O aksiomu izbora, cipelama i čarapama

Aksiom izbora može se izreći u raznim ekvivalentnim formama. Dokazi ekvivalencije aksioma izbora npr. sa Zornovom lemom, ili pak sa Zermelovim teoremom o dobrom uređaju, vrlo su složeni (vidi npr. [1]). U ovom članku nećemo se baviti tim kompliciranim stvarima. Pokušat ćemo razmotriti neke jednostavne situacije u kojima za "izbor" elemenata (ne) trebamo aksiom izbora. Za ova naša razmatranja koristit ćemo sljedeće dvije (ekvivalentne) forme aksioma izbora:

(1) *Neka je $\{A_i : i \in I\}$ proizvoljna familija skupova, pri čemu je za svaki $i \in I$ skup A_i neprazan, te za sve različite $i, j \in I$ vrijedi $A_i \cap A_j = \emptyset$. Tada postoji skup B tako da je za svaki $i \in I$ skup $B \cap A_i$ jednočlan. Skup B se obično naziva* **izborni skup**.

(2) *Neka je $\{A_i : i \in I\}$ proizvoljna familija skupova, pri čemu je za svaki $i \in I$ skup A_i neprazan. Tada postoji funkcija $f : I \to \cup_{i \in I} A_i$ tako da za svaki $i \in I$ vrijedi $f(i) \in A_i$. Funkcija f se obično naziva* **funkcija izbora**.

U daljnjem tekstu umjesto "aksiom izbora" pisat ćemo kratko samo AC, što je skraćenica od engleskog naziva *axiom of choice*. Počet ćemo priču o AC sa sljedećim pitanjem:

> *Ako imamo konačno mnogo nepraznih u parovima disjunktnih skupova $A_1, \ldots, A_n$, je li nužno koristiti aksiom izbora kako bi se dokazalo da postoji skup B takav da je za svaki $i \in \{1, \ldots, n\}$ ispunjeno da je skup $A_i \cap B$ jednočlan?*

Uočimo da je navedeno pitanje ekvivalentno sa sljedećim:

> *Ako imamo konačno mnogo nepraznih skupova $A_1, \ldots, A_n$, je li nužno koristiti aksiom izbora kako bi se dokazalo da postoji funkcija izbora za tu familiju?*

Prije nego što obrazložimo da nije nužno koristiti AC za dokaz navedene tvrdnje, pokušat ćemo prvo objasniti što se smije koristiti osim AC. To su svi aksiomi Zermelo–Fraenkelove teorije skupova i pravila zaključivanja logike prvog reda. U daljnjem tekstu umjesto *Zermelo–Fraenkelova teorija* pišemo samo kratko "ZF teorija". Istaknimo najprije da sve tvrdnje u teoriji ZF iskazujemo koristeći samo sljedeće simbole:

a) $v_0, v_1, \ldots,$ (prebrojivo mnogo varijabli; obično koristimo oznake: $x, y, z, x_1, x_2, \ldots$)

b) $\neg, \wedge, \vee, \rightarrow, \leftrightarrow, \forall, \exists$ (logički veznici i kvantifikatori)

c) (), (pomoćni simboli: lijeva i desna zagrada, te zarez)

d) simbol $=$ za jednakost, te simbol $\in$ za relaciju "biti element"

Sada navodimo aksiome ZF teorije.

(1) *Aksiom ekstenzionalnosti:* $\forall z(z \in x \leftrightarrow z \in y) \to x = y$

(2) *Aksiom praznog skupa*: $\exists x \forall y(\neg(y \in x))$.
Iz aksioma ekstenzionalnosti slijedi da je skup s tim svojstvom jedinstven. Iz tog razloga smijemo alfabetu teorije ZF dodati novi konstantski simbol: $\emptyset$.

(3) *Aksiom para*: $\forall x \forall y \exists z \forall u\Big(u \in z \leftrightarrow (x = u \lor y = u)\Big)$
Ako su x i y skupovi tada iz ovog aksioma slijedi da postoji skup čiji su jedini elementi x i y. Iz aksioma ekstenzionalnosti slijedi da je takav skup jedinstven. To nam daje za pravo da alfabetu teorije ZF dodamo novi dvomjesni funkcijski simbol kojeg označavamo sa $\{,\}$. Tada skup čiji su jedini elementi x i y označavamo sa $\{x, y\}$. Umjesto $\{x, x\}$ kratko pišemo $\{x\}$.

