O grupách a svazech

2.5 Theorie (konečných) Booleových algeber

In: Ladislav Rieger (author): O grupách a svazech. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 150–159.

Persistent URL: http://dml.cz/dmlcz/403375

být doplňkem jen nulový prvek a k nulovému prvku jen jednotkový prvek — je-li splněn axiom 7 doplňku.

3. Dokažte, že rovnost $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$ je v každém svazu vždy splněna, je-li některý z prvků (a, b, c) nulou svazu. Totéž pro jednotku svazu na místě nuly. Totéž pro rovnost duální $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

4.*Dokažte, že svaz geometrického spojování a protínání bodů, přímek a rovin (k nimž přidána prázdná část prostoru = nulový prvek svazu) a celý prostor = jednotkový prvek svazu) není distributivní. (Návod: Zvolte a, b, c vhodně jako bod, přímku, rovinu.)

5.*Najděte, které ze svazů na obr. 16, 17, 18, 19 jsou distributivní. Které z nich splňují axiom doplňku? Které obojí?

6.*Dokažte, že svaz je distributivní, když a jen když neobsahuje podsvaz tvaru IV ani podsvaz tvaru V z obr. 19.

(Ukažte, že existence takových podsvazů by porušovala distributivní zákon — a obráceně, že tři prvky a, b, c porušující distributivní zákon, by vytvořily podsvaz typu IV nebo V z obr. 19.)

7.* Dokažte, že svaz všech kladných celistvých dělitelů libovolného celého čísla $N \geq 1$ (ve smyslu dělitelnosti jakožto částečného uspořádání) je konečný distributivní. Kolik prvků má tento svaz? Co je nulou a co jednotkou svazu?

8. Dokažte, že svaz všech racionálních dělitelů celého čísla N, které jsou celistvými násobky čísla $\frac{1}{N}$ (ve smyslu cvičení 4 k 2,3) je distributivní konečný svaz o jednotce svazu rovně číslu N a nule svazu rovné číslu $\frac{1}{N}$.

2,5. THEORIE (KONEČNÝCH) BOOLEOVÝCH ALGEBER.

Odvoďme si nejprve několik jednoduchých a potřebných důsledků z axiomů pro distributivní a komplementární svazy (Booleovy algebry).

1. *V distributivním svazu může existovat* (ve smyslu axiomu 7) *nejvýše jeden doplněk k danému prvku.* — Neboť vskutku, nechť k prvku x daného distributivního svazu — rozumí se svazu s nulou n a s jednotkou j — máme dva doplňky, x' a x^+. Pak je tedy (dle axiomu 7)

$$x \cup x' = j, \quad x \cap x' = n, \quad x \cup x^+ = j, \quad x \cap x^+ = n.$$

Protněme první z napsaných rovností na obou stranách prvkem x^+. Pomocí axiomů 6′ a 5′ dostáváme

$$\begin{aligned} x^+ = (x \cup x') \cap x^+ = (x \cap x^+) \cup (x' \cap x^+) = \\ = n \cup (x' \cap x^+) = x' \cap x^+, \end{aligned}$$

tedy

$$x^+ = x' \cap x^+.$$

Záměnou x' za x^+ dostáváme právě tak $x' \cap x^+ = x'$, když jsme užili ještě cestou axiomu komutativity 3″. Tedy musí být $x' = x^+$; doplněk je jen jeden.

2. *V každé Booleově algebře platí užitečná početní t. zv. pravidla De Morganova*:

$$(x \cup y)' = x' \cap y'$$

(slovy: Doplněk spojení je průnikem doplňků).

$$(x \cap y)' = x' \cup y'$$

— obojí pro libovolné dva prvky x, y (slovy: Doplněk průniku je spojením doplňků).

Dokažme třebas jen druhé z obou pravidel. První se dokáže duálním způsobem, což si opět čtenář provede laskavě sám jako cvičení.

