot (y \cdot z)$$
$$\forall x \forall y(x+1) \cdot y=x \cdot y+y$$
$$\forall x \forall y\ x \cdot y=y \cdot x$$

Definer nu $t_1<t_2$ som $t_1+1 \leq t_2$, $t_1>t_2$ som $t_2<t_1$ og $t_1 \geq t_2$ som $t_2 \leq t_1$. Definer endvidere $\forall x \leq t\ a(x)$ og $\exists x \leq t\ a(x)$ som $\forall x(x \leq t \Rightarrow a(x))$ og $\exists x(x \leq t \wedge a(x))$, og tilsvarende med $<$, $\geq$ og $>$. Udsagnene

$$b(0) \wedge \forall x(\forall y<x\ b(y) \Rightarrow b(x)) \Rightarrow \forall x b(x)$$

vises ved at anvende induktionsaksiomet med $\forall y<x\ b(y)$ som $a(x)$. Dette giver en noget kraftigere type induktionsaksiomer, som er nyttige enkelte steder i det følgende. Vi sigter nu direkte efter at vise Euklids sætning om eksistensen af uendeligt mange primtal.

$$\forall x \forall y(x \cdot y=1 \Rightarrow x=1 \wedge y=1)$$
$$\forall x \forall y(\neg\, x=1 \wedge \exists z\ x \cdot z=y \Rightarrow \neg \exists u\ x \cdot u=y+1)$$
$$\forall x \exists y \forall z \leq x \exists u\ z \cdot u=y$$

Definer $P(t)$ som $t>1 \wedge \forall u>1 \forall v>1\ \neg\, u \cdot v=t$, hvor u og v er de to første variable, der ikke forekommer i termen t.

$$\forall x>1(P(x) \vee \exists y \exists z(P(y) \wedge x=y \cdot z))$$
$$\forall x \exists y>x P(y)$$

Hvis nogen har lyst til mere af samme karakter kan de f.eks. prøve at udlede sætningen om at hvis et primtal er divisor i et produkt, så er det divisor i mindst en af faktorerne, altså

$$\forall x \forall y \forall z(P(z) \wedge \exists u\ z \cdot u=x \cdot y \Rightarrow \exists u\ z \cdot u=x \vee \exists u\ z \cdot u=y)\ .$$

16. Mængdelærens aksiomer.

Det er klart, at det er ret begrænset, hvor meget matematik man kan udvikle ved hjælp af det i §15 fremstillede system. Endvidere bliver behandlingen af en række emner besværliggjort ved at man f.eks. ikke (naturligt) kan tale om endelige mængder af naturlige tal.

Overraskende nok kan man lave et mindst lige så simpelt formelt system, som tillader fremstilling af praktisk talt al kendt matematik. Det drejer sig om mængdelæren, som vi her formulerer i en version meget lig den oprindeligt af Zermelo anvendte (han opererede dog ikke med en formel logik):

Vi benytter et formelt sprog med alfabet

$$\{\wedge, \Rightarrow, \vee, \neg, \forall, \exists, =, \in\} \cup \langle\text{variabel}\rangle$$

og mængden af udsagn defineret ved

$\langle$kvantor$\rangle$::= $\forall \mid \exists$

$\langle$atomisk udsagn$\rangle$::=$\langle$variabel$\rangle$=$\langle$variabel$\rangle$ | $\langle$variabel$\rangle\in\langle$variabel$\rangle$ | $\langle$kvantor$\rangle\langle$variabel$\rangle\langle$udsagn$_3\rangle$

I dette system bliver lighedsaksiomerne

L1 $\forall x\ x=x$

L2 $\forall x \forall y (x=y \Rightarrow y=x)$

L3 $\forall x \forall y \forall z\ (x=y \wedge y=z \Rightarrow x=z)$

L4 $\forall x \forall y \forall z \forall u (x=y \wedge z=u \wedge x\in z \Rightarrow y\in u)$

og med forkortelsen $a \Leftrightarrow b$ for $(a \Rightarrow b) \wedge (b \Rightarrow a)$ kan de ikke-logiske aksiomer formuleres således:

Z1	$\forall x \forall y (\forall z (z\in x \Leftrightarrow z\in y) \Rightarrow x=y)$	Ekstensionalitet
Z2	$\forall x \forall y \exists z \forall u (u\in z \Leftrightarrow u=x \vee u=y)$	Uordnet par
Z3	$\forall x \exists y \forall z (z\in y \Leftrightarrow \exists u (z\in u \wedge u\in x))$	Foreningsmængde
Z4	$\forall x \exists y \forall z (z\in y \Leftrightarrow \forall u (u\in z \Rightarrow u\in x))$	Potensmængde
Z5	$\exists x (\forall y (\forall z \neg z\in y \Rightarrow y\in x) \wedge \forall y (y\in x \Rightarrow \exists z (z\in x \wedge \forall u (u\in z \Rightarrow u=y))))$	Uendelighed
	$Z_{a(z)} [\forall x \exists y \forall z (z\in y \Leftrightarrow a(z) \wedge z\in x)]$	Komprehension

I komprehensionsaksiomet $Z_{a(z)}$ må y ikke være fri i $a(z)$.

