1. Uspořádání na množině (svazy, úplné svazy, Booleovy algebry)

Tato kapitolka nejprve přináší úvod do teorie uspořádaných množin. Pak budou dokázány některé hlubší věty z teorie Booleových algeber a topologie.

Definice: Nechť M je množina ($M \neq \emptyset$). Částečné uspořádání (zn. $\leq$) je binární relace, která je *reflexivní, antisymetrická* a *tranzitivní*. Tedy:

REFL:	$a \leq a \;\; \forall a \in M$,
ANTISYM:	$a \leq b, b \leq a \;\Rightarrow\; a = b$,
TRANS:	$a \leq b, b \leq c \;\Rightarrow\; a \leq c$.

Částečné uspořádání $\leq$ se nazývá *lineární* (resp. *řetězec*), pokud jsou každé dva prvky $a, b \in M$ v uspořádání $\leq$ srovnatelné (tj. $\forall a, b \in M$ buď $a \leq b$ nebo $b \leq a$).

Částečné uspořádání $\leq$ na M se nazývá *dobré*, pokud je každá neprázdná podmnožina má (v sobě při uspořádání zděděném z M!) nejmenší prvek. Je ovšem zřejmé, že $\leq$ musí být lineární.

Dvojice $(M, \leq)$, kde M je neprázdná množina a $\leq$ je částečné uspořádání se nazývá částečně uspořádaná množina (zkráceně *Čum*).

Připomeňme ještě, že *Čum* $(M, \leq)$ se nazývá usměrněná (directed), jestliže platí: $\forall x, y \in M$, $\exists z \in M$ tak, že $x \leq z,\; y \leq z$.

Příklady:

(i) $(\mathbb{R}, \leq)$, kde $\leq$ je obvyklé uspořádání na reálných číslech, je *Čum*; zde $\leq$ je lineární uspořádání, není dobré (např. otevřený interval $(0, 1)$ nemá v sobě nejmenší prvek).

(ii) $(\mathbb{R}^n, \leq)$, kde $\leq$ je uspořádání "po složkách" – je *Čum*; zde $\leq$ není lineární.

(iii) Nechť $C\langle a, b\rangle$ je množina všech spojitých reálných funkcí na uzavřeném reálném intervalu $\langle a, b\rangle$. Nechť $f, g \in C\langle a, b\rangle$. Pišme $f \preceq g$ pokud $f(x) \leq g(x)$ $\forall x \in \langle a, b\rangle$. Pak $\preceq$ je částečné uspořádání na $C\langle a, b\rangle$.

(iv) Nechť M je podmnožinou množiny $\exp X$; vezmeme-li na M uspořádání $\leq$ dané inkluzí ($A \leq B \Leftrightarrow A \subset B$), vznikne částečně uspořádaná množina; zde $\leq$ není lineární.

(v) Nechť X je nekonečná množina a nechť $M \subset \exp X$ se skládá ze všech podmnožin X, které jsou doplňky konečné množiny. Pak M je *Čum* bez největšího prvku a je usměrněná.

(vi) $(N, \leq)$, kde N je množina přirozených čísel, $\leq$ obvyklé uspořádání "menší nebo rovno", je *Čum*; zde $\leq$ je dobré uspořádání.

Dříve, než budeme vyšetřovat uspořádané množiny podrobněji, všimněme si užitečné charakterizace (lineárně) uspořádaných spočetných množin. Tato charakterizace se často používa.

Tvrzení:

1. Každá spočetná dobře uspořádaná množina $(X, \preceq)$, ve které má každý prvek svého předchůdce, je (izotonně) izomorfní s množinou N všech přirozených čísel (N uspořádaná obvyklým způsobem).

2. Buď $(X, \preceq)$ spočetná lineárně uspořádaná množina bez nejmenšího a největšího prvku. Nechť $(X, \preceq)$ splňuje následující podmínku: Pro každé dva prvky $x, y \in X$ takové, že $x \prec y$ existuje $z \in X$ tak, že $x \prec z \prec y$. Pak $(X, \preceq)$ je (izotronně) izomorfní s množinou Q racionálních čísel (Q uspořádaná obvyklým způsobem).

Důkaz:

1. Pišme $N = \{1, 2, \cdots, n, \cdots\}$. Konstruujme požadovaný izomorfismus $\varphi \colon N \to X$. Označme $x_1 \in X$ nejmenší prvvek v Xa položme $\varphi(1) = x_1$. Dále postupujeme evidentní indukcí. Dostaneme izotonní zobrazení $\phi \colon N \to X$ do X. Předpokládejme, že není na množinu X. Pak existuje nejmenší prvek v množině $X - \varphi(N)$. Označme ho x. Ten ale musí mít předchůdce a pro něj je φ definováno. Takže musí být ϕ definováno i pro x a to je spor. První část je dokázána.

2. Zde je důkaz trošku složitější. Pišme $X = \{x_0, x_1, x_2, \cdots, x_n, \cdots\}$ a $Q = \{q_0, q_1, q_2, \cdots, q_n, \cdots\}$. Požadovaný izomorfismus budeme konstruovat indukcí metodou "tam a zpět". Nejdříve popíšeme "manuál" této metody, pak ji zapíšeme i formálně. Postupujeme zhruba takto: Obraz $\varphi(x_0)$ definujme libovolně. Pak se podívejme na q_0. Pokud $q_0 \prec \varphi(x_0)$ (resp. $q_0 \succ \varphi(x_0)$), vezměme libovolné x_n s vlastností $x_n \prec x_0$ (resp. $x_n \succ x_0$) a položme $\varphi^{-1}(q_0) = x_n$. Pak

postupujeme analogicky pro x_1: Podíváme se na jeho pozici vůči x_0 a $\varphi^{-1}(q_0)$ a vezmeme libovolné q_n, které tuto pozici "kopíruje" na Q vůči $\varphi(x_0)$ a q_0, atd. Je zřejmé, že vzhledem k předpokladu "hustoty" X můžeme takto stále postupovat a nakonec získat zobrazení $\varphi\colon X \to Q$, které je na Q. Z konstrukce plyne, že je to izomorfismus.

Formálně bychom zapsali tento důkaz asi takto. Máme zkonstruovat izomorfismus $\varphi\colon X \to Q$. Toto φ získáme jako "sjednocení" zobrazení $\varphi_0 \subset \varphi_1 \subset \varphi_2 \subset \cdots$, které budeme konstruovat induktivně. Položme $\varphi_0 = \emptyset$ (tj. $\varphi_0\colon \emptyset \to \emptyset$). Předpokládejme, že φ_{2n} je zkonstruováno a že máme množiny $C \subset X$ a $D \subset Q$, $\{x_0, \cdots, x_{n-1}\} \subset C$, $\{q_0, \cdots, q_{n-1}\} \subset D$ a prostou funkci $\varphi_{2n}\colon C \to D$ s vlastností monotonicity: Pokud $c_1, c_2 \in C$, pak $c_1 \prec c_2 \Leftrightarrow f_{2n}(c_1) \prec f2n(c_2)$. Uvažujme x_n. Pokud $x_n \in C$, pak položme $f_{2n+1} = f_{2n}$. Předpokládejme, že $x_n \notin C$. Pak určíme konfiguraci x_n vůči prvkům množiny C. Pokud je x_n větší (resp. menší) než prvky v C, zvolíme za jeho obraz libovolné $q \in B$ větší (resp. menší) než všechny prvky v D (to je možné, ježto Q nemá největší (resp. nejmenší) prvek). Zbývá případ, kdy některé prvky v C jsou menší a některé větší než x_n. Buď pak c_1 největší z oněch menších a c_2 nejmenší z oněch větších. Platí $c_1 \prec x_n \prec c_2$ a stačí nyní položit q libovolně tak, aby $f_{2n}(c_1) \prec q \prec f_{2n}(c_2)$. To samozřejmě lze splnit, jelikož interval $[f_{2n}(c_1), f_{2n}(c_2)]$ je v Q neprázdný. Pak položíme $f_{2n+1} = f_{2n} \cup \{[x_n, q]\}$ (zde $\cup$ chápeme jako sjednocení relací, tj. $f_{2n+1}(x_n) = q$.) Analogicky postupujeme v kroku $2n+1$: Máme-li $q_n \in D$, zvolíme $x \in X$ tak, aby funkce $f_{2n+2} = f_{2n+1} \cup \{[x, q_n]\}$ zachovávala uspořádání (to lze splnit ze zcela analogických důvodů, jako předtím využijeme toho, že X není omezená a je "v sobě hustá"). Druhá část je dokázána.

QED.

Důsledek: Každé dvě uspořádané a v sobě husté množiny jsou izotonně izomorfní (a jsou izotonně izomorfní s racionálními čísly). Pokud shora i zdola omezené, jsou rovněž izomorfní (a tedy jsou izomorfní s racionálními čísly intervalu $[0, 1]$).

Každá podmnožina částečně uspořádané množiny je (s příslušnou zděděnou relací) také částečně uspořádaná množina. Kartézský součin *Čum'ů* je *Čum* při uspořádání "po složkách".

Definice: Buďte $(M, \leq), (K, \prec)$ nějaké *Čum'y*. Zobrazení $\varphi\colon (M, \leq) \to (K, \preceq)$

se nazývá *izotonní* $\overset{\text{def.}}{\equiv}$ $(a \leq b \Rightarrow \varphi(a) \preceq \varphi(b))$;

je *izomorfizmus* $\overset{\text{def.}}{\equiv}$ φ je takové *prosté* zobrazení *na* K tak, že zobrazení φ i φ^{-1} jsou izotonní;

je *vnoření*, pokud $\varphi\colon M \to K$ je prosté a $\varphi\colon M \to \varphi(M)$ je izomorfismus.

Pozorování: Každou *Čum* $(M, \leq)$ lze izotonně vnořit do *Čum* všech podmnožin množiny M, tj. existuje vnoření $(M, \leq) \to (\exp M, \subset)$. Tedy *Čum* typu $(\exp M, \subset)$ je v jistém smyslu universální.

Důkaz: Stačí vzít zobrazení $a \to \varphi(a) = \{x \in M \mid x \leq a\}$. **QED.**

Podmínky minimality pro Čum (duálně: podmínky maximality)

Definice: Nechť $(M, \leq)$ je *Čum*. Pak $a \in M$ nazveme minimální $\stackrel{\text{def.}}{\equiv}$ v M neexistuje x tak, že $x < a$ (duálně definujeme: $a \in M$ maximální).

Uvědomme si rozdíl mezi minimální a nejmenší (nejmenší je takový prvek $a \in M$, že $x \geq a \ \forall x \in M$). Nejmenší (největší) prvek je porovnatelný se všemi prvky dané množiny; minimálních (maximálních) prvků může být víc.

