UNIVERSITETET I OSLO
Institutt for informatikk

Frste ordens teorier og grunnleggende rekursjonsteori

Lars Kristiansen

Kompendium 66

2. utgave (1998)

Forord

Kompendiet du har mellom hendene er forhåpentligvis dømt til et kort liv. Meningen er at det skal absorberes av et mer omfattende kompendium som Herman Ruge Jervell og undertegnede arbeider med. Forfatteren vil ikke bruke for mye tid på å finpusse denne ytterst midlertidige presentasjonen av stoffet. Derfor er kompendiet ufullendt i visse henseende. For det første er oppgavestoffet noe vilkårlig. Det er lite gjennomtenkt. For det andre er teksten blottet for referanser til annen litteratur. For det tredje kommer første kapittel noe "brått på" leseren. Den andre og tredje svakheten har jeg forsøkt å bøte på med enkle midler. Jeg har lagt til et lite kapittel helt til slutt hvor det gis noen viktige referanser, og i en liten innledning hinter jeg om hva leseren bør være fortrolig med før han eller hun tar fatt på første kapittel.

... og på tross av alt dette, mener jeg bestemt at kompendiet er en rimelig ferdig og selvstendig enhet. Det gir en historie om klassiske resultater i matematisk logikk. Det dreier seg blant annet om kompletthet, kompakthet, ikke-standard modeller, elementært ekvivalente teorier, primitivt rekursive funksjoner, rekursive funksjoner, rekursive og rekursivt tellbare mengder, Churchs-Turings tese og mye mer. Utgangspunktet er noen løse betraktninger rundt matematikk og første ordens teorier. Derfra driver et naturlig hendelsesforløp historien fram til en like naturlig slutt: ufullstendighets- og uavgjørbarhetsresultater. Enhver med grunnleggende kunnskap om formell logikk vil ha forutsetning for å lese kompendiet. Jeg tror mange databehandlere kan ha utbytte av å lese det.

Vuokko Helena Caseiro, Jo Erskine Hannay og Geir Kirkebøen har lest korrextur, å hjelpt meg med sproget og presentasjonen av stoffet. Det er flere en meg som bør takke dem, og det er fint om andre fortsetter arbeidet disse tre har begynt på. Si i fra om du finner noe i kompendiet som bør rettes på eller forandres. Den elektroniske postadressen min er larsk@ifi.uio.no. Ingen feil er for liten til å rettes opp!

Lars Kristiansen
Institutt for informatikk
Universitetet i Oslo
Oslo, november 1995

Forord til andre utgave

Den andre utgaven er ikke dramatisk forskjellig fra den første. En del mindre feil er rettet opp. (Ja, ja, ... vi kan kanskje snakke om en eller to *store* feil også.) Dessuten er kompendiet utvidet med litt historisk stoff om Church-Turings tese.

Lars Kristiansen
Matematisk institutt
Universitetet i Oslo
Oslo, januar 1998

Hva kreves av leseren?

Kurt Gödel viste i 1929 at

Teorem 0.1 *Det finnes et formelt bevissystem T som er slik at et første ordens utsagn A er sant i enhver modeller hvis og bare hvis A kan utledes i T.*

Dette er kompletthetsteoremet for første ordens logikk. Man bør ha en god forståelse av teoremet før man gir seg i kast med dette kompendiet. Ideelt sett bør man også kjenne til tremetoden. (Tremetoden er et formelt bevissystem.) Skulle tremetoden være en fremmed, kan man likevel ha tilnærmet fullt utbytte av kompendiet hvis man er kjent med et annet formelt bevissystem, det være seg et Frege-Hilbert-system, et sekventkalkylesystem eller et system basert på naturlig deduksjon. Det viktigste er at leseren er seg bevisst slike systemers syntaktiske karakter. Videre bør man ha god trening i å tolke og manipulere formelle logiske uttrykk, og sammenhenger som

Teorem 0.2 *La $A_1, \ldots, A_n$ og B være lukkede første ordens utsagn. Følgende tre påstander er ekvivalente. (i) Mengden $\{A_1, \ldots, A_n, \neg B\}$ er ikke tilfredsstillbar. (ii) B følger logisk fra $A_1, \ldots, A_n$ (dvs. B er sann i enhver modell for $A_1, \ldots, A_n$). (iii) $A_1 \wedge A_2 \wedge \ldots \wedge A_n \rightarrow B$ er gyldig (dvs. sant i alle modeller).*

regner jeg også med at leserne er innforstått med. En mindre sentral og mer teknisk sak man bør ha hørt om er Π_i^0-utsagn, Σ_i^0-utsagn og Δ_i^0-utsagn.

- Et kvantorfritt første ordens utsagn er på Π_0^0-form, Σ_0^0-form og Δ_0^0-form.
- La A være et utsagn på Σ_n^0-form og la B være et utsagn på formen $\forall x_1 \ldots \forall x_n\, A$. Da er B et utsagn på Π_{n+1}^0-form.
- La A være et utsagn på Π_n^0-form og la B være et utsagn på formen $\exists x_1 \ldots \exists x_n\, A$. Da er B et utsagn på Σ_{n+1}^0-form.
- Et Π_i^0-*utsagn* er et utsagn som er ekvivalent med et utsagn på Π_i^0-form.
- Et Σ_i^0-*utsagn* er et utsagn som er ekvivalent med et utsagn på Σ_i^0-form.
- Et Δ_i^0-*utsagn* er et utsagn som både er ekvivalent med et Π_i^0-utsagn og med et Σ_i^0-utsagn.

Vi skal se på et par enkle ekspempler. La $P(x, y)$ og $Q(x, y)$ være kvantorfrie utsagn. Da er utsagnet $(\exists x)(\forall y)[P(x, y)] \wedge (\exists x)(\forall y)[Q(x, y)]$ et Σ_2^0-utsagn siden det er ekvivalent med utsagnet $(\exists x)(\exists u)(\forall y)(\forall v)[P(x, y) \wedge Q(u, v)]$. Utsagnet $(\exists x)[P(x)] \wedge (\forall x)[Q(x)]$ er et Δ_2^0-utsagn siden det er ekvivalent med både $(\exists x)(\forall y)[P(x) \wedge Q(y)]$ og $(\forall y)(\exists x)[P(x) \wedge Q(y)]$.

Innhold

Kapittel 1

Kompletthet og kompakthet

1.1 Innledning

1.1.1 Tallteori

Primært er vi ikke opptatt av hva som er sant i alle mulige strukturer. Vanligvis ikke. Vanligvis interesserer vi oss for en bestemt struktur. Når en skolelærer forteller elevene at $(x/y)/(u/v) = (x \times v)/(y \times u)$ holder for alle x, y, u, v, så har han en bestemt struktur i tankene, nemlig en struktur der universet er de rasjonale tallene og hvor / og $\times$ tolkes på en bestemt måte. Forteller vi leseren at

$$(\forall x, y)[\,(\exists z)[0 \leq z \ \wedge \ x + z \leq y \ \wedge \ y + z \leq x] \ \rightarrow \ x = y\,]$$

så vil han eller hun kanskje nikke og si til seg selv at slik må det være. Da har leseren hatt en bestemt struktur i bakhodet. Utsagnet holder jo opplagt ikke i enhver første ordens struktur. Matematikk dreier seg vanligvis om bestemte strukturer. Tallteori er en disiplin de fleste er en smule fortrolig med. Universet er de naturlige tallene $\mathbf{N} = \{0, 1, 2, \ldots\}$, og

(1) Det finnes uendelig mange primtall

(2) Det finnes uendelig mange x, y, z slik at $x^2 + y^2 = z^2$.[1]

er eksempler på tallteoretiske påstander. Mange av leserne vil være i stand til å vise den første påstanden. Langt færre vil være i stand til å vise den andre, men det vil ikke være noen sensasjon om noen gjør det. Teoremet ble vist allerede i antikken. Den tallteoretiske påstanden

(3) Ligningen $x^n + y^n = z^n$ har ingen løsninger når $n > 2$ og $x, y, z > 0$.

er kjent under navnet Fermats gjetning. I over 300 år levde man i uvisshet om hvorvidt dette var sant. Det ble nylig bevist at gjetningen holder. De to tallteoretiske påstandene

(4) Ethvert partall kan skrives som summen av to primtall.

(5) Det finnes uendelig mange tvillingprimtall.[2]

[1] Ligninger av denne typen kalles diophantiske ligninger.

[2] Tvillingprimtall er primtallspar av typen $\langle 11, 13\rangle$, $\langle 17, 19\rangle$ og $\langle 29, 31\rangle$.

har man tross store anstrengelser aldri klart å bevise (eller motbevise). Vi forsøker nå å fortelle leseren, hvis han/hun mot formodning ikke allerede skulle vite det, at tallteori slett ikke er trivielt. Så langt der i fra.

La oss se på et språk som i tillegg til de første ordens logiske symbolene består av de ikke-logiske symbolene $+, \times, S$ og 0. Så tenker vi oss en modell $\mathcal{N}$ for dette språket hvor de ikke-logiske symbolene tolkes på den indikerte måten, dvs. det binære funksjonssymbolet $+$ tolkes som addisjonsfunksjonen, det binære funksjonssymbolet $\times$ tolkes som multiplikasjonsfunksjonen, det unære funksjonssymbolet S tolkes som etterfølgerfunksjonen og navnet 0 tolkes som tallet 0. Universet til $\mathcal{N}$ er de naturlige tallene. Dette ytterst begrensede språket har en uventet sterk uttrykkskraft. Det er nær sagt ingen grenser for hvilke første ordens utsagn om de hele tallene vi er i stand til å uttrykke ved dette utvalget av funksjoner og navn. Dette vil presiseres senere. La oss i første omgang se hvordan påstand (1) over kan uttrykkes. Utsagnet $(\forall z_1, z_2)[S(S(z_1)) \times S(S(z_2)) \neq y]$ uttrykker at y er et primtall. Utsagnet $(\exists z_3)[x + S(z_3) = y]$ uttrykker at x er ekte mindre enn y. Dermed kan (1) uttrykkes ved

$$(\forall x)(\exists y)\,[\,(\exists z_3)[x + S(z_3) = y] \;\wedge\; (\forall z_1, z_2)[S(S(z_1)) \times S(S(z_2)) \neq y]\,]\,. \quad (*)$$

Litt mer presist, – uttrykket (*) er sant i strukturen $\mathcal{N}$ hvis og bare hvis det finnes uendelig mange primtall. Påstandene (2), (3), (4) og (5) kan også uttrykkes ved det aktuelle språket i modellen $\mathcal{N}$. Så å avgjøre hvorvidt et utsagn holder i modellen $\mathcal{N}$ er slett ikke trivielt. Så langt der i fra.

1.1.2 Et fundament for tallteori

Engelskmannen Wiles har æren for beviset av Fermats gjetning. Han la fram et bevis på vårparten 1993. Mange mente at dette beviset ikke holdt mål. De så "hull" i resonnementene. Men beviset har blitt verifisert, og i dag, – et par år senere, er alle autoriteter skjønt enige om at vi har et all right bevis for at Fermats gjetning holder. På nittensyttitallet oppdaget man underligheter i arbeider av Herbrand[3]. Det viste seg at franskmannen rett og slett hadde "bevist" flere gale lemmaer. Tabbene hans var så subtile at de ble spredt gjennom journaler og andre akademiske kanaler i over 40 år uten å bli oppdaget. (De viktige teoremene Herbrand beviser ved hjelp av disse lemmaene er heldigvis korrekte. Hullene i Herbrands ressonementer ble forøvrig tettet av Stål Aanderaa[4].) I ettertid er det lett å se at Herbrands opprinnelige beviser må være gale, men det finnes flerfoldige andre eksempler på at man ikke kan enes om hvorvidt et bevis holder mål eller ikke. Situasjonen er uvanlig, men den forekommer. En autoritet sier ja, – en annen autoritet sier nei. Ja, det oppstod faktisk en betydelig skoleretning rundt århundreskiftet som avskrev vesentlige deler av klassisk matematikk. Tilhengere av denne retningen kalles intuisjonister eller konstruktivister, og setter strengere krav til et bevis enn det en klassisk matematiker gjør.

Disse kommentarene viser at matematikken, som enhver annen vitenskap, sliter med grunnlagsproblemer. Eksemplene over illustrerer det. Hva er kriteriet for at noe kan kalles et bevis? Hvordan skal en matematiker bære seg ad for å unngå å gjøre tabber? Hvilke påstander er trivielle og hvilke krever en begrunnelse? Når følger en påstand fra andre påstander? Og så videre. I slutten av forrige århundre og i begynnelsen av vårt eget var slike fundamentale

[3] Jacques Herbrand (uttales "ærbra"), fransk matematiker, 1908-1931.

[4] Stål Aanderaa, norsk matematiker, født 1931.

problemer særdeles presserende. Spesielt var man opptatt av konsistensspørsmålet. På attenhundretallet begynner man å aksiomatisere matematikken og oppdager muligheten av ikke-euklidsk geometri. Det er i kjølvannet av denne utviklingen at konsistensspørsmålet dukker opp. Hvordan kan man vite med sikkerhet at et sett aksiomer ikke er selvmotsigende? Og rundt århundreskiftet dukker faktisk en uventet selvmotsigelse opp i mengdelære, nemlig Russels[5] paradoks. Krisestemning. Utviklingen av formell logikk starter med Frege[6] i 1879. Den kulminerer på nittentredvetallet med Gödel[7] og Turing[8]. Drivkraften bak utviklingen er hele tiden et ønske om få bukt med matematikkens grunnlagsproblemer.

La oss se nærmere på muligheten for å danne et fundament for tallteori ved hjelp av formalisert logikk. La oss fantasere om et scenario der de grunnleggende problemene ved tallteori er fordrevet ved hjelp av logikkens metoder og redskaper. Det var et lignende scenario noen av logikkens pionérer, for eksempel den famøse Hilbert[9], drømte om (Hilberts program). Vi starter med en definisjon for å presisere hva som menes med tallteori og sannhet i forbindelse med tallteori.

Definisjon. Tallteorispråket er et første ordens språk med liket, med navnet 0, den unære funksjonen S (etterfølger) og de to binære funksjonene $+, \times$. Vi betegner den intenderte modellen (strukturen) for tallteorispråket med $\mathcal{N}$, dvs. modellen hvor universet er mengden $\mathbf{N}$, dvs. de naturlige tallene $0, 1, 2, \ldots$, og hvor $+$ tolkes som addisjon, hvor $\times$ tolkes som multiplikasjon, hvor $S(x)$ tolkes som etterfølgeren til x og navnet 0 tolkes som tallet 0. □

Et tallteoretisk utsagn er altså et utsagn i et begrenset språk, og et utsagn A i dette språket er sant om $\mathcal{N} \models A$. (Vi har allerede påpekt at det nevnte språket har en uventet stor uttrykkskraft og at det for eksempel kan uttrykke påstandene (1), (2), (3), (4) og (5) over. Likevel vil kanskje noen mene at tallteorien inneholder langt mer enn hva den her er definert til å inneholde. Det kan så være. Spiller ingen rolle. Poenget er at det vår definisjon avgrenser som tallteori med rimelighet kan sees som en del av den uformaliserte matematiske disiplinen vi alle kjenner.) En tallteoretikers oppgave er per definisjon å finne ut hvilke utsagn som holder i strukturen $\mathcal{N}$, men hvordan skal tallteoretikeren bevise at det for et gitt utsagn A er slik at $\mathcal{N} \models A$? Her er et forslag til et fundament for en tallteoretikers virke: Vi setter opp aksiomer.

$$
\begin{aligned}
&(P_1) \qquad (\forall x)\,[\,0 \neq S(x)\,] \\
&(P_2) \qquad (\forall x, y)\,[\,S(x) = S(y) \rightarrow x = y\,] \\
&(P_3) \qquad (\forall x)\,[\,x + 0 = x\,] \\
&(P_4) \qquad (\forall x, y)\,[\,x + S(y) = S(x + y)\,] \\
&(P_5) \qquad (\forall x)\,[\,x \times 0 = 0\,] \\
&(P_6) \qquad (\forall x, y)\,[\,x \times S(y) = (x \times y) + x\,] \\
&(P_7) \qquad (A(0) \wedge (\forall x)[A(x) \rightarrow A(S(x))]) \;\rightarrow\; (\forall x)[A(x)]
\end{aligned}
$$

Dette er Peanos[10] aksiomer (Peano-aritmetikk). (Legg merke til at P_7 er et aksiomskjema som angir uendelig mange aksiomer. Man får en instans av P_7 ved å bytte ut A med et

[5] Bertrand Russel, engelsk filosof og matematiker, 1872-1970.

[6] Gottlob Frege, tysk filosof og matematiker, 1848-1925.

[7] Kurt Gödel, amerikansk matematiker, 1906-1978. Født i Brno i det nåværende Tsjekkia. Emigrerte til USA i 1938.

[8] Alan M. Turing, engelsk matematiker, 1912-1953.

[9] David Hilbert, tysk matematiker, 1862-1943.

[10] Giuseppe Peano, italiensk matematiker, 1858-1932.

utsagn i tallteorispråket som har en fri variabel. Skjemaet kalles av innlysende årsaker for induksjonsaksiomet.) Ved hjelp av tremetoden, eller et annet bevissystem, kan utsagn i tallteorispråket utledes fra Peanos aksiomer. Tenk om, tenk om, tenk om. Tenk om vi kunne utlede ethvert utsagn som var sant i modellen $\mathcal{N}$, og at det var umulige å utlede utsagn som er usanne i modellen $\mathcal{N}$. Tenk hvilket fundament vi da hadde hatt for tallteori. Hvorvidt et bevis foreligger vil være et spørsmål om syntaks. Det vil ikke være rom for diskusjon blant seende mennesker om noe er bevist eller ikke. Til og med en datamaskin kan avgjøre det spørsmålet. Tenk videre om vi kunne vise med *enkle midler* at det ikke finnes et utsagn A slik at både A og $\neg A$ kan utledes fra Peanos aksiomer. Da hadde vi hatt et bevis for at tallteorien er konsistent. Det er viktig at et slikt bevis kan gjennomføres med enkle metoder. Bruker man for avanserte metoder i beviset, så kan det tenkes at man bruker metoder som er inkonsistente. Dermed blir ikke beviset mye verdt. Man må ikke bruke metoder hvis konsistens er mer tvilsom enn den tallteorien man viser konsistens av. Likevel kan det se ut som prosjektet lar seg gjennomføre. Det virker ikke som man skulle trenge så veldig avansert matematikk for å vise at det ikke finnes A slik at både A og $\neg A$ kan utledes. Videre kunne vi forsøke å vise at alle aksiomene til Peano er uavhengige av hverandre. Det vil si at ingen av aksiomene kan utledes fra de øvrige. Hvis et aksiom kan utledes fra de øvrige, er jo aksiomet overflødig. Vi kan også studere hvilke modeller aksiomene holder i. Er det slik at $\mathcal{N}$ er den eneste modellen hvor alle aksiomene holder?

Siste avsnitt gir en røff og anakronistisk skisse av Hilberts program. I dette kompendiet skal vi se at programmet er et fantasifoster. Det lar seg stort sett ikke gjennomføre. Likevel er ikke formell logikk en fiasko qua matematisk grunnlagsdisiplin. Logikken gir en meget verdifull analyse av grunnlaget for matematikk og all annen eksakt tenkning. Dessuten anvendes jo formell logikk innenfor utallige områder. Vi kan nevne vidt forskjellige domener som programverifikasjon, kognitiv psykologi, kunstig intelligens, analytisk filosofi, analyse av naturlige språk osv., osv. Ja, datamaskinen er et biprodukt av rent teoretiske problemstillinger innenfor logikk. Alt snakket om grunnlagsproblemer og tallteori har til hensikt å motivere leseren. Det har til hensikt å yte miljø og omgivelser for å presentere de mer tørre og tekniske sidene av stoffet. Kompendiet er slett ikke myntet på folk som er spesielt interessert i slike tema. Tvert i mot. Vi forsøker å spre grunnleggende kunnskap, – kunnskap som er av interesse for enhver som i en eller annen forstand beskjeftiger seg med formell logikk.

1.1.3 Andre typer teorier og Robinsons aksiomer

Det meste vi til nå har sagt om tallteori, kan sies om andre typer teorier. I mange henseende er det intet spesielt ved tallteori. Vi kan ha første ordens teorier om rasjonale tall, om geometri, om grafer med noder og kanter, om Turingmaskiner osv. Mengdelære er særs interessant i så måte. Omtrent all annen kjent matematikk kan avbildes i mengdelæren. Med dette mener vi at for enhver matematisk påstand P så kan man finne en påstand P' i mengdelære som er slik at P' er sann hvis og bare hvis P er sann. All matematikk kan med andre ord reduseres til mengdelære. Dermed blir studiet av aksiomer for mengdelæren et studium av aksiomer for matematikk overhodet. Det mest berømte aksiomsettet for mengdelæren heter ZF (Zermelo[11]-Frankel). I dette kompendiet vil vi primært jobbe med Robinsons[12]

[11] Ernst Friedrich Ferdinand Zermelo, tysk matematiker, 1871-1953

[12] Raphael Mitchel Robinson, amerikansk matematiker, 1911-1995. Ikke forveksl ham med Julia Robinson (kona) eller Abraham Robinson.

aksiomer for tallteori. Dette er til en viss grad et vilkårlig valg. For å understreke dette skal vi også arbeide litt med en teori om binære sekvenser, og vi vil illustrere hvordan resultater om tallteori lar seg overføre til denne teorien. Dette hjelper forhåpentligvis leseren til å innse at resultatene lar seg generalisere til alle mulige typer av matematiske teorier. La oss nå se nærmere på teorien om binære sekvenser og et aksiomsett for denne teorien. Men først, noe vi har glemt ... Robinsons aksiomer:

$$
\begin{aligned}
&(R_1) \quad (\forall x, y)\,[\, S(x) = S(y) \rightarrow x = y \,] \\
&(R_2) \quad (\forall x)\,[\, x \neq 0 \;\rightarrow\; (\exists y)[x = S(y)] \,] \\
&(R_3) \quad (\forall x)\,[\, 0 \neq S(x) \,] \\
&(R_4) \quad (\forall x)\,[\, x + 0 = x \,] \\
&(R_5) \quad (\forall x, y)\,[\, x + S(y) = S(x + y) \,] \\
&(R_6) \quad (\forall x)\,[\, x \times 0 = 0 \,] \\
&(R_7) \quad (\forall x, y)\,[\, x \times S(y) = (x \times y) + x \,]
\end{aligned}
$$

1.1.4 Teorien om binære sekvenser: bitteori

En sekvens av 0'er og 1'ere kalles en *bitsekvens*. Vi lar ε stå for den tomme sekvensen, og vi lar $\bullet$ være den binære sammenlenkingsoperatoren på bitsekvenser. Vi har for eksempel at $0111 \bullet 00 = 011100$ og at $101 \bullet 010 = 101010$. Vi har $\varepsilon \bullet \alpha = \alpha \bullet \varepsilon = \alpha$ for alle bitsekvenser α. (Vi bruker små greske bokstaver for variabler som rangerer over bitsekvenser.)

Bitteorispråket er et første ordens språk med likhet og følgende ikke-logiske symboler:

- ett navn e
- to unære funksjonssymboler S_0, S_1
- ett binært funksjonssymbol $\circ$ (som vi skriver infiks)

Vi skal beskrive en struktur $\mathcal{B}$ for dette språket. Grunnmengden til $\mathcal{B}$ er

$$|\,\mathcal{B}\,| \;=\; \{\alpha \mid \alpha \text{ er en bitsekvens}\} \;=\; \{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, \ldots\}$$

Videre har vi

$$\mathcal{B}(e) = \varepsilon \qquad \mathcal{B}(S_0)(\alpha) = 0 \bullet \alpha \qquad \mathcal{B}(S_1)(\alpha) = 1 \bullet \alpha \qquad \alpha\ \mathcal{B}(\circ)\ \beta \;=\; \alpha \bullet \beta$$

La B være en første ordens teori for bitteorispråket, og la B ha følgende (ikke-logiske) aksiomer:

$$
\begin{aligned}
&(B_1) \quad (\forall x)\,[x \neq e \;\rightarrow\; (\exists y)[x = S_0(y) \,\vee\, x = S_1(y)]] \\
&(B_2) \quad (\forall xy)\,[x \neq y \;\rightarrow\; S_0(x) \neq S_0(y) \,\wedge\, S_1(x) \neq S_1(y)] \\
&(B_3) \quad (\forall xy)\,[S_0(x) \neq S_1(y) \,\wedge\, S_1(x) \neq S_0(y)] \\
&(B_4) \quad (\forall y)\,[e \circ y = y] \\
&(B_5) \quad (\forall xy)\,[S_0(x) \circ y = S_0(x \circ y)] \\
&(B_6) \quad (\forall xy)\,[S_1(x) \circ y = S_1(x \circ y)]
\end{aligned}
$$

Det er lett å se at alle aksiomene i B holder i strukturen $\mathcal{B}$.

1.2 Kompletthet og kompakthet

Definisjon. La $\models A$ bety at A er gyldig, dvs. at A er sann i alle modeller. La $\vdash A$ bety at treet over A er lukket. Hvis vi sier at A *er bevisbar*, så mener vi $\vdash A$.

Vi definerer en *første ordens teori* T. En slik teori består av et endelig antall aksiomer $A_1, A_2, \ldots A_n$. (Det som her kalles aksiomer kalles ofte *ikke-logiske* aksiomer i andre sammenhenger.) Et aksiom A_i kan være et aksiomskjema, dvs. at A_i formelt sett har en uendelig konjunksjon som ytterste konnektiv. La B være et første ordens utsagn. Vi definerer

$$T \vdash B \quad \stackrel{\text{def}}{\Leftrightarrow} \quad \vdash A_1 \wedge \cdots \wedge A_n \rightarrow B$$

der $A_1, \ldots, A_n$ er aksiomene i T. Om $T \vdash B$ så kan vi for eksempel si at B *kan utledes i* T eller at B *er bevisbar i* T. Notasjonen $T \nvdash B$ betyr at B ikke kan utledes i T.

Hvis vi ikke eksplisitt gir uttrykk for noe annet, så skal vi i det følgende ta det for gitt at vi har rekursiv kontroll over aksiomskjemaene våre, dvs. vi antar at det finnes en algoritme for å generere den n'te konjunkten i en uendelig konjunksjon. (Noen av resultatene våre vil holde uten denne forutsetningen. Andre vil ikke holde.) Det betyr at vi for eksempel ser bort fra teorier med overtellbart mange aksiomer. Vi ser også bort fra teorier hvor enhver sannhet i første ordens tallteori er et aksiom, siden det ikke finnes noen algoritme for å liste opp alle slike utsagn.

En teori T er *endelig* om T er fri for aksiomskjemaer. En teori T_1 er en *delteori* av en teori T_2 om ethvert aksiom i T_1 kan utledes i T_2. Hvis T_1 er en delteori av T_2, så er T_2 en *utvidelse* av T_1.

