

Matematik, KTH

Bengt Ek

december 2017

MATERIAL TILL KURSEN
SF1679, DISKRET MATEMATIK:

Om urvalsaxiomet mm

Vi har tidigare nämnt Zermelo-Fraenkels axiom för mängdläran, de upprepas på sista sidan av dessa blad. De kallas ofta ZFC , där C :et står för "Choice", dvs urvalsaxiomet, nr 9 i listan. Axiomen 1.–8., dvs ZFC utan C , kallas då ZF .

Urvalsaxiomet har tidvis varit omdebatterat och flera (kända) matematiker har vägrat acceptera det, eftersom det som vi skall beskriva kan användas för att bevisa oväntade och "paradoxala" resultat.

Axiom som är ekvivalenta med urvalsaxiomet

Det finns många påståenden som är ekvivalenta med urvalsaxiomet, dvs sådana att ZFC är ekvivalent med (har samma modeller som) ($ZF +$ vart och ett av dem). Vi upprepar först

URVALSAXIOMET: Om $\mathcal{F}$ är en familj av icke-tomma mängder, så finns en funktion $f: \mathcal{F} \rightarrow \cup \mathcal{F}$ sådan att $f(x) \in x$ för alla $x \in \mathcal{F}$.

Så man kan (i varje modell) "välja" ett element ur varje mängd i familjen.

VÄLORDNINGSPRINCIPEN: Varje mängd kan välordnas.

Det betyder att det för varje mängd x (dvs element i domänen för en modell för axiomen) finns en relation $\mathcal{R}$ (dvs en mängd av ordnade par) som är en välordning av x (vilket som vi minns innebär att varje icke-tom delmängd till x har ett $\mathcal{R}$ -minimalt element).

ZORNS LEMMA: Om $(P, \prec)$ är en partialordnad mängd och varje kedja i P har en övre begränsning, så har P ett maximalt element.

Här är en **kedja** i P en delmängd $C \subseteq P$ som är totalordnad av $\prec$, $u \in P$ är en **övre begränsning** till kedjan C om $c \prec u$ för alla $c \in C$ och $a \in P$ är ett **maximalt element** i P om det inte finns $x \in P$ med $a \prec x$.

TUKEYS LEMMA: Om en icke-tom familj mängder $\mathcal{F}$ har ändlig karaktär, så har $\mathcal{F}$ ett maximalt element (m.a.p. $\subseteq$).

Att $\mathcal{F}$ har **ändlig karaktär** betyder att en mängd x tillhör $\mathcal{F}$ omm varje ändlig delmängd till x tillhör $\mathcal{F}$. (Tukeys lemma är känt under flera namn, bl.a. Teichmüller, Bourbaki, Grothendieck, ensamma eller i kombinationer.)

Exempel: Om V är ett vektorrum har mängden av linjärt oberoende delmängder till V ändlig karaktär ($M \subseteq V$ är linjärt oberoende omm det för alla $\{\mathbf{v}_1, \dots, \mathbf{v}_k\} \subseteq M$ gäller att $\lambda_1 \mathbf{v}_1 + \dots + \lambda_k \mathbf{v}_k = \mathbf{0} \Rightarrow \lambda_1 = \dots = \lambda_k = 0$).

Tukeys lemma medför då att varje vektorrum har en maximal linjärt oberoende delmängd, dvs en bas (där en bas är en mängd med egenskapen att varje vektor i V är en **ändlig** linjärkombination av basvektorer, så inte detsamma som en bas i t.ex. ett hilbertrum).

En bas för $\mathbb{R}$ som vektorrum över $\mathbb{Q}$ kallas en **hamelbas**.

Sats (några urvalsaxiomsekvivalenter):

Följande påståenden är ekvivalenta (i ZF):

- (1) Urvalsaxiomet,
- (2) Välordningsprincipen,
- (3) Zorns lemma,
- (4) Tukeys lemma.

Ty: (skiss) (1) $\Rightarrow$ (2): Låt A vara en mängd. En välordning på A motsvarar precis en bijektion mellan A och ett ordinaltal (se längre fram i kursen) α . En sådan bijektion kan konstrueras rekursivt med hjälp av en urvalsfunktion f på $\mathcal{P}(A) \setminus \{\emptyset\}$ enligt $a_0 = f(A)$, $a_\xi = f(A \setminus \{a_\eta \mid \eta < \xi\})$ tills $\{a_\eta \mid \eta < \alpha\} = A$.