Příklad: Nechť R je množina reálných čísel s obvyklým uspořádáním. Pak ovšem R nemá minimální prvek. Další příklad: vezměme v $(\exp R, \subset)$ podmnožinu "kokonečných" (kokonečná $\equiv$ doplněk konečné) množin uspořádanou $\subset$; tato množina nemá minimální prvek v M.

Důležitá otázka v teorii uspořádaných množin je otázka dobrého uspořádání. Ukázalo se, že tento problém nutně vede k použití tzv. axiomu výběru (tj. každou množinu lze dobře uspořádat $\Leftrightarrow$ přijmeme axiom výběru). Shrňme několik ekvivalentních vyjádření toho, že množinu lze dobře uspořádat.

Věta: Následující tvrzení jsou ekvivalentní:

(i) *Axiom výběru:* Pro každou množinu M existuje funkce $\varphi\colon (\exp M - \{\emptyset\}) \to M$ tak, že pro každou $X \in \exp M - \{\emptyset\}$ máme $\varphi(X) \in X$ (φ vybírá prvek z každé neprázdné podmnožiny množiny M).

(ii) *Zermelova věta:* Každou množinu lze dobře uspořádat (tj. pro každou množinu M existuje uspořádání $\leq$ s tou vlastností, že každá podmnožina má nejmenší prvek v sobě).

(iii) *Hausdorfova věta:* Každý řetězec (tj. každá lineárně uspořádaná množina) v částečně uspořádané množině je obsažen v nějakém maximálním řetězci (maximální $\equiv$ nelze již dále zvětšit).

(iv) *Kuratowského – Zornova věta* (populární *"Zornovo lemma"*): Je-li každý řetězec v částečně uspořádané množině M shora omezený, je každý prvek v M "obsažen" v některém maximálním prvku množiny M (jinými slovy: (R je řetězec v $M \Rightarrow \exists a \in M, a \geq r \ \forall r \in R$) $\Rightarrow$ ($\forall b \in M$ existuje maximální prvek v M obsahující b, tj. existuje nějaké minimální $c \in M$ tak, že $b \leq c$)).

Předchozí tvrzení (která jsou, jak jsme řekli, ekvivalentní axiomu výběru, důkaz lze najít v každé učebnici teorie množin či např. v již citované knize Kurošově) mají bohatou aplikaci i v jiných oborech matematiky než jen v teorii množin a uspořádání.

Příklad: Každý lineární (= vektorový) prostor L má bázi. (Bázi chápeme v obvyklém smyslu známém z lineárních prostorů.)

Důkaz: Náš *Čum* bude podmnožina $(\exp L, \subset)$, jejíž prvky jsou soustavy lineárně nezávislých vektorů. Podle Zornova lemma tato množina má max. prvek. Skutečně, je-li $\mathscr{S}_\alpha, \alpha \in I$ řetězec v našem *Čum* (tj. každá $\mathscr{S}_\alpha$ je lineárně nezávislá a tyto soustavy jsou inkluzí "lineárně" uspořádané – slovo lineárně je zde trochu přetíženo), pak sjednocení $\bigcup \mathscr{S}_\alpha$ je lineárně nezávislá soustava vektorů a tedy patří do našeho *Čum*. Max. prvek (= max. lin. nezáv. soustava vektorů) už musí být báze (dokaž!). (Přidáním jednoho vektoru by se ztratila lineární nezávislost. Úvahy platí i pro nekonečnou dimenzi, jelikož M je $LN \iff$ každá konečná podmnožina M je LN).
QED.

Příklad: Nechť (P, d) je metrický prostor. Buď dáno $\varepsilon > 0$. Pak v P existuje podmnožina D taková, že každé dva body v D mají vzdálenost $\geq \varepsilon$ a navíc taková, že po přidání jakéhokoli bodu už množina D *není* metricky diskrétní řádu ε (tato soustava se někdy nazývá *maximální ε-síť* v P).

Důkaz: Cvičení na Zornovo Lemma. Budeme uvažovat metricky diskrétní soustavy řádu ε, uspořádáme je inkluzí, ověříme Zornovo lemma a vezmeme maximální element. To bude požadovaná množina D. **QED.**

Definice (Svaz): Částečně uspořádaná množina $(M, \leq)$ se nazývá *svaz* ("lattice"), jestliže každá dvojice prvků $a, b \in M$ má (v M) supremum a infimum (vzhledem k $\leq$).

Připomeňme, že $c = a \wedge b$ je *infimum* $\stackrel{\text{def}}{\equiv}$ $c \leq a, c \leq b$ a navíc platí: Pokud $c' \leq a, c' \leq b$, pak $c' \leq c$. (Infimum $a \wedge b$ je největší dolní závora prvků a, b v M. Supremum $c = a \vee b$ se definuje duálně, je to nejmenší horní závora.)

Příklad: Nechť $\Omega = \{1, 2, 3, 4, \}$. Uvažujme *Čum* $(M, \leq)$, kde M se skládá ze všech podmnožin Ω o sudém počtu prvků, $\leq$ je inkluze $\subset$ na M.

Je to svaz? Ano.

Např.

$$a = \{1, 2\}, b = \{2, 3\}, \quad a \wedge b = \emptyset, a \vee b = \Omega.$$

Příklad: Totéž pro $\Omega = \{1, 2, 3, 4, 5, 6\}$, M rovněž "sudoprvky" v Ω, $\leq$ opět inkluze. Pak *Čum* $(M, \leq)$ *není* svaz. Např. pro prvky

$$a = \{1, 2, 3, 4\}, b = \{2, 3, 4, 5\}$$

neexistuje infimum, neboť $\{2, 3\}, \{3, 4\}$ jsou dvě nesrovnatelné dolní závory.

Definice: Nechť $(M, \leq)$ je částečně uspořádaná množina. Pak $(M, \leq)$ se nazývá *úplný svaz*, jestliže každá podmnožina množiny M má (v M) supremum a infimum. Jinými slovy, je-li $A \subset M$, pak existují $c, d \in M, c = \inf A; d = \sup A$.

Připomeňme, že $c = \inf A$, jestliže $\forall a \in A, c \leq a$ a jestliže navíc platí $c' \leq a \; \forall a \in A \Rightarrow c' \leq c$. Tedy $c = \inf A$ je největší dolní závora množiny A. Sup A je definováno duálně.

Příklady:

1. Interval $< 0, 1 >$ je úplný svaz.
2. $(\exp P, \subset)$ je úplný svaz pro každou množinu P ($\exp P$ jako vždy znamená množinu všech podmnožin množiny P).

Poznámka: Nejmenší prvek 0 a největší prvek 1 musí v úplném svazu $(M, \leq)$ být. Skutečně, $0 = \inf M, 1 = \sup M$. Pokud *Čum* $(M, \leq)$ má největší prvek, pak existence infima stačí k existenci suprema (a duálně). Platí totiž:

Tvrzení: $(M, \leq)$ je úplný svaz $\iff 1 \in M$ (M má největší prvek) a $\inf A$ existuje (vM) pro každou neprázdnou podmnožinu $A, A \subset M$. (Tedy když M má největší prvek a také má všechna infima $\Rightarrow$ má všechna suprema) **Důkaz**: Je-li $B \subset M$ a

$A = \{x \mid x \geq b \; \forall b \in B\}$, pak $A \neq \emptyset$ $(1 \in A)$ a $\sup B = \inf A$. **QED.**

Následující pozoruhodné tvrzení osvětluje vnitřní vlastnosti úplných svazů. (Je zajímavé, že platí i opačné tvrzení, takže jde zde o *charakterizaci* úplných svazů.)

Věta (Tarského věta o pevném bodě pro úplné svazy): Nechť $(L, \leq)$ je úplný svaz a nechť $f\colon L \to L$ je izotonní zobrazení (tj. $f\colon L \to L$ zachovává uspořádání ($x \le y \Rightarrow f(x) \le f(y)$). Pak f má pevný bod, tj. $\exists a \in L$ tak, že : $f(a) = a$.

Důkaz: Položme $S = \{x \in L \mid x \le f(x)\}$. Pak $S \ne \emptyset$, neboť $0 \in S$ (0 je nejmenší prvek v S). Položme $a = \sup S \Rightarrow \forall x \in S\colon x \le f(x) \le f(a)$ (f je izotonní). Tudíž (jak plyne z definice suprema)

$$a = \sup S \le f(a) \Rightarrow a \in S \ (a \le f(a)); f \text{ je izotonní}$$

$$\Rightarrow f(a) \le f(f(a)) \Rightarrow f(a) \in S \Rightarrow f(a) \le \sup S = a.$$

Tedy $f(a) = a$. **QED.**

Uveďme zajímavý důsledek předchozí věty.

Věta (klasika – Cantorova–Bernsteinova věta): Nechť B, C jsou množiny, nechť $f\colon B \overset{\text{inj}}{\to} C, g\colon C \overset{\text{inj}}{\to} B$ (inj znamená injektivní = prosté) $\Rightarrow \exists$ izomorfizmus $i\colon B \to C$ (tj. lze zkonstruovat *prosté* zobrazení B *na* C).

Jinými slovy, je-li $\operatorname{card} B \le \operatorname{card} C$ a $\operatorname{card} C \le \operatorname{card} B$, pak $\operatorname{card} B = \operatorname{card} C$.

Důkaz (užitím Tarského věty o pevném bodě): Nechť zobrazení $h\colon \exp B \to \exp B$ ($\exp B$ je množina všech podmnožin $B, \exp B$ je úplný svaz vzhledem k inklusi) je definováno takto: Pro $X \subset B$ klademe

$$h(X) = [B - g(C - f(X))]$$

Jelikož složení izotonních zobrazení je izotonní zobrazení $\Rightarrow h$ je izotonní. Pak (Tarského věta) $\exists$ pevný bod zobrazení h, tj. lze najít $X_0 \subset X$ tak, že $h(X_0) = X_0$. Zbývá dokázat, že zobrazení

$$\begin{array}{ll} i(x) = f(x) & \text{pokud } x \in X_0 \\ i(x) = g^{-1}(x) & \text{pokud } x \in X - X_0 \text{ je izomorfismus.} \end{array}$$

To je snadné. **QED.**

Poznámka: Jak již řečeno, platí i opačné tvrzení: Pokud L je svaz a každé izotonní zobrazení má pevný bod, pak L je úplný svaz A. C. Davis. *Pacific J. Math.*, 1955;důkaz je poněkud netriviální).

Definice (Modulární svaz): Svaz $(M, \le)$ se nazývá *modulární*, jestliže v něm platí

$$a \ge b \Rightarrow a \wedge (b \vee c) = b) \vee (a \wedge c).$$

Příklad: Svaz (lineárních) podprostorů lineárního prostoru vzhledem k inklusi je modulární svaz (odtud jeho název, neboť lineární prostor se též někdy nazývá lineární modul).

