Kodiranje matematičnih objektov z množicami

Z množicami smo izrazili številne matematične objekte, na primer:

- preslikavo `f : A → B` lahko izrazimo kot funkcijsko relacijo med `A` in `B`, torej kot podmnožico `A × B`,
- kvocientna množica `A/R` je množica ekvivalenčnih razredov, ekvivalenčni razredi so spet množice,

Ali je možno vse matematične objekte predstaviti z množicami? Da!

Urejeni pari

Par `(x, y)` lahko predstavimo z množico `{{x}, {x,y}}`. Tako dobimo

```
A × B := { {{x}, {x,y}} | x ∈ A, y ∈ B }
```

Vsota

Elemente vsote `A + B` kodiramo takole:

```
ι₁(x) = (x, 0) = {{x}, {x,∅}}
ι₂(x) = (x, 1) = {{x}, {x,{∅}}}
```

Naravna števila

Na množicah definiramo operacijo naslednik:

```
x⁺ := x ∪ {x}
```

Naravna števila nato kodiramo tako, da za ničlo vzamemo ∅ in uporabljamo operacijo naslednik:

```
0 = ∅
1 = ∅⁺ = {0} = {∅}
2 = 1⁺ = {0, 1} = {∅, {∅}}
3 = 2⁺ = {0, 1, 2} = {∅, {∅}, {∅, {∅}}}
4 = 3⁺ = {0, 1, 2, 3} = {∅, {∅}, {∅, {∅}}, {∅, {∅}, {∅, {∅}}}}
...
```

Vidimo, da je vsako naravno število kar množica svojih predhodnikov.

Cela števila

Cela števila so kvocient `N × N`:

```
Z = (N × N)/~
```

kjer je

```
(a,b) ~ (c,d) ⇔ a + d = c + b.
```

Urejeni par `(a, b)` predstavlja razliko števil `a` in `b`.

Racionalna števila

Racionalna števila so kvocient:

$\mathbb{Q} = (\mathbb{Z} \times \{n \in \mathbb{N} \mid n > 0\})/\approx$

kjer je

$(a,m) \approx (b,n) \Leftrightarrow a\ n = b\ m.$

Realna števila

Realno število je Dedekindov rez, torej podmnožica $\mathbb{Q}$.

In tako naprej. Ne pravimo, da je kodiranje vseh matematičnih objektov z množicami vedno dobra ideja, vendar pa je dejstvo, da je to možno, pomembno spoznanje osnov matematike. Iz njega na primer sledi tole: če je teorija množic neprotislovna, potem je neprotislovna tudi vsa matematika, ki jo lahko kodiramo z množicami (torej več ali manj vsa običajna matematika).

Aksiomi teorije množic

Zermelo-Fraenkelovi aksiomi teorije množic:

1. **Ekstenzionalnost:** množici A in B, ki imata iste elemente, sta enaki.
2. **Neurejeni par**: za vsak x in y je $\{x, y\}$ množica, ki vsebuje natanko x in y:

   $\forall\ x\ y\ z\ .\ z \in \{x, y\} \Leftrightarrow z = x \vee z = y$

   Okrajšava: $\{x\} = \{x, x\}$.
3. **Unija:** za vsako množico A je $\cup\ A$ množica, ki vsebuje natanko vse elemente množic iz A

   $\forall\ A\ x\ .\ x \in \cup\ A \Leftrightarrow \exists\ B \in A\ .\ x \in B$
4. **Prazna množica:** množica $\varnothing$ nima elementa:

   $\forall\ x\ .\ x \notin \varnothing$
5. **Neskončna množica:** obstaja množica, ki vsebuje $\varnothing$ in je zaprta za operacijo naslednik ($x^+ = x \cup \{x\}$).

   $\exists\ A\ .\ \varnothing \in A \wedge \forall\ x \in A\ .\ x^+ \in A$
6. **Podmnožica:** za vsako množico A in formulo φ je $\{x \in A \mid \varphi(x)\}$ množica, ki vsebuje natanko vse element iz A, ki zadoščajo φ:

   $\forall\ y\ .\ y \in \{x \in A \mid \varphi(x)\} \Leftrightarrow \varphi(y)$
7. **Potenčna množica:** za vsako množico A je $P(A)$ množica, ki vsebuje natanko vse njene podmnožice:

   $\forall\ S\ .\ S \in P(A) \Leftrightarrow S \subseteq A$

8. Zamenjava: če je `A` množica in `f : A → Set` preslikava, je razred

   `{ y ∈ V | ∃ x ∈ A . y = f(x) }`

   množica.

