Aksiom izbire

Odvisna izbira

V dokazu o karakterizaciji dobro osnovanih relacij smo uporabili

Aksiom odvisne izbire: Naj bo `A` neprazna množica in `R ⊆ A × A` celovita relacija, t.j.,

```
∀ x ∈ A . ∃ y ∈ A . x R y.
```

Tedaj obstaja zaporedje `a : N → A`, da za vse `n ∈ N` velja `a(n) R a(n+1)`.

Aksiom izbire

Aksiom odvisne izbire sledi iz aksioma izbire (tega ne bomo dokazali):

Aksiom izbire (AC): Vsaka družina nepraznih množic ima funkcijo izbire.

Povedano z drugimi besedami:

- formulacija AC: družina nepraznih množic ima funkcijo izbire
- vsaka surjekcija ima prerez ⇔ AC
- propaganda: The Banach–Tarski Paradox

Moč množic

Končne množice

Definicija: *Standardna* končna množica z `n` elementi je

```
[n] = {k ∈ N | k < n}
```

Torej:

```
[0] = {}
[1] = {0}
[2] = {0, 1}
[3] = {0, 1, 2}
```

Definicija: Množica je **končna**, če je izomorfna kaki standardni končni množici.

Velja naslednje (ne bomo dokazali): če je `A ≅ [m]` in `A ≅ [n]`, je `m = n`. Torej za končno množico `A` obstaja natanko en `n ∈ N`, da velja `A ≅ [n]`. Temu n pravimo **moč** množice `A`, saj nam pove, koliko elementov ima `A`. Moč množice `A` označimo z `|A|`.

Zakoni za moč množic:

```
|[n]| = n
```

```
|A × B| = |A| × |B|
```

$|A + B| = |A| + |B|$

$|B^A| = |B|^{|A|}$

Pravilo vključitve/izključitve:

$|A \cup B| = |A| + |B| - |A \cap B|$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|$

In podobno za unijo štirih ali več množic.

Neskončne množice in njihova moč

Definicija: Množica je **neskončna**, če ni končna.

Izrek: Množica A je neskončna natanko tedaj, ko obstaja injektivna preslikava $N \to A$.

Dokaz:

(⇒) Denimo da A ni končna. Injektivno preslikavo $e : N \to A$ definiramo s pomočjo akisoma odvisne izbire. Ker A ni izomorfna $[0]$, ni prazna, torej obstaja $e(0) \in A$. Denimo, da smo že definirali e kot injektivno preslikavo $[n] \to A$. Tedaj jo lahko razširimo na injektivno preslikavo $e : [n+1] \to A$ takole: ker e ni surjektivna (če bi bila, bi veljalo $A \cong [n]$), obstaja $x \in A$, ki ni v sliki e. Torej *izberemo* $e(n) \in A$, ki ni v sliki. Tako dobimo $e : N \to A$, ki je injektivna.

(⇐) Denimo, da obstaja injektivna preslikava $e : N \to A$. Če bi veljalo $A \cong [n]$, bi imeli izomorfizem $f : A \to [n]$. Tedaj bi bil $f \circ e : N \to [n]$ injektivna preslikava, ta pa ne obstaja (dokaz opustimo). □

Moč množic

Tudi neskončnim množicam želimo prirediti *moč*. Potrebujem taka "števila", da lahko vsaki množici A priredimo "število" $|A|$, ki pove, koliko elementov ima. Za končne množice so to kar naravna števila. Za splošne množice so to **kardinalna števila**. Zaenkrat še ne bomo povedali natančno, kaj kardinalna števila so. Lahko pa jih primerjamo med sabo, ne da bi zares vedeli, kaj so!

Definicija: Naj bosta A in B poljubni množici. Pravimo:

1. A ima enako moč kot B, pišemo $|A| = |B|$, ko obstaja bijektivna preslikava $A \to B$.
2. A ima moč manjšo ali enako B, pišemo $|A| \leq |B|$, ko obstaja injektivna preslikava $A \to B$.
3. A ima moč manjšo kot B, pišemo $|A| < |B|$, če velja $|A| \leq |B|$ in $|A| \neq |B|$.