Máme dokázat, že prvek $x' \cup y'$ splňuje požadavky na doplněk k prvku $x \cap y$. Za pomocí axiomů 2′, 5′ a 6′ máme vskutku

$$\begin{aligned} (x \cap y) \cup (x' \cup y') = [(x \cap y) \cup x'] \cup y' = \\ = [(x \cup x') \cap (x' \cup y)] \cup y' = (x' \cup y) \cup y' = x' \cup (y \cup y') = \\ = x' \cup j = j \end{aligned}$$

to jest (poněvadž ostrá nerovnina je zřejmě vyloučena)

$$(x \cap y) \cup (x' \cup y') = j.$$

Stejně je i

$$\begin{aligned} (x \cap y) \cap (x' \cup y') = x \cap [y \cap (x' \cup y')] = \\ = x \cap [(x' \cap y') \cup (y \cap y')] = x \cap (x' \cap y') = \\ = (x \cap x') \cap y' = n \cap y' = n \end{aligned}$$

3. *Pravidlo o převrácení polouspořádání doplňováním*: Když je $x \subseteq y$, pak je $y' \subseteq x'$.

$x \subseteq y$ značí totiž $x \cup y = y$, tedy i $y' = (x \cup y)'$ (dle jednoznačnosti doplňku). Dle prvního De Morganova pravidla je však $y' = x' \cap y'$, což značí $y' \subseteq x'$.

4. *Pravidlo o dvojím doplňku*:

Pro každý prvek x platí

$$(x')' = x.$$

Neboť ve smyslu axiomu 7 prvek x splňuje požadavky toho, aby byl doplňkem k prvku x' — jestliže ovšem ještě přihlédneme k axiomům komutativity 3', 3''.

5. *Pravidlo o převádění polouspořádání na anulovanou rovnost*: Je $x \subseteq y$ tehdy a jen tehdy, když $x \cap y' = n$.

Jednak totiž protnutím nerovniny $x \subseteq y$ na obou stranách prvkem y' máme $x \cap y' \subseteq y \cap y' = n$, jednak spojením obou stran rovnosti $x \cap y' = n$ s prvkem y máme (užitím axiomu distributivity)

$$(x \cup y) \cap (y \cup y') = x \cup y = y,$$

což značí

$$x \subseteq y.$$

A nyní velmi potřebná obecná definice:

Říkáme, že prvek p svazu, (po případě Booleovy algebry) B je atomem (též někdy sousedem nuly), když jediným prvkem z z B splňujícím nerovnost $z \subset p$ je nula $n = z$ svazu (algebry) B.

Věta (o množinové representaci konečné Booleovy algebry):

Každá konečná Booleova algebra B je isomorfní s Booleovou algebrou (t. j. s množinovým okruhem) B_N *všech skupin utvořených z vhodného konečného počtu N předmětů.*

Důsledek věty: *Každá Booleova konečná algebra má 2^N prvků (při vhodném N přirozeném). Všechny Booleovy algebry o stejném konečném počtu prvků jsou navzájem isomorfní.*

Důkaz věty:

Nejprve dokažme, že každý od nuly různý prvek a dané konečné Booleovy algebry B obsahuje alespoň jeden atom p, t. j. je

$$p \subseteq a.$$

Najdeme za tím účelem — je-li to možno — k prvku $a \neq n$ prvek $a_1 \neq n$ tak, že je $a_1 \subset a$. Není-li to možno, pak ovšem musí být podle definice prvek a sám atomem, $a = p$, čímž jsme žádaného docílili. — V prvním případě učiňme dále totéž s prvkem a_1 místo původního prvku a. Opět buďto je $a_1 = p$ je sám atom, pak $p \subset a$ a jsme hotovi, anebo možno nalézt další prvek a_2 tak, že je $n \subset a_2 \subset a_1 \subset a$. Tak pokračujíce můžeme učinit nanejvýše tolik kroků a dospět k t. zv. klesajícímu řetězci

$$a_k \subset a_{k-1} \subset \ldots \subset a_1 \subset a$$

takové délky, kolik je prvků algebry B (ve skutečnosti, je ovšem nejvyšší možná délka klesajícího řetězce mnohem menší než počet prvků naší algebry). Zřejmě poslední člen a_k takového klesajícího řetězce, který se již nedá prodloužit, je hledaným atomem, $p = a_k \subset a$.

Utvořme nyní spojení $p_1 \cup p_2 \cup \ldots \cup p_r = b$ všech vzájemně různých atomů, které jsou obsaženy v daném prvku $a \neq n$, $p_i \subseteq a$ $(i = 1, 2, \ldots, r)$. (Je jasné, že těchto atomů je konečný počet r, protože všech prvků algebry je konečně mnoho.)