(2) $\Rightarrow$ (3): Om $(P, <)$ uppfyller förutsättningarna i Zorns lemma, välordna P med relationen $<$ och definiera rekursivt en följd mängder C_p , $p \in P$ enligt

$$C_p = \begin{cases} \bigcup_{q < p} C_q \cup \{p\} & \text{om } p \text{ är en övre begränsning för } \bigcup_{q < p} C_q, \\ \bigcup_{q < p} C_q & \text{annars.} \end{cases}$$

Kedjan $C = \bigcup_{p \in P} C_p$ (där $<$ och $\prec$ sammanfaller) har enligt förutsättning en övre begränsning, som tillhör C och är ett maximalt element i $(P, \prec)$.

(3) $\Rightarrow$ (4): Låt $\mathcal{F}$ vara en icke-tom familj mängder som har ändlig karaktär. $\mathcal{F}$ partialordnas av $\subseteq$ och om C är en kedja i $\mathcal{F}$ är $A = \bigcup C \in \mathcal{F}$ (varje ändlig delmängd ligger i ett element i C , så i $\mathcal{F}$) en övre begränsning till C . $\mathcal{F}$ har enligt Zorns lemma ett $\subseteq$ -maximalt element.

(4) $\Rightarrow$ (1): Låt $\mathcal{F}$ vara en familj av icke-tomma mängder. Vi söker en urvalsfunktion för $\mathcal{F}$. Låt

$$\mathcal{G} = \{f \mid f \text{ är en urvalsfunktion på någon mängd } \mathcal{E} \subseteq \mathcal{F}\}.$$

$\mathcal{G}$, partialordnad med $\subseteq$, har ändlig karaktär (en delmängd av en urvalsfunktion är en urvalsfunktion), så enligt Tukeys lemma har den ett maximalt element F , som är en urvalsfunktion på hela $\mathcal{F}$ (annars kunde den utvidgas). $\square$

Vi har tidigare använt Zorns lemma (utan att nämna det vid namn) för att visa att varje filter kan utvidgas till ett ultrafilter (unionen av en $\subseteq$ -kedja av filter är ett filter och ett maximalt filter är ett ultrafilter) och för att visa Gödels fullständighetssats (för att få en maximal konsistent sentensmängd Δ^*).

I båda fallen hade det räckt med ett lite svagare axiom, men det går vi inte in på här.

Är urvalsaxiomet rimligt?

En känd följd av urvalsaxiomet (och ett skäl till att en del vill förkasta det) ges av

Sats (Banach-Tarski):

Ett klot U kan partitioneras i två mängder $U = X \cup Y$, $X \cap Y = \emptyset$, så att $U \approx X$ och $U \approx Y$.

(Relationen $\approx$ mellan mängder $A, B \subseteq \mathbb{R}^3$ definieras här som att $A \approx B$ omm A och B kan partitioneras $A = A_1 \cup \dots \cup A_m$, $B = B_1 \cup \dots \cup B_m$ med A_i kongruent med B_i för $i = 1, \dots, m$. Satsen säger alltså att U kan delas upp i ett ändligt antal delar, som sedan kan sättas ihop till två kopior av U . Svårsmält, tycker många, men egentligen kanske inte så mycket värre än att $\mathbb{Z} = C \cup D$ (jämma och udda tal) och $|\mathbb{Z}| = |C| = |D|$, utom då att Banach och Tarski får geometrisk kongruens mellan bitarna.)

Vi bevisar inte satsen, men nämner att ett bevis kan grundas på en liknande uppdelning av en grupp G av rotationer i $\mathbb{R}^3$ som genereras av en rotation φ vinkeln π och en rotation ψ vinkeln $\frac{2\pi}{3}$ kring olika axlar, vilka valts så att alla element i G är **entydiga** (bortsett från att $\varphi^2 = 1$, $\psi^3 = 1$) produkter av φ, ψ (detta kallas att G är (isomorf med) **den fria produkten** av grupperna $\{1, \varphi\}$ och $\{1, \psi, \psi^2\}$).