Izrek: $|A| \leq |B|$ natanko tedaj, ko je $A = \emptyset$ ali obstaja surjekcija $B \to A$.

Dokaz.

(⇒) Denimo, da je $f : A \to B$ injektivna in $A \neq \emptyset$. Torej obstaja neki $x_0 \in A$. Tedaj definiramo surjektivno preslikavo $g : B \to A$ takole:

$$g(y) = x \iff f(x) = y \text{ ali } x = x_0.$$

(⇐) Denimo, da je A prazna ali obstaja surjekcija $f : B \to A$. Če je A prazna, je edina preslikava $\emptyset \to B$ injektivna. Če je $f : B \to A$ surjektivna, ima prerez, ki je injektivna preslikava. □

Cantorjev izrek

Izrek (Cantor): $|A| < |P(A)|$.

Dokaz:

Najprej dokažimo $|A| \leq |P(A)|$. Iščemo injektivno preslikava $f : A \to P(A)$. Vzemimo $f(x) = \{x\}$. Zlahka preverimo, da je f res injektivna.

Sedaj dokazujemo, da ne obstaja bijekcija $A \to P(A)$. Dokazali bomo, da ne obstaja surjekcija $A \to P(A)$, kar zadostuje. Denimo, da je $g : A \to P(A)$ poljbuna preslikava. Trdimo, da g ni surjekcija. Res, podmnožica

$$S = \{x \in A \mid x \notin g(x) \}$$

ni v sliki g. Če bi bila, bi za neki $y \in A$ veljalo $g(y) = S$, a to bi vodilo v protislovje:

1. velja $y \notin S$: če $y \in S$ potem $y \notin g(y) = S$ po definiciji S.
2. velja $\neg (y \notin S)$: če $y \notin S$ potem $y \notin g(y) = S$a. □

Števne in neštevne množice

Moč množice N označimo z $\aleph_0$. (Zaenkrat še vedno ne vemo, kaj točno so kardinalna števila, a privzemimo, da imamo kardinalno število $\aleph_0$, ki ustreza moči množice N.)

Definicija: Množica A je *števna*, če velja velja $|A| \leq \aleph_0$.

Definicija: Množica A je *neštevna*, če ni števna.

Izrek: Za vsako množico A so ekvivalentne naslednje izjave:

1. A je števna
2. obstaja injektivna preslikava $A \to N$
3. A je prazna ali obstaja surjektivna preslikava $N \to A$
4. obstaja surjektivna preslikava $N \to 1 + A$
5. A je končna ali izmoforna N

Dokaz.

(1 ⇒ 2) če je A števna, velja $|A| \leq \aleph_0 = |N$, torej obstaja injektivna $A \to N$ po definiciji relacije $\leq$.

(2 ⇒ 3) To sledi neposredno iz zgornjega izreka

(3 ⇒ 4) Denimo, da je A prazna ali obstaja surjektivna preslikava $N \to A$:

1. Če je $A = \emptyset$, potem seveda obstaja surjektivna preslikava $N \to 1 + A$, in sicer $n \mapsto \iota_1()$.

2. Če obstaja surjektivna preslikava $f : N \to A$, potem lahko definiramo surjektivno preslikavo $g : N \to 1 + A$ s predpisom

   $$g(0) = \iota_1()$$
   $$g(n) = \iota_2(f(n-1)) \text{ za } n > 1$$

(4 ⇒ 5) Denimo, da obstaja surjektivna preslikava $r : N \to 1 + A$. Dokazali bomo, da je A izomorfna N, če ni končna. Predpostavimo torej, da A ni končna. Preslikva r ima prerez $s : 1 + A \to N$, ki je seveda

injektivna preslikava. Preslikva $s \circ \iota_2 : A \to N$ je torej kompozitum injektivnih preslikav, zato je injektivna. Ker A ni končna, obstaja tudi injektivna preslikava $N \to A$. Po izreku Cantor-Schröder-Bernstein je torej A izomorfna N.

