Kombinatorické štruktúry

Martin Škoviera

5. júna 2003

Obsah

Kapitola 1

Usporiadané množiny

1.1 Základné pojmy

Čiastočne usporiadaná množina (skrátene čum, angl. poset) $(P, \leq)$ je množina s binárnou reláciou $\leq$ taká, že $\forall x, y, z \in P$:

1. $x \leq x$ reflexívnosť
2. $x \leq y \ \& \ y \leq z \implies x \leq z$ tranzitívnosť
3. $x \leq y \ \& \ y \leq x \implies x = y$ antisymetria

Príklad

1. $(\mathbb{N}, \leq)$ obyčajné lineárne usporiadanie
2. $(\mathcal{P}(X), \subseteq)$
3. $(\mathbb{N}, |)$ napríklad $3 \mid 6$ ale $3 \nmid 7$.
4. $\{0,1\}^n$ n-rozmerná kocka so zvyčajným usporiadaním.
5. Množina X a $\mathcal{D}(X)$ množina všetkých jej rozkladov. $\sigma, \tau \in \mathcal{D}(X)$: $\sigma \leq \tau$, ak σ je zjemnením τ.
6. $\mathrm{Eq}(X)$ množina všetkých ekvivalencií na X s $\subseteq$. $\mathrm{Eq}(X) \subseteq \mathcal{P}(X \times X)$ a usporiadanie je zdedené.

Nasleduje zopár ľahkých pojmov, ktoré sa do definície čumu nevošli.

- Ak $(P, \leq)$ je čum a $Q \subseteq P$, tak na Q máme *zdedené usporiadanie* $\leq_Q$.
- Ak $a \leq b$ alebo $b \leq a$, tak prvky a, b voláme *porovnateľné*, inak *neporovnateľné*.
- Ostrú nerovnosť definujeme ako $a < b \iff a \leq b \ \& \ a \neq b$.

- Maximálne, minimálne, najväčšie, najmenšie prvky definujeme ako zvyčajne. Najmenší prvok značíme 0 a najväčší 1 (ak existujú). Všetky minimálne (resp. maximálne) prvky sú neporovnateľné. Najmenší (resp. najväčší) je porovnateľný so všetkými prvkami.
- Ak $a \leq b$, tak $[a, b] = \{x \in P \mid a \leq x \leq b\}$ voláme *interval* čumu.
- Ak $A \subseteq P$ a v A sú každé dva prvky porovnateľné, tak A je *reťazec*. A je *antireťazec*, ak žiadne dva prvky nie sú porovnateľné.
- Hovoríme, že b *pokrýva* a, značíme $a \lessdot b$, ak $a < x \leq b \implies x = b$, t.j. ak $[a, b] = \{a, b\}$. Prvky pokrývajúce 0 voláme *atómy* a prvky pokryté 1 *koatómy*.
- *Dualita* čumov: Ak P je čum, tak P^* označuje tú istú množinu s duálnou reláciou $\leq^* = \geq$. Samozrejme $P^{**} = P$. Duálne pojmy:

$\leq$	$\geq$
min	max
najmenší	najväčší
0	1
atóm	koatóm

- *Dĺžka reťazca* $C = \#$ prvkov - 1 $= \#$ znakov nerovnosti $\lessdot$
- *Výška prvku* $h(a) =$ dĺžka najdlhšieho reťazca ukončeného prvkom a.
- *Nezjemniteľný reťazec* je taký, že medzi žiadne dva prvky nemožno vložiť tretí. Ekvivalentne povedané, každý prvok (okrem posledného) je pokrytý nasledujúcim.
- Existujú relácie podobajúce sa na usporiadanie, ale ním nie sú. Napríklad Q množina delení intervalu $\langle 0, 1\rangle$ ako v určitom intergráli. Pre $D_1, D_2, \in Q$ položíme $D_1 \trianglelefteq D_2 \iff ||D_1|| \leq ||D_2||$, kde $|| \cdot ||$ je norma delenia. Táto relácia je reflexívna a tranzitívna, ale nie je antisymetrická. Táketo čosi sa volá *kváziusporiadanie*. Ak $(P, \trianglelefteq)$ je kváziusporiadanie a zavedieme na ňom ekvivalenciu $x \sim y \iff x \trianglelefteq y \ \&\ y \trianglelefteq x$, tak dostávame čum na $P/\sim$.

Hovoríme, že $(P, \leq)$ spĺňa *podmienku klesajúcich reťazcov* (DCC), ak neexistuje nekonečná ostro klesajúca postupnosť $a_1 > a_2 > \dots$ (Ekvivalentne povedané, ak každá neostro klesajúca postupnosť $a_1 \geq a_2 \geq \dots$ sa *stabilizuje*, t.j. ak existuje n také, že $a_n = a_{n+1} = \dots$) Duálne definujeme *podmienku rastúcich reťazcov* (ACC).

Tvrdenie 1 *Nech P je čum. Nasledujúce podmienky sú ekvivalentné:*

1. *Každá neprázdna $Q \subseteq P$ má minimálny (maximálny) prvok.*
2. *P spĺňa DCC (ACC).*

1.2 Zväzy

Nech $(P, \leq)$ je čum. Ak $a, b \in P$, tak ich horným ohraničením je každý prvok taký, že $c \geq a$ a $c \geq b$. Najmenšie horné ohraničenie, ak existuje, sa nazýva *spojením* prvkov a, b, označuje sa $a \vee b$, alebo tiež *suprémom* $\sup(a, b)$. Teda $a \vee b$ je taký prvok d, že:

1. $d \geq a$, $d \geq b$
2. ak nejaký prvok k spĺňa 1., tak $k \geq d$.

Duálne definujeme *priesek* $a \wedge b$ ako najväčšie dolné ohraničenie prvkov a, b; tiež ho nazývame *infimum* a označujeme $\inf(a, b)$. Analogicky definujeme tieto pojmy pre ľubovoľnú podmnožinu $Q \subseteq P$, značíme $\inf M = \bigwedge M$ a $\sup M = \bigvee M$; nemusia však vo všeobecnosti existovať.

Príklad

1. $(\mathcal{P}(X), \subseteq)$, $\wedge = \cap$, $\vee = \cup$ a každá podmnožina $\mathcal{P}(X)$ má suprémum aj infimum.
2. $(\mathbb{N}, |)$, usporiadanie deliteľnosťou $\wedge = \text{nsd}$, $\vee = \text{nsn}$
3. $\{0, 1\}^n$, $\wedge = \min$, $\vee = \max$

Ak $(P, \leq)$ je usporiadaná množina, v ktorej pre každú dvojicu $a, b \in P$ existuje $a \vee b$, tak P nazývame $\vee$-*polozväz* (horný, spojovací polozväz). Analogicky definujeme $\wedge$-*polozväz* (dolný, priesekový polozväz) (angl. semilattice).

Teoréma 2 *Nech $(P, \leq)$ je $\vee$-polozväz. Potom platia identity:*

1. $a \vee a = a$ *(idempotencia)*
2. $a \vee b = b \vee a$ *(komutatívnosť)*
3. $(a \vee b) \vee c = a \vee (b \vee c)$ *(asociatívnosť)*
4. $a \leq b \iff a \vee b = b$

Obrátene, nech $(M, \circ)$ je grupoid s vlastnosťami 1–3. Ak položíme $a \preceq b \iff a \circ b = b$, tak $(M, \preceq)$ je usporiadaná množina, ktorá je vzhľadom na $\preceq$ horným polozväzom s operáciou spojenia $\sup(a, b) = a \circ b$. (Analogická veta platí pre $\wedge$-polozväzy.)

