SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Disjunktionsegenskaper och existensegenskaper inom intuitionistisk logik

av

Iris van Rooijen

2012 - No 17

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET, 106 91 STOCKHOLM

Disjunktionsegenskaper och existensegenskaper inom intuitionistisk logik

Iris van Rooijen

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Erik Palmgren

2012

Sammanfattning

Den största skillnaden mellan intuitionistisk logik och klassisk logik är att matematiska objekt tolkas som mentala konstruktioner istället för ting i en yttre värld. Då ändras tolkningen på disjunktionsegenskapen, eftersom *lagen om det uteslutna tredje* inte längre gäller och existensegenskapen för ett objekt, eftersom vi inte kan härleda existens med hjälp av *reductio ad absurdum*. Jag tänkte undersöka vad det kan få för följder att ha detta tankesätt, till exempel: Hur tolkas sanning inom intuitionistisk logik? Hur fungerar matematiken? Och varför kan man tänka sig att ogiltigförklara *reductio ad absurdum* och *lagen om det uteslutna tredje*?

Innehåll

1 Introduktion

För att visa att ofullständighet gäller för teorier som innehåller Peanos aritmetik, skapade Gödel en metod med vilken man kan uttrycka 'Denna sats är ej bevisbar' matematiskt. Det är en variant av Russells paradox 'Denna sats är inte sann', och när man försöker bevisa Gödels sats härleder man 'trubbel'. Det vill säga, om satsen är falsk, kan vi bevisa den, vilket ger att den är sann. Men om den är sann, bevisar vi att den inte är bevisbar. Men det medför att våra teorier inte kommer kunna bevisa sin egen konsistens.[1]

Inom den klassiska logiken gäller påståendet att, $\forall x : A(x) \vee \neg A(x)$. Det vill säga, för alla element x gäller antingen påståendet $A(x)$ eller dess motsats. Men vi kommer med största sannolikhet för åtminstone några $A(x)$, inte kunna bevisa vilket av dem det är som håller. Ett exempel på detta är till exempel ZFC och Cantors kontinuum-hypotes, som säger att det inte finns någon mängd vars kardinalitet är strikt emellan de naturliga talen, och de reella talens kardinalitet.

Problemet är att man inom den klassiska logiken antar att saker och ting kan vara sanna eller falska oavsett vad vi vet om dem. Detta synsätt härstammar från en sorts Platonsk världsbild, där de matematiska talen och lagarna existerar i en egen extern (ofta även 'högre') värld. Att då komma på, bevisa eller lära sig, nya matematiska lagar, innebär att man 'upptäcker' en ny (världs-)del i detta matematiska kosmos. Ett kosmos där allt är antingen sant eller falskt.

Det leder till att man i dessa fall anser sig kunna veta saker som man enligt den intuitionistiska logiken kanske inte kan dra allt för förhastade slutsatser om. Till exempel *lagen om det uteslutna tredje*, och därmed disjunktionsegenskaper, och *reductio ad absurdum*, och därför existensegenskaper för ett objekt.

Inom intuitionistisk logik bortser man från en extern matematisk värld. Detta har förstås stora konsekvenser. För att kunna säga något om ett ting alls, måste vi kunna konstruera det (in i minsta detalj) då vi inte längre kan referera till dem som yttre (konkreta) objekt. Sanning och falskhet förvandlas då snarare till någon form av konstruerbarhet eller bevisbarhet.

Vi kan nu se att *reductio ad absurdum* inte nödvändigtvis gäller längre eftersom vi kräver en explicit beskrivning av x och hur man konstruerar det. Inom intuitionism skulle man kunna tolka *reductio ad absurdum* som (Brouwer)[2] : 'Jag har konstruerat detta x eftersom jag inte ej kunde konstruera det.' Något som givetvis kan låta ganska absurt.

I dessa fall måste man antingen explicit visa att *reductio ad absurdum* gäller. Annars måste man härleda A på annat sätt.

[1] Att en teori **T** är konsistent innebär att man inte kan härleda både A är sann och A är falsk ur **T**.

[2] Översättning av författare- 'I have created this x because I couldn't not create it...' [1]

Påståenden som byggs upp med hjälp av *lagen om det uteslutna tredje* kan få en lika mystisk intuitionistisk tolkning, speciellt i samband med $\forall x$. Vi har till exempel att man inom klassisk logik kan tyda $\forall x(A(x) \vee \neg A(x))$ som att, för varje x är satsen $A(x)$ antingen sann eller falsk, vilket kan tyckas fullt rimligt (under förutsättning att matematiska objekt finns utanför vårt medvetande). Inom intuitionistisk logik tolkas samma formel som att man för varje x antingen kan konstruera det så att $A(x)$ gäller, annars gäller $\neg A(x)$. Detta är mycket mindre sannolikt, därför att det verkar kräva att vi för varje x ska veta huruvida den har egenskapen A eller $\neg A$. Men så länge vi har olösta mysterium, så som: 'finns det oändligt många tvillingsprimtal?' är denna sats falsk.[3] Antag till exempel att $A(x)$ omm det finns oändligt många primtalstvillingar, vi kommer kanske aldrig få reda på ifall det finns ett x så att $A(x)$.

Då vi intuitionistiskt sett inte får använda oss av *reductio ad absurdum* eller *lagen om det uteslutna tredje* i sammanhang där vi får använda oss av dem i klassisk logik, verkar man bli mer begränsad, samtidigt ser man fler nyanser. Vi kan därför inte säga att intuitionism är varken starkare eller svagare än klassisk logik, eftersom man inom båda områdena kan dra slutsatser som man inte kan inom den andra. Eftersom klassisk logik går på sanning och falskhet, medan intuitionistisk logik pratar om bevisbarhet och konstruerbarhet, kan man egentligen inte ens jämföra dem i styrka, då de mäter olika saker.

Detta tankesätt påverkar då mest disjunktionsegenskapen, på grund av *lagen om det uteslutna tredje* och existensegenskapen för ett objekt och på grund av att vi inte kan härleda existens med hjälp av *reductio ad absurdum*. Jag tänkte undersöka vad det kan få för följder att ha detta tankesätt, till exempel: Kan det ändå finnas något spår av sanning inom intuitionistisk logik? Om de matematiska talen inte existerar i någon yttre värld, hur existerar de då? Och vad kan det ha för följder att inte ogiltigförklara *reductio ad absurdum* och *lagen om det uteslutna tredje*?

2 Filosofi kring intuitionism

Vad är det som kan giltigförklara intuitionismen som logiskt giltigt, och att föredra framför den klassiska logiken? Dummett tar upp några aspekter av vad det innebär att se på matematiska objekt som mentala, och ifall vi faktiskt har åstadkommit något med detta.

[3] Vi har till exempel enligt Gödels ofullständighetssats, att vi aldrig kommer finna en fullständig teori (baserad på (Peano) aritmetik).

2.1 Meningen med mentala konstruktioner

Trots att mentala objekt verkar lösa en del problem, skapas samtidigt andra problem som behöver lösas. Till exempel, hur kan dessa matematiska objekt jämföras? Är mina 2:or desamma som dina 2:or, kommer mina bevis att hålla när dina bevis håller? Är mina 2:or idag detsamma som mina 2:or imorgon, eller måste jag bevisa varje sats igen varje gång jag vill använda den?

Heyting [9] tänkte sig att om man fäster vissa världsliga egenskaper vid objekten, har man möjlighet att jämföra ens egna, både i tiden, och med andra människors objekt. Även Dummett tänkte sig att matematiken inte endast kan vara mental, eftersom vi måste kunna kommunicera den på något sätt. Något som inte går att kommunicera går inte att förklara för folk, och vad är då matematikens mening?

Dummett [6] tänkte sig att mening endast kan fås genom användning. Han tänkte sig matematiska objekt som schackpjäser, vars mening bestäms av deras roll och användning i spelet. Här får inga spelregler vara helt (eller delvis) mentala, på så sätt att en del av schack-spelets regler befinner sig endast i spelarens huvud och inte går att kommunicera, eftersom det skulle medföra att ingen annan kan förstå schack. Detsamma gäller de matematiska påståenden man skapar i huvudet.

Detta går hand i hand med hur vi tänker oss att vi lär oss matematik. Vi ser hur andra använder addition, och skapar en teori för hur denna regel verkar fungera. Så länge folk runt omkring oss reagerar positivt när vi använder vår regel behåller vi den, men när folk reagerar negativt ifrågasätter vi vår teori och ändrar kanske på den lite för att försöka förbättra den till att bättre passa ihop med andras användning av addition. Vi kontrollerar även att vi reagerar rätt vid andras användning av addition för att se om vi har förstått rätt.

På det sättet lär vi oss även hur termer och påståenden fungerar och vilka roller de har i olika bevis, samt även vilka roller dessa bevis spelar inom olika teorier. Ingenstans kommer det in något krav, eller ens behov, av en extern värld vi ej kan se, där tal och teorier existerar. Utan det är endast med hjälp av användning som vi kan få bekräftat att du och jag tänker likadant om en viss regel eller ett visst bevis.

Språk, i såväl tal som skrift och naturligtvis även kroppsspråk, får då en mycket viktigare roll i matematiska sammanhang, och kan inte längre ses, som Brouwer tänkte sig, som ytterst opålitliga sätt att kommunicera på, och en biprodukt av matematiken. Det är snarare detta hela vår förmåga att tänka matematiskt beror på [5].

När vi tänker på mening på detta sätt för intuitionistisk logik, kan påståenden som varken går att bevisa eller motbevisa fortfarande ha mening. Åtminstone så länge vi vet hur vi ska använda dem.

2.2 Sanningen om mentala konstruktioner

Kommunikation kring matematik sker inte endast mellan intuitionister, ofta kan platonister och intuitionister resonera kring ett påstående på samma sätt. Frågan är hur intuitionister ska förstå ordet sanning (för att inte glömma falskhet), och ifall det är något som är tillgängligt för dem. För utan tolkning av sanning är det svårt att tänka sig hur vi ska förstå vad platonister menar när de är helt säkra på att något är 'sant'.

Hur ska då sanning tolkas intuitionistiskt? Ska sanning tolkas som en del av påståendet? Har vi någon form av sanning i de medel vi använder för att bevisa ett påstående? Något som giltigförklarar själva beviset, och försäkrar oss om, att så länge axiomen och beviset håller, kommer även slutsatsen att hålla.

Det är klart att sanning inte kan tolkas som klassiskt bevisbart. Det finns olika fall inom klassisk logik där ett påstående varken går att bevisa eller motbevisa, ett exempel, som redan tagits upp är ZFC och kontinuumhypotesen. Ändå anser man i dessa fall att påståndet ska vara antingen sant eller falskt.

Vad kan man då ha för sorts bevis där vi kan vara trygga i att ingen motsägelse eller falskhet kommer att kunna härledas? Dummett [7] undersökte två olika riktlinjer för intuitionistiska bevis, för att se om sanning skulle hålla i dessa teorier.