(4) *Aksiom unije*: $\forall x \exists y \forall z\Big(z \in y \leftrightarrow \exists t(t \in x \land z \in t)\Big)$
Primjenom aksioma ekstenzionalnosti slijedi da je skup y, čija egzistencija se tvrdi u aksiomu unije, jedinstven. Iz tog razloga opet smijemo alfabetu teorije ZF dodati novi jednomjesni funkcijski simbol kojeg označavamo sa $\cup$. Za dani skup x sa $\cup x$ označavamo skup čiji su elementi zapravo elementi elemenata od x, a čija se egzistencija tvrdi u ovom aksiomu.

Ako su x i y skupovi tada iz aksioma para slijedi egzistencija skupa $\{x, y\}$. Iz aksioma unije slijedi da je $\cup\{x, y\}$ također skup. Obično taj skup zapisujemo standardno sa $x \cup y$.

(5) *Aksiom partitivnog skupa*

Kako bismo ovaj aksiom iskazali u jasnijem i kraćem obliku uvodimo pokratu $x \subseteq y$ za formulu $\forall z(z \in x \to z \in y)$. Tada je *aksiom partitivnog skupa* sljedeća formula:

$$\forall x \exists y \forall z(z \in y \leftrightarrow z \subseteq x).$$

Ovaj aksiom jednostavno tvrdi da svi podskupovi nekog skupa opet čine skup.

(6) *Aksiom beskonačnosti*: $\exists x\Big(\emptyset \in x \land \forall y(y \in x \to y \cup \{y\} \in x)\Big)$
Iz ovog aksioma slijedi da postoje beskonačni skupovi.

(7) *Shema aksioma separacije*: $\forall x_1 \ldots \forall x_n \forall x \exists y \forall z\Big(z \in y \leftrightarrow (z \in x \land F(z, x_1, \ldots, x_n))\Big)$,
gdje je F proizvoljna formula teorije ZF u kojoj ne nastupaju varijable x i y. Ovaj aksiom izriče da iz svakog skupa možemo odvojiti, odnosno separirati, podskup koji ima neko dano svojstvo F. Varijable $x_1, \ldots, x_n$ možemo shvatiti kao parametre. Skup, čija se egzistencija tvrdi ovim aksiomom, označavamo sa $\{z \in x : F(z, x_1, \ldots, x_n)\}$.

(8) *Shema aksioma zamjene*:

$$\forall t_1 \ldots \forall t_k \Big(\forall x \exists! y F(x, y, t_1, \ldots, t_k) \rightarrow$$

$$\forall u \exists v \forall z (z \in v \leftrightarrow \exists w (w \in u \land F(w, z, t_1, \ldots, t_k))) \Big),$$

gdje je F proizvoljna formula teorije ZF, dok su u i v različite varijable koje su različite od x, y, z, $t_1, \ldots, t_k$ i w.

U prvom dijelu aksioma je zapisana "funkcionalnost" formule F, tj. ističe se da nas zanimaju formule koje opisuju neku "funkciju". Zatim se u drugom dijelu aksioma tvrdi da je slika skupa također skup (tj. ako je u skup tada je i slika skupa u, obzirom na "funkciju" koju definira formula F, također skup).

(9) *Aksiom dobre utemeljenosti*: $\forall x (x \neq \emptyset \rightarrow \exists y \Big(y \in x \land y \cap x = \emptyset) \Big)$,
gdje je $y \cap x$ pokrata za $\{z : z \in y \text{ i } z \in x\}$.
Ovaj aksiom tvrdi da ne postoji beskonačni niz skupova $(x_n)_{n \in \mathbb{N}}$ takav da za svaki $n \in \mathbb{N}$ vrijedi $x_{n+1} \in x_n$. Odatle pak posebno slijedi da ne postoji skup x za kojeg vrijedi $x \in x$.

Već smo naveli da Zermelo–Fraenkelovu teoriju skupova označavamo kratko sa ZF. Uočite da aksiom izbora nismo uključili u popis aksioma. Uobičajeno je teoriju, čiji su aksiomi oni teorije ZF i aksiom izbora, označavati sa ZFC.