Důkaz: Nechť M je množina všech lineárních podprostorů lineárního prostoru P ($M = L(P)$). Uspořádejme ji inkluzí. Je to zřejmě svaz. Nechť $A, B, C \in L(P)$. Máme ukázat, že $A \supset B \Rightarrow A \wedge (B \vee C) = B \vee (A \wedge C)$ (zde $\wedge$ vychází jako množinový průnik, ale $\vee$ vychází jako lineární spojení). Zřejmě $A \wedge (B \vee C) \supset (A \wedge B) \vee (A \wedge C)$. Ukažme opačnou inkluzi. Nechť $x \in A$ a také $x \in B \vee C \Rightarrow x = b + c$, $c = x - b$, $x \in A \wedge C \Rightarrow x \in B \vee (A \wedge C)$. **QED.**

Definice (Modulární ortokomplementární svaz): Nechť $(L, \leq, ', 0, 1)$ je trojice taková, že vůči $\leq$ je to svaz s 0 a 1 a navíc $': L \to L$ je unární operace s vlastnostmi:

$$\begin{aligned} a \leq b \quad & \Rightarrow b' \leq a', \\ a \vee a' \quad & = 1 \\ a \wedge a' \quad & = 0. \end{aligned}$$

Pak se L nazývá *modulární ortokomplementární* svaz.

Příklad: $L(R^n)$ - svaz lineárních podprostorů v R^n (uspořádání inkluse), $': L(R^n) \to L(R^n)$, $A \in L(R^n)$, $A' \equiv$ ortogonální doplněk v R^n k (prostoru) A. Takto dostaneme modulární ortokomplementární svaz.

Poznámka (Kaplanski, Von Neumann): Existuje svazová charakterizace svazů, které jsou geometrie (tj. svazů, které jsou svazově izomorfní se svazem podprostorů nějakého lineárního prostoru).

Tvrzení (zajímavá klasika – Möbius): Mějme tři vektory v_1, v_2, v_3 v R^3, které jsou v "obecné" poloze (lineárně nezávislé a žádný není kolmý k rovině dané zbývajícími dvěma vektory). Označme L "modulární podorthoprostor" v $L(R^3)$ generovaný v_1, v_2, v_3. Pak L je topologicky hustý v R^3, tj.

$$\forall \varepsilon > 0, \forall \vec{v},\ \|\vec{v}\| = 1,\ \exists \vec{w} \in L \text{ tak, že } \|\vec{v} - \frac{\vec{w}}{\|\vec{w}\|}\| < \varepsilon.$$

Jinými slovy, vezměme tři nezávislé jednotkové vektory a iterujme operace tvoření rovin generovaných dvěma vektory a tvoření normálního vektoru k těmto rovinám (tj. tvoření vektorového součinu dvou vektorů). Jako výsledek dostaneme množinu rovin a množinu vektorů. Uvažujme množinu takto získaných vektorů. Normalizace těchto vektorů na jednotkové vektory je soustava topologicky hustá na jednotkové sféře. Tedy ze tří vektorů těmito jednoduchými operacemi dostaneme "skoro" všechny vektory.

(Bylo by možná zajímavé se na to podívat podrobněji a najít nějaká kvantitativní ohodnocení rychlosti konvergence (k danému $\vec{w}$) v závislosti na konfiguraci počátečních vektorů. Může to být známé, může to být neznámé – je třeba nahlédnout do dobré monografie z projektivní geometrie …).

Věta (McNeillovo zúplnění, Dedekindovy řezy): Každou *Čum* je možno izomorfně zobrazit (ve smyslu izomorfizmu svazů *do*) do jistého úplného svazu. Platí dokonce obecnější tvrzení (McNeillovo zúplnění): Každou částečně uspořádanou množinu $(M, \leq)$ je možno izomorfně (ve smyslu uspořádání) zobrazit do jistého úplného svazu S, přičemž toto zobrazení zachovává všechna infima i suprema, která existovala v M.

Formálně

$$\begin{aligned}&\exists\varphi\colon (M,\leq) \hookrightarrow (L,\preceq), \text{ kde } L \text{ je úplný svaz a } \varphi \text{ vnoření tak, že}\\ &\varphi(\inf A) = \inf\varphi(A),\ \varphi(\sup A) = \sup\varphi(A)\end{aligned}$$

pokud ovšem $\inf A$ a $\sup A$ existují v M.

Důkaz (náznak): Buď S množina všech ideálů v M. (Množina $I \subset M$, $I \neq \emptyset$ se (v tomto kontextu) nazývá *ideál*, jestliže:

(i) $x \in I, y \leq x \Rightarrow y \in I$,

(ii) $X \subset I$ a navíc $p = \sup(X)$ existuje v $M \Rightarrow p \in I$.

Uspořádejme S inkluzí $\subset$ ($(S, \subset)$ je pak částečně uspořádaná množina). Pak $1 \in S$ (máme $M = 1$ a S je uzavřená na tvoření průniků (neboť průnik ideálů je ideál) $\Rightarrow$ S je úplný svaz. Zobrazení $a \to \varphi(a)$, kde $\varphi(a)$ je hlavní ideál daný prvkem a: $\varphi(a) = \{x \in M \mid x \leq a\}$. Toto bude žádané zobrazení. Je třeba dokázat: $c = \bigwedge\limits_A a \overset{?}{\Rightarrow} \varphi(c) = \bigcap\limits_A \varphi(a)$ (nalevo infimum podmnožiny, napravo průnik) a rovněž $d = \bigvee\limits_A a \overset{?}{\Rightarrow} \varphi(d) = \bigvee\limits_{a\in A} \varphi(a)$ (zde ovšem $\bigvee$ stojící napravo *nemusí být* $\bigcup$). (Např. $d = \bigvee\limits_A a \to \varphi(d) \supset \bigvee \varphi(a)$ podle definice ideálu, jestliže $a \in I$, $\forall a \in A \Rightarrow \bigvee\limits_A a \in I$, etc. (Podrobněji např. v A.G. Kuroš: Kapitoly z obecné algebry. Academia. Praha 1977.)

QED.

Nyní ukážeme důležitou souvislost uspořádání ve svazu s "univerzálně algebraickým" pojetím pojmu svaz. V některých knihách doporučených nespecialistům či uživatelům se tato souvislost často automaticky využívá.

Definice (alternativní definice svazu): Množina S s dvěma binárními operacemi $\bigwedge, \bigvee$ se nazývá “svaz”, pokud platí ($a, b \in S$):

(i) $a \wedge a = a, a \vee a = a$ (idempotence),

(ii) $a \wedge b = b \wedge a,\ a \vee b = b \vee a$ (komutativita),

(iii) $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$ (asociativita obou operací),

(iv) $a \wedge (a \vee b) = a, a \vee (a \wedge b) = a$ (absorbovatelnost).

Věta: Definice svazu vycházející z uspořádání je ekvivalentní s definicí “svazu” vycházející z algebraických operací $\wedge, \vee$ (při podmínkách (i) až (iv)).

Důkaz (náznak myšlenky, je to poměrně jednoduché cvičení): Od svazu ke “svazu”:

$$(S, \leq) \text{ svaz} \to \{\inf(a, b) \to a \wedge b, \sup(a, b) \to a \vee b\}$$

Vzhledem k uspořádání dostáváme dvě operace, pro něž musíme ověřit podmínky (i) až (iv). To je snadné. Naopak od “svazu” ke svazu:

$$(S, \wedge, \vee) \text{ “svaz”} \to a \leq b \overset{\text{def.}}{\equiv} a \wedge b = a$$

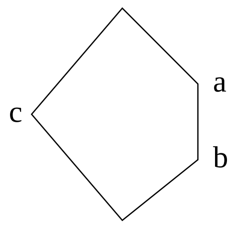
(resp. $a \vee b = b$, což ovšem dává totéž uspořádání). Pak $\leq$ činí z S svaz. **QED.**

Oba přechody se často používají, tedy svaz (při $\leq$) a “svaz” (při $\wedge, \vee$) je ekvivalentní přístup. Protože i “morfismy” si jednoznačně odpovídají, mohli bychom říci, že kategorie svazů je ekvivalentní kategorii “svazů”.

Definice: Nechť S je svaz. S se nazývá *distributivní*, jestliže $\forall a, b, c \in S$ platí následující podmínky:

$$\begin{aligned} a \wedge (b \vee c) &= (a \wedge b) \vee (a \wedge c), \\ a \vee (b \wedge c) &= (a \vee b) \wedge (a \vee c). \end{aligned}$$

Příklady:

1. $(\exp S, \subset)$ je distributivní svaz.
2. Svaz daný diagramem 

není distributivní svaz.

3. Svaz $L(R^n)$ podprostorů v lineárním prostoru R^n $(n \geq 3)$ není distributivní (stačí testovat jednodimenzionální podprostory v R^3). To je klasický příklad modulárního svazu, který není distributivní (příklad často používaný v kvantové fyzice).

Nejbohatší svaz a podle mnohých i nejzajímavější je ovšem Booleovský svaz. Má fundamentální důležitost v matematické logice a některých oborech algebry a analýzy. Zde je jeho definice.

Definice: Distributivní svaz S s 0 a 1 se nazývá *Booleovský svaz (Booleova algebra)*, pokud ke každému prvku $a \in S$ existuje prvek $a' \in S$ (komplement) tak, že platí $(a, b \in S)$:

$$\begin{array}{ll} a \leq b & \Rightarrow b' \leq a', \\ a \wedge a' & = 0, \quad a \vee a' = 1. \end{array}$$

Poznámka: Platí trochu více: $\forall a \ \exists! a'$ (existuje *právě jeden* komplement); to lze snadno dokázat již z naší (trochu slabší) definice s využitím distributivity.

Příklady:

1. $(\exp P, \subset)$ je Booleova algebra, operace $'$ je množinový komplement, $0 = \emptyset, 1 = S$.
2. "Abstraktní" Booleova algebra $(B, \wedge, \vee, ', 0, 1)$ se dá definovat jen axiomy svazu (jsou 4) a komplementu (jsou 3). Takto se to obvykle dělá.

Příklad (vymezení Booleovy algebry nějakých podmnožin jisté množiny): Nechť $\Delta \subset \exp S$, S množina, $\bigcap$ je průnik, $\bigcup$ je sjednocení, $^-$ komplement (v S). Nechť $(\Delta, \cap, \cup, ^-)$ splňuje následující podmínky:

1. $\emptyset \in \Delta$,
2. $A, B \Rightarrow A \cup B \in \Delta$, $A \cap B \in \Delta$,
3. $A \in \Delta \Rightarrow A' = \bar{A} = S - A \in \Delta$.

Pak Δ je Booleova algebra s operacemi $\bigcup, \bigcap, ^-$ a $0 = \emptyset, 1 = S$.

Podobně, jako u jiných algebraických struktur budeme říkat, že dvě Booleovy algebry B_1, B_2 jsou izomorfní, jestliže lze najít izomorfní zobrazení $i\colon B_1 \to B_2$, které respektuje všechny Booleovské operace. Vnoření pak bude injektivní zobrazení $e\colon B_1 \to B_2$, které je Booleovský izomorfismus na $f(B_2)$.