Dôkaz. V prvej časti teorémy sa 1 až 4 overí priamo. Nech $(M, \circ)$ je grupoid s vlastnosťami 1–3 a položme $a \preceq b \iff_{\text{def}} a \circ b = b$. Potom:

1. Idempotencia zaručuje reflexívnosť.
2. Nech $a \preceq b$ a $b \preceq a$. Potom $a \circ b = b$ a $b \circ a = b$. Z komutatívnosti máme $a = b \circ a = a \circ b = b$.

3. Nech $a \preceq b$ a $b \preceq c$, chceme dokázať $a \preceq c$. Vieme $a \circ b = b$, $b \circ c = c$, preto $a \circ c = a \circ (b \circ c) = (a \circ b) \circ c = b \circ c = c$. Teda $a \preceq c$.

4. Treba ešte ukázať, že vzhľadom na $\preceq$ je $\sup(a, b) = a \circ b$. Predovšetkým, $a \circ b$ je horným ohraničením pre a aj b, lebo:

$$\begin{array}{lllllllll} a \circ (a \circ b) & = & (a \circ a) \circ b & = & a \circ b & & & \Longrightarrow & a \preceq a \circ b \\ b \circ (a \circ b) & = & (a \circ b) \circ b & = & a \circ (b \circ b) & = & a \circ b & \Longrightarrow & b \preceq a \circ b \end{array}$$

   Ešte treba ukázať, že $a \circ b$ je najmenšie horné ohraničenie. Nech d je horným ohraničením a aj b, čiže $a \preceq d$, $b \preceq d$. Ukážeme, že $a \circ b \preceq d$. Naozaj, máme $a \circ d = d$, takže $(a \circ b) \circ d = a \circ (b \circ d) = a \circ d = d$. Teda $a \circ b \preceq d$.

□

Dokázali sme, že existuje 1–1 korešpondecia medzi hornými polozväzmi a komutatívnymi pologrupami, v ktorých každý prvok je idempotentný.

Zväz (angl. lattice) je usporiadaná množina $(P, \leq)$, v ktorej každá dvojica prvkov má aj priesek $\wedge$ aj spojenie $\vee$. Ak v zväze naviac každá podmnožina $A \subseteq P$ má $\bigwedge A$ aj $\bigvee A$, tak sa nazýva *úplný* zväz. Pritom definujeme, ako sa to tradične robí, $\bigwedge \emptyset = \bigvee P = 1$ (najväčší prvok) a $\bigwedge P = \bigvee \emptyset = 0$ (najmenší prvok).

Teoréma 3 *Nech $(P, \leq)$ je zväz. Potom platia identity:*

$$\begin{array}{lllllll} 1. & a \vee a & = & a & a \wedge a & = & a \\ 2. & a \vee b & = & b \vee a & a \wedge b & = & b \wedge a \\ 3. & (a \vee b) \vee c & = & a \vee (b \vee c) & (a \wedge b) \wedge c & = & a \wedge (b \wedge c) \\ 4. & (a \vee b) \wedge b & = & b & (a \wedge b) \vee b & = & b \wedge (b \wedge c) \\ 5. & a \leq b & \Longleftrightarrow & a \vee b = b & \Longleftrightarrow & a \wedge b = a. & \end{array}$$

Obrátene, nech $(P; \vee, \wedge)$ je algebra splňajúca identity 1–4. Potom definovaním $a \leq b \iff a \vee b = b$ vzniká usporiadaná množina, ktorá je zväzom, pričom $sup(a, b) = a \vee b$ a $\inf(a, b) = a \wedge b$.

Dôkaz. Ľavú časť 1–3 a 5 sme ukázali v Teoréme 2, pravá vyplýva z duality. 4: $a \vee b \geq b$, preto $(a \vee b) \wedge b = b$; pravá časť je duálna. Obrátene, ak máme 1–4, tak dôkazom Teóremy 2 dostávame usporiadanie, ktoré je horným polozväzom. Ukázali sme totiž, že $a \vee b = \sup(a, b)$. Ostáva dokázať, že $a \wedge b = \inf(a, b)$. To urobíme takto. Najprv ukážeme, že $a \vee b = b \iff a \wedge b = a$. „$\Longrightarrow$“: Nech $a \vee b = b$. Potom $a \wedge b = a \wedge (a \vee b) = (a \vee b) \wedge a = (b \vee a) \wedge a = a$. „$\Longleftarrow$“: Duálne. Teda nerovnosť definovaná pomocou $\wedge$ je tá istá ako nerovnosť definovaná pomocou $\vee$ (ktorú sme prijali za základnú). Preto z toho, že $a \vee b = \sup(a, b)$ a z princípu duality vyplýva, že $a \wedge b = \inf(a, b)$. □

Príklady zväzov

1. $(\mathcal{P}(X), \subseteq)$, úplný zväz

2. $(\mathbb{N}, |) = \mathcal{T}$, s operáciou deliteľnosti je úplný zväz
3. Zväz podgrúp, zväz normálnych podgrúp, zväz podpriestorov vektorového priestoru (pre priestory nad konečnými poľami má kombinatorický význam).
4. Zväz rozkladov danej množiny, zväz ekvivalencií na danej množine (v akom sú vzťahu). Má veľký význam pre kombinatoriku.
5. Príklad neuplného zväzu: Zväz otvorených množín na $\mathbb{R}$. (Otvorená množina je disjuktným zjednotením otvorených intervalov, aj nekonečného počtu.) Prienik nekonečného počtu otvorených množín nemusí byť otvorená.

Na každý zväz sa môžeme dívať z dvojakého hľadiska: ako na množinu s reláciou $\leq$, ale aj ako na množinu s dvoma binárnymi operáciami. Táto dvojznačnosť má svoje dôsledky pre porovnávanie zväzov pomocou morfizmov.

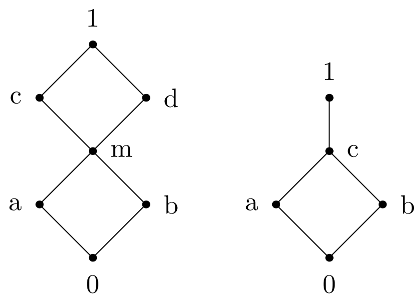
Morfizmus usporiadaných množín $(P, \leq)$ a $(Q, \leq)$ je *izotónne zobrazenie* $f : P \to Q$, teda také, že $a \leq b$ v P implikuje $f(a) \leq f(b)$. Ak zobrazenie prevracia nerovnosti ($a \leq b \implies f(a) \geq f(b)$), tak sa nazýva *antimónne.* Ak f je izotónna bijekcia, ešte nemusí byť izomorfizmus! *Izomorfizmus* je morfizmus taký, že aj f^{-1} je morfizmus. No $f : (\mathbb{N}, |) \to (\mathbb{N}, \leq)$, $x \mapsto x$ je izotónna bijekcia, lebo $a \mid b \implies a \leq b$, no f^{-1} nie je izotónne; teda f nie je izomorfizmus. Vo všeobecnosti, bijektívny morfizmus relačných štruktúr (takou je aj usporiadaná množina) nemusí byť izomorfizmom.

