Latvijas Universitāte
Fizikas un matemātikas fakultāte
Matemātikas nodaļa
Matemātiskās analīzes katedra

Jānis Buls

VARBŪTISKIE MODEĻI KLASISKAJĀ KRIPTOGRĀFIJĀ

2008

Ievads

Varbūtiskajos modeļos pamattekstu avots tiek aplūkots kā gadījumvirkņu avots. Pieņemsim, ka avots ģenerē alfabēta A galīga vai bezgalīga garuma tekstu. Precizēsim, proti, uzskatīsim, ka avots ģenerē galīgu vai bezgalīgu gadījuma burtu (simbolu) virkni $x_0, x_1, \ldots, x_{n-1}, \ldots$ kur visi $x_i \in A$. Nejauša ziņojuma $a_0a_1 \ldots a_{n-1}$ varbūtību definējam kā sekojošas notikumu virknes varbūtību:

$$P(a_0a_1 \ldots a_{n-1}) \rightleftharpoons P\{x_0 = a_0 \wedge x_1 = a_1 \wedge \ldots \wedge x_{n-1} = a_{n-1}\}.$$

Nejaušo ziņojumu kopa veido varbūtību telpu, ja izpildās sekojoši nosacījumi:

1. $P(a_0a_1 \ldots a_{n-1}) \geq 0$ katram nejaušam ziņojumam $a_0a_1 \ldots a_{n-1}$;
2. $$\sum_{(a_0,a_1,\ldots,a_{n-1})} P(a_0a_1 \ldots a_{n-1}) = 1;$$
3. katram nejaušam ziņojumam $a_0a_1 \ldots a_{n-1}$ un katram $s > n$:

   $$P(a_0a_1 \ldots a_{n-1}) = \sum_{(a_n,a_{n+1},\ldots,a_{s-1})} P(a_0a_1 \ldots a_{s-1}),$$

   proti, katra nejauša ziņojuma ar garumu n varbūtība ir visu to ziņojumu virkņu, kas papildinātas līdz garumam s, varbūtību summa.

Teksts, ko rada šāds avots, ir valodas varbūtiskais analogs. Uzdodot noteiktu varbūtību sadalījumu pamattekstu kopā, mēs uzdodam atbilstošu avota modeli.

Taču šajā brīdī rodas standartjautājums:
— Kas šai gadījumā ir elementāru notikumu telpa?

Mazliet vispārīgāk, taču turpinot to pašu domu:
— Kas tad šai gadījumā ir varbūtību telpa?

Šī raksta mērķis ir definēt varbūtību telpu tā, lai katrs ziņojums būtu šīs varbūtību telpas notikums.

Apzīmējumi

$\neg$ — negācija,
$\vee$ — disjunkcija, $\wedge$ — konjunkcija,
$\Rightarrow$ — implikācija, $\Leftrightarrow$ — ekvivalence,
$\mathfrak{A} \sim a$ — izteikums $\mathfrak{A}$ ir aplams,
$\mathfrak{A} \sim p$ — izteikums $\mathfrak{A}$ ir patiess,
$\exists$ — eksistences kvantors, $\forall$ — universālkvantors,
$\exists! x\ P(x)$ — eksistē viens vienīgs tāds x, kam izpildās nosacījums $P(x)$,

$x \in X$ — elements x pieder kopai X jeb x ir kopas X elements,
$A \subseteq B$ — kopa A ir kopas B apakškopa,
$A \cup B$, $A \cap B$, $A \setminus B$ — kopu A un B apvienojums, šķēlums, starpība,
$\min K$ — kopas K minimālais elements,
$\max K$ — kopas K maksimālais elements,

$\rightleftharpoons$, $\rightharpoonup$ — vienādības saskaņā ar definīciju,
$\overline{1,n} \rightleftharpoons \{1,2,\ldots,n\}$; $\overline{k,n} \rightleftharpoons \{k,k+1,\ldots,n\}$, te $k \leq n$,
$\mathbb{Z}$ — veselo skaitļu kopa, $\mathbb{Z}_+ \rightleftharpoons \{x \,|\, x \in \mathbb{Z} \wedge x > 0\}$,
$\mathbb{N} \rightleftharpoons \mathbb{Z}_+ \cup \{0\}$, $\mathbb{N}_- \rightleftharpoons \mathbb{Z} \setminus \mathbb{Z}_+$,
$\mathbb{P}$ — visu pirmskaitļu kopa,
$\mathbb{Q}$ — racionālo skaitļu kopa,
$\mathbb{R}$ — reālo skaitļu kopa, $\mathbb{C}$ — komplekso skaitļu kopa,
$|K|$ — kopas K apjoms,
$\aleph_0$ — kopas $\mathbb{N}$ apjoms, $\mathfrak{c}$ — reālo skaitļu kopas $\mathbb{R}$ apjoms,

$\langle x,y\rangle \rightleftharpoons (x,y) \rightleftharpoons \{\{x\},\{x,y\}\}$,
$x_1x_2\ldots x_n \rightleftharpoons \langle x_1,x_2,\ldots,x_n\rangle \rightleftharpoons (x_1,x_2,\ldots,x_n) \rightleftharpoons ((x_1,x_2,\ldots,x_{n-1}),x_n)$,
$A_1 \times A_2 \times \ldots \times A_n \rightleftharpoons \{(x_1,x_2,\ldots,x_n) \,|\, \forall i \in \overline{1,n}\,(x_i \in A_i)\}$, A^n, $|u|$,
$f : x \mapsto y$, $f : X \multimap Y$, $X \overset{f}{\multimap} Y$,
$\mathrm{Dom}(f) \rightleftharpoons \{x \,|\, \exists y \in Y\,(f : x \mapsto y)\}$, $\mathrm{Ran}(f) \rightleftharpoons \{y \,|\, \exists x \in X\,(f : x \mapsto y)\}$,
$f : X \to Y$, $X \overset{f}{\to} Y$, $f : X \twoheadrightarrow Y$, $f : X \hookrightarrow Y$,
$\mathrm{pr}_i \varrho$, $\mathrm{pr}_i g$,
A^+, λ, A^*, u^n,

$$\sum_{i=k}^{m} a_i \rightleftharpoons a_k + a_{k+1} + \ldots + a_m,$$

$\prod_{i=k}^{m} a_i \rightleftharpoons a_k a_{k+1} \dots a_m,$

$a \diagdown b$ — skaitlis b ir skaitļa a daudzkārtnis,
$D(a_1, a_2, \dots, a_n) \rightleftharpoons \{q \,|\, \forall i \in \overline{1,n}\ q \diagdown a_i\},$
$\mathrm{ld}(a_1, a_2, \dots, a_n) \rightleftharpoons \max D(a_1, a_2, \dots, a_n),$
$a \equiv b (\mathrm{mod}\ m)$ — skaitļi a un b ir kongruenti pēc moduļa m,
$\mathbb{Z}_m \rightleftharpoons \{0, 1, \dots, m-1\},$
$\mathbb{Z}_m^* \rightleftharpoons \{\ a \mid \mathrm{ld}(a, m) = 1\ \wedge\ a \in \mathbb{Z}_m\},$

$\square$ — pierādījuma sākums,
$\blacksquare$ — pierādījuma beigas;
$\Rightarrow$ — implikācijas zīmi pierādījuma sākumā mēs izmantojam, lai norādītu, ka tagad sākas teorēmas nepieciešamā nosacījuma pierādījums,
$\Leftarrow$ — šo zīmi pierādījumos mēs izmantojam, lai norādītu, ka tagad sākas teorēmas pietiekamā nosacījuma pierādījums.

1. Karateodori teorēma

Pieņemsim, ka dota patvaļīgi fiksēta kopa Ω un šīs kopas visu apakškopu kopa

$$\mathfrak{P}(\Omega) \rightleftharpoons \{\mathcal{A} \,|\, \mathcal{A} \subseteq \Omega\}.$$

Definīcija 1.1. *Kopas $\mathfrak{P}(\Omega)$ apakškopu $\mathfrak{A}$ sauc par algebru, ja:*

(i) $\Omega \in \mathfrak{A}$;

(ii) $\mathcal{A} \in \mathfrak{A} \Rightarrow \bar{\mathcal{A}} \rightleftharpoons \Omega \setminus \mathcal{A} \in \mathfrak{A}$;

(iii) $\mathcal{A} \in \mathfrak{A} \wedge \mathcal{B} \in \mathfrak{A} \Rightarrow \mathcal{A} \cup \mathcal{B} \in \mathfrak{A} \wedge \mathcal{A} \cap \mathcal{B} \in \mathfrak{A}$

Terminu *kopu saime* $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ mēs lietosim kā ekvivalentu apgalvojumam: kopas $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ elementi ir kopas $\mathcal{A}_i$. Kopu saimi $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ sauc par *galīgu*, ja $\mathcal{I}$ ir galīga kopa vai arī tā ir tukša kopa. Saimi $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ sauc par *sanumurējamu*, ja $\mathcal{I}$ ir sanumurējama, galīga vai tukša kopa.

Turpmāk, lai atslogotu apzīmējumus, ja no konteksta būs noprotama indeksu kopa $\mathcal{I}$ vai arī tās daba nebūs būtiska, mēs lietosim pierakstu

$$\{\mathcal{A}_i\} \rightleftharpoons \{\mathcal{A}_i \,|\, i \in \mathcal{I}\}.$$

Definīcija 1.2. *Kopu saimi $\{\mathcal{A}_i\}$ sauc par disjunktu, ja*

$$\forall i \forall j \; (i \neq j \Rightarrow \mathcal{A}_i \cap \mathcal{A}_j = \emptyset).$$

Speciālā gadījumā kopas $\mathcal{A}$ un $\mathcal{B}$ sauc par *disjunktām*, ja $\mathcal{A} \cap \mathcal{B} = \emptyset$.

Algebru $\mathfrak{A}$ sauc par σ–algebru, ja katrai sanumurējamai algebras $\mathfrak{A}$ kopu saimei $\{\mathcal{A}_i\}$

$$\bigcup_i \mathcal{A}_i \in \mathfrak{A} \qquad \text{un} \qquad \bigcap_i \mathcal{A}_i \in \mathfrak{A}.$$

Algebrā $\mathfrak{A}$ definētu attēlojumu

$$\mu \;:\; \mathfrak{A} \to [0; +\infty]$$

sauc par *aditīvu*, ja katram algebras $\mathfrak{A}$ disjunktam kopu pārim $\mathcal{A}$, $\mathcal{B}$

$$\mu(\mathcal{A} \cup \mathcal{B}) = \mu(\mathcal{A}) + \mu(\mathcal{B}).$$

σ–algebrā $\mathfrak{A}$ definētu aditīvu attēlojumu $\mu : \mathfrak{A} \to [0; +\infty]$ sauc par σ–*aditīvu*, ja katrai algebras $\mathfrak{A}$ sanumurējamai disjunktai kopu saimei $\{\mathcal{A}_i\}$

$$\mu(\bigcup_i \mathcal{A}_i) = \sum_i \mu(\mathcal{A}_i).$$

σ–algebrā $\mathfrak{A}$ definētu σ–aditīvu attēlojumu $\mu : \mathfrak{A} \to [0; +\infty]$ sauc par *mēru*, ja $\mu(\emptyset) = 0$. Mēru μ sauc par *varbūtību*, ja $\mu(\Omega) = 1$.

