POKRITJA RAZLIČNIH ALGEBRSKIH STRUKTUR

AJDA LEMUT

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku je predstavljen znan problem pokritja. Najprej nekoliko na splošno, potem pa na treh algebrskih strukturah, in sicer na grupah, kolobarjih in vektorskih prostorih. V zadnjem poglavju pa je predstavljena še posplošitev izrekov iz poglavja o vektorskih prostorih na afine prostore.

COVERING PROBLEM ON DIFFERENT ALGEBRAIC STRUCTURES

The article presents a well known covering problem. First somewhat generally, then on three algebraic structures, on groups, rings and vector spaces. In the last chapter, there is a generalization of the theorems from the chapter on vector spaces to affine spaces.

1. Uvod

Tako kot lahko množice pokrivamo z njihovimi podmnožicami, si želimo različne algebrske strukture pokrivati z njihovimi podstrukturami. Torej grupe s podgrupami, vektorske prostore z vektorskimi podprostori, kolobarje s podkolobarji ... V angleščini je ta problem znan kot »covering problem«. Znotraj problema nas torej zanima, ali neko algebrsko strukturo sploh lahko pokrijemo z njenimi pravimi podstrukturami in kolikšno je najmanjše število takšnih podstruktur, s katerimi jo lahko pokrijemo. Če torej obstoj pokritja že poznamo, postane problem pokritij minimizacijski problem. V splošnem tak problem velikokrat znamo predstaviti z linearnimi programi, katerih duali so potem znani kot problemi zlaganja ali v angleščini »packing problems«. Prav tako se problem pokritij uporablja v verjetnosti in statistiki, particije prostorov pa v računalniški grafiki, v načrtovanju krožnih vezij, kjer s particijami preverjajo, ali je dizajn sploh mogoče izdelati ([1], [2]). V splošnem je problem razdrobljen na posamezne algebrske strukture, tu pa je zajetih nekaj glavnih rezultatov znotraj problema na grupah, kolobarjih, vektorskih in afinih prostorih.

2. Osnovne definicije

Ker govorimo o pokritjih algebrskih struktur, moramo najprej definirati, kaj sploh so pokritja.

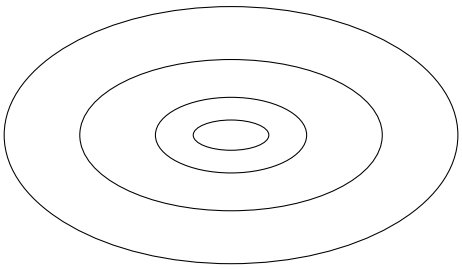
Definicija 1. *Pokritje* algebrske strukture M je družina $\{N_i\}_{i\in I}$ takih pravih podstruktur, da velja $M = \bigcup_{i\in I} N_i$. Rečemo, da je pokritje *končno*, če je moč indeksne množice I končno število.

Opomba 1. Seveda govorimo o pokritjih s pravimi podstrukturami v smislu, da v pokritje ne damo kar same strukture, ki bi tako že sama pokrila celo strukturo. Tak primer je torej trivialen in se z njim ne ukvarjamo. Tako bo od sedaj z besedo podstruktura vedno mišljena prava podstruktura.

Definicija 2. Pravimo, da je struktura *pokrivna*, če zanjo obstaja pokritje s pravimi podstrukturami.

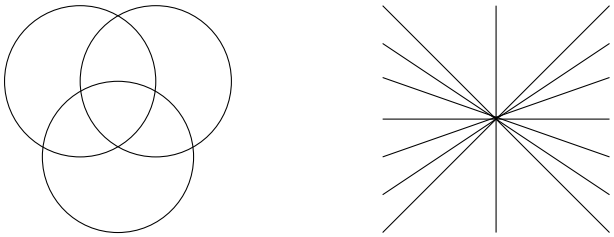
Definicija pokritja nam ne da nobene omejitve o tem, kako lahko pokrivamo našo strukturo. Kaj bi se torej zgodilo, če bi iz naše družine podstruktur odstranili kakšen člen? Bi to še vedno lahko bilo pokritje? Izkaže se, da obstajajo pokritja, ko to lahko naredimo in pokritja, ko tega ne moremo.

Zgled 1. Vzemimo za našo algebrsko strukturo vektorski prostor polinomov nad realnimi števili $\mathbb{R}[x]$. Naj bo W_n vektorski podprostor polinomov s stopnjo manjšo ali enako n. Tedaj je $\{W_n\}_{n\in\mathbb{N}}$ pokritje našega vektorskega prostora, za katerega velja, da lahko poljuben podprostor te družine odstranimo in še vedno prostor pokrijemo s preostankom podprostorov. To velja, ker vsak naslednji podprostor pokritja vsebuje vse prejšnje. Za lažjo predstavo si lahko tak tip pokritja intuitivno predstavljamo kot kroge oziroma elipse, kjer vsaka naslednja vsebuje vse manjše (slika 1).



Slika 1. Skica pokritja vektorskega prostora polinomov.

Smiselno se zdi definirati pokritje, kjer se to ne more zgoditi. Ker je v vsaki podstrukturi vsebovana enota (z izjemo polgrup, a te nas tu ne zanimajo), pokritja ne morejo imeti praznega preseka, zato si lahko tako pokritje spet intuitivno predstavljamo kot skupek krogov z nepraznim presekom, ki vsebuje enoto ali pa kot pokritje ravnine s premicami skozi izhodišče (slika 2).



Slika 2. Skica nereducibilnih pokritij.

Definirajmo sedaj tak tip pokritja.

Definicija 3. Pokritje $\{N_i\}_{i\in I}$ algebrske strukture M je *nereducibilno*, če za vsako pravo podmnožico J indeksne množice I velja $\bigcup_{i\in J} N_i \neq M$.

Poglejmo sedaj še dva primera takega tipa pokritja.

Zgled 2. Iz prejšnje intuitivne predstave takoj pomislimo na vektorski prostor $\mathbb{R}^2$, ki ga lahko pokrijemo s premicami skozi izhodišče. Če iz pokritja odstranimo katero koli premico, te ne bodo več pokrile celega $\mathbb{R}^2$. Opazimo tudi, da je teh premic neštevno neskončno.

Poglejmo še nekoliko enostavnejši primer.

Zgled 3. Vzemimo kolobar $\mathbb{Z}_2 \times \mathbb{Z}_2$, ki ga zapišemo kot unijo treh podkolobarjev $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(1,0),(0,0)\} \cup \{(1,1),(0,0)\} \cup \{(0,1),(0,0)\}$. Takoj vidimo, da z odstranitvijo katerega koli podkolobarja ne bomo dobili več celega prvotnega kolobarja. Tu smo torej potrebovali le tri podstrukture. $\mathbb{Z}_2 \times \mathbb{Z}_2$ lahko obravnavamo tudi kot vektorski prostor nad $\mathbb{Z}_2$. Spet imamo v tem vektorskem prostoru natanko tri premice, ki gredo skozi izhodišče in so ravno njegovo pokritje.