Tvrdím, že

$$b = a.$$

Za účelem tohoto důkazu si pišme

$$a = a \cap j = a \cap (b \cup b') = (a \cap b) \cup (a \cap b') = \\ = b \cup (a \cap b')$$

(protože je ovšem $b \subseteq a$, takže $a \cap b = b$). Kdyby bylo $b \neq a$, pak by z právě napsaného plynulo $a \cap b' \neq n$. Z druhé strany je ovšem $a \cap b' \subseteq a$. Tedy bychom podle svrchu řečeného mohli nalézt jakýsi atom p, splňující $p \subseteq a \cap b' \subseteq a$. Pak by platilo

$$b \cap p = (p_1 \cup p_2 \cup \ldots \cup p_r) \cap p \subseteq b \cap (a \cap b') = n,$$

čili — užitím distributivního zákona — by bylo

$$(p_1 \cap p) \cup (p_2 \cap p) \cup \ldots \cup (p_r \cap p) = n.$$

To ovšem znamená, že každý člen napsaného spojení by byl n, čili že je $p \neq p_i$ pro $i = 1,2, \ldots r$, ačkoli p je jeden z atomů obsažených v a. — Ježto tedy by možnost ostré nerovniny ve vztahu $b = p_1 \cup p_2 \cup \ldots \cup p_r \subseteq a$ vedla k nemožnému důsledku, musí ve skutečnosti nastat rovnost $b = a$.

Tvrdím dále, že vyjádření libovolného prvku $a \neq n$ naší algebry spojením všech atomů v něm obsažených je jednoznačné, t. j. že žádné jiné atomy nedávají svým spojením prvek a.

Že každý atom, vystupující v libovolném spojovém vyjádření prvku a, je obsažen v a — je jasné. Mohlo by se tedy nanejvýš snad stát, že by již i vlastní část atomů, obsažených v a stačila k vyjádření a jejich spojením. V takovém případě bychom však jistě vynecháním některého atomu (a budiž to při vhodném označení zrovna atom p_r) z napsaného spojového vyjádření prvku a ještě obdrželi prvek a, $a = p_1 \cup \cup p_2 \cup \ldots \cup p_{r-1}$. Avšak protněme tuto rovnost na obou stranách atomem p_r. Dostáváme — za pomoci distributivního zákona

$$p_r = a \cap p_r = (p_1 \cap p_r) \cup (p_2 \cap p_r) \cup \ldots \cup (p_{r-1} \cap p_r)$$

následkem $p_r \subseteq a$. Avšak na druhé straně je jasné, že jednotliví členové napsaného spojení, prvky $p_i \cap p_r$ (pro $i = 1, 2, \ldots, r - 1$), jsou podle definice atomu vesměs rovny nule n, tedy i jejich spojení $= n$, což dává spor. To znamená, že žádný z atomů obsažených v prvku $a \neq n$ nelze postrádat, chceme-li jejich spojením dostat a.

Utvořme nyní soubor (množinu) všech atomů naší Booleovy algebry, jichž budiž N. Utvořme všechny skupiny atomů (včetně skupiny prázdné a plné). Přiřaďme každému prvku $a \neq n$ naší algebry podle právě řečeného skupinu atomů, jež jsou v něm obsaženy. Pak každá skupina atomů vzájemně jednoznačně odpovídá prvku naší algebry. Nule n naší algebry přiřadíme pochopitelně prázdnou skupinu atomů. Přiřazení můžeme vyznačit takto: $a \longleftrightarrow (p_1, p_2, \ldots, p_r)$, jestliže $a = p_1 \cup p_2 \cup \ldots \cup p_r$, kde ovšem $0 \leqq r \leqq N$ ($r = 0$ pro $a = n$).

Jde již jen o to dokázat, že jestliže ještě prvku b je takto přiřazena skupina atomů $(q_1, q_2, \ldots, q_s)$, pak: Spojení $a \cup b$ je tímto způsobem přiřazeno sjednocení obou skupin atomů, průseku $a \cap b$ je přiřazen průnik obou skupin atomů a doplňku a' je přiřazena skupina atomů, neobsažených v a; neboť právě toho si žádá isomorfismus, o nějž ve větě jde.