Definīcija 1.3. *Trijnieku*

$$\langle \Omega, \mathfrak{A}, \mathcal{P} \rangle$$

sauc par varbūtību telpu, ja:

(i) Ω — *fiksēta kopa;*

(ii) $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ *ir* σ*–algebra;*

(iii) $\mathcal{P}$ *ir algebrā* $\mathfrak{A}$ *definēta varbūtība.*

Definīcija 1.4. *Kopu saimi* $\{\mathcal{A}_i\}$ *sauc par kopas* $\mathcal{A}$ *pārklājumu, ja*

$$\mathcal{A} \subseteq \bigcup_i \mathcal{A}_i.$$

Pārklājumu $\{\mathcal{A}_i \mid i \in \mathcal{I}\}$ sauc par *galīgu*, ja $\mathcal{I}$ ir galīga vai arī tukša kopa. Saskaņā ar definīciju mēs pieņemam, ka

$$\bigcup_{i \in \emptyset} \mathcal{A}_i = \emptyset.$$

Pārklājumu sauc par *sanumurējamu*, ja $\mathcal{I}$ ir sanumurējama, galīga vai tukša kopa.

Algebrā $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ definētu attēlojumu $\mu : \mathfrak{A} \to [0; +\infty]$ sauc par *pusaditīvu*, ja katram galīgam kopas $\mathcal{A} \in \mathfrak{A}$ pārklājumam $\{\mathcal{A}_i\}$ ar kopas $\mathfrak{A}$ elementiem

$$\mu(\mathcal{A}) \leq \sum_i \mu(\mathcal{A}_i).$$

Šo attēlojumu sauc par σ*–pusaditīvu*, ja katram sanumurējamam kopas $\mathcal{A}$ pārklājumam $\{\mathcal{A}_i\}$ ar kopas $\mathfrak{A}$ elementiem

$$\mu(\mathcal{A}) \leq \sum_i \mu(\mathcal{A}_i).$$

Definīcija 1.5. *Pieņemsim, ka*

$$\mu \ : \ \mathfrak{P}(\Omega) \to [0; +\infty]$$

ir σ–pusaditīvs attēlojums un $\mu(\emptyset) = 0$. Saka, ka kopa $\mathcal{A} \subseteq \Omega$ pareizi sadala kopu $E \subseteq \Omega$, ja

$$\mu(E) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}).$$

Kopu $\mathcal{A} \subseteq \Omega$ sauc par *μ–mērojamu*, ja tā pareizi sadala katru kopu $E \subseteq \Omega$. Tātad kopu $\mathcal{A}$ sauc par μ–mērojamu, ja

$$\forall E \subseteq \Omega \quad \mu(E) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}). \tag{1}$$

Apgalvojums 1.6. *Nosacījums* (1) *ir ekvivalents nosacījumam*

$$\forall E_1 \forall E_2 \ (E_1 \subseteq \mathcal{A} \wedge E_2 \subseteq \bar{\mathcal{A}} \ \ \Rightarrow \ \ \mu(E_1 \cup E_2) = \mu(E_1) + \mu(E_2)). \tag{2}$$

$\square \Rightarrow$ Pieņemsim, ka $E_1 \subseteq \mathcal{A}$ un $E_2 \subseteq \bar{\mathcal{A}}$, tad $E \rightleftharpoons E_1 \cup E_2$ un $E \cap \mathcal{A} = E_1$, $E \cap \bar{\mathcal{A}} = E_2$. No šejienes

$$\mu(E_1 \cup E_2) = \mu(E) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}) = \mu(E_1) + \mu(E_2).$$

$\Leftarrow$ Pieņemsim, ka $E \subseteq \Omega$, tad $E_1 \rightleftharpoons E \cap \mathcal{A} \subseteq \mathcal{A}$ un $E_2 \rightleftharpoons E \cap \bar{\mathcal{A}} \subseteq \bar{\mathcal{A}}$. No šejienes

$$\mu(E) = \mu(E_1 \cup E_2) = \mu(E_1) + \mu(E_2) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}). \quad \blacksquare$$

Teorēma 1.7 (Karateodori). *Ja $\mu : \mathfrak{P}(\Omega) \to [0; +\infty]$ ir σ–pusaditīvs attēlojums un $\mu(\emptyset) = 0$, tad visu μ–mērojamo kopu saime $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ ir σ–algebra un μ sašaurinājums kopā $\mathfrak{A}$ ir mērs.*

$\square$ Tā kā μ ir σ–pusaditīvs attēlojums, tad

$$\mu(E) \leq \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}),$$

jo $\{E \cap \mathcal{A}, E \cap \bar{\mathcal{A}}\}$ ir kopas E pārklājums. Tas ļauj secināt, ka kopa $\mathcal{A}$ pareizi sadala kopu E tad un tikai tad, ja

$$\mu(E) \geq \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}).$$

(i) *Kopu saime $\mathfrak{A}$ ir algebra.*

- Tā kā $\mu(\emptyset) = 0$, tad

$$\begin{aligned}\mu(E \cap \Omega) + \mu(E \cap \bar{\Omega}) &= \mu(E) + \mu(E \cap \emptyset) = \mu(E) + \mu(\emptyset) \\ &= \mu(E) + 0 = \mu(E).\end{aligned}$$

  Līdz ar to $\Omega \in \mathfrak{A}$. Tai pašā laikā

$$\mu(E \cap \emptyset) + \mu(E \cap \bar{\emptyset}) = \mu(\emptyset) + \mu(E \cap \Omega) = 0 + \mu(E) = \mu(E).$$

  Tātad arī $\emptyset \in \mathfrak{A}$.

- Pieņemsim, ka $\mathcal{A} \in \mathfrak{A}$, tad

$$\mu(E) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}) = \mu(E \cap \bar{\mathcal{A}}) + \mu(E \cap \bar{\bar{\mathcal{A}}}).$$

  Tas parāda, ka $\bar{\mathcal{A}} \in \mathfrak{A}$.

- Pieņemsim, ka $\mathcal{A}_1 \in \mathfrak{A}$ un $\mathcal{A}_2 \in \mathfrak{A}$, tad $\mathcal{A} \rightleftharpoons \mathcal{A}_1 \cap \mathcal{A}_2$ un

$$\mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}) = \mu(E \cap \mathcal{A}_1 \cap \mathcal{A}_2) + \mu(E_1),$$

  kur

$$E_1 \rightleftharpoons E \cap \overline{\mathcal{A}_1 \cap \mathcal{A}_2} = E \cap (\bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2).$$

  Tā kā $\mathcal{A}_1 \in \mathfrak{A}$, tad

$$\begin{aligned}\mu(E_1) &= \mu(E_1 \cap \mathcal{A}_1) + \mu(E_1 \cap \bar{\mathcal{A}}_1); \\ E_1 \cap \mathcal{A}_1 &= E \cap (\bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2) \cap \mathcal{A}_1 = E \cap \mathcal{A}_1 \cap \bar{\mathcal{A}}_2; \\ E_1 \cap \bar{\mathcal{A}}_1 &= E \cap (\bar{\mathcal{A}}_1 \cup \bar{\mathcal{A}}_2) \cap \bar{\mathcal{A}}_1 = E \cap \bar{\mathcal{A}}_1.\end{aligned}$$

  Līdz ar to

$$\mu(E_1) = \mu(E \cap \mathcal{A}_1 \cap \bar{\mathcal{A}}_2) + \mu(E \cap \bar{\mathcal{A}}_1)$$

  Pieņemsim, ka $E_2 \rightleftharpoons E \cap \mathcal{A}_1$, tad

$$\begin{aligned}\mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}) &= \mu(E \cap \mathcal{A}_1 \cap \mathcal{A}_2) + \mu(E_1) \\ &= \mu(E_2 \cap \mathcal{A}_2) + \mu(E_1 \cap \mathcal{A}_1) + \mu(E_1 \cap \bar{\mathcal{A}}_1) \\ &= \mu(E_2 \cap \mathcal{A}_2) + \mu(E \cap \mathcal{A}_1 \cap \bar{\mathcal{A}}_2) + \mu(E \cap \bar{\mathcal{A}}_1) \\ &= \mu(E_2 \cap \mathcal{A}_2) + \mu(E_2 \cap \bar{\mathcal{A}}_2) + \mu(E \cap \bar{\mathcal{A}}_1) \\ &= \mu(E_2) + \mu(E \cap \bar{\mathcal{A}}_1) \\ &= \mu(E \cap \mathcal{A}_1) + \mu(E \cap \bar{\mathcal{A}}_1) = \mu(E).\end{aligned}$$

Tātad $\mathcal{A} = \mathcal{A}_1 \cap \mathcal{A}_2 \in \mathfrak{A}$.

Tā kā $\mathcal{A}_1 \in \mathfrak{A}$ un $\mathcal{A}_2 \in \mathfrak{A}$, tad $\bar{\mathcal{A}}_1 \in \mathfrak{A}$ un $\bar{\mathcal{A}}_2 \in \mathfrak{A}$, tāpēc $\bar{\mathcal{A}}_1 \cap \bar{\mathcal{A}}_2 \in \mathfrak{A}$. No šejienes $\overline{\bar{\mathcal{A}}_1 \cap \bar{\mathcal{A}}_2} \in \mathfrak{A}$. Līdz ar to

$$\mathcal{A}_1 \cup \mathcal{A}_2 = \overline{\overline{\mathcal{A}_1 \cup \mathcal{A}_2}} = \overline{\bar{\mathcal{A}}_1 \cap \bar{\mathcal{A}}_2} \in \mathfrak{A}.$$

(ii) *Attēlojuma μ sašaurinājums algebrā $\mathfrak{A}$ ir aditīvs.*
Pieņemsim, ka $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$ un $\mathcal{A}_1 \in \mathfrak{A}$, $\mathcal{A}_2 \in \mathfrak{A}$, tad

$$\mu(\mathcal{A}_1 \cup \mathcal{A}_2) = \mu((\mathcal{A}_1 \cup \mathcal{A}_2) \cap \mathcal{A}_1) + \mu((\mathcal{A}_1 \cup \mathcal{A}_2) \cap \bar{\mathcal{A}}_1) = \mu(\mathcal{A}_1) + \mu(\mathcal{A}_2 \cap \bar{\mathcal{A}}_1).$$

Tā kā $\mathcal{A}_1 \cap \mathcal{A}_2 = \emptyset$, tad $\mathcal{A}_2 \subseteq \bar{\mathcal{A}}_1$, tāpēc $\mathcal{A}_2 \cap \bar{\mathcal{A}}_1 = \mathcal{A}_2$. Līdz ar to

$$\mu(\mathcal{A}_1 \cup \mathcal{A}_2) = \mu(\mathcal{A}_1) + \mu(\mathcal{A}_2).$$

