ERDÖS-KO-RADOJEV IZREK

TJAŽ SILOVŠEK

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Članek obravnava Erdös-Ko-Radojev izrek s področja ekstremalne kombinatorike, ki podaja zgornjo mejo za velikost družin množic z določenimi lastnostmi. Za konec se pokaže s kakšnimi konstrukcijami družin je zgornja meja dosežena in kdaj jo je mogoče doseči le na en način.

ERDÖS-KO-RADO THEOREM

The article presents the Erdös-Ko-Rado Theorem from the area of extremal combinatorics. The theorem establishes the upper limit for the size of family of sets with certain properties. At the end of the paper it is also shown how to construct our families in order to reach the upper limit, and when the upper limit can be reached in only one way.

1. Uvod

Kombinatorika je matematična disciplina, ki preučuje končne ali števne diskretne strukture ter ugotavlja, na koliko načinov je možno razporediti, preurediti oziroma izbrati določeno množico elementov iz množice s končno mnogo elementi. Elementi so lahko poljubni, na primer: osebe, predmeti, števila, ki se jih označi s simboli, števkami, črkami, barvami in podobno. Erdös-Ko-Radojev izrek sodi v področje ekstremalne kombinatorike, ki se ukvarja z iskanjem »največjih«, »najmanjših« ali »optimalnih« objektov. Preden povemo kaj več o izreku, si pripravimo osnovne pojme in definicije, ki jih bomo kasneje potrebovali.

2. Erdös-Ko-Radojev Izrek

Zanimale nas bodo družine k-elementnih podmnožic množice U, za katere velja, da imata poljubni množici iz družine neprazen presek.

Definicija 1. Družina k-elementnih podmnožic množice U je *presečna k-družina*, če imata poljubni množici neprazen presek.

$$\mathcal{F} \text{ presečna k-družina} \iff \forall A, B \in \mathcal{F},\ A \cap B \neq \emptyset$$

Z $[n]$ bomo označevali množico, ki vsebuje prvih n naravnih števil, torej $[n] = \{1, 2, \ldots, n-1, n\}$. Zdaj si bomo pogledali primere presečnih k-družin.

Primer 1.

$$\begin{aligned}
U &= [4] \\
\mathcal{A} &= \{\{1,2,3\},\{2,3,4\},\{1,3,4\}\} \\
\mathcal{B} &= \{\{1,2\},\{2,3\},\{3,1\}\} \\
\mathcal{C} &= \{\{1\},\{2\},\{3\}\} \\
\mathcal{D} &= \{\{1,3\},\{2,3\},\{1,2\},\{2,4\}\}
\end{aligned}$$

$\mathcal{A}$ je presečna 3-družina, $\mathcal{B}$ presečna 2-družina, $\mathcal{C}$ pa ni presečna 1-družina, saj sta $\{1\}$, $\{2\} \in \mathcal{C}$ in $\{1\} \cap \{2\} = \emptyset$. Tudi družina $\mathcal{D}$ ni presečna 2-družina, saj imata množici $\{1,3\}$ in $\{2,4\}$ prazen presek.

Vemo, kaj so presečne k-družine podmnožic množice $[n]$, zdaj pa nas zanima, kako velike so lahko takšne družine.

Najprej si poglejmo primer, ko velja $n < 2k$. Takrat imata poljubni k-elementni množici skupaj $2k$ elementov. Ker je vseh elementov $n < 2k$, imata po Dirichletovem načelu ti množici neprazen presek. Poljubna k-družina bo v tem primeru presečna. Maksimalna družina torej vsebuje vse k-elementne podmnožice množice $[n]$, teh pa je natanko $\binom{n}{k}$.

V primeru, ko je $n \geq 2k$, nam na vprašanje odgovori naš glavni izrek.

Izrek 1 (Erdös–Ko–Rado). *Naj bo $\mathcal{A}$ presečna k-družina podmnožic množice $[n]$, kjer je $n \geq 2k$. Tedaj je*

$$|\mathcal{A}| \leq \binom{n-1}{k-1}. \tag{1}$$

Z izrekom se spoznajmo s pomočjo primera.

Primer 2.

$$\begin{aligned} U &= [4] \\ \mathcal{A} &= \{\{1,2\},\{2,3\},\{3,1\}\} \\ \mathcal{B} &= \{\{3\}\} \end{aligned}$$

Družina $\mathcal{A}$ je presečna 2-družina, ki dosega zgornjo mejo izreka; $\binom{4-1}{2-1} = 3$. Tudi družina $\mathcal{B}$ je presečna 1-družina in dosega zgornjo mejo izreka; $\binom{4-1}{1-1} = 1$.