Tvrzení: Každá konečná Booleova algebra je (booleovsky) izomorfní s algebrou $(\exp S, \subset)$ pro nějakou konečnou množinu S. Důsledek: Je-li B konečná Booleova algebra, pak $\operatorname{card} B = 2^n$ a B může být chápána jako množina n-tic z 0 a 1 (charakteristické funkce na množině $\{1, 2, 3, 4, \ldots, n\}$.

Důkaz: Konečná Booleova algebra B musí mít konečný počet atomů (atom $\stackrel{\text{def.}}{\equiv}$ nejmenší prvek větší než 0). Pak lze užitím distributivity snadno ukázat, že všechny prvky B jsou v jednoznačné korespondenci se supremy množin atomů. Jestliže B má n atomů, pak zřejmě B je izomorfní s $\exp\{1, 2, \ldots, n\}$. Tedy $\operatorname{card} B = 2^n$. **QED.**

Dá se ukázat, že dokonce *každá* (i nekonečná) Booleova algebra je Booleovsky izomorfní s množinovou Booleovskou algebrou. Tato pozoruhodná věta (ekvivalentní s axiomem výběru, takže ji nelze dokázat v "naivní" matematice) je základem několika moderních matematických teorií.

Věta(Stone, 1936): Každá Booleova algebra "je" (tj. je booleovsky izomorfní s) Booleovou algebrou podmnožin nějaké množiny. (Tj. pokud $(B, \wedge, \vee, ', 0, 1)$ je *abstraktní* Booleova algebra, pak můžeme identifikovat B s množinou nějakých podmnožin nějaké množiny S tak, že abstraktní operace $\wedge, \vee, '$ přejdou v množinové operace $\bigcap, \bigcup$ a abstraktní komplement $'$ přejde v množinový komplement $^-$ (množinové operace fungují ovšem v "universu" S).

Výše uvedenou větu si teď dokážeme. Nejprve pár pojmů.

Definice: Nechť je dána Booleova algebra $(B, \wedge, \vee, ', 0, 1)$. *Stavem* na B (alternativně *pravděpodobnostní mírou* na B) rozumíme zobrazení $s\colon B \to \langle 0, 1\rangle$ takové, že

(i) $s(1) = 1$ (první 1 je v B, druhá 1 je v R),

(ii) pokud $a \wedge b = 0$, pak $s(a) + s(b) = s(a \vee b)$.

Pokud s nabývá jen hodnot 0 a 1, říkáme, že s je *dvouhodnotový stav (dvouhodnotová míra)*. Značení:

$\mathscr{S}(B)$ - množina všech stavů na B,

$\mathscr{S}_2(B)$ - množina všech dvouhodnotových stavů na B.

Definice: Nechť B je Booleova algebra. Pak $I \subset B$ se nazývá (booleovský) *ideál* (v B) jestliže platí (samozřejmě $\leq$ a $\vee$ je příslušná relace a operace v B):

(i) $a \in I, b \leq a \Rightarrow b \in I$,

(ii) $a, b \in I \Rightarrow a \vee b \in I$,

(iii) $1 \notin I$.

Definice: Ideál I na Booleově algebře B nazvěme *selektivní*, jestliže $\forall a \in B$ buď $a \in I$ nebo $a' \in I$ (a tedy $\operatorname{card}(\{a, a'\} \cap I) = 1$).

Příklad: Pro $a \neq 1$ je množina $I_a = \{x \in B \mid x \leq a\}$ ideál v B; nemusí ovšem být selektivní.

Příklad: Nechť $B = \exp N$ (B je Booleova algebra všech podmnožin N, N množina přirozených čísel), I – množina všech konečných podmnožin v N. Pak I je ideál, který není selektivní (množina všech sudých čísel nepatří do I, její doplněk – množina všech lichých čísel – tam také nepatří).

Tvrzení: Pokud $s \in \mathscr{S}_2(B)$, pak $I = \{a \in B \mid s(a) = 0\}$ je selektivní ideál. Platí i opačné tvrzení: Selektivní ideál indukuje přirozeným způsobem dvouhodnotovou míru.

Důkaz je zřejmý. Je-li I selektivní ideál, pak $s\colon B \to \{0,1\}$ dané předpisem

$$(s\colon B \to \{0,1\} \text{ tak, že } s(a) = 0 \iff a \in I) \text{ dává } s \in \mathscr{S}_2(B).$$

Následující tvrzení má fundamentální význam pro teorii Booleových algeber. Dokazuje se v něm, že každá Booleova algebra má "dost" selektivních ideálů (resp. dvouhodnotových měr). Předpokládá se axiom výběru (toto tvrzení je s ním ve skutečnosti ekvivalentní).

Tvrzení: Nechť $a \in B, a \neq 1$. Pak existuje selektivní ideál I takový, že $a \in I$.

Důkaz: Položme $I_a = \{x \in B \mid x \leq a\}$. Vezměme množinu $\mathscr{J}$ všech ideálů na B, které obsahují a. Tudíž $I_a \in \mathscr{J}$ a tedy $\mathscr{J} \neq \emptyset$. Uspořádejme $\mathscr{J}$ inkluzí. Pak $\mathscr{J}$ má maximální prvek (ověř předpoklady Zornova lemmatu – sjednocení rostoucího řetězce ideálů je ideál!). Označme ho I. Tvrdíme, že I je selektivní.

Sporem: Nechť I není selektivní. Pak existuje $b \in B$ tak, že ani b ani b' nepatří do I. Vezměme nyní ideál $\tilde{I}$ generovaný tím maximálním I a I_b ($I_b = \{x \in B \mid x \leq b\}$). Existuje skutečně takový ideál v B, který obsahuje $\tilde{I} \cup I_b$? Pokud ano, máme spor, neboť $\tilde{I}$ je striktně větší než I.

Položme $\tilde{I} = \{u \vee v,\ u \in I, v \in I_b\}$. Dá se snadno ukázat, že $\tilde{I}$ splňuje podmínky (i), (ii) z definice ideálu (použije se distributivita).

Zbývá dokázat, že $1 \notin \tilde{I}$. Předpokládejme, že $1 \in \tilde{I}$. Pak ale $1 = u \vee v = u \vee b$. Odtud

$$b' \wedge 1 = b' \wedge (u \vee b) \Rightarrow b' = (b' \wedge u) \vee (b' \wedge b) = b' \wedge u \Rightarrow b' \leq u \Rightarrow b' \in I$$

– spor. **QED.**

Tvrzení: Pokud $a \not\leq b, a, b \in B \Rightarrow \exists\, s \in \mathscr{S}_2(B), s(a) = 1, s(b) = 0$.

Důkaz: $a \not\leq b \Rightarrow c = a \wedge b' \neq 0$ (kdyby $a \wedge b' = 0 \Rightarrow b \vee (a \wedge b') = (b \vee a) \wedge (b \vee b') = b$; distributivní zákon tedy dává

$$b \vee a = b \Rightarrow a \leq b \quad \text{spor}).$$

Tudíž existuje (podle předchozích úvah) dvouhodnotový stav $s \in \mathscr{S}_2(B)$ tak, že $s(c) = s(a \wedge b') = 1$. Pak $s(a \wedge b') = 1 \Rightarrow s(a) = 1, s(b') = 1 \Rightarrow s(b) = 0$.
QED.

Důkaz(Stoneovy věty): Teď už snadno dokážeme Stoneovu větu (tj. najdeme pro B množinovou representaci). B bude (Booleovsky) izomorfní s jistou soustavou podmnožin množiny $\mathscr{S}_2(B)$. Určitěji, B bude izomorfní se soustavou všech podmnožin množiny $\mathscr{S}_2(B)$, které jsou typu $S_a = \{s \in \mathscr{S}_2(B) \mid s(a) = 1\}$ pro nějaké $a \in B$. Příslušný izomorfismus $B \to (\Delta, \bigcup, \bigcap, ^{-}, \emptyset, \mathscr{S}_2(B)$, kde $\Delta \subset \exp \mathscr{S}_2(B)$ se skládá z právě všech S_a, $a \in B$, bude definován takto:

$0 \to \emptyset$

$1 \to \mathscr{S}_2(B)$

$a \wedge b \to S_a \cap S_b$

$a \vee b \to S_a \cup S_b$

$a' \to S_{a'}$

$a \to S_a \subset \mathscr{S}_2(B)$

Snadno se ověří s užitím předchozího tvrzení, že toto zobrazení je booleovský izomorfismus. **QED.**

Každá Booleova algebra má také *topologickou representaci*: Ke každé Booleově algebře můžeme najít kompaktní topologický prostor T_B tak, že B je booleovsky izomorfní s Clop T_B, kde Clop značí soustavu všech podmnožin T_B, které jsou současně uzavřené i otevřené v T_B. Důkaz se získá dalším zjemněním výše uvedené techniky (nosná množina T_B je $\mathscr{S}_2(B)$). Literatura vhodná pro studium: P.R. Halmos: Lectures on Boolean Algebras, Springer 1974 a R. Sikorski: Boolean Algebras, Springer 1960.

Závěrem ještě dokážeme dvě hlubší věty z teorie Booleových algeber. Jsou důležité pro pochopení vnitřních vlastností Boleových algeber, ale mají i rozličné aplikace (např. v matematické logice).

Nejprve si ukážeme jednu důležitou vlastnost stavů na Booleově algebře – možnost rozšiřování stavů z menších na větší Booleovy algebry. K tomu budeme potřebovat následující klasickou větu z obecné topologie (definici topologického prostoru uvádíme dříve).

Věta (součin kompaktních prostorů je kompaktní prostor – Tichonovova věta): Buďte $(X_\alpha \mid \tau_\alpha)$, $\alpha \in I$ kompaktní topologické prostory a buď $X = (\Pi_{\alpha\in I} X_\alpha, \tau)$ topologický součin prostorů X_α, τ topologie součinu. Pak X je kompaktní prostor.

Důkaz: Tento důkaz je poněkud netriviální. Nejprve učiňme následující pozorování: Jestliže v jakémkoliv topologickém prostoru T platí, že každá centrovaná soustava množin v tom prostoru má tu vlastnost, že průnik uzávěrů uvažovaných množin je neprázdný (tj. průnik všech množin vzniklých jako uzávěry množin z celého uvažovaného systému je neprázdný), pak T je kompaktní. Připomínáme, že $\{C_\beta \mid \beta \in J\}$, $C_\beta \subset T$ se nazývá centrovaná, pokud $C_{\beta_1} \cap C_{\beta_2} \cap \cdots \cap C_{\beta_n} \neq \emptyset$ při jakémkoliv *konečném* výběru množin ze systému $\{C_\beta \mid \beta \in J\}, \beta_1, \beta_2, \ldots, \beta_n \in J$. Vidíme tedy, že pokud pro každou centrovanou soustavu $\{C_\beta \mid \beta \in J\} \subset T$ platí $\bigcap\limits_{\beta\in J} \overline{C_\beta} \neq \emptyset$, pak T je kompaktní. (To se dokáže jednoduše: Nechť $\{O_\beta \mid \beta \in \tilde{J}, \tilde{J}$ nějaká indexová množina$\}$, je otevřené pokrytí prostoru T, z kterého nelze vybrat *konečné* pokrytí prostoru T. Pak $\{T - O_\beta \mid \beta \in \tilde{J}\}$ je centrovaná soustava uzavřených množin taková, že $\bigcap\limits_{\beta\in\tilde{J}} (T - O_\beta) = \emptyset$.)