En modell $\mathfrak{M}$ er en *modell for teorien* T dersom alle aksiomene i T er sanne i $\mathfrak{M}$. Notasjon: $\mathfrak{M} \models T$. Hvis A er et utsagn, så betyr $\mathfrak{M} \models A$ at utsagnet A holder i modellen $\mathfrak{M}$. Ordet *struktur* brukes synonymt med *modell*.

Et utsagn B *følger logisk* fra en teori T om B er sann i alle modeller for T. Vi bruker notasjonen $T \models B$ for å beskrive at det er slik, og $T \not\models B$ for å beskrive at det ikke er slik.

En teori T er *inkonsistent* om $T \vdash \bot$. En teori T er *konsistent* dersom den ikke er inkonsistent. □

Med vår nye notasjon kan kompletthetsteoremet (0.1) formuleres

$$\vdash A \text{ hvis og bare hvis } \models A\,.$$

Vi har også

Teorem 1.1 (Kompletthet) *$T \vdash A$ hvis og bare hvis $T \models A$.*

Bevis av Teorem 1.1. Enkel oppgave. □

Dette siste teoremet er Gödels opprinnelige formulering av kompletthetsteoremet for første ordens logikk. En annen formulering av teoremet er

Teorem 1.2 (Kompletthet) *Teorien T har en modell hvis og bare hvis T er konsistent.*

Dette kalles Henkins kompletthetsteorem, og vi skal se at det følger ganske lett fra Teorem 1.1. Henkins opprinnelig bevis av teoremet er viden berømt, men det vanlige beviset for kompletthet av tremetoden gir innsikter det er vanskelig å lese ut av Henkins bevis.

Bevis av Teorem 1.2. Vi viser at T er inkonsistent hvis og bare hvis T ikke har en modell. La $A_1, \ldots, A_n$ være aksiomene i T.

$$
\begin{array}{cl}
\{A_1, \ldots, A_n\} \text{ har ikke en modell} & \\
\Updownarrow & \\
\{A_1, \ldots, A_n, \neg\bot\} \text{ har ikke en modell} & \\
\Updownarrow & \text{Teorem 0.2} \\
\bot \text{ følger logisk fra } A_1, \ldots, A_n & \\
\Updownarrow & \text{def. av } \models \\
T \models \bot & \\
\Updownarrow & \text{Teorem 1.1} \\
T \vdash \bot & \\
\Updownarrow & \text{def. av inkonsistens} \\
T \text{ er inkonsistent.} & \square
\end{array}
$$

Tradisjonens språkbruk er forvirrende. La oss rydde opp litt. Dette betyr det samme:

- ... har en modell ...
- ... har en tolkning ...
- ... kan tolkes til sann ...
- ... er tilfredsstillbar ....

Dette betyr det samme:

- ... er en (logisk) selvmotsigelse ...
- ... er utilfredsstillbar ...
- ... er en kontradiksjon ...
- ... har ingen modell ....

Og dette betyr det samme:

- ... er gyldig ...
- ... er logisk sann ....

Vi kan oppsummere de to kompletthetsteoremene våre ved følgende blide:

Tilfredsstillbare			⟷⇔ Semantiske begrep
Gyldige		Selvmotsigelser	
$p \vee \neg p$	p	$p \wedge \neg p$	
$p \to p$	$p \wedge q$	$\neg\neg p \wedge \neg p$	
$\forall x \mid x = x$	$\forall x \mid Rx$	$\exists x \mid x \neq x$	
$\vdots$	$\vdots$	$\vdots$	
$\vdots$	$\vdots$	$\vdots$	
Bevisbare		Inkonsistente	
Konsistente			⟷⇔ Syntaktiske begrep

Teorem 1.3 (Kompakthet) *Teorien T har en modell hvis og bare hvis enhver endelig delteori av T har en modell.*

Bevis av Teorem 1.3. La $A_1, \ldots, A_n$ være aksiomene i T. Hvis $T \vdash C$, så må det finnes en endelig delteori T' av T slik at $T' \vdash C$. Dette er trivielt. I utledningen av C fra aksiomene i T har vi kun brukt endelig mange instanser av eventuelle aksiomskjema i T. (Mer formelt, i et lukket analysetre over $A_1 \wedge \ldots \wedge A_n \to C$ har vi kun analysert en uendelig disjunksjon endelig mange ganger.) Dermed – vi viser teoremet kontrapositivt –

T har ikke en modell	
$\Updownarrow$	Teorem 1.2
T er inkonsistent	
$\Updownarrow$	def. av inkonsistens
$T \vdash \bot$	
$\Updownarrow$	
$T' \vdash \bot$	T' endelig delteori av T
$\Updownarrow$	def. av inkonsistent
finnes endelig delteori av T som er inkonsistent	
$\Updownarrow$	Teorem 1.2
finnes endelig delteori av T som ikke har modell	$\square$

Beviset forteller at kompakthet er en triviell konsekvens av kompletthet. Den innsikten som ligger bak kompakthetsteoremet kan formuleres på mange måter. Det følgende korollaret gir en del alternativer.

Korollar 1.4 *Følgende seks punkter er ekvivalente.*

(i) *T har en modell hvis og bare hvis enhver endelig delteori av T har en modell.*

(ii) *T har ingen modell hvis og bare hvis det finnes en endelig delteori av T som ikke har modell.*

(iii) *T er inkonsistent hvis og bare hvis en endelig delteori av T er inkonsistent.*

(iv) T *er konsistent hvis og bare hvis alle endelige delteorier av* T *er konsistente.*

(v) $T \vdash A$ *hvis og bare hvis det finnes en endelig delteori* T' *av* T *slik at* $T' \vdash A$.

(vi) $T \models A$ *hvis og bare hvis det finnes en endelig delteori* T' *av* T *slik at* $T' \models A$.

Bevis av Korollar 1.4. En relativt enkel oppgave. □

1.3 Eksempler og utdypninger

La oss ta for oss noen utsagn i språket for teorien om binære sekvenser.

(1) $(\forall x)\,[e \neq S_0(x) \;\wedge\; e \neq S_1(x)]$.

(2) $(\forall xy)\,[y \circ x = x \;\rightarrow\; y = e]$.

(3) $(\forall xy)\,[x \circ y = y \circ x]$

Vi ser at (1) og (2) utvilsomt er sanne i strukturen $\mathcal{B}$, mens (3) like utvilsomt er usann i $\mathcal{B}$. Det betyr at (3) ikke følger logisk fra aksiomene i B siden vi har en modell der aksiomene er sanne og (3) er usann. Dermed kan vi ved å bruke kompletthetsteoremet (sunnhetsretningen) slutte at det ikke er mulig å utlede (3) i teorien B, dvs. $B \nvdash (3)$. La oss nå undersøke om (1) og (2) følger logisk fra aksiomene i B. (Det er veldig, veldig viktig å forstå at dette ikke er det samme som å undersøke om (1) og (2) er sanne i modellen $\mathcal{B}$.) Kompletthetsteoremet sier at hvis et utsagn A følger logisk fra aksiomene i B, så kan vi vise det ved å utlede A fra aksiomene i B. Hvis A ikke følger logisk fra aksiomene B, så kan det vises ved å konstruere en modell hvor A ikke holder og aksiomene i B holder.

En åpen gren i treet over utsagnet $B_1 \wedge \cdots \wedge B_6 \rightarrow A$ vil gi en slik modell. Problemet er at det ikke finnes en generell prosedyre for å avgjøre hvorvidt dette treet vil ha en åpen gren. (Senere i kompendiet skal presisere dette problemet og bevise at det er uavgjørbart.) Det finnes ingen mekanisk framgangsmåte. Tvert i mot. Av og til krever det en god porsjon fantasi og kreativitet for å konstruere den ettertraktede modellen. Det kan være en morsom sport.

Det er slett ikke lett å se hvorvidt (1) og (2) følger logisk fra aksiomene i B. Det forholder seg slik at (1) gjør det, mens (2) antagligvis ikke gjør det. Vi skal snart utlede (1) formelt ved tremetoden, men la oss først føre et "fritt" modellteoretisk resonnement for at (1) følger. Anta at alle aksiomene i B holder, men at (1) ikke holder. Da finnes det et individ α i universet slik at $e = S_0(\alpha)$ (*). La β være et vilkårlig individ i universet, og la γ betegne individet $\alpha \circ S_1(\beta)$. Da har vi

$$S_0(\gamma) \;=\; S_0(\alpha \circ S_1(\beta)) \overset{B_5}{=} S_0(\alpha) \circ S_1(\beta) \overset{(*)}{=} e \circ S_1(\beta) \overset{B_4}{=} S_1(\beta)\,.$$

Det finnes altså γ og β slik at $S_0(\gamma) = S_1(\beta)$. Dette strider mot aksiom B_3. Dermed fører antagelsen om at alle aksiomene i B holder og at (1) ikke holder til en selvmotsigelse. Fra dette slutter vi at (1) følger logisk fra aksiomene i B, dvs. $B \models (1)$. Siden tremetoden er komplett vet vi at $B \vdash (1)$, dvs. treet over $B_1 \wedge \cdots \wedge B_6 \rightarrow A$ er lukket. Her er en skisse av

treet.

1.$\neg B_3$	$(\exists x, y)[S_0(x) = S_1(y) \vee S_1(x) = S_0(y)]$	
2.$\neg B_4$	$(\exists y)[e \circ y \neq y]$	
3.$\neg B_5$	$(\exists xy)[S_0(x) \circ y \neq S_0(x \circ y)]$	
4.$\neg B_6$	$(\exists xy)[S_1(x) \circ y \neq S_1(x \circ y)]$	
5.	$(\forall x)[e \neq S_0(x) \wedge e \neq S_1(x)]$	
6.	$e \neq S_0(a) \wedge e \neq S_1(a)$	
7. fra 6	$e \neq S_0(a)$	
8. fra 3	$S_0(a) \circ S_1(a) \neq S_0(a \circ S_1(a))$	$e \neq S_1(a)$
9. fra 7,8	$e \circ S_1(a) \neq S_0(a \circ S_1(a))$	$\vdots$
10. fra 2	$e \circ S_1(a) \neq S_1(a)$	symmetrisk
11. fra 9,10	$S_1(a) \neq S_0(a \circ S_1(a))$	$\vdots$
12. fra 1	$S_0(a) = S_1(a \circ S_1(a)) \vee S_1(a) = S_0(a \circ S_1(a))$	$\vdots$
13. fra 12	$S_0(a) = S_1(a \circ S_1(a))$	$\surd$
14. fra 12	$S_1(a) = S_0(a \circ S_1(a))$	
15. fra 11,14	$\surd$	

Skal vi vise at (2) ikke følger logisk fra aksiomene i B, må vi konstruere en modell $\mathfrak{M}$ slik at $\mathfrak{M} \models B$ og $\mathfrak{M} \not\models$ (2). Det er vanskelig, og vi skal ikke bruke tid og krefter på det. La oss i stedet finne noen Π^0_1-utsagn som er sanne i $\mathcal{N}$, men som ikke kan utledes fra Robinsons aksiomer. Vi konstruerer en modell $\mathcal{N}'$ hvor de naturlige tallene $\mathbf{N}$ er en ekte delmengde av universet. (I forbindelse med første ordens tallteori er det vanlig å kalle elementene i en slik delmengde for *standard* elementene.) I tillegg har universet to ikke-standard elementer ∞_1 og ∞_2. I $\mathcal{N}'$ tolkes navnet 0 som tallet 0 og funksjonene $S, +$ og $\times$ tolkes som henholdsvis $S', +'$ og $\times'$. Begrenset til $\mathbf{N}$ er $S', +'$ og $\times'$ henholdsvis etterfølgerfunksjonen, addisjonsfunksjonen og multiplikasjonsfunksjonen. For ikke-standard individene gjelder

- $S'(x) = x$ når $x \in \{\infty_1, \infty_2\}$
- $x +' y = x$ når $x \in \{\infty_1, \infty_2\}$ og $y \in \mathbf{N}$
- $x +' \infty_1 = \infty_2$ og $x + \infty_2 = \infty_1$ når $x \in \mathbf{N} \cup \{\infty_1, \infty_2\}$
- $x \times' \infty_1 = \infty_1$ og $x \times' \infty_2 = \infty_2$ når $x \in \mathbf{N}$
- $\infty_1 \times' 0 = 0$ og $\infty_2 \times' 0 = 0$
- $\infty_1 \times' x = \infty_2$ og $\infty_2 \times' x = \infty_1$ for alle $x \neq 0$.

Leseren kan forsikre seg om at $\mathcal{N}' \models R$ på egenhånd. Hvert av de seks aksiomene i Robinsons teori er sanne når man tolker $S, +$ og $\times$ som henholdsvis $S', +'$ og $\times'$, men vi har også

(a) $\mathcal{N}' \models (\exists x)[x = S(x)]$. (Dette holder for eksempel fordi $S'(\infty_1) = \infty_1$.)

(b) $\mathcal{N}' \models (\exists x)[0 + x \neq x]$. (Dette holder for eksempel fordi $0 +' \infty_2 = \infty_1$.)

(c) $\mathcal{N}' \models (\exists x)[0 \times x \neq 0]$. (Dette holder for eksempel fordi $0 \times' \infty_1 = \infty_1$.)

Det er klart som vann at utsagnene i punkt (a), (b) og (c) ikke er sanne i $\mathcal{N}$. Negasjonene av dem

$$(\forall x)[x \neq S(x)] \qquad (\forall x)[0 + x = x] \qquad (\forall x)[0 \times x = 0]$$

holder jo i $\mathcal{N}$. Dermed har vi tre Π_1^0-utsagn som er sanne i $\mathcal{N}$, men som ikke kan utledes fra Robinsons aksiomer: De tre utsagnene er jo ikke sanne i alle modeller for Robinsons aksiomer. Dermed kan de heller ikke utledes fra Robinsons aksiomer. Det følger av kompletthetsteoremet (sunnhetsretningen).

Vi har nettopp sett at for eksempel utsagnet $(\forall x)[x \neq S(x)]$ ikke kan utledes fra Robinsons aksiomer. Dette vitner om en slags mangel ved aksiomsettet. Utsagnet er opplagt sant i $\mathcal{N}$ og er dertil enkelt. Det er kort og lite komplisert. Mange spør seg sikkert om vi ikke burde la utsagnet bli et aksiom i R. Eventuelt utvide R med andre aksiomer slik at utsagnet kan utledes i R? Det kan vi selvsagt gjøre. Utsagnet er for eksempel utledbart i Peano-aritmetikk. Situasjonen er imidlertid slik at for enhver første ordens tallteori T over språket $0, S, +, \times$, så må det finnes utsagn som er sanne i $\mathcal{N}$ og som ikke kan utledes i T. Dette er en konsekvens av ufullstendighetsteoremene for tallteori, som vi skal se nærmere på i kapittel 4. Vi kan utvide og utvide og utvide Robinsons aksiomsett. Så lenge mengden av aksiomer er rekursivt tellbar, dvs. så lenge vi har en algoritme for å liste opp aksiomene,[13] vil vi finne nye utsagn i slekt med $(\forall x)[x \neq S(x)]$, dvs. utsagn som er sanne i $\mathcal{N}$, men som ikke kan utledes i R. På bakgrunn av dette er det naturlig å spørre seg om hvilke utsagn som *kan* utledes i R. Kan vi utlede at "en pluss en er to" i R? Svaret er at Robinsons aksiomer i visse henseende faktisk er sterke. Vi kan utlede ethvert Σ_1^0-utsagn som er sant i $\mathcal{N}$ fra dem. Vi skal se senere at man ikke kan vente seg så mye mer av en første ordens tallteori for språket $+, \times, S$ og 0.

La oss se nærmere på hvordan vi kan utlede diverse utsagn fra Robinsons aksiomer. La $\overline{0} = 0$ og la $\overline{n+1} = S(\overline{n})$. Dermed har vi $\mathcal{N}(\overline{n}) = n$ for alle $n \in \mathbf{N}$. I første omgang forsikrer vi oss om at $R \vdash \overline{p} + \overline{q} = \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $p + q = r$. Tremetoden gir

1.	$(\exists x)[x + 0 \neq x]$	negasjonen av R_4
2.	$(\exists xy)[x + S(y) \neq S(x + y)]$	negasjonen av R_5
3.	$\overline{p} + 0 = \overline{p}$	
4.	$\overline{p} + 0 \neq \overline{p}$	fra 1
5.	$\surd$	fra 3 og 4

Treet for $\overline{p} + S(0) = \overline{p+1}$ er

1.	$(\exists x)[x + 0 \neq x]$	negasjonen av R_4
2.	$(\exists xy)[x + S(y) \neq S(x + y)]$	negasjonen av R_5
3.	$\overline{p} + S(0) = \overline{p+1}$	
4.	$\overline{p} + 0 \neq \overline{p}$	fra 1
5.	$\overline{p} + S(0) \neq S(\overline{p} + 0)$	fra 2
6.	$\overline{p} + S(0) \neq S(\overline{p})$	fra 4 og 5
7.	$\surd$	fra 3 og 6

[13] Bryter man dette kravet, så er det trivielt å finne en første ordens teori T slik at $T \vdash A$ for alle A sanne i $\mathcal{N}$. La simpelthen ethvert utsagn A som er sant i $\mathcal{N}$ være et aksiom i T.

og treet for $\overline{p} + S(S(0)) = \overline{p+2}$ er

1.	$(\exists x)[x + 0 \neq x]$	negasjonen av R_4
2.	$(\exists xy)[x + S(y) \neq S(x + y)]$	negasjonen av R_5
3.	$\overline{p} + S(S(0)) = \overline{p+2}$	
4.	$\overline{p} + 0 \neq \overline{p}$	fra 1
5.	$\overline{p} + S(0) \neq S(\overline{p} + 0)$	fra 2
6.	$\overline{p} + S(0) \neq S(\overline{p})$	fra 4 og 5
7.	$\overline{p} + S(S(0)) \neq S(\overline{p} + S(0))$	fra 2
8.	$\overline{p} + S(S(0)) \neq S(S(\overline{p}))$	fra 6 og 7
9.	$\surd$	fra 3 og 8.

Ved induksjon på q ser vi at $R \vdash \overline{p} + \overline{q} = \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \models \overline{p} + \overline{q} = \overline{r}$. Ved induksjon på q kan vi også vise at $R \vdash \overline{p} + \overline{q} \neq \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \models \overline{p} + \overline{q} \neq \overline{r}$. Videre kan vi vise, igjen ved induksjon på q, at $R \vdash \overline{p} \times \overline{q} = \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \models \overline{p} \times \overline{q} = \overline{r}$. Tilsvarende for $p \times q \neq r$. Deretter kan vi ved induksjon på den syntaktiske oppbygningen av et kvantorfritt utsagn A vise at $R \vdash A$ hvis $\mathcal{N} \models A$. Så fra Robinsons aksiomer kan vi utlede ethvert kvantorfritt utsagn som er sant i $\mathcal{N}$. Fra dette følger det at vi også kan utlede alle Σ_1^0-utsagn som er sanne i $\mathcal{N}$. Vi overlater det relativt enkle resonnementet bak den siste konklusjonen til leseren.

La oss avrunde dette delkapitlet med et eksempel på det man gjerne kaller *uavhengighetsbevis*. Vi sier at et aksiom er uavhengig av de øvrige aksiomene i en teori dersom verken aksiomet eller dets negasjon kan utledes fra de øvrige aksiomene. Ethvert aksiom i en teori bør være uavhengig av de øvrige. Kan et aksioms negasjon utledes i teorien, så er jo teorien inkonsistent. Kan et aksiom utledes fra de øvrige, så trenger vi jo ikke aksiomet. La oss vise at

$$(B_3) \quad (\forall xy)\,[S_0(x) \neq S_1(y) \ \wedge \ S_1(x) \neq S_0(y)]$$

er uavhengig av de øvrige aksiomene i B. Det følger fra sunnhetsretningen av kompletthetsteoremet og $\mathcal{B} \models B$ at $\neg B_3$ ikke kan utledes fra de øvrige aksiomene. For å vise at B_3 ikke kan utledes fra de øvrige aksiomene skal vi definere modellen $\mathfrak{M}$ for teorien B. Universet til $\mathfrak{M}$ er $\mathbf{N}$, dvs. de naturlige tallene. Videre lar vi $\mathfrak{M}(e) = 0$ og vi lar $\mathfrak{M}$ tolke både S_0 og S_1 som etterfølgerfunksjonen, dvs. $\mathfrak{M}(S_0)(x) = \mathfrak{M}(S_1)(x) = x + 1$. Endelig lar vi $\mathfrak{M}$ tolke det binære funksjonssymbolet $\circ$ som addisjon. Nå har vi $\mathfrak{M} \models B_1$ siden alle tall forskjellig fra 0 er en etterfølger. Videre har vi $\mathfrak{M} \models B_2$ siden $x + 1 \neq y + 1$ når for alle x, y der $x \neq y$. Aksiomene B_4, B_5 og B_6 holder også i $\mathfrak{M}$. Dermed holder alle aksiomene i B i strukturen $\mathfrak{M}$ bortsett fra B_3. Vi må ha $\mathfrak{M} \not\models B_3$ siden det er tilfellet at $\mathfrak{M} \models (\forall x)[S_0(x) = S_1(x)]$. Dermed kan ikke B_3 utledes fra de øvrige aksiomene i B siden den logiske kalkylen vår (for eksempel tremetoden) er sunn.

1.4 Konsekvenser av kompakthet

Kompletthetsteoremet for første ordens logikk er et positivt resultat. Teoremet sier at vi effektivt kan kontrollere hvorvidt en konklusjon følger fra sine premisser. Enhver gyldig første ordens slutning kan uttrykkes i et formelt bevissystem. Dette er ingen selvfølgelighet. Andre typer logikker tillater intet kompletthetsteorem. For *endelig første ordens logikk*, dvs. en første ordens logikk hvor gyldighet er det samme som sannhet i alle *endelige* modeller, finnes intet kompletthetsteorem. Det samme gjelder for logikk med uendelige konnektiver

og høyere ordens logikk. Kompletthetsteoremet gjør at man ofte velger å holde fast ved første ordens logikk selv i situasjoner hvor en annen logikk gir en bedre analyse. Endelig logikk er aktuelt i forbindelse med databehandling. Der er man for eksempel interessert i om en påstand holder i alle databaser som tilfredsstiller visse betingelser, og en database er alltid endelig. Likevel velger man helst standard første ordens logikk som spesifikasjonsspråk fordi man vil ha mulighet til automatisk bevisføring og lignende.

Så kompletthet er utvilsomt en av første ordens logikkens dyder. Men dyder blir lett laster. Vi har sett at kompakthet var en triviell konsekvens av kompletthet. Nå skal vi se at kompakthet – og dermed kompletthet – impliserer en rekke negative resultater. Negative i den forstand at de uttaler essensielle begrensninger ved første ordens teorier. Vi skal vise at det ikke kan uttrykkes i et første ordens språk at (i) universet er velordnet, at (ii) universet er endelig og (iii) at universet består av de naturlige tallene og intet mer. De tre bevisene er sydd over samme lest og forstår man først ett av dem, bør det være lett å forstå de to andre. Når man har forstått denne bevisteknikken, ser man også at en lang rekke egenskaper som er beslektet med (i), (ii) og (iii) heller ikke lar seg karakterisere av første ordens utsagn. For eksempel kan (iii) generaliseres til å gjelde for andre datastrukturer enn de naturlige tallene.

Teorem 1.5 *En velordning er en lineær ordning hvor enhver delmengde har et minste element. La $\prec$ være et binært relasjonssymbol i språket til T og anta at T har følgende egenskap: $\mathfrak{M} \models T$ for enhver $\mathfrak{M}$ hvor $\prec$ tolkes som en velordning. Da har T en modell hvor $\prec$ ikke er tolket som en velordning.*

Bevis av Teorem 1.5. La $k_0, k_1, k_2, \ldots$ være navn som ikke forekommer i språket til T. Vi utvider T til T_1 ved å legge til aksiomene $k_{i+1} \prec k_i$ for $i = 0, 1, 2, \ldots$. (Formelt gjøres dette ved å benytte en uendelig konjunksjon.) Vi velger nå ut en vilkårlig endelig delmengde T' av T_1. Hvis vi klarer å vise at T' har en modell, så vil enhver endelig delmengde av T_1 ha en modell. Deretter kan vi ved hjelp av kompakthetsteoremet slutte at hele T_1 har en modell.

Her er argumentet for at T' har en modell: Siden T' er endelig finnes det et største tall n slik at k_n er med i språket til T'. Velg nå en modell $\mathfrak{M}$ for T hvor $\prec$ tolkes som en velordning av et univers med minst n individer. (En slik modell finnes siden alle modeller hvor $\prec$ tolkes som en velordning er en modell for T.) Nå kan $\mathfrak{M}$ utvides til en modell for T' ved at vi tolker $k_n, k_{n-1}, \ldots, k_0$ som de n første elementene under velordningen.

Så enhver endelig delmengde av T_1 har en modell. Dermed har T_1 en modell $\mathfrak{M}_1$. Siden T er en delteori av T_1, vil $\mathfrak{M}_1$ også være en modell for T. I denne modellen kan ikke $\prec$ tolkes som en velordning fordi $k_{i+1} \prec k_i$ holder for alle naturlige tall i. □

Teorem 1.6 *Hvis en teori har vilkårlig store endelige modeller, så har den også en uendelig modell.*

Bevis av Teorem 1.6. Anta at teorien T har vilkårlig store endelige modeller. Vi utvider T til T_1 ved å legge til aksiomene

$$
\begin{array}{ll}
A_2 & (\exists x_1, x_2)[x_1 \neq x_2] \\
A_3 & (\exists x_1, x_2, x_3)[x_1 \neq x_2 \wedge x_1 \neq x_3 \wedge x_2 \neq x_3] \\
A_4 & \ldots \\
\vdots &
\end{array}
$$

Formelt gjøres dette ved å bruke en uendelig konjunksjon. Aksiomet A_n sier at universet har minst n individer. La T' være en endelig delteori av T_1. La k være det største tallet slik at A_k er et aksiom i T'. Per antagelse har T en modell $\mathfrak{M}$ hvor det finnes minst k elementer i universet. Vi ser at $\mathfrak{M}$ også er en modell for T'. Nå er T' en vilkårlig delteori av T_1. Dermed har enhver endelig delteori av T_1 en modell, og vi kan bruke kompakthetsteoremet til å slutte at T_1 har en modell $\mathfrak{M}_1$. Siden T er en delteori av T_1 så må $\mathfrak{M}_1$ også være en modell for T. Videre ser vi at $\mathfrak{M}_1$ må ha et uendelig univers siden $\mathfrak{M}_1 \models A_i$ for alle i. □

Skolem[14]-Löwenheims[15] teorem (oppover) sier at hvis en teori har vilkårlig store endelige modeller, så har også teorien modeller av vilkårlig stor kardinalitet. Teorien har altså overtellbare modeller også. Dette er en generalisering av Teorem 1.6. For å vise dette trenger man en sterkere versjon av kompletthetsteoremet, nemlig at $T \models B \Leftrightarrow T \vdash B$ også holder når mengden av aksiomer i T er overtellbar. Da vil kompakthetsteoremet også holde for overtellbare utsagnsmengder. Med et slikt kompakthetsteorem kan beviset av Teorem 1.6 generaliseres til et bevis for Skolem-Löwenheims teorem.