Urvalsaxiomet kommer in genom att man bildar en mängd av precis ett element i var och en av G 's banor då den verkar på U och låter delarna av G verka på den.

Å andra sidan, med bara ZF (utan urvalsaxiomet) kan vi inte bevisa mycket som vi inte vill vara utan, t.ex. kan man konstruera en modell för ZF där

- $\mathbb{R}$ är en uppräknelig union av uppräkneliga mängder,
- $\mathbb{R}$ kan partitioneras i strikt fler delar än det finns element i $\mathbb{R}$ (sic!).

Kompakthetssatsen och följder

Som nämnt behövde vi (något lite svagare än) urvalsaxiomet för att visa Gödels fullständighetssats (för första ordningens predikatlogik). Vi skall här behandla en viktig följd av den, den s.k. kompakthetssatsen.

Sats (kompakthetssatsen):

En sentensmängd Δ har en modell omm varje **ändlig** $\Delta' \subseteq \Delta$ har en modell.

Ty: $\Delta \models \perp \Leftrightarrow \Delta \vdash \perp \Leftrightarrow \Delta' \vdash \perp$ för någon ändlig $\Delta' \subseteq \Delta \Leftrightarrow \Leftrightarrow \Delta' \models \perp$ för någon ändlig Δ' .

(Första och tredje $\Leftrightarrow$ från Gödels fullständighetssats, andra $\Leftrightarrow$ från att varje härledning är ändlig.)

Det ger att $\Delta \not\models \perp \Leftrightarrow \Delta' \not\models \perp$ för alla ändliga $\Delta' \subseteq \Delta$. $\square$

Alternativt, med ultraprodukt: ('Endast om' självklart, vi visar 'om'.)

Låt varje ändlig $\Delta' \subseteq \Delta$ ha modellen $\mathfrak{A}_{\Delta'}$ och $I = \{\Delta' \subseteq \Delta \mid \Delta' \text{ ändlig}\}$.

Om $I_\varphi = \{\Delta' \in I \mid \varphi \in \Delta'\}$ har $\{I_\varphi \mid \varphi \in \Delta\}$ äse (ändligskärningsegenskapen), så den kan utvidgas till ett ultrafilter $\mathcal{U}$. Då är $\mathfrak{A} = \prod_{\Delta' \in I} \mathfrak{A}_{\Delta'} / \mathcal{U}$ en modell för Δ , $\mathfrak{A} \models \Delta$, ty $\{\Delta' \in I \mid \mathfrak{A}_{\Delta'} \models \varphi\} \supseteq I_\varphi \in \mathcal{U}$ för alla $\varphi \in \Delta$. $\square$

Eftersom $\Gamma \models \varphi \Leftrightarrow \Gamma \cup \{\neg\varphi\} \models \perp$ för varje sentensmängd Γ och sentens φ , får vi som en direkt följd (också ofta kallad kompakthetssatsen):

Följdsats:

För varje sentensmängd Γ och sentens φ :

$$\Gamma \models \varphi \text{ omm } \Gamma' \models \varphi \text{ för varje ändlig } \Gamma' \subseteq \Gamma.$$

□

Exempel: En sentensmängd Γ som har godtyckligt stora ändliga modeller har en oändlig modell, ty om φ_n är sentenser som är sanna precis om domänen har minst $n \in \mathbb{Z}_+$ element (t.ex. $\varphi_2 : \exists x \exists y \neg x = y$), har $\Delta = \Gamma \cup \{\varphi_1, \varphi_2, \dots\}$ bara oändliga modeller och varje ändlig $\Delta' \subseteq \Delta$ har en modell.

Exempel (icke-standardmodeller för aritmetiken):

Vi visar att det finns andra modeller än $\mathfrak{N} = (\mathbb{N}, \{0, S, +, *\})$ för $T = \text{Th } \mathfrak{N}$. Inför en ny konstant c och sätt $\Delta = T \cup \{c \neq 0, c \neq S(0), c \neq S(S(0)), \dots\}$. Då har alla ändliga delmängder till Δ modeller, så det har Δ också. Om vi ”glömmer” konstanten c får vi en $\mathcal{L}_{\text{Peano}}$ -struktur $\mathfrak{M}$ med $\mathfrak{N} \preceq \mathfrak{M}$ med ett (och därmed många) element i domänen som inte svarar mot element i $\mathbb{N}$.