9. **Dobra osnovanost:** relacija $\in$ je dobro osnovana.

10. **Aksiom izbire:** vsaka družina nepraznih množic ima funkcijo izbire

Aksiom izbire

Definicija: Veriga v delni urejenosti `(P, ≤)` je taka podmnožica `V ⊆ P`, ki je z $\leq$ linearno urejena, kar pomeni `∀ x y ∈ V . x ≤ y ∨ y ≤ x`.

Primeri:

- Če je `(P, ≤)` linearno urejena, je vsaka podmnožica veriga
- V `(P(Q), ⊆)` imamo neštevno verigo

  `V = {S ∈ P(Q) | S je doljna množica}`

  Množica `S ⊆ Q` je *doljna*, če velja `∀ x y ∈ Q . x ≤ y ∧ y ∈ Q ⇒ x ∈ Q`.

Zornova lemma: Če ima v delni urejenosti `(P, ≤)` vsaka veriga zgornjo mejo, potem ima `P` maksimalni element.

Dokaz: dokaz se naslanja na aksiom izbire in Bourbaki-Wittov izrek o negibnih točkah (glej spodaj). Naj bo `C` množica vseh verig v `P`. Uredimo jo z `⊆`. Na njej definiramo preslikavo `f : C → C`, ki razširi verigo, če ni maksimalna, sicer je ne spremeni (tu uporabimo izbiro):

- Če je `V ∈ C` maksimalna veriga v `P` (glede na `⊆`), definiramo `f(V) := V`.
- Če `V ∈ C` ni maksimalna veriga v `P`, potem obstaja tak `x ∈ P \ V`, da je `V ∪ {x}` spet veriga. V tem primeru *izberemo* tak `x` in definiramo `f(V) := V ∪ {x}`.

Po izreku Bourbaki-Witt ima `f` negibno vrednost `V ∈ C`. Ta `V` je maksimalna veriga `V`, saj bi sicer veljalo, da je `V = f(V) = V ∪ {x}` za neki `x ∉ V`, kar ni možno. Naj bo `m` zgornja meja za verigo `V`. Trdimo, da je `m` maksimalni element v `P`: denimo, da velja `m ≤ y` za `m ∈ P`. Ker je `V ∪ {y}` veriga, ki vsebuje maksimalno verigo `V`, sledi `V = V ∪ {y}`, od tod pa `y ∈ V` ter `y ≤ m`. Torej je `m = y` in `m` je res maksimalni element. □

Definicija: Naj bo `(P, ≤)` delna ureditev. Preslikava `f : P → P` je **progresivna**, ko velja `x ≤ f(x)` za vsak `x ∈ P`.

Opomba: progresivna preslikav ni nujno monotona (poiščite protiprimer!).

Izrek (Bourbaki-Witt): Naj bo `(P, ≤)` neprazna delna ureditev, v kateri ima vsaka veriga zgornjo mejo in `f : P → P` progresivna preslikava. Tedaj ima `f` negibno točko: to je tak `x ∈ P`, da velja `f(x) = x`.

Dokaz: opuščen.

Izrek: V teoriji množic *brez* aksioma izbire so naslednje izjave ekvivalentne:

1. Aksiom izbire

2. Zornova lema
3. Princip dobre urejenosti: vsaka množica ima dobro ureditev

Dokaz:

(1 ⇒ 2) Glej Zornovo lemo.

(2 ⇒ 3) Skica dokaza: naj bo A poljubna množica, ki jo želimo dobro urediti.