Definisjon. Teorien T er *fullstendig* hvis den er konsistent og $T \vdash A$ eller $T \vdash \neg A$. Hvis den ikke er fullstendig, så er den *ufullstendig*.[16]

To modeller $\mathfrak{M}_1$ og $\mathfrak{M}_2$ er *elementært ekvivalente* dersom ethvert første ordens utsagn har samme sannhetsverdi i de to modellene, det vil si $\mathfrak{M}_1(B) = \mathfrak{M}_2(B)$ for alle B. □

De siste teoremene er i en forstand negative resultater. Teoremene forteller at vi har begrenset kontroll over hvilke modeller som tilfredstiller første ordens teoriene våre. Vi klarer ikke å karakterisere velordninger, vi klarer ikke å karakterisere endelighet, og verre skal det bli. En velordning er tross alt et noe esoterisk begrep. Det neste teoremet sier at vi heller ikke klarer å karakterisere de naturlige tallene. Dette er spesielt sørgelig siden de naturlige tallene er allemannseie og en av matematikkens mest interessante størrelser.

Teorem 1.7 (Skolem) *La T være en første ordens teori slik at $\mathcal{N} \models T$. (i) Da har T en modell $\mathcal{N}^*$ som ikke er isomorf med $\mathcal{N}$ og (ii) $\mathcal{N}^*$ og $\mathcal{N}$ er elementært ekvivalente.*

Bevis av Teorem 1.7. For å vise (i) innfører vi et konstanttegn k som ikke forekommer i språket til T. Så utvider vi T til T_1 ved å legge til aksiomene

$$0 < k, \quad S0 < k, \quad SS0 < k, \quad SSS0 < k \ldots \quad .$$

(Formelt bruker vi en uendelig konjunksjon.) La T' være en endelig delteori av T_1. Da vil T' ha en modell. Hvorfor? Jo, T' vil inneholde et største numeral. (Et numeral er en rekke S'er etterfulgt av 0.) La oss si at det største numeralet i T' tolkes som n i $\mathcal{N}$. La $\mathcal{N}'$ være som $\mathcal{N}$ og la $\mathcal{N}'(k) = n + 1$. ($\mathcal{N}$ tolker ikke k.) Da har vi $\mathcal{N}' \models T'$. Så T' har en modell, og T' er en vilkårlig valgt endelig delteori av T_1. Dermed har enhver endelig delteori av T_1 en modell. Dermed – vi bruker kompakthetsteoremet – har T_1 en modell $\mathcal{N}^*$. Siden T er en delteori av T_1 har vi også at $\mathcal{N}^* \models T$.

Universet til $\mathcal{N}^*$ inneholder et individ 0 som er tolkningen av 0, et individ 1 som er tolkingen av $S0, \ldots$. Dessuten inneholder universet til $\mathcal{N}^*$ et individ ∞ som er "større enn" $0, 1, \ldots$.

[14] Toralf Skolem, norsk matematiker, 1887-1963. Professor ved Universitetet i Oslo 1938-1957.

[15] Leopold Löwenheim, tysk matematiker, 18??-19??

[16] Det er også vanlig å kalle en fullstendig teori for en *komplett* teori. Vi bruker "fullstendig" om teorier og "komplett" om logikken slik at leseren ikke skal blande de to tingene sammen.

(Universet inneholder mange andre rare individer også.) Individet ∞ vitner om at $\mathcal{N}^*$ ikke er isomorf med $\mathcal{N}$.

Nå skal vi vise (ii) ved et absurdum resonnement. Anta at $\mathcal{N}$ og $\mathcal{N}^*$ ikke er elementært ekvivalente. Da finnes et utsagn A slik at $\mathcal{N} \models A$ og $\mathcal{N}^* \models \neg A$ (*). La første ordens teorien T være slik at A er et aksiom i T og at $\mathcal{N} \models T$. Ved å "gjenta" beviset over kan vi vise $\mathcal{N}^* \models T$. Modellen $\mathcal{N}^*$ som konstrueres, blir den samme uansett hvilke aksiomer T inneholder. Dermed $\mathcal{N}^* \models A$. Det strider mot (*). $\square$

En modell som $\mathcal{N}^*$ kalles gjerne en ikke-intendert modell. Hvorfor må enhver elementær tallteori ha en ikke-intendert modell? Hvorfor tilfredsstiller en modell med "noe grums etter tallrekken" ethvert første ordens aksiomsett for tallteori? Vi sier jo ved hjelp av aksiomer at det ikke finnes elementer foran tallrekken. En struktur hvor det finnes elementer mindre enn 0 er ikke modell for Robinsons eller Peanos aksiomer. Hvorfor kan vi rett og slett ikke ha aksiomer som sier at det ikke finnes elementer etter tallrekken? Svaret er ganske enkelt at slike aksiomer ikke lar seg uttrykke i et første ordens språk. Vi trenger "mer språk" for å bli kvitt ikke-intenderte modeller. Hadde vi tilgang til uendelige disjunksjoner, kunne vi utvidet Robinson med aksiomet

$$(\forall x)[x = 0 \ \vee \ x = S0 \ \vee \ x = SS0 \ \vee \ \ldots \ ] .$$

Dette aksiomet sier at det ikke er andre elementer i universet enn de som finnes i den naturlige tallrekken. Dermed vil enhver modell for denne utvidete Robinsonteorien være isomorf med $\mathcal{N}$. Så teorier formulert ved uendelig predikatlogikk behøver ikke å ha ikke-intenderte modeller. Det behøver heller ikke høyere ordens teorier. (Hvorfor er vi da så opptatt av første ordens teorier? Jo, fordi vi har et kompletthetsteorem for første ordens logikk.)

Eksistensen av den ikke-intenderte modellen $\mathcal{N}^*$ fra beviset av Teorem 1.7 har i en viss forstand ikke så store konsekvenser: Ethvert første ordens utsagn har samme sannhetsverdi i $\mathcal{N}$ og $\mathcal{N}^*$. Først når vi klarer å vise at enhver elementær tallteori har en modell som ikke er elementært ekvivalent med $\mathcal{N}$, går drømmen om en fullstendig første ordens tallteori i vasken. Neste teorem gir sammenhengen mellom elementær ekvivalens og fullstendige teorier.

Teorem 1.8 *La T være en første ordens teori. Da gjelder*

(1) *Alle tellbare modeller for T er isomorfe.*

$\Downarrow$

(2) *Alle modeller for T er elementært ekvivalente.*

$\Updownarrow$

(3) *T er fullstendig.*

Bevis av Teorem 1.8. Vi viser ikke (1) $\Rightarrow$ (2). Blant annet fordi vi ikke har definert nøyaktig hva det betyr at to modeller er isomorfe. Vi går løs på ekvivalensen mellom (2) og (3). Den

viser vi kontrapositivt. La $A_1, \ldots, A_n$ være aksiomene i T.

$$
\begin{array}{cl}
T \text{ er ikke fullstendig} & \\
\Updownarrow & \text{def. av fullstendig} \\
T \nvdash B \text{ og } T \nvdash \neg B & \text{finnes slik } B \\
\Updownarrow & \text{Teorem 1.1} \\
T \not\models B \text{ og } T \not\models \neg B & \\
\Updownarrow & \text{Teorem 0.2} \\
\text{Både } \{A_1, \ldots, A_n, B\} \text{ og } \{A_1, \ldots, A_n, \neg B\} \text{ har en modell.} & \\
\Updownarrow & \\
\text{Det finnes modeller } \mathfrak{M}_1, \mathfrak{M}_2 \text{ for } T \text{ slik at } \mathfrak{M}_1(B) \neq \mathfrak{M}_2(B). & \\
\Updownarrow & \\
\text{Alle modeller for } T \text{ er ikke elementært ekvivalente.} \quad \square &
\end{array}
$$

Vi har allerede antydet at første ordens teorier har større skavanker enn at de tillater ikke-intenderte modeller a la $\mathcal{N}^*$. Enhver rimelig komplisert første ordens teori vil også ha en modell som ikke er elementært ekvivalent med den intenderte. En hver rimelig komplisert første ordens teori er nemlig ufullstendig. Før vi er i stand til å vise dette, må vi sette oss inn i litt rekursjonsteori.

1.5 Oppgaver

Oppgave 1
Vi tar for oss de tallteoretiske påstandene

(1) Det finnes uendelig mange primtall

(2) Det finnes uendelig mange x, y, z slik at $x^2 + y^2 = z^2$.

(3) Ligningen $x^n + y^n = z^n$ har ingen løsninger når $n > 2$ og $x, y, z > 0$.

(4) Ethvert partall kan skrives som summen av to primtall.

(5) Det finnes uendelig mange tvillingprimtall.

Punkt a
For hver av påstandene over, bortsett fra (3), skal du lage et utsagn A slik at $\mathcal{N} \models A$ hvis og bare hvis påstanden holder. Det skal altså ikke brukes ikke-logiske språk utover $+, \times, S, 0$. (Modellen $\mathcal{N}$ tolker ikke andre ikke-logiske symboler enn disse.)

Punkt b
En konsekvens av teoremer vi vil vise i senere kapitler er at det også er mulig å uttrykke (3) i strukturen $\mathcal{N}$. I øyeblikket er det antageligvis en for stor oppgave for leseren å finne et slikt utsagn. (Hvis man da ikke allerede har tittet litt på de neste kapitlene.) Hva er så spesielt ved (3)? Hva er problemet ved (3) versus (1), (2), (4) og (5)?

Oppgave 2
La nå $\overline{0} = 0$ og la $\overline{n+1} = S(\overline{n})$. (Vi skal kalle $\overline{n}$ for et numeral.) La R som vanlig være første ordens teorien med Robinsons aksiomer.

Punkt a
Vis at $R \vdash \overline{1} + \overline{1} \neq \overline{3}$.

Punkt b
Vis for alle $p, q, r \in \mathbf{N}$ at $R \vdash \overline{p} + \overline{q} \neq \overline{r}$ hvis $\mathcal{N} \models \overline{p} + \overline{q} \neq \overline{r}$.

Punkt c
Vis for alle $p, q, r \in \mathbf{N}$ at $R \vdash \overline{p} \times \overline{q} = \overline{r}$ hvis $\mathcal{N} \models \overline{p} \times \overline{q} = \overline{r}$. Vis for alle $p, q, r \in \mathbf{N}$ at $R \vdash \overline{p} \times \overline{q} \neq \overline{r}$ hvis $\mathcal{N} \models \overline{p} \times \overline{q} \neq \overline{r}$.

Oppgave 3
I slutten av delkapittel 1.3 forklarte vi hva det betyr at utsagn er *uavhengige* av hverandre.

Punkt a
Vi har sett at utsagnet $(\forall x)\ [e \neq S_0(x)\ \wedge\ e \neq S_1(x)]$ ikke er uavhengig av aksiomene i teorien om bitsekvenser B. Du skal vise at utsagnet er uavhengig av aksiomene B_1, B_2 og B_3.

Punkt b
Vis at ethvert aksiom i Robinsons teori R er uavhengig av de øvrige aksiomene i teorien.

Oppgave 4
Vis at en teori T er konsistent hvis og bare hvis det finnes et utsagn A slik at $T \nvdash A$.

Oppgave 5
Bevis Gödels kompletthetsteorem (1.1) ved å benytte Henkins kompletthetsteorem.

Oppgave 6
Vis at Peanos aksiomer er sterkere enn Robinsons aksiomer. Vis først: $R \vdash A \ \Rightarrow\ P \vdash A$. Vis deretter at $P \vdash (\forall x)[x \neq S(x)]$. Da må mengden av utsagn som kan utledes i R være ekte inneholdt i mengden av utsagn som kan utledes i P. (Vi har sett at $R \nvdash (\forall x)[x \neq S(x)]$.)

Oppgave 7
Teoriene T_1 og T_2 er ekvivalente når den ene er en delteori av den andre og omvendt. Hvis en teori T er ekvivalent med en endelig teori, så er T *endelig aksiomatiserbar*. I denne oppgaven skal du vise at det finnes første ordens teorier som ikke er endelig aksiomatiserbare.

La T være en første ordens teori med aksiomer $A_1, A_2, A_3, \ldots$ slik at A_i ikke er et aksiomskjema og

$$\models A_n \rightarrow A_m \quad \Leftrightarrow \quad n \geq m\,. \quad (*)$$

Nå skal vi vise (Påstand):

Det finnes ikke utsagn B slik at $T \vdash B$ og $B \vdash A_n$ for alle n.

Anta motsatt. Ved kompakthetsteoremet har vi $A_1, A_2, \ldots, A_k \vdash B$ for et fast tall k. Siden $\models A_k \rightarrow A_l$ når $l \leq k$, så betyr dette at $A_k \vdash B$. (Her brukte vi kompletthetsteoremet.) Vi har antatt at $B \vdash A_{k+1}$. Ved kompletthetsteoremet har vi altså at $A_k \models B$ og $B \models A_{k+1}$. Dermed må det være slik at $A_k \models A_{k+1}$, dvs. at $\models A_k \rightarrow A_{k+1}$. Dette taler i mot (*), og vi har vist (Påstand).

Punkt a
Bruk ren første ordens logikk med likhet og lag en sekvens av utsagn $B_1, B_2, B_3, \ldots$. (Du får ikke bruke andre relasjons- og funksjonssymboler enn $=$.) Utsagnet B_i skal være sant

i alle modeller med minst i individer i universet, og usant i alle modeller med færre enn i individer i universet.

Punkt b

La T være teorien der $B_1, B_2, B_3, \ldots$ er de eneste aksiomene. Bruk (Påstand) og vis at T ikke er endelig aksiomatiserbar.

Oppgave 8

Vis at teorien B om binære sekvenser har ikke-intenderte modeller, dvs. vis at det finnes en modell $\mathcal{B}^*$ som er elementært ekvivalent med $\mathcal{B}$, men ikke isomorf med $\mathcal{B}$.

Kapittel 2

Turings tese og de beregnbare funksjonene

2.1 Nittenseksogtredvetesene

Både Church[1], Kleene[2], Post[3] og Turing publiserer i det selvsamme år nittenseksogtredve artikler som inneholder "teser". Jeg bruker gåseøyne fordi opphavsmennene til de diverse "tesene" aldri fremsetter eksplisitte teser. Når vi f.eks. snakker om "Church-Turings tese" eller "Turings tese", så benytter vi en upresis terminologi som har kommet til i etterhånd.

En ting har nittenseksogtredvetesene utvilsomt felles, nemlig motivasjonen. De er i all hovedsak motivert av et ønske om å gjøre det mulig å bevise at diverse matematiske problemer er uavgjørbare. Vi kan nevne ordproblemet for grupper (Dehn[4] 1911) og ordproblemet for semigrupper (Thue[5] 1914). Videre hadde man Hilberts "entscheidungs"-problemer. Et av dem kalles Hilberts tiende problem: *Finnes det en effektiv metode for å avgjøre hvorvidt et vilkårlig polynom med heltallskoeffisienter har en rot blant de hele tallene?* Et annet har blitt kjent som selve *entscheidungsproblemet*: *Finnes det en effektiv metode for å avgjøre hvorvidt et vilkårlig utsagn i første ordens logikk er tilfredstillbart?* Vi har formulert moderne varianter av begge disse problemene, og det siste er, gitt Gödels kompletthetsteorem, ekvivalent med hvorvidt det finnes en effektiv metode for å avgjøre hvorvidt et vilkårlig utsagn i første ordens logikk kan utledes i en formell beviskalkyle. Dette problemet står i en absolutt særstilling. Entscheidungsproblemet griper direkte inn i matematikkens mest fundamentale grunnlagsproblemer anno 1936.

Vi har alle en sterk intuitiv forståelse av hva det vil si å ha en *effektiv metode* for å løse et matematisk problem. Gitt en strengt voksende og deriverbar funksjon $f : \mathbf{R} \to \mathbf{R}$, så har vi en effektiv metode for å finne vilkårlig gode tilnærminger til en x slik at $f(x) = 0$, dersom slik x finnes (Newtons metode). Videre har vi f.eks. en effektiv metode for å finne minste felles multiplum av to naturlige tall (Euclids algoritme) og en effektiv metode for å avgjøre hvorvidt en formel i ren utsagnslogikk er en tautologi (lag en sannhetsverditabell). En effektiv metode er et sett av utvetydige regler som vi slavisk, blindt og fantasiløst kan

[1] Alonzo Church, amerikansk matematiker, 1903-1995.
[2] Stephen C. Kleene, amerikansk matematiker, 1909-1994
[3] Emil Post, amerikansk matematiker, 1897-1954
[4] Max Dehn, tysk matematiker, 1878-1952
[5] Axel Thue, norsk matematiker, 1863-1922

følge for å løse et problem i endelig tid. Ofte brukes ordet "algoritme" synonymt med "effektiv metode". Vi vil også bruke ordet "prosedyre" synonymt med ordet "metode".

Skal vi bevise at det finnes en effektive metode for å løse et gitt problem, har vi en grei mal. Beskriv metoden og vis at metoden alltid gir en korrekt løsning av problemet. Ut fra selve beskrivelsen av metoden, kan den som leser beviset konstatere at metoden kan gjennomføres effektivt. Selvfølgelig er det ikke alltid like enkelt å forvisse seg om hvorvidt en metode gitt i et bevis er effektiv, men det er som regel lettere å sjekke dette enn å verifisere beviset forøvrig. Det at vi ikke opererer med en formell definisjon av effektiv metode betyr vanligvis ikke så mye i en slik situasjon. Vi kjenner igjen en effektiv metode når vi ser en, på samme måte som vi kjenner igjen et punkt på den reelle tallinjen når vi ser ett. Situasjonen forandres radikalt i det øyeblikk man ønsker å gi et fullverdig matematisk bevis for at det *ikke* finnes en effektiv metode for å løse et problem, dvs. at et problem er uavgjørbart. I en slik situasjon må man gi begrepet "effektiv metode" et mer presist matematisk innhold. Man trenger matematisk kontroll over *mengden* som inneholder *alle* effektive metoder.

Dette lar seg sammenligne med at vi ønsker å gi et stringent bevis for at det er umulig å utføre en eller annen geometrisk konstruksjon utelukkende ved hjelp av passer og linjal, f.eks. å tredele en vinkel. Da har vi behov for en matematisk modell av selve passeren og av selve linjalen. Dette behovet er ikke presserende dersom vi f.eks. skal vise at det *er mulig* å todele en vinkel med passer og linjal.

Tesemakeriet i nittenseksogtredve avspeiler et behov for å gi det intuitive begrepet "effektiv metode" et mer presist matematisk innhold. Behovet er knyttet til et ønske om å vise uavgjørbarhetsteoremer. Dette er igjen knyttet til sentrale grunnlagsproblemer i matematikk. Church sine "teser" er mislykket. Kleene og Post mislykkes også. Det er bare Turing som lykkes.

2.2 Turings tese

Jeg skal nå gi en analyse av hva som faktisk sies i del 9 av artikkelen " On computable numbers, with an application to the Entscheidungsproblem" fra 1936. Det er der Turing fremsetter sin såkalte tese..

Tenk deg at du sitter med en penn og en regneblokk med ruteark og blindt manipulerer symboler etter utvetydige og uforanderlige regler. (Situasjonen skulle ikke være fremmed for en som har opplevd det norske skoleverket.) Videre kan du forsøke å abstrahere bort alle andre trekk ved deg selv enn dine evner til å manipulere symboler i overensstemmelse med gitte regler. En slik abstraksjon kan vi kalle for et *regnedyr*. Et regnedyr gjør ikke tabber, det blir ikke gammelt og dør, og det er ikke stand til å forandre reglene sine. La oss videre anta at et regnedyr har uendelig mange penner og uendelig mange ruteark tilgjenglig. Turing analyserer et slikt regnedyr. Han kommer frem til fem aksiomer som et regnedyr tilfredstiller:

(A1) Det neste regnedyret foretar seg er utelukkende og entydig bestemt av en symbolkonfigurasjon i regneboken og tilstanden i regnedyrets sjel.

(A2) Et regnedyr kan bare kjenne igjen endelig mange symbolkonfigurasjoner i regneboken.

(A3) Regnedyrets sjel er alltid i en av et endelig antall mulige tilstander. (Regnedyr er enfoldige skapninger.)

Fra dette følger det at et regnedyr kun kan utføre et endelig antall handlinger. Disse handlingene er begrenset av at

(A4) regnedyret kan bare forandre ett og ett tegn i symbolkonfigurasjoner det allerede har observert.

(A5) det finnes en øvre grense for avstanden mellom de rutene i regneboken regnedyret iakttar på tidspunkt t og de det iaktar på tidspunkt $t + 1$.

Legg merke at Turing ikke analyserer f.eks. idealisert mekanikk eller den menneskelig tenkeevne i sin alimmelighet. Han analyserer et regnedyr. For enkelhets skyld sier vi at et regnedyr pr. definisjon tilfredstiller (A1), (A2), (A3), (A4) og (A5). Vi kan nå gi en nøyaktig formulering av det viktigste resultatet i del 9 av Turings "On computable numbers".

(Turings Teorem) *En metode (for å manipulere symboler) kan utføres av et regnedyr hvis og bare hvis den kan utførese av en Turingmaskin.*

Dette teoremet har et stringent matematisk bevis. I beviset må man benytte at et regnedyr tilfredstiller aksiomene (A1), (A2), (A3), (A4) og (A5). For å forstå forholdet mellom Turings Teorem og det vi vanligvis kaller *Turings tese*, skal vi introdusere det vi for anledningen kan kalle *Turings Påstand*.

(Turings Påstand) *En metode er effektiv hvis og bare hvis den kan utføres av et regnedyr.*

Vi kan nå gi et bilde av forholdet mellom Turings tese og Turings Teorem ved en slags ligning.

$$\text{Turings tese} \quad = \quad \textbf{Turings Påstand} \quad + \quad \textbf{Turings Teorem}$$

Turings tese er en kombinasjon av et matematisk teorem og Turings Påstand. Tesen følger logisk fra teoremet og påstanden. Her er en presis formulering:

(Turings tese) *En metode er effektiv hvis og bare hvis den kan utføres av en Turingmaskin.*

2.3 Turings tese vs. andre teser

Turings Påstand hviler på en analyse. Det intuitive begrepet om en effektiv metode analyseres dithen at det kan fanges inn av et regnedyr som tilfredstiller de fem aksiomene over. En slik analyse er Turing alene om i 1936. Church har riktignok sine tilløp, men de er langt fra tilfredstillende. Så de øvrige aktørene i 1936 har ingen mulighet til å gi et stringent bevis av noe som svarer til Turings Teorem. Dette teoremet forutsetter jo den analysen som munner ut i Turings Påstand. Dermed koker f.eks. Churchs "tese" ned til noe i nærheten av et rent (men ikke nødvendigvis ubegrunnet) forslag om at klassen av effektivt beregnbare funksjoner skal defineres lik klassen av λ-definerbare (evt. Gödel-Herbrand rekursive) funksjoner. Så selv om alle "tesene" som verserer i 1936 er ekvivalente i den forstad at de leder til den samme klasse av beregnbare funksjoner, så er bare *Turings* tese begrunnet tilfredstillende. Turing, og ingen andre, treffer spikeren på hodet.

Det er verdt å merke seg at Turing sier lite om mentale prosesser generelt i seksogtredveartikkelen sin. Han forsøker overhodet ikke å argumentere for at slike prosesser kan reduseres til Turingberegnbare prosesser. Ikke i "On computable numbers". Han gjør det ved andre anledninger. Så Turings tese er opplagt ikke en tese om at Turingmaskiner kan danne adekvate matematiske modeller av mental aktivitet i sin alminnelighet. Turings tese er heller ikke et resultat av å analysere de beregninger som kan utføres av en eller annen form

for maskin. Dermed kan vi slutte at Turing heller ikke intenderer å si noe generelt om beregnbarhetsstyrken til maskiner. Beregnbarhetsstyrken til maskiner undersøkes systematisk først i 1980 av Robin Gandy[6]. I en artikkel fra 1980 bruker Gandy samme fremgangsmåte som Turing i "On computable numbers" til å analysere diskrete deterministiske mekaniske innretninger. Han fremsetter en påstand som svarer til Turings Påstand, og viser et teorem som svarer til Turings Teorem. Konklusjonen er, kanskje ikke overraskende, at slike innretninger ikke har større beregningskraft enn Turingmaskiner. Vi kan også nevne at Gandy indirekte gir et meget detaljert bevis av Turings Teorem. Den som ikke er fornøyd med Turings eget bevis kan kikke på Gandys artikkel. Det er nok mest korrekt å si at Turing selv gir en bevis*skisse*.

2.4 Turings tese er et teorem

Den gjengse lærdom om Turings tese er noe á la: *Den kan ikke bevises. Simpelthen fordi den ikke er en matematisk påstand. Turings tese er mer lik en empirisk kjensgjerning enn et matematisk teorem. Tesen bør sees som en hypotese som står så lenge den ikke strider mot våre erfaringer. Den dagen vi står ovenfor noe som rimeligvis kan kalles en beregning, men som en Turingmaskin bevislig ikke kan utføre, må vi revurdere Turings tese.* En slike katekisme er nedfelt i lærebøker og messes fra katetere med pedagogisk anstrengelse og apostotelisk overbevisning. I beste fall er dette sterkt misvisende. Skal noe være en falsifiserbar hypotese, må det være den komponenten av Turings tese som vi har kalt for Turings Påstand. Undertegnede mener imidlertid at det både er naturlig, fornuftig og i pakt med matematisk sedvane å betrakte Turings Påstand som en *definisjon*. Dermed blir Turings tese et helt aminnelig teorem, et teorem som sier at klassen av beregnbare funksjoner er lik klassen av Turingbergnbare funksjoner. Jeg gir en utførlig argumentasjon for dette synspunktet i artikkelen "Turings teorem" [11]. (Så det som kalles *Churchs tese* er egentlig *Turings teorem*. Snakk om *logikk* !)

2.5 De rekursive funksjonene

Teorem eller ikke? La oss avblåse den diskusjonen. Leseren må gjerne være uenig med undertegnede. Resultatene i dette kompendiet vil kun avhenge av det vi over har kalt Turings Teorem, dvs. den komponenten av Turings tese som uten tvil er en matematisk kjensgjerning. Det kan hellller ikke være mye tvil om at Turingmaskinen er en adekvat matematisk modell av beregnbarhet. Adekvat i den forstand at vi ikke kan finne en annen matematisk modell som gir en større klasse av beregnbare funksjoner. Alternative adekvate matematiske modeller av beregnbarhet er for eksempel utypet λ-kalkyle, registermaskiner, Kleene rekursjon ... og ganske mange flere. Alle gir samme klasse av beregnbare funksjoner som teorien om Turingmaskiner. I mange henseende er det imidlertid ikke likegyldig hvilken av disse modellene vi benytter. De forskjellige modellene er mer eller mindre egnet til å belyse forskjellige aspekter ved beregnbarhet. Er vi interessert i å studere hvilke funksjoner som er beregnbare i praksis – beregnbare i polynom tid – så er Turingmaskinen et godt valg. λ-kalkylen er for eksempel egnet til å studere sammenhenger mellom selve den ekstensjonale funksjonen og forskjellige mulige beregninger av den.