(iii) *Ja $\{\mathcal{A}_i\}$ ir disjunktu kopu saime un $\forall i$ $\mathcal{A}_i \in \mathfrak{A}$, tad*

$$\forall E \subseteq \Omega \; \forall n \in \mathbb{Z}_+ \quad \mu(E \cap (\bigcup_{i=1}^{n} \mathcal{A}_i)) = \sum_{i=1}^{n} \mu(E \cap \mathcal{A}_i).$$

Vispirms šo vienādību pierādīsim divām kopām.

$$\mu(E \cap (\mathcal{A}_1 \cup \mathcal{A}_2)) = \mu((E \cap \mathcal{A}_1) \cup (E \cap \mathcal{A}_2)).$$

$$E \cap \mathcal{A}_1 \subseteq \mathcal{A}_1 \quad \text{un} \quad E \cap \mathcal{A}_2 \subseteq \mathcal{A}_2 \subseteq \bar{\mathcal{A}}_1,$$

tāpēc (Apgalvojums 1.6)

$$\mu((E \cap \mathcal{A}_1) \cup (E \cap \mathcal{A}_2)) = \mu(E \cap \mathcal{A}_1) + \mu(E \cap \mathcal{A}_2).$$

Tālākie spriedumi induktīvi.

$$\mu(E \cap (\bigcup_{i=1}^{n+1} \mathcal{A}_i)) = \mu[(E \cap \mathcal{A}_1) \cup (E \cap (\bigcup_{i=2}^{n+1} \mathcal{A}_i))].$$

$$E \cap \mathcal{A}_1 \subseteq \mathcal{A}_1 \quad \text{un} \quad E \cap (\bigcup_{i=2}^{n+1} \mathcal{A}_i) \subseteq \bigcup_{i=2}^{n+1} \mathcal{A}_i \subseteq \bar{\mathcal{A}}_1,$$

tāpēc (Apgalvojums 1.6)

$$\mu[(E\cap\mathcal{A}_1)\cup(E\cap(\bigcup_{i=2}^{n+1}\mathcal{A}_i))] = \mu(E\cap\mathcal{A}_1)+\mu(E\cap(\bigcup_{i=2}^{n+1}\mathcal{A}_i))$$

tagad izmantojam indukcijas pieņēmumu

$$= \mu(E\cap\mathcal{A}_1)+\sum_{i=2}^{n+1}\mu(E\cap\mathcal{A}_i)$$
$$= \sum_{i=1}^{n+1}\mu(E\cap\mathcal{A}_i).$$

(iv) *Ja* $\{\mathcal{A}_i\}$ *ir sanumurējama disjunkta kopu saime un* $\forall i\ \mathcal{A}_i\in\mathfrak{A}$*, tad*

$$\mathcal{A}=\bigcup_{i=1}^{\infty}\mathcal{A}_i\in\mathfrak{A}.$$

Ievērojam:

$$\mathcal{A}=\bigcup_{i=1}^{\infty}\mathcal{A}_i\supseteq\bigcup_{i=1}^{n}\mathcal{A}_i,$$

tāpēc $\bar{\mathcal{A}}\subseteq\overline{\bigcup_{i=1}^{n}\mathcal{A}_i}$. Līdz ar to $E\cap\bar{\mathcal{A}}\subseteq E\cap\overline{\bigcup_{i=1}^{n}\mathcal{A}_i}$. Ņemot vērā μ pusaditivitāti, iegūstam

$$\mu(E\cap\overline{\bigcup_{i=1}^{n}\mathcal{A}_i})\geq\mu(E\cap\bar{\mathcal{A}}).$$

Tā kā $\mathfrak{A}$ ir algebra, tad $\bigcup_{i=1}^{n}\mathcal{A}_i\in\mathfrak{A}$, tāpēc, ievērojot (iii), patvaļīgai kopai $E\subseteq\Omega$

$$\mu(E)=\mu(E\cap(\bigcup_{i=1}^{n}\mathcal{A}_i))+\mu(E\cap\overline{\bigcup_{i=1}^{n}\mathcal{A}_i})\geq\sum_{i=1}^{n}\mu(E\cap\mathcal{A}_i)+\mu(E\cap\bar{\mathcal{A}}).$$

No šejienes

$$\mu(E)\geq\lim_{n\to\infty}\sum_{i=1}^{n}\mu(E\cap\mathcal{A}_i)+\mu(E\cap\bar{\mathcal{A}})=\sum_{i=1}^{\infty}\mu(E\cap\mathcal{A}_i)+\mu(E\cap\bar{\mathcal{A}}).$$

Tā kā μ ir σ–pusaditīvs, tad

$$\mu(E\cap\mathcal{A})=\mu(E\cap(\bigcup_{i=1}^{\infty}\mathcal{A}_i))=\mu(\bigcup_{i=1}^{\infty}(E\cap\mathcal{A}_i))\leq\sum_{i=1}^{\infty}\mu(E\cap\mathcal{A}_i).$$

Līdz ar to

$$\mu(E) \geq \sum_{i=1}^{\infty} \mu(E \cap \mathcal{A}_i) + \mu(E \cap \bar{\mathcal{A}}) \geq \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}).$$

Tas atsaucoties uz teorēmas pierādījuma sākumā teikto ļauj secināt, ka

$$\mu(E) = \mu(E \cap \mathcal{A}) + \mu(E \cap \bar{\mathcal{A}}),$$

t.i., $\mathcal{A} \in \mathfrak{A}$.

(v) *Ja* $\{\mathcal{A}_i\}$ *ir sanumurējama disjunkta kopu saime,* $\forall i$ $\mathcal{A}_i \in \mathfrak{A}$ *un* $\mathcal{A} = \bigcup\limits_{i=1}^{\infty} \mathcal{A}_i \in \mathfrak{A}$*, tad*

$$\mu(\mathcal{A}) = \sum_{i=1}^{\infty} \mu(\mathcal{A}_i).$$

Pierādījuma (iv) punktā mēs konstatējām, ka patvaļīgai kopai $E \subseteq \Omega$

$$\mu(E) \geq \sum_{i=1}^{\infty} \mu(E \cap \mathcal{A}_i) + \mu(E \cap \bar{\mathcal{A}}).$$

Tagad ņemot E lomā kopu $\mathcal{A}$ iegūstam

$$\mu(\mathcal{A}) \geq \sum_{i=1}^{\infty} \mu(\mathcal{A} \cap \mathcal{A}_i) + \mu(\mathcal{A} \cap \bar{\mathcal{A}}) = \sum_{i=1}^{\infty} \mu(\mathcal{A}_i) + \mu(\emptyset) = \sum_{i=1}^{\infty} \mu(\mathcal{A}_i).$$

Tā kā μ ir σ–pusaditīvs attēlojums, tad

$$\mu(\mathcal{A}) = \mu(\bigcup_{i=1}^{\infty} \mathcal{A}_i) \leq \sum_{i=1}^{\infty} \mu(\mathcal{A}_i).$$

Līdz ar to $\mu(\mathcal{A}) = \sum\limits_{i=1}^{\infty} \mu(\mathcal{A}_i)$.

(vi) $\mathfrak{A}$ *ir* σ*–algebra.*

Pieņemsim, ka $\{\mathcal{A}_i \mid i \in \mathbb{Z}_+\}$ ir algebras $\mathfrak{A}$ kopu saime. Mums jāparāda, ka $\bigcup\limits_{i=1}^{\infty} \mathcal{A}_i \in \mathfrak{A}$. Definējam jaunas kopas

$$\mathcal{B}_i \leftarrows \begin{cases} \mathcal{A}_i, & \text{ja} \quad i = 1; \\ \mathcal{A}_i \setminus \bigcup\limits_{j=1}^{i-1} \mathcal{A}_j, & \text{ja} \quad i > 1. \end{cases}$$

Tā kā $\mathfrak{A}$ ir algebra, tad $\forall i$ $\mathcal{B}_i \in \mathfrak{A}$. Kopu saime $\{\mathcal{B}_i\}$ ir disjunkta, tāpēc (punkts (iv)) $\bigcup\limits_{i=1}^{\infty} \mathcal{B}_i \in \mathfrak{A}$. Līdz ar to $\bigcup\limits_{i=1}^{\infty} \mathcal{A}_i = \bigcup\limits_{i=1}^{\infty} \mathcal{B}_i \in \mathfrak{A}$. ■

2. Ārējais mērs

Teorēma 2.1. *Ja* $\mu : \mathfrak{A} \to [0; +\infty]$ *ir algebrā* $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ *definēts aditīvs attēlojums un* $\mu(\emptyset) = 0$*, tad kopā* $\mathfrak{P}(\Omega)$ *definētais attēlojums*

$$\mu^*(E) \rightleftharpoons \inf \left\{ \sum_{i \in \mathcal{I}} \mu(\mathcal{A}_i) \;\middle|\; |\mathcal{I}| \leq \aleph_0 \ \wedge \ \forall i \in \mathcal{I} \ (\ \mathcal{A}_i \in \mathfrak{A} \ ) \ \wedge \ E \subseteq \bigcup_{i \in \mathcal{I}} \mathcal{A}_i \right\}$$

ir σ*–pusaditīvs un* $\mu^*(\emptyset) = 0$.

□ (i) $\emptyset \in \mathfrak{P}(\Omega)$ un $\mu(\emptyset) = 0$. Tā kā $\emptyset$ pārklājums ir $\emptyset$, tad $\mu^*(\emptyset) = 0 = \mu(\emptyset)$.

(ii) Mums jāpierāda nevienādība

$$\mu^*(E) \leq \sum_i \mu^*(E_i)$$

katram sanumurējamam kopas E pārklājumam $\{E_i\}$. Ja nu gadījumā $\sum\limits_i \mu^*(E_i) = +\infty$, tad nevienādība izpildās automātiski. Šī iemesla dēļ turpmāk pieņemsim, ka $\sum\limits_i \mu^*(E_i) < +\infty$.

Tagad ņemam vērā $\mu^*(E_i)$ definīciju, proti,

$$\mu^*(E_i) = \inf\{ \sum_j \mu(\mathcal{A}_{ij}) \mid E_i \subseteq \bigcup_j \mathcal{A}_{ij}\},$$

kur $\{\mathcal{A}_{ij}\}$ ir sanumurējams kopas E_i pārklājums un $\forall i \forall j \ \mathcal{A}_{ij} \in \mathfrak{A}$.