Bevis och konstruerbara exempel. Inom den intuitionistiska logiken har vi att vi explicit måste ha bevisat hur man konstruerar ett tal med en viss egenskap, för att kunna anta att det är sant att ett tal kan ha den egenskapen. Vi måste kunna undersöka, just detta objekt och se ifall vårt påstående om det stämmer.

Kan vi säga att, eftersom vi vet hur man adderar, kan vi säga att 1) '867592+223159=1090751' är antingen sant eller falskt, trots att vi inte vet svaret förrän vi faktiskt har gjort beräkningen? Det verkar helt absurt att anta att vi inte kan utesluta ett mellanting, vad skulle detta mellanting överhuvudtaget kunna vara? Vi verkar kunna anta att, för någon tidpunkt k har vi:

$$(\vdash_k \forall y.A(y)) \to (\forall y.\exists n. \vdash_n A(y)$$

Här betyder $\vdash_k$ att vi har härlett det vid tidpunkt k. I detta fall kan det tolkas som, (efters)om vi, vid tidpunkt k, har ett bevis för till exempel addition, som gäller för alla tal, har vi för alla tal, ett bevis för att addition gäller för just 1) tal. Det verkar inte vara så mycket konstigt med detta. Samtidigt var vi tvungna att göra ovanstående beräkning innan vi faktiskt kunde 'bevisa' att den var sann. Och det finns ingenting som säger att någon faktiskt någonsin skulle göra just denna beräkning.

Ska man anta att ett bevis för något gäller, även om objektet beviset gäller för aldrig har konstruerats? Och då de mentalt konstruerade objekten är de enda som finns, medför det att vi har skapat ett bevis som gäller för ting som inte existerar? Ett induktionsbevis, bygger till exempel på att beviset fungerar för föregående tal. Men om A(5383982) aldrig har realiserats, kan vi då verkligen anta A(5383983)?

Detta skulle kunna leda till att vi till slut kan bevisa saker vi vet ej är sanna.

Endast bevisbarhet genom konstruktion. Om vi istället antar att vi endast kan veta sånt som vi har konstruerat eller beräknat explicit, finns det inte mycket vi kan anta. Vi kommer aldrig kunna bygga något på all-kvantifikatiorer och i princip inte kunna hålla på ens med de naturliga talen. På det sättet kan vi undvika att någonsin dra en falsk slutsats, men det är däremot extremt begränsande.

Man kanske i detta fall kunna ifrågasätta hur mycket man kan ta bort från bevisbarhetens hållbarhet. Ett 'bevis' verkar då snarare bygga på lösa exempel. All generalitet verkar ouppnåelig för större mängder.

Det verkar som att vi får två olika fall av existens. En mer användbar som, då vi konstruerat och bevisat hållbarheten för tillräckligt många x, antar att vi även kan konstruera och bevisa hållbarheten för fler x. Men med denna version riskerar vi bevisa påståenden som är falska. Och en annan snävare version som kräver explicit konstruktion av varje x, innan man får använda sig av det i ett bevis. Men denna version leder till att vi endast kan kvantifiera över 'mycket små' mängder'.

3 Disjunktion och existens, olika tolkningar

Här ges några exempel på fall som kan tolkas olika beroende på hur strikt man ser på sanning i relation till mentala konstruktioner. Men även i jämförelse med hur de kan tolkas enligt klassisk logik.

3.1 Existens och oändligt många primtal?

Det finns oändligt många primtal, och inom klassisk logik fungerar beviset som följande: anta att det inte finns oändligt många primtal, och härled sedan en motsägelse. Det vill säga, vi verkar kunna härleda påståendet $A =$'det finns oändligt många primtal' med hjälp av *reductio ad absurdum*. Något vi inte alltid bara kan använda oss av inom intuitionistisk logik.

Ändå fungerar detta bevis inom intuitionistisk logik, helt enkelt eftersom det vi faktiskt försöker bevisa är $B(x) =$ 'existensen av ett tal x med en speciell egenskap (att vara det största primtalet)'. Vi bevisar sedan (dock inte längre med hjälp av *reductio ad absurdum*) att ett sådant tal inte existerar, det går inte att konstruera, vilket alltså leder till $\neg B(x)$.

Att det inte finns oändligt många primtal p_i, innebär att det ska gå att konstruera ett p_n som är det största primtalet. För att följa det klassiska receptet, kan vi nu konstruera talet $q = (p_1 \cdot p_2 \cdot \cdots \cdot p_n) + 1$ där p_i för $1 \leq i \leq n$ är ett primtal. Det följer då att q inte kan vara ett sammansatt tal $q = x \cdot y$ sådant att minst ett av x eller y är mindre än eller lika med p_n. Då får vi att q antingen är ett primtal, eller ett tal $q = x \cdot y$ för minst ett primt x så att $p_n < x < q$. Det innebär att vi, för varje mängd av primtal, vet hur vi ska hitta ett nytt primtal. Det vill säga, vi kan konstruera oändligt många primtal. [4]

I den väldigt snäva tolkningen av existens inom intuitionistisk logik, kan man dock inte säga så mycket om existensen av ett största primtal. Vi kan där endast prata om det existensen av det största primtal som vi har skapat hittills, samt de sammansatta tal vi har konstruerat. Även om vi skulle utföra tekniken ovanför, skulle det endast leda till att att vi har konstruerat ett (eller flera) primtal till, men inte bevisa att det finns oändligt många.

3.2 a^b är rationellt för irrationella a,b

Inom klassisk logik går det att bevisa att det existerar ett rationellt tal a^b där a och b är irrationella med hjälp av $\sqrt{2}^{\sqrt{2}}$, som antingen är rationellt eller irrationellt. Vi vet däremot att $\sqrt{2}$ är irrationellt, vilket ger två fall:
a) $\sqrt{2}^{\sqrt{2}}$ är irrationellt, då är $a = \sqrt{2}^{\sqrt{2}}$ och $b = \sqrt{2}$.
b) $\sqrt{2}^{\sqrt{2}}$ är rationellt, då är $a = \sqrt{2}$ och $b = \sqrt{2}$.
Intuitionistiskt sett gäller inte detta eftersom man inte kan bygga något på $A \vee \neg A$ utan att veta vilket av dem som gäller. För att konstruera ett intuitionistiskt exempel måste man hitta a och b som är bevisbart irrationella.[5] Vi kan då helt enkelt ta $a = e$ och $b = ln(2)$.

3.3 $10^{10^{10}} + 1$ är antingen ett primtal eller inte ett primtal

Hur ska vi tolka giltigheten för detta påstående? I den mindre snäva definitionen av disjunktion och existens inom intuitionism, kan vi utgå ifrån att jag, även om jag inte vet vilket alternativ som håller, kan göra uträkningen och därmed komma fram till svaret. På så sätt är jag ändå berättigad att, för $x = 10^{10^{10}}+1$ och då $A(x)$ innebär att x är ett primtal, säga att $A(x) \vee \neg A(x)$ gäller.

I den snävare intuitionismen skulle jag däremot inte kunna påstå något sådant. Jag har inte explicit kontrollerat vilket av allternativen som håller, och kan därför inte dra några slutsatser om påståendet. Jag kan definitivt inte bygga något bevis på $A(x) \vee \neg A(x)$, vilket jag skulle kunna göra annars.

[4] Vi måste förstås även visa att vi för varje tal $q_i > p_n$ vet huruvida det är ett primtal eller inte, vilket enkelt går genom att vi successivt prövar att dela q_i med $k = 2, 3, 4, \cdots, q_i - 1$.

[5] Det visar sig dock att $\sqrt{2}^{\sqrt{2}}$ är irrationellt [10].

4 Logiska uttryck

Inom intuitionistisk logik ses inte logiken som ett sätt att förklara matematiken [9, s. 123] [1, s. 39], utan snarare som ett redskap för att visa regulariteter [5, s. 8]. Och man kan undra vilket som kom först. Vi har visserligen skapat den intuitionistiska logiken, som resultat av att se matematiska tal och formler som mentala objekt och dess egenskaper och relationer till andra objekt. Å andra sidan kanske vi inte skulle välja att tro på ett matematiskt bevis om vi inte fick någon form av sanningskänsla, som talar om för oss vad som är det rätta att göra.

På så sätt påverkar vi vilka teorier som 'håller' genom att själva bestämma de regler som bestämmer vilka teorier som är hållbara. Vi anpassar logiken efter våra egna önskemål och då kan man förstås undra hur pålitlig den faktiskt är.

Men trots att logiken inte har haft så högt anseende för alla, har många ändå formulerat formella system för att tydligt kunna klargöra vad som fås och inte får göras inom den intuitionistiska logiken, matematiken och tankesättet.

$\wedge$: $A \wedge B$ gäller omm A gäller **och** B gäller.
$\vee$: $A \vee B$ gäller omm vi vet att A gäller **eller** vi vet att B gäller.
$\exists$: $\exists x A(x)$ är sant om det finns ett bevis för något/några tal n i $A(\overline{n})$.
Detta ger upphov till endast en (ändlig mängd) beräkning (-ar).
$\forall$: $\forall x A(x)$ gäller omm vi för något tal n har att $A(\overline{n})$ gäller.
$\rightarrow$: $A \rightarrow B$ de antaganden som leder till A (tillsammans med eventuella andra antaganden), leder även till B.
$\neg$: $\neg A$ Negation definieras $\neg A \leftrightarrow (A \rightarrow 1 = 0)$. Det vill säga, när vi bevisar A kommer vi även bevisa att $1 = 0$, men eftersom vi vet att detta aldrig kommer att hända, vet vi att vi heller aldrig kommer konstruera ett bevis för A.

För ett tal n har vi $\overline{n}$ som betecknar talet. För samma n skulle $\overline{n}$ alltså kunna vara 'elva', '11', 'XI'...

4.1 Olika exempel

Vi har att 1) $A \rightarrow \neg\neg A$, vilket man kan tolka som; då vi har ett bevis för A kommer vi aldrig kunna bevisa att vi aldrig kan bevisa A. Däremot gäller inte, $\neg\neg A \rightarrow A$, eftersom vi inte använder oss av *reductio ad absurdum*. Även om vi har bevisat att vi aldrig kommer bevisa att A inte kan bevisas, betyder inte det att vi kan sluta oss till att A gäller.