Definirajmo *delne* dobre ureditev množice A: to so pari (B,R), kjer je $B \subseteq A$ in $R \subseteq B \times B$ dobra ureditev na B. Za delni dobri ureditvi (B,R) in (C,Q) pravimo, da je (C,Q) *razširitev* (B,R), kadar velja $B \subseteq C$, $R \subseteq Q$ in še, da je B začetni segment v C, kar pomeni:

$$\forall\, x\ y \in C\colon\ x\ Q\ y \wedge y \in B \Rightarrow x \in B.$$

Kadar je (C,Q) razširitev (B,R), pišemo $(B,R) \preccurlyeq (C,Q)$. Naj bo P množica vseh delnih dobrih ureditev množice A,

$$P = \{\ (B, R)\ \mid\ B \subseteq A \text{ in } R \subseteq B \times B \text{ in } R \text{ je dobra ureditev } B\ \},$$

urejena z relacijo $\preccurlyeq$. Očitno je $\preccurlyeq$ delna ureditev. Trdimo, da imajo verige v P zgornje meje glede na $\preccurlyeq$: če je $V \subseteq P$ veriga dobro urejenih podmnožic A, je njena zgornja meja (D,S) kar unija po komponentah:

$$D := \bigcup \{B \mid (B, R) \in V\}$$
$$S := \bigcup \{R \mid (B, R) \in V\}$$

Preverimo, da velja $(D,S) \in P$. Očitno je (D,S) stroga linearna ureditev (vaja). Denimo, da bi v (D,S) imeli neskončno padajočo verigo

$$\ldots\ S\ x_3\ S\ x_2\ S\ x_1\ S\ x_0.$$

Obstaja $(B,R) \in V$, da je $x_0 \in B$. Potem bi bila $x_0, x_1, x_2, x_3, \ldots$ padajoča veriga v (B,R), kar ni možno, saj je (B,R) dobro urejena. Res, ker je $x_i \in V$, obstaja (C,Q), da je $x_i \in C$. Če velja $(B,R) \preccurlyeq (C,Q)$, potem $x_i \in B$ po definiciji $\preccurlyeq$. Če velja $(C,Q) \preccurlyeq (B,R)$, potem $x_i \in B$, ker velja $C \subseteq B$. Torej je (D,S) res delna ureditev P.

Preverimo še, da velja $(B,R) \preccurlyeq (D,S)$ za vsak $(B,R) \in V$. Denimo, da je $y \in D$, $x \in B$ in $y\ S\ x$. Obstaja $(C,Q) \in V$, da je $y \in C$. Če velja $(C,Q) \preccurlyeq (B,R)$, potem $y \in C \subseteq B$. Če pa velja $(B,R) \preccurlyeq (C,Q)$, potem je $y \in B$ po definiciji $\preccurlyeq$.

Po Zornovi lemi obstaja maksimalni element (B,R) v P. Trdimo, da je $B = A$. Če bi namreč obatajal $x \in B \setminus A$, bi lahko razširili (B,R) na večjo dobro ureditev tako, da bi dodali x na konec B:

$$(B \cup \{x\},\ R')$$

$$y\ R'\ z \Leftrightarrow z = x \wedge (y,z) \in R$$

To ni možno, ker je (B,R) maksimalna delna ureditev. Torej je res $A = B$ in našli so dobro ureditev A.

(3 ⇒ 1) Naj bo $A : I \to \mathrm{Set}$ družina neprazniih množic. Naj bo $<$ dobra ureditev na uniji $\bigcup A$. Ker so vse množice A_i neprazne, ima vsaka od njih prvi element glede na $<$. Torej lahko definiramo funkcijo izbire f s predpisom

$$f(i) = \text{prvi element } A_i. \ \square$$

Izrek: Vsak vektorski prostor ima vektorsko bazo.

Dokaz: Naj bo L vektorski prostor. Definiramo množico

P = { B ⊆ L | B je linearno neodvisna }.

Množico P delno uredimo z relacijo ⊆. Trdimo, da imajo verige v P zgornje meje: zgornja meja verige V ⊆ P, je kar njena unija ∪_(B ∈ V) B. Seveda je treba preveriti, da je unija verige linearno neodvisnih množic spet linearno neodvisna (vaja). Po Zornovi lemi obstaja maksimalni element v P, torej maksimalna linearno neodvisna množica B v L. To pa je seveda vektorksa baza za L. □