Pieņemsim, ka $\varepsilon > 0$, tad saskaņā ar infīma definīciju eksistē tāds kopas E_i sanumurējams pārklājums $\{\mathcal{A}_{ij}\}$, ka

$$\sum_j \mu(\mathcal{A}_{ij}) < \mu^*(E_i) + \frac{\varepsilon}{2^i}.$$

Tā kā $E \subseteq \bigcup\limits_i \bigcup\limits_j \mathcal{A}_{ij}$, tad

$$\begin{aligned} \mu^*(E) &\leq \sum_i \sum_j \mu(\mathcal{A}_{ij}) < \sum_i (\mu^*(E_i) + \frac{\varepsilon}{2^i}) \\ &= \sum_i \mu^*(E_i) + \sum_i \frac{\varepsilon}{2^i} \leq \sum_i \mu^*(E_i) + \varepsilon. \end{aligned}$$

Tā rezultātā esam parādījuši, ka katram pozitīvam ε

$$\mu^*(E) \leq \sum_i \mu^*(E_i) + \varepsilon.$$

Tas nozīmē, ka

$$\mu^*(E) \leq \sum_i \mu^*(E_i). \quad \blacksquare$$

Tikko definēto attēlojumu μ^* sauc par *ārējo mēru*, kas asociēts ar μ.

Apgalvojums 2.2. *Ja μ ir σ–algebrā $\mathfrak{A}$ definēts mērs, $\forall i\, \mathcal{A}_i \in \mathfrak{A}$ un $\{\mathcal{A}_i\}$ ir sanumurējama kopu saime, tad*

$$\mu(\bigcup_i \mathcal{A}_i) \leq \sum_i \mu(\mathcal{A}_i).$$

□ Tā kā $\mathfrak{A}$ ir σ–algebra, tad $\bigcup\limits_i \mathcal{A}_i \in \mathfrak{A}$. Tas nozīmē, ka $\mu(\bigcup\limits_i \mathcal{A}_i)$ ir definēts.

(i) Vispirms pieņemsim, ka

$$\{\mathcal{A}_i\} = \{\mathcal{A}_i \,|\, i \in \overline{1,n}\},$$

proti, tā ir galīga kopu saime. Definējam jaunas kopas

$$\mathcal{B}_i \rightleftharpoons \begin{cases} \mathcal{A}_i, & \text{ja} \quad i = 1; \\ \mathcal{A}_i \setminus \bigcup\limits_{j=1}^{i-1} \mathcal{A}_j, & \text{ja} \quad i > 1. \end{cases}$$

Saskaņā ar $\mathcal{B}_i$ definīciju $\bigcup\limits_{i=1}^{n} \mathcal{B}_i = \bigcup\limits_{i=1}^{n} \mathcal{A}_i$. Tā kā $\mathfrak{A}$ ir algebra, tad $\forall i\ \mathcal{B}_i \in \mathfrak{A}$. Kopu saime $\{\mathcal{B}_i\}$ ir disjunkta, tāpēc

$$\mu(\bigcup_{i=1}^{n} \mathcal{B}_i) = \sum_{i=1}^{n} \mu(\mathcal{B}_i).$$

Ievērojam $\forall i\, \mathcal{B}_i \subseteq \mathcal{A}_i$, tādēļ $\mu(\mathcal{B}_i) \leq \mu(\mathcal{A}_i)$. Līdz ar to

$$\mu(\bigcup_{i=1}^{n} \mathcal{A}_i) = \mu(\bigcup_{i=1}^{n} \mathcal{B}_i) = \sum_{i=1}^{n} \mu(\mathcal{B}_i) \leq \sum_{i=1}^{n} \mu(\mathcal{A}_i).$$

(ii) Pieņemsim, ka

$$\{\mathcal{A}_i\} = \{\mathcal{A}_i \,|\, i \in \mathbb{Z}_+\},$$

proti, tā ir bezgalīga sanumurējama kopu saime. Definējam jaunas kopas

$$\mathcal{B}_i \rightleftharpoons \begin{cases} \mathcal{A}_i, & \text{ja} \quad i = 1; \\ \mathcal{A}_i \setminus \bigcup\limits_{j=1}^{i-1} \mathcal{A}_j, & \text{ja} \quad i > 1. \end{cases}$$

Saskaņā ar $\mathcal{B}_i$ definīciju $\bigcup\limits_{i=1}^{\infty} \mathcal{B}_i = \bigcup\limits_{i=1}^{\infty} \mathcal{A}_i$. Tā kā $\mathfrak{A}$ ir algebra, tad $\forall i\ \mathcal{B}_i \in \mathfrak{A}$. Kopu saime $\{\mathcal{B}_i\}$ ir disjunkta, tāpēc

$$\mu(\bigcup_{i=1}^{\infty} \mathcal{B}_i) = \sum_{i=1}^{\infty} \mu(\mathcal{B}_i).$$

Ievērojam $\forall i\, \mathcal{B}_i \subseteq \mathcal{A}_i$, tādēļ $\mu(\mathcal{B}_i) \leq \mu(\mathcal{A}_i)$. Līdz ar to

$$\mu(\bigcup_{i=1}^{\infty} \mathcal{A}_i) = \mu(\bigcup_{i=1}^{\infty} \mathcal{B}_i) = \sum_{i=1}^{\infty} \mu(\mathcal{B}_i) \leq \sum_{i=1}^{\infty} \mu(\mathcal{A}_i). \quad \blacksquare$$

Apgalvojums 2.3. *Ja $\mu : \mathfrak{A} \to [0; +\infty]$ ir σ–algebrā $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ definēts mērs un μ^* — ārējais mērs, kas asociēts ar μ, tad*

$$\forall \mathcal{A} \in \mathfrak{A}\ \mu(\mathcal{A}) = \mu^*(\mathcal{A}).$$

□ Pieņemsim, ka $\mathcal{A} \in \mathfrak{A}$. Saskaņā ar $\mu^*(\mathcal{A})$ definīciju

$$\mu^*(\mathcal{A}) = \inf\{ \sum_{i \in \mathcal{I}} \mu(\mathcal{A}_i) \mid \mathcal{A} \subseteq \bigcup_{i \in \mathcal{I}} \mathcal{A}_i \},$$

kur $\{\mathcal{A}_i\}$ ir sanumurējams kopas $\mathcal{A}$ pārklājums un $\forall i\, \mathcal{A}_i \in \mathfrak{A}$. Tā kā $\mathfrak{A}$ ir σ–algebra, tad $\bigcup\limits_i \mathcal{A}_i \in \mathfrak{A}$. Tā rezultātā

$$\mu(\mathcal{A}) \leq \mu(\bigcup_i \mathcal{A}_i) \overset{\text{A2.2}}{\leq} \sum_i \mu(\mathcal{A}_i).$$

Tas demonstrē, ka $\mu(\mathcal{A}) \leq \mu^*(\mathcal{A})$. Taču $\{\mathcal{A}\}$ arī ir kopas $\mathcal{A}$ pārklājums, tāpēc $\mu^*(\mathcal{A}) \leq \mu(\mathcal{A})$. Līdz ar to $\mu^*(\mathcal{A}) = \mu(\mathcal{A})$. ■

3. Varbūtību telpas konstrukcija

Varbūtību teorijā izved likumus, kas ļauj aprēķināt vienu gadījumlielumu varbūtības, ja zināmas kādu citu gadījumlielumu varbūtības. Matemātiskā statistika analīzē metodes, kā atrast sākotnējās gadījumlielumu varbūtības.

Karateodori teorēma mums ļauj konstruēt mēru, ja mūsu rīcībā ir σ–pusaditīvs attēlojums μ^* pie nosacījuma, ka $\mu^*(\emptyset) = 0$. Savukārt Teorēma 2.1 dod iespēju konstruēt tādu σ–pusaditīvu attēlojumu μ^*, ka $\mu^*(\emptyset) = 0$, ja tikai mūsu rīcībā ir kāda algebra $\mathfrak{A} \subseteq \mathfrak{P}(\Omega)$ ar tajā definētu aditīvu attēlojumu μ (pie nosacījuma, ka $\mu(\emptyset) = 0$).

Ja mēs analizējam kādu konkrētu valodu, tad varbūtību telpa iepriekš mums nav dota. Skaitļus $\mu(\mathcal{A})$ mēs varam definēt vācot datus, un tos apstrādājot. Taču konstruējot varbūtību telpu var izrādīties, ka

$$\exists \mathcal{A} \in \mathfrak{A}\ \mu(\mathcal{A}) \neq \mu^*(\mathcal{A}).$$

Nākošais piemērs demonstrē, ka principā šāda nepatīkama situācija ir iespējama. Vispirms tomēr mums ir nepieciešama viena konstrukcija, kas definē algebru.

Apgalvojums 3.1. *Ja* $\forall i \in \mathcal{I}\ \ \mathfrak{A}_i \subseteq \mathfrak{P}(\Omega)$ *ir algebra, tad* $\mathfrak{A} \rightleftharpoons \bigcap\limits_{i\in\mathcal{I}} \mathfrak{A}_i$ *ir algebra.*

□ (i) Tā kā $\forall i \in \mathcal{I}\ \ \Omega \in \mathfrak{A}_i$, tad $\Omega \in \bigcap\limits_{i\in\mathcal{I}} \mathfrak{A}_i = \mathfrak{A}$.

(ii) Pieņemsim, ka $\mathcal{A} \in \mathfrak{A}$ un $\mathcal{B} \in \mathfrak{A}$, tad $\forall i \in \mathcal{I}\ (\mathcal{A} \in \mathfrak{A}_i \wedge \mathcal{B} \in \mathfrak{A}_i)$. Tā kā $\forall i \in \mathcal{I}\ \ \mathfrak{A}_i$ ir algebra, tad $\mathcal{A} \cup \mathcal{B} \in \mathfrak{A}_i$ un $\mathcal{A} \cap \mathcal{B} \in \mathfrak{A}_i$. No šejienes $\mathcal{A} \cup \mathcal{B} \in \mathfrak{A}$ un $\mathcal{A} \cap \mathcal{B} \in \mathfrak{A}$.

(iii) Pieņemsim, ka $\mathcal{A} \in \mathfrak{A}$, tad $\forall i \in \mathcal{I}\ \ \mathcal{A} \in \mathfrak{A}_i$. Tā kā $\forall i \in \mathcal{I}\ \ \mathfrak{A}_i$ ir algebra, tad $\bar{\mathcal{A}} \in \mathfrak{A}_i$. No šejienes $\bar{\mathcal{A}} \in \mathfrak{A}$. ■

Pieņemsim, ka $\mathcal{E} \subseteq \mathfrak{P}(\Omega)$ un $\mathfrak{A}_i(\mathcal{E})$, $i \in \mathcal{I}$, ir visas tās algebras, kas satur kopu $\mathcal{E}$, proti, $\mathcal{E} \subseteq \mathfrak{A}_i(\mathcal{E})$.

Definīcija 3.2. *Kopu saimi* $\langle\mathcal{E}\rangle \rightleftharpoons \bigcap\limits_{i\in\mathcal{I}} \mathfrak{A}_i(\mathcal{E})$ *sauc par sistēmas* $\mathcal{E}$ *ģenerēto algebru.*

Tā kā $\mathfrak{P}(\Omega)$ pati ir algebra, kas satur $\mathcal{E}$, tad $\mathcal{I} \neq \emptyset$. Tagad atsaucoties uz Apgalvojumu 3.1 secināms: $\langle\mathcal{E}\rangle$ ir algebra.