Skutečně, patrně je

$$a \cup b = p_1 \cup p_2 \cup \ldots \cup p_r \cup q_1 \cup q_2 \cup \ldots \cup q_s,$$

při čemž ovšem některé atomy se v tomto spojení mohou vyskytovat dvakráte. Podržíme-li z takových dvakráte se vyskytujících atomů vždy jen jeden ve spojení, obdrželi jsme jednoznačné vyjádření prvku $a \cup b$ jakožto spojení vzájemně různých atomů. Avšak soubor těchto atomů je nyní zřejmě sjednocením skupiny $(p_1, \ldots, p_r)$ se skupinou$(q_1 \ldots q_s)$.

Podobně máme pomocí axiomů distributivity:

$$a \cap b = (p_1 \cup \ldots \cup p_r) \cap (q_1 \cup \ldots \cup q_s) =$$
$$= (p_1 \cap q_1) \cup (p_1 \cap q_2) \cup \ldots \cup (p_1 \cap q_s) \cup \ldots \cup (p_r \cap q_s) =$$

= spojení všech průniků každého atomu, obsaženého v a — s každým atomem, obsaženým v b. Z definice atomu však plyne, že je $p_i \cap q_k \neq n$ (pro $i = 1, 2, \ldots, r$, $k = 1, 2, \ldots, s$) tehdy a jen tehdy, když $p_i = q_k$, kdy ovšem $p_i \cap q_k = p_i = q_k$ je atom, obsažený jak v a tak i v b. Tím však je řečeno, že v průseku obou prvků a, b jsou právě a jen obsaženy ty atomy, jež jsou současně obsaženy v obou, čili jež tvoří dohromady průnik obou skupin atomů, přiřazených jednomu a druhémů prvku.

Konečně pokud jde o doplněk: Je-li $a = p_1 \cup \ldots \cup p_r$, pak nechť všechny ostatní atomy (navzájem různé a různé od všech p_i $(i = 1, 2, \ldots, r)$ jsou $q_1, q_2, \ldots, q_s$. (Pak ovšem $s = N - r$.) Utvořme jejich spojení, prvek $q_1 \cup \ldots \cup q_s$. Čtenář se již sám přesvědčí, že tento prvek má vlastnosti, jež jsou požadovány od doplňku k prvku a, čímž je důkaz naší věty dokončen.

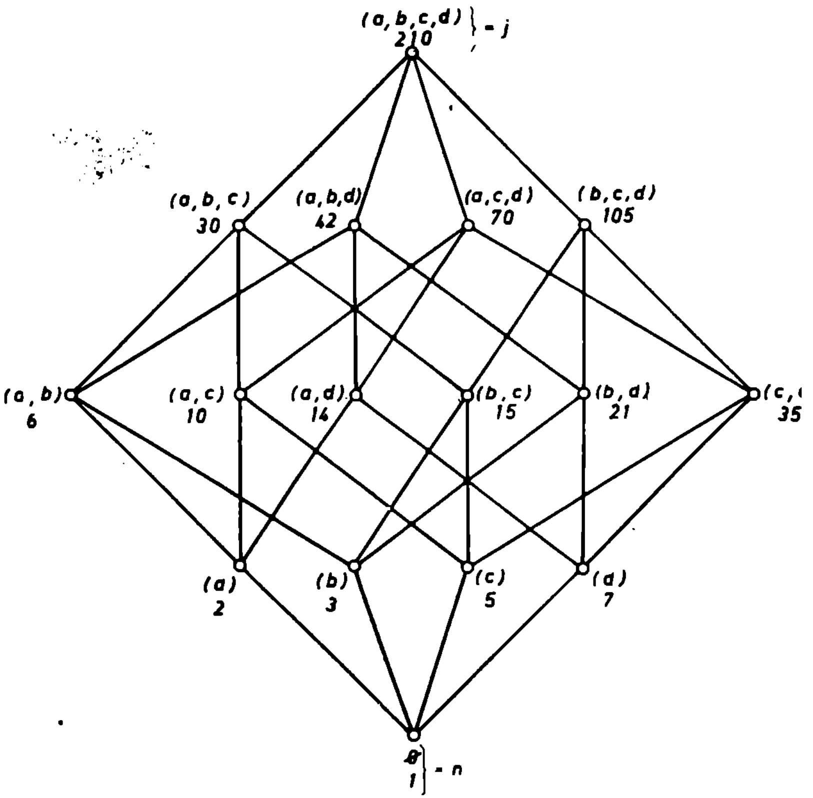
Vidíme tedy, že dle věty 1 lze studium konečných Booleových algeber převést na studium systémů všech částí konečných množin.