Exempel (utan självreferens på Knarrön):

I slutet av bladen om induktion påstods att det alltid finns minst en lösning till knarrögåtor där varje person gör högst ett uttalande och ingen självreferens (ens indirekt) förekommer (detta i motsats till Yabloos paradox, där uttalandena inte kan formuleras i första ordningens predikatlogik). Det är dags att visa det.

Låt person ι göra uttalandet $\phi_\iota(\{A_\kappa\}_{\kappa \in I})$ (där bara ett ändligt antal A_κ förekommer i ϕ_ι) och relationen $\mathcal{R}$ vara ”omtalas av”, som i induktionsbladen. Att ingen självreferens förekommer innebär precis att det inte finns några cykler i $\mathcal{R}$:s riktade graf. Men då har varje ändlig delmängd av sentenserna $A_\iota \leftrightarrow \phi_\iota(\{A_\kappa\}_{\kappa \in I})$ en modell (bara ett ändligt antal A_ι förekommer och då är $\mathcal{R}$ välgrundad omm det saknas cykler, så en lösning för A_ι bestäms rekursivt). Kompakthetssatsen ger att det finns en lösning till hela problemet.

Varför heter den kompakthetssatsen?

(Frivilligt avsnitt, för den som studerat topologi)

För den som är lite bevandrad i topologi kan det vara intressant att veta att kompakthetssatsen säger precis att mängden av (ekvivalensklasser av) $\mathcal{L}$ -strukturer är kompakt (dvs varje övertäckning av den med öppna mängder har en ändlig delövertäckning, eller (ekvivalent) om en uppsättning slutna mängder har äse, är skärningen av dem alla icke-tom) i en viss naturlig topologi.

Vi inför $S = \{[\mathfrak{A}]_\equiv \mid \mathfrak{A} \text{ en } \mathcal{L}\text{-struktur}\}$, ekvivalensklasser av $\mathcal{L}$ -strukturer (med $\mathfrak{A} \equiv \mathfrak{B}$ omm $\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{B} \models \varphi$ för alla φ), och $[\varphi] = \{[\mathfrak{A}] \in S \mid \mathfrak{A} \models \varphi\}$ för alla $\mathcal{L}$ -strukturer $\mathfrak{A}$ och låter de öppna mängderna i S vara alla unioner av $[\varphi]$:n, så de slutna mängderna är alla skärningar av $[\varphi]$:n (eftersom $[\varphi]^c = [\neg\varphi]$ är $[\varphi]$:na både öppna och slutna (S är ”fullständigt osammanhängande”, sammanhängande mängder är bara tomma mängden och mängder med bara ett element)). Då säger kompakthetssatsen att $\bigcap_{\varphi \in \Delta} [\varphi] \neq \emptyset \Leftrightarrow \bigcap_{\varphi \in \Delta'} [\varphi] \neq \emptyset$ för alla ändliga $\Delta' \subseteq \Delta$, dvs att S är kompakt.

Om stora strukturer

En önskan kunde vara att finna sentensmängder (axiom) som är sådana att alla modeller av dem är isomorfa, men följande klassiska sats visar att det inte är möjligt om det handlar om oändliga modeller.

Sats (Löwenheim-Skolem):

Om $\mathfrak{A}$ är en $\mathcal{L}$ -struktur, $C \subseteq A$ och κ ett oändligt kardinaltal:

- (1) Om $\max(|C|, |\mathcal{L}|) \leq \kappa \leq |A|$ finns $\mathfrak{B} \preceq \mathfrak{A}$ med $|B| = \kappa$, $C \subseteq B$,
- (2) om $\mathfrak{A}$ är oändlig och $\max(|A|, |\mathcal{L}|) \leq \kappa$ finns $\mathfrak{B}$ med $\mathfrak{A} \preceq \mathfrak{B}$ och $|B| = \kappa$.

Ty: 1. Tag C' med $C \subseteq C' \subseteq A$ och $|C'| = \kappa$ och lägg till alla element från A som satisfierar $\mathcal{L}$ -formler $\varphi(c_1, \dots, c_n, x)$ med $c_i \in C'$ i $\mathfrak{A}$. Unionen av alla dessa utvidgningar kallas B och visas ha kardinalitet κ .