Definīcija 3.3. *Kopu* $]a;b] \subseteq \mathbb{R}$*, kur* $a < b$*, sauc par bultu.*
Bultas $]a_1;a_2],]a_3;a_4], \ldots,]a_{n-1};a_n]$ *sauc par disjunktām, ja*

$$a_1 < a_2 < \ldots < a_n.$$

Lemma 3.4. *Divu bultu apvienojums ir bulta vai divu disjunktu bultu apvienojums.*

□ Pieņemsim, ka $B_1 =]a_1;b_1]$ un $B_2 =]a_2;b_2]$. Ja $B_1 \cap B_2 \neq \emptyset$, tad

$$B_1 \cup B_2 =]\min(a_1,a_2); \max(b_1,b_2)].$$

Pretējā gadījumā B_1 un B_2 ir disjunktas bultas. ■

Lemma 3.5. *Ja* $B = \bigcup_{i=1}^{n} B_i$ *ir disjunktu bultu* B_i *apvienojums un* A *ir bulta, tad* $A \cup B$ *ir galīgs disjunktu bultu apvienojums.*

Vienošanās. Ja $n = 1$, arī šai gadījumā mēs teiksim, ka B ir disjunktu bultu apvienojums.

□ Pieņemsim, ka $A =]a;b]$,

$$B_1 =]a_1;b_1], B_2 =]a_2;b_2], \ldots, B_n =]a_n;b_n]$$

un $\forall i \ a_i < a_{i+1}$. Ja $\forall i \in \overline{s,k} \ A \cap B_i \neq \emptyset$, bet pārejiem indeksiem $i \notin \overline{s,k} \ A \cap B_i = \emptyset$, tad

$$\begin{aligned} A \cup B &= A \cup (\bigcup_{i=1}^{n} B_i) \\ &= (\bigcup_{i=1}^{s-1} B_i) \cup]\min(a,a_s); \max(b_k,b)] \cup (\bigcup_{i=k+1}^{n} B_i). \end{aligned} \tag{3}$$

Ja $a \neq b_{s-1}$ un $b \neq a_{k+1}$, tad (3) ir lemmā minētais disjunkto bultu apvienojums. Ja $a = b_{s-1}$, bet $b \neq a_{k+1}$, tad

$$A \cup B = (\bigcup_{i=1}^{s-2} B_i) \cup]a_{s-1}; \max(b_k,b)] \cup (\bigcup_{i=k+1}^{n} B_i).$$

Ja Ja $a = b_{s-1}$ un $b = a_{k+1}$, tad

$$A \cup B = (\bigcup_{i=1}^{s-2} B_i) \cup]a_{s-1}; b_{k+1}] \cup (\bigcup_{i=k+2}^{n} B_i).$$

Ja Ja $a \neq b_{s-1}$, bet $b = a_{k+1}$, tad

$$A \cup B = (\bigcup_{i=1}^{s-1} B_i) \cup]\min(a, a_s); b_{k+1}] \cup (\bigcup_{i=k+2}^{n} B_i).$$

Ja $\forall i\ A \cap B_i = \emptyset$, tad

$$A \cup B = A \cup (\bigcup_{i=1}^{n} B_i). \qquad \blacksquare$$

Lemma 3.6. *Ja* $A = \bigcup\limits_{i=1}^{n} A_i$ *un* $B = \bigcup\limits_{i=1}^{m} B_i$ *ir disjunktu bultu apvienojumi, tad* $A \cup B$ *ir galīgs disjunktu bultu apvienojums.*

□ Pierādījums iduktīvs pēc n. Ja $n = 1$, tad tā ir Lemma 3.5.

Ja $A = \bigcup\limits_{i=1}^{n+1} A_i$, tad saskaņā ar indukcijas pieņēmumu

$$A \cup B = A_{n+1} \cup ((\bigcup_{i=1}^{n} A_i) \cup B) = A_{n+1} \cup (\bigcup_{j=1}^{k} C_j),$$

kur $C_1, C_2, \ldots, C_k$ ir disjunktas bultas. Tagad atsaucoties uz Lemmu 3.5 secināms:

$$A \cup B = A_{n+1} \cup (\bigcup_{j=1}^{k} C_j) = \bigcup_{j=1}^{\varkappa} D_j,$$

kur $D_1, D_2, \ldots, D_\varkappa$ ir disjunktas bultas. ■

Lemma 3.7. *Ja* $B = \bigcup\limits_{i=1}^{n} B_i$ *ir disjunktu bultu* B_i *apvienojums un* $\forall i\ B_i \subseteq]a; b]$*, tad* $]a; b] \setminus B$ *ir galīgs disjunktu bultu apvienojums.*

□ Pieņemsim, ka

$$B_1 =]a_1; b_1], B_2 =]a_2; b_2], \ldots, B_n =]a_n; b_n]$$

un $\forall i\ a_i < a_{i+1}$, tad

$$]a; b] \setminus B =]a; a_1] \cup]b_1; a_2] \cup \ldots \cup]b_{n-1}; a_n] \cup]b_n; b]. \qquad \blacksquare$$

Apgalvojums 3.8. *Ja* $\Omega =]0;1]$, $\mathcal{E} = \{\,]a;b] \mid 0 \le a < b \le 1\}$ *un*

$$\mathcal{G} = \{A | A \text{ ir saimes } \mathcal{E} \text{ disjunktu bultu galīgs apvienojums}\} \cup \{\emptyset\},$$

tad $\mathcal{G} = \langle\mathcal{E}\rangle$*, proti,* $\mathcal{G}$ *ir sistēmas* $\mathcal{E}$ *ģenerētā algebra.*

□ Pieņemsim, ka $\mathfrak{A}_i(\mathcal{E})$, $i \in \mathcal{I}$, ir visas tās algebras, kas satur kopu $\mathcal{E}$, proti, $\mathcal{E} \subseteq \mathfrak{A}_i(\mathcal{E})$. Vispirms parādīsim, ka $\mathcal{G}$ ir viens no saimes $\{\mathfrak{A}_i(\mathcal{E}) \mid i \in \mathcal{I}\}$ elementiem.

Saskaņā ar $\mathcal{G}$ definīciju $\mathcal{E} \subseteq \mathcal{G}$. Tagad pārliecināsimies, ka $\mathcal{G}$ ir algebra, proti, tā apmierina visus definīcijas 1.1 nosacījumus.

(i) Tā kā $\Omega =]0;1] \in \mathcal{E}$, tad $\Omega \in \mathcal{G}$.

(ii) Ja $A \in \mathcal{G}$, tad saskaņā ar Lemmu 3.7 $\bar{A} \in \mathcal{G}$.

(iii) Ja $A \in \mathcal{G}$ un $B \in \mathcal{G}$, tad saskaņā ar lemmu 3.6 $A \cup B \in \mathcal{G}$. Visbeidzot, $A \cap B = \overline{\bar{A} \cup \bar{B}}$, tāpēc $A \cap B \in \mathcal{G}$.

Līdz ar to $\mathcal{G}$ ir viens no saimes $\{\mathfrak{A}_i(\mathcal{E})\}$ elementiem. Tas nozīmē, ka $\langle\mathcal{E}\rangle = \bigcap\limits_{i\in\mathcal{I}} \mathfrak{A}_i(\mathcal{E}) \subseteq \mathcal{G}$.

Katra saime $\mathfrak{A}_i(\mathcal{E})$ satur saimi $\mathcal{E}$ kā apakšsaimi, proti, $\mathcal{E} \subseteq \mathfrak{A}_i(\mathcal{E})$. Tā kā $\mathfrak{A}_i(\mathcal{E})$ ir algebra, tad tā satur visus saimes $\mathcal{E}$ galīgos apvienojumus un tukšo kopu $\emptyset$. Tātad tā satur $\mathcal{G}$. Līdz ar to $\mathcal{G} \subseteq \bigcap\limits_{i\in\mathcal{I}} \mathfrak{A}_i(\mathcal{E}) = \langle\mathcal{E}\rangle$.

Esam konstatējuši, ka $\mathcal{G} \subseteq \langle\mathcal{E}\rangle$ un $\langle\mathcal{E}\rangle \subseteq \mathcal{G}$; tātad $\mathcal{G} = \langle\mathcal{E}\rangle$. ■

Piemērs 3.9. *Algebrā* $\mathcal{G}$ *(Apgalvojums 3.8) definējam attēlojumu*

$$\mu(A) \rightleftharpoons \begin{cases} 1, & \text{ja} \quad \exists\varepsilon > 0\ ]\frac{1}{2}; \frac{1}{2} + \varepsilon] \subseteq A; \\ 0, & \text{pretējā gadījumā.} \end{cases}$$

Parādīsim, ka attēlojums $\mu : \mathcal{G} \to]0;1]$ ir aditīvs. Pieņemsim, ka A un B ir algebras $\mathcal{G}$ disjunktas kopas.

(i) Ja $\mu(A) = 1$, tad $\exists\varepsilon > 0\ ]\frac{1}{2}; \frac{1}{2} + \varepsilon] \subseteq A$. Tā kā A un B ir disjunktas kopas, tad $\forall\varepsilon > 0\ ]\frac{1}{2}; \frac{1}{2} + \varepsilon] \not\subseteq B$. Līdz ar to $\mu(B) = 0$. Tā rezultātā

$$\mu(A \cup B) = 1 = 1 + 0 = \mu(A) + \mu(B).$$

(ii) Ja $\mu(B) = 1$, tad, līdzīgi spriežot kā punktā (i), iegūstam: $\mu(A) = 0$, tāpēc $\mu(A \cup B) = 1 = 0 + 1 = \mu(A) + \mu(B)$.

(iii) Pieņemsim, ka $\mu(A) = \mu(B) = 0$. Ņemam vērā, ka $A \in \mathcal{G}$, tāpēc tā ir disjunktu bultu galīgs apvienojums. Tātad eksistē tādas bultas

$$]a_1; a_2],]a_3; a_4], \ldots,]a_{2n-1}; a_{2n}], \tag{4}$$

ka $0 \leq a_1 < a_2 < \ldots < a_{2n} \leq 1$ un

$$A =]a_1; a_2] \cup]a_3; a_4] \cup \ldots \cup]a_{2n-1}; a_{2n}]. \tag{5}$$

Tagad izanalizēsim trīs dažādus gadījumus.