[6] Robin Oliver Gandy, engelsk matematiker, 1919-1995.

Dette kompendiets innfallsvinkel til de beregnbare funksjonene er Kleene rekursjon. Da kan vi økonomisk uttrykke en del innsikter om beregnbarhet som er sentrale for oss, og vi får abstrahert bort ting og tang som for anledningen ikke interesserer oss. Enhver funksjon definert ved Kleene rekursjon speiler de naturlige tallene på seg selv, og hvis vi ikke eksplisitt har gitt uttrykk for noe annet, så har en funksjon en delmengde av de naturlige tallene som definisjons- og verdiområde. Vi følger opp tradisjonens språkbruk og kaller de funksjonene vi studerer for *de rekursive funksjonene*. Teorien om de rekursive funksjonene kalles for *rekursjonsteori*. Det neste kapitlet gir en innføring i grunnleggende rekursjonsteori[7].

[7] De siste to-tre årene har flere og flere begynt å snakke om *bergnbarhetsteori* (computabilty theory) istedet for *rekursjonsteori* (recursion theory), *beregnbare funksjoner* istedet for *rekursive funksjoner*, osv. En slik språkbruk er åpenbart både mer informativ og mer korrekt historisk sett. Det er ikke like åpenbart at det er lurt å forandre på en teminologi som har vært vel etablert i over femti år.

Kapittel 3

Grunnleggende rekursjonsteori

3.1 Rekursive og primitivt rekursive funksjoner

Definisjon. Funksjonene $\mathcal{O}$, $\mathcal{S}$ og $\mathcal{I}_i^n$ er de *rekursive initialfunksjonene*. Her er n og i naturlige tall slik at $0 < i \leq n$. Vi har $\mathcal{I}_i^n(x_1, \ldots, x_n) = x_i$. Videre har vi $\mathcal{O} = 0$ og $\mathcal{S}(x) = x + 1$. Vi kaller $\mathcal{O}$ for *nullfunksjonen*. Vi kaller $\mathcal{S}$ for *sucsessor-* eller *etterfølgerfunksjonen*. Vi kaller $\mathcal{I}_i^n$ for $0 < i \leq n$ for projeksjonsfunksjonene. (Legg merke til at det er snakk om uendelig mange projeksjonsfunksjon*er*. Verken n eller i skal oppfattes som argumenter til $\mathcal{I}_i^n$.)

La n og m være faste tall. Skjemaet

$$f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

viser hvordan funksjonen f kan defineres fra funksjonene $g_1, \ldots, g_m$ og h. Skjemaet kalles *komposisjon*. Sier vi for eksempel at f *er komposisjon over* $g_1, \ldots, g_m$ og h, eller at f er *gitt ved komposisjon*, så betyr det at f kan defineres ved skjemaet. Skjemaet

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &= g(x_1, \ldots, x_n) \\ f(x_1, \ldots, x_n, y+1) &= h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \end{aligned}$$

viser hvordan en funksjon f kan defineres fra funksjonene g og h. Skjemaet kalles *primitiv rekursjon*. Sier vi at f *er primitiv rekursjon over* g og h, eller at f er gitt ved *primitiv rekursjon*, betyr det at f kan defineres ved skjemaet. De *primitivt rekursive funksjonene* er den minste tillukningen av de rekursive initialfunksjonene under komposisjon og primitiv rekursjon. Sier vi at en funksjon *er primitivt rekursiv*, betyr det at funksjonen er med i denne klassen. (Du bør merke deg den litt tvetydige språkbruken. Når diverse bøyningsformer av frasen "primitiv rekursiv" benyttes, må konteksten fortelle hvorvidt vi har et definisjonsskjema eller en klasse av funksjoner i tankene.)

Hvis g er en funksjon, kan en ny funksjon f defineres ved skjemaet

$$f(x_1, \ldots, x_n) = (\mu i)[g(x_1, \ldots, x_n, i)] \stackrel{\text{def}}{=} \begin{cases} \text{Den minste } i \text{ slik at } g(x_1, \ldots, x_n, i) = 0 \\ \text{og } g(x_1, \ldots, x_n, j) \text{ definert for alle } j < i. \\ \\ \text{Udefinert, hvis en slik } i \text{ ikke finnes} \end{cases}$$

Dette skjemaet kalles *minimalisering*. De *rekursive funksjonene* er den minste tillukningen av de rekursive initialfunksjonene under komposisjon, primitiv rekursjon og minimalisering.

En relasjon R er *(primitivt) rekursiv* når den karakteristiske funksjonen til relasjonen er (primitivt) rekursiv, dvs. når det finnes en (primitivt) rekursiv funksjon f med rang $\{0,1\}$ slik at $R(x_1,\ldots,x_n) \Leftrightarrow f(x_1,\ldots,x_n) = 0$. $\square$

Definisjonsskjemaene over er rigide. Formelt sett er det et ork å definere selv den enkleste funksjon. Det kan vi ikke leve med. Når vi selv synes det er passe trivielt hvordan en funksjon kan defineres ved hjelp av skjemaene, vil vi uten videre slå fast at dette er mulig. Denne trivialitetsterskelen kan være høy for en novise. Vi skal derfor gi et par eksempler. La oss si at g_1, g_2 og h er primitivt rekursive, og at

$$h'(x_1,x_2,x_3) = h(g_1(x_2,x_1,x_1),g_2(x_3))\,.$$

Da vil vi uten videre slå fast at h' er primitivt rekursiv, eller at h' er komponert av g_1, g_2 og h. Vi går ut fra leseren ser at h' kan defineres med gjentatt bruk av komposisjonsskjemaet. For eksempel slik:

$$\begin{aligned} h'(x_1,x_2,x_3) &= h(g_1'(x_1,x_2,x_3),g_2'(x_1,x_2,x_3)) \\ g_1'(x_1,x_2,x_3) &= g_1(\mathcal{I}_2^3(x_1,x_2,x_3),\mathcal{I}_1^3(x_1,x_2,x_3),\mathcal{I}_1^3(x_1,x_2,x_3)) \\ g_2'(x_1,x_2,x_3) &= g_2(\mathcal{I}_3^3(x_1,x_2,x_3))\,. \end{aligned}$$

Idéen er at projeksjonsfunksjonen brukes til å stokke om på argumentene, og til å regulere antall argumenter. La oss videre anta at

$$\begin{aligned} f(x_1,x_2,0) &= x_1 \\ f(x_1,x_2,y+1) &= h(g_1(x_2,x_1,x_1),g_2(f(x_1,x_2,y)))\,. \end{aligned}$$

Hvis vi nå sier at f er primitivt rekursiv, forventer vi at leseren henger med. Vi forventer også å bli forstått når vi for eksempel sier at f er primitiv rekursjon over g_1, g_2 og h. En formell rekursiv – og håpløst uoversiktlig – definisjon av f ser slik ut:

$$\begin{aligned} f(x_1,x_2,0) &= \mathcal{I}_1^2(x_1,x_2) \\ f(x_1,x_2,(y)) &= h''(x_1,x_2,y,f(x_1,x_2,y)) \\ h''(x_1,x_2,x_3,x_4) &= h'(\mathcal{I}_1^4(x_1,x_2,x_3,x_4),\mathcal{I}_2^4(x_1,x_2,x_3,x_4),\mathcal{I}_4^4(x_1,x_2,x_3,x_4)) \\ h'(x_1,x_2,x_3) &= h(g_1'(x_1,x_2,x_3),g_2'(x_1,x_2,x_3)) \\ g_1'(x_1,x_2,x_3) &= g_1(\mathcal{I}_2^3(x_1,x_2,x_3),\mathcal{I}_1^3(x_1,x_2,x_3),\mathcal{I}_1^3(x_1,x_2,x_3)) \\ g_2'(x_1,x_2,x_3) &= g_2(\mathcal{I}_3^3(x_1,x_2,x_3))\,. \end{aligned}$$

Vi vil også fritt bruke infiks og postfiks og mange andre notasjonsformer for rekursive funksjoner.

Lemma 3.1 *Konstantfunksjonen c_i^n er gitt ved $c_i^n(x_1,\ldots,x_n) = i$ for alle $i,n \in \boldsymbol{N}$. Funksjonen c_i^n er primitivt rekursiv for alle $i,n \in \boldsymbol{N}$.*

Bevis av Lemma 3.1. Vi har $c_0^0 = \mathcal{O}$. Vi kan definere c_0^k for $k > 1$ med komposisjonsskjemaet: $c_0^k(x_1,\ldots,x_k) = \mathcal{O}$. Vi bruker en instans av skjemaet der $m = 0$. Anta (induksjonshypotese) at c_i^k er primitivt rekursiv for alle $k \in \mathbf{N}$. Da kan c_{i+1}^k kan genereres fra c_i^k ved komposisjon av to primitivt rekursive funksjoner: $c_{i+1}^k(x_1,\ldots,x_k) = \mathcal{S}(c_i^k(x_1,\ldots,x_k))$. Ergo er c_i^n er primitivt rekursiv for alle $i,n \in \mathbf{N}$. $\square$

Lemma 3.2 *Funksjonene $+$, $\times$ og x^y (addisjon, multiplikasjon, eksponensiering) er primitivt rekursive. Den modifiserte subtraksjonsfunksjonen $\dot{-}$ er primitivt rekursiv. ($x \dot{-} y = 0$ når $y > x$, $x \dot{-} y = x \Leftrightarrow y$ (vanlig subtraksjon) ellers.)*

Bevis av Lemma 3.2. La c_0^1 og c_1^1 være funksjonene fra Lemma 3.1. Vi har

- $x + 0 = \mathcal{I}_1^1(x)$ og $x + \mathcal{S}(y) = \mathcal{S}(x + y)$
- $x \times 0 = c_0^1(x)$ og $x \times \mathcal{S}(y) = x + (x \times y)$
- $x^0 = c_1^1(x)$ og $x^{\mathcal{S}(y)} = x \times x^y$

så $+$, $\times$ og x^y er primitivt rekursive. Videre har vi at

- $P(0) = \mathcal{O}$ og $P(\mathcal{S}(y)) = \mathcal{I}_1^2(y, P(y))$
- $x \dot{-} 0 = \mathcal{I}_1^1(x)$ og $x \dot{-} \mathcal{S}(y) = P(x \dot{-} y)$.

(Her er P forgjengerfunksjonen.) Dermed er $\dot{-}$ primitivt rekursiv. □

Lemma 3.3 *De primitivt rekursive relasjonene er lukket under de utsagnslogiske operatorene.*

Bevis av Lemma 3.3. La p være den karakteristiske funksjonen for relasjonen P, og la q være den karakteristiske funksjonen for relasjonen Q. Da er den primitivt rekursive funksjonen $p(\vec{x}) \times q(\vec{y})$ den karakteristiske funksjonen for relasjonen $P(\vec{x}) \vee Q(\vec{y})$. Den primitivt rekursive funksjonen $1 \dot{-} p(\vec{x})$ er den karakteristiske funksjonen for relasjonen $\neg P(\vec{x})$. Alle andre utsagnslogiske operatorer kan uttrykkes ved hjelp av $\neg$, $\vee$ og komposisjon. Dermed holder lemmaet. □

Lemma 3.4 *Relasjonene $\leq$ og $=$ er primitivt rekursive.*

Bevis av Lemma 3.4. Den primitivt rekursive funksjonen $1 \dot{-} ((y + 1) \dot{-} x)$ er den karakteristiske funksjonen for relasjonen $x \leq y$. Så $\leq$ er primitivt rekursiv. Videre har vi $x = y \Leftrightarrow x \leq y \wedge y \leq x$. Dermed er likhetsrelasjonen primitivt rekursiv ved Lemma 3.3. □

Definisjon. Skjemaet

$$f(\vec{x}) = (\mu i \leq n)[g(\vec{x}, i)] \stackrel{\text{def}}{=} \begin{cases} \text{Den minste } i \leq n \text{ slik at } g(x_1, \ldots, x_n, i) = 0 \\ 0, \text{ hvis en slik } i \text{ ikke finnes} \end{cases}$$

viser hvordan funksjonen f kan genereres fra funksjonen g. Dette skjemaet kalles *bundet minimalisering.* □

Lemma 3.5 *De primitivt rekursive funksjonene er lukket under bundet sum ($\sum_{i \leq n} f(\vec{x}, i)$), bundet produkt ($\prod_{i \leq n} f(\vec{x}, i)$) og bundet minimalisering.*

Bevis av Lemma 3.5 Vi har

$$\sum_{i\leq 0} f(\vec{x},i) = f(\vec{x},0) \quad \text{og} \quad \sum_{i\leq \mathcal{S}(y)} f(\vec{x},i) = f(\vec{x},\mathcal{S}(y)) + \sum_{i\leq y} f(\vec{x},i)\ .$$

Dermed er det lett å se at $\sum_{i\leq n} f(\vec{x},i)$ kan defineres ved primitivt rekursive skjema når f kan defineres ved primitiv rekursive skjema. At de primitivt rekursive funksjonene også er lukket under bundet produkt kan leseren forsikre seg om på egen hånd. La $\overline{x} \stackrel{\text{def}}{=} 1 \dot{-} (1 \dot{-} x)$. Så $\overline{x} = 0$ når $x = 0$, og $\overline{x} = 1$ når $x \neq 0$. De primitivt rekursive funksjonene er lukket under bundet minimalisering fordi

$$(\mu i \leq y)[g(\vec{x},i)] \quad = \quad (\sum_{z\leq y} \prod_{i\leq z} \overline{g(\vec{x},i)}) \times (1 \dot{-} \prod_{i\leq y} \overline{g(\vec{x},i)}).$$

Den siste likheten er innlysende, ikke sant? □

Lemma 3.6 *De primitivt rekursive relasjonene er lukket under de bundne første ordens kvantorene* $(\exists i \leq n)$ *og* $(\forall i \leq n)$.

Bevis av Lemma 3.6. La p være den karakteristiske funksjonen til den primitivt rekursive relasjonen $P(\vec{x},y)$. Da er den primitivt rekursive funksjonen $\prod_{i\leq n} p(\vec{x},i)$ den karakteristiske funksjon for relasjonen $(\exists i \leq n)[P(\vec{x},i)]$. Dermed ser vi at de primitivt rekursive relasjonene er lukket under bundet eksistenskvantor. At de også er lukket under bundet allkvantor følger fra Lemma 3.3 og at $(\forall i \leq n)[P(\vec{x},i)] \Leftrightarrow \neg(\exists i \leq n)[\neg P(\vec{x},i)]$

Lemma 3.7 *Funksjonen $p(n)$ som gir det n'te primtallet, er primitivt rekursiv. (Det 0'te primtallet er 2, det første er 3, ...) Funksjonen $m[i]$ som gir eksponenten til det i'te primtallet i primtallsfaktoriseringen av m, er primitivt rekursiv. (Vi lar $0[i] = 0$ for alle i.)*

Bevis av Lemma 3.7. La $P(x) \stackrel{\text{def}}{\Leftrightarrow} (\forall y,z \leq x)[(y+2)\times(z+2) \neq x]$. Ved lemmaene over er relasjonen P primitivt rekursiv, og vi ser at $P(x)$ sier at x er et primtall. Dermed er det en smal sak å definere en funksjon f primitivt rekursivt slik at $f(x) = 1$ når x er et primtall, og $f(x) = 0$ når x ikke er det. La så $g(y) = \sum_{i\leq y} f(i)$. Da gir $g(y)$ antall primtall mindre eller lik y. Det er et faktum at det n'te primtallet er mindre enn 2^{n+1}. Dermed har vi $p(n) = (\mu i \leq 2^{n+1})[g(i) = n+1]$. Ved lemmaene over er p primitivt rekursiv.

Eksponenten til det i'te primtallet i primtallsfaktoriseringen av m må være den største j slik at m er delelig på $p(i)^j$. Dermed har vi at

$$m[i] \quad = \quad (\mu j \leq m)\ [\ (\exists x \leq m)[x \times p(i)^j = m]\ \wedge\ (\forall x \leq m)[x \times p(i)^{j+1} \neq m]\ ]$$

og lemmaene over gir at $m[i]$ er primitivt rekursiv. □

Hvorfor er vi så ivrige etter å finne en primitivt rekursiv definisjon av $p(i)$ og den noget esoteriske funksjonen $m[i]$? Er ikke det siste lemmaet myntet på spesielt interesserte? Nei. Det har betydelige konsekvenser at nettopp disse funksjonene er primitivt rekursive. Ethvert heltall ekte større enn 1 har en entydig primtallsfaktorisering. Dette skal vi benytte til å representere en sekvens av tall ved hjelp av ett enkelt tall. Vi koder sekvensen $x_1,\ldots,x_n$ ved hjelp av tallet $y = p(0)^{x_1} \times p(1)^{x_2} \times \cdots \times p(n \Leftrightarrow 1)^{x_n}$. Dermed har vi $x_i = y[i \dot{-} 1]$ for $i = 1,\ldots,k$. Beviset av neste lemma forteller oss at det er essensielt at en slik koding og dekoding kan gjennomføres ved hjelp av primitivt rekursive funksjoner.

Definisjon. La n og k være faste tall og la $j_i(y) \leq y$ for $i = 1, \ldots k$. Skjemaet

$$\begin{aligned} f(x_1, \ldots, x_n, 0) &= g(x_1, \ldots, x_n) \\ f(x_1, \ldots, x_n, y+1) &= h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, j_1(y)), \ldots, f(x_1, \ldots, x_n, j_k(y))) \end{aligned}$$

viser hvordan funksjonen f kan defineres ved funksjonene $g, h, j_1, \ldots, j_k$. Dette skjemaet kalles *verdiforløp rekursjon.*

La k og n være faste tall, og la f_i for $i = 1, \ldots, k$ være gitt ved

$$\begin{aligned} f_i(x_1, \ldots, x_n, 0) &= g_i(x_1, \ldots, x_n) \\ f_i(x_1, \ldots, x_n, y+1) &= h_i(x_1, \ldots, x_n, y, f_1(x_1, \ldots, x_n, y), \ldots, f_k(x_1, \ldots, x_n, y)) \,. \end{aligned}$$

Dette skjemaet viser hvordan funksjonene $f_1, \ldots, f_k$ kan defineres ved funksjonene $g_1, \ldots, g_k$ og $h_1, \ldots, h_k$. Skjemaet kalles *simultan rekursjon.*

Skjemaet

$$\begin{aligned} f(x, 0) &= g(x) \\ f(x, y+1) &= h(x, y, f(j(x, y), y)) \end{aligned}$$

viser hvordan funksjonen f kan defineres ved funksjonene g, h og j. Dette skjemaet kalles *rekursjon med parametersubstitusjon.*

Skjemaet

$$f(x_1, \ldots, x_n) = \begin{cases} g_1(x_1, \ldots, x_n) & \text{hvis } h(x_1, \ldots, x_n) = 0 \\ g_2(x_1, \ldots, x_n) & \text{ellers} \end{cases}$$

viser hvordan en funksjon f kan defineres ved funksjonene g_1, g_2 og h. Dette skjemaet kan vi kalle *tilfelle-definisjon.* (Du har nettopp sett et dårlig forsøk på å oversette *definition by cases.*) □

Lemma 3.8 *De primitivt rekursive funksjonene er lukket under (i) verdiforløp rekursjon, (ii) simultan rekursjon, (iii) rekursjon med parametersubstitusjon og (iv) tilfelle-definisjon.*

Bevis av Lemma 3.8. (i) Anta at $j_1, \ldots, j_k$, g og h er primitivt rekursive, og at $j_i(y) \leq y$ for $i = 1, \ldots k$. La $\vec{x}$ stå for $x_1, \ldots, x_n$, og la f være gitt som i definisjonen av verdiforløp-rekursjon. Vi definerer

$$\begin{aligned} F(\vec{x}, 0) &= p(0)^{g(\vec{x})} \\ F(\vec{x}, y+1) &= F(\vec{x}, y) \times p(y+1)^{h(\vec{x}, F(\vec{x},y)[j_1(y)], \ldots, F(\vec{x},y)[j_k(y)])} \,. \end{aligned}$$

Denne definisjonen av F kan lett skrives om til en ren primitivt rekursiv definisjon ved hjelp av lemmaene over. Så F er primitivt rekursiv. Siden $j_i(y) \leq y$ for $i = 1, \ldots k$, så har vi

$$F(\vec{x}, y) = p(0)^{f(\vec{x},0)} \times p(1)^{f(\vec{x},1)} \times \cdots \times p(y)^{f(\vec{x},y)} \,.$$

Dette betyr at f er gitt ved komposisjonen $f(\vec{x}, y) = F(\vec{x}, y)[y]$. Dermed er f primitivt rekursiv.

(ii) Anta at funksjonene $g_1, \ldots, g_k$ og $h_1, \ldots, h_k$ er primitivt rekursive, og la $f_1, \ldots, f_k$ være gitt som i definisjonen av simultan rekursjon. Vi definerer

$$\begin{aligned} F(\vec{x}, 0) &= p(1)^{g_1(\vec{x})} \times \cdots \times p(k)^{g_k(\vec{x})} \\ F(\vec{x}, y+1) &= p(1)^{h_1(\vec{x}, y, F(\vec{x},y)[1], \ldots, F(\vec{x},y)[k])} \times \cdots \times p(k)^{h_k(\vec{x}, y, F(\vec{x},y)[1], \ldots, F(\vec{x},y)[k])} \end{aligned}$$

Denne definisjonen er det rimelig enkelt å skrive om til en ren primitivt rekursiv definisjon ved hjelp av lemmaene over. Vi konkluderer derfor at F er primitivt rekursiv. Videre har vi at

$$F(\vec{x}, y) \quad = \quad p(1)^{f_1(\vec{x},y)} \times p(2)^{f_2(\vec{x},y)} \times \ldots \times p(k)^{f_k(\vec{x},y)} .$$

Dermed ser vi av komposisjonen $f_i(\vec{x}, y) = F(\vec{x}, y)[i]$ at f_i er en primitivt rekursive funksjon for $i = 1, \ldots, k$.

Vi dropper bevisene av (iii) og (iv). Beviset for (iii) er klinete. Beviset for (iv) er enkelt. □

De første fibonaccitallene er $0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots$. Hvert tall i rekken er summen av de to foregående, og de to første tallene er henholdsvis 0 og 1. Funksjonen $f(n)$ som gir det n'te tallet i rekken, er gitt ved

$$f(0) = 0 \qquad\qquad f(1) = 1 \qquad\qquad f(n+2) = f(n) + f(n+1) .$$

Dette er et eksempel på tilfelle-definisjon og verdiforløp-rekursjon. Lemmaene over forteller oss at f er primitivt rekursiv.

Definisjon. La p_i være det i'te primtallet. ($p_0 = 2, p_1 = 3, \ldots$) *Sekvenstallet* $\langle x_1, \ldots, x_n \rangle$ er gitt ved $p_0^n \times p_1^{x_1} \times \cdots \times p_n^{x_n}$. Vi kaller x_i for det i'te *koordinatet* i sekvensen $\langle x_1, \ldots, x_n \rangle$ (der $1 \leq i \leq n$). Vi lar $lh(x)$ være funksjonen som gir antall koordinater i x hvis x er et sekvenstall (og 0 ellers). Vi lar $(\langle x_1, \ldots, x_n \rangle)_i \stackrel{\text{def}}{=} x_i$ når $1 \leq i \leq n$, og vi lar $(x)_i \stackrel{\text{def}}{=} 0$ hvis x ikke er et sekvenstall eller hvis det ikke er tilfellet at $1 \leq i \leq n$. □

Et sekvenstall representerer en sekvens av tall entydig, og enhver sekvens av tall kan representeres av et sekvenstall. Dette følger av hva vi har sagt om primtallskoding tidligere.

Lemma 3.9 *Funksjonen $\langle x_1, \ldots, x_n \rangle$ er primitivt rekursiv. Den karakteristiske funksjonen til mengden av sekvenstall er primitivt rekursiv, dvs. funksjonen som gir 0 hvis x er et sekvenstall og 1 ellers, er primitivt rekursiv. Videre er funksjonene lh og $(x)_i$ primitivt rekursive.*

Bevis av Lemma 3.9. Dette følger greit fra lemmaer vi har bevist tidligere. □

Definisjon. Vi definerer $\lceil f \rceil$ induktivt over den rekursive definisjonen av en funksjon f. Vi lar

- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 0 \rangle$ hvis $f = \mathcal{O}$
- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 1 \rangle$ hvis $f = \mathcal{S}$
- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 2, n, i \rangle$ hvis $f = \mathcal{I}_i^n$ for $0 < i \leq n$
- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 3, \lceil h \rceil, \lceil g_1 \rceil, \ldots, \lceil g_m \rceil \rangle$ når f er komposisjon av $g_1, \ldots, g_m$ og h
- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 4, \lceil g \rceil, \lceil h \rceil \rangle$ når f er primitiv rekursjon over g og h
- $\lceil f \rceil \stackrel{\text{def}}{=} \langle 5, \lceil g \rceil \rangle$ når f er definert fra g ved hjelp av minimalisering.

La $e = \lceil f \rceil$. Vi skriver $\{e\}(\vec{x})$ for $f(\vec{x})$, og vi sier at e er en *rekursiv indeks* for f. □

Vi skal bevisst og systematisk være unøyaktig i vår omgang med funksjoner, og vi skal hemningsløst blande sammen to forskjellige betydninger av uttrykk som $f(x)$ og $\{e\}(x)$.

Den siste definisjonen vitner til de grader om det. Av og til antar vi at en eller annen rekursiv definisjon hefter ved en funksjon, dvs. vi antar at vi har en eller annen rekursiv definisjon av funksjonen for hånden selv om en slik definisjon ikke er eksplisitt gitt. Det er for eksempel tilfellet i definisjonen av $\lceil f \rceil$. Av og til betrakter vi en funksjon rent ekstensjonalt, altså som en mengde av par. Det er for eksempel tilfellet når vi sier at $x + x = 2 \times x$. Det finnes uendelig mange rekursive definisjoner av funksjonene $+$ og $\times$. Likevel bruker vi kanskje uttrykket $\lceil + \rceil$, selv om $\lceil\ \rceil$ strengt talt er en avbildning fra rekursive *definisjoner* inn i sekvenstallene, og ikke en avbildning fra rekursive *funksjoner* inn i sekvenstallene. I slike situasjoner må man velge en definisjon av $+$ for å gi uttrykket $\lceil + \rceil$ mening.

Av og til kan det virke klargjørende å se på en rekursiv indeks som programkode. La e være en rekursiv indeks for funksjonen f. Ved hjelp av definisjonen over kan man da lese ut av e hvordan en rekursiv definisjon av funksjonen f ser ut. Den rekursive definisjonen gir ganske direkte en algoritme for å beregne f. Det er for eksempel lett å lage et Pascal[1]-aktig program. Skjemaet for primitiv rekursjon svarer til en FOR-løkke. Skjemaet vi kaller minimalisering svarer til en WHILE-løkke.