Kot rečeno v uvodu, nas bosta znotraj problema zanimali dve stvari. Kdaj neko algebrsko strukturo sploh lahko pokrijemo z njenimi podstrukturami in kolikšno je najmanjše število takih podstruktur. V ta namen definirajmo naslednji pojem.

Definicija 4. *Pokrivno število* algebrske strukture A je najmanjša kardinalnost (moč indeksne množice) pokritja $\{B_i\}_{i\in I}$ za A. V splošnem uporabljamo oznako $o(A) = |I|$.

Poglejmo si sedaj problem na nekaj algebrskih strukturah.

3. Pokritja grup

Definicija 5. Množica G skupaj z binarno operacijo $(x, y) \to xy$ je *grupa*, če je operacija asociativna, ima enoto in je vsak element obrnljiv.

Hitro opazimo, da lahko vsako neciklično grupo (torej vsako, ki ni generirana samo z enim elementom) predstavimo kot unijo pravih podgrup. Elementi pokritja so lahko na primer vse ciklične podgrupe. Te vedno pokrijejo celo grupo, saj je poljuben element iz grupe vsebovan v ciklični grupi generirani s tem elementom. Z naslednjim zgledom iz [3] vidimo, da obstajajo grupe, za katere ne obstaja končno pokritje.

Zgled 4. Vzemimo grupo racionalnih števil. Denimo, da se jo da pokriti s končno mnogo podgrupami $H_1, \ldots, H_n$, za nek $n \in \mathbb{N}$. Ker gre za končno pokritje, lahko predpostavimo, da je nereducibilno. V nasprotnem primeru bi sicer odstranili nepotrebne podstrukture. To pomeni, da vsak H_i vsebuje neko pozitivno racionalno število, ki ni v vseh ostalih. Naj recimo H_1 vsebuje $r = \frac{m}{n}$ in r ni vsebovan v nobenem H_i za $i \neq 1$. Sledi, da je tudi za vsako naravno število h potem $\frac{r}{h}$ lahko samo v H_1. Torej to velja tudi za $h = dm$, kjer je $d \in \mathbb{N}$ poljuben. Če je torej $\frac{r}{h} = \frac{m}{ndm} = \frac{1}{nd}$ v H_1, je potem tudi $\frac{l}{nd}$ v H_1 za vsako naravno število l. In če za l vzamemo cn, dobimo torej, da je $\frac{c}{d}$ v H_1. To pa pomeni, da je H_1 kar cela grupa pozitivnih racionalnih števil.

Kaj pa ciklične grupe? Vemo, da so vse neskončne ciklične grupe izomorfne grupi $(\mathbb{Z}, +)$, torej zadošča obravnavati le to. Vse podgrupe $\mathbb{Z}$ so oblike $d\mathbb{Z}$, kjer je $d \in \mathbb{N} \cup \{0\}$, te pa za $d \neq 1$ nikoli ne bodo vsebovale elementa 1. Torej so take grupe nepokrivne. Pri končnih cikličnih grupah prav tako naletimo na problem. Če je grupa ciklična, je generirana z nekim elemntom a. Element a torej ne more biti vsebovan v nobeni pravi podgrupi. Omejimo se sedaj na končne neciklične grupe in si poglejmo dve trditvi iz [3].

Trditev 1. *Nobena grupa ne more biti unija dveh pravih podgrup.*

Dokaz. Recimo, da je grupa G unija dveh podgrup A in B. To pokritje mora biti nereducibilno. V nasprotnem primeru bi lahko odvzeli enega izmed dveh elementov pokritja in bi to še vedno bilo pokritje. To bi pomenilo, da preostala podgrupa ni prava podgrupa, ampak kar cela grupa sama. Torej zaradi nereducibilnosti pokritja obstajata element x, ki je v A in ni v B, ter element y, ki je v B in ni v A. Če je xy v A, potem mora biti tudi $x^{-1}xy$ v A, kar je v protislovju z izbiro elementov x in y. Enako dobimo protislovje, ko predpostavimo, da je xy v B. Torej xy ni ne v A in ne v B, kar je protislovje s tem, da je to pokritje.

Trditev 2. *Naj bo $\{H_i\}_{i\in I}$ končno nereducibilno pokritje grupe G. Potem za vsak i H_i vsebuje presek vseh ostalih podgrup pokritja.*

Dokaz. Uporabimo podoben argument kot v prejšnji trditvi. Ker je pokritje nereducibilno, H_i ne more biti vsebovan v uniji vseh ostalih elementov pokritja. Naj bo torej x element, ki je vsebovan samo v H_i in y element, ki je vsebovan v preseku vseh ostalih. Ker je G grupa, je xy v G in torej mora biti vsaj v eni od podgrup pokritja. Če je xy v H_j za $j \neq i$, je potem tudi $xyy^{-1} = x$ v H_j, kar je v protislovju z izbiro elementa x. Torej mora biti xy v H_i in zato tudi $x^{-1}xy = y$. S tem smo pokazali našo trditev.

Od sedaj naprej naj bodo podgrupe v pokritju urejene tako, da bodo imele nepadajoče indekse $[G : H_1] \leq [G : H_2] \leq \cdots \leq [G : H_n]$ oziroma, da so glede na svojo moč v nenaraščajočem vrstnem redu.

Opomba 2. Indeks podgrupe H je število vseh njenih odsekov, torej število različnih množic $aH = \{ah, h \in H\}$ za $a \in G$. Označimo ga z $[G : H]$ in po Lagrangeevem izreku velja $[G : H] = \frac{|G|}{|H|}$.

Zanima nas, ali lahko kaj povemo o velikosti grupe G glede na velikosti podgrup iz njenega pokritja. To nam pove trditev iz [4].

Trditev 3. *Če grupo G lahko pokrijemo s podgrupami H_r, $r = 1, \ldots, n$, potem velja $|G| \leq \sum_{r=2}^{n} |H_r|$. V posebnem primeru velja enakost natanko tedaj, ko je $H_1 H_r = G$ za $r \neq 1$ in $H_r \cap H_s \subset H_1$ za $r \neq s$.*

Dokaz. Najprej pokažimo znano produktno formulo $|HK| = \frac{|H||K|}{|H \cap K|}$ za H, K pogrupi grupe G. Očitno za HK dobimo $|H||K|$ potencialnih elementov. Preveriti moramo samo, koliko smo jih šteli večkrat. Torej, kdaj je $hk = h'k'$ za $h, h' \in H$ in $k, k' \in K$. Enakost z leve množimo s h^{-1}, z desne pa s k'^{-1}. Taka elementa obstajata, ker sta H in K grupi. Tako dobimo

$$\begin{aligned} h^{-1}hkk'^{-1} &= h^{-1}h'k'k'^{-1} \\ kk'^{-1} &= h^{-1}h' = t. \end{aligned}$$

Ker je t očitno iz $H \cap K$, produktna formula sledi.