- Ja $a_1 > \frac{1}{2}$, tad $]\frac{1}{2}; \frac{1}{2} + \varepsilon'] \cap A = \emptyset$, kur $\varepsilon' = a_1 - \frac{1}{2}$.
- Ja $a_{2n} \leq \frac{1}{2}$, tad $]\frac{1}{2}; \frac{1}{2} + \varepsilon'] \cap A = \emptyset$, kur $\varepsilon' = \frac{1}{2}$.
- Ja $a_{s-1} \leq \frac{1}{2} < a_s$, tad $s \neq 2k$, jo $\mu(A) = 0$ (skatīt (4) un (5)). Tātad $]\frac{1}{2}; \frac{1}{2} + \varepsilon'] \cap A = \emptyset$, kur $\varepsilon' = a_s - \frac{1}{2}$.

Līdzīgi secināms, ka eksistē tāds $\varepsilon'' > 0$, ka $]\frac{1}{2}; \frac{1}{2} + \varepsilon''] \cap B = \emptyset$. Līdz ar to $]\frac{1}{2}; \frac{1}{2} + \varepsilon] \cap (A \cup B) = \emptyset$, kur $\varepsilon = \min(\varepsilon', \varepsilon'')$. Tātad

$$\mu(A \cup B) = 0 = 0 + 0 = \mu(A) + \mu(B).$$

Katram $n > 1$ izvēlamies kopu $A_n \rightleftharpoons]\frac{1}{2} + \frac{1}{n+1}; \frac{1}{2} + \frac{1}{n}]$. Iegūstam

$$\bigcup_{n=2}^{\infty} A_n = \left]\frac{1}{2}; 1\right].$$

Tagad pievēršamies Teorēmas 2.1 konstrukcijai

$$\mu^*(\,]\frac{1}{2}; 1]) \rightleftharpoons \inf\left\{ \sum_{i \in \mathcal{I}} \mu(\mathcal{B}_i) \;\middle|\; |\mathcal{I}| \leq \aleph_0 \;\wedge\; \forall i \in \mathcal{I}\ (\ \mathcal{B}_i \in \mathcal{G}\ ) \wedge]\frac{1}{2}; 1] \subseteq \bigcup_{i \in \mathcal{I}} \mathcal{B}_i \right\}$$

$$= \sum_{n=2}^{\infty} \mu(A_n) = 0 \neq 1 = \mu((\,]\frac{1}{2}; 1])).$$

Tātad, ja mēs vēlamies, lai izpildītos vienādība

$$\forall \mathcal{A} \in \mathfrak{A}\ \mu(\mathcal{A}) = \mu^*(\mathcal{A}),$$

mums par to jārūpējas īpaši.

4. Cilindru algebra

Pieņemsim, ka A ir galīga kopa, ko turpmāk sauksim par *alfabētu*, bet kopas A elementus par — *burtiem*. Katru kopas $A^+ \rightleftharpoons \bigcup_{n=1}^{\infty} A^n$ elementu $u \in A^+$ sauc par alfabēta A *netukšu vārdu*. Pieņemsim, ka $u = (u_1, u_2, \ldots, u_k)$, $v = (v_1, v_2, \ldots, v_m)$ ir alfabēta A netukši vārdi, tad

$$u\#v \rightleftharpoons (u_1, u_1, \ldots, u_k, v_1, v_2, \ldots, v_m).$$

Šo kopā A^+ definēto operāciju sauc par *konkatenāciju*. Tā kā

$$(u\#v)\#w = u\#(v\#w)$$

visiem alfabēta A netukšiem vārdiem u, v, w, tad $\langle A^+, \# \rangle$ ir pusgrupa. Šo pusgrupu sauc par *kopas A veidoto brīvo pusgrupu A^+*.

Pieņemsim, ka $\lambda \notin A^+$ un $A^* \rightleftharpoons A^+ \cup \{\lambda\}$, tad kopu A^* var sekojoši pārvērst par monoīdu:

$$\lambda\#\lambda \rightleftharpoons \lambda, \quad \lambda\#u \rightleftharpoons u \rightleftharpoons u\#\lambda\,.$$

Šo monoīdu sauc par *kopas A veidoto brīvo monoīdu A^**. Kopas A^* elementus sauc par *vārdiem*, λ — par *tukšo vārdu*. Kā tas tradicionāli pieņemts, ja nerodas pārpratumi, tad konkatenācijas operāciju izlaiž un lieto pierakstu $uv \rightleftharpoons u\#v$, bez tam $u_1u_2 \ldots u_k \rightleftharpoons (u_1, u_2, \ldots, u_k)$. Ja $u = u_1 = u_2 = \ldots = u_n$, tad lieto arī pierakstu $u^n \rightleftharpoons u_1u_2 \ldots u_n$. Savukārt $u^0 \rightleftharpoons \lambda$.

Pieņemsim, ka $u \in A^n$, tad skaitli n sauc par vārda u garumu, ko turpmāk apzīmēsim ar $|u|$. Saskaņā ar definīciju pieņemsim, ka $|\lambda| \rightleftharpoons 0$.

Definīcija 4.1. *Visur definētu attēlojumu $x : \mathbb{N} \to A$ sauc par alfabēta A ω-vārdu.*

Mēs lietosim šādus apzīmējumus:

$$x_i \rightleftharpoons x[i] \rightleftharpoons x(i), \qquad x \rightleftharpoons (x_i) \rightleftharpoons x_0x_1 \ldots x_n \ldots$$

Alfabēta A visu ω-vārdu veidoto kopu turpmāk apzīmēsim ar A^ω.

Definīcija 4.2. *Alfabēta A ω-vārdu $ux \rightleftharpoons u_1u_2 \ldots u_kx_0x_1 \ldots x_n \ldots$ sauc par vārdu $u = u_1u_2 \ldots u_k \in A^*$ un $x \in A^\omega$ konkatenāciju. Vārdu $w \in A^*$ sauc par vārda $x \in A^\omega$ dalītāju, ja eksistē tādi $v \in A^*$ un $y \in A^\omega$, ka $x = vwy$. Šai situācijā vārdu v sauc par priedēkli, bet y — par piedēkli.*

Vārda $x \in A^\omega$ visu priedēkļu kopu apzīmēsim ar $\mathrm{Pref}(x)$.

Pieņemsim, ka $u \in A^*$, tad

$$u\rangle \rightleftharpoons \{x \in A^\omega \,|\, u \in \mathrm{Pref}(x)\}.$$

Definīcija 4.3. *Katru kopu* $\bigcup\limits_{u\in\mathcal{U}} u\rangle$, *kur* $\mathcal{U} \subseteq A^n$, *sauc par* n*–tā ranga cilindru.*

Saskaņā ar definīciju mēs pieņemam, ka $\bigcup\limits_{u\in\emptyset} u\rangle \rightleftharpoons \emptyset$. Ar $\mathcal{C}_n$ apzīmēsim visu n–tā ranga cilindru veidoto saimi, proti,

$$\mathcal{C}_n \rightleftharpoons \{\mathcal{A} \,|\, \mathcal{A} \text{ ir } n\text{–tā ranga cilindrs}\}.$$

Cilindru $\lambda\rangle = A^\omega$ mēs nosauksim par 0–tā ranga cilindru. Tas ir vienīgais 0–tā ranga cilindrs. Kopu $\mathcal{C} \rightleftharpoons \bigcup_{n=0}^{\infty} \mathcal{C}_n$ sauc par *cilindru algebru*.

Mūs interesē kopu saime

$$A^*\rangle \rightleftharpoons \{u\rangle \,|\, u \in A^*\}.$$

Apgalvojums 4.4. $\mathcal{C} = \langle A^*\rangle\rangle$

□ Pieņemsim, ka $\mathfrak{A}_i$, $i \in \mathcal{I}$, ir visas tās algebras, kas satur kopu $A^*\rangle$, proti, $A^*\rangle \subseteq \mathfrak{A}_i$. Vispirms parādīsim, ka $\mathcal{C}$ ir viens no saimes $\{\mathfrak{A}_i \,|\, i \in \mathcal{I}\}$ elementiem.

Saskaņā ar $\mathcal{C}$ definīciju $\mathcal{A}^*\rangle \subseteq \mathcal{C}$. Tagad pārliecināsimies, ka $\mathcal{C}$ ir algebra, proti, tā apmierina visus definīcijas 1.1 nosacījumus.

(i) Mūsu gadījumā $\Omega = A^\omega = \lambda\rangle \in \mathcal{C}$.

(ii) Pieņemsim, ka $\mathcal{A} \in \mathcal{C}$, tad eksistē tāda kopa $\mathcal{U} \subseteq A^n$, ka $\mathcal{A} = \bigcup\limits_{u\in\mathcal{U}} u\rangle$. No šejienes

$$\bar{\mathcal{A}} = \bigcup_{u\in A^n\setminus\mathcal{U}} u\rangle,$$

jo

$$A^\omega = \bigcup_{u\in A^n} u\rangle.$$

(iii) Pieņemsim, ka $\mathcal{A} \in \mathcal{C}$ un $\mathcal{B} \in \mathcal{C}$, tad

$$\mathcal{A} = \bigcup_{u\in\mathcal{U}_1} u\rangle \quad \text{un} \quad \mathcal{B} = \bigcup_{u\in\mathcal{U}_2} u\rangle,$$

kur $\mathcal{U}_1 \subseteq A^n$, bet $\mathcal{U}_2 \subseteq A^m$. Konkrētības labad pieņemsim, ka $n \leq m$.

Saskaņā ar $u\rangle$ definīciju

$$u\rangle = \bigcup_{a\in A} ua\rangle.$$

Tas induktīvi ļauj secināt: eksistē tāda kopa $\mathcal{U} \subseteq A^m$, ka

$$\mathcal{A} = \bigcup_{u\in\mathcal{U}} u\rangle.$$

No šejienes

$$\mathcal{A} \cup \mathcal{B} = \bigcup_{u\in\mathcal{U}\cup\mathcal{U}_2} u\rangle \in \mathcal{C}.$$

Visbeidzot, $\mathcal{A}\cap\mathcal{B} = \overline{\bar{\mathcal{A}} \cup \bar{\mathcal{B}}}$, tāpēc $\mathcal{A}\cap\mathcal{B} \in \mathcal{C}$. Līdz ar to $\mathcal{C}$ ir viens no saimes $\{\mathfrak{A}_i\}$ elementiem. Tas nozīmē, ka $\langle A^*\rangle\rangle = \bigcap_{i\in\mathcal{I}} \mathfrak{A}_i \subseteq \mathcal{C}$.

Katra saime $\mathfrak{A}_i$ satur saimi $A^*\rangle$ kā apakšsaimi, proti, $A^*\rangle \subseteq \mathfrak{A}_i$. Tā kā $\mathfrak{A}_i$ ir algebra, tad tā satur visus saimes $A^*\rangle$ galīgos apvienojumus un tukšo kopu $\emptyset$. Tātad tā satur $\mathcal{C}$. Līdz ar to $\mathcal{C} \subseteq \bigcap_{i\in\mathcal{I}} \mathfrak{A}_i = \langle A^*\rangle\rangle$.