Vi har däremot att $\neg\neg\neg A \to \neg A$.

$$\dfrac{\dfrac{\dfrac{[\neg\neg\neg A]^3 \qquad \dfrac{\dfrac{[\neg A]^1 \quad [A]^2}{\bot}}{\neg\neg A}\,{\scriptstyle 1}}{\bot}}{\neg A}\,{\scriptstyle 2}}{\neg\neg\neg A \to \neg A}\,{\scriptstyle 3}$$

Vi har att $(\neg A \land \neg B) \leftrightarrow \neg(A \lor B)$, vilket kan tolkas som, då vi aldrig kommer hitta ett bevis för A, och aldrig kommer hitta ett bevis för B, kommer det inte vara så att vi någonsin hittar ett bevis för att $(A \lor B)$ gäller. Härledning för $\to$:

$$\dfrac{\dfrac{\dfrac{\dfrac{[A \lor B]^2 \quad [B]^1 \quad \dfrac{\dfrac{\dfrac{[A]^1 \quad \dfrac{[\neg A \land \neg B]^3}{\neg A}}{\bot}}{B}}{}}{B}\,{\scriptstyle 1} \qquad \dfrac{[\neg A \land \neg B]^3}{\neg B}}{\bot}}{\neg(A \lor B)}\,{\scriptstyle 2}}{(\neg A \land \neg B) \to \neg(A \lor B)}\,{\scriptstyle 3}$$

Vi har även att $(\neg A \lor \neg B) \to \neg(A \land B)$, men däremot kan vi inte härleda $\neg(A \land B) \to (\neg A \lor \neg B)$ utan att använda oss av *reductio ad absurdum*[3].[6]

Intuitionistisk logik är på så sätt grunden till den konstruktiva logiken som, som namnet antyder, ser vad som går att konstruera och beräkna.[7] Då ett objekt måste konstrueras in i minsta detalj, kan man inte härleda något ur $A \lor B$ så länge man inte vet vilket av A eller B som gäller. Det är just dessa slutsatser som även en dator kan göra, då en dator, för att kunna konstruera något, måste veta explicit vilket utav A eller B den ska konstruera på.

5 Heyting och Peanos axiom

Naturliga talen $\mathbb{N}$ går inte att definiera på samma sätt som i den klassiska matematiken, där de anses finnas i någon yttre värld, utan måste ges en utförlig förklaring.

Heyting använder sig av Peanos axiomatiska system för att bygga upp en grund till matematiken.

För att visa hur man konstuerar själva de naturliga tal, skapade Peano nio axiom. För att kunna konstruera de naturliga talen, eller något överhuvudtaget, måste man ha något att börja med, att bygga resten på. Peano använder 0,

[6] Se [9, s. 100] för ett motexempel till $\neg(A \land B) \to (\neg A \lor \neg B)$

[7] Konstruktiv logik skiljer sig dock genom att man inte utesluter extern värld.

vilket ger första axiomet:
P.1 $0 \in \mathbb{N}$

Sedan behöver man en operation, efterföljaroperationen $'$, för $x \in \mathbb{N}$ och genererar x:ets nästföljande tal. Med hjälp av dessa kan man sedan generera, konstruera, resten av de naturliga talen:
P2. $\forall x \in \mathbb{N} : x' \in \mathbb{N}$

Ett naturligt tal $n \in \mathbb{N}$ konstrueras alltså genom att man succesivt bygger upp det från 0 med hjälp av operationen $'$. Vid varje tillfälle kan man sedan stanna upp i kedjan och se på det tal man är på.

Man behöver nu skapa relationen: '=' (och dess motsats $\neq$ som gäller då denna relation ej gäller)[8] och för att vara säkra på att den är en ekvivalensrelation, visar vi att den åtminstone har reflexivitet, symmetri och transitivitet samt att den är sluten under operationen.
P3. $\forall x . x = x$
P4. $\forall x \forall y . (x = y \to y = x)$
P5. $\forall x \forall y \forall z . ((x = y \land y = z) \to x = z)$
P6. $\forall x \forall y . x = y \land x \in \mathbb{N} \to y \in \mathbb{N}$

Vi vill nu definiera 2 egenskaper för våra tal med hjälp av relationen '='.
P7. $\forall x . x' \neq 0$
P8. $\forall x \forall y . (x' = y' \to x = y)$

Sist vill vi ha en induktionsoperation:
P9. $A(0) \land \forall x (A(x) \to A(x')) \to \forall x (A(x))$ [9]

Least number principle: Trots att induktion gäller, kan man inom intuitionismen inte säga att LNP gäller så länge inte $A(x)$ är avgörbar. LNP ges av:

$$\exists x : A(x) \to \exists x : ((A(x) \land \forall y_{<x} \neg A(y))$$

Det vill säga, bara för att vi vet att $A(x)$ gäller för ett visst x, behöver det inte vara avgörbart för alla $y < x$ ifall $A(x)$ gäller. Då ett oavgörbart y inträffar vet vi inte vilket utav x eller y som är det minsta sådant att A gäller.

[8] Inom den intuitionistiska logiken (främst geometrin) skiljer man på $\neq$ och $\#$, som i den konstruktiva matematiken endast ses som $\neq$. Skillnaden inom den intuitionistiska logiken är att $\neq$ innebär att x och y är olika, medan $\#$ innebär att det finns en 'positiv skillnad' mellan x och y. Det vill säga, att x och y faktiskt är skilda åt. Inom aritmetik kan man dock visa att $\neq$ och $\#$ är ekvivalenta, till exempel på grund av efterföljar funktionen när det gäller naturliga tal [9].

[9] I de fall man inte vill använda sig av all-kvantifikatorn över mängder (utan endast de naturliga talen), kan man ersätta den med ett axiomatiskt schema, som tar upp varje fall för sig. Detta leder dock till att vi får oändligt antal axiom [6].

5.1 Exempel på funktioner i PA.

Med hjälp av andra ordningens logik (logik med mängder och t.ex. $\in$) kan vi skapa följande binära funktioner[10] och sist relationen:

+) $\forall x.x + 0 = x$
$\forall x, y.x + (y)' = (x + y)'$

$\cdot$) $\forall x.x \cdot 0 = 0$
$\forall x, y.x \cdot y' = x + x \cdot y$

<) $x < y := \exists z(z \neq 0 \wedge x + z = y)$

Vi får då till exempel att 2+2 ger:
$((0)')' + ((0)')' = \big(((0)')' + (0)'\big)' = \big(\big(((0)')' + 0\big)'\big)' = \big(\big(((0')')'\big)'\big)'$

Vilket är detsamma som 4. Multiplicering av två tal går att räkna ut på liknande sätt. För ett tal $m \neq n$ kan vi se om det finns i kedjan av talen 0 till och med n eller ej. Om ja, $m \leq n$. Om nej, $m > n$.

5.2 Heyting-Aritmetik (HA)

Heyting använder axiomen, ett delsystem av Peanos (klassiska) aritmetik **PA**, för att sedan visa hur intuitionistisk logik går ihop med detta system. Heyting inför en omskrivning A^* av det formella uttrycket A sådant att, om ett antagande A^* är sant i **PA** är det även sant i **Heytingaritmetik (HA)** om A är atomär, dvs. inte innehåller några konnektiv ($\vee, \wedge, \neg, \rightarrow$). Dummett [6, s. 36] definierar då: A^* och man får dessa regler för att översätta **PA** $\rightarrow$ **HA**.

1. $A^* = A$ om A är atomär.
2. $(A \wedge B)^* = A^* \wedge B^*$
3. $(A \vee B)^* = \neg(\neg A^* \wedge \neg B^*)$
4. $(A \rightarrow B)^* = A^* \rightarrow B^*$
5. $(\neg A)^* = \neg A^*$
6. $(\forall x.A(x))^* = \forall x.A^*(x)$
7. $(\exists x.A(x))^* = \neg\forall x.\neg A^*(x)$

Exempel Att $\forall x.(A(x) \vee \neg A(x))^*$ är sant i den klassiska Peanoaritmetiken, ger $\forall x.\big((A(x) \vee \neg A(x))\big)^*$, vilket enligt 3. ger $\forall x.\big(\neg(\neg(A^*(x)) \wedge \neg(\neg(A^*(x))))\big)$, där A är atomär. Ur detta får vi med hjälp av intuitionistiska härledningsregler, till exempel $(\neg A \wedge \neg B) \rightarrow \neg(A \vee B)$, att $\forall x.\big(\neg(\neg(A(x) \vee \neg A(x)))\big)$. Men som vi vet medför inte dubbel negation att ett påstående faktiskt

[10] Dessa funktioner kan sägas vara primitivt rekursiva funktioner (på så sätt att ett visst tal definieras med hjälp av dess föregångare), men för att visa att (primitivt) rekursiva funktioner överhuvudtaget får användas i en teori byggd på Peanos axiom, behöver vi använda oss av + och $\cdot$. Vi kan istället se på +, $\cdot$ och < som att tillhöra det aritmetiska språket, och tolkas som adition, multiplikation och 'mindre än'.

gäller, alltså får vi inte samma påstående för **HA** som vi har i **PA**.

6 Definitioner

6.1 Existensegenskaper och disjunktionsegenskapen

Intuitionistiska formella system, med en teori **T**, kan innehålla såväl en **disjunktionsegenskap (DP)** [1]

$$\mathbf{T} \vdash (A \vee B) \rightarrow \mathbf{T} \vdash A \text{ eller } \mathbf{T} \vdash B$$

som en **numerisk existensegenskap (NE)** [1]

$$\mathbf{T} \vdash \exists x : A(x) \rightarrow \mathbf{T} \vdash A(\overline{n})$$

för något $\overline{n}$, där endast x är fri i A.

DP följer mycket väl det informella intuitionistiska sättet att se på disjunktion, och att se på hur matematiken och intuitionen kommer före det formella. Det vill säga, det stämmer överens med att man inom intuitionismen menar att vi vet att $A \vee B$ om och endast om vi antingen vet att A eller vet att B.

Man skulle nu kunna fråga sig om detta faktiskt alltid stämmer, eller om det går att konstruera ett exempel där $A \vee B$ går att deducera, utan att det går att bestämma huruvida det är A eller B som är formellt bevisbar.

Ungefär detsamma gäller för numerisk existens. Det går att tänka sig en situation där vi vet att $\exists x.A(x)$ gäller men där vi inte har bevisat $A(\overline{n})$ för något specifikt n.[11]

Till exempel har vi även termexistensegenskapen (TE) [1]:

$$\exists x.A(x) \rightarrow (A(t) \wedge t\downarrow)$$

[11] För exempel på en intuitionistisk teori **T** där **NE** inte håller har vi enligt Troelstra [11, 1.11.2] teorin $\mathbf{T} = \mathbf{HA} \cup \exists x.A(x)$ där $A(x)$ är:

$$\mathit{Proof}\,(x, \#(1=0)) \vee \forall y \neg \mathit{Proof}\,(y, \#(1=0))$$

där, för alla påståenden P: $\mathit{Proof}\,(y, \#P)$ om och endast om $\mathbf{HA} \vdash P$.

Då **HA** är konsistent är $\forall y \neg \mathit{Proof}\,(y, \#(1=0))$ intuitionistiskt sant i **HA**, och alltså även $\exists x.A(x)$ sann. Men om $\forall y \neg \mathit{Proof}\,(y, \#(1=0))$ kan vi härleda $\mathit{Proof}\,(\overline{n}, \#(1=0))$ vilket $\overline{n}$ som helst. Det vill säga 1): $\vdash A(\overline{n}) \leftrightarrow \forall y.\neg \mathit{Proof}\,(y, \#(1=0))$ för något $\overline{n}$.