Vrnimo se na dokazovanje trditve. Element iz grupe G je bodisi iz H_1 bodisi iz $H_r \backslash H_1$ za nek $r = 2, \ldots, n$. Število vseh elementov v H_r, ki niso v H_1, izračunamo kot

$$\begin{aligned} |H_r| - |H_1 \cap H_r| &= |H_r| \left(1 - \frac{|H_1|}{|H_1 H_r|}\right), \text{ kjer smo uporabili produktno formulo} \\ &\leq |H_r| \left(1 - \frac{|H_1|}{|G|}\right). \end{aligned}$$

Tu se enakost ohrani le v primeru $H_1 H_r = G$. Seštejemo po vseh $r \geq 2$ in dobimo

$$\begin{aligned} |G| &\leq \sum_{r=2}^{n} |H_r \backslash H_1| + |H_1| \\ &\leq |H_1| + \left((1 - \frac{|H_1|}{|G|}\right) \sum_{r=2}^{n} |H_r|, \end{aligned}$$

kjer enakost velja natanko tedaj, ko je $H_r \cap H_s \subset H_1$ za $r \neq s$, saj so takrat $H_r \backslash H_1$ med seboj disjunktni. Nato postopamo na sledeč način.

$$\begin{aligned} |G| &\leq |H_1| \left(1 - \sum_{r=2}^{n} \frac{|H_r|}{|G|}\right) + \sum_{r=2}^{n} |H_r| \\ |G| - \sum_{r=2}^{n} |H_r| &\leq |H_1| \left(1 - \sum_{r=2}^{n} \frac{|H_r|}{|G|}\right) \\ 1 - \sum_{r=2}^{n} \frac{|H_r|}{|G|} &\leq \frac{|H_1|}{|G|} \left(1 - \sum_{r=2}^{n} \frac{|H_r|}{|G|}\right) \end{aligned}$$

Ker je $\frac{|H_1|}{|G|} < 1$ neenakost sledi.

Oglejmo si še nekaj rezultatov iz [4].

Lema 4. *Naj bo pokrivno število grupe G enako $o(G) = n$. Tedaj je indeks podgrupe H_2 manjši ali enak $n-1$, tj. $[G : H_2] \leq n-1$.*

Dokaz.

$$\begin{aligned}[G : H_2] &= \frac{|G|}{|H_2|} \text{ (Lagrangeev izrek)} \\ &\leq \frac{\sum_{r=2}^{n} |H_r|}{|H_2|} \text{ (Uporabili smo trditev 3.)} \\ &= 1 + \frac{|H_3|}{|H_2|} + \cdots + \frac{|H_n|}{|H_2|} \leq n-1, \text{ saj zaradi urejenosti po indeksih } H_r \text{ velja } \frac{|H_r|}{|H_2|} \leq 1.\end{aligned}$$

Opomba 3. S to lemo še enkrat vidimo, da nobena grupa ne more biti unija dveh podgrup.

Lema 5. *Naj bo N podgrupa edinka grupe G. Tedaj velja $o(G) \leq o(G/N)$.*

Dokaz. Pokritje G/N inducira pokritje G na sledeč način. Če je $G/N = \bigcup H_i/N$, potem je $G = \bigcup H_i N$.

Trditev 6. *Pokrivno število končnega direktnega produkta grup je manjše ali enako najmanjšemu izmed pokrivnih števil posameznih grup, tj. $o(\Pi_{i=1}^{t} G_i) \leq \min\limits_{1 \leq i \leq t} \{o(G_i)\}$.*

Dokaz. Naj bo i indeks, pri katerem $o(G_i)$ doseže minimum in naj bo $o(G_i) = m$. Torej lahko grupo G_i zapišemo kot unijo $G_i = \bigcup_{j=1}^{m} S_j$. Pokritje $\Pi_{i=1}^{m} G_i$ z m podgrupami lahko tvorimo kot $\bigcup_{j=1}^{m} (G_1 \times \cdots \times G_{i-1} \times S_j \times G_{i+1} \times \cdots \times G_t)$. Torej je pokrivno število lahko kvečjemu manjše.

Dokazali smo, da nobena grupa ne more biti pokrita z dvema podgrupama. Naravno se je nato vprašati, ali je lahko pokrita s tremi, štirimi in tako naprej. Izkaže se, da obstajajo pogoji, kdaj se to lahko zgodi. Oglejmo si pogoj iz [3].

Trditev 7. *Pokrivno število grupe G je 3 natanko tedaj, ko je Kleinova četverka homomorfna slika grupe G.*

Opomba 4. Kleinova četverka je grupa z natanko 4 elementi, kjer je vsak element svoj inverz. Torej je oblike $\{1, a, b, c\}$, kjer je $aa = 1$, $bb = 1$ in $cc = 1$. Izkaže se, da je izomorfna znani $\mathbb{Z}_2 \times \mathbb{Z}_2$ grupi za seštevanje.

Dokaz. Takoj opazimo, da Kleinovo četverko lahko pokrijemo s tremi podgrupami: $\{1, a\}$, $\{1, b\}$, $\{1, c\}$. Za homomorfizme vemo, da je praslika podgrupe tudi podgrupa in tako za pokritje grupe G vzamemo praslike podgrup, ki pokrijejo Kleinovo četverko.

Obratno predpostavimo, da je G unija treh podgrup A, B, C. Po trditvi 1 vemo, da mora biti to nereducibilno pokritje. To pa pomeni, da so množice $A' = A - (B \cup C)$, $B' = B - (A \cup C)$, $C' = C - (A \cup B)$ vse neprazne. Tako dobimo $H := A \cap B \cap C = B \cap C = A \cap B = A \cap C$, kjer smo uporabili trditev 2. G je disjunktna unija A', B', C' in H. Po lemi 4 imata dve izmed podgrup A, B, C indeks 2 in zato sta podgrupi edinki. Sledi, da je tudi njun presek, ki pa je ravno H, podgrupa edinka. Pokažimo sedaj, da so odseki po tej podgrupi edinki ravno A', B' in C'. Brez škode za splošnost sta A in B tisti dve podgrupi z indekosm 2. Tedaj velja $[G : A \cap B] \leq [G : A] \cdot [G : B]$, saj je preslikava

$$\begin{aligned}\phi : \{g(A \cap B); g \in G\} &\to \{gA; g \in G\} \times \{gB; g \in G\} \\ \phi(g(A \cap B)) &\mapsto (gA, gB)\end{aligned}$$

očitno injektivna. Ker sta v našem primeru A in B tisti dve podgrupi z indekosm 2, je torej $[G : H] \leq 4$. Naj bo sedaj $a \in A'$ poljuben. Dokazujemo $aH \subseteq A'$. Naj bo $h \in H$ poljuben. Tedaj je $ah \in A$, saj je $a \in A$, $H \subseteq A$ in A je podgrupa. Če $ah \notin H$, potem je $ah \in A'$ in s tem dobimo željeno. Denimo, da temu ni tako, torej naj bo $ah \in H$ oziroma $ah = h'$ za nek $h' \in H$. Ker je H podgrupa, obstaja h^{-1} in zato je $a = h'h^{-1} \in H$. To pa je v protislovju z izbiro a. Enako naredimo za $b \in B'$ in $c \in C'$. Tako smo dobili štiri disjunktne odseke, ki so torej ravno vsi odseki po podgrupi edinki H, vsi odseki pa pokrijejo grupo G. Zato so A', B' in C' res odseki po H ($aH = A'$, $bH = B'$, $cH = C'$) in G/H je res Kleinova četverka.