Esam konstatējuši, ka $\mathcal{C} \subseteq \langle A^*\rangle\rangle$ un $\langle A^*\rangle\rangle \subseteq \mathcal{C}$; tātad $\mathcal{C} = \langle A^*\rangle\rangle$. ■

Piemērs 4.5. *Pieņemsim, ka* $A = \{0, 1\}$,

$\mathcal{A} = 001\rangle \cup 100\rangle \cup 101\rangle$, $\mathcal{B} = 01\rangle \cup 10\rangle$, tad

$$\bar{\mathcal{A}} = 000\rangle \cup 010\rangle \cup 011\rangle \cup 110\rangle \cup 111\rangle, \quad \bar{\mathcal{B}} = 00\rangle \cup 11\rangle.$$

Ievērojam: $\mathcal{B} = 01\rangle \cup 10\rangle = 010\rangle \cup 011\rangle \cup 100\rangle \cup 101\rangle$, tāpēc

$$\begin{aligned} \mathcal{A} \cup \mathcal{B} &= 001\rangle \cup 100\rangle \cup 101\rangle \cup 010\rangle \cup 011\rangle \cup 100\rangle \cup 101\rangle \\ &= 001\rangle \cup 010\rangle \cup 011\rangle \cup 100\rangle \cup 101\rangle. \end{aligned}$$

Kopā $A^*\rangle$ induktīvi definēsim attēlojumu $\mathcal{P}$.

(i) $\mathcal{P}(\lambda\rangle) \rightharpoonup 1$.

(ii) Pieņemsim, ka $A = \{a_1, a_2, \ldots, a_n\}$. Izvēlamies n nenegatīvus skaitļus $p_1, p_2, \ldots, p_n$ tā, lai $\sum_{i=1}^n p_i = 1$, tad $\mathcal{P}(a_i) \rightharpoonup p_i$.

(iii) Induktīvais solis. Pieņemsim, ka $\mathcal{P}(u\rangle)$ ir definēts visiem $u \in A^k$. Izvēlamies n nenegatīvus skaitļus $p_{u1}, p_{u2}, \ldots, p_{un}$ tā, lai $\sum_{i=1}^n p_{ui} = \mathcal{P}(u\rangle)$, tad $\mathcal{P}(ua_i) \rightharpoonup p_{ui}$.

Attēlojumu $\mathcal{P}$ turpināsim kopā $\langle A^*\rangle\rangle$.
(i) $\mathcal{P}(\emptyset) \rightleftharpoons 0$.
(ii) Pieņemsim, ka $A^\omega \neq \mathcal{A} \in \langle A^*\rangle\rangle$, tad (Apbalvojums 4.4)

$$\mathcal{A} = \bigcup_{u\in\mathcal{U}} u\rangle, \qquad \text{kur} \qquad \exists m \in \mathbb{Z}_+ \ \mathcal{U} \subseteq A^m.$$

$$\mathcal{P}(\mathcal{A}) \rightleftharpoons \sum_{u\in\mathcal{U}} \mathcal{P}(u\rangle).$$

Sekas 4.6. $\forall m \in \mathbb{N}\ \forall u \in A^* \ \mathcal{P}(u\rangle) = \sum\limits_{v\in A^m} \mathcal{P}(uv\rangle)$.

□ Saskaņā ar $\mathcal{P}$ definīciju

$$\mathcal{P}(u\rangle) = \sum_{i=1}^{n} p_{ui} = \sum_{i=1}^{n} \mathcal{P}(ua_i\rangle) = \sum_{a\in A} \mathcal{P}(ua\rangle).$$

Tālākie spriedumi induktīvi. Pieņemsim, ka $\mathcal{P}(u\rangle) = \sum\limits_{v\in A^m} \mathcal{P}(uv\rangle)$. Tai pašā laikā esam jau pierādījuši, ka $\mathcal{P}(uv\rangle) = \sum\limits_{a\in A} \mathcal{P}(uva\rangle)$. No šejienes

$$\mathcal{P}(u\rangle) = \sum_{v\in A^m} \mathcal{P}(uv\rangle) = \sum_{v\in A^m}\sum_{a\in A} \mathcal{P}(uva) = \sum_{w\in A^{m+1}} \mathcal{P}(uw\rangle). \quad \blacksquare$$

Sekas 4.7. *Attēlojums $\mathcal{P} : \mathcal{C} \to [0;1]$ ir aditīvs.*

□ Pieņemsim, ka $\mathcal{A} \in \mathcal{C}$, $\mathcal{B} \in \mathcal{C}$ un $\mathcal{A} \cap \mathcal{B} = \emptyset$. Ja gadījumā kāda no kopām $\mathcal{A}$ vai $\mathcal{B}$ ir $\emptyset$ vai A^ω, tad fakta $\mathcal{P}(\mathcal{A}\cup\mathcal{B}) = \mathcal{P}(\mathcal{A}) + \mathcal{P}(\mathcal{B})$ pierādījums ir triviāls. Šī iemesla dēļ turpmāk pieņemsim, ka nedz $\mathcal{A}$, nedz $\mathcal{B}$ nav neviena no kopām $\emptyset$ vai A^ω.

Tā rezultātā, ņemot vērā Apgalvojuma 4.4 pierādījuma punktā (iii) izklāstīto,

$$\exists m \in \mathbb{Z}_+ \ \exists \mathcal{U}_1 \subseteq A^m \ \exists \mathcal{U}_2 \subseteq A^m \ [\ \mathcal{A} = \sum_{u\in\mathcal{U}_1} u\rangle \ \wedge \ \mathcal{B} = \sum_{u\in\mathcal{U}_2} u\rangle\ ].$$

Tagad atsaucoties uz Sekām 4.6 secināms:

$$\mathcal{P}(\mathcal{A}) = \sum_{u\in\mathcal{U}_1} \mathcal{P}(u\rangle) \qquad \text{un} \qquad \mathcal{P}(\mathcal{B}) = \sum_{u\in\mathcal{U}_2} \mathcal{P}(u\rangle).$$

Tā kā $\mathcal{A} \cap \mathcal{B} = \emptyset$, tad $\mathcal{U}_1 \cap \mathcal{U}_2 = \emptyset$. No šejienes

$$\begin{aligned} \mathcal{P}(\mathcal{A} \cup \mathcal{B}) &= \sum_{u \in \mathcal{U}_1 \cup \mathcal{U}_2} \mathcal{P}(u\rangle) = \sum_{u \in \mathcal{U}_1} \mathcal{P}(u\rangle) + \sum_{u \in \mathcal{U}_2} \mathcal{P}(u\rangle) \\ &= \mathcal{P}(\mathcal{A}) + \mathcal{P}(\mathcal{B}). \qquad \blacksquare \end{aligned}$$

Definīcija 4.8. *Kopu saimi* $\{\mathcal{A}_i \,|\, i \in \mathcal{J}\}$ *sauc par kopas* $\mathcal{A}$ *pārklājuma* $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ *apakšpārklājumu, ja*

$$\mathcal{A} \subseteq \bigcup_{i \in \mathcal{J}} \mathcal{A}_i \qquad \text{un} \qquad \mathcal{J} \subseteq \mathcal{I}.$$

Kā redzams, apakšpārklājuma jēdziens ir piekārtots kādam fiksētam pārklājumam. Ja no konteksta būs noprotams pārklājums $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$, tad mēs to īpaši neizcelsim.

Apakšpārklājumu $\{\mathcal{A}_i \,|\, i \in \mathcal{J}\}$ sauc par *galīgu*, ja $\mathcal{A} \subseteq \bigcup_{i \in \mathcal{J}} \mathcal{A}_i$ un $\mathcal{J}$ ir galīga kopa. Te mēs klusuciešot pieņemam, ka $\mathcal{A} \subseteq \bigcup_{i \in \mathcal{J}} \mathcal{A}_i$ ir tieši pārklājuma $\mathcal{A} \subseteq \bigcup_{i \in \mathcal{I}} \mathcal{A}_i$ apakšpārklājums.

Mēs teiksim, ka kopai $\mathcal{A}$ neeksistē galīgs apakšpārklājums, ja

$$\forall \mathcal{J} \subseteq \mathcal{I}\ (\mathcal{A} \subseteq \bigcup_{i \in \mathcal{J}} \mathcal{A}_i \Rightarrow |\mathcal{J}| \geq \aleph_0).$$

Apgalvojums 4.9. *Katram kopas* $u\rangle$ *pārklājumam* $\{\, u_i\rangle\}$ *eksistē galīgs apakšpārklājums.*

□ Apgalvojumu pierādīsim no pretējā, proti, pieņemsim, ka neeksistē kopas $u\rangle$ galīgs apakšpārklājums. Ievērojam

$$u\rangle = \bigcup_{a \in A} ua\rangle.$$

Mūsu gadījumā alfabēts A ir galīgs, tāpēc vismaz vienam burtam, teiksim, $b_1 \in A$ neeksistē galīgs kopas $ub_1\rangle$ apakšpārklājums.

Tālākie spriedumi induktīvi, proti, pieņemsim, ka neeksistē kopas

$$ub_1b_2 \ldots b_k\rangle$$

galīgs apakšpārklājums. Ievērojam

$$ub_1b_2 \ldots b_k\rangle = \bigcup_{a \in A} ub_1b_2 \ldots b_ka\rangle.$$

Mūsu gadījumā alfabēts A ir galīgs, tāpēc vismaz vienam burtam, teiksim, $b_{k+1} \in A$ neeksistē galīgs kopas $ub_1 \dots b_k b_{k+1}\rangle$ apakšpārklājums.

Līdz ar to induktīvi definēts

$$x \rightharpoonup ub_1 \dots b_k b_{k+1} \dots \in A^\omega$$

ar īpašību: katram vārda x priedēklim $v \in \mathrm{Pref}(x)$ neeksistē galīgs kopas $v\rangle$ apakšpārklājums. Taču $x \in u\rangle$, tāpēc eksistē tāda kopa

$$u_j\rangle \in \{\, u_i\rangle\}, \qquad \text{ka} \qquad x \in u_j\rangle.$$

No šejienes $u_j \in \mathrm{Pref}(x)$, un tādēļ neeksistē galīgs kopas $u_j\rangle$ apakšpārklājums. Pretruna, jo $u_j\rangle \subseteq u_j\rangle$, proti, šai kopai eksistē galīgs apakšpārklājums. Tas sastāv no vienas pašas kopas $u_j\rangle \in \{\, u_i\rangle\}$. ■

Sekas 4.10. *Katram kopas $\mathcal{A} \in \mathcal{C}$ pārklājumam $\{\, u_i\rangle\}$ eksistē galīgs apakšpārklājums.*

□ Sekas pierādīsim no pretējā, proti, pieņemsim, ka neeksistē kopas $\mathcal{A} \in \mathcal{C}$ galīgs apakšpārklājums. Tā kā $\mathcal{A} \in \mathcal{C}$, tad

$$\mathcal{A} = \bigcup_{u \in \mathcal{U}} u\rangle, \qquad \text{kur} \qquad \exists m \in \mathbb{Z}_+ \;\; \mathcal{U} \subseteq A^m.$$

Mūsu gadījumā kopa $\mathcal{U}$ ir galīga, tāpēc vismaz vienai no kopām $u\rangle$ neeksistē galīgs apakšpārklājums, kas ir pretrunā ar Apgalvojumu 4.9. ■

Sekas 4.11. *Katram kopas $\mathcal{A}$ pārklājumam $\{\mathcal{A}_i \in \mathcal{C} \mid i \in \mathcal{I}\}$ eksistē galīgs apakšpārklājums.*

□ Tā kā $\mathcal{A}_i \in \mathcal{C}$, tad

$$\mathcal{A}_i = \bigcup_{u \in \mathcal{U}_i} u\rangle, \qquad \text{kur} \qquad \exists m_i \in \mathbb{Z}_+ \;\; \mathcal{U} \subseteq A^{m_i}.$$

Līdz ar to

$$\mathcal{A} \subseteq \bigcup_{i \in \mathcal{I}} \bigcup_{u \in \mathcal{U}_i} u\rangle.$$

Tātad saime $\{u\rangle \mid \exists i \in \mathcal{I} \;\; u \in \mathcal{U}_i\}$ ir kopas $\mathcal{A}$ pārklājums. Tas ļauj secināt (Sekas 4.10), ka eksistē kopas $\mathcal{A}$ pārklājuma $\{u\rangle \mid \exists i \in \mathcal{I} \;\; u \in \mathcal{U}_i\}$ galīgs apašpārklājums $\{u_i\rangle \mid i \in \mathcal{J}\}$.