Enligt defenintionen av $A(x)$ har vi även 2):
$\vdash \exists x.A(x) \leftrightarrow \big(\exists y.\mathit{Proof}\,(x, \#(1=0)) \vee \forall y \neg \mathit{Proof}\,(y, \#(1=0))\big)$
Antag nu att $\vdash \exists x.A(x) \leftrightarrow A(\overline{n})$, då har vi enligt 1) och 2) att 3):
$\vdash \big(\exists y.\mathit{Proof}\,(x, \#(1=0)) \vee \forall y \neg \mathit{Proof}\,(y, \#(1=0))\big) \rightarrow \forall y \neg \mathit{Proof}\,(y, \#(1=0)$
Och därför att $\vdash \exists y.\mathit{Proof}\,(x, \#(1=0)) \rightarrow \forall y \neg \mathit{Proof}\,(y, \#(1=0))$ vilker ger:
$\vdash \forall y \neg \mathit{Proof}\,(y, \#(1=0))$. Men enligt Gödels andra ofullständighetssats kan en axiomatiserbar och konsisten teori (vilket $\mathbf{HA} \cup \exists x.A(x)$ är), inte visa sin egen konsistens.

Den numeriska existensegenskapen gäller alltså inte i detta fall, trots att teorin **T** är intuitionistisk.

där t är en term och $t\downarrow$ utläses att 't är definierad'. $\exists x.A(x)$ måste inte vara sluten i detta fall, men t måste ha sina fria variabler bland de fria variablerna i $\exists x A(x)$.

För en viss teori **T** kan det hända att termexistensegenskapen inte håller, helt enkelt eftersom det finns fler objekt än det finns termer. Däremot har vi att termexistensegenskapen kan hålla utan att den numeriska existensegenskapen håller eftersom vi kanske inte kan hitta ett specifikt tal m sådant att en viss term $t = \overline{m}$.

Det visar sig disjunktionsegenskapen ofta gäller samtidigt som den numeriska existensegenskapen (**NE**) för Heytingaritmetiken samt eventuella utvidgningar av den, vilket bland annat beskrivs av Anne Sjerp Troelstra [10].

Sedan ska vi visa att disjunktionsegenskapen faktiskt medför den numeriska existensegenskapen för flersortiga[12] (aritmetiska) extensioner av Heytingaritmetiken, vilket visas av Harvey Friedman [8]. Men för ett bevis för flersortiga aritmetiska extensioner behövs först några definitioner.

6.2 Primitivt rekursiva funktioner

En primitivt rekursiv funktion är en funktion $f : \mathbb{N}^k \to \mathbb{N}$ som kan beräknas med hjälp av funktionerna 0, efterföljarfunktionen $'$, samt:
$U_1^n(x_1, x_2, ..., x_i, ..., x_n) = x_i$ det vill säga, en funktion som väljer det i:te elementet bland en rad element. Klassen av primitivt rekursiva funktioner ska även vara sluten under substitution och rekursiva operationer, vilket kräver komposition.[13]

Sluten under komposition innebär att vi, för primitivt rekursiva funktionen $f(x_1, ..., x_n)$ och primitivt rekursiva funktionerna
$g_1(y_1, ..., y_m), ..., g_n(y_1, ..., y_m)$ får en ny primitivt rekursiv funktion:

$$h(y_1, ..., y_m) = f(g_1(y_1, .., y_m), ..., g_n(y_1, ..., y_m))$$

Man kan även få en ny funktion f med hjälp av primitiv rekursion, så att:

$$f(x, 0) = k(x)$$

$$f(x, y+1) = g(x, y+1, f(x, y))$$

för en n-ställig funktion f, en godtycklig n-1-ställig funktion k och en godtycklig n+1-ställig funktion g.

[12] Att vara ensortig innebär att man endast har en domän, detta kan till exempel vara de naturliga talen eller de reella talen. Att en teori är flersortig innebär att den har flera olika domäner. Ett exempel på det är vektorrummet, där den ena domänen består av vektorer, och den andra skalärer, t.ex. de reella talen.

[13] För bevis för att dessa går att beskriva i en teori **T** som är en extension till Peanoaritmetiken, se [2].

Även relationer (och mängder), $P(x)$, kan vara primitivt rekursiva. Det gäller när det finns en primitivt rekursiv funktion $c_P(x)$ som, för varje x, kan tala om ifall $P(x)$ gäller eller inte, (eller om x tillhör mängden eller ej). Det vill säga:

$$c_P(x) = \begin{cases} 1 & \text{om } P(x) \text{ gäller} \\ 0 & \text{om } P(x) \text{ inte gäller} \end{cases}$$

Vi har även *rekursivt uppräkneliga* mängder, dessa har inte kravet att det ska gå att bestämma vilka objekt som inte ingår i mängden. Vi kan endast få reda på ifall ett objekt, efter ändlig tid, tillhör mängden. Det karaktäristiska funktionen blir då istället:

$$c_P(x) = \begin{cases} 1 & \text{om } x \text{ tillhör mängden} \\ \textit{odefinierad} & \text{om } x \text{ inte tillhör mängden} \end{cases}$$

6.3 Gödelnumrering

Vi kommer behöva Gödelnumrering. Gödelnumrering innebär att vi sätter ett unikt nummer för varje konnektiv, kvantifikator, variabel, predikat och formel i **T**. Vi kan då till exempel få ett schema som ser ut på föjlande sätt:

Tabell 1 *exempel på schema till Gödelnumrering*

symbol	(	)	,	$\neg$	$\vee$	$\wedge$	$\rightarrow$	$\exists$	$\forall$	$=$	v_i	A_i^n	f_i^n
kod	1	3	5	7	9	11	13	17	19	23	$2 \cdot 5^i$	$2^2 \cdot 3^n \cdot 5^i$	$2^3 \cdot 3^n \cdot 5^i$

Predikatet $<$ som då till exempel är A_0^2 får då kodnummret $2^2 \cdot 3^2 \cdot 5^0 = 36$, och $0 = f_0^0$ får på samma sätt kodnummret $2^3 {\cdot} 3^0 {\cdot} 5^0 = 8$, efterföljarfunktionen $' = f_0^1$ får då kodnummer 24 och $+ = f_0^2$ får kodnummer 72. Hur vet man vilken funktion som tillhör vilket f_i^n? Det bestämmer man själv, men man ska se till att vara konsekvent, har man en gång satt $<$ som A_0^2 är den alltid det.

Vi använder alltså en injektiv funktion # för att tolka om påståenden, formler etc. en teori **T** till kod-tal. Mängden av dessa kod-tal kallas Gödeltal och noteras med ω. Mängden ω innehåller alltså naturliga tal men poängterar att de står för påståenden etc. i **T**. Exakt vilka tal som ingår beror på vilken funktion # man väljer, och att den är injektiv syns, i just denna version, genom att inga primtal större än 23 förekommer i mängden.

7 Bevis i HA

7.1 Disjunktions- och existensegenskaper gäller samtidigt

Visa vill nu visa att **HA**, har **DP** och **NE**, med hjälp av Anne Sjerp Troelstras bevis[10].

Vi ska visa att **DP** och **NE** gäller samtidigt för **HA** samt för ensortiga extensioner av **HA**. Vi börjar med att introducera en *Aczel-slashrelation* för att lättare kunna avgöra vilka härledningar som får göras i **HA**.

Ur **HA** kan man härleda den intuitionistiska definitionen av disjunktion, vilket kräver att det måste finnas existens:

$$\mathbf{HA} \vdash A \vee B \leftrightarrow \exists x.((x = 0 \to A) \wedge (x \neq 0 \to B))$$

Aczel-slashrelationens (härefter förkortad *slashrelationen*) intuitionistiska uppbyggnad försäkrar oss om att vi inte kommer kunna härleda något som inte är intuitionitiskt. Relationen uttrycker de intuitionistiska förväntningarna på konnektionerna och kvantifikationerna.

Definition: **slash-relation**.
Γ är en mängd påståenden i **HA**, $\vdash$ är härledningsbarhet i **HA** och $|$ är *slashrelationen.* Att A är prim innebär att A endast består av ekvationer och := betyder att vänsterled är definierat av högerled.

För slutna påståenden A definierar vi då:

(i)	$\Gamma \| A$	$:= \Gamma \vdash A$ om A är prim eller $A \equiv \perp$
(ii)	$\Gamma \| A \wedge B$	$:= \Gamma \| A$ och $\Gamma \| B$
(iii)	$\Gamma \| A \vee B$	$:= \Gamma \| A$ eller $\Gamma \| B$
(iv)	$\Gamma \| A \to B$	$:= \Gamma \| A \Rightarrow \Gamma \| B$ och $\Gamma \vdash A \to B$
(v)	$\Gamma \| \forall x.A(x)$	$:= \Gamma \vdash \forall x.A(x)$ och $\Gamma \| A(\overline{n})$ för alla namn på tal $\overline{n}$
(vi)	$\Gamma \| \exists x.A(x)$	$:= \Gamma \| A(\overline{n})$ för något $\overline{n}$

Lemma 1 $\Gamma|A \Rightarrow \Gamma \vdash A$.

Beviset fås med hjälp av induktion på (längden av) formeln A. Då A är prim eller $\perp$ är det enkelt att se att detta gäller. När konnektiv läggs till kan man reducera det till att endast vara över A och B vilka vi redan vet att detta fungerar på.

Fall $A \vee B$ Vi vill visa att $\Gamma|A \vee B$ ger $\Gamma \vdash A \vee B$. Då vi har att $\Gamma|A \vee B$, har vi enligt (iii) att antingen 1) $\Gamma|A$ eller att 2) $\Gamma|B$. I fall 1) har vi enligt (i) at $\Gamma \vdash A$, och i fall 2) har vi enligt (i) att $\Gamma \vdash B$. I båda fallen kan vi använda oss av $\vee$-introduktion för att få $\Gamma \vdash A \vee B$.

Fall $\exists x.A(x)$ Vi vill visa att $\Gamma|\exists x.A(x)$ medför $\Gamma \vdash \exists x.A(x)$. Då vi har att $\Gamma|\exists x.A(x)$ har vi enligt (vi) att $\Gamma|A(\overline{n})$ för något $\overline{n}$. Men då har vi enligt (i) $\Gamma \vdash A(\overline{n})$ för något $\overline{n}$, men då har vi enligt $\exists$-introduktion att $\Gamma \vdash \exists x.A(x)$.

Vi vill dock även försäkra oss om att då det finns en sluten term t så att $\Gamma|A(t)$, kommer även finnas ett tal så att $A(\overline{t_1}, \cdots, \overline{t_n})$. Detta får vi med hjälp av nästa lemma.