Cohn je v [4] z malce drugačnim pristopom zapisal pogoj za $o(G) = 3$ in nato še za $o(G) = 4, 5$. Računanje pokrivnega števila za končne grupe ostaja odprt problem, nekaj grup, za katere je izračunano pokrivno število, pa lahko najdete v [5], [6], [7], [8] in v [9].

4. Pokritja kolobarjev

4.1 Uvodni pojmi

Definicije kolobarjev in podkolobarjev se nekoliko razlikujejo med seboj, zato poglejmo našo definicijo.

Definicija 6. Množico R skupaj z binarnima operacijama $+, \cdot$ imenujemo *kolobar*, če velja:

- $(R, +)$ je Abelova grupa,
- $(R, \cdot)$ je polgrupa (velja asociativnost),
- operaciji povezujeta distributivnostna zakona.

V tej definiciji torej ne privzemamo obstoja enote za množenje. Tako definiramo podkolobar kot podmnožico R, ki je tudi sama kolobar po zgornji definiciji.

Takoj lahko rečemo, da noben kolobar ne more biti pokrit s samo dvema podkolobarjema. V nasprotnem primeru bi to pomenilo, da bi njegovo aditivno grupo lahko pokrili z dvema grupama, kar pa smo v poglavju o pokritju grup pokazali, da ni mogoče. Kolobarje, ki jih lahko pokrijemo s tremi podkolobarji, sta opisala A. Lucchini in A. Maróti v [11].

Definicija 7. Naj bo R kolobar. *Podkolobar generiran z* $a \in R$ je množica vseh elementov oblike

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a;\ n \geq 1,\ c_i \in \mathbb{Z}.$$

Tak podkolobar označimo z $\langle a \rangle$.

Opomba 5. Pravimo, da je R generiran z a, če je $R = \langle a \rangle$.

4.2 Glavni izrek

Poglejmo si naš glavni izrek za pokritja kolobarjev iz [12].

Izrek 8 (Glavni izrek).

1. *R je pokriven natanko tedaj, ko za vsak $a \in R$ velja $R \neq \langle a \rangle$.*
2. *Za vsak $a \in R$ je $\langle a \rangle$ komutativen kolobar.*
3. *Če je $\langle a \rangle$ maksimalen podkolobar, potem je vsebovan v vsakem pokritju R.*

4. *Naj bo I nek ideal kolobarja R. Če je R/I pokriven, potem je tudi R pokriven in velja $o(R) \leq o(R/I)$.*

5. *Če je R končen produkt kolobarjev R_i in je vsaj en izmed R_i pokriven, potem je R pokriven. Še več, če so maksimalni podkolobarji kolobarja R oblike $M = R_1 \times \cdots \times R_{i-1} \times M_i \times R_{i+1} \times \cdots R_t$, kjer je M_i maksimalen podkolobar kolobarja R_i, potem je R pokriven natanko tedaj, ko je vsaj en izmed R_i pokriven. Tedaj velja $o(R) = \min\limits_{1 \leq i \leq t} \{o(R_i)\}$.*

Opomba 6. Podkolobar S kolobarja R je *maksimalen*, če je maksimalen med vsemi podkolobarji glede na relacijo inkluzije. Torej če ne obstaja podkolobar strogo med S in R.

Opomba 7. Če v točki 5 kolobarji niso take oblike, potem lahko nimajo pravih podkolobarjev in zato ne moramo postopati na enak način.

Zgled 5. Kolobar $\mathbb{Z}_2 \times \mathbb{Z}_2$ je produkt dveh nepokrivnih kolobarjev ($\mathbb{Z}_2 = \langle 1 \rangle$), ampak je pokriven, saj ga lahko zapišemo kot unijo treh podkolobarjev $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (1,0) \rangle \cup \langle (1,1) \rangle \cup \langle (0,1) \rangle$.

Dokaz. 1. Če $R \neq \langle a \rangle$ za vsak $a \in R$, potem za pokritje lahko vzamemo vse podkolobarje generirane s posameznimi elementi. Tako pokritje je sicer lahko reducibilno, vendar obstaja. Obratno naj bo R pokriven in naj za nek $a \in R$ velja $R = \langle a \rangle$. Po konstrukciji je $\langle a \rangle$ najmanjši podkolobar, ki vsebuje a. Torej R ne moremo pokriti s pravimi podstrukturami, saj lahko element a pokrijemo le z $R = \langle a \rangle$.

2. Iz konstrukcije $\langle a \rangle$ vemo, da so vsi njegovi elementi oblike $c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a$, $n \geq 1$, $c_i \in \mathbb{Z}$. Od tu pa je komutativnost takih dveh elementov očitna.

3. Če je $\langle a \rangle$ maksimalen kolobar, mora očitno biti vsebovan v pokritju, saj je hkrati najmanjši in največji podkolobar, ki vsebuje element a.

4. Pokritje R/I inducira pokritje R na sledeč način. Če je $R/I = \bigcup S_i/I$, potem je $R = \bigcup (S_i + I)$. Neenakost od tod očitno sledi.

5. Naj bo $R = \prod_{i=1}^{n} R_i$ in naj bo R_j pokriven za nek $j = 1, \ldots, n$. Torej $R_j = \bigcup_{i=1}^{k} S_i$ in za pokritje R lahko vzamemo kar $R = \bigcup_{i=1}^{k} R_1 \times R_2 \times \cdots \times R_{j-1} \times S_i \times R_{j+1} \times \cdots R_n$. Torej je R res pokriven.