Važno je još naglasiti da u Zermelo–Fraenkelovoj teoriji skupova možemo definirati prirodne brojeve, za koje možemo dokazati da zadovoljavaju sve Peanove aksiome. Vrijedi i shema aksioma matematičke indukcije (treba biti pažljiv; to nije isto što i aksiom matematičke indukcije). Primjenom prirodnih brojeva možemo definirati pojam konačnog skupa, a onda i beskonačnog skupa. Za sve to nam ne treba AC.[1]

Bili smo na početku spomenuli da se u dokazima osim aksioma teorije ZF, koje smo upravo bili naveli, smiju koristiti i pravila zaključivanja logike prvog reda. Ovdje nećemo strogo definirati što je logika prvog reda (vidi npr. [5]). Kratko ćemo samo reći da pravila zaključivanja logike prvog reda sadrže sva uobičajna pravila zaključivanja koja se koriste u dokazima na diplomskim studijima matematike.

Što zapravo znači dokazati da za neku familiju skupova $\{A_i : i \in I\}$ postoji izborna funkcija? U ZF to znači dokazati da postoji neka formula $\varphi(v_0, v_1, \ldots, v_k)$ teorije ZF sa $k+1$ slobodnom varijablom, za neki $k \in \mathbb{N}$, te postoje skupovi $b_1, \ldots, b_{k-1}$ tako da je u teoriji ZF dokaziva formula $(\forall i \in I)(\exists! a \in A_i)\varphi(a, b_1, \ldots, b_{k-1}, i)$. No, dokazi se gotovo nikad ne provode tako formalno. Ako je neki dokaz "sumnjiv" tada se navođenjem aksioma teorije ZF pokušava opravdati određen korak u dokazu.

[1] Međutim, za Dedekindovu karakterizaciju: *Skup je beskonačan ako i samo ako je ekvipotentan s nekim svojim pravim podskupom*, kao i za neke jednostavne posljedice, treba nam AC.

Pošto ćemo u daljnjim razmatranjima često koristiti činjenicu da iz svakog nepraznog skupa možemo bez aksioma izbora izabrati jedan element, sada to posebno promotrimo.

Tvrdnja 1. Iz svakog nepraznog skupa A u teoriji ZF skupa možemo izabrati jedan element.

Mogli bismo zapravo jednostavno reći da nepraznost skupa A znači da sadrži barem jedan element. No, pokušat ćemo danu tvrdnju nešto formalnije argumentirati. Primjenom aksioma para i sheme aksioma zamjene slijedi da je $\{\{x\} : x \in A\}$ neprazan skup. Očito je svaki element tog skupa jedan izborni skup familije $\{A\}$.

Obično u matematici umjesto izreke kao u tvrdnji 1 koristimo sljedeću formu: "*Neka je $y \in A$ proizvoljan, ali fiksiran*".

Sada ćemo dati odgovor na postavljeno pitanje sa samog početka ovog članka, tj. kako samo pomoću aksioma ZF teorije možemo dokazati egzistenciju funkcije izbora za svaku konačnu familiju $\{A_i, \dots, A_n\}$ nepraznih skupova.

Indukcijom po n dokazujemo da za svaki $n \in \mathbb{N}$ i svaku familiju $\{A_1, \dots, A_n\}$ nepraznih skupova postoji izborna funkcija.

Promotrimo prvo slučaj kada je $n = 1$. Po pretpostavci je skup A_1 neprazan. Neka je $a_1 \in A_1$ proizvoljan element (vidi prije dokazanu Tvrdnju 1). Definiramo funkciju $f : \{1\} \to A_1$ sa $f(1) = a_1$. Očito je f jedna tražena funkcija izbora.

Pretpostavimo sada da smo za neki $k \in \mathbb{N}$ i svaku k–članu familiju nepraznih skupova dokazali da tvrdnja vrijedi. Neka je $\{A_1, \dots, A_n, A_{n+1}\}$ neka familija nepraznih skupova. Iz pretpostavke indukcije slijedi da postoji funkcija $f : \{1, \dots, n\} \to \cup_{i=1}^{n} A_i$ takva da za svaki $i \in \{1, \dots, n\}$ vrijedi $f(i) \in A_i$. Po pretpostavci je skup A_{n+1} neprazan. Neka je $x \in A_{n+1}$ proizvoljan, ali fiksiran (vidi dokazanu tvrdnju 1). Definiramo proširenje g funkcije f na skup $\{1, \dots, n+1\}$ stavljajući $g(n+1) = x$. Očito je g jedna izborna funkcija za familiju $\{A_1, \dots, A_{n+1}\}$.