Jak již bylo řečeno, v nekonečných Booleových algebrách nejsou poměry zdaleka tak jednoduché. Každá i nekonečná Booleova algebra se dá sice isomorfně representovat jistým množinovým okruhem, který však jen zcela výjimečně může být systémem všech části vhodné (nekonečné) množiny. Jednoduchý příklad Booleovy algebry podstatně různé od systému všech částí množiny nám to osvětlí. Mysleme si systém všech částí (podmnožin) množiny všech přirozených čísel 1, 2, 3, ... Vyberme si však z tohoto systému jen: *Podmnožiny konečné a jejich doplňky*, t. j. nekonečné množiny s konečnými doplňky. (Tak na př. množina (2, 4) a množina (1, 3, 5, 6, 7, ...) budou patřit mezi takto vybrané množiny přirozených čísel.) Tvrdím, že tento systém množin tvoří nejen množinový okruh, ale právě Booleovu algebru. Skutečně, sjednocení a ovšem i průnik dvou konečných množin přirozených čísel je zase konečná množina. Rovněž průnik konečné množiny s nekonečnou množinou (která má konečný doplněk, ale nejen s takovou, nýbrž vůbec s každou) je konečný. Sjednocení konečné množiny s nekonečnou, která má konečný doplněk, je ovšem nekonečná množina, která má tím spíše konečný doplněk. Sjednocení dvou množin nekonečných o konečných doplňcích je rovněž tím spíše nekonečná množina, která má konečný doplněk. A konečně i průnik dvou nekonečných množin o vesměs konečných doplňcích je opět množina nekonečná o konečném doplňku, protože tento doplněk průniku je jako dle De Morganova pravidla, jak čtenář snadno nahlédne, roven sjednocení doplňků, což jsou však dle předpokladu konečné množiny. Co se týče doplňků, je nyní již jasno, že jsou v pořádku.

Avšak je nejen zřejmo, že takto sestrojená nekonečná Booleova algebra neobsahuje všechny části množiny přirozených čísel jako prvky (na př. není v ní množina všech lichých čísel), nýbrž snadno se dá ukázat, že ani nemůže být s žádným systémem všech částí nějaké množiny isomorfní. (Čtenář, který zná Pospíšilovu knížku o nekonečnu v matematice, resp. který ví, co jsou to nespočetné mohutnosti množin, ví již odtud, proč nemůže být naše spočetná algebra isomorfní s algebrou všech částí nějaké množiny.)

Dříve, než se obrátíme k zběžnému naznačení aplikací (konečných) Booleových algeber, pozdržme se chvilku u geometrického (grafického) znázornění konečných Booleových algeber. Tvrdím, co bylo již na obrázcích naznačeno: Že totiž za geometrické (grafické) znázornění Booleovy algebry lze vždy pokládat krychli, postavenou na jeden vrchol, ovšem v prostoru o příslušné dimensi N, jestliže algebra má (dle věty 1) 2^N prvků. (Pro $N = 1, 2, 3$ to již známe z obr. 16, 18 I a 14.) Dle věty 1 lze totiž každou konečnou Booleovu algebru v podstatě pokládat za systém všech podmnožin jakékoli konečné množiny o N prvcích. Mysleme si N navzájem orientovaných os (euklidovského) N-rozměrného prostoru. Na kladnou polovičku každé z nich nanesme od počátku délku 1. Pak takto získaných N bodů (o souřadnicích vždy až na jednu (i-tou) vesměs rovných nule (i probíhá $1, \dots, N$)), nechť tvoří naši konečnou množinu. Z ní nyní máme utvořit všechny části, t. j. všechny skupiny základních (nejprostších číselných N-tic, kde však jsou v každé N-tici samé nuly, a jen na jednom místě (i-tém) je 1. Každou takovou skupinu N-tic lze však považovat za jedinou N-tici, která vykazuje 1 na těch a jen těch místech, kde byla 1 v některé ze základních N-tic z dané skupiny (na ostatních místech má výsledná N-tice nuly). To však není nic jiného než souřadnice jednotlivých rohů N-rozměrné krychle o hraně 1. Snadno se pak dokáže, že spojení dvou prvků dané konečné Booleovy algebry se nyní geometricky representuje takto: Ke dvěma prvkům, t. j. teď rohům naší N-rozměrné krychle, najdeme jejich *spojení* jakožto roh, který je *co nejblíže počátku* (jenž odpovídá nule algebry), z těch rohů, do nichž se lze dostat z jednoho i z druhého daného rohu po hranách krychle za *neustálého vzdalování se od počátku* souřadnic. Podobně přechází vyhledávání *průseku* dvou prvků algebry, t. zn. dvou rohů naší krychle, ve vyhledávání od počátku co nejvzdálenějšího rohu krychle, do něhož se lze dostat z obou daných vrcholků po hranách krychle, za *neustálého blížení se k počátku*. Konečně není těžké nahlédnout, že doplněk k danému vrcholku naší krychle jakožto prvku Booleovy algebry, je protilehlý vrcholek, t. j. ten, do něhož vede přímá spojnice daného vrcholku se středem krychle (4-rozměrná krychle, představující Booleovu algebru o $2^4 = 16$ prvcích, je na obr. 21).