   Obratno implikacijo pokažemo z dokazom formule $o(R) = \min\limits_{1 \leq i \leq t} \{o(R_i)\}$. Brez škode za splošnost se lahko omejimo na primer $R = R_1 \times R_2$, saj v nasprotnem nadaljujemo z indukcijo. Prav tako lahko predpostavimo, da je $o(R_1) \leq o(R_2) \leq \infty$, kjer $o(R_i) = \infty$ tu pomeni, da je kolobar nepokriven. Očitno velja, da je $o(R)$ kvečjemu manjši od $o(R_1)$, saj lahko za pokritje R vzamemo kar produkt pokritja R_1 z R_2. Vzemimo sedaj nek $r < o(R_1)$ in naj bodo $S_1, \ldots, S_r$ maksimalni podkolobarji R. Dokazati moramo, da unija teh podkolobarjev ne more biti R. Podkolobarji S_j so oblike $A_j \times B_j$, kjer je A_j podkolobar R_1 in B_j podkolobar R_2 (ne nujno oba prava podkolobarja). Velja

$$\bigcup_{j=1}^{r} S_j \subseteq \left(\bigcup_{j=1}^{r} A_j \right) \times \left(\bigcup_{j=1}^{r} B_j \right).$$

   Ker je $r < o(R_1) \leq o(R_2)$, potem $\bigcup^{r}_{\substack{j=1 \\ A_j \neq R_1}} A_j \neq R_1$ in $\bigcup^{r}_{\substack{j=1 \\ B_j \neq R_2}} B_j \neq R_2$. Torej lahko vzamemo $a \in R_1$, ki ni vsebovan v $\bigcup^{r}_{\substack{j=1 \\ A_j \neq R_1}} A_j$, in $b \in R_2$, ki ni vsebovan v $\bigcup^{r}_{\substack{j=1 \\ B_j \neq R_2}} B_j$. Naj bo $(a,b) \in S_k$ za nek indeks k. Torej je $a \in A_k$ in $b \in B_k$. Po konstrukciji pa mora potem biti $A_k = R_1$ in $B_k = R_2$, kar pomeni, da mora biti $S_k = R$. Sledi torej $o(R) = o(R_1)$.

Opomba 8. Zapis $o(A) = \infty$ za neko algebrsko strukturo A se razlikuje glede na kontekst. Lahko označuje neskončnost pokrivnega števila ali pa, da pokritje sploh ne obstaja. V končnih algebrskih strukturah je nesmiselno govoriti o neskončnih pokritjih, zato tu oznaka pomeni neobstoj pokritja.

Posledica 9. *Vsak nekomutativen kolobar je pokriven.*

Dokaz. Po drugi točki izreka je $\langle a \rangle$ komutativen kolobar za vsak a. To pomeni, da $\langle a \rangle \neq R$ in zato je R po prvi točki izreka pokriven.

Opomba 9. Iz izreka vidimo, da je veliko lažje dokazati, da nek kolobar ni pokriven, saj moramo najti le tak $a \in R$, da bo $R = \langle a \rangle$.

Poglejmo si sedaj nam najbližje kolobarje ostankov.

4.3 Kolobarji ostankov

Očitno so vsi kolobarji ostankov nepokrivni, saj je $\mathbb{Z}_n = \langle 1 \rangle$ za vsak n. Kaj pa produkti teh kolobarjev? V prejšnjem poglavju smo videli, da je $\mathbb{Z}_2 \times \mathbb{Z}_2$ pokriven in našli smo tudi njegovo pokritje. Kaj pa kakšni drugi primeri? Oglejmo si nekaj rezultatov iz [13].

Lema 10. *Naj bo p praštevilo večje ali enako 3. Tedaj je $\mathbb{Z}_p \times \mathbb{Z}_p = \langle (1, p-1) \rangle$ in je torej nepokriven.*

Dokaz. Naj bo $y = (1, p-1)$. Potem je $y^2 = (1, 1)$, kar je enota v $\mathbb{Z}_p \times \mathbb{Z}_p$. Elementi kolobarja $\langle y \rangle$ so oblike $a(1, p-1) + b(1, 1) = (a + b, a(p-1) + b)$, kjer je $0 \leq a, b \leq p-1$. To nam da vse elemente $\mathbb{Z}_p \times \mathbb{Z}_p$.

Podobno lahko naredimo za $\mathbb{Z}_p \times \mathbb{Z}_q$, ker sta p in q dve različni praštevili.

Lema 11. *Naj bosta p in q dve različni praštevili. Tedaj je $\mathbb{Z}_p \times \mathbb{Z}_q = \langle (1, 1) \rangle$ in je nepokriven.*

Dokaz. Dovolj je pokazati, da $(1, 1)$ res generira ta kolobar. Naj bo $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q$. Iščemo $n \in \mathbb{Z}$, da bo veljalo:

$$(x, y) = n(1, 1) = (n \pmod p, n \pmod q).$$

Dobili smo sistem enačb

$$\begin{aligned} n &\equiv x \pmod p, \\ n &\equiv y \pmod q. \end{aligned}$$

Po kitajskem izreku o ostankih obstaja tak n, ki reši sistem, in torej $(1, 1)$ res generira naš kolobar.

Opomba 10. Dokaz nam pravzaprav pokaže znano dejstvo $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.

5. Pokritja vektorskih prostorov

5.1 Uvodni pojmi

Ponovimo najprej definicijo vektorskih prostorov in podprostorov.

Definicija 8. Naj bo F komutativen obseg (torej polje). Tedaj množico V skupaj z binarno operacijo $+ : V \times V \to V, (v, w) \mapsto v + w$ in zunanjo binarno operacijo $\cdot : F \times V \to V, (\lambda, v) \mapsto \lambda \cdot v$ imenujemo *vektorski prostor* nad F, če velja:

- $(V, +)$ je Abelova grupa,

- $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ za vse $\lambda, \mu \in F$ in vse $v \in V$,
- $\lambda \cdot (u + v) = \lambda \cdot u + \lambda \cdot v$ za vse $\lambda \in F$ in vse $v, u \in V$,
- $(\lambda\mu) \cdot v = \lambda \cdot (\mu \cdot v)$ za vse $\lambda, \mu \in F$ in vse $v \in V$,
- $1 \cdot v = v$ za vse $v \in V$.

Definicija 9. Podmnožica vektorskega prostora V je *vektorski podprostor*, če je za isti operaciji tudi sama vektorski prostor.

Nadaljnje definicije, leme, izreki in dokazi v tem poglavju temeljijo na [14]. Ker se v angleščini vektorskim prostorom reče tudi linearni prostori, je v literaturi za pokritja vektorskih prostorov uporabljen izraz linearna pokritja, česar se bomo držali tudi mi v tem poglavju. Pripomnim še to, da bosta v tem poglavju iz praktičnih razlogov dostikrat uporabljena izraza prostor in podprostor, čeprav je v resnici seveda mišljeno za vektorski prostor in vektorski podprostor.

Hitro opazimo, da vektorskih prostorov dimenzije 1 ne moremo pokriti s pravimi podprostori, saj je edini pravi podprostor trivialen vektorski prostor. Vse ostale vektorske prostore višjih dimenzij pa lahko pokrijemo na primer z vsemi njegovimi enorazsežnimi vektorskimi podprostori. Zato se bomo v tem poglavju osredotočili na iskanje števila podprostorov, s katerimi pokrivamo prostor. V ta namen definirajmo novi oznaki za pokrivno število.