No zväz (polozväz) je aj algebraický systém – špeciálny prípad univerzálnej algebry – s dvoma binárnymi operáciami $\wedge$ a $\vee$. Homomorfizmus zväzov $(P; \wedge, \vee)$ a $(Q; \wedge, \vee)$ je zobrazenie $f : P \to Q$ také, že $f(x \wedge y) = f(x) \wedge f(y)$ a $f(x \vee y) = f(x) \vee f(y)$, t.j. f zachováva operácie. Na to, aby f bolo izomorfizmom zväzov, stačí povedať, aby zachovávalo operácie a bolo bijektívne. Naozaj, nech f je bijektívny homorfizmus. Potom $f(x \wedge x) = f(x) \wedge f(y)$ a f^{-1} existuje. Ukážeme, že aj f^{-1} zachováva operáciu $\wedge$. Položme $f(x) = a$ a $f(y) = b$, čiže $f^{-1}(a) = x$ a $f^{-1}(b) = y$. (Pre ľubovoľné a, b, také x, y existujú.) Potom z rovnosti:

$$\begin{aligned} f(x \wedge y) &= f(x) \wedge f(y) \quad \text{dostávame} \\ f^{-1}(f(x \wedge y)) &= f^{-1}(f(x) \wedge f(y)), \\ x \wedge y &= f^{-1}(a \wedge b), \\ f^{-1}(a) \wedge f^{-1}(b) &= f^{-1}(a \wedge b). \end{aligned}$$

Záver *Ak $(P; \wedge, \vee, \leq)$ a $(Q; \wedge, \vee, \leq)$ sú zväzy a $f : P \to Q$, tak nasledujúce výroky sú ekivalentné:*

1. *f je izomorfizmus.*
2. *f je izotónna bijekcia taká, že aj f^{-1} je izotónne zobrazenie.*
3. *f je bijektívny homorfizmus vzhľadom na operácie $\wedge$ a $\vee$.*



Obr. 1.1: Zväzy P a Q

Nech $(P; \wedge, \vee)$ je zväz a nech $Q \subseteq P$. Potom Q nazývame *podzväzom* zväzu P, ak Q je zväz a pre ľubovoľné dva prvky $a, b \in Q$ platí $\inf_Q(a,b) = \inf_P(a,b)$ a $\sup_Q(a,b) = \sup_P(a,b)$; teda výsledky operácií v zväze aj podzväze musia byť tie isté.

Može sa stať, že $Q \subseteq P$ s indukovaným usporiadaním dáva zväz, nie však podzväz zväzu P. Napríklad:

Tvrdenie 4 *V každom zväze $(P; \wedge, \vee)$ ľubovoľná jednoprvková množina a prázdna množina tvoria podzväz. Ak $a, b \in P$, tak interval $[a,b]$ je tiež podzväz. Prienik podzväzov je podzväz.* $\Box$

Nech $(P, \leq_P)$ a $(Q, \leq_Q)$ sú usporiadané množiny. Definujeme *priamy súčin* ako usporiadanú mnyožinu $(P \times Q, \leq_{PQ})$, kde $(a,b) \leq_{PQ} (c,d)$ práve vtedy, keď $a \leq_P c$ a $b \leq_Q d$.

Tvrdenie 5 *Ak $(P, \leq_P)$ a $(Q, \leq_Q)$ sú zväzy, tak aj $(P \times Q, \leq_{PQ})$ je zväz.* $\Box$

Dôsledok *Priamy súčin reťazcov je zväz.*

Dôkaz. Každý reťazec je triviálne zväz. $\Box$

Pri štúdiu kombinatorických štruktúr si často všímame zobrazenia $f, g : N \to R$, pričom porovnávame zobrazenia pomocou obrazov, ignorujúc podstatu prvkov množiny N (za ktoré berieme napr. $N = \{0, 1, \ldots, n\}$ ak študujeme napr. variácie k-tej triedy). Na takéto zobrazenia je niekedy výhodné sa dívať ako na *multimnožiny*, kde každý prvok množiny R sa môže opakovať potrebný počet krát (toľkokrát, koľkokrát je obrazom). Takto vzniká *zväz multimnožín* $\mathcal{M}(R)$ nad R. Pre dve multimnožiny $k = (b^{k_b}; b \in R)$ a $l = (b^{l_b}; b \in R)$ (k_b, l_b sú násobnosti prvku b v k resp. v l) položíme

$$
\begin{aligned}
k \wedge l &= (b^{\min(k_b, l_b)};\ b \in R), \\
k \vee l &= (b^{\max(k_b, l_b)};\ b \in R).
\end{aligned}
$$

Je to úplný zväz.

Platí:

1. Ak $|R| = n$ a $\mathbb{N}_0$ je množina nezáporných celých čísel lineárne usporiadaných podľa veľkosti, tak $\mathcal{M}(R) \cong \underbrace{\mathbb{N}_0 \times \mathbb{N}_0 \times \cdots \times \mathbb{N}_0}_{r}$

   Dôkaz. Zobrazenie $\varphi : \mathcal{M}(R) \to (\mathbb{N}_0)^r$, $k = (b^{k_b};\ b \in R) \mapsto (\ldots, k_b, \ldots)$ je hľadaný izomorfizmus. $\Box$

2. Ak R je nekonečná spočítateľná množina, tak $\mathcal{M}(R) \cong (\mathbb{N}, |) = \mathcal{T}$, kde vpravo je zväz prirodzených čísel usporiadaných deliteľnosťou.

   Dôkaz. Nech $R = \{r_1, r_2, \ldots\}$. Potom každú multimnožinu vieme zapísať v tvare $k = r_1^{k_1} r_2^{k_2} \ldots$ Nech $p_1, p_2, \ldots$ je postupnosť prvočísel v rastúcom poradí. Potom dostávame izomorfizmus $\varphi : k = r_1^{k_1} r_2^{k_2} \ldots \mapsto p_1^{k_1} p_2^{k_2} \ldots$ $\Box$

3. Nech $\mathcal{C}(n)$ je reťazec dĺžky n (a teda mohutnosti $n+1$), t.j. $\mathcal{C}(n) = \{0 < 1 < 2 < \cdots < n\}$. Skúmajme interval $[1, 360]$ zväzu deliteľnosti $\mathcal{T}$. Keďže $360 = 2^3 \cdot 3^2 \cdot 5$, ľahko sa nahliadne, že $[1, 360] \cong \mathcal{C}(3) \times \mathcal{C}(2) \times \mathcal{C}(1)$.

4. Zväz rozkladov $\mathcal{D}(n)$. Nech $\mathcal{D}(n)$ je napríklad množina všetkých rozkladov n-prvkovej množiny $\{1, 2, \ldots, n\}$. Nech $\pi \in \mathcal{D}(n)$ a nech (π) označuje reláciu ekvivalencia odpovedajúcu π. Potom priesek a spojenie sa ľahko opíše. Potom pre ľubovoľné dva prvky a, b

$$\begin{aligned} a(\pi \wedge \sigma)b &\iff a(\pi)b \text{ a } a(\sigma)b \\ a(\pi \vee \sigma)b &\iff \exists \text{ postupnosť } a = u_1, u_2, \ldots, u_t = b \text{ taká, že} \\ & \text{pre každé } i\ \exists \tau \in \{\pi, \sigma\} : u_i(\tau)u_{i+1} \end{aligned}$$

   Napr. pre $n = 11$:

$$\begin{aligned} \pi &= \{\{1,2\},\{3,4,5\},\{6,7,8\},\{9,10,11\}\}, \\ \sigma &= \{\{1,3,4\},\{2,5\},\{6,7,11\},\{8\},\{9,10\}\}. \end{aligned}$$

   Potom

$$\begin{aligned} \pi \wedge \sigma &= \{\{1\},\{2\},\{3,4\},\{5\},\{6,7\},\{8\},\{9,10\},\{11\}\}, \\ \pi \vee \sigma &= \{\{1,2,3,4,5\},\{6,7,8,9,10,11\}\}. \end{aligned}$$

   Tieto zväzy sú v kombinatorike aj v teórii zväzov veľmi dôležité. Dlhé roky bol otvorený problém štruktúry podzväzov zväzu $\mathcal{D}(n)$. Whitman (1946) vyslovil hypotézu, že každý zväz možno vložiť ako podzväz nejakého zväzu $\mathcal{D}(n)$. Túto hypotézu dokázali P. Pudlák a J. Tůma (1977). S týmto zväzom sa čoskoro stretneme.