Prethodno smo promatrali jedan poseban slučaj familije skupova (konačna familija beskonačnih skupova). Sada želimo promotriti razne slučajeve. Za svaku od sljedećih familija skupova postavljamo pitanje možemo li egzistenciju fukcije izbora dokazati u ZF bez korištenja aksioma izbora, te odmah odgovaramo na postavljena pitanja.

a) konačna familija nepraznih konačnih skupova.
Uočimo da je ovo specijalni slučaj prethodno dokazane tvrdnje. No, navest ćemo ideju alternativnog dokaza za ovaj slučaj. Nije potreban aksiom izbora kako bi se dokazala egzistencija funkcije izbora. Neka su $A_1, \dots, A_n$ konačni skupovi. Iz teorema o uzastopnom prebrojavanju slijedi da je $k(A_1 \times \ldots \times A_n) = k(A_1) \cdot \ldots \cdot k(A_n) > 0$ (teorem se inače dokazuje indukcijom). To znači da je skup $A_1 \times \ldots \times A_n$ neprazan, tj. da postoji barem jedna izborna funkcija.

b) beskonačna familija jednočlanih skupova;
Nije potreban aksiom izbora kako bi se dokazala egzistencija funkcije izbora. Neka je $\{\{x_i\} : i \in I\}$ familija skupova, gdje je I beskonačan skup. Neka je $f : I \to \cup_i \{x_i\}$ definirana sa $f(i) = x_i$ (primjenom aksioma teorije ZF nije teško argumentirati da je

f stvarno dobro definirana funkcijska relacija). Očito je f jedna funkcija izbora dane familije.

c) beskonačna familija (proizvoljnih) dvočlanih skupova.
Općenito nije moguće dokazati egzistenciju funkcije izbora bez primjene aksioma izbora.

d) prebrojiva familija beskonačnih skupova.
Općenito nije moguće dokazati egzistenciju funkcije izbora bez primjene aksioma izbora. U tzv. Cohenovom modelu N postoji prebrojiv (gledano u modelu) skup skupova realnih brojeva za koji ne postoji izborna funkcija.

e) beskonačna familija dvočlanih skupova realnih brojeva.
Nije potreban aksiom izbora kako bi se dokazala egzistencija funkcije izbora. Svakom elementu familije pridružimo njegov najmanji element (možemo i najveći). Važno je istaknuti da se u teoriji ZF može definirati skup realnih brojeva, te relacija uređaja $<$ na njemu. Iz toga slijedi da se u teoriji ZF može izraziti pojam "biti najmanji element nekog podskupa od $\mathbb{R}$".

f) beskonačna familija konačnih podskupova od $\mathbb{R}$.
Nije potreban aksiom izbora kako bi se dokazala egzistencija funkcije izbora. Objašnjenje je analogno onom iz prethodnog pitanja.

h) familija svih nepraznih podskupova skupa $\mathbb{N}$
Za dokaz egzistencije funkcije izbora nije potreban aksiom izbora. Jednostavno svakom nepraznom podskupu skupa $\mathbb{N}$ pridružimo njegov najmanji element. Važno je istaknuti da se u teoriji ZF može definirati relacija uređaja $<$ na skupu prirodnih brojeva, te se mogu dokazati razna njena svojstva. Posebno, u teoriji ZF se može dokazati da svaki neprazni podskup skupa prirodnih brojeva ima najmanji element.

Sada navodimo razne “dokaze” u kojima se ne koristi AC (tako se bar čini na prvi pogled).

“Dokaz” da svaki beskonačan skup sadrži prebrojiv podskup.