Definisjon. Vi definerer et *beregningstre* for $f(\vec{x})$ der f er en rekursiv funksjon.

- La $\lceil f \rceil = \langle 0 \rangle$. (Så $f = \mathcal{O}$.) Da er sekvenstallet $\langle \lceil f \rceil, 0 \rangle$ et beregningstre for f.
- La $\lceil f \rceil = \langle 1 \rangle$. (Så $f = \mathcal{S}$.) Da er sekvenstallet $\langle \lceil f \rceil, x, x+1 \rangle$ et beregningstre for $f(x)$.
- La $\lceil f \rceil = \langle 2, n, i \rangle$. (Så $f = \mathcal{I}_i^n$.) Da er sekvenstallet $\langle \lceil f \rceil, x_1, \ldots, x_n, x_i \rangle$ et beregningstre for $f(x_1, \ldots, x_n)$.
- La $\lceil f \rceil = \langle 3, \lceil h \rceil, \lceil g_1 \rceil, \ldots, \lceil g_m \rceil \rangle$. (Så $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$.) Videre la t_i være et beregningstre for $g_i(\vec{x})$ og la z_i være siste koordinat i t_i for $i = 1, \ldots, m$. La t være et beregningstre for $h(z_1, \ldots, z_m)$ og la z være siste koordinat i t. Da er sekvenstallet $\langle \lceil f \rceil, t, t_1, \ldots, t_m, z \rangle$ et beregningstre for $f(\vec{x})$.
- La $\lceil f \rceil \stackrel{\text{def}}{=} \langle 4, \lceil g \rceil, \lceil h \rceil \rangle$. (Så $f(\vec{x}, 0) = g(\vec{x})$ og $f(\vec{x}, y+1) = h(\vec{x}, y, f(\vec{x}, y))$.) La t_0 være et beregningstre for $g(\vec{x})$ og la z_0 være siste koordinat i t_0. Videre la t_{i+1} være et beregningstre for $h(\vec{x}, i, z_i)$ og la z_{i+1} være siste koordinat i t_{i+1}. Da er sekvenstallet $\langle \lceil f \rceil, t_0, t_1, \ldots, t_y, z_y \rangle$ et beregningstre for $\{\lceil f \rceil\}(\vec{x}, y)$.
- La $\lceil f \rceil \stackrel{\text{def}}{=} \langle 5, \lceil g \rceil \rangle$ (Så $f(\vec{x}, 0) = (\mu i)[g(\vec{x}, i)]$.) La t_i være et beregningstre for $g(\vec{x}, i)$ der siste koordinat er forskjellig fra 0 for $i = 0, 1, \ldots m \Leftrightarrow 1$. La t_m være et beregningstre for $g(\vec{x}, m)$ der siste koordinat er 0. Da er sekvenstallet $\langle \lceil f \rceil, t_0, t_1, \ldots, t_m, m \rangle$ et beregningstre for $f(\vec{x})$.

La $n \geq 1$ og la $T_n(e, x_1, \ldots, x_n, t)$ bety at t er et beregningstre for $\{e\}(x_1, \ldots, x_n)$. Relasjonen T_n kalles Kleenes T-predikat. Hvis vi sier at $f(x_1, \ldots, x_n)$ *konvergerer*, så mener vi det finnes et beregningstre t slik at relasjonen $T_n(\lceil f \rceil, x_1, \ldots, x_n, t)$ holder. Sier vi at $f(x_1, \ldots, x_n)$ *divergerer*, så mener vi at $f(x_1, \ldots, x_n)$ ikke konvergerer. $\square$

At $f(x_1, \ldots, x_n)$ konvergerer betyr i bunn og grunn at det er mulig å beregne f i argumentene $x_1, \ldots, x_n$. Det er lett å se at enhver primitivt rekursiv funksjon konvergerer i alle argumenter. Dermed er enhver primitivt rekursiv funksjon total. Det er også rimelig lett å se at det finnes rekursive funksjoner som divergerer i noen argumenter. En rekursiv

[1] Blaise Pascal, fransk filosof, matematiker og naturforsker, 1623-1662

funksjon kan altså være partiell, og de primitivt rekursive funksjonene må være en ekte delmengde av de rekursive. Vi skal se at det også finnes totale funksjoner som er rekursive, men ikke primitivt rekursive. Vi vil også skrive $f(\vec{x}) = g(\vec{x})$ når f og g kan være partielle rekursive funksjoner. Da mener vi at enten divergerer både f og g i $\vec{x}$, eller så konvergerer begge og verdien av $f(\vec{x})$ er den samme som verdien av $g(\vec{x})$.

Lemma 3.10 *Kleenes T-predikat er primitivt rekursivt.*

Bevis av Lemma 3.10. Vi har sett lemmaer som sier at koding og dekoding av sekvenser er primitivt rekursive operasjoner, og vi har lemmaer som sier at de primitivt rekursive funksjonene er lukket under diverse definisjonsskjemaer. Ved å bruke disse lemmaene kan man vise at Kleenes T-predikat er primitivt rekursivt. Beviset er omfattende, men byr ikke på noen prinsipielle vanskeligheter. Det kreves ingen metoder og teknikker utover dem vi allerede har stiftet bekjentskap med. □

Teorem 3.11 (Kleenes normalformteorem) *La U være en primitiv rekursiv funksjon slik at $U(x)$ gir siste koordinat i x når x er et sekvenstall. La T_n være Kleenes T-predikat. For enhver n-ær rekursiv funksjon f finnes et fast tall e slik at*

$$f(x_1, \ldots, x_n) = U((\mu t)[T_n(e, x_1, \ldots, x_n, t)]) .$$

Bevis av Teorem 3.11. La $e = \lceil f \rceil$. Hvis det finnes et beregningstre t for $\{e\}(x_1, \ldots, x_n)$, så ligger tallet $f(x_1, \ldots, x_n)$ i siste koordinat i t. □

Definisjon. Anta at vi har en opptelling av en klasse funksjoner. (Det vil si at vi har en surjeksjon ψ fra de naturlige tallene inn i klassen. Vi sier at e er en indeks for funksjonen g i klassen om $\psi(e) = g$.) En funksjon f er universalfunksjon for klassen (under denne opptellingen) om det for enhver unær funksjon g i klassen og for enhver indeks e for g er slik at $f(e, x) = g(x)$.

Teorem 3.12 *Det finnes en rekursiv universalfunksjon for de rekursive funksjonene.*

Bevis av Teorem 3.12. Ved Kleenes normalformteorem vil $f(e, x) \stackrel{\text{def}}{=} U((\mu t)[T_1(e, x, t)])$ være en universalfunksjon for de rekursive funksjonene. Vi har også at U og T_1 er (primitivt) rekursive. Dermed er f rekursiv siden de rekursive funksjonene er lukket under komposisjon og minimalisering. □

Teorem 3.12 svarer til teoremet i teorien om Turingmaskiner som sier at det finnes en universell Turingmaskin. Når $f(e, x)$ er en universalfunksjon for de rekursive funksjonene, kan vi tenke på e som et program og på x som input til programmet. At programmet e tilsynelatende tar kun ett heltall x som input er ikke vesentlig. Ved kodeteknikkene vi har skissert over kan x representere enhver tenkelig form for input. Så en universalfunksjon for de rekursive funksjonene er i en forstand datamaskinen med stor D, den programmérbare maskinen hvis regnekapasitet ikke kjenner grenser. At det finnes rekursive univeralfunksjoner for de rekursive funksjonene er ikke opplagt. For eksempel holder ikke et tilsvarende teorem for de primitivt rekursive funksjonene:

Teorem 3.13 *Det finnes ikke en primitivt rekursiv universalfunksjon for de primitivt rekursive funksjonene.*

Bevis av Teorem 3.13. Vi teller opp de primitivt rekursive funksjonene på samme måte som vi talte opp de rekursive funksjonene over. Vi bare kutter ut skjemaet for minimalisering. For hver primitivt rekursive f finnes da et tall e slik at $f(\vec{x}) = \{e\}(\vec{x})$. Anta så at det finnes en primitivt rekursiv universalfunksjon ρ for de primitivt rekursive funksjonene, og la $g(x) \stackrel{\text{def}}{=} \rho(x,x) + 1$. Hvis ρ er primitivt rekursiv, så vil g være det. Da har vi

$$\{\lceil g \rceil\}(\lceil g \rceil) \;=\; g(\lceil g \rceil) \;=\; \rho(\lceil g \rceil, \lceil g \rceil) + 1 \;=\; \{\lceil g \rceil\}(\lceil g \rceil) + 1$$

og dette er opplagt tøv. (Den andre likheten holder ved definisjonen av g. Den tredje likheten holder fordi ρ er en universalfunksjon.) □

Funksjonene ρ og g som opptrer i det siste beviset er opplagt både totale og rekursive. Dermed har vi sett eksempler på totale beregnbare funksjoner som ikke er primitivt rekursive. Teknikken som benyttes i beviset kalles *diagonalisering*. For enhver interessant klasse av totale rekursive funksjoner kan man ved hjelp av diagonalisering vise at en universalfunksjon for klassen ikke kan være med i klassen selv. Det vil for eksempel gjelde for klassen av funksjoner som kan beregnes i polynom tid ved hjelp av en Turingmaskin. (Så hvis du skal lage et programmeringsspråk som er slik at ethvert program i språket terminerer, ... ja, da bør du ikke forsøke å skrive en interpreter for språket i språket selv.) Men hvorfor kan ikke diagonaliseringsteknikk benyttes til å vise at en universalfunksjon for de rekursive funksjonene ikke kan være rekursiv? Fordi det motsatte er sant selvsagt, men hvorfor holder ikke resonnementet i beviset av Teorem 3.13 for de rekursive funksjonene? Vi lar det spørsmålet henge i luften. Nå skal vi se at diagonaliseringsteknikk *kan* benyttes til å vise at det finnes totale og veldefinerte funksjoner som ikke er rekursive.

Teorem 3.14 (Stoppeproblemet) *Funksjonen*

$$\xi(x,y) \stackrel{\text{def}}{=} \begin{cases} 0 & \textit{hvis } \{x\}(y) \textit{ konvergerer} \\ 1 & \textit{ellers} \end{cases}$$

er ikke rekursiv.

Bevis av Teorem 3.14. Anta at ξ er rekursiv. La $f(x) \stackrel{\text{def}}{=} \{x\}(x) + 1$ når $\xi(x,x) = 0$. La $f(x) \stackrel{\text{def}}{=} 1$ ellers. Siden ξ er rekursiv, vil f være rekursiv. Dermed kan vi snakke om en rekursiv indeks $\lceil f \rceil$ for f. La oss nå se på verdien av $f(\lceil f \rceil)$. Vi må se på to tilfeller: (i) $\xi(\lceil f \rceil, \lceil f \rceil) = 0$ og (ii) $\xi(\lceil f \rceil, \lceil f \rceil) = 1$. Anta (i). Da har vi $f(\lceil f \rceil) = \{\lceil f \rceil\}(\lceil f \rceil)$ fordi $\lceil f \rceil$ er en indeks for f, men vi har også $f(\lceil f \rceil) = \{\lceil f \rceil\}(\lceil f \rceil) + 1$ fra definisjonen av f. Dermed har vi viklet oss inn i en selvmotsigelse. Anta (ii). Siden $\xi(\lceil f \rceil, \lceil f \rceil) = 1$, så divergerer $f(\lceil f \rceil)$. Ved definisjonen av f har vi at $f(\lceil f \rceil) = 1$. Selvmotsigelse. □

Teorem 3.14 tilsvarer "stoppeproblemet" i teorien om Turingmaskiner: Det er ikke mulig for en Turingmaskin å avgjøre hvorvidt en vilkårlig Turingmaskin med gitt input stanser. Resultatet ble unnfanget av Alan Turing selv og publisert i 1937.

3.2 Rekursive og rekursivt tellbare mengder

Definisjon. En mengde av hele tall er *rekursivt tellbar* (r.t.) om den er verdiområdet[2] til en total rekursiv unær funksjon. I tillegg regner vi den tomme mengden som en rekursivt

[2] Et verdiområde kalles også ofte for et bilde eller for et kodomene.

tellbar mengde. En n-ær relasjon R er *rekursivt tellbar* (r.t.) dersom mengden av sekvenstall $\langle x_1, \ldots, x_n \rangle$ slik at $R(x_1, \ldots, x_n)$ holder, er en r.t. mengde. En mengde (relasjon) er *rekursiv* dersom den karakteristiske funksjonen til mengden (relasjonen) er rekursiv. □

Litt intuisjon: Hvis en mengde A er verdiområdet til en total rekursiv funksjon f, så finnes det en algoritme for å liste medlemmene i A. Vi kan effektivt generere listen $f(0), f(1), f(2), \ldots$. Dette betyr ikke at vi har en algoritme for å avgjøre om et gitt element a er medlem i A. Hvis $a \in A$, så kan det bekreftes ved å generere listen inntil a dukker opp, men vi kan aldri bekrefte $a \notin A$. På et gitt tidspunkt vil vi aldri ha generert mer enn en endelig del av listen. Det kan hende at a dukker opp i listen dersom vi genererer en liten bit til av den. Hvis den karakteristiske funksjonen til en mengde er rekursiv, så har vi en algoritme for å avgjøre om et vilkårlig element er med i mengden. Vi har altså delvis algoritmisk kontroll over de rekursivt tellbare mengdene. Vi har full algoritmisk kontroll over de rekursive mengdene.

Teorem 3.15 *La A være en mengde. Det tre påstandene under er ekvivalente.*

(i) *A er rekrusivt tellbar.*

(ii) *A er definisjonsområdet til en rekursiv funksjon.*

(iii) *Det finnes en primitivt rekursiv relasjon S slik at $x \in A \Leftrightarrow (\exists y)[S(x,y)]$.*

Bevis av Teorem 3.15. (i) $\Rightarrow$ (ii). Siden A er r.t, så er A verdiområdet til en total rekursiv funksjon f. La $g(x) = (\mu i)[f(i) = x]$. Da er g rekursiv og A er definisjonsområdet til g.

(ii) $\Rightarrow$ (iii). La A være definisjonsområdet til f. Da vil $x \in A \Leftrightarrow (\exists y)[T_1(\lceil f \rceil, x, y)]$ der T_1 er Kleenes primitivt rekursive T-predikat. Så la $S(x,y) \overset{\text{def}}{\Leftrightarrow} T_1(\lceil f \rceil, x, y)$ og alt er okay.

(iii) $\Rightarrow$ (i). Hvis A er endelig eller tom, er beviset uproblematisk. Anta derfor at A er uendelig og at $x \in A \Leftrightarrow (\exists y)[S(x,y)]$. La

$$\begin{aligned} f(0) &\overset{\text{def}}{=} (\mu i)[lh(i) = 2 \ \wedge \ S((i)_1, (i)_2)] \\ f(x+1) &\overset{\text{def}}{=} (\mu i)[i > f(x) \ \wedge \ lh(i) = 2 \ \wedge \ S((i)_1, (i)_2)] \\ g(x) &\overset{\text{def}}{=} (f(x))_1 \, . \end{aligned}$$

Da er A verdiområdet til g, og g er både total og rekursiv. □

Det siste teoremet gir oss en opptelling av r.t. mengdene. Siden enhver r.t. mengde er definisjonsområdet til en eller annen rekursiv funksjon, blir neste definisjon meningsfull.

Definisjon. Vi definerer den e'te r.t. mengden W_e ved

$$W_e = \begin{cases} \{x \mid \{e\}(x) \text{ konvergerer}\} & \text{om } \{e\} \text{ er en unær funksjon} \\ \emptyset & \text{ellers.} \quad \square \end{cases}$$

Teorem 3.16 *En mengde A er rekursiv hvis og bare hvis både A og komplementmengden $\overline{A}$ er r.t.*

Bevis av Teorem 3.16. Det er lett å se at teoremet holder når $A = \emptyset$ eller når $A = \mathbf{N}$.

Anta så at A er rekursiv, at $A \neq \emptyset$ og $A \neq \mathbf{N}$. La a_0 være et fast element i A. Videre la

$$f(x) = \begin{cases} x & \text{om } x \in A \\ a_0 & \text{ellers.} \end{cases}$$

Da er A verdiområdet til f, og f er både total og rekursiv. Helt analogt kan vi konstruere en total og rekursiv funksjon g slik at $\overline{A}$ er verdiområdet til g. Ergo er A og $\overline{A}$ r.t.

Anta at både A og $\overline{A}$ er r.t. mengder. Da finnes en total rekursiv funksjon f slik at A er verdiområdet til f, og en totalt rekursiv funksjon g slik at $\overline{A}$ er verdiområdet til g. La

$$h'(x) \;=\; (\mu i)[x = f(i) \vee x = g(i)]$$

og la

$$h(x) \;=\; \begin{cases} 0 & \text{om } x = f(h'(x)) \\ 1 & \text{om } x = g(h'(x)) \end{cases}$$

Da er h den karakteristiske funksjonen til A. Det er lett å se at h er rekursiv. □

For å gi leseren en intuitiv forståelse av begrepene skal vi ta for oss en mer uformell variant av det siste beviset. Anta at A er rekursiv. Da kan vi effektivt avgjøre om x er med i A eller ikke. Dermed har vi en algoritme for å liste opp $\overline{A}$: Trinn 0. Test om 0 er med i A. Hvis "nei", legg 0 til listen. Trinn 1. Test om 1 er med i A. Hvis "nei", legg 1 til listen. ... og så videre. Tilsvarende har vi en algoritme for å liste opp elementene i A. Dermed er både A og $\overline{A}$ r.t. mengder.

Anta så at både A og $\overline{A}$ er r.t. mengder. Det betyr at vi har en algoritme som lister opp elementene i A, og en algoritme som lister opp elementene i $\overline{A}$. Nå skal vi lage en algoritme for å avgjøre om en vilkårlig x er med i A eller ikke. Her er den: List opp A og $\overline{A}$ parallelt. Hvis x forekommer i opplistingen av A, så kan algoritmen terminere og svare "Ja, x er med i A". Hvis x forkommer i opplistingen av $\overline{A}$, så kan algoritmen terminere og svare "Nei". Siden x enten forekommer i A eller $\overline{A}$, så vil algoritmen før eller siden gi en output. Dermed er A er rekursiv mengde.

Definisjon. Vi definerer den *komplette r.t. mengden* K ved $K = \{\langle x, y\rangle \mid x \in W_y\}$. □

Teorem 3.17 *La A være en r.t. mengde. Da finnes det en primitivt rekursiv funksjon f slik at $x \in A \Leftrightarrow f(x) \in K$.*

Bevis av Teorem 3.17. Siden A er en r.t. mengde, så finnes det en rekursiv indeks n slik at $A = W_n$. La $f(x) = \langle x, n\rangle$. Da er f primitivt rekursiv ved Lemma 3.9. Ved definisjonen av K, har vi $x \in A \Leftrightarrow f(x) \in K$. □

La oss forsøke å få en intuitiv forståelse av den komplette r.t. mengden K. Anta en eller annen opptelling av mengden av Turingmaskiner, og en eller annen opptelling av mengden av mulige input til en Turingmaskin. Da kan man tolke det at m er med i den n'te r.t. mengden, dvs. $m \in W_n$, som at Turingmaskin nummer m stanser med input nummer n. Dette betyr at hvis man kan avgjøre hvorvidt sekvenstallet $\langle m, n\rangle$ er med i K, så kan man også avgjøre stoppeproblemet. Det neste teoremet sier at K ikke er en rekursiv mengde. Denne innsikten kan tolkes som at stoppeproblemet for Turingmaskiner er uavgjørbart. Teoremet sier også at K er en r.t. mengde. Det betyr at vi har en algoritme som lister opp alle par α, M slik at Turingmaskinen M stanser med input α.

Teorem 3.18 *Mengden K er r.t. men ikke rekursiv.*

Bevis av Teorem 3.18 Husk at T_1 er Kleenes T-predikat for unære funksjoner. La

$$f(x) = \begin{cases} (\mu y)[T_1((x)_2, (x)_1, y)] & \text{om } lh(x) = 2 \\ \textit{udefinert} & \text{ellers.} \end{cases}$$

Da er f en rekursiv funksjon, og K er definisjonsområdet til f. Dermed forteller Teorem 3.15 oss at K er en r.t. mengde.

Anta så at K er rekursiv. Da er også mengden $K_1 \stackrel{\text{def}}{=} \{x \mid \langle x, x\rangle \in K\}$ rekursiv. La $\overline{K}_1$ være komplementmengden til K_1. Ved Teorem 3.16 er $\overline{K}_1$ en r.t. mengde. Det betyr at det finnes en indeks n slik at $\overline{K}_1 = W_n$. Dermed

$$n \in \overline{K}_1 \quad \Leftrightarrow \quad n \in W_n \quad \Leftrightarrow \quad \langle n, n\rangle \in K \quad \Leftrightarrow \quad n \in K_1 \, .$$

Selvmotsigelse. (Den første ekvivalensen holder fordi $\overline{K}_1 = W_n$, den andre ved definisjonen av K, den tredje ved definisjonen av K_1.) $\square$

Når man sier at et problem (spørsmål) er *uavgjørbart*, så mener man at det ikke finnes en algoritme for å løse problemet (besvare spørsmålet). Teorem 3.18 gir en strategi for å vise at et problem er uavgjørbart. Man viser at hvis det finnes en algoritme som løser problemet, så finnes det også en algoritme som avgjør medlemskap i K. (Dette kalles gjerne å *redusere stoppeproblemet til problemet.*) Deretter brukes Teorem 3.18 til å konkludere at problemet ikke er avgjørbart.

La oss utbrodere dette litt. Mengden K gir en "grense" for hva vi har algoritmisk kontroll over. Ethvert matematisk veldefinert problem kan assosieres med en mengde A slik at å løse en instans av problemet koker ned til å besvare spørsmålet "$n \in A$?". Viser man at det finnes en total rekursiv funksjon f slik at $x \in K \Leftrightarrow f(x) \in A$, så må problemet være uavgjørbart. Viser man at det finnes en total rekursiv funksjon f slik at $f(x) \in K \Leftrightarrow x \in A$, så kan problemet delvis behandles av en algoritme. Det kan behandles i den forstand at hvis x er medlem i mengden A, så kan medlemskapet bekreftes av en algoritme. Ad denne vei kan vi med matematisk presisjon studere og forstå både hva datamaskiner kan og ikke kan. Det må da være et matnyttig studium? Mengden K er matnyttig!

3.3 Om bruk av begreper, intuisjon og Turings teorem

Holder vi oss til dette kapitlets definisjoner, gir det bare mening å bruke adjektivfrasene "rekursiv" og "rekursivt tellbar" om delmengder av de naturlige tallene. Det går imidlertid glatt å generalisere disse begrepene. La $A \subseteq B$ der B er en tellbar mengde av "hva-som-helst". La $\Phi : B \to \mathbf{N}$ være en beregnbar en-til-en funksjon (injeksjon). Da sier vi at A er rekursiv dersom $\Phi(A)$ er rekursiv, og at A er rekursivt tellbar dersom $\Phi(A)$ er rekursivt tellbar. (Her er $\Phi(A) = \{x \mid \text{finnes } y \in A \text{ s.a. } \Phi(y) = x\}$.) Vi krever at Φ skal være beregnbar og en-til-en. Det betyr at vi har en algoritme for å avgjøre medlemskap i A når A er rekursiv, og en algoritme for å liste elementene i A når A er rekursivt tellbar.

Vi illustrerer dette ved et par eksempler. La $\mathbf{Z}$ være mengden av hele tall. La $\Phi : \mathbf{Z} \to \mathbf{N}$ være gitt ved

$$\Phi(x) = \begin{cases} x \times 2 & \text{når } x \geq 0 \\ (\Leftrightarrow x \times 2) \Leftrightarrow 1 & \text{når } x < 0. \end{cases}$$

Da vil de naturlige tallene entydig representere de hele tallene etter mønsteret $0 = \Phi(0)$, $1 = \Phi(\Leftrightarrow 1)$, $2 = \Phi(1)$, $3 = \Phi(\Leftrightarrow 2)$, $4 = \Phi(2)$, ... Dermed kan vi snakke om rekursive og rekursivt tellbare delmengder av de hele tallene.

I kommende kapitler vil vi snakke om rekursive og rekursivt tellbare delmengder av språk og utsagn. All syntaks kan effektivt kodes inn i tallene. La $\Phi((A \wedge B)) = \langle 2, \Phi(A), \Phi(B) \rangle$, la $\Phi(\neg(A)) = \langle 1, \Phi(A) \rangle$ og la $\Phi(P_i) = \langle 0, i \rangle$. Nå er Φ en beregnbar en-til-en funksjon. Dermed kan vi, når vi kjenner Φ, på en innlysende måte representere utsagnslogiske utsagn over språket $\{\neg, \wedge,), (, P_0, P_1, P_2, \ldots\}$ ved de naturlige tallene. Videre kan vi for eksempel si at mengden av utsagnslogiske tautologier er rekursiv. Formelt sett påstår vi da at det finnes en rekursiv funksjon f slik at $f(\Phi(U)) = 0$ når U er en tautologi og $f(\Phi(U)) = 1$ ellers.

Syntaks kan effektivt kodes inn i $\mathbf{N}$ på uendelig mange måter. I vår sammenheng spiller det ingen rolle hvordan det gjøres. Det vesentlige er at det kan gjøres. Derfor gidder vi heller ikke å mase om hvordan det er gjort. Så lenge vår intuisjon sier det finnes en beregnbar en-til-en funksjon fra en mengde A inn i $\mathbf{N}$, vegrer vi oss ikke for å omtale delmengder av A som rekursive og rekursivt tellbare. Videre kan vi omtale funksjoner generelt som rekursive. Når vi gjør det, har vi gjort uuttalte forutsetninger om at funksjonenes domener og verdiområder kan representeres effektivt ved naturlige tall.

Mange av bevisene våre blir pene og oversikligee fordi vi benytter et kjempesterkt teorem:

Teorem 3.19 (Turings teorem) *Vi har en algoritme for å beregne en funksjon f hvis og bare hvis f er rekursiv.*

Dette teoremet gir ikke mening uten følgnde definisjon:

Definisjon. Vi har en *algoritme* for å beregne en funksjon f hvis og bare hvis f kan beregnes av et regnedyr som tilfredstiller aksiomene (A1), (A2), (A3), (A4) og (A5) i Kapittel 2.2. □

(Så når vi i det følgende sier at vi har en algoritme for å beregne en funksjon, så mener vi altså *per definisjon* at funksjonen kan beregnes av et regnedyr.) For enkelhets skyld kaller vi Teorem 3.19 for Turings teorem. Det ville kanskje vært mer passende å kalle teoremet for Turing-Church-Kleenes teorem. Turing beviste at

vi har en algoritme for å beregne f hvis og bare hvis f kan beregnes av en Turingmaskin

og at

f kan beregnes av en Turingmaskin hvis og bare hvis f kan defineres i λ-kalkyle.

Church og Kleene viste at

f kan defineres i λ-kalkyle hvis og bare hvis f er rekursiv.

Teoremet følger trivelt fra disse tre ekvivalensene.

