Konstruktiv mängdteori

Peter Bohlin

Magisteruppsats i matematik
Göteborgs universitet
19 november 1998

Handledare: Jan Smith,
Institutionen för datavetenskap,
Göteborgs universitet

Sammanfattning

Denna uppsats är ett försök att beskriva hur man kan formulera den traditionella mängdteorin konstruktivt. En del ickekonstruktiva axiom måste bytas ut mot alternativa varianter. Den teori som uppkommer är Peter Aczels konstruktiva Zermelo-Fraenkel. Det konstruktiva i teorin rättfärdigas genom tolkning i Martin-Löfs typteori.

Innehåll

1 Inledning

Syftet med denna uppsats är att beskriva hur man kan modifiera Zermelo-Fraenkels klassiska mängdteori, hädanefter kallad ZF, enligt ett konstruktivistiskt synsätt. En mängdteori CZF, beskriven i (Aczel 1978) och vidareutvecklad i (Aczel 1982) och (Aczel 1986), definieras och det konstruktiva i teorin rättfärdigas genom Aczels översättning till Martin-Löfs typteori.

Den tilltänkte läsaren bör kunna första ordningens predikatlogik. Dessutom skadar det inte med viss kännedom om Zermelo-Fraenkels mängdteori, konstruktiv matematik och Martin-Löfs typteori, även om dessa områden kortfattat beskrivs i uppsatsen. Förslag till läsning om predikatlogik är (Bennet et al 1986). Klassisk Zermelo-Freankel behandlas i (Halmos 1996) och (Bennet 1996). En kortfattad introduktion till konstruktiv matematik är (Palmgren 1997), mer ingående är (Beeson 1985) och (Troelstra och van Dalen 1988). Martin-Löfs typteori beskrivs i (Martin-Löf 1972), (Martin-Löf 1975), (Martin-Löf 1984) och (Nordström et al 1990).

I kapitel 2 beskrivs klassisk mängdteori, först de grundläggande intuitionerna, sedan Zermelo-Fraenkels axiomsystem och slutligen definieras de vanligaste mängdteoretiska och matematiska begreppen. Kapitel 3 beskriver kortfattat intuitionen bakom den konstruktiva synen på matematik, samt förklarar varför den klassiska mängdteorin inte är konstruktivt giltig. Kapitel 4 beskriver några exempel på hur man skulle kunna gå tillväga för att formulera en konstruktivt giltig mängdteori. Kapitel 5 går in mer noggrant på en av dessa konstruktiva mängdteorier, nämligen Aczels CZF, samt visar några enkla resultat om relationen mellan denna teori och ZF. I kapitel 6 beskrivs kortfattat Martin-Löfs konstruktiva typteori, vilken sedan i kapitel 7 används för att tolka CZF och visa att axiomen är konstruktivt giltiga. Slutligen diskuteras i kapitel 8 möjliga utvidgningar och förändringar av teorin, bevisteoretisk styrka samt frågan om hur konstruktiv teorin egentligen är.

2 Klassisk mängdteori

Det var i slutet av 1800-talet som mängdteorin började diskuteras. Ledande i detta sammanhang var Cantor, som började göra matematik med mängder som byggstenar. Sedan byggde Frege på det hela till en formell teori. Freges intuintioner var att en mängd helt enkelt är extensionen av en egenskap. Utgående från en viss given egenskap kunde man skapa mängden av alla objekt som har den egenskapen, dvs. givet en egenskap $\phi(x)$ så kan man skapa mängden A av alla objekt x som uppfyller $\phi(x)$:

$$A = \{\, x \mid \phi(x) \,\}$$

Ett objekt a ligger i mängden A, vilket skrivs $a \in A$, om och endast om $\phi(a)$.

Problemet med denna självklara definition är att man enkelt kan skapa en paradox, Russells paradox. Låt R vara mängden av alla objekt som inte är element i sig själva:

$$R = \{\, x \mid x \notin x \,\}$$

Men detta är enligt Frege bara ett annat sätt att skriva $x \in R \Leftrightarrow x \notin x$. Paradoxen uppkommer när man ställer frågan om R är ett element i R, och låter x vara R.

Då gäller $R \in R \Leftrightarrow R \notin R$, vilket är en motsägelse. Observera att detta bevis inte använder sig av lagen om det uteslutna tredje och alltså även är ett konstruktivt korrekt bevis (mer om detta i kapitel 3).

2.1 Det mängdteoretiska språket

Språket för mängdteori är egentligen en variant av första ordningens predikatlogik med endast en ickelogisk symbol — en tvåställig relation $\in$. Semantiken för $a \in b$ är att mängden a är ett element i mängden b. Detta innebär att formler i mängdteori definieras induktivt som följer:

- $a \in b$ är en formel om a och b är variabler.
- $\phi \wedge \psi$, $\psi \vee \psi$, $\phi \rightarrow \psi$ och $\neg\phi$ är formler om ϕ och ψ är formler.
- $\exists v\, \phi$ och $\forall v\, \psi$ är formler om v är en variabel och ϕ är en formel.

Mängder som man har bevisat existensen av brukar ofta ges egna namn i form av nya individkonstanter som läggs till i språket. Dessutom brukar man särskilja begränsade och obegränsade kvantifieringar. Detta är särskilt viktigt när man sysslar med konstruktiv matematik. En begränsad kvantifiering är när variabeln v löper över en given mängd, dvs. påståendet gäller för alla mängder (alternativt någon mängd) som är element i en given mängd:

$$\begin{array}{lll} \forall v \in a\, \phi(v) & =_{def} & \forall v(v \in a \rightarrow \phi(v)) \\ \exists v \in a\, \phi(v) & =_{def} & \exists v(v \in a \wedge \phi(v)) \end{array}$$

En formel sägs vara begränsad om alla kvantifikatorer som förekommer i formeln är begränsade.

I den fortsatta framställningen kommer, om inget annat sägs, grekiska bokstäver (ϕ, ψ etc.) att användas för formler och latinska bokstäver (a, b, x etc.) för mängder. Bokstäverna x, y och z betecknar alltid variabler, medan övriga bokstäver kan beteckna variabler eller givna mängder beroende på sammanhanget. Ibland kan även fetstil användas om det är någon variabel eller mängd som är extra intressant.

2.2 Zermelo-Fraenkels mängdteori

För att komma runt problemet med Russells paradox skapar man sig ett antal axiom som garanterar att olika typer av mängder existerar. Dessa axiom är dock inte speciellt självklara och man får ingen klar bild av om de stämmer överens med den intuition man har om mängder. Det försöker man hjälpa upp med den hierarkiska modellen, först beskriven i (Zermelo 1930). Denna modell säger att mängder är uppbyggda i steg: Det första steget består av den tomma mängden, det andra består av de mängder som kan bildas ur mängderna i det första steget, det tredje består av de mängder som kan bildas ur mängderna i de första två stegen, etc. Allmänt består ett steg av de mängder som kan bildas ur alla mängder som redan har bildats. Då uppkommer en hierarki av mängder, därav namnet hierarkisk modell.

Axiomen i ZF är till antalet åtta stycken och beskrivs i det som följer. Ibland brukar man lägga till ett nionde axiom, Urvalsaxiomet, den resulterande teorin kallas då ZFC och diskuteras kortfattat i sektion 8.1.

Extensionalitet Mängder är per definition extensionella, dvs. det enda som avgör om två mängder är lika är deras element:

$$a = b \leftrightarrow \forall x \in a(x \in b) \wedge \forall x \in b(x \in a)$$

Regularitet Detta axiom säger att varje icketom mängd har ett $\in$-minimalt element, dvs. ett element som inte har något element gemensamt med den ursprungliga mängden:

$$\forall a(\exists x(x \in a) \rightarrow \exists x \in a \forall y \in a(y \notin x))$$

Axiomet är inget axiom för att skapa nya mängder, utan snarare för att kunna visa egenskaper om mängder. Exempelvis garanterar Regularitet att alla mängder är uppbyggda så som intuitionen gör gällande — det förhindrar "konstiga" mängder, t.ex. mängder som är element i sig själva. Man kan även visa att om man tar ut ett element ur en mängd och sedan ett element ur den nya mängden och upprepar detta så kommer man slutligen till den tomma mängden. Det finns alltså inga "oändliga kedjor" när man ska plocka ut element ur mängder. Däremot kan naturligtvis en mängd innehålla oändligt många element — man kan se en mängd som ett träd med ett ändligt djup och möjligtvis oändlig förgrening.

Separation Givet en mängd a och en predikatlogisk formel $\phi(x)$ så existerar en mängd $\mathbf{d}$ som innehåller alla de element x i a som även uppfyller $\phi(x)$:

$$\forall a \exists \mathbf{d} \forall x(x \in \mathbf{d} \leftrightarrow x \in a \wedge \phi(x))$$

Denna mängd brukar skrivas $\{\, x \in a \mid \phi(x) \,\}$, och är vad som är kvar av Freges mängdbildningsprincip. Axiomet behövs för att definiera i princip alla de mängder man vanligen behöver, eftersom de andra axiomen bara förutsäger mängder som omfattar en viss mängd.

Par Detta axiom säger att givet två mängder a och b existerar en mängd $\mathbf{p}$ som innehåller både a och b som element:

$$\forall a b \exists \mathbf{p}(a \in \mathbf{p} \wedge b \in \mathbf{p})$$

Observera att axiomet inte garanterar existensen av en mängd med exakt dessa två element, bara att det finns en mängd med minst dessa två element. Med hjälp av Separation kan man dock definiera det äkta paret $\{a, b\}$ till mängderna a och b.

Union Givet en mängd a finns det en mängd $\mathbf{u}$ vilken som element har elementen i alla a:s element:

$$\forall a \exists \mathbf{u} \forall y \in a \forall x \in y(x \in \mathbf{u})$$

Precis som ovan kan man till mängden a definiera den äkta unionen $\bigcup a$ med hjälp av Separation.

Potensmängd Potensmängden $\mathbf{p}$ till en given mängd a, dvs. mängden av alla delmängder till a, existerar:

$$\forall a \exists \mathbf{p} \forall x (x \subseteq a \rightarrow x \in \mathbf{p})$$

Här är begreppet $x \subseteq a$, som betyder att x är en delmängd till$?a$, definierat som $\forall y \in x (y \in a)$. Observera att även här krävs Separation för att kunna definiera den äkta potensmängden som inte innehåller annat än delmängder till den givna mängden. Denna mängd skrivs $\mathcal{P}(a)$ för den givna mängden a.

Oändlighet Detta axiom garanterar existensen av en mängd $\mathbf{n}$ med oändligt många element. Axiomet säger (i) $\mathbf{n}$ är icketom, och (ii) för varje element x i $\mathbf{n}$ finns det ett annat element i $\mathbf{n}$ som innehåller x:

$$\exists \mathbf{n} (\exists x (x \in \mathbf{n}) \wedge \forall x \in \mathbf{n} \exists y \in \mathbf{n} (x \in y))$$

Detta är det enda axiom som garanterar existensen av en mängd, vilket betyder att utan detta axiom kan man inte skapa några mängder alls. Regularitet krävs för att vara säker på att denna mängd verkligen är oändlig, eftersom utan regularitet kan mängder vara element i sig själva. Mängden av de naturliga talen kan definieras ur denna mängd $\mathbf{n}$, vilket vi gör i sektion 2.3.

Substitution Om $\phi(x, y)$ är en funktionell relation på a, dvs. om det för varje $x \in a$ finns exakt ett y så att $\phi(x, y)$ är sann, kan man även bilda mängden av de y för vilket formeln gäller:

$$\forall a (\forall x \in a \exists! y \; \phi(x, y) \rightarrow \exists \mathbf{b} \phi'(a, \mathbf{b}))$$

Här är $\exists! y$ (vilket betyder att det finns ett och endast ett y som passar) och $\phi'(a, b)$ (vilket är en förkortning för att a respektive b är domänen respektive bilden till ϕ) definierade enligt:

$$\begin{array}{rcl} \exists! x \psi(x) & =_{def} & \exists x (\psi(x) \wedge \forall y (\psi(y) \rightarrow x = y)) \\ \phi'(a, b) & =_{def} & \forall x \in a \exists y \in b \phi(x, y) \wedge \forall y \in b \exists x \in a \phi(x, y) \end{array}$$

Om man för varje $x \in a$ skriver $f(x)$ för det unika y som gör att $\phi(x, y)$ är sann, kan man säga att Substitution garanterar att mängden $\mathbf{b} = \{ f(x) \mid x \in a \}$ existerar.