Připomeňme, že $X = (\Pi_{\alpha\in I} X_\alpha, \tau)$ má podle definice součinové topologie bázi okolí obecného bodu $x = (x_\alpha)$ tvořenou množinami typu $\bigcap\limits_{\alpha\in K} p_\alpha^{-1}(U_\alpha)$, kde K je konečná podmnožina I, U_α okolí složky x_α v topologii τ_α a $p_\alpha \colon \Pi_{\alpha\in I} X_\alpha \to X_\alpha$ je příslušná projekce na X_α.

Zpět k důkazu Tichonovovy věty: Nechť $\mathscr{B} = \{B_\beta \mid \beta \in J\}$ je centrovaná soustava množin v topologickém součinu $(\prod\limits_{\alpha\in I} X_\alpha, \tau)$. Budeme se snažit dokázat, že $\bigcap\limits_{\beta\in I} \overline{B_\beta} \neq \emptyset$ (uzávěry jsou brány v topologii τ topologického součinu $(\prod\limits_{\alpha\in I} X_\alpha, \tau)$). Podle Zornova lemmatu (dokaž!) můžeme $\mathscr{B} = \{B_\beta\}$ rozšířit na *maximální* centrovanou soustavu. Nazvěme ji $\mathscr{C}$. Tedy $\mathscr{C} = \{C_{\beta'} \mid \beta' \in J'\}$. Je zřejmé, že každá nadmnožina jakéhokoliv $C_{\beta'} \in \mathscr{C}$ patří do $\mathscr{C}$ a pokud $C \cap C_{\beta'} \neq \emptyset\ \forall \beta' \in J'$, pak $C \in \mathscr{C}$. Uvažujme projekce $p_\alpha \colon \prod\limits_{\alpha\in I} X_\alpha \to X_\alpha$, $\alpha \in I$. Pak $p_\alpha(\mathscr{C})$ je zřejmě centrovaná soustava v $X_\alpha \Rightarrow \forall \alpha \in I, \exists x_\alpha \in X_\alpha, x_\alpha \in \bigcap\limits_{\beta'\in J'} \overline{p_\alpha(C_{\beta'})}$. Dokážeme, že $x = (x_\alpha) \in \prod\limits_{\alpha\in I} X_\alpha$ patří do $\bigcap\limits_{\beta\in J'} \overline{C_{\beta'}}$ a tím bude ukázána kompaktnost prostoru $\prod\limits_{\alpha\in I} X_\alpha$.

Máme ukázat, že $x \in \overline{C_{\beta'}}$, $\forall \beta' \in J'$, tj. že každé okolí bodu $x = (x_\alpha) \in \prod_{\alpha \in I} X_\alpha$ (okolí v součinové topologii) protíná $\forall C_{\beta'}$. Stačí dokázat, že to platí pro standardní okolí, což jsou konečné průniky $p_\alpha^{-1}(U_\alpha)$ při U_α okolí $x_\alpha \in X_\alpha$. Ale jelikož $\forall \alpha \in I, p_\alpha^{-1}(U_\alpha)$ protíná každé z $C_{\beta'}$, musí být $p_\alpha^{-1}(U_\alpha)$ rovno nějaké množině $C_{\beta''}$ ze systému $\mathscr{C}$ ($\mathscr{C}$ je maximální). Tudíž i konečné průniky patří do systému $\mathscr{C} \Rightarrow x \in \overline{C_{\beta'}}\ \forall \beta' \in J'$ (ježto jeho každé okolí protíná $C_{\beta'}$!) $\Rightarrow x \in \bigcap_{\beta' \in J'} \overline{C_{\beta'}}$. **QED.**

Poznámka: Předchozí věta nám dává jiný důkaz tvrzení: $M \subset R^n$ je kompaktní $\iff$ M je uzavřená a omezená. Netriviální bylo dokázat jenom platnost implikace $\Leftarrow$. Je-li M omezená, pak $M \subset \langle a, b\rangle^n$. Jelikož $\langle a, b\rangle$ je kompaktní (dokaž! – snadné cvičení), pak $\langle a, b\rangle^n$ je (podle Tichonovovy věty) kompaktní a M je uzavřený podprostor kompaktu $\Rightarrow$ je to také kompakt.

Je zajímavé a důležité si všimnout, jak "Tichonovská topologie" (tj. topologie na součinu) souvisí s "topologií bodové konvergence usměrněného souboru funkcí" funkcí.

Věta: Nechť $P =< a, b >^X$ je množina všech funkcí $f\colon X \to < a, b >$, X nějaká množina. Opatřeme P "topologií bodové konvergence", tj. vezměme nejhrubější topologii (P, τ) tak, že $f_p \to f \iff f_p(x) \to f(x)\ \forall x \in X$ (p probíhá nějakou usměrněnou množinu). Dá se snadno ukázat, že topologie τ bude mít následující okolí: Je-li $f \in \langle a, b\rangle^X$, pak okolí bodu f v topologii τ jsou právě všechny nadmnožiny množin typu $O(x_1, x_2, \ldots, x_n; \varepsilon) = \{g \in \langle a, b\rangle^X \mid |g(x_i) - f(x_i)| < \varepsilon\ \forall i \le n\}$. Pak P je kompaktní prostor.

Důkaz: Topologie bodové konvergence na P je vlastně stejná se součinovou ("Tichonovskou") topologií na $\prod_{x \in X} X_x$, kde $X_x =< a, b >\ \forall x \in X$ (X_x je x-tá kopie X). Pak už to ihned plyne z Tichonovovy věty. **QED.**

Nyní dokážeme ohlášenou větu o rozšiřování stavů na Booleově algebře. Nejprve uveďme důležité pozorování.

Pozorování: Nechť B je Booleova algebra a nechť $\mathscr{S}(B)$ je množina všech stavů na B (resp. $\mathscr{S}_2(B)$ množina všech dvouhodnotových stavů na B). Pak $\mathscr{S}(B)$ i $\mathscr{S}_2(B)$ je kompaktní prostor (chápán s topologií bodové konvergence). Navíc $\mathscr{S}(B)$ je konvexní.

Důkaz: Aplikujme Tichonovovu větu. Víme, že $\langle 0, 1\rangle^B$ je kompakt. Ukážeme, že $\mathscr{S}(B)$ je uzavřený podprostor v $\langle 0, 1\rangle^B$ a musí být tedy taky kompakt (uzavřený podprostor kompaktu je samozřejmě kompakt). Skutečně, snadno se dokáže, že bodová limita stavů je stav. Ověřme to. Jde o to, že konečná aditivita se bodovou limitou zachovává. Nechť $s_\alpha \to s$, kde α probíhá nějakou usměrněnou množinu J a každé s_α je stav na B. Dokazujeme, že s je stav. Zřejmě $s(1) = 1$ neboť $s_\alpha(1) = 1\ \forall \alpha \in J$. Nechť $a, b \in B$, $a \wedge b = \emptyset$. Budiž dáno $\epsilon > 0$. Pak $\exists\, \alpha_1 \in J$ tak, že $\forall \alpha > \alpha_1$ máme $|s_\alpha(a \vee b) - s(a \vee b)| < \epsilon$. Analogicky, $\exists\, \alpha_2, \alpha_3 \in J$ tak, že $\forall \alpha > \alpha_2$ máme $|s_\alpha(a) - s(a)| < \epsilon$ a pro $\forall \alpha > \alpha_3$ $|s_\alpha(b) - s(b)| < \epsilon$. Jelikož $s_\alpha(a \vee b) = s_\alpha(a) + s_\alpha(b)\ \forall \alpha \in J$, dostáváme pro všechna $\alpha > \max\{\alpha_1, \alpha_2, \alpha_3\}$ nerovnost $|s(a \vee b) - s(a) - s(b)| < 3\epsilon$. Protože tato nerovnost platí $\forall \epsilon > 0$, musí zde být rovnost a tedy $s(a \vee b) = s(a) + s(b)$. **QED.**

Poznámka: Analogická věta platí i pro další struktury (i jiné, než Booleova algebra) – stavový prostor $\mathscr{S}(M)$ (= prostor konečněaditivních měr na M) je vždy kompaktní! Nic takového (bohužel) neplatí pro σ-aditivní míry.

Věta (Hornova–Tarského, zde podáváme topologický důkaz): Nechť B_1 je Booleova podalgebra Booleovy algebry B. Pak každý stav $s_1 \in \mathscr{S}(B_1)$ (resp. každý $s_1 \in \mathscr{S}_2(B)$) je možné rozšířit na stav $s \in \mathscr{S}(B)$ (resp. $s \in \mathscr{S}_2(B)$). **Důkaz**: Ukážeme hlavní ideu důkazu. Nechť $e\colon B_1 \to B$ je vnoření (e je prosté zobrazení, které zachovává všechny Booleovské operace). Nechť $s_1 \in \mathscr{S}(B_1)$. Můžeme (a budeme) chápat B_1 přímo jako "podmnožinu" B (ušetří to psaní – místo $e(b) \in B$ píšeme rovnou $b \in B_1 \subset B$). Uvažujme "rozklady jednotky" v B_1 ($\{P = \{p_1, \ldots, p_n\}$ je rozklad jednotky v Booleově algebře B_1, jestliže $p_i \wedge p'_j = 0\ \forall i, j, i \neq j$ a $\bigvee_{i \le n} p_i = 1 \in B_1$).

Uvědomme si, že množina $\mathscr{P}$ všech rozkladů jednotky v B_1 je částečně uspořádaná relací "býti jemnější" a při tomto uspořádání je $\mathscr{P}$ usměrněná. To je zřejmé – společné zjemnění dostaneme provedením průniků "každý s každým" (využíváme distributivitu B_1). Pak je-li P, Q rozklad, máme $P \wedge Q \le P, P \wedge Q \le Q$ ($P \wedge Q$ zde značí nejhrubší společné zjemnění rozkladů $P = \{p_1, p_2, \cdots, p_n\}$ a $Q = \{q_1, q_2, \cdots, q_n\}$; jinak vyjádřeno, $P \wedge Q = \{p_i \wedge q_j |\ p_i \in P,\ q_j \in Q\}$). Pro obecný rozklad jedničky P v B_1, $P = \{p_1, \ldots, p_n\}$, položme

$$F_P = \{\bar{s} \in \mathscr{S}(B) \mid \bar{s}(p_i) = s_1(p_i)\ \forall i \le n\}.$$

Všimněme si, že $F_P \neq \emptyset$. Skutečně, pro každé p_i, $p_i \neq 0$, existuje stav $\bar{s}_i \in \mathscr{S}(B)$ tak, že $\bar{s}_i(p_i) = 1$. Máme dokonce takový dvouhodnotový stav – stačí vzít stav, co odpovídá nějakému selektivnímu ideálu, který obsahuje p'_i. Pak položme $\bar{s} = \sum_{i=1}^n s_1(p_i)\, \bar{s}_i$, což je konvexní kombinace stavů na B a tudíž $\bar{s}$ je rovněž stav na B.