Turings teorem er så sentralt at vi (paradoksalt nok) skal benytte det mer eller mindre stilltiende. Når vi intuitivt ser at det finnes en algoritme for å beregne en funksjon, vil vi uten mere om og men slå fast at funksjonen er rekursiv. Likevel, for å minne oss selv om at Turings teorem svever over vannene, setter vi et merke ved bevisene som hviler på teoremet.

I dette underkapitlet har vi snakket litt om ved hvilke andledninger vi skal være en smule uformelle og stole på vår intuisjon. Bruk av intuisjon letter bevisføringen betraktelig. Vi kan konsentrere oss om essensielle punkter i resonnementer i stedet for å fortape oss i ørkesløs formalisering. Du bør imidlertid være klar over at man skal være en ganske dreven håndverker for å overføre enkelte av de "intuitive" bevisene til mer detaljerte og formaliserte versjoner.

3.4 Mer uavgjørbarhet

Beviset av det neste teoremet er en god demonstrasjon av to bevisteknikker vi har snakket om over. For det første benyttes Turings teorem. Det er alt annet enn trivielt at en funksjon f som dukker opp er total og rekursiv, men i beviset argumenteres det for nettopp det ved å appellere til Turings teorem (3.19). For det andre vises det at en mengde A ikke er rekursiv ved å vise at den selvsamme f er slik at $x \in K \Leftrightarrow f(x) \in A$. Man viser at det er umulig å avgjøre et problem ved å redusere et annet uavgjørbart problem til problemet.

Definisjon. En mengde A er en *indeksmengde* for en mengde $\mathfrak{A}$ av partielt rekursive funksjoner dersom $A = \{e \mid \{e\} \in \mathfrak{A}\}$.

En mengde $\mathfrak{A}$ av partielt rekursive og unære funksjoner er *triviell* dersom $\mathfrak{A}$ enten er tom eller inneholder alle partielt rekursive og unære funksjoner. □

Teorem 3.20 (Rice) *La $\mathfrak{A}$ være en mengde partielt rekursive og unære funksjoner, og la A være en indeksmengde for $\mathfrak{A}$. Hvis $\mathfrak{A}$ ikke er triviell, så er A ikke rekursiv.*

Bevis av Teorem 3.20. Anta at $\mathfrak{A}$ ikke er triviell. Da finnes rekursive indekser e og d slik at $\{e\} \in \mathfrak{A}$ og $\{d\} \notin \mathfrak{A}$. La ψ være en unær og totalt udefinert funksjon, det vil si at $\psi(x)$ er udefinert for enhver x. (Funksjonen ψ er selvsagt rekursiv.) Vi har nå to muligheter: enten $\psi \in \mathfrak{A}$ eller $\psi \notin \mathfrak{A}$. Anta at det er tilfellet at $\psi \notin \mathfrak{A}$. Tenk på n som et fast tall, og la

$$g(x) = \begin{cases} \{e\}(x) & \text{hvis } n \in K \\ \psi(x) & \text{ellers.} \end{cases}$$

Vel, g er en rekursiv funksjon. Og ikke nok med det. Vi har en algoritme for å finne en indeks for g uniformt i n. (Det blir kanskje lettere å henge med i svingene hvis du tenker på en rekursiv indeks som programkode. Se på e som en gitt programkode. Hvis du får vite n, kan du mekanisk konstruere programkode for å beregne $g(x)$, nemlig koden til dette programmet: Elementene i den rekursivt tellbare mengden K listes opp ett for ett. Hvis n dukker opp i listen, eksekveres programkoden e med input x. Hvis $n \notin K$, vil opplistingen av elementer fra K fortsette til evig tid.) Ved Teorem 3.19 finnes det da en rekursiv funksjon f som er slik at $\{f(n)\}(x) = g(x)$. Videre: Hvis $n \in K$, så $\{f(n)\} = \{e\} \in \mathfrak{A}$. Hvis $n \notin K$, så $\{f(n)\} = \psi \notin \mathfrak{A}$. Dermed

$$n \in K \quad \Leftrightarrow \quad \{f(n)\} \in \mathfrak{A} \quad \Leftrightarrow \quad f(n) \in A\,.$$

Vi ser at hvis A er en rekursiv mengde, så vil også K være det. At K er rekursiv strider mot Teorem 3.18. Fra dette slutter vi at A ikke er rekursiv. Dette var beviset for tilfellet $\psi \notin \mathfrak{A}$. Tilfellet $\psi \in \mathfrak{A}$ vises analogt. Da benytter vi at $\{d\} \notin \mathfrak{A}$ til å vise at komplementmengden til A ikke er rekursiv. Fra dette følger det at A ikke er rekursiv. (De rekursive mengdene er lukket under komplementdannelse.) □

Dette teoremet bør være sterke saker for en databehandler. Det sier noe i retning av at ethvert ikke-trivielt spørsmål som angår de rekursive funksjonene er uavgjørbart. Ser vi på en rekursiv indeks som en programkode, kan teoremet tolkes dithen at ethvert interessant spørmål om resultatet av å eksekvere en kode er uavgjørbart. Vel, leseren kan selv arbeide med en mer uformell tolkning og forståelse av Rices teorem. Her er noen korollarer.

Korollar 3.21 *(i) Det er ikke avgjørbart om en rekursiv funksjon er definert i argumentet 17.*

(ii) Det er ikke avgjørbart om det for to rekursive funksjoner f og g finnes en n slik at $f(n) = g(n)$.

(iii) Det er ikke avgjørbart om en rekursiv funksjon er total.

(iv) Det er ikke avgjørbart om en rekursiv funksjon f er slik at $f(x) = x$ for alle x.

$\vdots$

(?) Lag flere korollarer selv.

$\vdots$

Bevis av Korollar 3.21. La oss vise (iv) som et eksempel. Det er like enkelt å vise de andre punktene. Først presiserer vi påstanden. I punkt (iv) påstås det at mengden

$$\{e \mid e \text{ er indeks for en unær funksjon og } \{e\}(x) = x \text{ for alle } x\}$$

ikke er rekursiv. Vel, mengden er opplagt forskjellig både fra $\emptyset$ og $\mathbf{N}$. Dermed kan ikke mengden være rekursiv ved Teorem 3.20. □

3.5 De μ-rekursive funksjonene

Definisjon. La $k_<$ være den karakteristiske funksjonen til relasjonen "ekte mindre enn", dvs. $k_<(x, y) = 0$ når $x < y$, og $k_<(x, y) = 1$ når $x \geq y$.

De *μ-rekursive initialfunksjonene* er $k_<$, $+$ (addisjon), $\times$ (multiplikasjon) og $\mathcal{I}_i^n$ (projeksjonsfunksjonene).

De *μ-rekursive funksjonene* er den minste klassen av funksjoner som inneholder de *μ-rekursive initialfunksjonene* og som er lukket under komposisjon og minimalisering.

En *μ-rekursive mengde*, *μ-rekursive relasjon* osv., defineres på en innlysende måte ved hjelp av karakteristiske funksjoner. □

De μ-rekursive funksjonene kan føres tilbake til Gödel. Det er innlysende at enhver μ-rekursiv funksjon er rekursiv. Vi skal vise det omvendte, dvs. at enhver rekursiv funksjon er μ-rekursiv. I utgangspunktet virker det lite sannsynlig at det for eksempel er mulig å definere eksponensiering x^y μ-rekursivt. Forsøk! Så dette resultatet er meget overraskende, og beviset er like tungt som overraskelsen er stor. Vi må dessverre ty til en del tallteoretisk ekvilibrisme. Ved første gangs lesning bør man kanskje bare godta at det er slik, droppe beviset og gi seg i kast med neste kapittel.

Når vi først har etablert forholdet mellom de rekursive og de μ-rekursive funksjonene, blir det lettere å bevise sentrale resultater senere. Det er hovedgrunnen til at vi bruker tid og krefter på denne sammenhengen.

Lemma 3.22 *(i) Likhetsrelasjonen er μ-rekursiv. (ii) De μ-rekursive relasjonene er lukket under de utsagnslogiske operatorene. (iii) De μ-rekursive relasjonene er lukket under de bundne første ordens kvantorer $(\exists i < n)$ og $(\forall i < n)$. (iv) Etterfølgerfunksjonen $\mathcal{S}$ er μ-rekursiv.*

Bevis av Lemma 3.22 La p og q være henholdsvis de karakteristiske funksjonene for relasjonene P og Q. Da er den μ-rekursive funksjonen $p(\vec{x}) \times q(\vec{y})$ den karakteristiske funksjonen for relasjonen $P(\vec{x}) \vee Q(\vec{y})$. Den μ-rekursive funksjonen $k_<(0, p(\vec{x})$ er den karakteristiske funksjonen for relasjonen $\neg P(\vec{x})$. Alle andre utsagnslogiske operatorer kan uttrykkes ved hjelp av $\neg$ og $\vee$ og komposisjon. Dermed holder (ii). Videre har vi at $k_<((\mu y)[P(\vec{x}, y) \vee y = n], n)$ er den karakteristiske funksjonen til relasjonen $(\exists y < n)[P(\vec{x}, y)]$. Dermed holder også (iii) siden bunden allkvantor kan uttrykkes ved hjelp av negasjon, bunden eksistenskvantor og komposisjon. Du skal få lov til å pusle med (i) og (iv) på egenhånd. □

Lemma 3.23 *La b være et vilkårlig fast tall. La c være det minste tallet som er delelig på alle tall mindre eller lik b. Hvis $x \leq b$, $y \leq b$ og $x \neq y$, så er $1 + (x \times c)$ og $1 + (y \times c)$ innbyrdes prime. (To tall m, n er innbyrdes prime når brøken $\frac{m}{n}$ ikke kan forkortes, dvs. når m og n ikke har andre felles faktorer enn 1.)*

Bevis av Lemma 3.23. Vi overlater dette til de aller ivrigste av leserne. □

Funksjonen β som introduseres i neste lemma er viden berømt under navnet Gödels β-funksjon.

Lemma 3.24 (Gödels lemma) *Det finnes en μ-rekursiv funksjon β slik at (i) $\beta(x, i) < x$ for enhver i og (ii) for enhver sekvens av naturlige tall $a_0, a_1, \ldots, a_n$ så finnes det et tall m slik at $\beta(m, i) = a_i$ for $i = 0, 1, \ldots, n$.*

Bevis av Lemma 3.24. Viktig underliggende ide: En sekvens $a_0, a_1, \ldots a_n$ skal representeres ved en mengde $\{b_0, \ldots, b_n\}$ som i sin tur skal representeres av et trippel b, c, d.

La $\psi(x, y) \stackrel{\text{def}}{=} (x + y)^2 + x$. Så $\psi : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ er en μ-rekursiv injeksjon. Det betyr at ψ koder par av tall inn i tallene. La $b_i = \psi(a_i, i)$ for $i = 0, \ldots, n$. Da vil mengden $\{b_0, \ldots, b_n\}$ representere sekvensen $a_0, \ldots, a_n$. (En sekvens er ordnet. En mengde er ikke ordnet.)

La $b = \max\{b_1, \ldots, b_n\}$. La c være det minste tallet som er delelig på alle tall mindre eller lik b. La $d = (1 + b_0 c)(1 + b_1 c) \cdots (1 + b_n c)$. Ved Lemma 3.23 har vi nå at

$$d \text{ er delelig på } 1 + xc \text{ og } x \leq b \quad \Leftrightarrow \quad x \in \{b_0, \ldots, b_n\} .$$

Dermed kan trippelet b, c, d representere mengden $\{b_0, \ldots, b_n\}$. Trippelet b, c, d kan selvsagt i sin tur representeres av et enkelt tall a ved å la $a = \psi(b, \psi(c, d))$. Dermed representeres sekvensen $a_0, \ldots, a_n$ av tallet a. Vi skal nå konstruere en μ-rekursiv funksjon β som er slik at $\beta(a, i) = a_i$ når $i \leq n$. Videre vil $\beta(x, i) < x$ for alle x som ikke koder en sekvens som er minst i lang.

La $D(x,y) \overset{\text{def}}{\Leftrightarrow} (\exists z \leq y)[x \times z = y]$. Videre la

$$R(y,x) \quad \overset{\text{def}}{\Leftrightarrow} \quad (\exists u,v,w \leq y)\,[\, y = \psi(u,\psi(v,w)) \;\wedge\; x \leq u \;\wedge\; D(\mathcal{S}(x \times v), w)\,]\,.$$

Det er lett å se at predikatet R er μ-rekursivt ved Lemma 3.22. Videre la

$$\beta(x,i) \quad \overset{\text{def}}{=} \quad (\mu z)\,[\, R(x,\psi(z,i)) \vee \mathcal{S}(z) = x\,]\,.$$

Ved Lemma 3.22 ser vi at også β er μ-rekursiv. Vi har definert R slik at

$$R(\psi(b,\psi(c,d)),x) \quad \Leftrightarrow \quad d \text{ er delelig på } 1 + xc \text{ og } x \leq b \quad \Leftrightarrow \quad x \in \{b_0,\ldots,b_n\}\,.$$

Dermed, la $a = \psi(b,\psi(c,d))$ hvor b, c og d er slik vi har beskrevet over. Da har vi at $\{b_0,\ldots,b_n\} = \{x \mid R(a,x)\}$. Videre har vi $\beta(a,i) = a_i$ for $i = 0,\ldots n$ og vi har $\beta(x,y) < x$ for alle x,y. Quod erat demonstrandum. □

Teorem 3.25 *Enhver rekursiv funksjon er μ-rekursiv.*

Bevis av Teorem 3.25. Det holder å vise at de μ-rekursive funksjonene er lukket under primitiv rekursjon. (Teoremet følger trivielt når vi har vist dette.) Så anta at $f(\vec{x},0) = g(\vec{x})$, at $f(\vec{x},y+1) = h(\vec{x},y,f(\vec{x},y))$, og at g og h er μ-rekursive funksjoner. Vi viser at f er μ-rekursiv. La

$$f_0(\vec{x},y) \quad = \quad \beta(\;(\mu z)[(\forall i < y)[\beta(z,0) = g(\vec{x}) \;\wedge\; \beta(z,i+1) = h(\vec{x},i,\beta(z,i))]]\;,\; y\;)$$

hvor β er Gödels β-funksjon fra Lemma 3.24. Ved lemmaene 3.24 og 3.22 er f_0 en μ-rekursiv funksjon. Ved induksjon på n kan man se at $f(\vec{x},n) = f_0(\vec{x},n)$. Dermed kan vi slutte at de μ-rekursiv funksjonene er lukket under primitiv rekursjon. □

3.6 Oppgaver

Oppgave 1
Vis at en uendelig mengde A er rekursiv hvis og bare hvis A er verdiområdet til en total rekursiv og strengt monotont voksende funksjon. (At f er strengt monotont voksende betyr at vi har $f(x) < f(x+1)$ for alle x.)

Oppgave 2
I denne oppgaven skal vi ta en liten titt på et felt innenfor rekursjonsteorien som kalles gradteori. La A og B være mengder av naturlige tall. Vi definerer så relasjonen $\leq_m$ ved

$$A \leq_m B \quad \overset{\text{def}}{\Leftrightarrow} \quad \text{finnes en total rekursiv funksjon } f \text{ s.a. } x \in A \Leftrightarrow f(x) \in B.$$

Det er vanlig å uttale "$A \leq_m B$" slik: "A er m-reduserbar til B".

Punkt a
Hvilke mengder er m-reduserbare til $\mathbf{N}$? Hvilke mengder er m-reduserbare til $\emptyset$? Denne oppgaven er enkel, og forkynner intet annet budskap enn at $\emptyset$ og $\mathbf{N}$ er patologiske mengder med hensyn på m-reduserbarhet.

Punkt b
La A og B være vilkårlige rekursive mengder, men forskjellig fra $\emptyset$ og $\mathbf{N}$. Vis at $A \leq_m B$ og $B \leq_m A$.

Vi definerer litt igjen.

$$A <_m B \quad \overset{\text{def}}{\Leftrightarrow} \quad A \leq_m B \wedge A \not\leq_m B \; .$$
$$A \equiv_m B \quad \overset{\text{def}}{\Leftrightarrow} \quad A \leq_m B \wedge B \leq_m A \; .$$

Vi sier at A og B har samme m-grad når $A \equiv_m B$. Ved punkt b av denne oppgaven så er alle rekursive mengder av samme m-grad om vi ser bort fra de patologiske tilfellene $\emptyset$ og $\mathbf{N}$. Graden til de rekursive mengdene kalles $\mathbf{0}$ i gradteorien.

Punkt c

Vis at den komplette r.t. mengden K ikke er av grad $\mathbf{0}$. Litt mer presist: Vis at $A <_m K$ for enhver rekursiv mengde A. (Graden til K kalles $\mathbf{0'}$. Vi uttatler $\mathbf{0'}$ "null hopp".)

Punkt d

(Vanskelig.) La A være en rekursiv mengde forskjellig fra $\emptyset$ og $\mathbf{N}$. Vis at det finnes en mengde B slik at $A <_m B <_m K$. Det finnes altså en mengde som er for komplisert til å være rekursiv, men ikke så komplisert som den komplette r.t. mengden. Vi sier at det finnes en m-grad mellom $\mathbf{0}$ og $\mathbf{0'}$.

Punkt e

(Ganske vanskelig.) Vis at det finnes en mengde A slik at $K <_m A$.

Oppgave 3

La den unære funksjonen f_0 være gitt ved $f_0(x) = 0$, dvs. f_0 er konstantfunksjonen som gir 0. Vis at f_0 er μ-rekursiv ved å konstruere den med hjelp av μ-rekursive skjema fra de initielle μ-rekursive funksjonene. Vis på samme måte at funksjonen f_n der $f_n(x) = n$, er μ-rekursiv for alle $n \in \mathbf{N}$. Vis deretter at funksjonen $g_{n,m}(x_1, \ldots, x_m) = n$ er μ-rekursiv for alle $m \geq 1$.

Kapittel 4

Ufullstendighet og uavgjørbarhet

4.1 Innledning

Definisjon. Vi sier at en første ordens teori T er *fullstendig for strukturen* $\mathfrak{M}$ dersom $\mathfrak{M} \models T$ og $\mathfrak{M} \models A \Rightarrow T \vdash A$. $\square$

Vi har tidligere kalt en teori T *fullstendig* dersom den er konsistent og at vi har $T \vdash A$ eller $T \vdash \neg A$ for enhver A i språket til T. Dermed er en første ordens teori T *fullstendig* dersom det finnes en struktur $\mathfrak{M}$ slik at T er fullstendig for $\mathfrak{M}$. Det er enkelt å vise dette. Vi overlater det til leseren.

Hvis T er fullstendig for $\mathfrak{M}$, så vil $T \vdash A \Rightarrow \mathfrak{M} \models A$. Slik må det være siden $\mathfrak{M}$ er en modell for T. På grunn av sunnhet vil da alle utsagn som kan utledes i T være sanne i $\mathfrak{M}$. Dermed er T fullstendig for $\mathfrak{M}$ hvis og bare hvis $\{A \mid T \vdash A\} = \{A \mid \mathfrak{M} \models A\}$. Hvis det finnes en fullstendig teori for en struktur $\mathfrak{M}$, så kan vi altså føre et formelt bevis (tremetode, sekventkalkyle) for ethvert utsagn som er sant i $\mathfrak{M}$.

Vi skal se at det finnes en fullstendig teori for en struktur hvis og bare hvis mengden av utsagn som holder i strukturen er rekursiv. At det finnes en fullstendig teori for en struktur, er altså ekvivalent med at det finnnes en algoritme for å avgjøre om et vilkårlig utsagn holder i strukturen. Dermed virker det lite sannsynlig at det for eksempel skal finnes en fullstendig første ordens tallteori, dvs. en teori som er fullstendig for strukturen $\mathcal{N}$. Vi har tidligere sett at det går glatt å uttrykke i første ordens tallteori at det finnes uendelig mange parprimtall, men ingen har klart å bevise eller motbevise at så er tilfelle. Det ville være besynderlig om en *maskin* kunne besvare spørsmålet. Og ikke bare dette spørsmålet og alle andre ubesvarte spørsmål i første ordens tallteori. Maskinen skulle også være i stand til å avgjøre holdbarheten av en flora av andre ikke-trivielle påstander i diverse matematiske disipliner. Det forholder seg nemlig slik at store deler av matematikken kan reduseres til første ordens tallteori.

Det er mye etterpåklokskap i betrakningene over. (Og etterpåklokskap er en eksakt vitenskap.) Vi kjenner algoritmebegrepet. Vi er fortrolig med Turings teorem osv., osv. Det som i dag er utenkelig var en gang tenkelig. Hilberts program ble statuert rundt århundreskiftet. En av programmets målsetninger var en fullstendig aksiomatisering av matematikken. En annen var å vise at aksiomatiseringen var konsistent uten å bruke matematikk som var mer tvilsom enn den matematikk man allerede hadde aksiomatisert. Ufullstendighetsteoremene i dette kapitlet viser at programmet ikke lar seg gjennomføre.

Lemma 4.1 *Mengden av utsagn som er sanne i en første ordens struktur er rekursivt tellbar hvis og bare hvis den er rekursiv.*

Bevis av Lemma 4.1. (Turings teorem.) Hvis en mengde er rekursiv, så er det trivielt at den er rekursivt tellbar. Anta så at mengden av utsagn som er sanne i en struktur $\mathfrak{M}$ er rekursivt tellbar. Vi har altså en algoritme som lister opp alle elementene i mengden $\{B \mid \mathfrak{M} \models B\}$. La A være et vilkårlig utsagn i språket til $\mathfrak{M}$. Enten vil A forekomme i en slik opplisting, eller så vil $\neg A$ forekomme. Forekommer A i listen, vet vi at $A \in \{B \mid \mathfrak{M} \models B\}$. Forekommer $\neg A$ i listen, vet vi at $A \notin \{B \mid \mathfrak{M} \models B\}$. Vi har altså en algoritme for å avgjøre medlemskap i $\{B \mid \mathfrak{M} \models B\}$. Dermed er denne mengden rekursiv. □

Teorem 4.2 *La $\mathfrak{M}$ være en første ordens struktur. Anta at vi uniformt i to heltall m, n effektivt kan konstruere et utsagn A slik at $\mathfrak{M} \models A \Leftrightarrow \langle m, n\rangle \in K$. Da er ikke mengden $\{B \mid \mathfrak{M} \models B\}$ rekursivt tellbar.*

Bevis av Teorem 4.2. (Turings teorem) Anta motsatt, altså at mengden $\{B \mid \mathfrak{M} \models B\}$ er rekursivt tellbar. Ved Lemma 4.1 er denne mengden også rekursiv. Men da har vi en algoritme for å avgjøre medlemskap i K. (Konstruer utsagnet A og test om utsagnet er med i $\{B \mid \mathfrak{M} \models B\}$. Hvis ja, har vi $\langle m, n\rangle \in K$. Hvis nei, har vi $\langle m, n\rangle \notin K$.) Dermed er K rekursiv. Det sier i mot Teorem 3.18. □

Teorem 4.3 *La T være en første ordens teori. Mengden av utsagn som kan utledes i T er rekursivt tellbar. (Vi minner om den forutsetningen vi har gjort om første ordens teorier på side 12, – nemlig at aksiomene er rekursivt tellbare.)*

Bevis av Teorem 4.3. (Turings teorem) Vi gir en effektiv prosedyre for å liste opp alle utsagn i mengden $\{B \mid T \vdash B\}$. La $A_0, A_1, A_2, \ldots$ være en opptelling av utsagnene i språket til T. En slik opptelling kan genereres effektivt. Så bruker vi tremetoden: (1) Bygg ut ett trinn av "treet" $T \vdash A_0$. (2) Bygg ut to trinn i hver av "trærne" $T \vdash A_0$ og $T \vdash A_1$. (3) Bygg ut tre trinn i hver av "trærne" $T \vdash A_0$, $T \vdash A_1$ og $T \vdash A_2$. (4) Bygg ut fire .... Hver gang et "tre" $T \vdash A_i$ lukkes, listes utsagnet A_i og treet fjernes fra den uendelige prosessen. □

Når en struktur er tilstrekkelig komplisert, finnes det ingen fullstendig første ordens teori for strukturen. Det er et hovedbudskap i dette delkapitlet. Kan vi for vilkårlige m, n uttrykke "$\langle m, n\rangle \in K$" i en struktur, så har vi nemlig et ufullstendighetsteorem for strukturen.

Teorem 4.4 (Ufullstendighet) *La $\mathfrak{M}$ være en første ordens struktur. Anta at vi uniformt i to heltall m, n effektivt kan konstruere et utsagn A slik at $\mathfrak{M} \models A \Leftrightarrow \langle m, n\rangle \in K$. Da finnes det ingen fullstendig første ordens teori T for $\mathfrak{M}$.*

Bevis av Teorem 4.4. Teorem 4.2 sier at mengden $\{B \mid \mathfrak{M} \models B\}$ ikke er rekursivt tellbar. Teorem 4.3 sier at mengden $\{B \mid T \vdash B\}$ er rekursivt tellbar. Dermed må de to mengdene være forskjellige. □

4.2 Ufullstendighetsteoremer for tallteori

Vi har nå dekket bordet for å vise at det umulig kan finnes fullstendige første ordens teorier for interessante matematiske strukturer. Når en struktur et komplisert, er ethvert

forsøk på å aksiomatisere sannhet i strukturen ved hjelp av første ordens logikk og et rekursivt tellbart aksiomsett, dømt til å mislykkes. Og strukturen trenger ikke være så veldig komplisert heller. Vi skal snart se at den vanlige modellen $\mathcal{N}$ for første ordens logikk pluss funksjonene $+, \times, S$ og navnet 0, er en tilstrekkelig komplisert struktur.

Definisjon. Numeralene er en delmengde av termene i tallteorispråket. For ethvert naturlig tall n finnes det ett numeral $\overline{n}$, og vi definerer $\overline{0} = 0$ og $\overline{n+1} = S(\overline{n})$.

Vi definerer $x < y \overset{\text{def}}{\Leftrightarrow} (\exists z)[x + S(z) = y]$. La A være et tallteoretisk utsagn. Vi definerer $(\exists x < n)[A] \overset{\text{def}}{\Leftrightarrow} (\exists x)[x < n \ \wedge \ A]$ og $(\forall x < n)[A] \overset{\text{def}}{\Leftrightarrow} (\forall x)[x < n \rightarrow A]$. Dette betyr at $x < y$ er syntaks for det tallteoretiske utsagnet $(\exists z)[x + S(z) = y]$. Så $x < y$ kan sees på som en forkortelse. Dermed er det også gitt hvordan $x < y$ skal tolkes. På samme måte er $(\exists x < n)[A(x)]$ og $(\forall x < n)[A(x)]$ kun forkortelser og tolkningen er gitt. Vi kaller $(\exists x < n)$ og $(\forall x < n)$ for *begrensede kvantorer.*

Vi skal nå omdefinere hva som menes med Σ_i^0-utsagn, Π_i^0-utsagn og Δ_i^0-utsagn for utsagn i tallteorispråket.