Ur Substitution kan man härleda Separation, vilket alltså är ett redundant axiom. Man brukar dock ändå ha med Separation, eftersom det är ett naturligare axiom, rent intuitivt. Dessutom undersöker man ofta systemet Z vilket är ZF utan Substitution.

2.3 Definitioner av några vanliga begrepp

Med hjälp av dessa axiom kan man uttrycka all traditionell matematik. De vanligaste begreppen följer här.

Tomma mängden Eftersom Oändlighet förutsäger existensen av en mängd $\mathbf{n}$, kan man använda den och Separation för att definiera den tomma mängden:

$$\emptyset =_{def} \{ x \in \mathbf{n} \mid \bot \}$$

Dessutom garanterar Extensionalitet att det endast finns en tom mängd.

Oordnade och ordnade par Det oordnade paret av två mängder a och b, vilket garanteras av Par och Separation, skrivs helt enkelt $\{a, b\}$. Mängden med ett element, $\{a\}$, kan definieras som $\{a, a\}$ och mängden med tre element, $\{a, b, c\}$, är helt enkelt unionen av $\{a\}$ och $\{b, c\}$ (se nästa paragraf för en beskrivning av unionen). På liknande sätt kan mängder med ändligt antal element definieras.

Det ordnade paret $\langle a, b\rangle$ kan nu definieras som $\{\,\{a\},\,\{a, b\}\,\}$. En trippel $\langle a, b, c\rangle$ är som vanligt $\langle a, \langle b, c\rangle\rangle$, osv.

Union, snitt och differens Unionen av en mängd a garanteras av Union och Separation och skrivs $\bigcup a$. Unionen mellan två mängder $a \cup b$ kan nu definieras som $\bigcup\{a, b\}$. Med hjälp av Separation kan man så definiera snittet av en mängd a som:

$$\bigcap a \;=_{def}\; \{\, x \in \bigcup a \mid \forall y \in a(x \in y)\,\}$$

Sedan kan man definiera $a \cap b$ som $\bigcap\{a, b\}$. Differensen $a \setminus b$ kan definieras som $\{\, x \in a \mid x \notin b\,\}$.

Produkt, relationer och funktioner Om $x \in a$ och $y \in b$ så är det ordnade paret $\langle x, y\rangle$ en delmängd av potensmängden $\mathcal{P}(a \cup b)$ till $a \cup b$, vilket ses ur definitionen av det ordnade paret. Men om paret är en delmängd till en mängd så måste det vara ett element i den mängdens potensmängd, dvs. potensmängden till $\mathcal{P}(a \cup b)$. Alltså gäller $\langle x, y\rangle \in \mathcal{P}(\mathcal{P}(a \cup b))$, varför $a \times b$ måste vara en delmängd till $\mathcal{P}(\mathcal{P}(a \cup b))$, vilken sedan kan specificeras med Separation:

$$a \times b \;=_{def}\; \{\, z \in \mathcal{P}(\mathcal{P}(a \cup b)) \mid \exists x \in a \exists y \in b(z = \langle x, y\rangle)\,\}$$

Denna mängd $a \times b$ brukar ofta skrivas $\{\, \langle x, y\rangle \mid x \in a \wedge y \in b\,\}$. En relation är helt enkelt en delmängd till produkten, och en funktion är en relation f för vilken följande gäller:

$$\forall x \in a \exists! y \in b(\langle x, y\rangle \in f)$$

Att ett par $\langle x, y\rangle$ ligger i relationen R, brukar skrivas $xR\,y$, och för det unika y-värde som i par med ett givet x-värde ligger i funktionen f, skriver man $y = f(x)$.

Delmängder och transitiva mängder Delmängdsbegreppet har vi redan definierat som:

$$a \subseteq b \;=_{def}\; \forall x \in a(x \in b)$$

Detta innebär att Extensionalitet kan skrivas om till:

$$a = b \;\leftrightarrow\; a \subseteq b \wedge b \subseteq a$$

En mängd kallas transitiv om alla dess element även är delmängder till mängden:

$$\mathit{Trans}(a) \;=_{def}\; \forall x \in a(x \subseteq a)$$

Exempel på transitiva mängder är de naturliga talen och mängden av de naturliga talen, vilka definieras nedan. Det transitiva höljet till en mängd a är den minsta transitiva mängd som har a som delmängd. Man kan visa att det transitiva höljet existerar och är unikt för varje mängd a, vilket vi dock inte gör här.

Naturligt tal Ett naturligt tal är antingen 0 eller efterföljaren n^+ till något naturligt tal n. Mängdteoretiskt brukar man definera naturliga tal som: 0 är tomma mängden $\emptyset$, och efterföljaren till mängden n är $n^+ = n \cup \{n\}$. Med denna definition blir varje naturligt tal transitivt och att ett tal n är mindre än ett tal m blir då helt enkelt $n \in m$.

Mängden av de naturliga talen Oändlighet förusäger inte direkt existensen av mängden av de naturliga talen, här kallad $\mathbf{N}$. Men den mängden kan definieras med hjälp av de övriga axiomen.

Först måste man utifrån den mängd som garanteras i Oändlighet skapa en mängd som innehåller tomma mängden och alla naturliga tal som de är definierade ovan. Det är inte helt trivialt, men görs i t.ex. (Aczel 1997). Ett annat sätt är att ändra axiomet till att garantera just en sådan mängd:

$$\exists \mathbf{n} \mathit{NatSet}(\mathbf{n})$$

Här säger $\mathit{NatSet}(a)$ att a innehåller alla naturliga tal:

$$\mathit{NatSet}(a) \ =_{def} \ \emptyset \in a \wedge \forall x \in a (x^+ \in a)$$

Nu kan vi definiera mängden $\mathbf{N}$ till att vara den minsta delmängd till $\mathbf{n}$ som innehåller alla naturliga tal, där $\mathbf{n}$ är den oändliga mängd som sägs existera. Potensmängden $\mathcal{P}(\mathbf{n})$ till $\mathbf{n}$ existerar. Den innehåller alla delmängder till $\mathbf{n}$. Via Separation kan man välja ut endast de mängder som innehåller varje naturligt tal, och slutligen kan man ta snittet av denna mängd:

$$\mathbf{N} \ =_{def} \ \bigcap \{ \, y \in \mathcal{P}(\mathbf{n}) \mid \mathit{NatSet}(y) \, \}$$

Peanos axiom för de naturliga talen För att visa att $\mathbf{N}$ är just mängden av de naturliga talen bör man kunna visa Peanos fem axiom:

PA1 $\emptyset \in \mathbf{N}$
PA2 $\forall n \in \mathbf{N} (n^+ \in \mathbf{N})$
PA3 $\forall n, m \in \mathbf{N} (n^+ = m^+ \rightarrow n = m)$
PA4 $\forall n \in \mathbf{N} (0 \neq n^+)$
PA5 $\forall a \subseteq \mathbf{N} (\, (\emptyset \in a \wedge \forall n \in a (n^+ \in a)) \rightarrow a = \mathbf{N} \,)$

PA1 och **PA2** följer direkt ur definitionerna av $\mathbf{N}$ och successorn, och **PA4** följer ur Extensionalitet. För att visa **PA5** måste vi visa $a = \mathbf{N}$ för en given mängd a som uppfyller premissen. Men eftersom $\mathbf{N}$ är den minsta mängd som uppfyller premissen så måste $\mathbf{N} \subseteq a$ gälla. Dessutom gäller $a \subseteq \mathbf{N}$ enligt premissen, och därför även $a = \mathbf{N}$.

För att visa **PA3**, antar man först att $n^+ = m^+$, dvs. att $n \cup \{n\} = m \cup \{m\}$. Men då måste enligt Extensionalitet antingen $n = m$ eller $n \in m$ gälla, och dessutom gäller även $m = n$ eller $m \in n$. Om nu **PA3** inte ska vara sann så måste därför $n \in m \in n$, vilket förbjuds av Regularitet och alltså har vi visat **PA3**.

3 Konstruktiv matematik

Huvudidén med konstruktiv matematik är att för att kunna hävda att ett påstående är sant så måste man ha ett bevis för det. I klassisk matematik är

världen uppdelad i påståenden som antingen är sanna eller falska oavsett om vi har lyckats bevisa dem eller inte, och en matematikers uppgift är att utröna vilka påståenden som är sanna och vilka som är falska. I konstruktiv matematik finns endast bevisade respektive inte bevisade påståenden. Ett sant påstående är ett som det finns ett bevis för och ett falskt påstående är ett för vilket det kan bevisas att det leder till en motsägelse.

Klassisk första ordningens predikatlogik är inte konstruktiv, vilket kommer att visas nedan. För att kunna använda sig av ett predikatlogiskt språk konstruktivt blir man tvungen att formulera en ny semantik för konnektiverna. Denna intuitionistiska logik brukar definieras utifrån Brouwer-Heyting-Kolmogorovs tolkning av vad som krävs för ett bevis av en predikatlogisk sats:

- $\bot$ har inget bevis
- Ett bevis för $\phi \wedge \psi$ är ett bevis för ϕ och ett bevis för ψ.
- Ett bevis för $\phi \vee \psi$ är ett bevis för ϕ eller ett bevis för ψ samt information om vilken av de två som är bevisade.
- Ett bevis för $\phi \rightarrow \psi$ är en metod som givet ett bevis för ϕ ger ett bevis för ψ.
- Ett bevis för $\forall x \in A\, \phi(x)$ är en metod som givet ett godtyckligt element $a \in A$ ger ett bevis för $\phi(a)$.
- Ett bevis för $\exists x \in A\, \phi(x)$ är ett element $a \in A$ och ett bevis för $\phi(a)$.

Negationen $\neg A$ definieras av $A \rightarrow \bot$, och ekvivalensen $A \leftrightarrow B$ som vanligt av $(A \rightarrow B) \wedge (B \rightarrow A)$.

3.1 Konstruktivt icke korrekta principer

Att man omdefinierar predikatlogiken har en rad följder. Bland annat måste man avsäga sig följande klassiskt korrekta påståenden, vilka gäller för alla formler ϕ och ψ.

1. $\phi \vee \neg\phi$
2. $\neg\neg\phi \;\leftrightarrow\; \phi$
3. $\phi \rightarrow \psi \;\leftrightarrow\; \neg\phi \vee \psi$
4. $\neg(\phi \wedge \psi) \;\leftrightarrow\; \neg\phi \vee \neg\psi$
5. $\neg\forall x \phi(x) \;\leftrightarrow\; \exists x \neg\phi(x)$

(1) Det första exemplet brukar kallas lagen om det uteslutna tredje, vilket alltså säger att antingen är ett påstående sant eller så är det falskt — det finns inget tredje alternativ. Att denna princip inte är konstruktivt giltig kan man visa med hjälp av s.k. Brouwerska motexempel.

Anta att ϕ är ett påstående som man varken har lyckats bevisa eller motbevisa, t.ex. Goldbachs hypotes.[1] Om lagen om det uteslutna tredje, LT (dvs.

[1] Goldbachs hypotes säger att varje jämnt tal större än 2 kan skrivas som summan av två primtal. Hypotesen har hittills inte kunnat bevisas, man har inte heller funnit något motexempel till den.

$\phi \vee \neg\phi$ för alla formler ϕ och ψ) skulle vara sann, betyder det konstruktivt att man har ett bevis för detta påstående. Men, enligt tolkningen ovan, om man har bevisat en disjunktion vet man även vilken av disjunkterna som är sann, och alltså kan man få reda på om Goldbachs hypotes är sann eller ej utan att ha bevisat den, vilket är orimligt. Om någon till slut skulle bevisa Goldbachs hypotes, kan man alltid hitta ett annat obevisat påstående.