Lemma 2 Låt $t_1, \cdots, t_n$ vara slutna termer, och $\overline{t_1}, \cdots, \overline{t_n}$ de tal som fås genom att man utvecklar dem. Då har vi för slutna $A(t_1, \cdots, t_n)$:

$$\Gamma | A(t_1, \cdots, t_n) \Leftrightarrow \Gamma | A(\overline{t_1}, \cdots, \overline{t_n}).$$

Bevis. Steg 1). Vi måste först visa att vi (ur **HA**) kan härleda att en sluten term $t = \bar{t}$. För att visa detta, antag att alla primitivt rekursiva funktions-symboler φ_n är (oändligt) numrerbara genom att $\varphi_0, \varphi_1, \varphi_2, \cdots$ där varje φ_n endast är definierad med hjälp av de φ_i för $i < n$. Med hjälp av induktion över n ska vi först visa att 1):

$$\vdash \varphi_n(\overline{m_1}, \cdots, \overline{m_p}) = \overline{\varphi_n(m_1, \cdots, m_p)}$$

är bevisbar för alla $m_1, \cdots, m_p$.

Vi har först att $\varphi_0(\overline{m_1}, \cdots, \overline{m_p})$, inte är definierad med hjälp av några andra funktioner. Det vill säga, den består endast av basfunktionerna: 0, '-efterföljarfunktionen eller $U^i_n(x_1, \cdots, x_n) = x_i$ som väljer ut det i:e elementet.

Eftersom dessa är primitivt rekursiva funktioner, går de att räkna ut i **HA**, så oavsett vilken av dem φ_0 är, kan vi räkna ut värdet för $\varphi_0(\overline{m_1}, \cdots, \bar{m})$ till $\overline{\varphi_0(m_1, \cdots, m_p)}$. Vi har därmed att:

$$\vdash \varphi_0(\overline{m_1}, \cdots, \overline{m_p}) = \overline{\varphi_0(m_1, \cdots, m_p)}$$

Antag nu att 1) gäller för φ_r för $r \leq k-1$, vi har då φ_k endast är definierad med hjälp av φ_i för $i < k$ att:

$$\varphi_k(\overline{m_{1_k}}, \cdots, \varphi_{r_1}(\overline{m_{1_r}}, \cdots, \overline{m_{1_r}}), \cdots)$$

för någon kombination av $\overline{m_{i_k}}$ och $\varphi_{r_1}(\overline{m_{1_r}}, \cdots, \overline{m_{1_r}})$ i φ_k.

Enligt antagande kan vi beräkna $\varphi_{r_1}(\overline{m_{1_r}}, \cdots, \overline{m_{1_r}})$ till $\overline{\varphi_{r_1}(m_{1_r}, \cdots, m_{1_r})}$. Nu kan vi även beräkna φ_k, och vi har att 1) gäller. Vi kan därför beräkna varje slutna term t och få $\bar{t}$.

Steg 2). Vi har nu, enligt steg 1) samt Peanos axiom om ekvivalens-relationen för tal att 2):

$$\Gamma \vdash A(t_1, \cdots, t_n) \Leftrightarrow \Gamma \vdash A(\overline{t_1}, \cdots, \overline{t_n})$$

Steg 3). Med hjälp av induktion över A kan man nu visa lemmat. Fallet då A är prim visas med hjälp av steg 2) tillsammans med (i).

Fallet $A \equiv B \vee C$
Sätt B' och C' för de B och C där termerna $t_1, \cdots, t_n$ är utbytta till $\overline{t_1}, \cdots, \overline{t_n}$. Vi får då att:

$$\Gamma | B \vee C \rightarrow (\Gamma | B \text{ eller } \Gamma | C)$$

Vi kan då, enligt steg 3) byta ut termerna $t_1, \cdots, t_n$ till $\overline{t_1}, \cdots, \overline{t_n}$ i B och C och vi får då, med hjälp av (iii) att:

$$\Gamma | B \vee C \Leftrightarrow (\Gamma | B\text{' eller } \Gamma | C\text{'}) \Leftrightarrow \Gamma | B\text{'} \vee C\text{'}$$

Fallet $A \equiv B \to C$
Sätt B' och C' för de B och C där termerna $t_1, \cdots, t_n$ är utbytta till $\overline{t_1}, \cdots, \overline{t_n}$. Vi får då enligt (iv) att:

$$\Gamma | B \to C \Leftrightarrow (\Gamma | B \Rightarrow \Gamma | C) \text{ och } \Gamma \vdash B \to C$$

Vi kan nu byta ut termerna $t_1, \cdots, t_n$ till $\overline{t_1}, \cdots, \overline{t_n}$ i B och C enligt steg 3) och steg 2). Vi får då, enligt (iv) att:

$$\Gamma | B \to C \Leftrightarrow (\Gamma | B\text{'} \Rightarrow \Gamma | C\text{'}) \text{ och } \Gamma \vdash B\text{'} \to C\text{'} \Leftrightarrow \Gamma | B\text{'} \to C\text{'}$$

□

Detta visar att man kan gå åt ena hållet, för att kunna bevisa att **HA** har disjunktionsegenskapen såväl som existensegenskapen måste vi även kunna gå åt andra hållet.

Sats 1 Om $\Gamma | A \ \forall A \in \Gamma$ har vi att

$$\Gamma \vdash B \Rightarrow \Gamma | B$$

Även detta lemma visas med hjälp av induktion över formler, och jag nöjer mig med att visa några exempel.

Fall A Detta följer per definition av (i).

Fall $A \wedge B$ **introduktion** Vi kan beskriva introduktionen genom $\Gamma | A \to (B \to A \wedge B)$. Vi måste nu visa att 1) $\Gamma \vdash A \to (B \to A \wedge B)$ och att 2) $\Gamma | A \Rightarrow \Gamma | B \to A \wedge B$. Vi har 1) gäller då vi kan härleda detta i **HA**. För att få 2), anta att vi har $\Gamma | A$, och anta sedan att $\Gamma | B$, vi har då att $\Gamma | A \wedge B$, vilket enligt **lemma 1** ger att vi har $\Gamma \vdash A \wedge B$. Vi får nu enligt (iv) att $\Gamma | B \to A \wedge B$, och därmed har vi visat $\Gamma | A \to (B \to A \wedge B)$.

Fall $A \vee B$ **introduktion** Detta visas enkelt då vi har att $\Gamma | A \Rightarrow \Gamma | A \vee B$ gäller per definition, samt $\Gamma \vdash A \to (A \vee B)$ på grund av introduktionsregeln. Vilket ger att $\Gamma | A \to (A \vee B)$ enligt (iv).

Vi kan nu undersöka ifall olika påståenden är intuitionistiskt bevisbara genom att se ifall de är härledbara ur Heyting-aritmetiken.

Exempel: $\mathbf{HA} \vdash \forall x.(x = 0 \vee \exists y.x = (y)')$

Vi vill börja med att visa att $\mathbf{HA} \vdash \overline{n} = 0 \vee \exists y.\overline{n} = (y)'$ gäller för alla $\overline{n}$, så att vi kan använda (v).

För att kunna använda (iii) behöver vi visa att: $|\overline{n} = 0$ eller att $|\exists y.\overline{n} = (y)'$. Vi får två fall:

Fall 1): $|\overline{n} = 0$. Då den är atomär har vi enligt (i) att $\mathbf{HA} \vdash \overline{n} = 0$ i det fall då $\overline{n} = 0$ är sann, annars är det falskt, och för att exemplet då ska hålla måste fall 2 hålla i dessa fall.

Fall 2): $|\exists y.\overline{n} = (y)'$. Detta gäller, enligt (vi) då $|\overline{n} = (\overline{m})'$ för något $\overline{m}$. Detta utesluter dock att $\overline{n} = (\overline{m})' = 0$ enligt **Peanos** sjunde axiom, men då har vi redan sett att fall 1 gäller. Vad gäller alla andra $\overline{n}$ har vi enligt **Peanos** andra axiom att, då $m \in \mathbb{N}$ att $n \in \mathbb{N}$ och därmed att fall 2, och alltså även $\mathbf{HA} \vdash \forall x.(x = 0 \vee \exists y.x = (y)')$ gäller.

Lemma 3

$$(A \vee B) \leftrightarrow \exists x\big((x = 0 \to A) \vee (x \neq 0 \to B)\big)$$

är bevisbar i **HA**.

Bevis. Vi visar först $\to$. På grund av reglerna för $\vee$-elimination måste vi alltså visa att A medför 1) $\exists x\big((x = 0 \to A) \vee (x \neq 0 \to B)\big)$ samt att B medför 1). För att 1) ska gälla, behöver vi visa att antingen 2a) $\overline{n} = 0 \to A$ eller 2b) $\overline{n} \neq 0 \to B$ för något n, enligt (vi) och (iii).

Antag att A gäller. Vi vill då visa att $\overline{n} = 0 \to A$ gäller, men vi har att $A \to (P \to A)$ för något påstående P, alltså även för $P = (\overline{n} = 0)$. Det vill säga, A medför att 1) gäller.

Antag att B gäller. Vi vill då visa att 2b) gäller, vilket vi får genom samma resonemang. Alltså medför B att 1) gäller.

Nu vill vi visa att $\leftarrow$ gäller. Vi har enligt (iv) och (vi) sedan att $(\overline{n} = 0 \to A) \vee (\overline{n} \neq 0 \to B)$ ska medföra $A \vee B$. Vi ser att då $\overline{n} = 0$ gäller, får vi att A gäller. I annat fall har vi att $\overline{n} = ((\cdots(0)')'\cdots)$ för något antal efterföljarfunktioner, vilket enligt Peanos 7e axiom medför att $\overline{n} \neq 0$, vilket ger att B gäller. I båda fallen får vi $A \vee B$ med hjälp av $\vee$-introduktion. $\square$

Sats 2: HA har **DP** och **NE**.

Vi kan definiera disjunktionsegenskapen i HA med hjälp av:

$$(A \vee B) \leftrightarrow \exists x\big((x = 0 \to A) \vee (x \neq 0 \to B)\big)$$

I **lemma 3** såg vi att detta kunde härledas ur **HA**. Vi behöver nu endast visa att disjunktionsegenskapen eller existensegenskapen gäller. För att visa disjunktionsegenskapen antar vi att **HA** $\vdash (A \vee B)$. Då har vi att $|(A \vee B)$ vilket gäller antingen då $|A$ eller $|B$, det vill säga antingen $\vdash A$ eller $\vdash B$. För den numeriska existensegenskapen antar vi att **HA** $\vdash \exists x.A(x)$ vilket ger att $|\exists x.A(x)$. Detta gäller då $|A(\overline{n})$ för något $\overline{n}$, vilket ger att **HA** $\vdash A(\overline{n})$ för något $\overline{n}$.

Sats 3: En teori **T**=**HA**+Γ, då $\Gamma|C$ för alla $C \in \Gamma$, har **DP** och **NE**.