Klammerne [ ] skal fortolkes på samme måde i komprehensionsaksiomskemaet som i induktionsaksiomskemaet på side 27.

Dette aksiomsystem er tilstrækkeligt til at definere 0 som den tomme mængde ved hjælp af $Z_{\neg z=z}$, og $\mathbb{N}_0$ som fællesmængden af alle mængder, der indeholder 0 som element og er afsluttet overfor operationen $x \rightsquigarrow \{x\}$. D.v.s. at de naturlige tal bliver 0 , $\{0\}$,... . Ordnede par (x,y) defineres som $\{\{x\},\{x,y\}\}$, hvorefter funktioner, rationale tal, reelle tal, etc. kan defineres på sædvalig vis.

I videregående matematik må aksiomsystemet suppleres med udvalgsaksiomet, der siger at der for enhver mængde x findes en funktion f, så $f(y) \in y$ for alle ikke-tomme y i x, samt substitutionsaksiomet, der sikrer, at hvis $a(x,y)$ er et udsagn med den egenskab, at der til hvert x findes netop ét y så $a(x,y)$ er opfyldt, så definerer $a(x,y)$ en mængdeteoretisk funktion (en mængde af ordnede par) på enhver mængde.

17. Bemærkelsesværdige metamatematiske resultater.

Når man har præcist formulerede formelle systemer som de tidligere omtalte, så kan man betragte disse som matematiske objekter. Man kan f.eks. spørge om et system er fuldstændigt, d.v.s. om det for ethvert afsluttet udsagn a gælder, at enten a eller $\neg$ a kan bevises; man kan spørge om det er konsistent, d.v.s. om det er sikkert, at man ikke kan udlede både a og $\neg$ a for et eller andet (og dermed alle) udsagn a; man kan spørge om systemet er afgørligt, d.v.s. om det rent algoritmisk kan afgøres om et udsagn a kan bevises. Disse spørgsmål blev stort set afklaret i løbet af 1930'erne i det væsentlige takket være Gödel. Der viser sig at være en snæver forbindelse mellem fuldstændighed, konsistens og afgørlighed. Hovedresultaterne er følgende:

For systemerne i §15 og §16 gælder, at hvis de er konsistente, så er de ufuldstændige, og de kan ikke gøres

fuldstændige ved tilføjelse af nye aksiomer, når man kræver at det algoritmisk skal kunne lade sig gøre at afgøre hvad der er et aksiom (og det er jo nødvendigt, hvis man algoritmisk skal kunne afgøre om et bevis er korrekt, hvilket er et rimeligt forlangende).

For de talteoretiske og mængdeteoretiske systemer gælder, at danner man et udsagn, der siger at systemet er konsistent (det kan f.eks. ske ved en passende nummerering af symbolstrenge), så kan dette udsagn ikke bevises i systemet selv (under forudsætning af konsistens). Man kan naturligvis tilføje udsagnet som et nyt aksiom, men så kan processen gentages, o.s.v.

Endvidere er systemerne uafgørlige. Ellers kunne man jo udvide aksiomsystemerne til fuldstændige, afgørlige aksiomsystemer ved at nummerere de afsluttede udsagn og tilføje dem ét efter ét, såfremt konsistensen bevares.

Som et andet interessant metamatematisk resultat kan nævnes, at man intuitionistisk kan vise, at hvis det talteoretiske system i §15 er konsistent, når man kun tillader brug af den svage form for indirekte bevis, så er det også konsistent, når man tillader brug af den stærke form for indirekte bevis. Man opnår altså ikke større garanti for konsistens ved at afholde sig fra den stærke form for indirekte beviser.

18. Diskussionsemner.

Det stof vi har været igennem kan benyttes som baggrund for en diskussion af følgende emner:

(1) Drejer matematik sig udelukkende om deduktion fra aksiomer?
(2) Hvad vil det sige at lære at tænke?
(3) Kan matematik lære én at tænke?
(4) Hvordan anvender man matematik?
(5) Bør matematik fremstilles aksiomatisk i skolen?
(6) Hvad er egentlig motiveringen for "the new math."?
(7) Kan kendskab til logik udnyttes til at forenkle matematikundervisningen?