Obr. 1.2: $\mathcal{D}(3)$

Obr. 1.3: Youngov zväz

5. Usporiadaným analógom multimnožiny je *multireťazec*. Ak $f : N \to R$ je zobrazenie, kde N je reťazec, povedzme $N = \{1, 2, \dots, m, \dots\}$, R je usporiadaná množina a f je izotónne, tak $f(N)$ je reťazec v R, presnejšie *multireťazec*, ak zoberieme do úvahy aj usporiadanie v R. Budú nás zaujímať konečné multireťazce $a = a_1a_2 \dots a_k$, pričom sa dohodneme, že členy budeme zapisovať v nerastúcom poriadku, teda $a_1 \geq a_2 \geq \cdots \geq a_k$. Kvôli porovnávaniu multireťazcovje vhodné zaviesť nový prvok do množiny $\widehat{R} = R \cup \{0\}$, s tým, že $0 < b$ pre každé $b \in R$. Multireťazec $a_1a_2 \dots a_k$ potom môžeme reprezentovať nekonečným vektorom $(a_1, a_2, \dots, a_{k+1}, \dots)$, kde $a_{k+1} = a_{k+2} = \cdots = 0$.

   Máme nasledujúce tvrdenie:

   Tvrdenie 6 *Množina všetkých konečných multireťazcov čiastočne usporiadanej množiny R je usporiadaná reláciou usporiadania po súradniciach ($a \leq b \iff a_i \leq b_i,\ i \in \mathbb{N}$). Ak je R zväz (špeciálne, ak je R reťazec), tak táto usporiadaná množina tvorí zväz, ktorý je podzväzom súčinu $\prod_{i=1}^{\infty} R_i$, kde $R_i = \widehat{R}$ pre každé i.*

   Dôkaz. Stačí overiť, že priesek a spojenie monotónne klesajúcich slov je tiež také slovo. □

   Osobitne sú zaujímavé špeciálne prípady tvrdenia 6. Nech $R = \mathbb{N}$ a teda $\widehat{R} = \mathbb{N}_0$. Potom vzniknutý zväz sa nazýva *Youngovým* zväzom a označuje sa $\mathcal{Y}$. Jeho prvky sú nerastúce reťazce prirodzených čísel, kde od istého miesta sú samé nuly.

   Je tu ešte jedna dôležitá interpretácia. Nech $n = n_1 + n_2 + \cdots + n_k$ je partícia čísla n na k neusporiadaných kladných čísel, *k-partícia*. Kedže sú neusporiadané, môžeme prepokladať, že $n_1 \geq n_2 \geq \cdots \geq n_k$. Potom

   $$(n_1, n_2, \dots, n_k, 0, \dots) \leftrightarrow n_1 + n_2 + \cdots + n_k$$

   definuje izomorfizmus Youngovho zväzu so zväzom všetkých neusporiadaných partícií. Nulou tohto zväzu je prázdne slovo 0.

6. Partície čísla n. Uvažujem zväz $\mathcal{D}(n)$ rozkladov n-prvkovej množiny $\{1, 2, \dots, n\}$. Potom každému rozkladu $\pi = A_1 \uplus A_2 \uplus \cdots \uplus A_k$ prislúcha partícia $z(\pi)$ čísla n: $z(\pi) = n_1 + n_2 + \cdots + n_k$, kde $n_i = |A_i|$ pre $i = 1, 2, \dots, k$. Relácia usporiadania na $\mathcal{D}(n)$ daná zjemnením rozkladu indukuje usporiadanie na

Obr. 1.4: Diagram zväzu $\mathcal{N}(7)$ partícií čísla 7

množine $\mathcal{N}(n)$ neusporiadaných partícií čísla n:

$$\sum n_i \leq \sum m_j \iff \text{existujú } \pi, \sigma \in \mathcal{D}(n)$$
$$\text{také, že } \pi \leq \sigma \text{ a} z(\pi) = \sum n_i \text{ a } z(\sigma) = \sum m_j.$$

Dá sa nahliadnuť, že toto naozaj definuje reláciu usporiadania na $\mathcal{N}(n)$ a toto usporiadanie je ekvivalentné s nasledujúcim:

$$\sum_{i=1}^{k} n_i \lessdot \sum_{j=1}^{l} m_j \iff l = k-1 \text{ a všetky } m_j \text{ sú totožné s } n_i$$
$$\text{okrem jednej dvojice } \textbf{ďalej nečitateľné}.$$

Zobrazenie $z : \mathcal{D}(n) \to \mathcal{N}(n)$ je morfizmus usporiadaných množín. Je aj morfizmus zväzov? (Nie, v príklade č. 4 vyššie $z(\pi) \gtrdot z(\sigma)$, takže $z(\pi) \wedge z(\sigma) = z(\sigma) > z(\pi \wedge \sigma)$.) Vo všeobecnosti platí:

Tvrdenie 7 *Nech $(P; \wedge, \vee)$ a $(Q; \wedge, \vee)$ sú zväzy. Potom každý homomorfizmus zväzov je aj morfizmus usporiadania. Obrátene to neplatí. Platí však, že každý izomorfizmus usporiadania je izomorfizmus.* $\square$

Príklad Zrejme φ je morfizmus usporiadania, ale $\varphi(a \vee b) = 1 \neq m =$

$a' \vee b' = \varphi(a) \vee \varphi(b)$. φ nie je ani $\vee$-homorfizmom ani $\wedge$-homorfizmom.

Na záver tejto časti dokážeme zaujímavé tvrdenie o úplných zväzoch.

Teoréma 8 (Knaster–Tarského o pevnom bode) *Nech $(P, \leq)$ je úplný zväz a $\varphi : P \to P$ je izotónne zobrazenie. Potom φ má pevný bod, t.j. existuje $x \in P$ také, že $\varphi(x) = x$.*

Dôkaz. Nech $M = \{x \in P; x \leq \varphi(x)\}$. Zrejme $M \neq \emptyset$, lebo $0 \leq \varphi(0)$. Nech $c = \sup M$. Keďže pre každé $x \in M$ platí $x \leq c$, z izotónnsoti vyplýva $x \leq \varphi(x) \leq \varphi(c)$. Odtiaľ $c = \sup M \leq \varphi(c)$. Teda

$$c \leq \varphi(c).$$

Aplikovanín φ dostávame $\varphi(c) \leq \varphi(\varphi(c))$, z čoho vyplýva, že $\varphi(c) \in M$. No potom $\varphi(c) \leq \sup M = c$, čiže

$$\varphi(c) \leq c.$$

Z týchto nerovností máme $\varphi(c) = c$. □

Príklad Cantor-Bernsteinova teoréma: Nech A, B sú množiny. Ak existujú injekcia $\varphi : A \to B$ a injekcia $\psi : B \to A$, tak exituje bijekcia $A \to B$. Idea dokôzu: Nech $X \subseteq A$. Skonštujme postupne

$$X \mapsto \varphi(X) \mapsto B - \varphi(X) \mapsto \psi(B - \varphi(X)) \mapsto A - \psi(B - \varphi(X)).$$

Uvažujme zobrazenie $\Psi : \mathcal{P}(A) \to \mathcal{P}(A)$,

$$X \mapsto A - \psi(B - \varphi(X)).$$

Ľahko sa overí (s použitím známych inklúzií), že Ψ je izotónne. Keďže $\mathcal{P}(A)$ je uplný zväz, Ψ má pevný bod – nejakú $C \subseteq A$. Pomocou tejto množiny sa už ľahko nadefinuje bijekcia.

1.3 Distributívne zväzy

Na úvod pripomenieme nasledovné tvrdenie.