Detta har vi eftersom teorin **T** då uppfyller kraven för **sats 1**, vilket leder till att vi kan definiera disjunktion med hjälp av existens på samma sätt som när vi endast befinner oss i **HA**. Beviset är alltså som för i förra satsen.

8 Generellt bevis

Det är ingen tillfällighet att **HA** innehar både disjunktionsegenskapen och den numeriska existensegenskapen.

Låt ensortig $\mathbf{HA}_0$ vara **HA** utan kvantifikatorer. En teori **T** formulerad i flersortig intuitionistisk predikatlogik med identitet, är en extension av $\mathbf{HA}_0$ om dess axiom inkluderar alla axiomen i $\mathbf{HA}_0$. Denna extension **T** kommer att ha disjunktionsegenskapen, om och endast om, för varje sluten konsekvens $A \vee B$, A är en konsekvens av **T** eller B är en konsekvens av **T**.

Friedman [8] har lyckats visa att disjunktionsegenskapen finns en teori $\mathbf{T} \supseteq \mathbf{HA}_0$ alltid leder till numerisk existens oavsett hur **T** ser ut, så länge den är rekursivt uppräknelig och en extension till aritmetiken (det vill säga en flersortig extension av $\mathbf{HA}_0$ utan identitet).

Däremot sägs ingenting om andra existensegenskaper. Man kan tänka sig en teori **T** där disjunktionsegenskapen gäller, men där till exempel term existens egenskapen inte håller. Antag att vi har en teori $\{\exists x.A(x)\}$ där A är atomär, det vill säga utan konnektiv, i ensortig intuitionistisk predikatlogik. Här gäller disjunktionsegenskapen, men det är inte säkert att det finns tillräckligt många termer för att nämna alla t så att $A(t)$ gäller.

Vi kommer börja med att anta en teori **T** som innehåller $\mathbf{HA}_0$, och vill sedan, utifrån (i ett metaperspektiv), studera hur de olika påståenden i **T** påverkar varandra. Detta gör vi enklast genom att först införa en (Gödel-)kodning som ger alla olika formler i **T** ett unikt nummer.

När vi väl har dessa nummer kan vi skapa funktioner som kan visa hur de olika koderna (och därmed påståenden, formler etc i **T**) sitter ihop. Vi kan sedan utifrån detta konstruera ett visst påstående $A(x)$ och med den visa att ett påstående $\exists x.P(x)$ kan visa sin egen existensegenskap.

Lemma 1 Det finns en injektiv funktion $\# : \mathbf{T} \rightarrow \omega$ dvs, från mängden av formler i den rekursivt uppräkneliga teorin **T** till de naturliga (kod)talen ω, det vill säga helt enkelt ett specifikt sätt att koda alla talen. Samt primitivt rekursiva funktioner *neg*, *prf* och *sub* från de ω till ω sådana att:

1) för alla formler A gäller att: $neg(\#(A)) = \#(\neg A)$.
2) för alla formler B gäller att:

$$\mathbf{T} \vdash B \text{ om och endast om } \exists n.prf(n, \#(B)) = 0$$

3) för alla formler $C = C(x)$ gäller att: $sub(\#(C)) = \#(C(\overline{\#(C)}))$

Det som händer är att vi sätter namn på alla de olika påståendena i **T** och fixerar dem på så sätt att det t.ex. finns en funktion (*neg*) över det tal till påståendet A och som motsvarar koden till påståendet $\neg A$[14].

För 2) utläses $\mathbf{T} \vdash B$ som 'B är härledbar ur **T**'. Vi får då att n är koden för beviset av B.

När det gäller *sub* gör man en diagonalisering, det vill säga (av alla tal) väljer vi att substituera med det tal som själva formeln har.

Lemma 2 För varje symbol $F : \omega^k \to \omega$ till en k-ställig primitivt rekursiv funktion som kan beskrivas i **T** finns en primitivt rekursiv funktion $|F| : \mathbb{N}^k \to \mathbb{N}$ sådan att $|F|(n) = m \to T \vdash F(\overline{n}) = \overline{m}$.

För varje primitivt rekursiv funktion $f : \omega^k \to \omega$ finns det en primitivt rekursiv funktionssymbol F så att $f = |F|$.
Det vill säga, varje primitivt rekursiva funktion f över kod-tal beskriver en primitivt rekursiv funktion $|F|$ i **T**. Varje primitivt rekursiv funktion $|F|$ i **T** kommer även ha en representation F över kod-talen.

Exempel (för addition) Antag att vi vill representera **addition**, en funktion i **T**, som en funktion härledbar ur **T**. Det vill säga att vi för tvåställiga $|F|(x, y) = z$ vill skapa $F : \omega^2 \to \omega$ så att $F(\overline{x}, \overline{y}) = \overline{z}$.

Vi har till exempel $|F|(3, 2) = 3 + 2 = 5$, samt Gödelnumreringen av invärden och utvärden:

Tabell 2 *Gödelnumrering för tal*

symbol	$\|F\|^0_2$	$\|F\|^0_3$	$\|F\|^0_5$
kod	$2^3 \cdot 3^0 \cdot 5^2 = 200$	$2^3 \cdot 3^0 \cdot 5^3 = 1000$	$2^3 \cdot 3^0 \cdot 5^5 = 25000$

Vi vill nu att $|F|^2_0(3, 2) = 5$ ska koden med 3 och 2 som invärden i F innebära attska ge att $F^2_0(200, 1000) = 25000$.

[14] $\neg A$ i sig är en speciell kod byggd på en sekvens: $< \neg, A >$, även här kan man själv välja hur man vill bygga upp koden för sin sekvens, bara man är konsekvent. Ett exempel är att ge sekvensen $x_0, x_1, \cdots, x_{n-1}$ koden $2^n \cdot 3^{x_0} \cdot 5^{x_1} \cdots \pi^{x_{n-1}}$ där π^i är ett primtal. Vi får då att $< \neg, A >$, med $\neg = 7$ och t.ex. $A = 36$ ger koden $2^2 \cdot 3^7 \cdot 5^{36}$. I detta fall är alltså funktionen $neg(\#(A))$ förslagsvis $2^2 \cdot 3^7 \cdot \#(A)$ som givetvis är primitivt rekursiv.

Mer allmänt kan $F : \omega^2 \to \omega$ då fås genom att vi hittar de x_1 och y_1 som 5 är upphöjt till i de två invärden $\overline{x}$ och $\overline{y}$. Vi får sedan $x_1 + y_1 = z_1$ skapar den nya koden $z = 2^3 \cdot 3^0 \cdot 5^{z_1}$. På grund av Aritmetikens Fundamentalsats kan vi få det unika x_1 sådant att talet x får kodtalet $x = 2^3 \cdot 3^0 \cdot 5^{x_1}$. På så sätt kan vi även vara säkra på att $\overline{z}$ är kodtalet för något tal i **T**.

Man kan tänka sig att vi i detta fall får att $f : \omega^2 \to \omega$ sådan att $f(\overline{a}, \overline{b}) = \overline{c}$, där $\overline{a} = x$, $\overline{b} = y$ och $\overline{c} = z$. Men detta är tyvärr inte fallet eftersom funktionen # är injektiv. Då vi till exempel sätter x och y som kod-talen för 0, det vill säga $x = y = 8$ får vi att $f(8, 8) = 16 = 2^4$, men 2^4 ligger inte i ω och är alltså inget kodtal. Det vill säga, det finns inget $\overline{c}$ så att $\overline{c} = 16$, och funktionen är odefinierad där (och alltså inte primitivt rekursiv).

Vi fixerar nu $Neg : \omega^k \to \omega$ sådan att $|Neg| = neg$, för $|Neg| : \mathbb{N}^k \to \mathbb{N}$ och $neg : \omega^k \to \omega$, och sätter Prf så att $|Prf| = prf$ och Sub så att $|Sub| = sub$.

Vi har enligt lemma 1: $neg(\#(A)) = \#(\neg(A))$, vilket, enligt lemma 2 skulle ge $|Neg|(x) = y$, där $x = \#(A)$ och $y = \#(\neg A)$. Vi får sedan att $Neg(\overline{x}) = \overline{y}$. Som man kan se har Neg inte lika mycket med negation att göra som *neg*, utan kommer endast vara en funktion.

Lemma 3 Om A är en formel i **T** finns det ett tal k sådant att:
$\#(A(Sub(\overline{k})) = sub(k)$.

Bevis. Antag $k = \#(A(Sub(x)))$, då får vi att:
$sub(k) = sub(\#(A(\overline{Sub(x)})))$, vilket enligt *lemma 1,3* ger:
$sub(k) = \#(A(Sub(\overline{\#A(Sub(x))})))$ vilket enligt antagande blir:
$sub(k) = \#(A(Sub(\overline{k}))$. □

Vi inför nu den naturliga tvåställiga funktionen $+$[15] sådan att $|+| =$ *addition*. Vi kan ha *addition* eftersom vi är i $\mathbf{HA}_0$, i vilket vi kan skapa denna funktion. Vi kan nu skapa ordning bland de tal som representerar formler i **T** med hjälp av relationerna $\leq$ och $<$ som vi definierar genom:
$x \leq y = \exists z.(x + z = y)$ och $x < y = (x \leq y \wedge (\neg x = y))$.
Vi låter $P(y)$ vara en formel (över en annan formel i **T**) sådan att den inte har några andra fria variabler än y. Låt $A(x)$ vara formeln:

$$\exists y.(Prf(y, Neg(x)) = 0 \vee P(y)) \wedge \forall z.(Prf(z, x) = 0 \to y \leq z)$$

Den första delen säger att antingen kan man härleda $\neg x$ ur **T** vilket medför att det finns ett bevis för $neg(x)$ med kodtalet y, annars har vi att $P(y)$ gäller. Den andra delen säger att alla eventuella bevis av formeln x måste ha en kod z som, som minst är y, eftersom $y \leq z$.

[15] Denna har vi eftersom **T** är en extension av aritmetiken

Vi kan nu till nästa lemma (och i fortsättningen) välja k sådant att $\#(A(Sub(\overline{k})) = sub(k)$ enligt **lemma 3**.

Lemma 4 Om $\mathbf{T}\vdash A(Sub(\overline{k}))$ har vi att $\mathbf{T}\vdash P(\bar{n})$ för något n.

Bevis. Antag att $\mathbf{T}\vdash A(Sub(\overline{k}))$, då har vi enligt **lemma 1** och **lemma 3** att $prf(n, sub(k)) = 0$ det vill säga att det finns ett påstående eller en funktion P i $\mathbf{T}$, med kod-talet $\overline{p} = k$ sådant att vi kan härleda $sub(k)$ ur $\mathbf{T}$. Det vill säga, ur $\mathbf{T}$ kan vi härleda $P(k)$, där k ersatt en fri variabel i P, i det fall en sådan existerar.