Preden se lotimo dokaza izreka, si bomo pripravili še nekaj dodatnih definicij in dokazali lemo, ki nam bo olajšala dokazovanje izreka. Spomnimo se, da je ciklična permutacija n elementov vsaka permutacija, ki je cikel dolžine n. Vemo, da je takšnih permutacij natanko $(n-1)!$. Rekli ji bomo *ciklična ureditev.*

Definicija 2. *Ciklična ureditev* množice $[n]$ je ena izmed $(n-1)!$ cikličnih permutacij množice $[n]$.

Množica s tremi elementi, $[3]$, ima le dve ciklični ureditvi. To sta $(1,2,3)$ in $(1,3,2)$.

Dokaz, da je cikličnih ureditev množice $[n]$ natanko $(n-1)!$, bi moral matematično podkovan bralec dobro poznati, ostali pa lahko to poskusijo dokazati za vajo. Nas bodo zanimali deli cikličnih ureditev.

Definicija 3. Ciklična ureditev $C = (c_0, c_1, \ldots, c_{n-1})$ množice $[n]$ *vsebuje množico* A, če obstaja $i \in \{0,1,\ldots,n-1\}$, da je $\{c_i, \ldots, c_{i+|A|-1}\} = A$, kjer indekse računamo po modulu n.

Naslednji primer nam pokaže, katere množice vsebuje določena ciklična ureditev.

Primer 3.

$$\begin{aligned} U &= [8] \\ C &= (3,1,5,4,2,7,6,8) \end{aligned}$$

$$\begin{aligned} I_1 &= \{3,1,5\} & I_2 &= \{1,5,4\} \\ I_3 &= \{5,4,2\} & I_4 &= \{4,2,7\} \\ I_5 &= \{2,7,6\} & I_6 &= \{7,6,8\} \\ I_7 &= \{6,8,3\} & I_8 &= \{8,3,1\} \end{aligned}$$

Ureditev C je ena izmed možnih cikličnih ureditev množice U. Množice I_1 , ... , I_8, so vse množice moči 3, ki jih C vsebuje.

Lema nam bo povedala, koliko množic iz presečne k-družine podmnožic množice $[n]$ lahko ciklična ureditev množice $[n]$ vsebuje.

Lema 2. *Naj bo $\mathcal{A}$ presečna k-družina podmnožic množice $[n]$, kjer je $n \geq 2k$. Tedaj poljubna ciklična ureditev množice $[n]$ vsebuje največ k množic iz družine $\mathcal{A}$.*

Pred formalnim dokazom, si bomo na primeru ogledali idejo dokaza.

Primer 4.

$$U = [8]$$
$$C = (3, 1, 5, 4, 2, 7, 6, 8)$$

$$I_1 = \{3, 1, 5\} \qquad I_2 = \{1, 5, 4\}$$
$$I_3 = \{5, 4, 2\} \qquad I_4 = \{4, 2, 7\}$$
$$I_5 = \{2, 7, 6\} \qquad I_6 = \{7, 6, 8\}$$
$$I_7 = \{6, 8, 3\} \qquad I_8 = \{8, 3, 1\}$$

Če je $\mathcal{A}$ presečna 3-družina podmnožic množice U in je $I_1 \in \mathcal{A}$, potem $\mathcal{A}$ vsebuje kvečjemu en element iz $\{I_2, I_7\}$ in en elelent iz $\{I_3, I_8\}$, ker imata elementa parov prazen presek. Ostale množice tudi ne morejo biti v $\mathcal{A}$, ker imajo prazen presek z I_1. Cikel C vsebuje največ 3 elemente iz $\mathcal{A}$, kar je skladno z lemo.

Dokaz. Naj bo $C = (a_0, a_1, \ldots, a_{n-1})$ ciklična ureditev množice $[n]$ in $\mathcal{F} = \{F_0, F_1, \ldots, F_{n-1}\}$ družina vseh "intervalov" dolžine k na ciklu C, torej množic oblike $F_i = \{a_i, a_{i+1}, \ldots, a_{i+k-1}\}$, kjer indekse računamo po modulu n. Recimo, da je $F_i \in \mathcal{A}$. Potem lahko $\mathcal{A}$ od množic iz $\mathcal{F}$ za vsak $\ell = i+1, i+2, \ldots, i+k-1$ (zaradi pogoja o sekanju) poleg F_i vsebuje le še največ eno od množic $\{a_{\ell-k}, a_{\ell-k+1}, \ldots, a_{\ell-1}\}$ in $\{a_\ell, a_{\ell+1}, \ldots, a_{\ell+k-1}\}$. Pri tem smo upoštevali predpostavko, da je $n \geq 2k$, saj bi se sicer množici $\{a_{\ell-k}, a_{\ell-k+1}, \ldots, a_{\ell-1}\}$ in $\{a_\ell, a_{\ell+1}, \ldots, a_{\ell+k-1}\}$, ki imata vsaka po k elementov, sekali med seboj. Velja torej

$$|\mathcal{A} \cap \mathcal{F}| \leq 1 + (k-1) = k.$$

□

Spomnimo se glavnega izreka tega članka. Dokazati želimo, da je maksimalna velikost presečne k-družine podmnožic množice $[n]$, pri pogoju, da je $n \geq 2k$, navzgor omejena z $\binom{n-1}{k-1}$.