(2) Däremot kan man bevisa att $\neg\neg$LT gäller för alla formler ϕ. Låt oss förutsätta att $\neg$LT är sann för något ϕ, vilket innebär att vi vet $(\phi \vee \neg\phi) \to \bot$. Detta är en metod som tar ett bevis för ϕ eller ett bevis för $\neg\phi$ och ger en motsägelse. Men då måste $\phi \to \bot$ gälla, vilket är ekvivalent med $\neg\phi$. Enligt förutsättningen så kan vi då dra slutsatsen $\bot$, vilket är en motsägelse. Därmed har vi bevisat att $\neg$LT implicerar $\bot$, dvs. $\neg\text{LT} \to \bot$ för varje formel ϕ. Men detta är ju bara ett annat skrivsätt för $\neg\neg$LT.

Detta i sin tur gör naturligtvis att $\neg\neg\phi \to \phi$ inte gäller konstruktivt för alla formler ϕ, och alltså inte heller $\neg\neg\phi \leftrightarrow \phi$. Däremot är $\phi \to \neg\neg\phi$ konstruktivt giltigt, vilket inte är svårt att bevisa.

(3) Påståendet $\phi \to \phi$ är konstruktivt sant. Ett bevis för detta är helt enkelt en algoritm som tar ett bevis för ϕ och ger tillbaka precis samma bevis, dvs. identitetsalgoritmen. Men eftersom $\phi \vee \neg\phi$ inte är giltig enligt ovan, kan inte heller $\phi \to \psi$ vara ekvivalent med $\neg\phi \vee \psi$ för alla formler ϕ och ψ. Däremot gäller alltid $(\neg\phi \vee \psi) \to (\phi \to \psi)$.

(4) Om vi sätter ψ till att vara $\neg\phi$ så ser vi att vänsterledet $\neg(\phi \wedge \neg\phi)$ måste vara sant för alla formler ϕ. Negationen av en formel betyder ju att formeln implicerar en motsägelse, och vänsterledet säger då att om vi vet ϕ och dessutom att ϕ implicerar en motsägelse så kan vi härleda en motsägelse. Däremot kan inte högerledet $\neg\phi \vee \neg\neg\phi$ gälla för alla ϕ, av samma anledning som varför lagen om det uteslutna tredje inte är giltig. Alltså kan inte $\neg(\phi \wedge \psi)$ vara ekvivalent med $\neg\phi \vee \neg\psi$ för alla formler ϕ och ψ. Däremot kan man bevisa att högerledet implicerar vänsterledet.

(5) Om vi begränsar oss till att titta på en modell med endast två element, ϕ_0 och ϕ_1, så blir vänsterledet ekvivalent med $\neg(\phi_0 \wedge \phi_1)$ och högerledet ekvivalent med $\neg\phi_0 \vee \neg\phi_1$. Men enligt paragrafen ovan så är inte dessa två påståenden ekvivalenta för alla formler ϕ_0 och ϕ_1, och därför kan inte heller $\neg\forall x\phi(x)$ vara ekvivalent med $\exists x\neg\phi(x)$ i alla modeller med två element. Med liknande resonemang kan man visa att påståendena inte är ekvivalenta i större modeller. Däremot är $\neg\forall x\phi(x)$ härledbart ur $\exists x\neg\phi(x)$ i alla modeller.

3.2 Impredikativitet

Impredikativitet är ett vanligt fenomen i klassisk matematik, vilket även förekommer i vissa varianter av konstruktiv matematik. En definition är impredikativ när man använder det som ska definieras i själva definitionen, dvs det blir någon typ av cirkularitet. Ett exempel (i mängdläran) är om man försöker definiera en mängd som innehåller alla mängder, ett universum. Då måste ju

universumet vara element i sig självt, vilket är orimligt. Nu kan inte universummängden defineras i klassisk mängdlära, men det finns andra exempel. Givet en formel $\phi(x, y)$ så kan man i ZF definiera en delmängd a till de naturliga talen $\mathbf{N}$ som $a = \{ x \in \mathbf{N} \mid \forall y \in \mathcal{P}_{\mathbf{N}}\, \phi(x, y) \}$, där $\mathcal{P}_{\mathbf{N}}$ är potensmängden till $\mathbf{N}$. Men eftersom a är en delmängd till $\mathbf{N}$ så ligger den redan i $\mathcal{P}_{\mathbf{N}}$. Det betyder att mängden y kommer att instansieras till a i definitionen av a, vilket många konstruktivister tycker är orimligt.

3.3 Konstruktivt problematiska axiom i ZF

Om man byter ut den klassiska logiken i ZF mot intuitionistisk logik så kan man ändå härleda lagen om det uteslutna tredje. Det är dock endast axiomet Regularitet som är icke-konstruktivt på det sättet. Av de övriga axiomen i ZF är två impredikativa — Separation och Potensmängd. De medför alltså inte lagen om det uteslutna tredje och är därför inte direkt icke-konstruktiva, men de ger upphov till cirkulariteter vilket enligt ovan kan anses orimligt.

Regularitet Låt ϕ vara ett givet påstående. Definiera mängden S som:

$$S =_{def} \{ x \in 2 \mid x = 1 \vee (x = 0 \wedge \phi) \}$$

Här är mängderna 0, 1 respektive 2 mängderna $\emptyset$, $\{0\}$ respektive $\{0, 1\}$. Att S är en mängd garanteras av Separation. Enligt Regularitet finns nu ett $\in$-minimalt element som vi dessutom känner till vilket det är, enligt tolkningen av $\exists$-kvantifikatorn. Varje element i S är antingen lika med 0 eller $\{0\}$. Om det minimala elementet är 0 så måste också ϕ gälla, och om det är $\{0\}$ så säger Regularitet att 0 inte kan ligga i S varför $\neg\phi$ måste gälla. Alltså har vi härlett lagen om det uteslutna tredje ur Regularitet. Den konstruktiva varianten blir axiomet Mängdinduktion, som på ett mer direkt sätt uttrycker att alla mängder byggs upp underifrån från den tomma mängden.

Separation Separation är impredikativt eftersom kvantifikatorerna i formeln får variera över hela mängduniversumet. Det gör att man kan definiera mängder med hjälp av en formel som löper över alla mängder, dvs. även den mängd man försöker definiera. Den konstruktiva ersättningen blir helt enkelt att begränsa kvantifikatorerna i formeln till att bara löpa över redan existerande mängder, dvs. endast tillåta begränsade formler.

Potensmängd Potensmängd är tillsammans med den begränsade varianten av Separation impredikativt. Med dem kan man, givet en mängd, definiera en delmängd med Separation genom att kvantifiera över potensmängden till den givna mängden. Men i potensmängden finns ju även den mängd man håller på att definiera, och alltså blir det en impredikativ definition. Den vanliga konstruktiva varianten är Exponentiering (Myhill 1975) som säger att mängden av alla funktioner mellan två givna mängder alltid existerar. Det motsvarande axiomet i Aczels konstruktiva teori är Delmängd, vilket är en starkare variant.

4 Konstruktiv mängdteori

Eftersom den klassiska mängdläran inte är konstruktivt giltig, kan man fundera på hur en konstruktiv variant av ZF kan se ut. Vilka axiom bör förändras och hur ser de nya ut? Det finns ett antal olika teorier, vissa svagare, andra starkare. Här följer tre olika mängdteorier, och i nästa kapitel ska vi koncentrera oss på en fjärde, kallad konstruktiv Zermelo-Fraenkel.

Intuitionistisk Zermelo-Fraenkel Den enklaste sättet att göra en konstruktiv mängdlära är att helt enkelt ta de vanliga axiomen för ZF och använda intuitionistisk logik. Då måste man dessutom byta ut de axiom som implicerar lagen om det uteslutna tredje. Enligt sektion 3.3 är det endast Regularitet som behöver bytas ut, vanligast är att man gör det mot det klassiskt ekvivalenta Mängdinduktion. Dessutom brukar man göra en smärre förändring av Substitution, eftersom det blir svagare konstruktivt än klassiskt. Med dessa smärre förändringar får man en ny teori som dels är konstruktivt giltig och dels är ekvivalent med ZF klassiskt sett. Denna teori brukar kallas Intuitionistisk Zermelo-Fraenkel, IZF, och beskrivs bland annat i (Beeson 1985). Det kan visas att IZF är bevisteoretiskt lika stark som ZF, med en så kallad negativ översättning. Det innebär att alla påståenden som kan bevisas i ZF också kan bevisas, i sin negativt översatta form, i IZF. Tyvärr finns problemen med impredikativitet kvar i IZF, vilket gör att många konstruktivister förkastar teorin.

Myhills konstruktiva mängdteori Myhill föreslår i (Myhill 1975) ett axiomsystem för en konstruktiv mängdteori. Den har Begränsad Separation i stället för vanlig och Exponentiering istället för Potensmängd, vilket gör att teorin är predikativ (motsatsen till impredikativ). I sektion 5.3 visas att teorin är ekvivalent med ZF om man använder klassisk logik. Teorin CZF som beskrivs i nästa kapitel är en utvidgning av Myhills mängdteori.

Fregestrukturer En helt annan angreppsvinkel på problemet att översätta mängdlära till något konstruktivt är att ta fasta på Freges ursprungliga idé med mängder som extensioner av påståenden. Aczel beskriver i (Aczel 1980) ett sådant system, och visar att Russells paradox inte uppkommer om man använder en intuitionistisk tolkning av påståenden.

5 Konstruktiv Zermelo-Fraenkel — CZF

I (Aczel 1978) beskrivs ett antal axiom för en konstruktiv mängdteori, kallad Constructive Zermelo-Fraenkel, CZF. Den är en starkare variant av Myhills mängdteori, beskriven i (Myhill 1975). Det betyder att Myhills mängdteoretiska axiom går att bevisa i CZF, men att CZF inte kan bevisas i Myhills teori (i alla fall är det osannolikt, enligt Aczel).

Axiomen i CZF är, med fyra undantag, exakt likadana som ZF. De fyra undantagen är Regularitet, Separation, Potensmängd och Substitution. De ickekonstruktiva respektive impredikativa problemen med Regularitet respektive Separation och Potensmängd har beskrivits sektion 3.3. Anledningen att Substitution byts ut är lite mer subtil. Substitution innehåller en unik existenskvantifikator — det krävs att det för varje x finns ett och endast ett y. Klassiskt sett

implicerar detta axiom det allmänare Utökad Substitution. Tyvärr gäller inte detta för intuitionistisk logik, vilket gör att vi byter ut Substitution mot Utökad Substitution.

5.1 Axiomen i CZF

Först behöver vi en definition som i princip uttrycker att två mängder är domän respektive bild till en relation. Det kan sägas vara en utvidgning av begreppen domän och bild för funktioner:

$$\phi'(a,b) \ =_{def} \ \forall x \in a \, \exists y \in b \, \phi(x,y) \wedge \forall y \in b \, \exists x \in a \, \phi(x,y)$$

Observera här att för en given mängd a kan det finnas flera olika mängder b som passar in i definitionen. Bilden b är alltså inte entydigt given. Detta beror på att formeln ϕ kan ses som en flertydig funktion med domän a, och bilderna b beror på vilket funktionsvärde man väljer.

Extensionalitet

$$a = b \ \leftrightarrow \ \forall x \in a (x \in b) \wedge \forall x \in b (x \in a)$$

Mängdinduktion Mängdinduktion ersätter Regularitet, och säger att ett påstående ϕ gäller för alla mängder om man, givet en godtycklig mängd y för vilken ϕ gäller för alla elementen, kan bevisa att ϕ gäller även för y:

$$\forall y (\forall x \in y \, \phi(x) \rightarrow \phi(y)) \rightarrow \forall x \phi(x)$$

Detta axiom är en utvidgning av induktionsprincipen för naturliga tal. Något basfall behövs däremot inte, eftersom den tomma mängden passar in i schemat (om $y = \emptyset$ så gäller automatiskt ϕ för alla y:s element, eftersom y inte har några element).