Tvrdenie 9 *Nech $(P, \leq)$ je ľubovoľný zväz. Potom sú pravdivé tieto tvrdenia:*

1. *(izotónnosť $\vee$) $x \leq y \implies x \vee z \leq y \vee z$*
   (izotónnosť $\wedge$) $x \leq y \implies x \wedge z \leq y \wedge z$
2. *(všeobecná izotónnosť) $x \leq z \ \&\ z \leq t \implies x \wedge z \leq y \wedge t$, podobne pre $\vee$*
3. *(distributívne nerovnosti)*
   $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$
   $x \wedge (y \vee z) \geq (x \wedge y) \vee (x \wedge z)$
4. *(modulárna nerovnosť) $x \leq z \implies x \vee (y \wedge z) \leq (x \vee y) \wedge z$*

Dôkaz.

1. Izotónnosť $\wedge$: Ak $x \leq y$ a $z \in P$, tak $x \wedge z \leq x \leq y$ a zároveň $x \wedge z \leq z$. Teda $x \wedge z$ je dolným ohraničením pre $\{y, z\}$. Odtiaľ $x \wedge z \leq y \wedge z$. Izotónnosť $\vee$ sa dokáže podobne.
2. Všeobecná izotónnosť sa dokáže dvojnásobným použitím 1.
3. Distributívnosť $\vee$: Zrejme $y \wedge z$, takže z izotónnosti pre $\vee$ dostávame $x \vee (y \wedge z) \leq x \vee z$. Analogicky $y \wedge z \leq z$, takže $x \vee (y \wedge z) \leq x \vee z$. Teda $x \vee (y \wedge z)$ je spoločným dolným ohraničením pre $\{x \vee y, x \vee z\}$, odkiaľ $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z)$. Distributívnosť $\wedge$ podobne.
4. Modulárna nerovnosť: Z distributívnej nerovnosti a predpokladu $x \leq z$ máme $x \vee (y \wedge z) \leq (x \vee y) \wedge (x \vee z) = (x \vee z) \wedge z$.

$\square$

Zväz sa nazýva *distributívny*, ak v ňom namiesto distributívnych nerovností platí rovnosť, teda ak pre každé x, y, z:

$$\begin{aligned} x \vee (y \wedge z) &= (x \vee y) \wedge (x \vee z), \\ x \wedge (y \vee z) &= (x \wedge y) \vee (x \wedge z). \end{aligned}$$

Zväz sa nazýva *modulárny* (Dedekindov), ak v ňom namiesto modulárnej nerovnosti platí rovnosť, t.j. ak pre $x \leq z$ platí $x \vee (y \wedge z) = (x \vee y) \wedge z$. Modulárnymi zväzmi sa budeme zaoberať neskôr, teraz len distributívnymi.

Každá z distributívnych nerovností implikuje druhú. (Ak platí prvá, počítajme z pravej strany druhú: $\underbrace{(x \wedge y)}_{} t \vee (x \wedge z) = t \vee (x \wedge z)$, použijeme druhú rovnosť, využijeme bežné identity a máme.)

Naviac platia aj (konečné !) zovšeobecnené rovnosti

$$\begin{aligned} \left(\bigwedge_i x_i\right) \vee \left(\bigwedge_j y_j\right) &= \bigwedge_{i,j} (x_i \vee y_j), \\ \left(\bigvee_i x_i\right) \wedge \left(\bigvee_j y_j\right) &= \bigvee_{i,j} (x_i \wedge y_j). \end{aligned}$$

Keďže definujúce rovnosti sú navzájom duálne, tak duál distributívneho zväzu je distributívny.

Príklady

1. Zväzy rádu ≤ 4 sú všetky distrinutívne. Medzi 5-prvkovými (je ich 5) sú dva nedistributívne, jeden dokonca nemodulárny:

2. $\{0, 1\}^n = \mathcal{P}(X)$ je distributívny.

3. Každý reťazec je distributívny zväz.

4. Súčin distributívnych zväzov je distributívny (aj nekonečný súčin funguje).

5. Podzväz distributívneho zväzu je distributívny zväz. Vyplýva to z toho, že operácie $\wedge, \vee$ sú totožné s operácia v celom zväze.

6. Z ??? vyplýva, že Youngov zväz všetkých partícií (ako podzväz súčinu $\prod^{\infty} \mathbb{N}_0$) a zväz $(\mathbb{N}, \mathrm{nsd}, \mathrm{nsn}) = \mathcal{T}$ (ako podzväz $\prod^{\infty} \mathbb{N}_0$) sú distributívne.

7. Zväz ??? grupy S_3 permutácií 2-prvkovej množiny nie je distributívny.

Prvok p (?distributívneho) zväzu L sa nazýva *ireducibilný* (presnejšie $\vee$-*ireducibilný*), ak pre ľubovoľné $x, y \in L$ zo vzťahu $p = x \vee y$ vyplýva $p = x$ alebo $p = y$. Výraz $a = p_1 \vee p_2 \vee \ldots \vee p_k$, v ktorom všetky p_i sú ireducibilné sa nazýva *rozkladom* prvku a na ireducibilné prvky. Rozklad je *neskrátiteľný* (*iredundantný*), ak $a \neq p_1 \vee p_2 \vee \ldots p_{i-1} \vee p_{i+1} \vee \ldots \vee p_k$, pre každé i. (Atómy a 0 sú zjavne ireducibilné prvky.)

Je zrejmé, že v ľubovoľnom rozklade sú všetetky prvky neporovnateľné, teda tvoria antireťazec. Našim cieľom je ukázať, že štruktúra zväzu je jednoznačne určená množinou jeho ireducibilných prvkov.

Lema *Nech p je ireducibilný prvok distribitívneho zväzu. Potom z nerovnosti $p \leq a_1 \vee \ldots \vee a_k$ vyplýva, že existuje i také, že $p \leq a_i$.*

Dôkaz. Nech $p \leq \bigvee_i a_i$. Potom $p = p \wedge (\bigvee_i a_i) = \bigvee_i p \wedge a_i$. Z ireducibility prvku p teraz vyplýva, že existuje i také, že $p = p \wedge a_i$, čiže $p \leq a_i$. $\square$

Prijmime teraz všeobecný a trvalý predpoklad o tom, že sa budeme zaoberať len usporiadanými množinami spĺňajúcimi podmienku:

(F) *Medzi ľubovoľnými dvoma prvkami je každý reťazec konečný.*

(Všetky množiny kombinatorického pôvodu túto podmienku splňajú.)

Z tohto predpokladu nám hneď vyplýva, že element zväzu s 0 má rozklad na ireducibilné prvky, a teda aj iredudantný rozklad. Ak $\{p_1, p_2, \ldots\}$ je nejaká množina atómov, tak $p_1 < p_1 \vee p_2 < p_1 \vee p_2 \vee p_3$ tvoria rast[cu postupnosť – to vyplýva z faktu, že atómy sú ireducibilné z lemy. Ak toto aplikujeme na atómy intervalu dostávame, že interval má konečný počet atómov, a teda, indukciou, je aj sám konečný.

Teoréma 10 *Nech L je distributívny zväz (spĺňajúci podmienku (F)) a nech $P \subseteq L$ množina jeho nenulových ireducibilných prvkov. Potom každý prvok a má jednoznačný iredundantný rozklad $a = p_1 \vee p_2 \vee \ldots \vee p_k$ na ireducibilné prvky, čo zapisujeme $P(a) = \{p_1, p_2, \ldots, p_k\}$, pričom $P(0) = \emptyset$.*

Dôkaz. Existencia rozkladu je zrejmá (existuje 0 a platí (F), čo zabezpečuje, že množina všetkých ireducibilných prvkov $\neq 0$ pod $a \in L$; potom treba zobrať všetky také). Jednoznačnosť: Nech

$$a = p_1 \vee p_2 \vee \ldots \vee p_k = q_1 \vee q_2 \vee \ldots \vee q_\ell$$

sú dva jednoznačné rozklady. Pre každé p_i máme $p_i \leq q_1 \vee q_2 \vee \ldots \vee q_\ell$, odtiaľ $p_i \leq q_j$ pre nejaké j. Keďže ireducibilné prvky sú neporovnateľné, dostávame $p_i = q_j$. Zopakovaním tejto úvahy potrebný počet krát dostávame, že $k \leq \ell$ a analogicky aj $\ell \leq k$. Teda $\ell = k$ a možiny $\{p_1, p_2, \ldots, p_k\}$ a $\{q_1, q_2, \ldots, q_\ell\}$ sú totožné. $\square$

Podmožina I usporiadanej množiny P je *ideál*, ak pre $\forall x, y : x \in I \;\&\; y \leq x \implies y \in I$. *Hlavný ideál* je ideál tvaru $\{x \in P; x \leq a\}$, (a môže byť aj mimo množiny P, z nejakej nadmnožiny).