Definicija 10. *Linearno pokrivno število vektorskega prostora V ($LC(V)$)* je najmanjša možna kardinalnost linearnega pokritja $\{W_i\}_{i \in I}$ za V (moč indeksne množice).

Definicija 11. *Nereducibilno linearno pokrivno število vektorskega prostora V ($ILC(V)$)* je najmanjša možna kardinalnost nereducibilnega linearnega pokritja $\{W_i\}_{i \in I}$ za V (moč indeksne množice).

Opomba 11. Oznaka $LC(V)$ in $ILC(V)$ izhaja iz angleškega izraza »linear covering number« in »irredundant linear covering number«.

Kakšna pa je povezava med temi dvemi števili? Katero je večje, ali sta vedno enaki? V splošnem se nam sicer zdi, da bi moralo najmanjše pokritje biti tudi nereducibilno, a temu ni tako. Iz zgleda 1 o pokritju vektorskega prostora polinomov vidimo, da najmanjše linearno pokritje ($\{W_n\}_{n \in \mathbb{N}}$, kjer je W_n vektorski podprostor polinomov s stopnjo manjšo ali enako n) ni nujno tudi nereducibilno. Izkaže se, da velja $LC(V) \leq ILC(V)$, mi pa bomo pokazali še več. Poglejmo si glavni izrek, ki govori o kardinalnosti pokritij, njegovemu dokazu pa je namenjeno tretje in četrto podpoglavje tega poglavja.

5.2 Glavni izrek

Izrek 12 (Glavni izrek). *Naj bo V vektorski prostor nad poljem F.*

1. *Če je vektorski prostor končno razsežen ($\dim V < \infty$) ali je polje, nad katerim se prostor razpenja, končno ($|F| < \infty$), potem velja $LC(V) = |F| + 1$.*
2. *Če sta dimenzija prostora in moč njegovega polja ($\dim V$ in $|F|$) obe neskončni, potem je $LC(V) = |\mathbb{N}| = \aleph_0$.*
3. *$ILC(V) = |F| + 1$.*

Iz prvega dela izreka opazimo precej presenetljivo dejstvo, da ima končno razsežen vektorski prostor nad neskončnim poljem vedno neskončno pokritje in vsak neskončno razsežen prostor nad končnim poljem končno pokritje. Opazimo tudi, da je za nereducibilna pokritja formula precej enostavnejša, saj velja za vse primere. Poglejmo si zdaj neenakost $LC(V) \leq ILC(V)$ na zgledu 1.

Zgled 6. Po točki 2 glavnega izreka ima pokritje vektorskega prostora polinomov nad realnimi števili ($\mathbb{R}[x]$) moč naravnih števil oziroma je števno neskončno. Naše pokritje $\{W_n\}_{n\in\mathbb{N}}$ je res števno neskončno in je zato po izreku najmanjše kardinalnosti. Po točki 3 glavnega izreka pa vidimo, da je $ILC(V) = |\mathbb{R}|+1$, kar je neštevno neskončna množica. Poiščimo sedaj primer takega nereducibilnega pokritja vektorskega prostora polinomov. Za poljuben polinom $p \in \mathbb{R}[x]$ je enorazsežen vektorski prostor, ki ga pokrije, oblike $t \cdot p$ za $t \in \mathbb{R}$. To so očitno res enorazsežni vektorski podprostori in z njimi res pokrijemo ves $\mathbb{R}[x]$. Očitno je to tudi nereducibilno pokritje (seveda večkrat dobljen isti podprostor damo v pokritje le enkrat). Pokazati moramo še, da je moč tega pokritja res $|\mathbb{R}|$. Naj bo $\{1, x, x^2, x^3, \ldots\}$ baza tega prostora. Definiramo skupino enorazsežnih podprostorov v tej bazi kot $t(a_1, a_2, a_3, \ldots)$, kjer je $t \in \mathbb{R}$ in $a_i \in \{0, 1\}$. Takih podprostorov je ravno $2^{|\mathbb{N}|} = |\mathbb{R}|$. Ker naše pokritje vsebuje vse te, je moč tega pokritja res vsaj $|\mathbb{R}|$, oziroma kar $|\mathbb{R}|$, saj je $|\mathbb{R}[x]| = |\mathbb{R}|$. V tem primeru po izreku velja stroga neenakost $LC(V) < ILC(V)$.

5.3 Pomožne leme in trditve

Za dokaz glavnega izreka si najprej poglejmo tri leme.

Lema 13. *Naj bosta V in W taka vektorska prostora nad poljem F, da velja* $\dim V \geq \dim W \geq 2$. *Potem velja: $LC(V) \leq LC(W)$ in $ILC(V) \leq ILC(W)$.*

Opomba 12. Predpostavka, da sta prostora dimenzije vsaj 2, je potrebna, saj prostori dimenzije 1 nimajo pravih podprostorov in je torej nesmiselno govoriti o pokritjih.

Dokaz. Vemo, da obstaja surjektivna linearna preslikava $q : V \to W$. Naj bo $\{W_i\}_{i\in W}$ neko linearno pokritje vektorskega prostora W. Tedaj je praslika $\{q^{-1}(W_i)\}_{i\in I}$ linearno pokritje vektorskega prostora V in zato je $LC(V)$ kvečjemu manjši od $LC(W)$.
Za nereducibilno linearno pokrivno število naredimo enako, dodatno pa je potreben premislek, da je praslika nereducibilnega pokritja tudi nereducibilno pokritje. Iz osnovnega znanja o množicah in preslikavah vemo, da je to res.

Dokazali smo torej nenavadno dejstvo, da imajo večji prostori (prostori z večjo dimenzijo) manjše pokrivno število kot tisti manjši nad istim poljem. Poglejmo si naslednjo lemo.

Lema 14. *Za poljubno polje F je edino linearno pokritje F^2 množica vseh premic skozi izhodišče. To pokritje je nereducibilno in kardinalnosti $|F| + 1$.*

Dokaz. Očitno je množica premic skozi izhodišče res pokritje, zato je dovolj dokazati, da je to res edino in preveriti kardinalnost ($ILC(F^2)$) tega pokritja. Vemo, da vsak neničelen element $v \in F^2$ leži na natanko eni premici, ki gre skozi izhodišče (premica mora potekati skozi izhodišče, saj vsak podprostor vsebuje enoto za seštevanje, ki je v F^2 ravno izhodišče). Torej res potrebujemo vse take premice: $\{y = \alpha x; \alpha \in F\}$ in dodatno premico $x = 0$. Teh premic je natanko $|F| + 1$.