A nyní se obraťme k naznačení některých aplikací konečných Booleových algeber.



Obr. 21.

Cvičení k 2,5.

1. Dokažte první De Morganovo pravidlo (identitu) pro Booleovy algebry.

2. Dokažte, že atom je právě takový prvek q v Booleově algebře, pro nějž platí, když je $x \cup y = q$, pak buďto $x = q$, nebo $y = q$.

3. Dokažte, že atom je v Booleově algebře právě takový prvek q, pro který platí, když je $x \supset q'$, pak je již $x = j$ (jednotka algebry).

4. Dokažte, že distributivní svaz všech celistvých dělitelů celého čísla $N > 1$ (ve smyslu svazového polouspořádání dle vztahu dělitelnosti) je Booleova algebra tehdy a jen tehdy, když číslo N nemá čtvercových dělitelů. (Viz cvičení 6 k 2,4.)

2,6. „RACIONÁLNÍ FUNKCE" NA BOOLEOVĚ ALGEBŘE (BOOLEOVSKÉ FUNKCE). ÚPLNÉ NORMÁLNÍ FORMY.

Vyjděme opět z analogie s čísly.

Čtenář si vzpomene, že t. zv. racionální funkce ve školské algebře jsou zhruba řečeno takové funkce (mající za hodnoty t. zv. argumentu vždy jedno nebo i více čísel a za hodnoty funkce vždy jedno číslo), kde hodnota funkce se dá vypočítat z hodnot argumentu dle vhodného početního předpisu, skládajícího se z kombinovaného sečítání, odčítání, násobení a (pokud dělitel není nula) dělení.

(Příklady takových racionálních početních předpisů, jež čtenář dobře zná, jsou

$$f(x) = \frac{x^2 - 1}{x}, \quad g(x, y) = \frac{x^2 + 2xy + 3}{x + y},$$

$$h(x, y, z) = \frac{1 + x^2}{3{,}2 \cdot y} + y + \frac{2{,}5}{z}, \text{ atp.}).$$

V takovém početním předpisu pro racionální funkci vystupují, jak známo, jednak určitá pevná čísla, t. zv. k o n s t a n t y a jednak t. zv. n e z á v i s l e p r o m ě n n é (neurčité), a to v konečném (ale zásadně neomezeném) počtu m, na př. jsou to $x, y, z, \ldots$ anebo jsou to $x_1, x_2, \ldots$ Provedení předpisu spočívá v tom, že při daném argumentu, t. j. uspořádané skupině čísel $a_1, a_2, \ldots, a_m$ se prostě dosadí za odpovídající nezávisle proměnné jim odpovídající čísla, t. zn. řekněme číslo a_1 za proměnnou x_1, a_2 za x_2 atd. až posléze a_m za x_m, a takto naznačené početní úkony se provedou (s výjimkou neproveditelného dělení nulou, pokud se vyskytne). Výsledek je hodno-