Zjednotenie aj prienik ideálov sú ideály. Teda systém $\mathcal{I}(P)$ všetkých ideálov množiny P tvorí podzväz zväzu $\mathcal{P}(P)$. Teda $\mathcal{I}(P)$ je distrinutívny zväz. V ňom 0 a hlavné ideály sú očividne iredicibilné prvky. Iný dôležitý podzväz je zväz konečných hlavných ideálov $\mathcal{I}_f(P)$. Teraz ukážeme, že každý distributívny zväz spĺňajúci podmienku (F) je tohto tvaru.

Teoréma 11 *Nech L je distributívny zväz s 0 (spĺňajúci (F)) a nech P je množina všetkých jeho iredibilných prvkov $\neq 0$. Potom $L \cong \mathcal{I}_f(P)$ a izomorfizmus je daný vzťahom $\varphi : a \mapsto I(a) = \{x \in P; x \leq a\}$, $a \in L$. Obrátene zväz $\mathcal{I}_f(P)$ je distributívny a množina jeho ireducibilných prvkov je izomorfná s P. Ak L je konečný, tak $L \cong I(P)$.*

Dôkaz. Keďže každý prvok zväzu L je určený ireducibilnými prvkami, ktoré majorizuje, zobrazenie $\varphi : L \to \mathcal{I}_f(P)$ je injektívne. Na dôkaz surjektívnosti stačí ukázať, že každý konečný ideál je hlavný. Nech $I = \{p_1, p_2, \ldots, p_r$. Nech $b = p_1 \vee p_2 \vee \ldots, p_r$. Potom $b \in L$. Uvažujme hlavný ideál $I(b)$. Zrejme $I \subseteq I(b)$.

Obrátene, nech $p \in I(B)$. Je to ireducibilný prvok a $p \leq b = p_1 \vee p_2 \vee \ldots \vee p_r$. Z lemy vyplýva, že $p = p_i \in I$. Teda $I(B) \subseteq I$, čiže $I = I(b)$. Teda každý ideál je hlavný, odkiaľ vyplýva, že φ je bijekcia.

Ak $a \leq b$, $a, b \in L$, tak $I(a) \subseteq I(B)$. Obrátene $I(a) \subseteq I(b)$ implikuje $a = \sup I(a) \leq \sup I(b) = b$ (???) izomorfizmus a teda izomorfizmus zväzov. □

Dôsledok *Dva distributívne zväzy sú izomorfné, ak sú izomorfné usporiadané množiny ich ireducibilných prvkov.*

Poznámka: Analogickú konštrukciu možno urobiť pomocou $\wedge$-ireducibilných prvkov a duálneho pojmu filtra. Keďže výsledky musia byť izomorfné, dostávame, že usporiadaná množina $\wedge$-ireducibilných prvkov musí byť v distributívnom zväze izomorfná s usporiadanou množinou $\vee$-ireducibilných prvkov.

V teoréme 11 sme zistili, že distributívny zväz L s 0 je izomorfný s $\mathcal{I}_f(P)$, kde P je množina jeho ireducibilných prvkov. Keďže usporiadanie v $\mathcal{I}_f(P)$ je obyčajná inklúzia, dostávame, že každý distributívny zväz (s podmienkou (F), ako obyčajne) je izomorfný s podzväzom booleovského podzväzu $\mathcal{P}(X)$. Keďže $\mathcal{P}(X)$ je súčin reťazcov, dokázali sme

Teoréma 12 *Každý distributívny zväz s 0 je izomorfný s nejakým podzväzom booleovkského zväzu $\mathcal{P}(X)$, a teda aj s podzväzom súčinu reťazcov. Obrátene, každý podzväz súčinu reťazcov je distributívny.* □

Charakterizačná teoréma 12, kladie takúto prirodzenú otázku: Koľko je pre daný distributívny zväz L nevyhnutné zobrať reťazcov C_i na to, aby L bol podzväzom súčinu $\prod_i C_i$?

Budeme predpokladať, že $C_i = \{0 < 1 < \cdots < c_i\}$. Vnorenie $L \to \prod_{i=1}^d C_i$ nazývame *kódovaním zväzu*, číslo d dimenziou zväzu. Booleovský zväz $\mathcal{P}(X)$ má kódovanie $\mathcal{P}(X) \to \{0, 1\}^X$ v súčine $|X|$ reťazcov. Je možné tento počet znížiť za cenu predĺženie reťazcov? Z nasledujúcej teorémy vyplynie, že v tomto prípade nie.

Teoréma 13 *Nech L je distributívny zväz s 0 a nech P je usporiadaná množina jeho nenulových ireducibilných prvkov. Nech $P = \biguplus_i P_i$ je ľubovoľný rozklad usporiadanej množiny P na reťazce. Položme $C_i = \{0\} \cup P_i$, pre všetky i. Potom existuje izomorfizmus $\varphi : L \to \prod_i C_i$ na podzväz zväzu $\prod_i C_i$.*

Dôkaz. Pre ľubovoľné $x \in L$ a index i položme

$$x_i = \sup\{z \in C_i; z \leq x\}.$$

Na množine indexov zavedieme úplné usporiadanie a položíme

$$\begin{aligned} \varphi : L &\to \prod_i C_i, \\ x &\mapsto (x_i)_i. \end{aligned}$$

(Poznamenávame, že pre skoro všetky indexy (okrem konečného počtu) je $x_i = 0$. To vyplýva z podiemky (F), ktorá implikuje, že interval distributívneho zväzu má iba konečne veľa atómov a teda je konečný.)

Zobrazenie φ je injektívne, lebo keby $\varphi(x) = \varphi(y)$, tak $x_i = y_i$ pre všetky i, a teda $I(x) = I(y)$, odkiaľ $x = y$.

Okrem toho, podľa lemy o ireducibilných prvkoch máme $(x \vee y)_i = \sup\{z \in C_i; z \leq x \vee y\} = \sup\{z \in C_i; z \leq x \text{ alebo } z \leq y\} = x_i \vee y_i$. Podobne $\wedge$. $\square$

Keďže podľa teorémy 13, každý rozklad množiny P indukuje kódovanie, problém dimenzie usporiadanej množiny sa redukuje na čisto kombinatorickú úlohu nájsť pre ľubovoľnú usporiadanú množinu P rozklad na minimálny počet $d(P)$ reťazcov. Číslo $d(P)$ sa nazýva Dilworthovým číslom usporiadanej množiny. Je zrejmé, že

$$d(P) \geq \min_{A \text{ je antireťazec}} |A|.$$

V skutočnosti platí rovnosť – to je jeden z fundamentálnych výsledkov kombinatoriky.

Príklad $d(\mathcal{P}(\{1, 2, \ldots, n\})) = n$, s využitím vyššie uvedenej nerovnosti.

Teoréma 14 (Dilworth, 1950) *Nech P je konečná usporiadaná množina. Potom minimálny počet reťazcov, ktorých zjednotením je P sa rovná maximálnej mohutnosti antireťazca v P.*

Dôkaz. Ostáva nám dokázať, že ak v P existuje antireťazec mohutnosti n, tak P sa dá pokryť n reťazcacmi. Maximálnu mohutnosť antireťazca nazveme *šírkou* usporiadanej množiny P.