Lema 15. *Naj bo V vektorski prostor nad poljem F dimenzije* $\dim V \geq 2$. *Potem v V obstaja vsaj $|F| + 1$ hiperravnin (tj. podprostorov dimenzije* $\dim V - 1$*).*

Dokaz. Denimo, da je $\dim V = 2$. Vemo, da je potem V izomorfen F^2 ($V \cong F^2$) in ima zato po prejšnji lemi $|F| + 1$ hiperravnin. Označimo pokritje s temi hiperravninami z $\{L_i\}$.
Poglejmo sedaj za splošno dimenzijo prostora V. Ker je $\dim V \geq 2$, obstaja surjektivna linearna preslikava $q : V \to F^2$. Potem so $\{q^{-1}(L_i)\}$ hiperravnine prostora V. Torej jih je res vsaj $|F| + 1$.

Kaj pa se zgodi, če imamo poljubno pokritje končno razsežnega vektorskega prostora? Po lemi 14 je edino pokritje prostora F^2 množica hiperravnin. Ali se lahko zgodi, da je pokrivno število nekega končnega prostora manjše od števila vseh njegovih hiperravnin? Izkaže se, da ne. Poglejmo si naslednjo trditev.

Trditev 16. *Naj bo V končno razsežen vektorski prostor nad poljem F in naj bo $\{W_i\}_{i\in I}$ poljubno linearno pokritje prostora V. Potem velja $|I| \geq |F| + 1$.*

Dokaz. Ker je vsak pravi podprostor vsebovan v neki hiperravnini, lahko gledamo pokritja s hiperravninami. Dokažimo sedaj našo neenakost z indukcijo po d, kjer je d dimenzija opazovanega prostora.

- $d = 2$: Po lemi 14 tu velja enakost $|I| = |F| + 1$.
- $d - 1 \to d$: Predpostavimo, da neenakost velja za $d - 1$ in dokazujemo, da velja za d. To bomo dokazali s protislovjem. Denimo, da neenakost ne velja za d, torej obstaja linearno pokritje $\{W_i\}_{i\in I}$, da je $|I| < |F| + 1$. Iščemo protislovje. Po lemi 15 obstaja hiperravnina W, ki ni v tem pokritju, saj vemo, da je teh vsaj $|F| + 1$. Potem je $\{W_i \cap W\}_{i\in I}$ pokritje za W. Ker je W hiperravnina, je $\dim W = d - 1$. Dobili smo pokritje za W, za katerega velja $|I| < |F| + 1$, kar pa je v protislovju z indukcijsko predpostavko.

Sedaj je vse pripravljeno za dokaz glavnega izreka. Začnimo s tretjo točko, ki nam pove nereducibilno pokrivno število. Pokazali bomo, da je kardinalnost vsakega nereducibilnega pokritja poljubnega vektorskega prostora nad poljubnim poljem večja ali enaka moči polja plus ena ($|I| \geq |F|+1$). Ker po prej dokazanem vemo tudi $ILC(V) \overset{\text{lema13}}{\leq} ILC(F^2) \overset{\text{lema14}}{=} |F| + 1$ bo res $ILC(V) = |F| + 1$.

5.4 Dokaz glavnega izreka s pomočjo dokazanih lem in trditve

Dokaz (3. dela glavnega izreka). Naj bo $\{W_i\}_{i\in I}$ poljubno nereducibilno linearno pokritje vektorskega prostora V. $W_\star$ naj bo poljuben podprostor iz tega pokritja. Ker je to pokritje nereducibilno, obstajata $u \in W_\star \backslash \bigcup_{i\neq\star} W_i$ in $v \in V \backslash W_\star$. Naj bo $l = \{tu + v; t \in F\}$ afina premica. Očitno velja $|l| = |F|$. Denimo, da obstaja $w = tu + v \in l \cap W_\star$. Potem je $v = w - tu \in W_\star$, kar je v protislovju z izbiro v-ja in zato je torej $l \cap W_\star = \emptyset$. Če bi za nek $i \neq \star$ veljalo $|l \cap W_i| \geq 2$, bi bil $l \subset W_i$ in ker je W_i podprostor, je tudi linearna ogrinjača l-ja vsebovana v W_i. Torej je linearna kombinacija $u = (2u + v) - (u + v)$ vsebovana v W_i, kar je v protislovju z izbiro u-ja. Sledi, da je $|l| = |F| \leq |I\backslash\{\star\}| = |I| - 1$ oziroma $|I| \geq |F| + 1$. Seveda pa v primeru neskončnih kardinalnosti velja $|I| - 1 = |I|$.

Preostane nam še dokaz prvih dveh točk izreka. Dokaz razdelimo na tri dele. V prvem primeru obravnavamo končno razsežne prostore, v drugem neskončno razsežne prostore nad končnim poljem in v zadnjem primeru, ko sta dimenzija prostora in moč polja neskončni.

Dokaz.

Primer 1. Naj bo vektorski prostor V končno razsežen dimenzije $\dim V \geq 2$. Po trditvi 16 je $LC(V) \geq |F| + 1$, po lemi 13 in lemi 14 pa velja $LC(V) \overset{\text{lema13}}{\leq} LC(F^2) \overset{\text{lema14}}{=} |F| + 1$ (saj lahko F^2 gledamo kot podprostor v V). Torej velja $LC(V) = |F| + 1$.

Primer 2. Naj bo sedaj V neskončno razsežen vektorski prostor nad končnim poljem F. Potem je $LC(V) \overset{\text{lema13}}{\leq} LC(F^2) \overset{\text{lema14}}{=} |F| + 1 < \aleph_0$. Denimo, da obstaja tako linearno pokritje $\{W_i\}_{i=1}^n$ prostora V, da velja $n < |F| + 1$. Ker je n končno število, lahko najdemo nereducibilno podpokritje z odvzemanjem podprostorov. Tako smo dobili nereducibilno pokritje z m podprostori ($m \leq n$), za katerega velja $m \leq n < |F| + 1$, kar pa je v protislovju z že dokazano tretjo točko glavnega izreka. Torej velja $LC(V) = |F| + 1$.

Primer 3. Naj bosta zdaj dimenzija prostora V in moč polja neskončni. Naj bo $W = \bigoplus_{i=1}^{\infty} F$ vektorski prostor dimenzije $\aleph_0$ (neskončna števna direktna vsota). Za $n \in \mathbb{N}$ naj bo $W_n := \bigoplus_{i=1}^{n} F$. Potem je $\{W_n\}_{n=1}^{\infty}$ pokritje prostora W s kardinalnostjo $\aleph_0$. Ker je $\dim V \geq \dim W$, je po lemi 13 $LC(V) \leq LC(W) = \aleph_0$. Preostane nam še pokazati, da V ne moremo pokriti s končnim pokritjem. Denimo, da obstaja končno pokritje. Kot pri primeru 2 bi sledilo, da obstaja končno nereducibilno pokritje. Prišli bi v protislovje z že dokazano tretjo točko izreka.