(5 ⇒ 1) Če je A končna, je števna, ker očitno velja $A = |[n]| \leq |N| = \aleph_0$. Če je A izomorfna N, potem seveda velja $|A| = |N| \leq |N| = \aleph_0$. □

Izrek: $N \times N \cong N$.

Pravimo, da je družina $A : I \to \mathrm{Set}$ **števna**, če je števna njena indeksna množica I.

Izrek: Unija števne družine števnih množic je števna.

Dokaz.

Najprej obravnavajmo unijo družine $A : N \to \mathrm{Set}$, kjer je A_n števna za vse $n \in N$. Tu uporabimo aksiom izbire, da dokažemo števnost unije. Za vsak $n \in N$ obstaja surjektivna preslikava $N \to A_n + 1$. Po aksiomu izbire obstaja preslikava

```
e : ∏_{n ∈ N} { f : N → A_n + 1 | f surjekcija }.
```

Definiramo $e' : N \times N \to 1 + \cup_n A_n$:

```
e'(n, k) = e(n)(k).
```

Trdimo, da je e' surjekcija iz $N \times N$ na $1 + \cup_n A_n$.

Nato obravnavamo še unijo družine $A : I \to \mathrm{Set}$, kjer je I števna in A_i števna za vsak $i \in I$. □

Cantor-Schröder-Bernsteinov izrek in zakon trihotomije

Izrek (Cantor-Schröder-Bernstein): Če obstajata injektivni preslikava $A \to B$ in $B \to A$, potem obstaja bijektivna preslikava $A \to B$.

Dokaz. Dokaz je v priloženi datoteki [csb.pdf](csb.pdf)

Posledica: Če $|A| \leq |B|$ in $|B| \leq |A|$, potem $|A| = |B|$.

Dokaz. To sledi neposredno iz izreka CSB in definicije $\leq$. □

Brez dokaza omenimo še, da velja **zakon trihotomije**: za vsaki množici A in B velja $|A| < |B|$ ali $|A| = |B|$ ali $|B| < |A|$, oziroma ekvivalentno

$$|A| \leq |B| \lor |B| \leq |A|.$$

Relacija $\leq$ potemtakem uredi moči množic linearno.

TODO: podaj referenco na dokaz (verjetno Prijateljeve Strukture 1).

Moč kontinuuma in Cantorjeva hipoteza

Vemo, da ima množica realnih števil R enako moč kot $P(N)$, potenčna množica naravnih števil (to boste naredili na vajah). Tej moči pravimo **moč kontinuuma** (ker je "kontinuum" tudi staro ime za R).

Že Goerg Cantor, utemelitelj teorije množic, še je vprašal naslednje vprašanje:

Cantorjeva hipoteza: Vsaka neštevna podmnožica realnih števil izomorfna `R`.

Povedano, z drugimi besedami, po moči ni nobene množice strogo med `N` in `R`. Cantorjeva hipoteza je ostala odprta dlje časa. Dokončno je Cohen pred dobrega pol stoletja dokazal naslednje:

Izrek (Cohen): Iz Zermelo-Fraenkelovih aksiomov teorije množic Cantorjeve hipoteze ne moremo niti dokazati niti ovreči.

Pravimo, da je Cantorjeva hipoteza **neodvisna** od aksiomov teorije množic.

Poznamo še posplošeno Cantorjevo hipotezo, ki se glasi:

Posplošena Cantorjeva hipoteza: Če je `|A| ≤ |B| ≤ |P(A)|`, potem je `|B| = |A|` ali `|B| = |P(A)|`.

Tudi posplošena Cantorjeva hipoteza je nedovisna od aksiomov teorije množic. Danes vemo zelo veliko o tej hipotezi in poznamo, še mnoge druge izjave o množicah, ki so neodvisne od Zermelo-Fraenkelovih aksiomov teorije množic. Ti veljajo za nekakšno uradno različičo teorije množic in jih bomo obravnavali na naslednjih predavanjih.