> *Neka je A proizvoljan beskonačan skup.*
>
> *Prvo ćemo indukcijom dokazati da za svaki $k \in \mathbb{N}$ postoji k–člani podskup A_k skupa A.*
>
> *Kako je po pretpostavci skup A beskonačan tada je posebno $A \neq \emptyset$. Sa a_1 označimo proizvoljan, ali fiksirani element skupa A. Iz aksioma para slijedi da je tada $\{a_1\}$ skup, pa smo dokazali da postoji jednočlani podskup skupa A.*
>
> *Pretpostavimo da je $n \in \mathbb{N}$ takav da postoji n–člani podskup skupa A. Neka je A_n neki n–člani podskup skupa A. Pošto je po pretpostavci skup A beskonačan tada je očito $A \setminus A_n \neq \emptyset$, pa postoji neki element $a_{n+1} \in A \setminus A_n$. Iz aksioma para i aksioma unije slijedi da je $A_n \cup \{a_{n+1}\}$ skup, koji je jedan traženi $(n+1)$–člani podskup skupa A.*
>
> *Sada definiramo $A' = \cup_k A_k$. Očito je A' prebrojiv podskup skupa A.*

Komentar prethodnog “dokaza”. Dokazano je da je za dokaz tvrdnje da beskonačan skup sadrži prebrojiv skup nužno koristiti AC. U prethodnom“dokazu” na samom kraju koristili smo da postoji familija skupova $\{A_k : k \in \mathbb{N}\}$, gdje je svaki skup A_k neki k–člani podskup skupa A. No, mi smo prethodno samo bili dokazali da za svaki $k \in \mathbb{N}$ imamo k–člani podskup skupa A.

“Dokaz” da se iz svakog beskonačnog skupa S parova čarapa može formirati skup koji sadrži točno jednu čarapu iz svakog para.

> *Iz svakog para nasumično izaberemo po jednu čarapu. Time smo dobili novu hrpu čarapa. Pošto smo na početku bili pretpostavili da je S skup, tada je očito i nova hrpa skup.*

Kometar prethodnog “dokaza”. Naravno, opravdani prigovor može biti da čarapa nije skup, pa ni hrpa parova čarapa nije skup. Ovim primjerom želi se istaknuti da ako imamo beskonačni skup neuređenih dvočlanih skupova tada općenito ne možemo formirati izborni skup bez uporabe AC. Možemo samo primijetiti da je nasumično biranje po jedne čarape iz svakog para svakako “sumnjivo”, tj. u aksiomima teorije ZF ne nalazimo opravdanje za takav postupak. Spomenimo još da je B. Russell uz ovu priču o beskonačnom skupu parova čarapa naveo i kao primjer beskonačni skup parova cipela iz kojeg bez primjene aksioma izbora možemo iz svakog para izabrati po jednu cipelu (npr. iz svakog para biramo lijevu cipelu).

"Dokaz" dijagonalnim postupkom da je unija prebrojivo mnogo prebrojivih skupova također prebrojiv skup.

Neka je $\{A_i : i \in \mathbb{N}\}$ familija prebrojivih skupova. Kako je svaki skup A_i prebrojiv, tada njegove elemente možemo poredati u niz: $A_i = \{a_i^0,\ a_i^1,\ a_i^2,\ a_i^3, \ldots\}$. Sada definiramo bijekciju $f : \cup_i A_i \to \mathbb{N}$ dijagonalnim postupkom ovako:

$$f(a_i^k) = \Big(\sum_{j=1}^{i+k} j\Big) \ + \ i+1 = \frac{1}{2}(i+k)\cdot(i+k+1) \ + \ i+1$$

Lako je provjeriti da je funkcija f bijekcija, pa smo dokazali da je unija $\cup_i A_i$ prebrojiv skup.

Komentar prethodnog "dokaza". Nakon što smo svaki skup A_i napisali u obliku $A_i = \{a_i^0,\ a_i^1,\ a_i^2,\ a_i^3, \ldots\}$, tada je ostatak dokaza konstruktivan, tj. više nije nužno koristiti AC. No, primjena aksioma izbora je upravo skrivena odabirom nizanja elemenata svakog skupa A_i.

Literatura

Literatura

[1] F. M. Brückler, V. Čačić, M. Doko, M. Vuković, Zbirka zadataka iz teorije skupova, PMF–MO, Zagreb, 2008., http://web.math.hr/∼vukovic

[2] P. Cohen, Set theory and the continuum hypothesis, Addison-Wesley, 1966.

[3] T. Jech, Set Theory, The Third Millennnium Edition, Springer, 2002.

[4] W. Just, M. Weese, Discovering Modern Set Theory I, AMS, 1996.

[5] M. Vuković, Matematička logika, Element, Zagreb, 2009.