Begränsad Separation Här gäller det att $\phi(x)$ är en begränsad formel, dvs. att alla kvantifikatorer i $\phi(x)$ är begränsade. I övrigt är axiomet likadant som klassisk Separation:

$$\forall a \exists \mathbf{d} \forall x (x \in \mathbf{d} \leftrightarrow x \in a \wedge \phi(x))$$

Par

$$\forall a b \exists \mathbf{p} (a \in \mathbf{p} \wedge b \in \mathbf{p})$$

Union

$$\forall a \exists \mathbf{u} \forall y \in a \forall x \in y (x \in \mathbf{u})$$

Oändlighet

$$\exists \mathbf{n} (\exists x (x \in \mathbf{n}) \wedge \forall x \in \mathbf{n} \exists y \in \mathbf{n} (x \in y))$$

Utökad Substitution Detta axiom (kallat Strong Collection på engelska) är nästan som det klassiska Substitution, förutom att formeln $\phi(x,y)$ här inte behöver vara en funktionell relation, utan kan vara vilken relation som helst (man skulle också kunna säga att ϕ är en flervärd funktion):

$$\forall a (\forall x \in a \, \exists y \, \phi(x,y) \rightarrow \exists \mathbf{b} \, \phi'(a, \mathbf{b}))$$

Delmängd Detta axiom (kallat Subset Collection på engelska) är den konstruktiva ersättningen av Potensmängd, det är också det axiom som är svårast att förstå intuitivt. För alla mängder a och b finns en mängd $\mathbf{p}$ som innehåller någon bild av varje möjlig flervärd funktion från a till b. Med en flervärd funktion menas här en predikatlogisk formel $\phi(x, y)$ som det för varje $x \in a$ finns minst ett $y \in b$ så att $\phi(x, y)$ är sann. Eftersom det inte finns något sätt att kvantifiera över formler, låter man $\phi(x, y)$ även bero på en tredje variabel u som kvantifieras över alla mängder, vilket här skrivs $\phi_u(x, y)$:

$$\forall ab \exists \mathbf{p} \forall u(\forall x \in a \exists y \in b\, \phi_u(x, y) \rightarrow \exists c \in \mathbf{p}\, \phi'_u(a, c))$$

Med hjälp av en så kallad Gödelnumrering kan man översätta predikatlogiska formler till naturliga tal, och därmed kvantifiera över formler. Observera att det är starkare ändå att kvantifiera över mängder, eftersom det finns ouppräkneligt många mängder men bara uppräkneligt många formler.

5.2 De vanligaste begreppen omformulerade

De flesta begrepp som definierades i sektion 2.3 är inga problem att överföra till CZF. I de instanser av Separation som används är redan alla kvantifikatorer begränsade, och Potensmängd används endast på två ställen. Dessa två ställen är vid definitionen av produkten $a \times b$ och vid definitionen av mängden av de naturliga talen $\mathbf{N}$. Dessutom används Regularitet på ett ställe i beviset av Peanos axiom. Eftersom vi har förkastat Potensmängd och Regularitet såsom varande icke-konstruktiva, måste nyss nämnda begrepp omdefinieras.

Produkt Klassiskt definieras produkten $a \times b$ av två mängder a och b som en delmängd till potensmängden av potensmängden till unionen, vilket alltså inte går konstruktivt. Följande resonemang är dock konstruktivt.

Eftersom mängden $b_x = \{\, \langle x, y \rangle \mid y \in b \,\}$ är en mängd för alla mängder x och b enligt Substitution, är också unionen av alla b_x för $x \in a$ en mängd, vilken vi definierar som produkten:

$$a \times b \;=_{def}\; \bigcup_{x \in a} b_x = \bigcup \{\, b_x \mid x \in a \,\}$$

Mängden av de naturliga talen De naturliga talen $\mathbf{N}$ definieras klassiskt som snittet av alla mängder som omfattar alla naturliga tal, men eftersom detta involverar potensmängden så måste definitionen förkastas. I stället kan man göra på följande sätt.

För att förenkla beräkningarna så ersätter vi som tidigare Oändlighet med den förenklade versionen, vilken säger att det finns en mängd som innehåller varje naturligt tal:

$$\exists \mathbf{n} \mathit{NatSet}(\mathbf{n})$$

Predikatet $\mathit{NatSet}(a)$ säger här att a innehåller alla naturliga tal:

$$\mathit{NatSet}(a) \;=_{def}\; \emptyset \in a \wedge \forall x \in a(x^+ \in a)$$

Nu kan vi definiera $\mathbf{N}$, mängden av de naturliga talen, konstruktivt som:

$$\mathbf{N} \;=_{def}\; \{\, x \in \mathbf{n} \mid \exists y \in \mathbf{n}(\mathit{NatNum}(y) \wedge x \in y) \,\}$$

Här betyder $NatNum(b)$ att b endast innehåller naturliga tal:

$$NatNum(b) \ =_{def} \ \forall x \in b(x = \emptyset \vee \exists y \in b(x = y^+))$$

Att se att denna definition av $\mathbf{N}$ verkligen är mängden av de naturliga talen är inte helt trivialt. Därför visar vi det.

Först måste vi visa att $\mathbf{N}$ innehåller alla naturliga tal, dvs. att $NatSet(\mathbf{N})$ gäller, eller om man så vill att (i) $\emptyset \in \mathbf{N}$, och (ii) $x \in \mathbf{N} \rightarrow x^+ \in \mathbf{N}$. Men (i) gäller eftersom $\emptyset \in \mathbf{n}$ och $NatNum(\emptyset^+)$. Dessutom gäller (ii): Om $x \in \mathbf{N}$ så gäller $x \in \mathbf{n}$ och därför även $x^+ \in \mathbf{n}$. Men eftersom $NatNum((x^+)^+)$ gäller så måste $x^+ \in \mathbf{N}$ gälla.

Nu måste vi även visa att $\mathbf{N}$ verkligen är den minsta mängden som innehåller de naturliga talen, dvs. för alla mängder a ska gälla $NatSet(a) \rightarrow \mathbf{N} \subseteq a$. Antag alltså att $NatSet(a)$ gäller för en given mängd a. Vi visar då $\forall x(x \in \mathbf{N} \rightarrow x \in a)$ med hjälp av Mängdinduktion där vi sätter formeln $\phi(x)$ till $x \in \mathbf{N} \rightarrow x \in a$. Som induktionsantagande kan vi anta att $\forall y \in x \phi(y)$ gäller. Givet ett $x \in \mathbf{N}$ så vet vi att $NatNum(x^+)$ gäller och därför är (i) $x = \emptyset$ eller så är (ii) $x = y^+$ för något y. I fall (i) gäller att $x \in a$ eftersom $\emptyset \in a$. I fall (ii) gäller att $y \in x$ och alltså $y \in \mathbf{N}$ enligt transitiviteten hos $\mathbf{N}$. Men enligt induktionsantagandet gäller då $y \in a$ och därför $y^+ = x \in a$.

I detta bevis har vi använt det faktum att $\mathbf{N}$ är transitiv, vilket även det kan bevisas med Mängdinduktion. Sätt formeln $\phi(x)$ till att vara $x \in \mathbf{N} \rightarrow x \subseteq \mathbf{N}$, och antag att $x \in \mathbf{N}$. Då gäller $NatNum(x^+)$ och därför antingen $x = \emptyset \subseteq \mathbf{N}$ eller $x = y^+ = y \cup \{y\}$ för något y. Men eftersom $y \subseteq \mathbf{N}$ och $\{y\} \subseteq \mathbf{N}$ så måste $x \subseteq \mathbf{N}$.

Bevisen av att $\mathbf{N}$ uppfyller Peanos fem axiom är alla konstruktivt giltiga, utom en liten detalj: Eftersom vi inte har Regularitet måste vi använda Mängdinduktion till att bevisa att en mängd inte kan vara element i sig själv, vilket vi dock inte gör här.

5.3 Relationen mellan CZF och ZF

En av de viktigaste egenskaperna med systemet CZF är att det klassiskt är ekvivalent med ZF. Det vill säga att ZF har samma teorem som CZF med klasssik logik. Eller om man så vill: ZF $\equiv$ CZF + LT. Här visas endast den ena riktningen, dvs. att ZF:s axiom kan härledas ur CZF + LT.

För att visa detta ska alltså visas att CZF + LT implicerar (i) Substitution, (ii) Regularitet, (iii) Separation, och (iv) Potensmängd.

Substitution Substitution är en instans av Utökad Substitution, varför axiomet måste gälla.

Regularitet Axiomet Regularitet säger alla mängder antingen är tomma mängden eller regulära. Att en mängd är regulär definieras som att den innehåller ett $\in$-minimalt element:

$$Reg(a) \ =_{def} \ \exists x \in a \forall y \in a(y \notin x)$$

Definiera en mängd som välgrundad om alla mängder som innehåller den mängden är regulära:

$$Grund(b) \ =_{def} \ \forall a(b \in a \rightarrow Reg(a))$$

Om alla mängder är välgrundade så är Regularitet uppfyllt: Givet en godtycklig mängd a, så är den antingen tomma mängden i vilket fall Regularitet är uppfyllt, eller så finns det ett $b \in a$. Detta b är välgrundat enligt hypotesen och alltså är a regulär, och Regularitet är uppfyllt.

Det återstår då att visa att alla mängder är välgrundade, vilket vi gör med Mängdinduktion. Antag nu att alla element i en given mängd b är välgrundade, dvs. $\forall x \in b, \mathit{Grund}(x)$. Låt nu ett a som innehåller b (dvs. $b \in a$) vara givet, och betrakta snittet $a \cap b$. Om snittet är tomt så har a och b inga gemensamma element och då är b ett $\in$-minimalt element i a, och alltså gäller $\mathit{Reg}(a)$. Om snittet inte är tomt så finns det ett element $x \in b$ som också ligger i a. Men enligt induktionsantagandet så gäller då $\mathit{Grund}(x)$ och eftersom $x \in a$ så gäller $\mathit{Reg}(a)$. Men eftersom a är en godtycklig mängd som omfattar b så måste b vara välgrundad. Därmed har vi för varje mängd b visat:

$$\forall x \in b \mathit{Grund}(x) \rightarrow \mathit{Grund}(b)$$

Enligt Mängdinduktion är då alla mängder välgrundade, och därur följer Regularitet.

Exponentiering Axiomet Exponentiering är ett helt och hållet konstruktivt axiom, det följer direkt ur Delmängd. Det säger att för alla mängder a och b finns mängden av funktioner från a till b. Anledningen till att vi visar det här är att vi behöver det i beviset av Potensmängd.

Låt alltså mängderna a och b vara givna. En funktion f från a till b är en delmängd till $a \times b$ som uppfyller:

$$\forall x \in a \exists! y \in b(\langle x, y \rangle \in f)$$

Definiera nu formeln $\phi_f(x, z)$ till att uppfylla:

$$\phi_f(x, \langle x, y \rangle) \leftrightarrow \langle x, y \rangle \in f$$

Då säger Delmängd att det finns en mängd $\mathbf{p}$ med bilder till $\phi_f(x, z)$ för alla möjliga f. Men en bild till ϕ_f är ju f själv, och därför kommer $\mathbf{p}$ att innehålla alla funktioner från a till b. Sedan kan man definiera mängden ${}^a b$ av funktioner med hjälp av Begränsad Separation:

$${}^a b =_{def} \{ f \in \mathbf{p} \mid \forall x \in a \exists! y \in b(\langle x, y \rangle \in f) \}$$

Potensmängd Enligt Exponentiering så finns för alla mängder a och b mängden av funktioner ${}^a b$ från a till b. Först visar vi att Exponentiering tillsammans med antagandet att $\{\emptyset\}$ har en potensmängd implicerar att alla mängder har potensmängd. Observera att vi här endast använder inuitionistisk logik, vilket alltså innebär att inte ens mängder med endast ett element kan ha en potensmängd (om inte teorin ska vara impredikativ).