Dokaz (Erdös-Ko-Radojev izrek). Naj bo p število urejenih parov oblike (M, C), kjer je M ena od množic iz družine $\mathcal{A}$ in C ena od cikličnih ureditev množice $[n]$, pri kateri je M "interval" na ciklu C. Par (M, C) konstruiramo takole:

1. izberemo $M \in \mathcal{A}$ (na $|\mathcal{A}|$ načinov),

2. izberemo permutacijo množice M (na $k!$ načinov),

3. izberemo permutacijo množice $[n] \setminus M$ (na $(n-k)!$ načinov),

4. permutaciji zlepimo v cikel dolžine n (na en način).

Po pravilu produkta sledi, da je

$$p = |\mathcal{A}|k!(n-k)!. \tag{2}$$

Po drugi strani pa zaradi leme 2 vemo, da pri izbrani ciklični ureditvi C družina $\mathcal{A}$ vsebuje največ k množic, ki so “intervali” na ciklu C. Ker lahko množico $[n]$ ciklično uredimo na $(n-1)!$ načinov, je

$$p \leq k(n-1)!. \tag{3}$$

Če združimo rezultata (2) in (3), dobimo $|\mathcal{A}|k!(n-k)! \leq k(n-1)!$, od tod pa sledi ocena

$$|\mathcal{A}| \leq \binom{n-1}{k-1}.$$

□

V dokazu izreka smo izračunali zgornjo mejo za moč družine množic, nas pa zanima, katere družine to zgornjo mejo tudi dosežejo. Najprej si bomo ogledali primera, kjer je zgornja meja dosežena, in poskusili uganiti splošno pravilo za konstrukcijo takšnih družin.

Primer 5.

$$\begin{aligned} U &= [5] \\ \mathcal{A} &= \{\{1,2\},\{1,3\},\{1,4\},\{1,5\}\} \\ |\mathcal{A}| = 4 &= \binom{5-1}{2-1} = \binom{4}{1} \end{aligned}$$

Kot vidimo, moč družine $\mathcal{A}$ doseže zgornjo mejo izreka. Hitro opazimo, da so elementi družine $\mathcal{A}$ vse podmnožice množice $\{2,3,4,5\}$ moči 1, ki smo jim dodali element 1. Zgornja meja bi bila dosežena tudi, če bi vlogo 1 menjali s poljubnim elementom iz $[5]$. V splošnem bi takšno družino konstruirali tako, da bi izbrali poljuben element iz množice $[n]$ in nato izmed preostalih $n-1$ elementov sestavili vse $k-1$ elementne podmnožice in vsaki podmnožici dodali izbrani element. Vse množice bi imele k elementov in neprazen presek, ker smo vsem dodali element, ki smo ga na začetku izbrali. Izmed $n-1$ elementov bi izbirali $k-1$ elementov, kar je ravno $\binom{n-1}{k-1}$ različnih množic in se sklada z zgornjo mejo izreka.

Našli smo splošno konstrukcijo, pri kateri družina množic doseže zgornjo mejo iz izreka. Zanima nas, ali je ta konstrukcija edina možna. Naslednji primer nam da alternativno konstrukcijo.

Primer 6.

$$\begin{aligned} U &= [4] \\ \mathcal{B} &= \{\{1,2\},\{2,3\},\{1,3\}\} \\ |\mathcal{B}| = 3 &= \binom{4-1}{2-1} = \binom{3}{1} \end{aligned}$$

Preverimo lahko, da ne obstaja element, ki bi bil skupen množicam iz $\mathcal{B}$. To pomeni, da prejšnji način ni edini možni.

A primer 6 je poseben, saj velja $2k = n$. V tem primeru lahko maksimalno družino konstruiramo tako, da izberemo element $a \in [n]$ in nato izberemo vse k-elementne podmnožice iz $[n] \setminus \{a\}$. Takšen izbor množic nam v splošnem ne daje nobenega zagotovila, da bo njihov presek paroma neprazen, a v tem primeru izmed $n-1$ elementov izberemo k elementov, se zaradi Dirichletovega načela poljubni k-elementni množici sekata.