Pak vzhledem ke konečné aditivitě stavů je množina $\{F_P \mid P \in \mathscr{P}\}$ centrovaná soustava neprázdných uzavřených množin v (kompaktu) $\mathscr{S}(B)$

$$\Rightarrow \bigcap_{P \in \mathscr{P}} F_P \neq \emptyset \,.$$

Průnik je tedy vzat přes všechny rozklady jednotky v B_1. Tudíž $\exists s \in \mathscr{S}(B)$ tak, že $s \in \bigcap F_P$.

Stačí už jen dokázat, že s je hledané rozšíření stavu s_1, ale to je snadné, neboť *každý* prvek $a \in B_1$ lze chápat jak prvek nějakého konečného rozkladu B_1 (např. rozkladu $\{a, a'\}$) a s se musí shodovat s s_1 na všech konečných rozkladech. **QED.**

Druhou hlubší větu z teorie Booleových algeber, kterou zařazujeme do tohoto textu je Vaughtova věta o spočetných neatomických Booleovských algebrách. Tato věta říká, že každé dvě spočetné neatomické Booleovy algebry jsou (Booleovsky) isomorfní.

Poznámka: Všimněmě si, že podaný důkaz Hornovy–Tarského věty je vlastně jinou formou "věty o kompaktnosti": Z toho, že umíme najít rozšíření stavů ze všech *konečných* podBooleových algeber algebry B_1 na celou B, umíme najít rozšíření daného stavu z *celé* B_1 na B. Podobný "kompaktnostní princip" se objevuje i v ředě oblastí moderní algebry a matematické logiky.

Definice: Booleova algebra B se nazývá *neatomická*, jestliže nemá žádný atom (tj. $\forall a \in B$, $a \neq 0$, $\exists\, b \in B$, $b \neq 0$ tak, že $b < a$).

Poznámka: Pro čtenáře znalého základů matematické logiky bychom tedy mohli uvažovat "teorii neatomických Booleových algeber" tak, že bychom k obvyklým axiomům Booleovy algebry ještě dodali axiom

$$x \not\approx 0 \Rightarrow (\exists\, y)\ 0 < y < x\,.$$

Poznamenejme, že pojem *neatomická* není ovšem "negací" obvyklého pojmu *atomická* Booleova algebra. Existují Booleovy algebry, jež nejsou ani atomické ani neatomické. V těchto algebrách existuje aspoň jeden atom, ale přitom ne nutně pod každým nenulovým prvkem, je atom.

Věta (Vaught): Buďte B_1, B_2 spočetné neatomické Booleovy algebry. Pak B_1 je Booleovsky izomorfní s B_2, tj. $B_1 \cong B_2$.

Důsledek: Je-li B spočetná neatomická Booleova algebra, pak $S(B) \cong \mathrm{Clop}\{0,1\}^N$, kde $\{0,1\}^N$ je spočetný Tichonovský součin diskrétního prostoru $\{0,1\}$.

Důkaz (Důsledku): Booleova algebra Clop $\{0,1\}^N$ je zřejmě spočetná a neatomická. Stačí si uvědomit, že její generátory jsou tvořeny množinami typu $\pi_i^{-1}\{1\}$ $(i \in N)$, kde $\pi_i \colon \{0,1\}^N \to \{0,1\}$ je i-tá projekce. **QED.**

V důkazu Vaughtovy věty užijeme rozšiřovací kriterium pro morfismy v Booleových algebrách (tzv. Sikorského lemma), které má i samostatný význam. Sikorského lemma teď dokážeme. Začněme některými konvencemi.

Buď A Booleova algebra. Je-li $a \in A$, pak položíme $a^1 = a$, $a^\perp = a^{\perp_A}$. Pro $n \geq 1$ položíme $E_n = \{1, \perp\}^{\{1,\ldots,n\}}$.

Nechť jsou nyní pevně dány prvky $x_1, \ldots, x_n \in A$. (Prvky $x_1, \ldots, x_n$ se nepředpokládají po dvou různé!) Pro $e \in E_n$ položme $p_e = x_1^{e(1)} \wedge \ldots x_n^{e(n)}$. Pro $\emptyset \neq M \subset E_n$ položme $s_M = \bigvee\limits_{e \in M} p_e$; dále položme $s_\emptyset = 0_A$.

Nejprve odvodíme několik pomocných tvrzení.

Lemma:

(a) $s_{E_n} = 1_A$;

(b) $s_{M \cup M'} = s_M \vee s_{M'}$;

(c) $s_{E_n \setminus M} = s_M^\perp$.

Důkaz:

(a) Indukcí dle n. Je-li $n = 1$, pak $s_{E_1} = x_1 \vee x_1^\perp = 1_A$.

Mějme nyní prvky $x_1, \ldots, x_n, x_{n+1} \in A$. Pak dostáváme

$$\begin{aligned}
s_{E_{n+1}} &= \bigvee_{e \in E_{n+1}} p_e = \Big(\bigvee_{e \in E_{n+1},\ e(n+1)=1} p_e\Big) \vee \Big(\bigvee_{e \in E_{n+1},\ e(n+1)=\perp} p_e\Big) \\
&= \Big(\bigvee_{e \in E_n} (x_1^{e(1)} \wedge \ldots x_n^{e(n)} \wedge x_{n+1})\Big) \vee \Big(\bigvee_{e \in E_n} (x_1^{e(1)} \wedge \ldots x_n^{e(n)} \wedge x_{n+1}^\perp)\Big) \\
&= \Big[\Big(\bigvee_{e \in E_n} (x_1^{e(1)} \wedge \ldots x_n^{e(n)})\Big) \wedge x_{n+1}\Big] \vee \Big[\Big(\bigvee_{e \in E_n} (x_1^{e(1)} \wedge \ldots x_n^{e(n)})\Big) \wedge x_{n+1}^\perp\Big] \\
&= [s_{E_n} \wedge x_{n+1}] \vee [s_{E_n} \wedge x_{n+1}^\perp].
\end{aligned}$$

Podle indukčního předpokladu platí $s_{E_n} = 1_A$. Z toho plyne, že $s_{E_{n+1}} = x_{n+1} \vee x_{n+1}^\perp = 1_A$.

(b) Tvrzení je zřejmé, pokud $M \cap M' = \emptyset$. V obecném případě máme

$$\begin{aligned}
s_{M \cup M'} &= s_{(M \setminus M') \cup (M' \setminus M) \cup (M \cap M')} = s_{M \setminus M'} \vee s_{M' \setminus M} \vee s_{M \cap M'} \\
&= (s_{M \setminus M'} \vee s_{M \cap M'}) \vee (s_{M' \setminus M} \vee s_{M \cap M'}) \\
&= s_{(M \setminus M') \cup (M \cap M')} \vee s_{(M' \setminus M) \cup (M \cap M')} \\
&= s_M \vee s_{M'}.
\end{aligned}$$

(c) Platí $s_{E_n\setminus M} \vee s_M = s_{(E_n\setminus M)\cup M} = s_{E_n} = 1_A$, $s_{E_n\setminus M} \wedge s_M = (\bigvee_{E\setminus M} p_e) \wedge (\bigvee_M p_f) = \bigvee_{e\in E\setminus M} \bigvee_{f\in M} (p_e \wedge p_f)$. Pro $e \neq f$ je ale vždy $p_e \wedge p_f = 0_A$. Tedy celkem $s_{E_n\setminus M} \wedge s_M = 0_A$. Musí tedy být $s_{E_n\setminus M} = s_M^{\perp}$.

QED.

Lemma: Nechť $\exp E_n$ značí Booleovu algebru všech podmnožin množiny E_n. Jelikož prvek $M \in \exp E_n$ lze ztotožnit s charakteristickou funkcí množiny M, definuje vlastně předchozí lemma zobrazení $s\colon \exp E_n \to A$. Platí, že zobrazení $s : M \mapsto s_M$ je surjektivní morfismus

$$\exp E_n \stackrel{\text{na}}{\to} A \downarrow [\{x_i;\ i = 1, \dots, n\}]_A.$$

Důkaz: Zobrazení s je morfismus podle předchozího lemma. Abychom ukázali surjektivnost, stačí ukázat, že $\{x_i;\ i = 1, \dots, n\} \subset s(\mathcal{P}(E_n))$: Buď $1 \leq i \leq n$. Položme $M_i = \{e \in E_n;\ e(i) = 1\}$. Pak platí $s_{M_i} = x_i$. **QED.**

Nyní již můžeme dokázat Sikorského rozšiřovací lemma. Uvedeme je přitom ve tvaru vhodném pro pozdější použití. V následujícím tvrzení a v celém důkazu Vaughtovy věty ještě uděláme následující dohodu: Jsou-li x_i $(i \leq n)$ prvky Booleovy algebry A, pak $A \downarrow [\{x_i;\ i = 1, \dots, n\}]_A$ značí Booleovu podalgebru algebry A generovanou množinou x_i $(i \leq n)$.

Lemma: Buďte A, B Booleovy algebry, A buď konečně generovaná. Buď $n \geq 1$, $x_1, \dots, x_n \in A$, $y_1, \dots, y_n \in B$, přičemž množina $X = \{x_i;\ i = 1, \dots, n\}$ generuje A. (Opět poznamenejme, že prvky $x_1, \dots, x_n$ ani prvky $y_1, \dots, y_n$ se nepředpokládají po dvou různé.) Uvažujme relaci $r = \{\langle x_i, y_i\rangle;\ i = 1, \dots, n\}$. Pak existuje morfismus $f : A \to B$ takový, že $r \subset f$ právě když pro každé $\epsilon_1, \dots, \epsilon_n \in \{1, \perp\}$ platí: Jestliže $x_1^{\epsilon_1} \wedge \dots x_n^{\epsilon_n} = 0_A$, pak $y_1^{\epsilon_1} \wedge \dots y_n^{\epsilon_n} = 0_B$.