6. Pokritja afinih prostorov

Definicija 12. Naj bo V končno razsežen vektorski prostor nad poljem F, U vektorski podprostor prostora V in naj bo $a \in V$. Množico $a+U = \{a+x; x \in U\}$ imenujemo *afin podprostor* vektorskega prostora V.

Afino pokritje vektorskega prostora je torej pokritje s primernimi translacijami vektorskih podprostorov. Na prvi pogled se zdi, da bodo števila teh pokritij enaka, vendar v resnici pride do manjših sprememb. Preden si pogledamo preoblikovan glavni izrek, definirajmo afino pokrivno število.

Definicija 13. *Afino pokrivno število vektorskega prostora V ($AC(V)$)* je najmanjša možna kardinalnost afinega pokritja $\{W_i\}_{i\in I}$ za V (moč indeksne množice).

Definicija 14. *Nereducibilno afino pokrivno število vektorskega prostora V ($IAC(V)$)* je najmanjša možna kardinalnost nereducibilnega afinega pokritja $\{W_i\}_{i\in I}$ za V (moč indeksne množice).

Definiciji sta tako rekoč enaki, le da sedaj štejemo kardinalnost afinega pokritja.

6.1 Prirejen glavni izrek

Izrek 17 (Prirejen glavni izrek). *Naj bo V vektorski prostor nad poljem F.*

1. *Če je vektorski prostor končno razsežen ($\dim V < \infty$) ali je polje, nad katerim se prostor razpenja, končno, potem velja $AC(V) = |F|$.*
2. *Če sta dimenzija prostora in moč njegovega polja ($\dim V$ in $|F|$) obe neskončni, potem je $AC(V) = |\mathbb{N}| = \aleph_0$.*
3. *$IAC(V) = |F|$.*

Izrek se torej spremeni v prvi in tretji točki. Poglejmo si, kje točno je prišlo do spremembe.

6.2 Vzporednice v dokazih

Dokaz prirejenega glavnega izreka je precej podoben dokazu glavnega izreka. Razlog za spremenjen rezultat je lema 14, ki se prepiše v naslednjo lemo.

Lema 18. *Za poljubno polje F je njegovo edino afino pokritje množica vseh točk iz F. To je nereducibilno afino pokritje kardinalnosti $|F|$.*

Posledično se spremenita tudi lema 15 in trditev 16.

Lema 19. *Za vektorski prostor V nad poljem F obstaja vsaj $|F|$ afinih hiperravnin.*

Preostanek dokaza je analogen dokazu glavnega izreka, kjer je upoštevano še dejstvo, da je presek dveh afinih hiperravnin prazen ali pa afina hiperravnina vsakega od teh dveh afinih prostorov.

V dokazu tretje točke premico l definiramo kot $l = \{(1-t)u + tv; t \in F\}$ in s tem je dokaz spremenjen. Opomnimo še, da tu ni potrebno preverjati, ali je $|l \cap W_i| \geq 2$.

7. Zaključek

Problem pokritja je zelo razdrobljen v različnih smereh. Nekateri rezutlati so že precej stari, večinoma gre pa za novejše rezultate. Opazimo, da je na nekaterih algebrskih strukturah enostavno ugotoviti pokrivnost in nas zato zanima predvsem pokrivno število. Tako je v vektorskih prostorih nesmiselno govoriti o pokrivnosti, saj so z izjemo enorazsežnih vektroskih prostorov ti vedno pokriti s svojimi enorazsežnimi podprostori. Na drugih, kot so grupe in kolobarji, pa imamo lahko probleme že s samim ugotavljanjem pokrivnosti in o pokrivnem številu ne znamo kaj dosti povedati. Zato se najprej zatečemo k posebnim primerom. Pri grupah smo tako videli, da lahko o pokritjih govorimo samo v primeru necikličnih grup. Najprej smo ugotovili, da pokrivno število ne more biti 2, imamo pa nekaj pogojev, kdaj je pokrivno število grupe $3, 4, 5$. V splošnem ne znamo izračunati pokrivnega števila. Pogledali smo si tudi, kako je s pokritji kvocientnih grup in pokritji končnih produktov grup. Za kolobarje imamo karakterizacijo za pokrivnost, ki nam da enostaven dokaz o neobstoju pokrivnosti, za dokaz obstoja pa je nekoliko nepraktična. Prav tako smo si tu ogledali, kako je s pokritji kvocientnih kolobarjev in pokritji končnih produktov kolobarjev. Pri vektorskih prostorih pa se izkaže, da znamo izračunati pokrivno število in nereducibilno pokrivno število za poljuben vektorski prostor. Videli smo torej, da še vedno obstaja veliko odprtih podproblemov znotraj problemov pokrivnosti.

LITERATURA

[1] N. Deo, *Graph theory with applications to engineering and computer science*, Courier Dover Publications, 2017.

[2] J. Csirik in G. J. Woeginger, *On-line packing and covering problems*, objavljeno v A. Fiat , G. J. Woeginger (urednika), *Online Algorithms*, Lecture Notes in Computer Science **1442**, Springer (1998), 147–177.

[3] S. Haber in A. Rosenfeld, *Groups as Unions of Proper Subgroups*, The American Mathematical Monthly **66**(6) (1959), 491–494.

[4] J. H. E. Cohn, *On n-Sum Groups*, Mathematica Scandinavica **75** (1994), 44–58.

[5] R. A. Bryce, V. Fedri in L. Serena, *Subgroup coverings of some linear groups*, Bulletin of the Australian Mathematical Society **60**(2) (1999), 227–238.

[6] P. E. Holmes, *Subgroup coverings of some sporadic groups*, Journal of Combinatorial Theory, Ser. A **113** (2006), 1204–1213.

[7] L. -C. Kappe in J. L. Redden, *On the covering number of small alternating groups*, Contemporary Mathematics **511** (2010), 109–125.

[8] A. Maróti, *Covering the symmetric groups with proper subgroups*, Journal of Combinatorial Theory, Ser. A **110** (2005), 97–111.

[9] M. J. Tomkinson, *Groups as the union of proper subgroups*, Mathematica Scandinavica **81** (1997), 191–198.

[10] A. Lucchini, A. Maróti, *Rings as the Unions of Proper Subrings*, Algebras and Representation Theory **15** (2012), 1035–1047.

[11] A. Lucchini, A. Maróti, *Rings as the Unions of Proper Subrings* (2010), dostopno na [http://arxiv.org/abs/1001.3984v1].

[12] N. J. Werner, *Covering numbers of finite rings*, The American Mathematical Monthly **122**(6) (2015), 552–566.

[13] H. E. Turkey in C. M. Pray, *A note on the covering number of some finite rings*, Minnesota Journal of Undergraduate Mathematics, **2**(1)(2017).

[14] P. L. Clark, *Covering numbers in linear algebra*, The American Mathematical Monthly **119** (2012) , 65–67.