$\mathfrak{B} \preceq \mathfrak{A}$ enligt konstruktionen.

2. Enligt kompakthetssatsen finns en $\mathcal{L}$ -struktur $\mathfrak{A}'$ som satisfierar $\text{Th}(\mathfrak{A}_A) \cup \{\neg k = k' \mid k, k' \in K\}$, där K med $|K| = \kappa$ är nya konstanter och $\text{Th}(\mathfrak{A}_A)$ är alla $\mathcal{L}$ -formler med element i A som konstanter. Då är $\mathfrak{A} \preceq \mathfrak{A}'$ och $|A'| \geq \kappa$. Tillämpa sedan 1. på $\mathfrak{A}'$ för $\mathfrak{A}$ och A för C . Det ger $\mathfrak{B} \preceq \mathfrak{A}'$, så $\mathfrak{A} \preceq \mathfrak{B}$, och $|B| = \kappa$. $\square$

ZERMELO-FRAENKELS AXIOM för mängder

Språk $\mathcal{L}_{\text{mgd}} = \{\in\}$

$\in$ en binär relationssymbol

1. Extensionalitet

Om x och y har samma element, så är $x = y$,

$$\forall x \forall y (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

2. Par

För alla x och y finns en mängd $\{x, y\}$ som innehåller precis x och y ,

$$\forall x \forall y \exists z \forall u (u \in z \leftrightarrow (u = x \vee u = y))$$

3. Separation

Om P är en egenskap (med en parameter q), så finns för varje x och q en mängd $y = \{z \in x \mid P(z, q)\}$ av alla $z \in x$ med egenskapen P ,

$$\forall x \forall q \exists y \forall z (z \in y \leftrightarrow (z \in x \wedge \phi(z, q)))$$

($\phi(z, q)$ en godtycklig $\mathcal{L}_{\text{mgd}}$ -formel (som definierar P))

4. Union

För varje mängd x finns en mängd $y = \bigcup x$, unionen av elementen i x ,

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists u (z \in u \wedge u \in x))$$

5. Potensmängd

För varje mängd x finns en mängd $y = \mathcal{P}(x)$, mängden av alla delmängder till x ,

$$\forall x \exists y \forall z (z \in y \leftrightarrow \forall u (u \in z \rightarrow u \in x))$$

6. Oändlighet

Det finns en oändlig mängd (en mängd som innehåller $\mathbb{N}$),

$$\exists x (\emptyset \in x \wedge \forall y (y \in x \rightarrow \bigcup \{y, \{y\}\} \in x))$$

($\emptyset$ existerar enligt 3. med $z \neq z$ som $\phi(z)$. $\{y\} = \{y, y\}$ existerar enligt 2.)

7. Substitution

Om f är en funktion, så finns för varje mängd x en mängd $y = \{f(y) \mid y \in x\}$

$$\forall p (\forall x \forall y \forall z ((\varphi(x, y, p) \wedge \varphi(x, z, p)) \rightarrow y = z) \rightarrow \forall x \exists y \forall z (z \in y \leftrightarrow \exists u (u \in x \wedge \varphi(u, z, p))))$$

(p en parameter, $\mathcal{L}_{\text{mgd}}$ -formeln φ definierar f)

8. Regularitet (välgrundning)

$\in$ är en välgrundad relation,

$$\forall x (x \neq \emptyset \rightarrow \exists y (y \in x \wedge \neg \exists z (z \in x \wedge z \in y)))$$

9. Urvalsaxiomet

Om $\emptyset \notin x$ finns en funktion f på x som väljer ett element från varje $y \in x$,

$$\forall x (\neg \emptyset \in x \rightarrow \exists f (f \text{ funk}(f) \wedge \forall y (y \in x \rightarrow f(y) \in y)))$$

($\text{funk}(f)$ är en $\mathcal{L}_{\text{mgd}}$ -formel som säger att f är en funktion, dvs en mängd ordnade par med $\forall x \forall y \forall z ((\langle x, y \rangle \in f \wedge \langle x, z \rangle \in f) \rightarrow y = z)$. $f(z)$ ges av $\langle z, f(z) \rangle \in f$.

$\langle a, b \rangle$ är $\{\{a\}, \{a, b\}\}$.)