Givet en mängd a, definiera potensmängden som:

$$\mathcal{P}(a) =_{def} \{ g(f) \mid f \in {}^a \mathcal{P}_1 \}$$

Här är $g(f) = \{ x \in a \mid \emptyset \in f(x) \}$ och $\mathcal{P}_1$ potensmängden till $\{\emptyset\}$. Eftersom $g(f)$ är en delmängd till a så blir då $\mathcal{P}(a)$ en mängd med delmängder till a. För att

visa att $\mathcal{P}(a)$ dessutom är potensmängden till a ska vi visa att alla delmängder till a är element i $\mathcal{P}(a)$. Låt oss alltså anta att b är en delmängd till a. Definiera f till att uppfylla $f(x) = \{\, y \in \{\emptyset\} \mid x \in b \,\}$ för varje $x \in a$. Eftersom $f(x) \subseteq \{\emptyset\}$ för alla $x \in a$ så är f ett element i ${}^a\mathcal{P}_1$ enligt Exponentiering. Detta i sin tur betyder att $g(f) \in \mathcal{P}(a)$, där $g(f) = \{\, x \in a \mid \emptyset \in f(x) \,\} = \{\, x \in a \mid x \in b \,\} = b$. Därmed är b element i $\mathcal{P}(a)$.

Nu behöver vi bara visa att lagen om det uteslutna tredje implicerar att $\{\emptyset\}$ har en potensmängd. Sätt $\mathcal{P}_1 = \{\emptyset, \{\emptyset\}\}$ och låt x vara en delmängd till $\{\emptyset\}$. Då gäller enligt lagen om det uteslutna tredje $\emptyset \in x \vee \emptyset \notin x$. Om $\emptyset \in x$ så är $x = \{\emptyset\}$, om $\emptyset \notin x$ så är $x = \emptyset$. Alltså måste $x \in \mathcal{P}_1$ gälla.

Separation För att visa Separation antar vi först att följande schema gäller för alla formler ϕ:

$$\exists y(\phi \leftrightarrow \emptyset \in y)$$

Ur detta antagande härleder vi Separation, vilket görs konstruktivt varför schemat är impredikativt.

Givet en mängd a och en formel $\phi(x)$ så ska vi visa existensen av mängden $\{\, x \in a \mid \phi(x) \,\}$. Schemat ger att $\forall x \in a \exists y(\phi(x) \leftrightarrow \emptyset \in y)$. Enligt Substitution finns det nu en funktion f så att $\forall x \in a(\phi(x) \leftrightarrow \emptyset \in f(x))$. Men då kan vi med Begränsad Separation definiera mängden $\{\, x \in a \mid \emptyset \in f(x) \,\}$ vilken alltså är lika med den sökta mängden $\{\, x \in a \mid \phi(x) \,\}$.

Nu återstår att visa att lagen om det uteslutna tredje medför att schemat gäller för alla formler ϕ. Givet en formel ϕ så gäller klasssikt $\phi \vee \neg\phi$. Nu kan vi sätta $y = \{\emptyset\}$ om ϕ och $y = \emptyset$ om $\neg\phi$. Denna mängd y uppfyller schemat varför Separation gäller.

6 Martin-Löfs typteori

I detta kapitel ges en högst informell beskrivning av typteori. Den version av typteori som beskrivs är en variant av den som beskrivs i (Martin-Löf 1972) och (Martin-Löf 1975). För den som tycker att detta kapitel ger för lite information rekommenderas (Martin-Löf 1984) eller (Nordström et al 1990) vilka går in mer på djupet.

Det finns två grundläggande begrepp i typteori — *objekt* och *typer*. Varje objekt är av en viss typ, eller rättare sagt, ett visst matematiskt objekt är alltid givet tillsammans med en tillhörande typ. En typ å andra sidan definieras av vad som behövs göras för att konstruera ett objekt av den typen.

Det finns två olika tolkningar av begreppen typ respektive objekt. Den ena, mer intuitiva, är att se en typ som en matematisk mängd, och typens objekt blir då mängens element. Den andra tolkningen är att jämställa en typ med ett påstående eller en proposition, dvs. en predikatlogisk formel. Ett objekt av en viss typ blir då ett bevis för att påståendet är sant. Att denna analogi verkligen är korrekt visas i (Howard 1969).

Ett begrepp som är skilt från påstående är begreppet omdöme (vilket på engelska kallas judgement). Ett omdöme har inget bevisobjekt utan bevisas med hjälp av härledningar inom teorin. Exempel på omdömen är A *type* och $a \in A$. Enligt analogin ovan finns det två tolkningar av varje omdöme. Å ena sidan kan dessa omdömen tolkas som "A är en mängd" respektive "a är ett element i

mängden A". Å andra sidan kan man tolka omdömena som "A är ett påstående" respektive "a är ett bevis för påståendet A". Förutom dessa omdömen finns även omdömen som säger att två typer är lika ($A = B$) och att två objekt av en viss typ är lika ($a = b \in A$).

Mer formellt definieras varje typ och dess objekt av *formeringsregler* som säger hur vi får skapa en instans av den typen, *introduktionsregler* som säger hur objekten i typen introduceras, *eliminationsregler* som säger hur induktion eller rekursion fungerar på objekten av den givna typen, samt *likhetsregler* som säger hur objekten beräknas.

6.1 De små typerna

I typteori finns sex grundläggande sätt att bilda typer, fyra av dem ligger lite närmare de logiska konnektiverna och kvantifikatorerna, och de övriga två är mer som matematiska mängder. Naturligtvis gäller analogin att typer kan ses som både mängder och propositioner för alla typer, det är bara det att vissa typer är mer självklara som propositioner och vissa är mer självklara som mängder.

Förutom dessa sex sätt att bilda typer finns åtminstone två till, likhetstypen $\mathsf{Id}(A, a, b)$ och typen $(\mathsf{W}x \in A)B(x)$ av välordningar eller träd över A och B. Dessa typer kommer vi inte att nämna i det följande, den intresserade hänvisas till (Nordström et al 1990) för mer information.

Π-typerna Antag att A är en typ och att B är en familj av typer som givet ett godtyckligt objekt a av typen A ger en typ $B(a)$. Då är $(\Pi x \in A)B(x)$ typen av funktioner som mappar objekt a av typen A till objekt av typen $B(a)$. Formeringsregeln för Π-typerna blir alltså:

$$\frac{A \ type \qquad B(x) \ type \ [\, x \in A \,]}{(\Pi x \in A)B(x) \ type}$$

Om vi har ett objekt $b(x)$ som är av typen $B(x)$ för varje $x \in A$, kan vi skapa funktionen $\lambda x.b(x)$ som är av den nyss definierade typen. Introduktionsregeln för Π-typerna blir:

$$\frac{b(x) \in B(x) \ [\, x \in A \,]}{\lambda x.b(x) \in (\Pi x \in A)B(x)}$$

Givet ett objekt $a \in A$ och ett objekt f av ovanstående typ, så kan vi nu applicera a på f och få ett objekt $f(a)$ av typen $B(a)$. Eliminationsregeln blir alltså:

$$\frac{a \in A \qquad f \in (\Pi x \in A)B(x)}{f(a) \in B(a)}$$

Men, detta objekt f är ju på formen $\lambda x.b(x)$, och när man applicerar a på f får man likhetsregeln:

$$(\lambda x.b(x))(a) = b(a)$$

Med hjälp av Π-typerna kan →-typerna definieras: $A \to B \ =_{def} \ (\Pi x \in A)B(x)$ om B inte beror av x. Denna typ $A \to B$ blir då typen av alla funktioner från typen A till typen B.

Σ-typerna Precis som för Π-typerna, skapar man Σ-typerna utifrån en typ A och en familj av typer B som för varje $a \in A$ ger en typ $B(a)$. Formeringsregeln är då:

$$\frac{A\ type \qquad B(x)\ type\ [\, x \in A \,]}{(\Sigma x \in A)B(x)\ type}$$

Objekten i denna typ är par med första elementet a i typen A och det andra elementet b i typen $B(a)$. Introduktionsregeln blir:

$$\frac{a \in A \qquad b \in B(a)}{\langle a, b \rangle \in (\Sigma x \in A)B(x)}$$

Antag att vi har en funktion h som tar ett $x \in A$ och ett $y \in B(x)$ och ger ett objekt i typen $H(\langle x, y \rangle)$, och att vi dessutom har ett objekt $p \in (\Sigma x \in A)B(x)$. Då ger funktionen h oss ett objekt i typen $H(p)$, vilket ger eliminationsregeln:

$$\frac{p \in (\Sigma x \in A)B(x) \qquad h(x, y) \in H(\langle x, y \rangle)\ [\, x \in A,\ y \in B(x) \,]}{split(p, h) \in H(p)}$$

Men objektet p är ju ett par av objekten $a \in A$ och $b \in B(a)$, vilket är precis vad funktionen h tar som argument. Det ger oss likhetsregeln:

$$split(\langle a, b \rangle, h) = h(a, b)$$

Med denna konstruktor *split* kan man definiera funktionerna som ger första- respektive andrakomponenten ur ett givet par:

$$\begin{array}{rcl} fst(p) & =_{def} & split(p, \lambda x\, y.x) \\ snd(p) & =_{def} & split(p, \lambda x\, y.y) \end{array}$$

I det forsatta kommer vi endast att ha användning av dessa två funktioner, varför vi inte kommer att nämna konstruktorn *split* mer.

Typen $A \times B$ av alla par med förstakomponenten i typen A och andrakomponenten i typen B kan nu definieras: $A \times B \ =_{def}\ (\Sigma x \in A)B(x)$ om B inte beror av x.

+-typerna Typen $A + B$ existerar givet två typer A och B, vilket ger formeringsregeln:

$$\frac{A\ type \qquad B\ type}{A + B\ type}$$

Objekten i denna typ är alla objekt i typen A samt alla objekt i typen B samt information om vilken typ objekten kommer ifrån. Detta ger två introduktionsregler:

$$\frac{a \in A}{i(a) \in A + B} \qquad \frac{b \in B}{j(b) \in A + B}$$

Antag att vi har en funktion h^i som tar ett $x \in A$ och ger ett objekt i typen $H(i(x))$, samt en funktion h^j som tar ett $y \in B$ och ger ett objekt i typen $H(j(y))$. Då kan vi påstå att det finns ett objekt i typen $H(c)$ för varje $c \in A + B$, vilket ger oss eliminationsregeln:

$$\frac{c \in A + B \qquad h^i(x) \in H(i(x))\ [\, x \in A \,] \qquad h^j(y) \in H(j(y))\ [\, y \in B \,]}{when(c, h^i, h^j) \in H(c)}$$

Slutligen är objekten i $A + B$ antingen på formen $i(a)$ eller $j(b)$, vilket ger oss två likhetsregler:

$$\begin{aligned} when(i(a), h^i, h^j) &= h^i(a) \\ when(j(b), h^i, h^j) &= h^j(b) \end{aligned}$$

De ändliga typerna De ändliga typerna $\mathsf{N_n}$ är de typer som innehåller n olika objekt. Observera att det rör sig om oändligt många typer, varje n ger upphov till en specifik typ. Formeringsreglen är helt enkelt att givet ett $n \geq 0$ så finns typen med n element:

$$\mathsf{N_n}\ type$$

I denna typ finns n olika objekt, vilka vi kan kalla 1, 2, ..., n. Vi får alltså n olika introduktionsregler:

$$1 \in \mathsf{N_n} \qquad 2 \in \mathsf{N_n} \qquad \ldots \qquad n \in \mathsf{N_n}$$

Givet ett objekt $i \in \mathsf{N_n}$ och de n objekten h_1, h_2, ..., h_n alla av typerna $H(1)$, $H(2)$, ..., $H(n)$, så får vi med hjälp av konstruktorn $case_n$ ett objekt av typen $H(i)$. Eliminationsregeln blir alltså:

$$\frac{i \in \mathsf{N_n} \qquad h_1 \in H(1) \qquad h_2 \in H(2) \qquad \ldots \qquad h_n \in H(n)}{case_n(i, h_1, h_2, \ldots, h_n) \in H(i)}$$

Men detta objekt i är helt enkelt på formen k där $1 \leq k \leq n$, vilket ger likhetsregeln:

$$case_n(k, h_1, h_2, \ldots, h_n) = h_k$$

Observera att dessa regler gäller även för typen $\mathsf{N_0}$, dvs. då $n = 0$. Denna typ har inga objekt, och därför inte heller några introduktionsregler eller likhetsregler. Däremot finns eliminationsregeln, som då för varje typ $H(i)$ helt enkelt blir:

$$\frac{i \in \mathsf{N_0}}{case_0(i) \in H(i)}$$

Man kan tolka $\mathsf{N_0}$ som absurditeten $\bot$, och då säger eliminationsregeln att om man har lyckats bevisa absurditeten så kan man bevisa vilket påstående som helst, dvs. $\bot \rightarrow \phi$ för alla påståenden ϕ.