Za poseben primer, kjer je $n = 2k$, smo našli alternativno konstrukcijo. V situacijah, kjer velja $n > 2k$, pa se izkaže, da je konstrukcija iz prejšnjega primera edina možna. Zapišimo to kot izrek.

Izrek 3. *Naj bo $\mathcal{A}$ presečna k-družina podmnožic množice $[n]$, $|\mathcal{A}| = \binom{n-1}{k-1}$ in $n > 2k$. Tedaj $\mathcal{A}$ vsebuje vse množice moči k, ki imajo skupen element $c \in [n]$.*

Dokaz. Naj bo $\mathcal{A}$ presečna k-družina podmnožic množice $[n]$, $|\mathcal{A}| = \binom{n-1}{k-1}$. Ločili bomo dva primera:

1. *Predpostavimo, da obstajata taka elementa $x, y \in [n]$, da vsaka k-elementna množica, ki vsebuje x in ne y, pripada družini $\mathcal{A}$.*

   Dokazujemo, da v tem primeru $\mathcal{A}$ vsebuje natanko vse k-elementne množice, ki vsebujejo x. Izberemo k-elementno množico K, ki ne vsebuje elementa x. Izberemo k-elementno množico L, ki vsebuje x, ne vsebuje y in ima prazen presek s K. To lahko storimo, ker velja $n > 2k$. Po predpostavki primera je množica L vsebovana v družini $\mathcal{A}$. Množici L in K imata prazen presek, zato množica K ne more biti element družine $\mathcal{A}$. Torej vsaka množica v družini vsebuje element x, zaradi predpostavke o velikosti družine pa mora vsebovati vse k-elementne množice, ki vsebujejo element x.

2. *Predpostavimo, da za vsak izbor elementov $x, y \in [n]$ obstaja k-elementna množica, ki vsebuje element x, ne vsebuje elementa y in ni element družine $\mathcal{A}$.*

   Obstajata k-elementni množici K in K', ki se razlikujeta v enem elementu in je K element družine $\mathcal{A}$, medted ko K' ni. Če takšni množici ne bi obstajali, bi lahko induktivno zaključili, da vse k-elementne množice pripadajo družini, kar vemo, da je nemogoče. Z 0 označimo element enojca $K \setminus K'$ in s k element enojca $K' \setminus K$. Po predpostavki primera obstaja k-elementna množica K'', ki ni element družine $\mathcal{A}$, vsebuje 0 in ne vsebuje k. Naj bo $K \cap K'' = \{0, \ldots, l-1\}, 0 < l < k$. Označimo preostale elemente iz K z $l, \ldots, k-1$ in preostale elemente iz K'' z $n-k+l, \ldots, n-1$. Iz dokaza Erdös-Ko-Radojevega izreka vidimo, da mora poljubna ciklična ureditev $[n]$ vsebovati k množic iz družine, če družina dosega maksmimalno velikost. Kratek razmislek nam pove, da morajo biti množice na ciklu zaporedne. Pri ciklični ureditvi $C = (0, 1, \ldots, n-2, n-1)$ pridemo v protislovje, saj $\mathcal{A}$ vsebuje množico $\{0, \ldots, k-1\}$, ne pa $\{1, \ldots, k\}$ in $\{n-k+l, \ldots, n-1, 0, 1, \ldots, l-1\}$. Prišli smo v protislovje s predpostavko primera in s tem je izrek dokazan.

□

Erdös-Ko-Radojev izrek nas je naučil, kakšna je največja presečna k-družina podmnožic neke končne množice. Dokazali smo tudi, na kakšen način lahko takšne družine konstruiramo in v katerem primeru je mogoč le en način konstrukcije. Zainteresiran bralec lahko poskusi razmisliti in dokazati, koliko različnih največjih družin lahko pri izbranih k in n konstruiramo.

LITERATURA

[1] Peter J. Cameron: *Notes on Combinatorics*, str. 72-76, [ogled 24. 03. 2019]. Dostopno na `https://camerancounts.files.wordpress.com/2013/11/comb.pdf`

[2] Peter J. Cameron: *Combinatorics: Solutions, Additions, Corrections*, [ogled 24. 03. 2019]. Dostopno na `http://www-groups.mcs.st-andrews.ac.uk/~pjc/books/comb/ekr.pdf`

[3] Wikipedia *Erdős–Ko–Rado theorem*, [ogled 24. 03. 2019]. Dostopno na `https://en.wikipedia.org/wiki/Erd%C5%91s%E2%80%93Ko%E2%80%93Rado_theorem`