- Et utsagn i tallteorispråket som er bygget opp fra atomære utsagn ved hjelp av konnektiver og begrensede kvantorer er på Δ_0^0-form, Π_0^0-form og Σ_0^0-form.
- La A være et utsagn i tallteorispråket på Σ_n^0-form, og la B være et utsagn på formen $(\forall x_1) \ldots (\forall x_n)\ [\ A\ ]$. Da er B et utsagn på Π_{n+1}^0-form.
- La A være et utsagn i tallteorispråket på Π_n^0-form, og la B være et utsagn på formen $(\exists x_1) \ldots (\exists x_n)\ [\ A\ ]$. Da er B et utsagn på Σ_{n+1}^0-form.
- Et Π_i^0-*utsagn* er et utsagn som er ekvivalent med et utsagn på Π_i^0-form.
- Et Σ_i^0-*utsagn* er et utsagn som er ekvivalent med et utsagn på Σ_i^0-form.
- Et Δ_i^0-*utsagn* er et utsagn som både er ekvivalent med et Π_i^0-utsagn og med et Σ_i^0-utsagn. $\square$

Legg merke til at denne nye definisjonen av Σ_i^0, Π_i^0 og Δ_i^0 bare gir mening for utsagn i tallteorispråket. Den gir ingen mening for et generelt første ordens logisk utsagn. (La A være et tallteoretisk utsagn. Hvis A er "logisk Δ_0^0", så er A også "tallteoretisk Δ_0^0". Det omvendte gjelder ikke.) I resten av dette kapitlet vil vi utelukkende bruke Σ_i^0, Π_i^0 og Δ_i^0 i tallteoretisk betydning.

Vi har at både $\Sigma_i^0 \subset \Delta_{i+1}^0$ og $\Pi_i^0 \subset \Delta_{i+1}^0$. Videre har vi selvsagt $\Delta_i^0 \subset \Sigma_i^0$ og $\Delta_i^0 \subset \Pi_i^0$. Dermed har vi et hierarki som gir et fornuftig mål på kompleksiteten av tallteoretiske utsagn. Dette vil bli klarere i løpet av de kommende sidene. Mengden av sanne lukkede Δ_0^0-utsagn er rekursiv. Så selv om utsagnene i Δ_0^0 kan være syntaktisk kompliserte, de kan inneholde mange kvantorer, så er de i en annen forstand alltid enkle: Det er avgjørbart om et lukket Δ_0^0 er sant i $\mathcal{N}$.

Teorem 4.5 (Representerbarhet) *For enhver n-ær rekursiv funksjon f finnes det et tallteoretisk Σ_1^0-utsagn $F(x_1, \ldots, x_n, y)$ slik at*

$$f(a_1, \ldots, a_n) = b \quad \Leftrightarrow \quad \mathcal{N} \models F(\overline{a}_1, \ldots, \overline{a}_n, \overline{b})\ .$$

Bevis av Teorem 4.5. Vi vet, på grunn av Teorem 3.25, at enhver rekursiv funksjon kan genereres fra initialfunksjonene $+, \times, \mathcal{I}_i^n$ og $k_<$ ved hjelp av komposisjon og minimalisering. Vi viser teoremet ved induksjon på en slik generering av f. Induksjonsstarten er grei. Vi har

$$\begin{aligned} a_1 + a_2 = b \quad &\Leftrightarrow \quad \mathcal{N} \models \overline{a}_1 + \overline{a}_2 = \overline{b_2} \\ a_1 \times a_2 = b \quad &\Leftrightarrow \quad \mathcal{N} \models \overline{a}_1 \times \overline{a}_2 = \overline{b_2} \\ \mathcal{I}_i^n(a_1, \ldots, a_n) = b \quad &\Leftrightarrow \quad \mathcal{N} \models \overline{a_i} = \overline{b} \ \wedge \ \overline{a}_1 = \overline{a}_1 \ \wedge \ \cdots \ \wedge \ \overline{a}_n = \overline{a}_n \\ k_<(a_1, a_2) = b \quad &\Leftrightarrow \quad \mathcal{N} \models (\overline{a}_1 < \overline{a}_2 \ \wedge \ \overline{b} = 0) \ \vee \ (\neg(\overline{a}_1 < \overline{a}_2) \ \wedge \ \overline{b} = S(0)) \, . \end{aligned}$$

Vi ser at alle de tallteoretiske utsagnene er kvantorfrie og dermed Σ_1^0-utsagn.

Anta så at f er komposisjonen $f(x_1, \ldots, x_n) = h(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$. Induksjonshypotesen gir oss Σ_1^0-utsagn $G_1, \ldots, G_m$ slik at

$$g_i(a_1, \ldots, a_n) = b \quad \Leftrightarrow \quad \mathcal{N} \models G_i(\overline{a}_1, \ldots, \overline{a}_n, \overline{b})$$

for $i = 1, \ldots, m$ og H slik at

$$h(a_1, \ldots, a_m) = b \quad \Leftrightarrow \quad \mathcal{N} \models H(\overline{a}_1, \ldots, \overline{a}_m, \overline{b}) \, .$$

La nå $F(x_1, \ldots, x_n, y)$ være utsagnet

$$(\exists z_1, \ldots, z_m)[G_1(x_1, \ldots, x_n, z_1) \ \wedge \ \cdots \ \wedge \ G_m(x_1, \ldots, x_n, z_m) \ \wedge \ H(z_1, \ldots, z_m, y)] \, .$$

Siden $G_1, \ldots, G_m$ og H er Σ_1^0-utsagn, så er F er logisk ekvivalent med et Σ_1^0-utsagn. (Sørg for at alle bundne variabler i F har forskjellig navn. Da kan enhver ubegrenset eksistenskvantorer flyttes så langt ut man måtte ønske.) Dermed er F et Σ_1^0 utsagn. Videre har vi

$$f(a_1, \ldots, a_n) = b \quad \Leftrightarrow \quad \mathcal{N} \models F(\overline{a}_1, \ldots, \overline{a}_n, \overline{b}) \, .$$

Så induksjonshypotesen opprettholdes i komposisjonstilfellet.

Anta så at f er gitt ved minimaliseringen $f(x_1, \ldots, x_n) = (\mu i)[g(x_1, \ldots, x_n, i)]$. Induksjonshypotesen gir oss et Σ_1^0-utsagn G slik at

$$g(a_1, \ldots, a_n, b) = c \quad \Leftrightarrow \quad \mathcal{N} \models G(\overline{a}_1, \ldots, \overline{a}_n, \overline{b}, \overline{c}) \, .$$

Først merker vi oss at

$$\mathcal{N} \models (\exists z)[G(\overline{a}_1, \ldots, \overline{a}_n, \overline{b}, z) \wedge 0 \neq z] \quad \Leftrightarrow \quad g(a_1, \ldots, a_n, b) \text{ konvergerer og } g(a_1, \ldots, a_n, b) \neq 0.$$

La F_0 være utsagnet

$$G(\overline{a}_1, \ldots, \overline{a}_n, \overline{b}, 0) \ \wedge \ (\forall i < \overline{b})(\exists z)[G(\overline{a}_1, \ldots, \overline{a}_n, i, z) \wedge 0 \neq z] \, .$$

V har nå at $f(a_1, \ldots, a_n) = b \Leftrightarrow \mathcal{N} \models F_0$. Dermed vil dette beviset være fullendt når vi har funnet et Σ_1^0-utsagn F som er slik at $\mathcal{N} \models F_0 \Leftrightarrow \mathcal{N} \models F$. (Merk at F og F_0 ikke vil være logisk ekvivalente.)

La C være et vilkårlig utsagn i tallteori hvor variabelen u ikke forekommer, og la n være et fast tall. Da gjelder

$$\mathcal{N} \models (\forall x < \overline{n})(\exists z)[C] \quad \Leftrightarrow \quad \mathcal{N} \models (\exists u)(\forall x < \overline{n})(\exists z < u)[C] \, . \qquad (*)$$

At (*) holder i høyre-venstre retningen er trivielt. At venstre-høyre retningen av (*) holder krever et lite resonnement som overlates til leseren. Ved å benytte (*) samt noen banale logiske omskrivninger kan vi konstruere Σ_1^0-utsagnet F fra F_0. Vi må for eksempel sørge for at bundne variabler har forskjellige navn, og deretter flytte ubegrensede eksistenskvantorer utover. □

Lemma 4.6 *La $a, b \in \boldsymbol{N}$ være gitt. Vi kan effektivt konstruere et utsagn A på Σ_1^0-form som er slik at $\mathcal{N} \models A \Leftrightarrow \langle a, b\rangle \in K$.*

Bevis av Lemma 4.6 Fra definisjonene har vi at $K = \{\langle x, y\rangle \mid x \in W_y\}$ og

$$W_e = \begin{cases} \{x \mid \{e\}(x) \text{ konvergerer}\} & \text{om } \{e\} \text{ er en unær funksjon} \\ \emptyset & \text{ellers.} \end{cases}$$

Vi har dermed $x \in W_e$ hvis og bare hvis det finnes z slik at $T_1(e, x, z)$. Her er T_1 Kleenes T-predikat for unære funksjoner. T-predikatet er rekursivt. Det vil si at det finnes en rekursiv funksjon ξ slik at

$$\xi(x, y, z) = \begin{cases} 0 & \text{dersom } T_1(y, x, z) \\ 1 & \text{ellers.} \end{cases}$$

Ved Teorem 4.5 finnes det et tallteoretisk Σ_1^0-utsagn $B(x, y, z, u)$ slik at $\xi(a, b, c) = 0$ hvis og bare hvis $\mathcal{N} \models B(\overline{a}, \overline{b}, \overline{c}, \overline{0})$. Dermed

$$\langle a, b\rangle \in K \Leftrightarrow a \in W_b \Leftrightarrow \text{finnes } z \text{ slik at } \xi(a, b, z) = 0 \Leftrightarrow \mathcal{N} \models (\exists z)[B(\overline{a}, \overline{b}, z, \overline{0})]\,.$$

La $A(x, y)$ være utsagnet $(\exists z)[B(x, y, z, \overline{0})]$. Vi ser at A er et Σ_1^0-utsagn. Dermed, når a, b er gitt, kan vi effektivt konstruere et utsagn A som er sant i $\mathcal{N}$ hvis og bare hvis $\langle a, b\rangle \in K$. Sett ganske enkelt numeralene $\overline{a}, \overline{b}$ inn i utsagnet $A(x, y)$ og få Σ_1^0-utsagnet $A(\overline{a}, \overline{b})$. Da holder $\langle a, b\rangle \in K \Leftrightarrow \mathcal{N} \models A(\overline{a}, \overline{b})$. □

Teorem 4.7 (Ufullstendighet) *(i) Det finnes ikke en fullstendig første ordens teori for $\mathcal{N}$. (ii) For enhver første ordens teori T slik at $\mathcal{N} \models T$, så finnes det et utsagn A slik at $\mathcal{N} \models A$ og $T \nvdash A$.*

Bevis av Teorem 4.7. (i) Fra Lemma 4.6 og Teorem 4.2 følger det at mengden $\{B \mid \mathcal{N} \models B\}$ ikke er rekursivt tellbar. Dermed har vi $\{A \mid T \vdash A\} \neq \{A \mid \mathcal{N} \models A\}$ for enhver første ordens teori T ved Teorem 4.3. (ii) La T være slik at $\mathcal{N} \models T$. Da har vi at $\{B \mid T \vdash B\}$ er en delmengde av $\{B \mid \mathcal{N} \models B\}$. Fra (i) har vi $\{B \mid T \vdash B\} \neq \{B \mid \mathcal{N} \models B\}$. Ergo må det finnes et utsagn A slik at $T \nvdash A$ og $\mathcal{N} \models A$. □

Vi merker oss at (ii) i siste teorem er en sterkere påstand enn (i), det vil si at (i) følger fra (ii). Vi skal styrke (ii) ytterligere og vise at utsagnet A som (ii) omtaler, er et Π_1^0-utsagn.

Lemma 4.8 *Mengden $\{A \mid A$ er et Σ_1^0-utsagn og $\mathcal{N} \models A\}$ er rekursivt tellbar.*

Bevis av Lemma 4.8. (Turings teorem) Det overlates til leseren å finne en algoritme som lister opp alle Σ_1^0-utsagn som er sanne i $\mathcal{N}$. Ta utgangspunkt i at mengden av Δ_0^0-utsagn som er sanne i $\mathcal{N}$ er rekursivt tellbar. Det er opplagt. Mengden er til og med rekursiv. □

Teorem 4.9 (Ufullstendighet) *For enhver første ordens teori T slik at $\mathcal{N} \models T$, så finnes det et Π_1^0-utsagn A slik at $\mathcal{N} \models A$ og $T \nvdash A$.*

Bevis av Teorem 4.9. (Turings teorem) Anta T er slik at $\mathcal{N} \models T$ og $T \vdash B$ for ethvert Π_1^0-utsagn B hvor $\mathcal{N} \models B$. Da er mengden av utsagn på Π_1^0-form som er sanne i $\mathcal{N}$, rekursivt tellbar siden $\{B \mid T \vdash B\}$ er rekursivt tellbar. (Ta utgangspunkt i algoritmen som lister opp $\{B \mid T \vdash B\}$ og stryk ethvert utsagn som ikke har Π_1^0-form fra listen.) Av dette kan vi slutte at mengden av utsagn på Σ_1^0-form som er usanne i $\mathcal{N}$ er rekursivt tellbar. Ved Lemma 4.8 har vi at mengden av utsagn på Σ_1^0-form som er sanne i $\mathcal{N}$ er rekursivt tellbar. Dermed har vi, ved Teorem 3.16, at mengden av utsagn på Σ_1^0-form som er sanne i $\mathcal{N}$, er rekursiv. Dermed kan vi avgjøre medlemskap i K ved Lemma 4.6. Det betyr at K er rekursiv. Selvmotsigelse. Teorem 3.18 sier jo at K ikke er rekursiv. □

Korollar 4.10 *For enhver første ordens teori T slik at $\mathcal{N} \models T$, så finnes det et Π_1^0-utsagn A slik at $T \nvdash A$ og $T \nvdash \neg A$. (T er altså ufullstendig.)*

Bevis av Korollar 4.10. La $\mathcal{N} \models T$. Da finnes det et Π_1^0-utsagn A slik at $\mathcal{N} \models A$ og $T \nvdash A$ ved Teorem 4.9. Anta $T \vdash \neg A$. Da kan det i T utledes et utsagn som er usant i $\mathcal{N}$. Dette sier i mot at $\mathcal{N} \models T$. □

Det siste korollaret gir en interessant situasjon. Når T er en første ordens tallteori, vil det alltid finnes et utsagn A slik at både $T \cup \{A\}$ og $T \cup \{\neg A\}$ er konsistente teorier. Bare en av de to teoriene kan ha $\mathcal{N}$ som modell. Dette åpner mulighetene for ikke-standard tallteori, dvs. en teori hvor det finnes "tall" i universet som viser en oppførsel som anstendige tall holder seg for god til. Ikke-standard tallteori blir analogt til ikke-euklidsk geometri.

Vi skal nå vise et enda sterkere ufullstendighetsteorem. Teoremene 4.7 og 4.9 sier bare at det *finnes* et Π_1^0 A slik at $\mathcal{N} \models A$ og $T \nvdash A$, og bevisene gir ingen algoritme for å konstruere A. Beviset av det neste teoremet gir en slik algoritme. Beviset og teoremet ligger også langt nærmere Gödels opprinnelige bevis og teorem. Mye av den rekursjonsteorien vi har profittert på over ble først unnfanget noen år etter at Gödel hadde gjort sine arbeider. Gödel benytter seg ikke av at man kan uttrykke "$\langle m, n\rangle \in K$" i strukturen $\mathcal{N}$. Han kjenner jo ikke til mengden K. I stedet benytter Gödel at det er mulig å uttrykke "utsagnet A kan utledes i teorien T" i $\mathcal{N}$.

Teorem 4.11 (Ufullstendighet) *La T være en første ordens teori T slik at $\mathcal{N} \models T$. Uniformt i T kan vi effektivt konstruere et Π_1^0-utsagn A slik at $\mathcal{N} \models A$ og $T \nvdash A$.*

Bevis av Teorem 4.11. (Turings teorem) Anta at vi har kodet utsagnene i språket til T inn i de naturlige tallene. Anta videre at vi har kodet utledninger i teorien T inn i de naturlige tallene. All syntaks kan kodes inn i $\mathbf{N}$, så dette skal gå bra. La $R(a, b)$ være predikatet

> a er et kodetall for et lukket tallteoretisk utsagn på formen $(\forall x)[A(x)]$, og b er et kodetall for en utledning av $A(\overline{a})$ i teorien T.

Ved Turings teorem er R et rekursivt predikat. Dermed finnes det et tallteoretisk Σ_1^0-utsagn $B_0(x, y)$ slik at $R(a, b) \Leftrightarrow \mathcal{N} \models B_0(\overline{a}, \overline{b})$ (Bruk Teorem 4.5.) La $B(x)$ være utsagnet $(\forall y)[\neg B_0(x, y)]$. Vi ser at B er et Π_1^0-utsagn. For alle tallteoretiske utsagn $A(x)$ der bare x er fri, og for alle naturlige tall n har vi nå at

$$\mathcal{N} \models B(\overline{n}) \quad \Leftrightarrow \quad \neg(n \text{ koder utsagnet } (\forall x)[A(x)]) \ \vee \ T \nvdash A(\overline{n})\,. \qquad (*)$$

Utsagnet $(\forall x)[B(x)]$ har et kodetall. La oss døpe dette tallet til k. Vi setter nå inn B og k i (*) og får

$$\mathcal{N} \models B(\overline{k}) \quad \Leftrightarrow \quad \neg(k \text{ koder utsagnet } (\forall x)[B(x)]) \ \vee \ T \nvdash B(\overline{k})\,. \qquad (**)$$

Disjunkten $\neg(k$ koder utsagnet $(\forall x)[B(x)])$ i (**) er usann ved valg av k og B. Dermed har vi $\mathcal{N} \models B(\overline{k}) \Leftrightarrow T \nvdash B(\overline{k})$. Vi har antatt at $\mathcal{N} \models T$. (Så vi kan ikke utlede noe i T som er usant i $\mathcal{N}$.) Dermed må det være tilfellet at $\mathcal{N} \models B(\overline{k})$ og $T \nvdash B(\overline{k})$. Videre ser vi at $B(\overline{k})$ må være et Π_1^0-utsagn siden $(\forall x)[B(x)]$ er det. Leseren kan selv forvisse seg om at utsagnet $B(\overline{k})$ effektivt kan konstrueres fra teorien T. $\square$

Teorem 4.11 kalles gjerne Gödels første ufullstendighetsteorem. Det er hentet fra *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme* (1931). Samme artikkel inneholder også Gödels andre ufullstendighetsteorem. Vi skal nøye oss med å forstå hva dette teoremet sier. Vi dropper beviset.

Det kan vises at en tilstrekkelig sterk første ordens tallteori T er inkonsistent hvis og bare hvis $T \vdash 0 = S(0)$. Anta som i beviset av Teorem 4.11 at vi har kodet utsagn og utledninger i T inn i de naturlige tallene. Ved Teorem 3.19 (Turings teorem) er relasjonen "tallet y koder et bevis i T for utsagnet som kodes av tallet x" rekursiv. Dermed finnes et utsagn $B(x,y)$ slik at $\mathcal{N} \models B(\overline{a},\overline{b})$ hvis og bare hvis "tallet b koder et bevis i T for utsagnet som kodes av tallet a". Dermed vil $\mathcal{N} \models \neg(\exists y)[B(\overline{a},y)]$ holde hvis og bare hvis utsagnet som kodes av tallet a ikke kan utledes i T. La nå k være kodetallet til utsagnet $0 = S(0)$. Da holder $\mathcal{N} \models \neg(\exists y)[B(\overline{k},y)]$ hvis og bare hvis teorien T er konsistent. Vi kan nå statuere Gödels andre ufullstendighetsteorem.

Teorem 4.12 (Gödels andre ufullstendighetsteorem) *La T, B og k være slik det er beskrevet over.*

$$\mathcal{N} \models T \quad \Rightarrow \quad T \nvdash \neg(\exists x)[B(x,\overline{k})]\,.$$

Teoremet må tolkes dithen at et konsistensbevis for en første ordens teori ikke kan formaliseres i den selvsamme teorien.

Vi må ikke glemme at vi opplever det som relativt enkelt å vise at for eksempel Peano-aritmetikk er en konsistent teori: $\mathcal{N}$ er en modell for Peanos aksiomene. Det er innlysende. Dermed er Peano-aritmetikk konsistent ved kompletthetsteoremet for logikk. Gödels andre ufullstendighetsteorem sier at et slikt konsistensbevis ikke kan formaliseres i Peano-aritmetikk. En påstand som holder i strukturen $\mathcal{N}$ hvis og bare hvis første ordens teorien over Peanos aksiomene er konsistent, kan ikke utledes i første ordens teorien over Peanos aksiomer. For å formalisere[1] et konsistensbevis av en første ordens teori T trenger vi en første ordens teori T' som er sterkere enn T. Dermed havner vi i en paradoksal situasjon. Den som tviler på konsistensen av T, har desto større grunn til å tvile på konsistensen av T'. Alt som kan utledes i T kan jo også utledes i T'. Vil man vise at T' er konsistent trenger man en teori T'' som er enda sterkere enn T' osv. Ut i fra dette er det ikke urimelig å si at spørsmålet om en første ordens teori er konsistent, er et spørsmål om tro. Man kan ikke vise det uten å anta noe som er enda mer kontroversielt. Noen vil kanskje spørre om man ikke kan føre "uformelle" konsistensbevis, dvs. konsistensbevis som ikke kan formaliseres i

[1] Nå snakker vi om å formalisere i en streng forstand. Et bevis er ikke formalisert før det er en endelig syntaktisk størrelse. Så for eksempel høyere ordens logikk, eller generell tallteori, kan ikke formaliseres i denne betydningen av ordet.

første ordens logikk? Med et slikt bevis kunne man kanskje unngå den kinkige situasjonen det andre ufullstendighetsteoremet byr på. Til dette er det å svare at et bevis som ikke kan formaliseres i første ordens logikk, utvilsomt er tvilsomt. Tviler man ikke på et slik bevis, har man ingen heller grunn til å tvile på at for eksempel Peano aritmetikk er konsistent.

4.3 Andre ufullstendige teorier

Ufullstendighetsteoremer er ikke noe som utelukkende hefter ved tall og tallteorier. Vi skal understreke dette ved å vise at det heller ikke finnes fullstendige første ordens teorier for teorien om binære sekvenser, dvs. strukturen $\mathcal{B}$. Leseren bør være i stand til å tenke videre på egenhånd og finne andre første ordens teorier som nødvendigvis må være ufullstendige, for eksempel en teori om kanter, noder og grafer, eller en teori om abstrakte regnemaskiner (for eksempel registermaskiner).

Hvis det er mulig å representere de rekursive funksjonene i en struktur (se for eksempel Teorem 4.5), så kan vi vise ufullstendighetsteoremer for strukturen. I så måte er det vesentlig at både $+$ (addisjon) og $\times$ (multiplikasjon) er med i tallteorispråket. Først da vil den vanlige modellen $\mathcal{N}$ for språket være komplisert nok til å representere de rekursive funksjonene slik som i Teorem 4.5. Utelater vi enten $+$ eller $\times$, er ikke dette mulig. Tvert i mot finnes det en fullstendig første ordens teori for den vanlige tallteoretiske modellen til funksjonene $+, S, 0$ og relasjonen $<$. Denne første ordens teorien kalles gjerne Presburger-aritmetikk. Det er kanskje en smule overraskende at strukturen $\mathcal{B}$ gir opphav til ufullstendighetsresultater. Strukturen virker ikke så mye mer komplisert enn modellen for Presburger-aritmetikk. Presburger-aritmetikk kan jo sees som en teori om unære sekvenser.

Definisjon. Bitnumeralene er en delmengde av termene i bitteorispråket. For ethvert naturlig tall n definerer vi bitnumeralet $\underline{n}$ rekursivt ved $\underline{0} = e$ og $\underline{m+1} = S_1(\underline{m})$.

La $x \preceq y \overset{\text{def}}{\Leftrightarrow} (\exists z)[x \circ z = y]$. Så $x \preceq y$ er rett og slett en syntaktisk forkortelse for uttrykket $(\exists z)[x \circ z = y]$ i språket for bitteori. Videre lar $x \prec y \overset{\text{def}}{\Leftrightarrow} x \preceq y \wedge \neg(x = y)$. Intuitivt betyr $x \preceq y$ at bitsekvensen x er et prefiks av bitsekvensen y.

Vi skal nå sette opp en konvensjon for hvordan en bitsekvens kan tolkes som en sekvens av naturlige tall. Når en bitsekvens α inneholder delsekvensen 001110111111100 tolker vi det som at 7 er tall nummer 3 i sekvensen som α representerer. Da kan tallsekvensen $\langle x_1, x_2, x_3, x_4 \rangle$ representeres ved

$$0010\overbrace{11\ldots11}^{x_1 \text{ stk.}}00110\overbrace{11\ldots11}^{x_2 \text{ stk.}}001110\overbrace{11\ldots11}^{x_3 \text{ stk.}}0011110\overbrace{11\ldots11}^{x_4 \text{ stk.}}00\,.$$

Så $00101100110001110100 = 001^1 01^2 001^2 01^0 01^3 01^1 00$ representerer $\langle 2, 0, 1 \rangle$. Det samme gjør bitsekvensene

$$\beta_1 = 000000000101100000000110001110100 = 000000000^1 01^2 000000001^2 01^0 001^3 01^1 00$$

og

$$\beta_2 = 0111010010110011000 = 01^3 01^1 001^1 01^2 001^2 01^0 00\,.$$

Bitsekvensen β_1 inneholder "overflødige 0'er" som vi overser. Bitsekvensen β_2 viser at i'te elementet i tallsekvensen kan godt være kodet inn i bitsekvensen til høyre for det $i+n$'te elementet i tallsekvensen. Bitsekvensen $\gamma = \ldots 001101110 \ldots 0011011110 \ldots$ koder derimot

ikke en sekvens av tall. Vi kan ikke entydig lese ut av γ hva det andre elementet i sekvensen skal være. Bitsekvensen $0010111100111011111111110 = 001^{1}01^{4}001^{3}01^{9}0$ koder heller ikke en sekvens av tall. Denne bitsekvensen gir bare verdier til element nummer en og tre i en tallsekvens når vi forsøker å tolke den etter mønsteret over. Det andre elementet gis ingen verdi.