De naturliga talen De naturliga talen är fundamentala i konstruktiv matematik, och i typteori finns en speciell typ som innehåller varje naturligt tal. Formeringsregeln är helt enkelt:

$$\mathsf{N}\ type$$

Den vanliga definitionen av naturliga tal är att 0 är ett naturligt tal och om n är ett naturligt tal så är även successorn till n ett naturligt tal. Med konstruktorn s som successorn blir då introduktionsregeln:

$$0 \in \mathsf{N} \qquad \frac{k \in \mathsf{N}}{s(k) \in \mathsf{N}}$$

Antag att vi har ett objekt h^o i typen $H(0)$ och en funktion h^s som tar ett naturligt tal x och ett objekt i typen $H(x)$ och ger ett objekt i typen $H(s(x))$.

Då vet vi att det för varje naturligt tal n finns ett objekt i typen $H(n)$. Det är en formulering av induktionsprincipen för de naturliga talen — Peanos femte axiom — men även ett sätt att definiera funktioner med rekursion. Eliminationsregeln blir:

$$\frac{i \in \mathsf{N} \qquad h^o \in H(0) \qquad h^s(x) \in H(x) \to H(s(x)) \; [\, x \in \mathsf{N} \,]}{natrec(i, h^o, h^s) \in H(i)}$$

Ett naturligt tal kan enligt introduktionsregeln vara på två former, antingen är det 0 eller en efterföljare. Om talet är 0 så ligger $h^o \in H(0)$ enligt premisserna. Om talet är på formen $s(k)$ så kan vi använda funktionen h^s för att få ett objekt i typen $H(s(k))$. Vi får alltså två likhetsregler:

$$\begin{aligned} natrec(0, h^o, h^s) &= h^o \\ natrec(s(k), h^o, h^s) &= h^s(k, natrec(k, h^o, h^s)) \end{aligned}$$

Som exempel på användning av *natrec* kan vi definiera addition för naturliga tal: Den vanliga definitionen är att (i) $n + 0 = n$, och (ii) $n + s(k) = s(n + k)$. Översätter man detta till typteori får man att $n + m = natrec(m, n, \lambda x\, y.s(y))$.

6.2 Det första universumet

För att kunna prata om typer i typteori krävs ett universum U, där alla hittills skapade typer ligger. Detta universum kan inte vara element i sig själv, $\mathsf{U} \in \mathsf{U}$, eftersom man då kan härleda en paradox, Girards paradox. De typer som är element i U kallas för de små typerna. När man har skapat universumet kan man skapa nya typer som baseras på U, vilka då kan tolkas som påståenden som säger något om typerna i U. Dessutom kan man skapa ett nytt universum som innefattar alla typer skapade med U och de olika typformerarna. Sedan kan man skapa ännu ett nytt universum, och så vidare. Vi kommer dock endast att använda det första universumet U.

Typen av små typer Formeringsregeln är helt enkelt:

$$\mathsf{U}\ type$$

Alla små typer ligger i U, vilket betyder att alla typer som har givits ovan ligger i U (förutsatt att de typer de är formade av ligger i U). Detta ger introduktionsreglerna:

$$\mathsf{N_n} \in \mathsf{U} \qquad \mathsf{N} \in \mathsf{U} \qquad \frac{A \in \mathsf{U} \qquad B \in \mathsf{U}}{A + B \in \mathsf{U}}$$

$$\frac{A \in \mathsf{U} \qquad B(x) \in \mathsf{U} \; [\, x \in A \,]}{(\Pi x \in A) B(x) \in \mathsf{U}} \qquad \frac{A \in \mathsf{U} \qquad B(x) \in \mathsf{U} \; [\, x \in A \,]}{(\Sigma x \in A) B(x) \in \mathsf{U}}$$

Om A ligger i U så är A också en typ. Denna regel brukar kallas eliminationsregel, fast den egentligen inte har några likheter med de andra typernas eliminationsregler:

$$\frac{A \in \mathsf{U}}{A\ type}$$

Universumet saknar likhetsregler, eftersom eliminationsregeln inte ger upphov till några.

Med hjälp av U kan man nu skapa funktioner som tar ett objekt $a \in A$ och ger en typ $B(a)$, vilka då i sin tur kan användas för att skapa nya Π- och Σ-typer eller för att bevisa påståenden om naturliga tal.

En begränsad variant av typen $A + B$ kan definieras med hjälp av Π, N_2 och U: Givet två typer $A \in \mathsf{U}$ och $B \in \mathsf{U}$, definiera $C \in \mathsf{N}_2 \to \mathsf{U}$ till att vara $C = \lambda n.case_2(n, A, B)$. Då är typen $(\Sigma x \in \mathsf{N}_2)C(x)$ en ekvivalent variant av $A + B$, där $i(a) \equiv \langle 1, a\rangle$ och $j(b) \equiv \langle 2, b\rangle$. Denna begränsade disjunkta union är fullt tillräcklig för våra behov i denna uppsats, så därför behövs inte typen $A + B$ i nästa kapitel.

7 En formulering av CZF i typteori

För att visa att teorin CZF är konstruktiv gör vi en översättning till typteori och visar att axiomen i CZF är sanna i denna tolkning. De typer i typteori som kommer att användas vid formuleringen av CZF är:

1. $(\Pi x \in A)B(x)$, typen av funktioner som tar objekt x i typen A och ger objekt av typen $B(x)$,
2. $(\Sigma x \in A)B(x)$, typen av par bestående av ett objekt x i typen A och ett objekt av typen $B(x)$,
3. N, typen av de naturliga talen,
4. $\mathsf{N_n}$, de ändliga typerna med n element, och
5. U, det första universumet, vilket innehåller typerna N och $\mathsf{N_n}$ och är slutet under Π- och Σ-formering.

Typerna $A \to B$, $A \times B$ och en begränsad variant av $A + B$ går att definiera i termer av de ovanstående typerna. Av typerna $\mathsf{N_n}$ kommer vi endast använda de tre första: $\mathsf{N_0}$, $\mathsf{N_1}$ och $\mathsf{N_2}$. Vi kommer inte att behöva någon likhetstyp, varken den extensionella eller den intensionella, inte heller typen $(\mathsf{W}x \in A)B(x)$ av välordningar eller träd över A och B, vilka alla finns beskrivna i (Nordström et al 1990).

Eftersom vissa relationssymboler finns både i typteori och i CZF är det passande att ändra utseendet på några av dem så att inga missförstånd uppstår. Därför kommer i detta kapitel de mängdteoretiska relationerna inklusion, likhet respektive implikation att skrivas $\dot{\in}$, $\doteq$ respektive $\dot{\to}$. De typteoretiska relationerna skrivs som vanligt.

7.1 Typen av CZF-mängder

Först introducerar vi en ny typ V, typen av CZF-mängder. Informellt kan man beskriva objekten i denna typ som par bestående av en liten typ och en funktion från denna typ till typen V.

Denna typ V skulle då innehålla samma objekt som typen $(\Sigma A \in \mathsf{U})(A \to \mathsf{V})$, vilken består av par med en liten typ $A \in \mathsf{U}$ och en funktion $f \in A \to \mathsf{V}$. Nu innehåller denna beskrivning typen V, och alltså kan detta inte vara definitionen av V.

Däremot kan V definieras med hjälp av typen av välordningar W. Med hjälp av denna kan man definiera V till att vara $(\mathsf{W}A \in \mathsf{U})A$. Här gör vi dock inte på

detta sätt, utan anger formerings-, introduktions-, eliminerings- och likhetsregler för typen V.

V-formering Det finns en typ V:

$$\mathsf{V}\ \mathit{type}$$

De element som finns i V kallas för mängder. Av de följande reglerna framgår att typen V inte är en liten typ, dvs. den ligger inte i universumet U.

V-introduktion Givet en liten typ A och en funktion f som för varje element i A ger en mängd, kan man skapa en mängd som bestäms av A och f:

$$\frac{A \in \mathsf{U} \qquad f \in A \to \mathsf{V}}{\mathit{set}(A, f) \in \mathsf{V}}$$

Typen A kallas för mängdens indextyp och elementen i A är index för mängdens element. Som vi ska se när vi definierar likhetsrelationen, kan två mängder som beskrivs av helt olika indextyper och funktioner vara lika. Ett lite mer naturligt skrivsätt för $\mathit{set}(A, f)$ är kanske $\{\, f(x) \mid x \in A \,\}$. Anledningen till att vi inte använder det sättet är att det då lätt kan bli missförstånd när man samtidigt pratar om mängder och dess tolkningar i typteori.

V-elimination Antag att vi har en påståendefunktion H som säger något om mängder. Antag vidare att det finns en funktion som, givet en godtycklig mängd och ett bevis för att H gäller för alla dess element, ger tillbaka ett bevis för att H gäller för mängden själv. Då har vi ett bevis för att H gäller för vilken mängd a som helst:

$$\frac{\begin{array}{l} a \in \mathsf{V} \\ H(x)\ \mathit{type}\ [\, x \in \mathsf{V} \,] \\ h(X, y, z) \in H(\mathit{set}(X, y))\ [\, X \in \mathsf{U},\ y \in X \to \mathsf{V},\ z \in (\Pi x \in X) H(y(x)) \,] \end{array}}{\mathit{setrec}(a, h) \in H(a)}$$

Funktionen h tar en indextyp X och en funktion y från X till V, dvs. en mängd, samt en funktion z som givet ett element i X ger ett bevis för att H gäller för den motsvarande mängden, och ger ett bevis för att H gäller för mängden $\mathit{set}(X, y)$. Denna regel är i princip CZF-axiomet Mängdinduktion översatt till typen V.

V-likhet Givet ett objekt på formen $\mathit{setrec}(a, h)$, så kan funktionen h appliceras på mängden a samt dess element rekursivt:

$$\mathit{setrec}(\mathit{set}(A, f), h) = h(A, f, \lambda x.\mathit{setrec}(f(x), h))$$

Konstruktorn *setrec* kommer egentligen bara att användas vid tre tillfällen, dels för att komma åt en mängds element, dels för att definiera likhets- och elementrelationerna, och dels för att bevisa axiomet Mängdinduktion. Överallt annars används endast de två funktionerna för att komma åt en mängds element, vilka nedan kommer att definieras ur *setrec*.

7.2 Att komma åt en mängds element

Den viktigaste användningen av konstruktorn *setrec* är när vi ska definiera funktioner som tar en mängd och ger dess indextyp respektive den funktion som översätter objekten i indextypen till mängder. Dessa funktioner skrivs $\bar{x}$ respektive $\tilde{x}$ för $x \in \mathsf{V}$, och är av typerna $\mathsf{V} \to \mathsf{U}$ respektive $(\Pi x \in \mathsf{V})(\bar{x} \to \mathsf{V})$. Funktionen $\bar{a}$ tar alltså en mängd $a = set(A, f)$ och ger indextypen A, medan funktionen $\tilde{a}$ ger funktionen f som resultat. Dessa funktioner definieras som följer:

$$\begin{array}{lll} \bar{a} & =_{def} & setrec(a, \lambda X\, y\, z.X) \\ \tilde{a} & =_{def} & setrec(a, \lambda X\, y\, z.y) \end{array}$$

Att dessa definitioner ger korrekta resultat ses i följande beräkningar:

$$\begin{array}{ll} \overline{set(A,f)} & = setrec(set(A,f), \lambda X\, y\, z.X) \\ & = \lambda X\, y\, z.X(A, f, \lambda x.setrec(\ldots)) = A \\ \widetilde{set(A,f)} & = setrec(set(A,f), \lambda X\, y\, z.y) \\ & = \lambda X\, y\, z.y(A, f, \lambda x.setrec(\ldots)) = f \end{array}$$

Ur dessa definitioner och beräkningar ser vi att för alla mängder a har $set(\bar{a}, \tilde{a})$ samma element som a, vilket mängdteoretiskt betyder att de är samma mängd.