Důkaz: Nutnost je jasná, neboť f má být morfismus. Dokážeme postačitelnost. Pro $e \in E_n$ položme $p_e = x_1^{e(1)} \wedge \dots x_n^{e(n)}$, $q_e = y_1^{e(1)} \wedge \dots y_n^{e(n)}$. Pro $M \subset E_n$ položme $s_M = \bigvee_{e\in M} p_e$, $t_M = \bigvee_{e\in M} q_e$ (opět $s_\emptyset = 0_A$, $t_\emptyset = 0_B$). Víme, že pak $[X]_A = \{s_M;\ M \in \mathcal{P}(E)\}$. Přitom samozřejmě $[X]_A = A$. Definujme nyní zobrazení $f : A \to B$ předpisem $f(s_M) = t_M$. Nyní tvrdíme, že tato definice je korektní.

Skutečně, nechť $s_M = s_{M'}$. Ukážeme, že pak $t_M = t_{M'}$. Platí $s_{M\triangle M'} = s_M \triangle s_{M'} = 0_A$. Tedy pro $e \in M \triangle M'$ platí $p_e = 0_A$. To znamená, že $x_1^{e(1)} \wedge \dots x_n^{e(n)} = 0_A$.

Podle našeho předpokladu nyní též $y_1^{e(1)} \wedge \ldots \wedge y_n^{e(n)} = 0_B$. Tedy pro $e \in M \triangle M'$ platí $q_e = 0_B$. Tedy $t_{M \triangle M'} = 0_B$, tj. $t_M = t_{M'}$.

To, že $f \colon A \to B$ je Booleovský izomorfismus, se dokáže snadno:

1. $f(s_M \vee s_{M'}) = f(s_{M \cup M'}) = t_{M \cup M'} = t_M \vee t_{M'} = f(s_M) \vee f(s_{M'})$;

2. $f(s_M^\perp) = f(s_{E_n \setminus M}) = t_{E_n \setminus M} = t_M^\perp = f(s_M)^\perp$;

3. $r \subset f$ (zřejmé).

Buď $1 \leq i \leq n$. Položme $M_i = \{e \in E_n;\ e(i) = 1\}$. Pak $x_i = s_{M_i}$, a tedy $f(x_i) = f(s_{M_i}) = t_{M_i} = y_i$. **QED.**

Předchozí lemma se obvykle uvádí v literatuře ve tvaru, kdy prvky $x_1, \ldots, x_n$ se předpokládají již po dvou různé. Toto lemma pak bude mít následující tvar.

Důsledek: Buďte A, B Booleovy algebry, $X = \{x_1, \ldots, x_n\}$ množina generátorů algebry A, $f_0 \colon X \to B$. Pak zobrazení f_0 lze rozšířit na morfismus $A \to B$ právě když pro každé $\epsilon_1, \ldots, \epsilon_n \in \{1, \perp\}$ platí: Jestliže $x_1^{\epsilon_1} \wedge \ldots x_n^{\epsilon_n} = 0_A$, pak $(f_0(x_1))^{\epsilon_1} \wedge \ldots (f_0(x_n))^{\epsilon_n} = 0_B$.

V následující větě zobecníme předchozí důsledek i pro algebry, jež nemusí být nutně konečně generované. Ikdyž tuto větu nebudeme již v plném znění potřebovat pro důkaz Vaughtovy věty (stačí nám předchozí lemma), nebudeme si ji vzhledem k její mimořádné důležitosti v teorii Booleových algeber a rozličných aplikací.

Věta (Sikorski): Buďte A, B Booleovy algebry, X množina generátorů algebry A, $f_0 \colon X \to B$. Pak zobrazení f_0 lze rozšířit na morfismus $A \to B$ právě když pro každé $n \geq 1$, $x_1, \ldots, x_n \in X$ a $\epsilon_1, \ldots, \epsilon_n \in \{1, \perp\}$ platí: Jestliže $x_1^{\epsilon_1} \wedge \ldots x_n^{\epsilon_n} = 0_A$, pak $(f_0(x_1))^{\epsilon_1} \wedge \ldots (f_0(x_n))^{\epsilon_n} = 0_B$.

Důkaz: Opět stačí dokázat jen postačitelnost. Buď $Y = \{x_1, \ldots, x_n\}$ konečná neprázdná část množiny X. Buď f_Y morfismus $A \downarrow [Y]_A \to B$ rozšiřující zobrazení $f_0|Y : Y \to B$. Nyní $\{f_Y\}_{Y \in \mathrm{Fin}(X) \setminus \{\emptyset\}}$ je (nahoru) usměrněný systém morfismů. Položíme-li $f = \bigcup_{Y \in \mathrm{Fin}(X) \setminus \{\emptyset\}} f_Y$, pak f je opět morfismus s definičním oborem $\bigcup_{Y \in \mathrm{Fin}(X) \setminus \{\emptyset\}} [Y]_A = [X]_A = A$ (ověří se snadno). **QED.**

Pokračujme v důkazu Vaughtovy věty. Je vhodné postupovat poněkud obecněji (viz následující definice). Pro $a \in A$, pišme $A \downarrow a = \{b \in A |\ b \leq a\}$; pak ovšem $A \downarrow a$ je opět Booleova algebra, ve které prvek a hraje roli 1.

Definice: Buď $\mathcal{R}$ binární relace na třídě Booleových algeber. Relace $\mathcal{R}$ se nazývá *Vaughtova relace*, jestliže splňuje následující podmínky:

V1 $\mathcal{R}$ je symetrická.

V2 Jestliže $A\mathcal{R}B$ a A je triviální (tj. $|A| = 1$), pak i B je triviální.

V3 Jestliže $A\mathcal{R}B$, $a \in A$, pak existuje $b \in B$ tak, že $(A \downarrow a)\mathcal{R}(B \downarrow b)$, $(A \downarrow a^{\perp})\mathcal{R}(B \downarrow b^{\perp})$ (*back and forth property*).

Poznámka: Víme, že každý direktní rozklad Booleovy algebry A má tvar kartézského součinu $A{\downarrow}a$ x $A{\downarrow}a^{\perp}$. Existence Vaughtovy relace $\mathcal{R}$ takové, že $A\mathcal{R}B$, vlastně znamená, že A a B se rozkládají do faktorů podobným způsobem.

Věta: Předpokládejme, že A, B jsou nejvýše spočetné Booleovy algebry a $A\mathcal{R}B$ pro některou Vaughtovu relaci $\mathcal{R}$. Pak A, B jsou izomorfní.

Důkaz: Jsou-li $\{a_i\}_{i\in\mathbf{N}}$, $\{b_i\}_{i\in\mathbf{N}}$ libovolné (ale v daném okamžiku jednoznačně dané) posloupnosti prvků z A, resp. z B, pak pro $e \in E_n$ položíme

$$p_e = \bigwedge_{1\le i\le n} a_i^{e(i)},\ q_e = \bigwedge_{1\le i\le n} b_i^{e(i)}\ .$$

Budeme směřovat ke konstrukci prvků $a_i \in A$, $b_i \in B$, $i \in \mathbf{N}$ takových, aby platily následující dvě podmínky:

(+) $A = \{a_i;\ i \in \mathbf{N}\}$, $B = \{b_i;\ i \in \mathbf{N}\}$,

$(++)_n$ Pro každé $n \in \mathbf{N}$ a každé $e \in E_n$ platí $(A \downarrow p_e)\mathcal{R}(B \downarrow q_e)$.

Důkaz nyní dokončíme ve dvou krocích:

(I) v prvním kroku ukážeme, jak pomocí posloupností $\{a_i\}_{i\in\mathbf{N}}$, $\{b_i\}_{i\in\mathbf{N}}$ sestrojíme izomorfismus algeber A a B;

(II) v druhém druhém pak ukážeme konstrukci posloupností s vlastnostmi (+) a $(++)_n$.

(I) Předpokládejme tedy, že posloupnosti $\{a_i\}_{i\in\mathbf{N}}$, $\{b_i\}_{i\in\mathbf{N}}$ s vlastnostmi (+) a $(++)_n$ (pro každé $n \ge 1$) již máme. Položme
$A_n = [\{a_i;\ i \le n\}]_A$, $B_n = [\{b_i;\ i \le n\}]_B$. Pak $A = \bigcup_{n\in\mathbf{N}} A_n$, $B = \bigcup_{n\in\mathbf{N}} B_n$. To plyne z podmínky (+).

Zvolme nyní $n \le 1$ pevně. Dokážeme, že pak existuje právě jeden izomorfismus $f_n : A_n \to B_n$ takový, že $f_n(a_i) = b_i$ pro každé $1 \le i \le n$:

Položme $r = \{\langle a_i, b_i\rangle;\ i = 1, \ldots, n\}$. Nyní použijeme Sikorského rozšiřovacího lemma. Nechť $a_1^{\epsilon_1} \wedge \ldots a_n^{\epsilon_n} = 0_A$, $\epsilon_1, \ldots, \epsilon_n \in \{1, \perp\}$. Buď $e \in E_n$ zobrazení takové, že $e(i) = \epsilon_i$ pro každé $i \leq n$. Pak $a_1^{\epsilon_1} \wedge \ldots a_n^{\epsilon_n} = p_e$. Z vlastnosti $(++)_n$ máme $(A \downarrow p_e)\mathcal{R}(B \downarrow q_e)$. Protože $A \downarrow p_e$ je triviální, je podle (V2) také $B \downarrow q_e$ triviální. To znamená, že musí být i $q_e = 0_B$, tj. $b_1^{\epsilon_1} \wedge \ldots b_n^{\epsilon_n} = 0_B$.

Tedy r lze rozšířit na morfismus $f_n : A_n \overset{\text{na}}{\to} B_n$. Analogicky zobrazení $b_i \mapsto a_i$, $1 \leq i \leq n$ lze rozšířit na morfismus $g_n : B_n \to A_n$. Protože $(f_n \circ g_n)(a_i) = a_i$, morfismy $f_n \circ g_n$ a id_{A_n} se shodují na množině generátorů algebry A_n. Musí tedy už být $f_n \circ g_n = \mathrm{id}_{A_n}$. Analogicky $g_n \circ f_n = \mathrm{id}_{B_n}$. Odtud plyne, že f_n, g_n jsou vzájemně inversní izomorfismy.

Tím jsme sestrojili řetězec $\{f_n\}_{n\in\mathbf{N}}$ injektivních morfismů $A_n \to B$. Položíme-li $f = \bigcup_{n\in\mathbf{N}} f_n$, pak f je hledaný izomorfismus a tedy $A \cong B$.

(II) Nyní přistoupíme ke konstrukci posloupností $\{a_i\}_{i\in\mathbf{N}}$, $\{b_i\}_{i\in\mathbf{N}}$ s vlastnostmi $(+)$ a $(++)_n$ (pro každé $n \geq 1$).

Zvolme pevně surjektivní zobrazení $\mathbf{a} : \{1, 3, 5, \ldots\} \to A$, $\mathbf{b} : \{2, 4, 6, \ldots\} \to B$. Označme $a_i = \mathbf{a}(i)$, $i \in \{1, 3, 5, \ldots\}$, $b_i = \mathbf{b}(i)$, $i \in \{2, 4, 6, \ldots\}$. (Tedy $a_1, a_3, a_5, \ldots$ je nějaké očíslování prvků algebry A; analogicky pro B.)