Budeme postupovaťindukciou vzhľadom na $|P|$. Ak $|P| = 1$, tak výsledok je triviálny. Predpokladajme, že trvdenie platí pre $|P| < k$ a uvažujme množinu $|P| = k$. Môžeme predpokldať, že šírka n množiny P je > 1.

Zvoľme nejaký maximálny prvok $x \in P$ a k nemu zoberme minimálny prvok y taký, že $y \leq x$. (Kedže P je konečná, toto sa vždy dá.) Nech $Q = P - \{x, y\}$ s indukovaným usporiadaním. Ak šírka množiny Q je menšia ako n, tak podľa indukčného predpokladu sa Q dá rozložiť na menej ako n reťazcov, čo spolu s reťazcom $\{x, y\}$ vytvára rozklad na (nanajvýš) n reťazcov. Takže môžeme prepokladať, že Q má šírku n. Odtiaľ vyplýva, že $y < x$.

V tejto situácii si vyberieme antireťazec $A = \{a_1, a_2, \dots, a_n\}$. Nech $H = \{z \in P; \exists i : z \geq a_i\}$ (horná množina) a nech $D = \{z \in P; \exists i : z \leq a_i\}$. Potom $H \cup D = P$ (inak by existoval širší antireťazec), $D \cap D = A$ (očividné) a keďže odtránením $\{x, y\}$ z P sa šírka nezúžila, máme $x \in H - D$, zatiaľ čo $y \in D - H$. Podľa indučného predpokladu existujú rozklady na $H = C_1' \cup C_2' \cdots \cup C_n'$ a $D = C_1'' \cup C_2'' \cdots \cup C_n''$. Rozklady možeme očíslovať tak, že $a_i \in C_i\prime \cap C_i''$ pre $i = 1, 2, \dots, n$. Potom $C_i = C_i\prime \cup C_i''$ je reťazec a požadovaný rozklad je $P = C_1 \cup C_2 \cup \cdots \cup C_n$. $\square$

Dôsledok *Ak L je konečný distributívny zväz a P je jeho množina nenulových ireducibilných prvkov, tak* $\dim(L) = d(P)$*.*

Teraz prejdeme k ďalšiemu aspektu distributívnosti – k poriadkovej (rangovej) funkcii. Poriadková (rangová) funckia na zväze L je funkcia $r : X \to \mathbb{N}_0$ spĺňajúca podmienky

1. $r(0) = 0$,
2. ak $a \lessdot b$, tak $r(b) = r(a) + 1$.

1.4 Modulárne a polomodulárne zväzy

Kapitola 2

Matroidy

2.1 Matroidové algoritmy

Kapitola 3

Kombinatorické konfigurácie

3.1 Konfigurácie

3.2 Zapĺňanie priehradok a urnové schémy

3.3 Latinské štvorce

3.4 Ortogonalita latinských štvorcov

3.5 (v, k, λ)-konfigurácie

Daná je množina $X = \{x_1, x_2, \ldots, x_v\}$. Systém $X_1, X_2, \ldots, X_v$ jej podmonožín množiny X tvorí (v, k, λ)-konfiguráciu, ak

1. $|X_i| = k$ pre všetky i,
2. $|X_i \cap X_j| = \lambda$ pre všetky $i \neq j$,
3. $0 < \lambda < k < v - 1$.

Množiny X_i sa nazývajú *bloky*. Matica incidencie (v, k, λ)-konfigurácie je $0, 1$-matica definovaná nasledovne

$$\begin{aligned} A &= (a_{ij}), \quad i, j = 1, 2, \ldots, v, \\ a_{ij} &= \begin{cases} 1 & x_j \in X_i, \\ 0 & \text{inak.} \end{cases} \end{aligned}$$

Označme I jednotkovú maticu rádu v, J maticu pozostávajúcu zo samých jednotiek.

1. Pretože $|X_i| = k$ je $\sum_{j=1}^{v} a_{ij} = k$, odtiaľ

$$AJ = kJ.$$

2. Keďže

$$c_{ij} = \sum_{q=1}^{v} a_{iq}a_{jq} = |X_i \cap X_j| = \begin{cases} k & i = j \\ \lambda & i \neq j \end{cases},$$

$$AA^T = \begin{pmatrix} k & \lambda & \dots & \lambda \\ \lambda & k & \dots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \lambda & \dots & k \end{pmatrix} = \lambda J + (k-\lambda)I$$

3. Matica A je regulárna, lebo

$$\begin{aligned}
\det(AA^T) &= \det(A)^2 \\
&= \begin{vmatrix} k & \lambda & \dots & \lambda \\ \lambda & k & \dots & \lambda \\ \vdots & & \ddots & \vdots \\ \lambda & \lambda & \dots & k \end{vmatrix} \\
&= \begin{vmatrix} k & \lambda - k & \lambda - k & \dots & \lambda - k \\ \lambda & k - \lambda & 0 & \dots & 0 \\ \vdots & 0 & k - \lambda & \ddots & \vdots \\ \lambda & \vdots & \ddots & \ddots & 0 \\ \lambda & 0 & \dots & 0 & k - \lambda \end{vmatrix} \\
&= \begin{vmatrix} \lambda(v-1) + k & 0 & \dots & 0 & 0 \\ \lambda & k - \lambda & \ddots & \vdots & 0 \\ \vdots & 0 & \ddots & 0 & \vdots \\ \lambda & \vdots & \ddots & k - \lambda & 0 \\ \lambda & 0 & \dots & 0 & k - \lambda \end{vmatrix} \\
&= [k + \lambda(v-1)](k-\lambda)^{v-1}
\end{aligned}$$

4. Pre každú (v, k, λ)-konfiguráciu platí

$$k(k-1) = \lambda(v-1).$$

Vychádzame z rovnosti

$$AA^T = \lambda J + (k-\lambda)I,$$

potom

$$AA^TJ = \lambda J^2 + (k-\lambda)J = \lambda vJ + (k-\lambda)J = (k+\lambda(v-1))J.$$

Pretože $0 < \lambda < k$ je matica A podľa predchádzajúcej vlastnosti regulárna a platí

$$A^{-1}J = \frac{1}{k}J.$$

Z toho dostávame

$$A^TJ = (k+\lambda(v-1))A^{-1}J = \frac{k+\lambda(v-1)}{k}J,$$

trasponovaním

$$\begin{aligned}(A^TJ)^T &= \frac{k+\lambda(v-1)}{k}J^T,\\ JA &= \frac{k+\lambda(v-1)}{k}J,\\ JAJ &= \frac{v}{k}(k+\lambda(v-1))J.\end{aligned}$$

Vieme, že $AJ = kJ$, čiže $JAJ = kJ^2 = vkJ$, porovnaním dostaneme

$$\begin{aligned}vkJ &= \frac{v}{k}(k+\lambda(v-1))J,\\ k &= \frac{k+\lambda(v-1)}{k},\\ k^2-k &= (\lambda(v-1)),\\ k(k-1) &= (\lambda(v-1)).\end{aligned}$$

3.6 Uplné diferenčné množiny

3.7 Hadamardove matice a konfigurácie

Štvorcová matica H rádu n sa nazýva *Hadamardova*, ak

1. $a_{ij} = \pm 1$
2. $HH^T = nI$ (I je jednotková matica)

Jednoduché dôsledky definície: Ak H_i, H_j sú riadkové vektory Hadamardovej matice, tak pre ich skalárny súčin platí:

$$(H_i, H_j) = \begin{cases} n & i = j,\\ 0 & i \neq j.\end{cases}$$

Čiže riadky sú na seba kolmé. Každá Hadamardova matica je regulárna, lebo $\det(H)^2 = \det(HH^T) = n^n$. Navyše Hadarmadove matice sú zrejme normálne, lebo

$$H^T H = H^{-1}HH^T H = H^{-1}nIH = nIH^{-1}H = nI = HH^T.$$

Ak H je Hadamardova, tak aj $(-1)H$ je Hadamardova. Preusporiadním riadkov a stĺpcov dostaneme opäť Hadamardovu maticu. Rovnako môžeme vynásobiť riadok alebo stĺpec (-1). Naozaj, je zrejmé, že vlastnosť

$$(H_i, H_j) = \begin{cases} n & i = j, \\ 0 & i \neq j, \end{cases}$$

je ekvivalentná podmienke

$$\sum_{k=0}^{n} h_{ik}h_{jk} \begin{cases} n & i = j, \\ 0 & i \neq j. \end{cases}$$

A táto rovnosť je invariantná voči uvedeným operáciám. Preto možno každú Hadamardovu maticu uviesť do tvaru, v ktorom prvý riadok a prvý stĺpec obsahujú kladné jednotky (normalizované).