7.3 Språket i CZF

Språket i CZF är intuitionistisk predikatlogik med endast en ickelogisk symbol, $\dot{\in}$. För att kunna rättfärdiga axiomen i typteori, behöver vi en översättning. Alla påståenden som kan uttryckas i CZF måste ha en motsvarande typ i typteori. För översättningen definierar vi en operation $\|\phi\|$, som tar en formel ϕ i CZF och ger översättningen i typteori. Vi definierar följande:

$$\begin{array}{l} \|\bot\| = \mathsf{N}_0 \\ \|\phi \dot{\to} \psi\| = \|\phi\| \to \|\psi\| \\ \|\phi \wedge \psi\| = \|\phi\| \times \|\psi\| \\ \|\phi \vee \psi\| = \|\phi\| + \|\psi\| \\ \|\forall x \dot{\in} a \phi(x)\| = (\Pi x \in \bar{a}) \|\phi(\tilde{a}(x))\| \\ \|\exists x \dot{\in} a \phi(x)\| = (\Sigma x \in \bar{a}) \|\phi(\tilde{a}(x))\| \\ \|\forall x \phi(x)\| = (\Pi x \in \mathsf{V}) \|\phi(x)\| \\ \|\exists x \phi(x)\| = (\Sigma x \in \mathsf{V}) \|\phi(x)\| \end{array}$$

Nu inses lätt att $\|\phi\|$ är en liten typ så fort ϕ är en begränsad formel. Detta eftersom $(\Pi x \in A)B(x)$ samt $(\Sigma x \in A)B(x)$ är små typer när A är en liten typ och B är en familj av små typer, och $\bar{a}$ är en liten typ för alla mängder a enligt den typteoretiska definitionen av mängder.

7.4 Likhet och element

De viktiga relationerna på mängder är extensionell likhet och element. Vi tar fasta på följande två fakta om likhets- och elementrelationen:

$$\begin{array}{lll} a \doteq b & \leftrightarrow & \forall x \dot{\in} a (x \dot{\in} b) \wedge \forall y \dot{\in} b (y \dot{\in} a) \\ a \dot{\in} b & \leftrightarrow & \exists y \dot{\in} b (y \doteq a) \end{array}$$

Utifrån detta kan vi definiera översättningen av dessa två relationer i typteori:

$$\begin{array}{lll} \|a \doteq b\| & =_{def} & (\Pi x \in \bar{a})\|\tilde{a}(x) \mathrel{\dot\in} b\| \times (\Pi y \in \bar{b})\|\tilde{b}(y) \mathrel{\dot\in} a\| \\ \|a \mathrel{\dot\in} b\| & =_{def} & (\Sigma y \in \bar{b})\|a \doteq \tilde{b}(y)\| \end{array}$$

Detta är dock en ömsesidig rekursion, vilket inte direkt kan uttryckas i typteori. Därför sätter vi in definitionen av $\mathrel{\dot\in}$ i definitionen av $\doteq$:

$$\|a \doteq b\| \;=_{def}\; (\Pi x \in \bar{a})(\Sigma y \in \bar{b})\|\tilde{a}(x) \doteq \tilde{b}(y)\| \times (\Pi y \in \bar{b})(\Sigma x \in \bar{a})\|\tilde{a}(x) \doteq \tilde{b}(y)\|$$

Detta är nu en dubbel rekursion som inte heller är direkt uttryckbar i typteori. Den formella definitionen blir då $\|a \doteq b\| = F(a)(b)$, där:

$$\begin{array}{lll} F(a) & =_{def} & setrec(\ a,\ \lambda A\, f\, h.\lambda b. \\ & & \quad (\Pi x \in A)(\Sigma y \in \bar{b})h(x)(\tilde{b}(y)) \times \\ & & \quad (\Pi y \in \bar{b})(\Sigma x \in A)h(x)(\tilde{b}(y))\ ) \in \mathsf{V} \to \mathsf{U} \end{array}$$

Elementrelationen definieras som ovan i termer av den nyss definierade likhetsrelationen:

$$\|a \mathrel{\dot\in} b\| \;=_{def}\; (\Sigma y \in \bar{b})\|a \doteq \tilde{b}(y)\|$$

7.5 Bevis av axiomen i CZF

Förutom att bevisa axiomens korrekthet i typteori, krävs även att man bevisar att likhetsrelationen är en ekvivalensrelation. Detta är dock ganska trivialt så vi lämnar detta, ett bevis finns i (Aczel 1978). Axiomen repeteras i början av varje bevis, för att underlätta läsandet och förståelsen av bevisen.

Mängdinduktion

$$\forall y(\forall x \mathrel{\dot\in} y\, \phi(x) \mathrel{\dot\to} \phi(y)) \mathrel{\dot\to} \forall x \phi(x)$$

Antag att vi har ett bevis h av förledet. Det betyder att h är ett objekt i typen $\|\forall y(\forall x \mathrel{\dot\in} y\, \phi(x) \mathrel{\dot\to} \phi(y))\|$. Enligt översättningen i sektion 7.3 är då h en funktion som tar ett $y \in \mathsf{V}$ och ger en funktion från typen $(\Pi x \in \bar{y})\|\phi(\tilde{y}(x))\|$ till typen $\|\phi(y)\|$. Men detta är precis vad som krävs av funktionen h i eliminationsregeln för V, förutom den lilla detaljen att där krävs att mängden y ges med sina komponenter $\bar{y}$ och $\tilde{y}$. Om vi då definierar funktionen h^* som $\lambda \bar{y}\, \tilde{y}.h(set(\bar{y}, \tilde{y}))$, ser vi att kraven i eliminationsregeln uppfylls:

$$h^*(\bar{y}, \tilde{y}, z) \in \|\phi(set(\bar{y}, \tilde{y}))\| \;\; [\ \bar{y} \in \mathsf{U},\ \tilde{y} \in \bar{y} \to \mathsf{V},\ z \in (\Pi x \in \bar{y})\|\phi(\tilde{y}(x))\|\ ]$$

Enligt eliminationsregeln kan vi nu, givet ett $a \in \mathsf{V}$, säga att $setrec(a, h^*)$ är ett bevis för $\|\phi(a)\|$. Men då är $\lambda x.setrec(x, h^*)$ ett bevis för $\|\forall x \phi(x)\|$, och slutligen $\lambda y\, x.setrec(x, y^*)$ ett bevis för Mängdinduktion.

Begränsad Separation

$$\forall a \exists \mathbf{d} \forall x(x \mathrel{\dot\in} \mathbf{d} \leftrightarrow x \mathrel{\dot\in} a \wedge \phi(x))$$

Givet mängden a och den begränsade formeln $\phi(x)$ kan vi definiera mängden:

$$\{\, x \mathrel{\dot\in} a \mid \phi(x)\,\} \;=_{def}\; set(\ \|\exists x \mathrel{\dot\in} a\, \phi(x)\|,\ g\ )$$

där $g(y) = \tilde{a}(fst(y))$. Detta är en korrekt definition av en mängd eftersom $\exists x \mathrel{\dot\in} a\, \phi(x)$ är en begränsad formel när $\phi(x)$ är begränsad. Då måste typen $\|\exists x \mathrel{\dot\in} a\, \phi(x)\|$ vara en liten typ enligt sektion 7.3. Denna typ består av par med $x \mathrel{\dot\in} a$ som förstakomponent och som dessutom uppfyller $\phi(x)$. Alltså är funktionen g korrekt då den tar förstakomponenten ur ett par och ger den motsvarande mängden.

Par

$$\forall ab \exists \mathbf{p}(a \mathrel{\dot\in} \mathbf{p} \wedge b \mathrel{\dot\in} \mathbf{p})$$

Givet mängderna a och b så kan vi definiera det oordnade paret som:

$$\{a, b\} =_{def} set(\mathsf{N}_2, f)$$

Funktionen $f \in \mathsf{N}_2 \to \mathsf{V}$ uppfyller här $f(0) = a$ och $f(1) = b$, vilket ger att $f = \lambda x.case_2(x, a, b)$.

Union

$$\forall a \exists \mathbf{u} \forall y \mathrel{\dot\in} a \forall x \mathrel{\dot\in} y(x \mathrel{\dot\in} \mathbf{u})$$

Givet mängden $a = set(A, f)$ så kan vi definiera unionen som:

$$\bigcup a =_{def} set(\ (\Sigma z \in A)\overline{f(z)},\ g\ )$$

Här är $g(\langle x, y\rangle) = \widetilde{f(x)}(y)$, dvs. $g = \lambda z.f(\widetilde{fst(z)})(snd(z))$. Att detta verkligen motsvarar unionen ses på följande sätt: Den definierade mängden är mängden av alla $\widetilde{f(x)}(y)$ för alla möjliga par $\langle x, y\rangle$, där $x \in A$ och $y \in \overline{f(x)}$. Här är x ett objekt i indextypen A, vilket gör att $f(x)$ är ett element i mängden a. Då är y ett objekt i indextypen till just det elementet, vilket i sin tur gör att $\widetilde{f(x)}(y)$ är ett element i ett element i a. Men eftersom den definierade mängden är mängden av alla möjliga sådana mängder, blir den mängden av alla element i något element i a, dvs. unionen.

Oändlighet

$$\exists \mathbf{n}(\exists x(x \mathrel{\dot\in} \mathbf{n}) \wedge \forall x \mathrel{\dot\in} \mathbf{n} \exists y \mathrel{\dot\in} \mathbf{n}(x \mathrel{\dot\in} y))$$

Mängden av de naturliga talen, $\mathbf{N}$, definieras med typen av de naturliga talen som indextyp. Men det behövs även en funktion $f \in \mathsf{N} \to \mathsf{V}$, som översätter varje typteoretiskt naturligt tal till motsvarande mängd:

$$\begin{aligned} f(0) &= \emptyset \\ f(s(n)) &= (f(n))^+ \end{aligned}$$

Här är $\emptyset$ den tomma mängden, som kan definieras som $set(\mathsf{N}_0, case_0)$, och x^+ efterföljaroperationen, definierad som brukligt enligt $x \cup \{x\}$. Funktionen f blir då $\lambda n.natrec(n, \emptyset, \lambda y\, x.x^+)$. Med hjälp av denna funktion kan vi nu definiera mängden av de de naturliga talen $\mathbf{N}$ till att vara:

$$\mathbf{N} =_{def} set(\mathsf{N}, f)$$

Utökad Substitution

$$\forall a(\forall x \mathrel{\dot\in} a\, \exists y\, \phi(x,y) \mathrel{\dot\rightarrow} \exists \mathbf{b}\, \phi'(a,\mathbf{b}))$$

Antag att vi har ett bevis för $\forall x \mathrel{\dot\in} a \exists y\, \phi(x,y)$, där $a = set(A,f)$ är en godtycklig mängd och $\phi(x,y)$ en formel. Det betyder att vi har ett bevisobjekt h i typen $(\Pi x \in A)(\Sigma y \in \mathsf{V})\|\phi(f(x),y)\|$. Men detta objekt är, enligt definitionerna av Π- och Σ-typerna, lika med $\lambda x.\langle g(x), i\rangle$ för något $g \in A \to \mathsf{V}$ och för något $i \in \|\phi(f(x),g(x))\|$. Det betyder att g är en funktion som tar ett objekt i indextypen A och ger en mängd, och att i är beviset för att ϕ gäller för denna mängd. Men då inses att för ett givet x är $g(x)$ det y vi söker, och vi kan definiera bildmängden b som:

$$b \;=_{def}\; set(A,g) \;=\; set(A, \lambda x.fst(h(x)))$$

Att bevisa att denna mängd verkligen är bildmängden är att visa $\phi'(a,b)$, vilket i sin tur är detsamma som att såväl $\forall x \mathrel{\dot\in} a \exists y \mathrel{\dot\in} b\, \phi(x,y)$ som $\forall y \mathrel{\dot\in} b \exists x \mathrel{\dot\in} a\, \phi(x,y)$ gäller. Men eftersom både a och b har samma indextyp A, och det finns funktioner f respektive g som givet ett index ger ett element i vardera mängden, och dessutom då $\|\phi(f(x),g(x))\|$ gäller för alla $x \in A$, så måste även $\phi'(a,b)$ gälla.