Vi får enligt **lemma 2** att (1):

$$\mathbf{T} \vdash Prf(\overline{n}, Sub(\overline{k})) = 0$$

Enligt definitionen av A har vi (2):

$$\mathbf{T} \vdash \exists y.((Prf(y, Neg(Sub(\overline{k}))) = 0 \vee P(y))\wedge \\ (Prf(\overline{n}, Sub(\overline{k})) = 0 \rightarrow y \leq \overline{n}))$$

På grund av (1) och (2) får vi då (3):

$$\mathbf{T} \vdash \exists y.((Prf(y, Neg(Sub(\overline{k}))) = 0 \vee P(y)) \wedge y \leq \overline{n}))$$

Antag att $\exists y \leq n.prf(y, neg(sub(k)) = 0$. Vi får då enligt **lemma 1.1** och **lemma 3** att $\exists y \leq n.prf(y, \#(\neg A(Sub(\overline{k})))) = 0$, vilket enligt **lemma 1,2** ger att $\mathbf{T} \vdash \neg A$ vilket medför att $\mathbf{T}$ är inkonsistent. Vi får då härleda vad som helst, alltså även $P(\overline{n})$ för något n.

Om däremot $\neg(\exists y \leq n.prf(y, neg(sub(k)) = 0)$ får vi enligt (ett flertal användningar av) **lemma 2** att:

$$\mathbf{T} \vdash \neg(\exists y \leq \overline{n}.Prf(y, Neg(Sub(\overline{k}))) = 0)$$

eftersom vi, enligt Gödelnumrering för tal har att $y \leq n \rightarrow \bar{y} \leq \bar{n}$. Men vi har även att, för alla tal $y \leq \bar{n}$ sådana att y inte är kod för någon formel, speciellt att y inte är kodtalet (av beviset) för $neg(sub(k))$. Notera därför att samma sak inte gäller för $\exists y \leq n.prf(y, neg(sub(k)) = 0$.

Vi får nu enligt (3) att $\mathbf{T}\vdash (\exists y.y \leq \overline{n} \wedge P(y))$ vilket innebär:

$$\mathbf{T} \vdash P(1) \vee P(2) \vee \cdots P(i) \vee \cdots P(n)$$

Eftersom disjunktionsegenskapen gäller för $\mathbf{T}$, måste åtminstone ett av alternativen vara sanna. Då vet vi att det finns åtminstone ett $i \leq n$ sådan att $\mathbf{T}\vdash P(i)$ och alltså något n sådant att $\mathbf{T}\vdash P(\overline{n})$. $\square$

Lemma 5 Om $\mathbf{T}\vdash \neg A(Sub(\overline{k}))$, är $\mathbf{T}$ inkonsistent.

Bevis. Antag att $\mathbf{T}\vdash \neg A(Sub(\overline{k}))$, vilket enligt **lemma 3** innebär att det finns ett kodnummer n så att $prf(n, neg(sub(k))) = 0$ gäller, vilket, enligt **lemma 2** medför att $\mathbf{T} \vdash Prf(\overline{n}, Neg(Sub(\overline{k}))) = 0$.

Detta är första delen av definitionen av $A(Sub(\overline{k}))$, som vi får från $A(x)$ som vi har definierat tidigare, det vill säga $A(Sub(\overline{k}))$ är:

$$\begin{aligned}&\exists y.((Prf(y, Neg(Sub(\overline{k}))) = 0 \vee P(y))\\ &\qquad\qquad\qquad \wedge \forall z.(Prf(z, Sub(\overline{k})) = 0 \rightarrow y \leq z))\end{aligned}$$

$\neg A(Sub(\overline{k}))$ kommer nu innebära:

$$\begin{aligned}&\neg(\exists y.((Prf(y, Neg(Sub(\overline{k}))) = 0 \vee P(y))\\ &\qquad\qquad\qquad \wedge \forall z.(Prf(z, Sub(\overline{k})) = 0 \rightarrow y \leq z)))\end{aligned}$$

Antag nu att:

$$\forall z.((prf(z, sub(k)) = 0) \rightarrow y \leq z)$$

Detta är detsamma som att vi för varje $z < y$, och vi har ett specifikt sådant y, nämligen n, har att $prf(z, sub(k)) = 1$, det vill säga att $prf(0, sub(k)) = 1 \wedge prf(1, sub(k)) = 1 \wedge \cdots \wedge prf(n-1, sub(k)) = 1$.

Vi har nu enligt **lemma 2** att 1):

$$\mathbf{T} \vdash Prf(\bar{0}, Sub(\bar{k})) = 1 \wedge \cdots \wedge \mathbf{T} \vdash Prf(\overline{n-1}, Sub(\bar{k})) = 1$$

vilket, eftersom varje $z < \overline{y}$ som inte nämns i 1), inte är ett kodtal för någon formel, speciellt inte för $Sub(\bar{k})$, ger att:

$$\mathbf{T} \vdash \forall z.(z < y \rightarrow (Prf(z, Sub(\overline{k})) = 1)$$

Och därför att

$$\mathbf{T} \vdash \forall z.(Prf(z, Sub(\overline{k})) = 0 \rightarrow \overline{n} \leq z)$$

Detta är andra delen på definitionen av $A(Sub(\overline{k}))$, och vi får $\mathbf{T} \vdash A(Sub(\overline{k}))$ och $\mathbf{T}$ är därför inkonsistent.

Om vi däremot har motsatsen $\exists z.z < n \wedge (prf(z, sub(k)) = 0)$ har vi enligt **lemma 3** att $\exists z.prf(z, \#A(Sub(\overline{k})) = 0$ och, enligt **lemma 1,2** även här att $\mathbf{T} \vdash A(Sub(\overline{k}))$ och att $\mathbf{T}$ är inkonsistent. $\square$

Lemma 6 $\mathbf{T} \vdash \exists y.P(y) \rightarrow (A(Sub(\overline{k})) \vee \exists z.Prf(z, Sub(\overline{k})) = 0))$. Om P är primitivt rekursiv får vi $\mathbf{T} \vdash \exists y.P(y) \rightarrow (A(Sub(\overline{k})) \vee \neg A(Sub(\overline{k})))$.

Bevis. Vi använder axiomen till **T**, för att vara säkra på att vi inte antar något $p(y)$ som inte går att härleda ur **T**.

Antag att $\exists y.P(y)$ och att $P(y)$. Om vi har att $\forall z.Prf(z, Sub(\overline{k})) = 0) \rightarrow y \leq z$ får vi, enligt definition att $A(Sub(\overline{k}))$. Annars har vi $\exists z.Prf(z, Sub(\overline{k})) = 0)$.

Då P är en primitivt rekursiv formel, har vi en primitivt rekursiv funktion som, för varje x talar om ifall $P(x)$ gäller eller ej. Detsamma gäller för $Prf(y, Neg(Sub(\overline{k}))) = 0) \vee P(y)$, eftersom vi vet att både P och Prf är primitivt rekursiva, och även negation, substitution och disjunktion är det[16]. Vi kan därför välja y sådan att det är det minsta värdet så att $Prf(y, Neg(Sub(\overline{k}))) = 0) \vee P(y)$ gäller. Vi får då att:

$$\exists y.Prf(y, Neg(Sub(\overline{k}))) = 0) \vee P(y) \wedge \\ \forall z.((Prf(z, Neg(Sub(\overline{k}))) = 0) \vee P(z)) \rightarrow y \leq z)$$

På grund av definitionen på $A(Sub(\overline{k}))$ får vi att:

$$A(Sub(\overline{k})) \leftrightarrow \forall z.((Prf(z, Neg(Sub(\overline{k}))) = 0)) \rightarrow y \leq z)$$

Vi får alltså att, då $\forall z.((Prf(z, Neg(Sub(\overline{k}))) = 0)) \rightarrow y \leq z)$ gäller har vi $\mathbf{T} \vdash A(Sub(\bar{k}))$, i annat fall har vi

$$\neg(\forall z.((Prf(z, Neg(Sub(\overline{k}))) = 0)) \rightarrow y \leq z))$$

vilket ger att $\mathbf{T} \vdash \neg A(Sub(k))$. □

Vi har hittills visat att vi har olika primitivt rekursiva funktioner med vars hjälp vi kan beskriva formlers egenskaper i **T**. Sedan har vi skapat $A(Sub(\overline{k}))$, visat att den (alltid) gäller i **T**, och visat att den på grund av att disjunktionsegenskapen gäller, medför existensen av ett påstå-ende P, samt att det finns tal n som uppfyller $P(n)$. Vi har sedan visat att existensen av ett påstående $\exists x.P(x)$ medför att antingen $A(Sub(\overline{k}))$ gäller, eller dess negation gäller, då P är primitivt rekursiv.

Vi kommer nu bevisa att existensegenskapen gäller, det vill säga, har vi ett godtyckligt påstående $\exists y.P(y)$ kommer vi även att kunna hitta ett specifikt y som uppfyller egenskaperna P. Först visar vi det i de fall då $P(y)$ är primitivt rekursiv, det vill säga, då vi för varje y har en funktion som beräknar ifall $P(y)$ gäller för just det y. Sedan visar vi det för alla $\exists y.P(y)$.

Lemma 7 Om $\mathbf{T}\vdash \exists y.P(y)$ och $P(y)$ är primitivt rekursiv, får vi $\mathbf{T}\vdash P(\overline{n})$ för något n.

[16]Disjunktion ger sekvensen $disj(x, y) = \#(\cdot\#x \cdot \# \vee \cdot\#y \cdot \#)$.

Bevis. Antag hypotesen, då får vi enligt **lemma 6** att $A(Sub(\overline{k})) \vee \neg A(Sub(\overline{k}))$ gäller. Om $\neg A(Sub(\overline{k}))$ gäller, får vi enligt **lemma 5** att **T** är inkonsistent, och vi kan härleda vad som helst ur **T**. Till exempel $P(\bar{n})$ för något n, och vi har alltså att $\mathbf{T}\vdash P(\bar{n})$.

Om däremot $A(Sub(\overline{k}))$ gäller, får vi enligt **lemma 4** att $P(n)$ för något n. Det vill säga, även här har vi att $\mathbf{T} \vdash P(\bar{n})$ för något n. □

Lemma 8 Om $\mathbf{T}\vdash \exists y.P(y)$ och $P(y)$, får vi $\mathbf{T}\vdash P(\overline{n})$ för några tal n.