Lemma 4.13 *Det finnes et bitteoretisk utsagn $A(x,y,z)$ slik at*

$$a \times b = c \quad \Leftrightarrow \quad \mathcal{B} \models A(\underline{a},\underline{b},\underline{c}) \, .$$

Bevis av Lemma 4.13. La $\mathrm{del}(x,y)$ være utsagnet $(\exists z_1, z_2)[(z_1 \circ x) \circ z_2 = y]$. Betydningen av $\mathrm{del}(x,y)$ i modellen $\mathcal{B}$ er at bitsekvensen x er en delsekvens av bitsekvensen y. La $\mathrm{nu}(x)$ være utsagnet $\neg(\exists y, z)[y \circ S_0(e) \circ z = x]$. Betydningen av $\mathrm{nu}(x)$ i modellen $\mathcal{B}$ er at bitsekvensen x er et bitnumeral. La så $\mathrm{seq}(x,y)$ være utsagnet

$$(\forall z)[z \preceq y \ \rightarrow \ (\exists! u)[\mathrm{del}(u,x) \ \wedge \ (\exists v)[u = S_0(S_0(e)) \circ z \circ S_0(e) \circ v \circ S_0(S_0(e)) \ \wedge \ \mathrm{nu}(z \circ v)]]].$$

Nå holder $\mathrm{seq}(x,\underline{b})$ i strukturen $\mathcal{B}$ for alle bitsekvenser x som koder en sekvens av naturlige tall, og hvor denne tallsekvensens lengde er større eller lik b. (Tallsekvensen er kodet slik det er skissert over.) La $B(x,i,y)$ være utsagnet

$$(\exists u) \, [\, \mathrm{del}(u,x) \quad \wedge \quad u = S_0(S_0(e)) \circ i \circ S_0(e) \circ y \circ S_0(S_0(e)) \,]$$

og la a være en bitsekvens som koder en sekvens av heltall som er minst b lang. Da holder $\mathcal{B} \models B(a,\underline{b},\underline{c})$ hvis og bare hvis det b'te elementet i heltallssekvensen som kodes av a, er c. La $A(x,y,z)$ være utsagnet

$$(\exists u)[\mathrm{seq}(u,y) \wedge B(u,e,e) \wedge (\forall v)[v \prec y \rightarrow (\exists w)[B(u,v,w) \wedge B(u,S_1(v),x \circ w)]] \wedge B(u,y,z)] \, .$$

Nå holder $A(\underline{a},\underline{b},\underline{c})$ i $\mathcal{B}$ hvis og bare hvis $a \times b = c$. Dermed har vi vist lemmaet. $\square$

Teorem 4.14 (Representerbarhet) *For enhver n-ær rekursiv funksjon f finnes det et bitteoretisk utsagn $F(x_1,\ldots,x_n,y)$ slik at*

$$f(a_1,\ldots,a_n) = b \quad \Leftrightarrow \quad \mathcal{B} \models F(\underline{a}_1,\ldots,\underline{a}_n,\underline{b}) \, .$$

Bevis av Teorem 4.14. Enhver rekursiv funksjon kan genereres fra de initielle μ-rekursive funksjonene $+, \times, \mathcal{I}_i^n$ og $k_<$ ved hjelp av komposisjon og minimalisering. (Teorem 3.25.) Vi benytter induksjon på en slik generering av f. (Så dette beviset blir analogt med beviset av Teorem 4.5, men vi behøver ikke lenger bemøye oss med å konstruere et Σ_1^0-utsagn.) I induksjonsstart får vi ett tilfelle for $+$, ett tilfelle for $\mathcal{I}_i^n$, ett for $k_<$ og ett for $\times$. Tilfellene for $+, \mathcal{I}_i^n$ og $k_<$ er greie. Vi har

$$\begin{aligned}
a_1 + a_2 = b \quad &\Leftrightarrow \quad \mathcal{B} \models \underline{a}_1 \circ \underline{a}_2 = \underline{b} \\
\mathcal{I}_i^n(a_1,\ldots,a_n) = b \quad &\Leftrightarrow \quad \mathcal{B} \models \underline{a_i} = \underline{b} \ \wedge \ \underline{a}_1 = \underline{a}_1 \ \wedge \ \cdots \ \wedge \ \underline{a}_n = \underline{a}_n \\
k_<(a_1,a_2) = b \quad &\Leftrightarrow \quad \mathcal{B} \models (\underline{a}_1 \prec \underline{a}_2 \ \wedge \ \underline{b} = e) \ \vee \ (\neg(\underline{a}_1 \prec \underline{a}_2) \ \wedge \ \underline{b} = S_1(e)) \, .
\end{aligned}$$

Problemet er å finne et utsagn $F(x,y,z)$ slik at $a_1 \times a_2 = b$ hvis og bare hvis $\mathcal{B} \models \underline{a}_1 \times \underline{a}_2 = \underline{b_2}$, men vi har allerede løst oppgaven. Vi har bevist Lemma 4.13, og vet dermed at et slikt utsagn finnes.

Det var induksjonsstarten. Tilfellet for multiplikasjon var en hard nøtt å knekke, ellers gikk det rimelig greit. Induksjonstrinnene er også greie. Anta at f er en komposisjonen $f(x_1,\ldots,x_n) = h(g_1(x_1,\ldots,x_n),\ldots,g_m(x_1,\ldots,x_n))$. Induksjonshypotesen gir oss utsagn $G_1,\ldots,G_m$ slik at

$$g_i(a_1,\ldots,a_n) = b \quad \Leftrightarrow \quad \mathcal{B} \models G_i(\underline{a}_1,\ldots,\underline{a}_n,\underline{b})$$

for $i = 1,\ldots,m$ og H slik at

$$h(a_1,\ldots,a_m) = b \quad \Leftrightarrow \quad \mathcal{B} \models H(\underline{a}_1,\ldots,\underline{a}_m,\underline{b})\ .$$

La $F(x_1,\ldots,x_n,y)$ være utsagnet

$$(\exists z_1,\ldots,z_m)\,[\,G_1(x_1,\ldots,x_n,z_1)\ \wedge\ \cdots\ \wedge\ G_m(x_1,\ldots,x_n,z_m)\ \wedge\ H(z_1,\ldots,z_m,y)]\ .$$

Dermed har vi $f(a_1,\ldots,a_n) = b \ \Leftrightarrow\ \mathcal{B} \models F(\underline{a}_1,\ldots,\underline{a}_n,\underline{b})$.

Anta så at f er gitt ved minimaliseringen $f(x_1,\ldots,x_n) = (\mu i)[g(x_1,\ldots,x_n,i)]$. Induksjonshypotesen gir G slik at

$$g(a_1,\ldots,a_n,b) = c \quad \Leftrightarrow \quad \mathcal{B} \models G(\underline{a}_1,\ldots,\underline{a}_n,\underline{b},\underline{c})\ .$$

La $F(x_1,\ldots,x_n,y)$ være utsagnet

$$G(x_1,\ldots,x_n,y,e) \quad \wedge \quad (\forall i)\,[\,i \prec y \quad \rightarrow \quad (\exists z)\,[\,G(x_1,\ldots,x_n,i,z) \wedge z \neq e\,]\,]\ .$$

Da har vi $f(a_1,\ldots,a_n) = b \Leftrightarrow \mathcal{B} \models F(\underline{a}_1,\ldots,\underline{a}_n,\underline{b})$. $\square$

Lemma 4.15 *La a og b være gitt. Vi kan effektivt konstruere et utsagn A (i bitteorispråket) som er slik at $\mathcal{B} \models A \ \Leftrightarrow\ \langle a,b\rangle \in K$.*

Bevis av Lemma 4.15. Helt analogt med beviset av Lemma 4.6. $\square$

Teorem 4.16 (Ufullstendighets Teorem) *(i) Det finnes ikke en komplett første ordens teori for $\mathcal{B}$. (ii) For enhver første ordens teori T slik at $\mathcal{B} \models T$, finnes det et utsagn A slik at $\mathcal{B} \models A$ og $T \nvdash A$.*

Bevis av Teorem 4.16. Følger av Lemma 4.15 på samme vis som Teorem 4.7 følger fra Lemma 4.6. $\square$

Det skulle også være uproblematisk å vise et ufullstendighetsteorem for bitteori som sier at utsagnet A i Teorem 4.16 (ii) kan konstrueres effektivt. Beviset av et slikt teorem vil være helt analogt med beviset av Teorem 4.11. Det vil derimot være mer problematisk å si noe interessant om kompleksiteten av A, for eksempel styrke Teorem 4.16 (ii) med at A er et Π^0_1-utsagn. Vi har ikke forsøkt å føre regnskap over kvantornestingen i dette delkapitlet, og vi har heller ikke definert noe som svarer til tallteoriens begrensede kvantorer for teorien om bitsekvenser.

4.4 Uavgjørbarhet av første ordens logikk

Merkelig nok trenger vi ikke ta hensyn til hvilke aksiomer en første ordens teori består av for å vise at den er ufullstendig. Hvis $\mathcal{N} \models T$ og det ikke-logiske språk til T er $+, \times, S, 0$, så kan ikke T være fullstendig. Verken i den forstand at alle utsagn som er sanne i $\mathcal{N}$ kan utledes i T, eller i den forstand at $T \vdash A$ eller $T \vdash \neg A$ for enhver A i språket. (De to formene for ufullstendighet er ekvivalente når $\mathcal{N} \models T$.) Uansett hvilke aksiomer T består av, finnes det et Π_1^0-utsagn A slik at $T \nvdash A$ og $T \nvdash \neg A$. Vi kan fortsatt håpe på at det er mulig å utlede alle sanne tallteoretiske Σ_1^0-utsagn i en første ordens teori. Og er det mulig? Ja. For å vise *dette* må vi selvsagt ta hensyn til hvilke aksiomer teorien består av.

Definisjon. Et tallteoretisk Δ_0^0-utsagn er på *begrenset negasjons normalform (BNNF)* dersom det er bygget opp av

- atomære setninger, dvs. setninger på formen $t_1 = t_2$
- negerte atomære setninger, dvs. setninger på formen $\neg\, t_1 = t_2$
- konnektivene $\wedge, \vee$ og de begrensede kvantorene $(\exists x < n)$ og $(\forall x < n)$.

Legg merke til at et tallteoretisk utsagn kan være på BNNF uten å være på NNF (negasjons normalform). Utsagnet $(\forall x < z)[(\exists y < z + 1)[x + y = z]]$ er på BNNF, men det er ikke på NNF. Husk at de begrensede kvantorene på samme måte som konnektivene $\rightarrow$ og $\leftrightarrow$, er syntaks vi har innført for å få behageligere uttrykk for visse utsagn. Omskriver vi utsagnet ved hjelp av forskjellige aktuelle definisjoner får vi et utsagn som ikke er på NNF:

$$
\begin{gathered}
(\forall x < z)\,[\,(\exists y < z + S(0))\,[\,x + y = z\,]\,] \\
== \\
(\forall x)\,[\,x < z \;\;\rightarrow\;\; (\exists y)[y < z + S(0) \;\wedge\; x + y = z]\,] \\
== \\
(\forall x)\,[\,\neg(\exists u)[x + S(u) = z] \;\;\vee\;\; (\exists y)\,[\,(\exists u)[y + S(u) = z + S(0)] \;\wedge\; x + y = z\,]\,]\,.
\end{gathered}
$$

Lemma 4.17 *Ethvert tallteoretisk Δ_0^0-utsagn er logisk ekvivalent med et tallteoretisk Δ_0^0-utsagn på BNNF.*

Bevis av Lemma 4.17. Vi har

(1) $\neg(\forall x)[A]$ er logisk ekvivalent med $(\exists x)[\neg A]$.

(2) $\neg(\exists x)[A]$ er logisk ekvivalent med $(\forall x)[\neg A]$.

Dermed kan ethvert tallteoretisk Δ_0^0-utsagn ved hjelp av (1), (2) og DeMorgans lover skrives om til et ekvivalent Δ_0^0-utsagn på BNNF. $\square$

Teorem 4.18 *La R være første ordens teorien som er gitt ved Robinsons aksiomer. (i) La A være et lukket tallteoretisk Δ_0^0-utsagn. Da $\mathcal{N} \models A \;\Leftrightarrow\; R \vdash A$. (ii) La A være et lukket tallteoretisk Σ_1^0-utsagn. Da $\mathcal{N} \models A \;\Leftrightarrow\; R \vdash A$.*

Bevis av Lemma 4.18. Vi viser (i). Punkt (ii) følger trivielt fra (i). La A og A' være logisk ekvivalente og anta at $R \vdash A'$. Da har vi også at $R \vdash A$ siden den logiske kalkylen vår

(tremetoden) er komplett. Ved Lemma 4.17 holder det nå å vise at $\mathcal{N} \models A \Leftrightarrow R \vdash A$ for ethvert Δ_0^0-utsagn på BNNF. Nå er det trivielt at $R \vdash A \Rightarrow \mathcal{N} \models A$ siden den logiske kalkylen er sunn og $\mathcal{N} \models R$. Dermed gjenstår det å vise

$$\mathcal{N} \models A \Rightarrow R \vdash A \text{ for ethvert lukket } \Delta_0^0\text{-utsagn } A \text{ på BNNF.} \qquad (*)$$

Det gjøres ved induksjon på den syntaktiske oppbygningen av A. Vi skisserer strukturen i beviset og lar en del detaljer ligge.

Vis at $R \vdash \overline{p} + \overline{q} = \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \models \overline{p} + \overline{q} = \overline{r}$. (Gjøres ved induksjon på q. Se side 18.)

Vis at $R \vdash \neg(\overline{p} + \overline{q} = \overline{r})$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \not\models \overline{p} + \overline{q} = \overline{r}$. (Gjøres ved induksjon på q. Se side 18.)

Vis at $R \vdash \overline{p} \times \overline{q} = \overline{r}$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \models \overline{p} \times \overline{q} = \overline{r}$, og vis at $R \vdash \neg(\overline{p} \times \overline{q} = \overline{r})$ for alle $p, q, r \in \mathbf{N}$ slik at $\mathcal{N} \not\models \overline{p} \times \overline{q} = \overline{r}$.

Nå er det mulig å vise at $R \vdash t_1 = t_2$ for alle termer t_1, t_2 slik at $\mathcal{N} \models t_1 = t_2$, og at $R \vdash \neg(t_1 = t_2)$ for alle termer t_1, t_2 slik at $\mathcal{N} \not\models t_1 = t_2$.

Nå har vi skissert et bevis av (*) for atomære og negerte atomære utsagn. Dette er induksjonsstart i et bevis av (*). Nå skal vi se på induksjonstrinnene.

Anta: A har formen $B \wedge C$ og $\mathcal{N} \models A$. Da har vi $\mathcal{N} \models B$ og $\mathcal{N} \models C$. Dermed gir induksjonshypotesen $R \vdash B$ og $R \vdash C$. Fra dette følger $R \vdash A$.

Induksjonstrinnet når A har formen $B \vee C$ byr heller ikke på nevneverdige problemer. Det gjør induksjonstrinnene for de begrensede kvantorene. Ja, trinnet for begrenset eksistenskvantor er forsåvidt ikke så ille: Anta at A har formen $(\exists x < t)[B(x)]$ og at $\mathcal{N} \models A$. Da finnes et numeral $\overline{n}$ slik at $\mathcal{N} \models \overline{n} < t$ og $\mathcal{N} \models B(\overline{n})$. Her er $B(\overline{n})$ et lukket Δ_0^0-utsagn A på BNNF. Dermed gir induksjonshypotesen $R \vdash B(\overline{n})$. Videre har vi at $\overline{n} < t == (\exists u)[\overline{n} + S(u) = t]$. Dermed finnes det numeral $\overline{m}$ slik at $\mathcal{N} \models \overline{n} + S(\overline{m}) = t$. Siden $\overline{n} + S(\overline{m}) = t$ er et lukket Δ_0^0-utsagn gir induksjonshypotesen $R \vdash \overline{n} + S(\overline{m}) = t$. Nå har vi altså $R \vdash B(\overline{n})$ og $R \vdash \overline{n} + S(\overline{m}) = t$. Dermed $R \vdash (\exists u)[\overline{n} + S(u) = t]$. Dermed $R \vdash \overline{n} < t$. Dermed $R \vdash \overline{n} < t \wedge B(\overline{n})$. Dermed $R \vdash (\exists x)[x < t \wedge B(x)]$. Dermed $R \vdash (\exists x < t)[B(x)]$. Dermed $R \vdash A$. Det var induksjonstrinnet for begrenset eksistenskvantor. For å få til induksjonstrinnet for begrenset allkvantor, må man blant annet benytte at $(\forall x)[x \neq 0 \rightarrow (\exists y)[x = S(y)]]$ er et aksiom i R. Vi lar detaljene rundt dette ligge. □

Når vi i tillegg til ufullstendighetsresultatene for tallteori har Teorem 4.18, er det enkelt å vise et uavgjørbarhetsteorem for første ordens logikk. Legg merke til at vi altså trenger at første ordens teorier har en viss styrke for å vise uavgjørbarhetsteoremet under. Det trengte vi ikke for å vise ufullstendighetsteoremene over.

Teorem 4.19 (Uavgjørbarhet) *Mengden av gyldige første ordens utsagn er ikke rekursiv.*

Bevis av Teorem 4.19. (Turings teorem) Ved Lemma 4.6 kan vi effektivt konstruere et tallteoretisk Σ_1^0-utsagn A slik at $\mathcal{N} \models A$ hvis og bare hvis $\langle m, n \rangle \in K$. Vi har dermed

$$\begin{aligned}
\langle m, n \rangle \in K &\Leftrightarrow \mathcal{N} \models A && \text{Teorem 4.18} \\
&\Leftrightarrow R \vdash A && \text{def. av } R \vdash A \\
&\Leftrightarrow \vdash R \rightarrow A && \text{kompletthet} \\
&\Leftrightarrow \models R \rightarrow A\,. &&
\end{aligned}$$

Anta så at mengden av gyldige første ordens utsagn ikke er rekursiv. Vi antar altså at vi har en algoritme for å avgjøre hvorvidt utsagnet $R \to A$ er gyldig. Da gir ekvivalensen over en algoritme for å avgjøre medlemskap i K. Dermed er K rekursiv. Det sier i mot Teorem 3.18. □

Spørsmålet som besvares ved Teorem 4.19, var i mange år åpent og ble kalt for "Hilberts Entscheidungsproblem". Beviset av teoremet kan spores tilbake til Church og Turing (1936-37). Deres beviser er annerledes enn vårt. Det er ikke nødvendig å gå veien om tallteori. Turing viste at stoppeproblemet for Turingmaskiner ikke kan avgjøres av en Turingmaskin. Deretter viste han at man kan konstruere et første ordens utsagn som er gyldig hvis og bare hvis eksekveringen av en gitt Turingmaskin med input terminerer. (Og at en Turingmaskin kan gjennomføre denne konstruksjonen.) Av dette kan man slutte at en Turingmaskin ikke kan avgjøre hvorvidt et vilkårlig første ordens utsagn er gyldig.

Korollar 4.20 *Mengden av gyldige førsteordens utsagn er rekursivt tellbar, men den er ikke rekursiv.*

Bevis av Korollar 4.20. Tremetoden er komplett. Dermed kan vi lage en algoritme som lister opp alle gyldige utsagn. Leseren kan overbevise seg selv om dette. Så mengden av gyldige førsteordens utsagn er rekursivt tellbar. Teorem 4.19 sier at mengden ikke er rekursiv. □

4.5 Oppgaver

Oppgave 1
Definisjonen av begrensede kvantorer står på side 50. Vis at utsagnene $(\forall x < n)[A(x)]$ og $\neg(\exists x < n)[\neg A(x)]$ er logisk ekvivalente. Bruk for eksempel tremetoden og vis at treet over $(\forall x < n)[A(x)] \leftrightarrow \neg(\exists x < n)[\neg A(x)]$ er lukket. Vis også at $\neg(\forall x < n)[\neg A(x)]$ og $(\exists x < n)[A(x)]$ er logisk ekvivalente.

Oppgave 2
Vi har definert relasjonen $<$ ved $x < y \overset{\text{def}}{\Leftrightarrow} (\exists z)[x + S(z) = y]$. Alternativt kunne vi ha innført symbolet $<$ som et primitivt relasjonssymbol i språket for tallteori, og latt modellen $\mathcal{N}$ tolke $<$ som vanlig ekte mindre enn på hele tall. Deretter kunne vi ha utvidet R med aksiomene

$$\begin{array}{ll} (R_8) & (\forall x)\,[\,\neg 0 < x\,] \\ (R_9) & (\forall x, y)\,[\,x < S(y) \;\leftrightarrow\; (x = y \vee x < y)\,]\,. \end{array}$$

Så kunne vi ha gått videre, definert de begrensede kvantorene, definert Δ_0^0 for tallteori, etc. Ad denne vei kunne vi ha bevist uavgjørbarhetsteoremet for første ordens logikk . Vi skal se litt nærmere på hvorfor denne alternative strategien virker.

Vi kaller det utvidede aksiomsettet for $R^<$. La A være et vilkårlig utsagn i språket til teorien $R^<$. Da er

$A^* \;==\; A$ hvor ethvert delutsagn på formen $t_1 < t_2$ er erstattet med $(\exists z)[t_1 + S(z) = t_2]$

(Her er t_1 og t_2 vilkårlige termer.)

Punkt a
Vis at $R \vdash A^*$ for ethvert aksiom A i $R^<$.

Punkt b
Vis at for alle utsagn A i språket til $R^<$ at $R \vdash A^* \Leftrightarrow R^< \vdash A^*$.

Oppgave 3
I denne oppgaven skal du forsøke å generalisere ideen om begrensede kvantorer til andre datastrukturer enn de naturlige tallene.

Punkt a
Definer noe som svarer til tallteoriens begrensede kvantorer for teorien om binære sekvenser, og definer Δ_0^0 for teorien om binære sekvenser analogt med Δ_0^0 for tallteori.

Punkt b
Vis at mengden av sanne lukkede Δ_0^0-utsagn i teorien om binære sekvenser er rekursiv.

Punkt c
I forrige oppgave ble man bedt om å vise at de tallteoretiske utsagnene $(\forall x < n)[A(x)]$ og $\neg(\exists x < n)[\neg A(x)]$ er logisk ekvivalente. Vis den analoge ekvivalensen for begrensede kvantorer i teorien om binære sekvenser.

Punkt d
Elementene i en datastruktur kan bygges opp fra en endelig mengde konstruksjonsfunksjoner med fast aritet. (0 og S er konstruksjonsfunksjonene for de naturlige tallene.) Diskuter hva som må være aksiomer i en første ordens teori om en vilkårlig datastruktur. Diskuter hvordan ideen om tallteoriens begrensede kvantorer kan generaliseres til første ordens teorier om vilkårlige datastrukturer.

Oppgave 4
I følge definisjonen er en første ordens teori T *fullstendig* dersom den er konsistent og slik at $T \vdash A$ eller $T \vdash \neg A$ for enhver A i det aktuelle språket. En første ordens teori T er *fullstendig for en modell* $\mathfrak{M}$ dersom $\mathfrak{M} \models T$ og $\mathfrak{M} \models A \Rightarrow T \vdash A$.

Punkt a
Vis at T er fullstendig hvis og bare hvis det finnes en modell $\mathfrak{M}$ slik at T er fullstendig for $\mathfrak{M}$.

Punkt b
La $\mathfrak{M}$ være en modell for et første ordens språk, og la T være en første ordens teori over samme språk. (i) Hvis T er fullstendig for $\mathfrak{M}$, så er T fullstendig. (ii) Hvis T er fullstendig, så er T fullstendig for $\mathfrak{M}$. Vis at (i) holder og at (ii) ikke holder.

Oppgave 5
Teorem 4.14 sier at for enhver n-ær rekursiv funksjon f, finnes det et bitteoretisk utsagn $F(x_1, \ldots, x_n, y)$ slik at

$$f(a_1, \ldots, a_n) = b \quad \Leftrightarrow \quad \mathcal{B} \models F(\underline{a}_1, \ldots, \underline{a}_n, \underline{b}) \, .$$

Vi viste teoremet ved induksjon på en μ-rekursiv generering av f. Vis teoremet ved induksjon på en rekursiv generering av f. Man slipper da det ubehagelige tilfellet for multiplikasjon i induksjonstart. Til gjengjeld får man et nytt induksjonstrinn som er omtrent like ubehagelig.

Kapittel 5

Referanser

La meg til slutt hjelpe leseren med litt litteratur rundt temaer som tas opp i dette kompendiet. Det finnes et utall innføringsbøker i logikk. Problemet er at de færreste av dem forteller hvor man kan finne mer lesestoff om de forskjellige temaene som berøres. Jeg nevner derfor [9]. Den har en liten litteraturliste og ser forøvrig ut til å være en temmelig vidtrekkende og all right innføringsbok.

Både [6] og [7] er omfattende introduksjonsbøker til klassisk rekursjonsteori. Boken [8] handler om subrekursjon, dvs. om funksjonsklasser som er delmengder av de rekursive funksjonene. Der kan man blant annet finne mer stoff om de primitivt rekursive funksjonene.

Den som er interessert i å få oversikt over logikkens historie og utvikling, kan lese første del av von Wrights bok [3]. Jeg vil i så henseende også anbefale [4] og [5]. [4] er en lettfattelig og lettlest bok som setter Gödels innsats inn i en historisk sammenheng. Boken forklarer for lekmenn hva et aksiomsystem er, hva et absolutt konsistensbevis er, osv. Boken kulminerer ved å bevise Gödels to ufullstendighetsteoremer. [5] er en samling skrifter fra den matematiske logikkens barndom og glanstid. Her finner man verker av Frege, Peano, Hilbert, Brouwer, Skolem, Zermelo, Frankel, Russel, Gödel osv. Hver artikkel har en innledning som hjelper leseren til å få et historisk perspektiv på stoffet. Har man først litt kunnskap om logikk, så er ikke dette så tungt å lese som man kanskje skulle tro.

Undertegnede har et nært forhold til kompendiene [1] og [2]. Begge steder finner man igjen en god del fra dette kompendiet.

I [10] kan man lese om alle noenlunde alminnelige temaer i matematisk logikk. Det er en slags oppslagsbok, og man bør vite sånn circa hva man er ute etter når man åpner boken.

Den som er interessert i å lese mer om Turings tese kan starte med å kikke på [11]. Der vil man finne referanser til en mye leseverdig litteratur om emnet.

Referanser

[1] Fenstad, J.E. Normann, D. *Innføring i matematisk logikk.* Matematisk Institutt, Universitetet i Oslo, 1990.

[2] Jervell, H. R. *Forelesninger i logikk.* Institutt for informatikk, Universitetet i Oslo, 1989.

[3] von Wright, G.H. *Logik, filosofi och språk.* Doxa Press, 1980.

[4] Nagel E., Newman J.R. *Gödels proof.* New York University Press, 1958.

[5] van Heijenoort, J *From Frege to Gödel. A source book in mathematical logic 1879 - 1931.* Harvard University Press, 1967.

[6] Oddifreddi, P. *Classical recursion theory.* North-Holland, 1989.

[7] Rogers, H. *Theory of recursive functions and effective computability.* McGraw Hill, 1967.

[8] Rose, H. E. *Subrecursion. Functions and hierarchies.* Clarendon Press, 1984.

[9] van Dalen, D. *Logic and structure.* Springer-Verlag, 1994.

[10] Barwise, J. (ed.) *Handbook of mathematical logic.* North-Holland Publ. Co., 1977.

[11] Kristiansen, L. *Turings teorem.* NORMAT (Nordisk matematisk tidskrift.) 199?. (Sendt til trykking jan. 98)