Delmängd

$$\forall ab \exists \mathbf{p} \forall u(\forall x \mathrel{\dot\in} a \exists y \mathrel{\dot\in} b\, \phi_u(x,y) \mathrel{\dot\rightarrow} \exists c \mathrel{\dot\in} \mathbf{p}\, \phi'_u(a,c))$$

Givna mängderna $a = set(A,f)$ och $b = set(B,g)$, så kan vi definiera en funktion $h \in (A \to B) \to \mathsf{V}$:

$$h(z) \;=_{def}\; set(A, \lambda x.g(z(x)))$$

Denna funktion ger alltså bilden, i form av en delmängd till b, av en given funktion z mellan indextyperna A och B. Samlingen av alla möjliga sådana delmängder är då en mängd av delmängder till b:

$$p \;=_{def}\; set(A \to B, h)$$

Antag nu att vi för en given mängd u har ett bevis för $\forall x \mathrel{\dot\in} a \exists y \mathrel{\dot\in} b\, \phi_u(x,y)$. Detta innebär att det finns ett objekt i typen $(\Pi x \in A)(\Sigma y \in B)\|\phi_u(f(x),g(y))\|$, vilket då är på formen $\lambda x.\langle s(x), t(x)\rangle$ för något s och t. Men s är ju en funktion av typen $A \to B$ och därför ett objekt i indextypen till p. Alltså är $c = h(s)$ ett element i mängden p, i själva verket bildmängden till ϕ_u.

För att visa att c verkligen är bildmängden till ϕ_u, ska vi visa att $\phi'_u(a,c)$ är sant, vilket ju är detsamma som att visa att både (i) $\forall x \mathrel{\dot\in} a \exists y \mathrel{\dot\in} c\, \phi_u(x,y)$ och (ii) $\forall y \mathrel{\dot\in} c \exists x \mathrel{\dot\in} a\, \phi_u(x,y)$ är sanna. Påstående (i) är trivialt eftersom $s(x)$ är just det y som får $\phi_u(x,y)$ att gälla enligt ovan. För påstående (ii) låter vi $y \mathrel{\dot\in} c$ vara givet. Men enligt definitionen av h så är detta y på formen $g(s(x))$ för något $x \in A$, och $f(x)$ är då ett element i a. Formeln som ska uppfyllas blir nu $\phi_u(f(x),g(s(x)))$, vilket ju är sant enligt ovan.

Därmed har vi visat att det för varje u finns en bildmängd av ϕ_u som ligger i mängden p.

8 Diskussion

I denna uppsats har visats hur man genom att förändra några axiom i den klassiska mängdteorin ZF kan få en konstruktiv variant CZF. Dessutom har det konstruktiva i teorin visats genom tolkning in i Martin-Löfs typeori.

I detta avslutande kapitel gås kortfattat igenom några frågor som kan ställas om konstruktiv mängdlära i allmänhet, och CZF i synnerhet.

8.1 Urvalsaxiom i CZF

Urvalsaxiomet säger för en given relation R att om det för alla x finns ett y som gör att relationen är uppfylld, så finns det en urvalsfunktion f som gör att x och $f(x)$ uppfyller relationen. Formellt blir det, givet en relation R så gäller:

$$\forall x \exists y (x R\, y) \rightarrow \exists f\, \forall x (x R\, f(x))$$

I klassisk Zermelo-Fraenkel brukar man ofta lägga till detta eller något liknande axiom. Den teori som då uppkommer brukar kallas för ZFC (efter det engelska "Axiom of Choice").

I typteori kan en variant av urvalsaxiomet bevisas, vilket betyder att det går att hitta ett objekt i typen:

$$(\Pi x \in A)(\Sigma y \in B) C(x, y) \rightarrow (\Sigma f \in A \rightarrow B)(\Pi x \in A) C(x, f(x))$$

Det innebär att det finns ett bevis för motsvarande påstående, och alltså är urvalsaxiomet bevisbart i typteori.

Däremot är inte urvalsaxiomet konsistent med CZF. Anledningen till detta är att extensionalitet tillsammans med urvalsaxiomet medför lagen om det uteslutna tredje, vilket visas i t.ex. (Beeson 1985). En viktig fråga blir då hur starka urvalsprinciper man kan tillföra utan att CZF blir icke-konstruktiv eller impredikativ. De vanligaste förslagen är "Countable Choice" och "Dependent Choice", vilka båda i princip säger att urvalsprincipen gäller för vissa mängder, t.ex. de naturliga talen. I (Aczel 1982) diskuteras vilka urvalsaxiom som är konsistenta med CZF, samt hur de resulterande utvidgningarna kan tolkas i typteori.

8.2 En möjlig utvidgning av CZF

I (Aczel 1986) diskuteras en ersättning av axiomet Delmängd, som kallas Reguljär Extension. Detta axiom gör CZF till en strikt starkare teori CZF^{+}. Axiomet är nödvändigt för att kunna definiera mängder induktivt, vilket är vanligt i såväl klassisk som konstruktiv matematik.

För att tolka detta nya axiom i typteori, behövs även typen $(\mathsf{W} x \in A) B(x)$ av välordningar eller träd över typerna A och B. Denna typ beskrivs i t.ex. (Nordström et al 1990), där det även beskrivs hur man definierar de ändliga typerna samt de naturliga talen med välordningar. Detta betyder att det räcker med typerna $(\Pi x \in A) B(x)$, $(\Sigma x \in A) B(x)$ och $(\mathsf{W} x \in A) B(x)$, samt universumet U.

8.3 Bevisteoretisk styrka

En viktig fråga är hur starkt ett system är. Vi har i kapitel 7 visat att CZF kan tolkas in i MLVU, vilket står för Martin-Löfs typteori med ett universum samt

typen V av mängder. Enligt ovan kan även den utökade teorin CZF^+ tolkas in i typteori, fast då i MLWU där W står för att typen av välordningar även är med. Detta betyder att typteori med ett universum är bevisteoretiskt minst lika starkt som konstruktiv mängdteori.

Frågan man genast ställer sig är huruvida typteori är starkare eller lika stark som mängdteori, dvs. om typteori kan tolkas in i mängdteori. Svaret på den frågan är nekande, men ett nästan lika bra resultat visas i (Aczel 1998).

Först visas att MLW, dvs. typteori med välordningar men utan universum, kan tolkas in i CZF^+. Sedan att man kan tolka MLWU i CZF^+ utökat med ett extra axiom som garanterar existensen av en ouppnåelig mängd enligt (Griffor et al 1998). Detta system, som vi kan kalla $\mathrm{CZF}^+\mathrm{u}$, kan i sin tur tolkas in i MLWU_2, dvs. typteori med två universa. MLWU_2 kan vidare tolkas in i $\mathrm{CZF}^+\mathrm{u}_2$ som kan tolkas in i MLWU_3 etc. ett uppräkneligt antal gånger.

Slutligen visas att systemen $\mathrm{CZF}^+\mathrm{u}_\omega$ och MLWU_ω kan tolkas in i varandra, där $\mathrm{CZF}^+\mathrm{u}_\omega$ är CZF^+ med ett uppränkeligt antal ouppnåeliga mängder, och MLWU_ω är Martin-Löfs typteori med ett uppräkneligt antal universa.

Till sist, eftersom Aczels tolkningar av mängdteori i typteori sker utan vare sig intensionell eller extensionell likhet, medan det är typteori med extensionell likhet som tolkas i mängdteori, så betyder det att följande teorier har samma bevisteoretiska styrka:

- $\mathrm{CZF}^+\mathrm{u}_\omega$ = konstruktiv mängdteori med ett uppräkneligt antal ouppnåeliga mängder
- MLWU_ω = Martin-Löfs typteori med ett uppräkneligt antal universa
- MLWU_ω med extensionell likhet

8.4 Är mängdteori konstruktiv?

En fråga som konsekvent har undvikits i uppsatsen är frågan om mängdteori verkligen är ett konstruktivt sätt att göra matematik på. Ett svar är att eftersom CZF kan tolkas in i typteori så är teorin konstruktiv. Men frågan kvarstår: är det egentligen så här man vill göra matematik såsom varande konstruktiv matematiker? Till syvende och sist blir det en fråga om personlig inställning.

Mitt personliga svar blir nog att det hela är en eftergift åt den klassiska matematiken — all klassisk matematik görs enligt Zermelo-Fraenkels mängdteori, och alltså kan man i många fall helt enkelt översätta de klassiska teoremen till en motsvariget i CZF. För att hårdra det så blir CZF ett system för de konstruktiva matematiker som tycker att det klassiska sättet att göra matematik är att föredra. Det vill säga för de matematiker som är konstruktivister i tanken men inte i själen.

Litteratur

Aczel, P. (1978). The type theoretic interpretation of constructive set theory. I *Logic Colloqium '77*. North-Holland.

Aczel, P. (1980). Frege strucures. I *The Kleene Symposium*. North-Holland.

Aczel, P. (1982). The type theoretic interpretation of constructive set theory: Choice principles. I *The L.E.J. Brouwer Centenary Symposium*. North-Holland.

Aczel, P. (1986). The type theoretic interpretation of constructive set theory: Inductive definitions. I *Logic, Methodology and Philosophy of Science VII*. North-Holland.

Aczel, P. (1997). Notes on constructive set theory. Artikeln finns att hämta på URL `<http://www.cs.man.ac.uk/~petera/index.html>`.

Aczel, P. (1998). On relating type theories and set theories. Artikeln finns att hämta på URL `<http://www.cs.man.ac.uk/~petera/index.html>`.

Beeson, M. J. (1985). *Foundations of constructive mathematics*. Springer-Verlag.

Bennet, C. (1996). *Något litet om mängder*. Institutionen för filosofi, Göteborgs Universitet.

Bennet, C., Haglund, B., och Westerståhl, D. (1986). *En introduktion till första ordningens logik*. Institutionen för filosofi, Göteborgs Universitet.

Griffor, E., Palmgren, E., och Rathjen, M. (1998). Inccessibility in constructive set theory and type theory. *Annals of Pure and Applied Logic*, vol 94.

Halmos, P. R. (1996). *Naive set theory*. D. van Norstrand.

Howard, W. A. (1969). The formulae-as-types notion of construction. Omtryckt i (Seldin och Hindley 1980).

Martin-Löf, P. (1972). An intuitionistic theory of types. Omtryckt i (Sambin och Smith 1998).

Martin-Löf, P. (1975). An intuitionistic theory of types: Predicative part. I *Logic Collocium '73*.

Martin-Löf, P. (1984). *Intuitionistic type theory*. Bibliopolis.

Myhill, J. (1975). Constructive set theory. *Journal of Symbolic Logic*, vol 40.

Nordström, B., Petersson, K., och Smith, J. M. (1990). *Programming in Martin-Löfs type theory*. Clarendon Press.

Palmgren, E. (1997). Constructive mathematics (course notes). Artikeln finns att hämta på URL `<http://www.math.uu.se/~palmgren/>`.

Sambin, G. och Smith, J., red (1998). *Twenty-five years of constructive type theory*. Clarendon Press.

Seldin, J. P. och Hindley, J. R., red (1980). *To H. B. Curry: Essays on combinatory logic, lambda calculus and formalism*. Academic Press.

Troelstra, A. S. och van Dalen, D. (1988). *Constructivism in mathematics I-II*. North Holland.

Zermelo, E. (1930). Über Grenzzahlen und Mengenbereiche. *Fundamenta Mathematicae*, vol 16.