Katram $i \in \mathcal{J}$ izvēlamies pa vienai kopai $\mathcal{A}_{k_i}$ tā, lai $u_i\rangle \subseteq \mathcal{A}_{k_i}$. Tā rezultātā $\mathcal{A} \subseteq \bigcup\limits_{i\in\mathcal{J}} \mathcal{A}_{k_i}$, t.i., $\{\mathcal{A}_{k_i} \,|\, i \in \mathcal{J}\}$ ir kopas $\mathcal{A}$ pārklājuma $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ galīgs apakšpārklājums. ■

Mūsu rīcībā ir algebra $\mathcal{C}$ un tajā definēts aditīvs attēlojums $\mathcal{P}$. Saskaņā ar Teorēmu 2.1 eksistē tāds σ–pusaditīvs attēlojums

$$\mathcal{P}^* : \mathfrak{P}(A^\omega) \to [0; +\infty], \qquad \text{ka} \qquad \mathcal{P}^*(\emptyset) = 0.$$

Apgalvojums 4.12. $\quad \forall \mathcal{A} \in \mathcal{C} \quad \mathcal{P}^*(\mathcal{A}) = \mathcal{P}(A).$

□ Pieņemsim, ka $\mathcal{A} \in \mathcal{C}$. Saskaņā ar $\mathcal{P}^*$ definīciju

$$\mathcal{P}^*(\mathcal{A}) = \inf\left\{ \sum_{i\in\mathcal{I}} \mathcal{P}(\mathcal{A}_i) \;\middle|\; |\mathcal{I}| \le \aleph_0 \;\wedge\; \forall i \in \mathcal{I}\ (\ \mathcal{A}_i \in \mathcal{C}\ ) \;\wedge\; \mathcal{A} \subseteq \bigcup_{i\in\mathcal{I}} \mathcal{A}_i \right\}.$$

Pieņemsim, ka $\{\mathcal{A}_i \in \mathcal{C} \,|\, i \in \mathcal{I}\}$ ir kopas $\mathcal{A}$ pārklājums. Ņemot vērā tikko pierādītās sekas, secināms: eksistē šī pārklājuma galīgs apakšpārklājums

$$\{\mathcal{A}_i \,|\, i \in \mathcal{J}\}.$$

Tā kā $\mathcal{P}$ ir nenegatīvs attēlojums un tas ir saimes $\mathcal{C}$ aditīvs attēlojums, tad

$$\sum_{i\in\mathcal{I}} \mathcal{P}(\mathcal{A}_i) \ge \sum_{i\in\mathcal{J}} \mathcal{P}(\mathcal{A}_i) \ge \sum_{i\in\mathcal{J}} \mathcal{P}(\mathcal{A} \cap \mathcal{A}_i).$$

Kopa $\mathcal{J}$ ir galīga, tāpēc (skatīt Apgalvojuma 4.4 pierādījuma punktā (iii) izklāstīto) eksistē $k \in \mathbb{Z}_+$ un tādas kopas V, $V_i, i \in \mathcal{J}$, ka

- $\mathcal{A} = \bigcup\limits_{u\in V} u\rangle \;\wedge\; V \subseteq A^k$;
- $\mathcal{A}_i = \bigcup\limits_{u\in V_i} u\rangle \;\wedge\; V_i \subseteq A^k$.

No šejienes $\mathcal{A} \cap \mathcal{A}_i = \bigcup\limits_{u\in V\cap V_i} u\rangle$, un tādēļ, ņemot vērā $\mathcal{P}$ aditivitāti,

$$\sum_{i\in\mathcal{J}} \mathcal{P}(\mathcal{A} \cap \mathcal{A}_i) = \sum_{i\in\mathcal{J}} \sum_{u\in V\cap V_i} \mathcal{P}(u\rangle) = \sum_{u\in V} \mathcal{P}(u\rangle) = \mathcal{P}(\mathcal{A}).$$

Tātad $\mathcal{P}^*(\mathcal{A}) = \mathcal{P}(\mathcal{A})$. ■

Karateodori teorēma apgalvo, ka $\mathcal{P}^*$–mērojamo kopu saime $\mathfrak{C} \subseteq \mathfrak{P}(A^\omega)$ ir σ–algebra un $\mathcal{P}^*$ sašaurinājums kopā $\mathfrak{C}$ ir mērs.

Apgalvojums 4.13. $\mathcal{C} \subseteq \mathfrak{C}$

□ Pieņemsim, ka $E \subseteq A^\omega$, tad

$$\mathcal{P}^*(E) = \inf \left\{ \sum_{i\in\mathcal{I}} \mathcal{P}(\mathcal{A}_i) \;\middle|\; |\mathcal{I}| \leq \aleph_0 \;\wedge\; \forall i \in \mathcal{I}\ (\ \mathcal{A}_i \in \mathcal{C}\ ) \;\wedge\; \mathcal{A} \subseteq \bigcup_{i\in\mathcal{I}} \mathcal{A}_i \right\}.$$

Saskaņā ar infīma definīciju $\forall \varepsilon > 0$ atrodams tāds sanumurējams pārklājums $\{\mathcal{A}_i\}$, ka

$$\mathcal{P}^*(E) + \varepsilon > \sum_i \mathcal{P}(\mathcal{A}_i).$$

Ņemam vērā, ka

$$\begin{aligned} E \cap \mathcal{A} &\subseteq (\bigcup_i \mathcal{A}_i) \cap \mathcal{A} = \bigcup_i (\mathcal{A}_i \cap \mathcal{A}), \\ E \cap \bar{\mathcal{A}} &\subseteq (\bigcup_i \mathcal{A}_i) \cap \bar{\mathcal{A}} = \bigcup_i (\mathcal{A}_i \cap \bar{\mathcal{A}}. \end{aligned}$$

Pieņemsim, ka $\mathcal{A} \in \mathcal{C}$. Tā kā $\mathcal{P}^*$ ir monotons un σ–pusaditīvs, tad

$$\mathcal{P}^*(E \cap \mathcal{A}) \leq \mathcal{P}^*(\bigcup_i (\mathcal{A}_i \cap \mathcal{A})) \leq \sum_i \mathcal{P}^*(\mathcal{A}_i \cap \mathcal{A}) = \sum_i \mathcal{P}(\mathcal{A}_i \cap \mathcal{A}).$$

Līdzīgi

$$\mathcal{P}^*(E \cap \bar{\mathcal{A}}) \leq \mathcal{P}^*(\bigcup_i (\mathcal{A}_i \cap \bar{\mathcal{A}})) \leq \sum_i \mathcal{P}^*(\mathcal{A}_i \cap \bar{\mathcal{A}}) = \sum_i \mathcal{P}(\mathcal{A}_i \cap \bar{\mathcal{A}}).$$

No šejienes

$$\begin{aligned} \mathcal{P}^*(E \cap \mathcal{A}) + \mathcal{P}^*(E \cap \bar{\mathcal{A}}) &\leq \sum_i \mathcal{P}(\mathcal{A}_i \cap \mathcal{A}) + \sum_i \mathcal{P}(\mathcal{A}_i \cap \bar{\mathcal{A}}) \\ &= \sum_i (\mathcal{P}(\mathcal{A}_i \cap \mathcal{A}) + \mathcal{P}(\mathcal{A}_i \cap \bar{\mathcal{A}})) \\ &= \sum_i (\mathcal{P}((\mathcal{A}_i \cap \mathcal{A}) \cup (\mathcal{A}_i \cap \bar{\mathcal{A}})) \\ &= \sum_i \mathcal{P}(\mathcal{A}_i) < \mathcal{P}^*(E) + \varepsilon. \end{aligned}$$

Tātad $\mathcal{P}^*(E \cap \mathcal{A}) + \mathcal{P}^*(E \cap \bar{\mathcal{A}}) \leq \mathcal{P}^*(E)$. Tagad atsaucoties uz Karateodori teorēmas pierādījuma sākumā minēto varam apgalvot, ka

$$\mathcal{P}^*(E \cap \mathcal{A}) + \mathcal{P}^*(E \cap \bar{\mathcal{A}}) = \mathcal{P}^*(E).$$

Līdz ar to kopa $\mathcal{A}$ pareizi sadala katru kopu $E \subseteq A^\omega$. Tas nozīmē, ka $\mathcal{A}$ ir $\mathcal{P}^*$– mērojama, t.i., $\mathcal{A} \in \mathfrak{C}$. ■

Pēdējie divi apgalvojumi demonstrē, ka $\mathcal{P}^*$ ir aditīvā attēlojuma $\mathcal{P}$ σ–aditīvs paplašinājums visu $\mathcal{P}^*$–mērojamo kopu σ–algebrā $\mathfrak{C}$. Tā rezultātā mūsu rīcībā ir varbūtību telpa $\langle A^\omega, \mathfrak{C}, \mathcal{P}^* \rangle$.

Tagad identificējam katru $u \in A^*$ ar kopu $u\rangle$. Esam ieguvuši varbūtību telpu, kas apraksta pamattekstu avotu.

Literatūra

[1] P. Billingsley. *Probability and Measure*. JOHN WILEY & SONS, New York, 1995. 593 p.

[2] I. Kārkliņš *Ievads integrāļa teorijā*. Latvijas Universitāte, Rīga, 1990. 105 lpp.

[3] В. М. Фомичев. Под общей редакцией доктора физико-математических наук Н. Д. Подуфалова. *Дискретная математика и криптология. Курс лекций.* Москва «ДИАЛОГ-МИФИ», 2003. 400 с.