Indukcí budeme nyní konstruovat "chybějící" prvky $b_1, b_3, b_5, \ldots$ z B a prvky $a_2, a_4, a_6, \ldots$ z A.

Konstrukce $\mathbf{b_1}$: Buď b_1 takový prvek z B, že $(A \downarrow a_1)\mathcal{R}(B \downarrow b_1)$, $(A \downarrow a_1^{\perp})\mathcal{R}(B \downarrow b_1^{\perp})$ (b_1 existuje dle (V3)). Pro takto definovaný prvek b_1 je zřejmě triviálně splněno $(++)_1$.

Konstrukce $\mathbf{a_{n+1}}$: Předpokládejme, že $n \geq 1$ je liché a že prvky $a_1, \ldots, a_n$ i $b_1, \ldots, b_n$ jsou již zkonstruovány tak, že $(++)_n$ platí. (Uvědomme si, že prvek b_{n+1} je již také určen.) Sestrojíme prvek a_{n+1}.

Zvolme $e \in E_n$ libovolně, ale od teď pevně. Pak podle předpokladu $(A \downarrow p_e)\mathcal{R}(B \downarrow q_e)$. Dále $q_e \wedge b_{n+1} \leq q_e$, tudíž $q_e \wedge b_{n+1} \in B \downarrow q_e$. Dle (V3) (a symetričnosti relace $\mathcal{R}$) existuje $x_e \in A \downarrow p_e$ tak, že $(A \downarrow p_e) \downarrow x_e \mathcal{R}(B \downarrow q_e) \downarrow (q_e \wedge b_{n+1})$, $(A \downarrow p_e) \downarrow x_e^{\perp_{A\downarrow p_e}} \mathcal{R}(B \downarrow q_e) \downarrow (q_e \wedge b_{n+1})^{\perp_{B\downarrow q_e}}$.

Přitom $(A \downarrow p_e) \downarrow x_e = A \downarrow x_e$, $(B \downarrow q_e) \downarrow (q_e \wedge b_{n+1}) = B \downarrow (q_e \wedge b_{n+1})$. Dále $x_e^{\perp_{A\downarrow p_e}} = x_e^{\perp} \wedge p_e$, $(q_e \wedge b_{n+1})^{\perp_{B\downarrow q_e}} = (q_e \wedge b_{n+1})^{\perp} \wedge q_e = q_e \wedge b_{n+1}^{\perp}$.

Tedy pro zkonstruovaný prvek x_e platí $(A \downarrow x_e)\mathcal{R}(B \downarrow (q_e \wedge b_{n+1}))$, $(A \downarrow (p_e \wedge x_e^{\perp}))\mathcal{R}(B \downarrow (q_e \wedge b_{n+1}^{\perp}))$.

Položme $a_{n+1} = \bigvee_{e \in E_n} x_e$. Ukážeme, že nyní platí podmínka $(++)_{n+1}$:

Buď $\epsilon \in E_{n+1}$. Položme $e = \epsilon|\{1, \dots, n\}$.

• Jestliže $\epsilon(n+1) = 1$, pak

$p_\epsilon = p_e \wedge a_{n+1} = p_e \wedge (\bigvee_{f \in E_n} x_f) = \bigvee_{f \in E_n} (p_e \wedge x_f)$. Buď $f \in E_n$, $f \neq e$. Pak $x_f \leq p_f$, tudíž $p_e \wedge x_f \leq p_e \wedge p_f = 0_A$, tj. $p_e \wedge x_f = 0_A$. Tedy $p_\epsilon = p_e \wedge x_e = x_e$, neboť $x_e \leq p_e$. Dále, $q_\epsilon = q_e \wedge b_{n+1}$.

Podmínka $(A \downarrow x_e)\mathcal{R}(B \downarrow (q_e \wedge b_{n+1}))$ nyní znamená, že $(A \downarrow p_\epsilon)\mathcal{R}(B \downarrow q_\epsilon)$.

• Nechť $\epsilon(n+1) = \perp$. Pak

$p_\epsilon = p_e \wedge a_{n+1}^\perp = p_e \wedge (\bigvee_{f \in E_n} x_f)^\perp = p_e \wedge (\bigwedge_{f \in E_n} x_f^\perp) = \bigwedge_{f \in E_n} (p_e \wedge x_f^\perp)$.

Buď $f \in E_n$, $f \neq e$. Pak $x_f \leq p_f \leq p_e^\perp$, tudíž $p_e \leq x_f^\perp$, tj. $p_e \wedge x_f^\perp = p_e$. To znamená, že $p_\epsilon = p_e \wedge x_e^\perp$. Dále, $q_\epsilon = q_e \wedge b_{n+1}^\perp$.

Podmínka $(A \downarrow (p_e \wedge x_e^\perp))\mathcal{R}(B \downarrow (q_e \wedge b_{n+1}^\perp))$ nyní znamená, že $(A \downarrow p_\epsilon)\mathcal{R}(B \downarrow q_\epsilon)$.

Ukázali jsme tedy, že v obou případech ($\epsilon(n+1) = 1$, $\epsilon(n+1) = \perp$) platí podmínka $(++)_{n+1}$.

Konstrukce $\mathbf{b_{n+1}}$: Předpokládejme, že $n \geq 1$ je sudé. Pak prvek b_{n+1} najdeme analogicky jako jsme našli prvek a_{n+1}. $\square$

QED.

Věta: Buďte A, B spočetné neatomické Booleovy algebry. Pak $A \cong B$.

Důkaz: Definujme relaci $\mathcal{R}$ mezi Booleovými algebrami takto:

$A\mathcal{R}B$ právě když A, B jsou buď obě triviální nebo obě netriviální a neatomické. Pak $\mathcal{R}$ je Vaughtova relace. **QED.**

Poznámka: Vzniká otázka, zda tvrzení analogická předchozím větám platí také pro Booleovy σ-algebry, jak je známe z teorie pravděpodobnosti. (Booleova σ-algebra B je Booleova algebra, ve které existují suprema i infima všech *spočetných* podmnožin v B.) Je zajímavý a trochu překvapivý fakt, že tomu tak vůbec není. Stoneova reprezentační věta *neplatí* pro Booleova σ-algebry. Dá se dokázat jen značně slabší výsledek (i když dosti významný v teorii Booleových σ-algeber a i jinde), že každá Booleova σ-algebra je jen homomorfním obrazem množinové Booleova σ-algebry (to říká známá Loomisova–Sikorského věta). Jdeme-li dál, nejen, že existují Booleovy σ-algebry, které nejsou množinově representovatelné (objevují se často v teoretické kvantové mechanice), ale dá se dokonce ukázat, že existují Booleovy σ-algebry, které nemají ani jeden dvouhodnotový σ-aditivní stav. Pokud jde o rozšiřování stavů, věta o rozšíření stavu neplatí ani pro množinově representovatelné Booleovy σ-algebry – např. Lebesgueova míra na σ-algebře Borelovských množin na $\langle 0,1\rangle$ se nedá rozšířit na $\exp\langle 0,1\rangle$ (tj. přirozenou Lebesgueovu míru μ měřící intervaly tak, že $\mu(\langle a,b\rangle) = b-a$, nelze rozšířit na σ-aditivní míru definovanou na všech podmnožinách intervalu $\langle 0,1\rangle$).

Poznámka o tenzorovém součinu booleovských algeber (tensor product, free product): Filosofie konstrukce tensorového součinu dvou (event. více) algebraických struktur je vždy zhruba tato: K daným dvěma strukturám hledáme jednu strukturu, která tyto dvě dané struktury "těsně" a nezávisle obsahuje. Někdy jsou s tím problémy. Pro dané dvě Booleovy algebry B_1, B_2 ale množinová representace dovoluje tvořit tenzorový součin snadno. Nechť $(S_1,\Delta_1),(S_2,\Delta_2)$ jsou množinové representace B_1, B_2 (tj. $\Delta_1 = B_1, \Delta_2 = B_2$). Vezměme $S = S_1 \times S_2$ a uvažujme (S,Δ), kde Δ je Booleova algebra (podmnožin množiny $S_1 \times S_2$), která je (Booleovsky) generovaná všemi "obdélníčky" $A_1 \times A_2$, kde $A_1 \in \Delta_1, A_2 \in \Delta_2$. Dá se snadno ukázat, že Δ se skládá *přesně* ze všech konečných disjunktních sjednocení takových obdélníčků. Pak (S,Δ) je tensorový součin Booleových algeber B_1, B_2. (Tento tenzorový součin má i další sympatické vlastnosti, např. dané dva stavy na B_1, B_2 dovolují rozšíření na celý tenzorový součin.)

Poznámka o volných Booleových algebrách:

Definice: Booleova algebra B se nazývá volná, pokud má "volné generátory", tj. pokud $\exists$ množina $G, G \subset B$ tak, že pokud $f\colon G \to \tilde{B}$ je zobrazení do Booleovy algebry $\tilde{B}$, pak f lze (jednoznačně) rozšířit na Booleovský morfismus $\tilde{f}\colon B \to \tilde{B}$.

Charakterizovat volné Booleovy algebry důležité v mnoha aplikacích Booleových algeber. Charakterizace volných Booleových algeber je např. možná dvěma následujícími způsoby (detailní a zajímavý výklad, dosažitelný pro každého, lze opět najít v v Halmosově či Sikorského knize).

1. Volné Booleovy algebry jako Lindenbaum–Tarského algebry: Utvoříme "algebru" booleovských slov nad danou abecedou a "vyfaktorizujeme" ji podle ekvivalence "být tautologicky ekvivalentní". Dostaneme Booleovu algebru. To je známé i z elementárních kurzů matematické logiky. Tyto algebry jsou volné. (Dá se ukázat, že takto můžeme konstruovat volné algebry v každé třídě algeber.)

2. Volné Booleovy algebry získané s použitím "Stoneovy duality": Platí následující pozoruhodná věta: Nechť $\{0, 1\}$ je dvoubodová množina, chápaná jako diskrétní topologický prostor. Utvořme topologický (Tichonovův) součin $P = \{0, 1\}^I$ (I je množina). Pak Booleova algebra Clop $\{0, 1\}^I$ všech podmnožin P, které jsou současně uzavřené i otevřené v P, tvoří volnou Booleovu algebru s I generátory. (Důsledek: Konečná Booleova algebra je volná právě když má 2^{2^n} prvků. Tento důsledek lze ovšem dokázat i elementárně.)

Poznamenejme závěrem, že s využitím Sikorského rozšiřovacího lemmatu, dokázaného v této kapitole, lze snadno nahlédnout, že Clop $\{0, 1\}^I$ je volná Booleova algebra. Tedy každá spočetná neatomická Booleova algebra je volná.