Bevis. Vi har enligt **lemma 6** att $\mathbf{T} \vdash \exists y.P(y) \rightarrow (A(Sub(\overline{k})) \vee \exists z.Prf(z, Sub(\overline{k})) = 0))$. Då disjunktionsegenskapen gäller har vi att antingen 1) $\mathbf{T} \vdash A(Sub(\overline{k}))$ gäller eller att 2) $\mathbf{T} \vdash \exists z.Prf(z, Sub(\overline{k})) = 0$ gäller.
I fall 1) har vi som förut, enligt **lemma 4** att $\mathbf{T} \vdash P(\overline{n})$ för några n.
I fall 2) har vi $\mathbf{T} \vdash Prf(\overline{n}, Sub(\overline{k})) = 0)$ för något tal n, på grund av **lemma 7** eftersom funktionen *Prf* är primitivt rekursiv per definition. Om sedan $prf(n, sub(k)) \neq 0$ så är **T** inkonsistent och vi kan härleda vad som helst, däribland $A(Sub(\overline{k}))$ vilket enligt **lemma 4** ger $P(\overline{n})$. Om istället $prf(n, sub(k)) = 0$ har vi enligt definitionen av $A(x)$ samt samt **lemma 1.2** att $\mathbf{T} \vdash A(Sub(\overline{k}))$. Vi får då enligt **lemma 4** att $P(\overline{n})$. □

Vi har härmed visat att:

Sats 1 Varje rekursivt uppräknelig extension av $\mathbf{HA}_0$ som har disjunktionsegenskapen, kommer även att ha den numeriska existensegenskapen.

Kravet på disjunktion ställdes i **lemma 4** som visade att det faktiskt fanns ett n så att $P(\bar{n})$ gäller.

8.1 Härledning av disjunktionsegenskap medför inkonsistens

Harvey Friedman[8] tog två steg till och visade även att, då vi ur extensionen **T** av $\mathbf{HA}_0$ kan härleda disjunktions egenskapen, samtidigt som **T** har disjunktionsegenskapen, kommer vi kunna härleda inkonsistens ur **T**.

Han skapade först ett påstående A som härleder sig själv, vilket betyder att vilket annat påstående som helst då medför detta påstående A.

lemma 9 [8] Låt **T** vara en rekursivt axiomatiserad extension av **HA**, och låt '$\mathbf{T}\vdash$' vara tillräckligt definierad i **T**. Antag sedan att A är en sats i **T** sådan att $\mathbf{T} \vdash ((\mathbf{T} \vdash A) \rightarrow A)$, då har vi att $\mathbf{T} \vdash A)$.

Detta lemma är baserat på **Löbs sats** [12] gjord för klassisk logik. Satsen i sig använder sig nästan bara av implikation, vilket vi vet fungerar på samma sätt för **PA** som för **HA**. Men den använder sig även av diagonallemmat samt Gödels fullständighetssats, som vi då också måste kontrollera ifall de håller i **HA**, eller om de kan göras om på så sätt att vi kan efterlikna **Löbs sats**.

Sats 2 Låt $\mathbf{T}$ vara en rekursivt uppräknelig extension av aritmetik, och låt $\mathbf{T}\vdash$ vara tillräckligt definierad i $\mathbf{T}$. Om vi, för alla slutna satser A och B har $\mathbf{T}\vdash((\mathbf{T}\vdash(A\vee B))\rightarrow\mathbf{T}\vdash A\vee\mathbf{T}\vdash B)$, då har vi att $\mathbf{T}\vdash(\mathbf{T}\vdash(1=0))$. Dessutom har vi att, om $\mathbf{T}$ har disjunktionsegenskapen, får vi $\mathbf{T}\vdash(1=0)$.

Satsen säger att, om vi kan härleda disjunktionsegenskapen ur $\mathbf{T}$, kan vi ur $\mathbf{T}$ härleda att vi kan härleda falskhet ur $\mathbf{T}$. Om disjunktionsegenskapen ingår i 'lagarna' av $\mathbf{T}$, kan vi härleda falskhet direkt ur $\mathbf{T}$.

Även detta bygger på **Löbs sats**, eller snarare är en följd av den [2][12], och går ut på att, om vi har ett sanningspredikat i $\mathbf{T}$ kan vi härleda falskhet. Vi har att $\mathbf{T}\vdash\neg(\mathit{prf}(y,\#(1=0)))$, men på grund av definitionen av $\neg$ är detta detsamma som att $\mathbf{T}\vdash(\mathit{prf}(y,\#(1=0))\rightarrow(1=0))$.

Bevis. Enligt **sats 1** vet vi att vi kan visa att existensegenskapen gäller för varje sant påstående. Vi har 1):

$$\mathbf{T}\vdash((\mathbf{T}\vdash(\mathbf{T}\vdash(1=0)))\rightarrow \\ \exists x.\mathbf{T}\vdash'\overline{x}\text{ är ett index till beviset att }(1=0)\text{ i }\mathbf{T}')$$

$\mathbf{T}$ ger att (om ($\mathbf{T}$ ger att vi ur $\mathbf{T}$ kunna härleda att påståendet '$1=0$' är sant) så kan vi enligt **sats 1** hitta ett $\overline{x}$ sådan att vi ur $\mathbf{T}$ kan härleda 'ett bevis av (1=0) i $\mathbf{T}$ har index $\overline{x}$').

Vi har även 2) att
$(\mathbf{T}\vdash(\mathbf{T}\vdash(1=0)))\rightarrow\exists x.\mathbf{T}\vdash'\overline{x}$ är ett index till beviset att $(1=0)$ i $\mathbf{T}'$. Om $\mathbf{T}$ härleder att vi kan härleda falskhet ur $\mathbf{T}$, så existerar ett bevis för falskhet som härleds ur $\mathbf{T}$ och som har index x. Detta gäller, eftersom vi inte kan ha någon sats som gäller i $\mathbf{T}$ utan att vi även har ett bevis för den satsen, enligt **lemma 1**. Vi har enligt samma resonemang även 3)
($\mathbf{T}\vdash'\overline{x}$ är ett index till beviset att $(1=0)$ i $\mathbf{T}'$) $\rightarrow\mathbf{T}\vdash(1=0)$ att, om vi kan härleda ett sådant bevis, kommer vi även kunna härleda falskhet ur $\mathbf{T}$. Det vill säga, $\mathbf{T}$ härleder att (om vi ur $\mathbf{T}$ kan göra en härledning av påståendet att ($\mathbf{T}$ härleder falskhet) så kommer vi kunna härleda falskhet ur $\mathbf{T}$). Vilket alltså blir 4):

$$\mathbf{T}\vdash((\mathbf{T}\vdash(\mathbf{T}\vdash(1=0))\rightarrow(\mathbf{T}\vdash(1=0))$$

Vi använder oss av **lemma 9** och sätter A som $\mathbf{T}\vdash(1=0)$ och vilket ger att 4) ger att $\mathbf{T}\vdash(\mathbf{T}\vdash(1=0))$.

Om vi nu dessutom har att $\mathbf{T}$ har disjunktions egenskapen, har vi enligt **sats 1** att vi kan hitta x sådana att $A(x)$ gäller. Vi har då att, eftersom $\mathbf{T} \vdash (\mathbf{T} \vdash (1 = 0))$ gäller, kan vi även hitta ett bevis för $\mathbf{T} \vdash (1 = 0)$ enligt **lemma 1** och vi får $\exists x.\mathbf{T} \vdash' \overline{x}$ är ett index till beviset att $(1 = 0)$ i $\mathbf{T}'$. Alltså har vi att $\mathbf{T} \vdash (1 = 0)$. $\square$

Vi har alltså visat att, en flersortig extension $\mathbf{T}$ av $\mathbf{HA}_0$ visar sin egen inkonsistens i det fall disjunktions egenskapen kan härledas ur den.

9 Slutsats

Vi har alltså tittat på den filosofiska skillnaden mellan intuitionistisk logik och klassisk logik, nämligen att klassisk logik förutsätter en yttre matematisk värld medan intuitionistisk logik utgår från att alla matematiska objekt är mentala. Vi har sedan sett hur dessa skillnader påverkar de logiska lagarna $\exists$ och $\vee$.

Speciellt har vi sett hur vi kan tolka $\exists$ på olika sätt. Det vill säga, antingen kan vi tolka $\exists$ som 'jag har konstruerat detta...', eller som 'jag kan konstruera detta...'.

Vi har även sett hur vi behöver skapa ett system för bygga upp de naturliga talen och aritmetiken, **Peano aritmetiken**, då vi inte längre kan hänvisa till deras existens i en extern värld. Vi har sedan förvandlat denna aritmetik till att följa de intuitionistiska lagarna, och därmed fått **Heyting-aritmetiken**, i vilket vi har kontrollerat att den faktiskt har disjunktionsegenskapen samt numeriska existensegenskapen.

Även för ensortiga extensioner av $\mathbf{HA}$, så att $\Gamma | A \to A \in \Gamma$, vet vi att de har disjunktionsegenskapen och numeriska existensegenskapen. För flersortiga extensioner har vi dessutom visat att, då $\mathbf{T}$ har disjunktionsegenskapen, kommer den även ha numeriska existensegenskapen. Samt att, då $\mathbf{T}$ har disjunktionsegenskapen (för alla formler i $\mathbf{T}$) och vi kan härleda disjunktionsegenskapen för $\mathbf{T}$ inom själva $\mathbf{T}$, kommer $\mathbf{T}$ att vara inkonsistent.

Det finns så klart andra intuitionistiska matematiska teorier än **HA**, till exempel en intuitionistisk version av Zermelo-Fraenkels mängdteori (**IZF**) som bygger upp matematiken med hjälp av tal och mängder istället. I Beeson [1] diskuteras en del olika teorier och deras olika för- och nackdelar.

Referenser

[1] **Beeson**, Michael J. 1985
Foundations of Constructive Mathematics Springer-verlag

[2] **Boolos**, George S. **Burgess**, John P. **Jeffrey**, Richard C. 2007
Computability and logic Cambridge university Press
fifth edition

[3] **Carlström**, Jesper. 2009
Logik Stockholms universitet.

[4] **Cutland**, Nigel J. 1997
Computability Cambridge University Press

[5] **van Dalen**, Dirk. 1999
The Role of Language and Logic in Brouwer's Work
Springer Vienna. Logic in action (ed. E. Orlovska)

[6] **Dummett**, Michael. 1977
Elements of intuitionism Clarendon Press. Oxford

[7] **Dummett**, Michael. 1975
The philosophical basis of intuitionistic logic
first published in *Studies in logic and the foundation of mathemtics, volym 80* sid. 5-40.
Ur: the philosophy of mathematics. 1996. Edited by W.D. Hart. Oxford university press.

[8] **Friedman**, Harvey. 1975
The disjunction property implies the numerical existence property
Proc. Nat. Acad. Sci. USA
Vol. 8, No. 8, pp. 2877-2878.

[9] **Heyting**, Arend. 1956
Intuitionism North Holland publishing company Amsterdam

[10] **Troelstra**, Anne Sjerp. **van Dalen** Dirk. 1988
Constructivism in mathematics An introduction Elsevier science publisher B.V.

[11] **Troelstra**, Anne Sjerp. 1973
Metamathematical investigation of intionitionistisc arithmetic and

analysis Springer verlag

[12] Stanford Encyclopedia of Philosophy
`http://plato.stanford.edu/`

[13] Wikipedia
`en.wikipedia.org/`
`sv.wikipedia.org/`
`nl.wikipedia.org/`