Veta 15 *Ak n je rád Hadamardovej matice, tak $n = 1, 2$ alebo $n \equiv 0 \pmod 4$.*

Dôkaz. Pre $n = 1, 2$ majú normalizované Hadamardove matice tvar:

$$(1) \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Nech je daná Hadamardova matica rádu $n \geq 3$, prepokladajmu ju normalizovanú. Stĺpce prvých troch riadkov tejto matice majú jeden z nasledujúcich tvarov

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}.$$

Nech počet stĺpcov prvé typu je x, druhého y, tretieho z a štvrtého w. Pretože ich je spolu n, platí $x + y + z + w = n$. Nech v množine I_j sú tie indexy stĺpcov našej matice, ktorého sú typu j $(j = 1, 2, 3, 4)$. Teda máme $|I_1| = x, |I_2| = y, |I_3| = z, |I_4| = w$. Pretože riadky H_1, H_2 sú na seba kolmé, máme $h_{11}h_{21} + h_{12}h_{22} + \cdots + h_{1n}h_{2n} = 0$.

Ak $i \in I_1$, tak $h_{1i} \cdot h_{2i} = 1 \cdot 1 = 1$,
$i \in I_2$, tak $h_{1i} \cdot h_{2i} = 1 \cdot 1 = 1$,
$i \in I_3$, tak $h_{1i} \cdot h_{2i} = 1 \cdot (-1) = -1$,
$i \in I_4$, tak $h_{1i} \cdot h_{2i} = 1 \cdot (-1) = 1$.

Odtiaľ $0 = (H_1, H_2) = \sum_{i=1}^{n} h_{1i}h_{2i} = \sum_{j=1}^{4} \sum_{i \in I_j} h_{1i}2i = x + y - z - w$. Analogicky z ortogonality H_1 a H_3 dostávame $x - y + z - w = 0$, a ortogonality H_2 a H_3 dostávame $x - y - z + w = 0$.

Máme teda systém rovníc

$$\begin{aligned} x+y+z+w &= n, \\ x+y-z-w &= 0, \\ x-y+z-w &= 0, \\ x-y-z+w &= 0. \end{aligned}$$

Vyriešením dostávame $x = y = z = w = n/4$. Keďže x, y, z, w sú celé čísla, je $n \equiv 0 \pmod 4$. $\square$

Kroneckerovým súčinom matíc $A \otimes B$ matíc typu $n \times n$ a $m \times m$ rozumieme maticu typu $mn \times mn$ typu

$$\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

Ľahko sa možno presvedčiť, že tatko definovaný súčin má nasledovné tri vlastnosti:

$$\begin{gathered} (A \otimes B)^T = A^T \otimes B^T \\ (A+B) \otimes C = A \otimes C + B \otimes C \\ (AB) \otimes (CD) = (A \otimes C)(B \otimes D) \end{gathered}$$

Kroneckerov súčin Hadamardových matíc je opäť Hadamarodva matica. Naozaj:

$$(H \otimes H')(H \otimes H')^T = (H \otimes H')(H^T \otimes H'^T) = HH^T \otimes H'H'^T = nI_n \otimes mI_m = mnI_{mn}.$$

Veta 16 *Pre $n = 2^k$ existuje Hadamardova matica.*

Dôkaz. Zoberme maticu

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Definujme

$$H_{2^k} = \underbrace{H_2 \otimes H_2 \otimes \cdots \otimes H_2}_{k\text{-krát}}.$$

Podľa vyššie popísaných vlastností je to Hadamardova matica rádu 2^k. $\square$

Veta 17 *Normalizovaná Hadamardova matica rádu $m = 4\mu$ je ekvivaletná (v, k, λ)-konfigurácii s parametrami*

$$v = 4\mu - 1, \quad k = 2\mu - 1, \quad \lambda = \mu - 1.$$

Dôkaz. Z normalizovanej Hadamardovej matice vyškrtneme prvý riadok a prvý stĺpec a -1 zmeníme na 0. Keďže ľubovoľný riadok rôzny od prvého je naň komý, tak platí $\sum_{i=1}^{n} h_{1i}h_{ji} = 0$ $(j > 1)$, ale $h_{1i} = 1$ pre všetky i, preto $\sum_{i=1}^{n} h_j i = 0$, čiže počet kladných jednotiek sa rovná počtu záporných jednotiek, teda počet kladných (záporných) jednotiek je 2μ.

Pretože pre $i \neq j$, $i, j > 1$ sú riadky na seba kolmé a každý má po 2μ kladných jednotiek, majú na (práve) μ miestach kladné jednotky v rovnakých stĺpcoch.

Z toho plynie, že v našej $0,1$-matici rádu $4\mu - 1$ je súčet riadku rovný $2\mu - 1$ a dva riadky majú $\mu - 1$ jednotiek v rovnakých stĺpoch. To svedčí o tom, že naša $0,1$-matica je maticou incidencie $(v, k\lambda)$-konfigurácie s vyššie udanými parametrami. Táto konfigurácia na nazýva Hadamardova konfigurácia. V obrátenom postupe možno každej Hadamardovej konfigurácii priradiť normalizovanú Hadamardovu maticu rádu 4μ. □

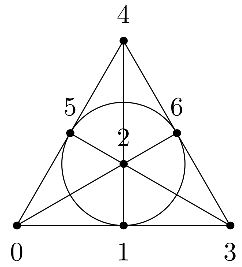
3.8 Konečné projektívne roviny

Konečnou projektívnou rovinou rádu n sa rozumie (v, k, λ)-konfigurácia s parametrami

$$v = n^2 + n + 1, \quad k = n + 1, \quad \lambda = 1.$$

Bloky X_i, $i = 1, 2, \ldots, n^2 + n + 1$ sa nazývajú priamkami a prvky blokov bodmi. Vzťah $x_i \in X_j$ znamená, že bod x_i leží na priamke X_j a vzťah $x_i \in X_j \cap X_k$, že priamky X_j, X_k sa pretínajú v bode x_i.

Príklad (v, k, λ)-konfigurácia určená úplnou diferenčnou množinou $1, 2, 4 \subset \mathbb{Z}_7$ je projektívnou rovinou, ktorú možno nasledovne znázorniť.



Čo sa týka existencie konečných projektívnych rovín, tak platí veta (dôsledok vety Buck-Ryser).

Veta 18 *Na existenciu konečnej projektívnej roviny rádu n je nutné, aby pri $n \equiv 1, 2 \pmod 4$ existovali celé čísla a, b spĺňajúce rovnosť $n = a^2 + b^2$.*

Z tejto vety vyplýva neexistencia konečných projektívnych rovín rádov napr. $6, 14, 21, 22$.

3.9 Ortogonálne latinské štvorce a projektívne roviny

3.10 Blokové konfigurácie: (b, v, r, k, λ)-konfigurácie

3.11 Steinerove trojice