

Matematická logika

Výroková logika - pokračování (3.přednáška)

Marie Duží

marie.duzi@vsb.cz



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Normální formy formulí výrokové logiky

- Každé formuli výrokové logiky přísluší právě jedna pravdivostní funkce, zobrazení $\{p, q, r, \dots\} \rightarrow \{0, 1\}$ (pravdivostní tabulka).
- Naopak, však jedné takové funkci odpovídá **nekonečně mnoho formulí**, které jsou navzájem *ekvivalentní*.

Definice: Formule A, B jsou **ekvivalentní**, značíme $A \Leftrightarrow B$, mají-li přesně stejné modely, tj. vyjadřují stejnou pravdivostní funkci. Jinými slovy,

$$A \Leftrightarrow B \quad \text{iff} \quad A \models B \quad \text{a} \quad B \models A.$$

Příklad: $p \supset q \Leftrightarrow \neg p \vee q \Leftrightarrow \neg(p \wedge \neg q) \Leftrightarrow (p \supset q) \wedge (p \vee \neg p) \Leftrightarrow (p \supset q) \vee (p \wedge \neg p) \Leftrightarrow \dots$

Pozn.: Nesmíme plést ekvivalenci formulí $A \Leftrightarrow B$ s formulí tvaru ekvivalence $A \equiv B$.
Platí však, že $A \Leftrightarrow B$ právě když formule $A \equiv B$ je tautologie.

Př.: $(p \equiv q) \Leftrightarrow [(p \supset q) \wedge (q \supset p)] \text{ iff }$
 $\models [(p \equiv q) \equiv ((p \supset q) \wedge (q \supset p))]$

Normální formy - příklad

p	q	$f(p,q)$
1	1	1
1	0	0
0	1	0
0	0	1

Této pravdivostní funkci odpovídá nekonečně mnoho formulí:

$$(p \equiv q) \Leftrightarrow$$

$$[(p \supset q) \wedge (q \supset p)] \Leftrightarrow$$

$$[(\neg p \vee q) \wedge (\neg q \vee p)] \Leftrightarrow$$

$$[(p \wedge q) \vee (\neg p \wedge \neg q)] \Leftrightarrow$$

....

Normální formy formulí výrokové logiky

$$\begin{aligned}(p \equiv q) &\Leftrightarrow [(p \supset q) \wedge (q \supset p)] \Leftrightarrow \\ &[(\neg p \vee q) \wedge (\neg q \vee p)] \Leftrightarrow \\ &[(p \wedge q) \vee (\neg p \wedge \neg q)] \Leftrightarrow \dots\end{aligned}$$

● Je užitečné stanovit nějaký **normální tvar** formule – tj. vybrat mezi těmito nekonečně mnoha ekvivalentními formulemi jeden nebo dva *kanonické normální tvary*. **Třída ekvivalentních formulí je pak reprezentována** touto vybranou formulí v normálním tvaru.

● V našem příkladu jsou v normálním tvaru formule na druhém a třetím řádku.

Normální formy formulí výrokové logiky

Literál je výrokový symbol nebo jeho negace. Př.: $p, \neg q, r, \dots$

Elementární konjunkce (EK) je konjunkce literálů. Př.: $p \wedge \neg q, r \wedge \neg r, \dots$

Elementární disjunkce (ED) je disjunkce literálů. Př.: $p \vee \neg q, r \vee \neg r, \dots$

Úplná elementární konjunkce (ÚEK) dané množiny výrokových symbolů je elementární konjunkce, ve které se každý symbol z dané množiny vyskytuje **právě jednou** (budto prostě nebo negovaný):

Př.: $p \wedge \neg q$

Úplná elementární disjunkce (ÚED) dané množiny výrokových symbolů je elementární disjunkce, ve které se každý symbol z dané množiny vyskytuje **právě jednou** (budto prostě nebo negovaný).

Př.: $p \vee \neg q$

Disjunktivní normální forma (DNF) dané formule je formule ekvivalentní s danou formulí a mající tvar disjunkce elementárních konjunktí. *Příklad:* $DNF(p \equiv p): (p \wedge p) \vee (\neg p \wedge \neg p), p \vee \neg p$

Konjunktivní normální forma (KNF) dané formule je formule ekvivalentní s danou formulí a mající tvar konjunkce elementárních disjunktí. *Příklad:* $KNF(p \equiv p): (\neg p \vee p) \wedge (\neg p \vee p)$

Úplná disjunktivní normální forma (UDNF) dané formule je formule ekvivalentní s danou formulí a mající tvar disjunkce úplných elementárních konjunktí. *Příklad:* $UDNF(p \equiv q): (p \wedge q) \vee (\neg p \wedge \neg q)$

Úplná konjunktivní normální forma (UKNF) dané formule je formule ekvivalentní s danou formulí a mající tvar konjunkce úplných elementárních disjunktí. *Příklad:* $UKNF(p \equiv q): (\neg p \vee q) \wedge (\neg q \vee p)$

ÚDNF a UKNF dané formule nazýváme **kanonickými (standardním) tvary** této formule.

Normální formy formulí výrokové logiky

Jak nalézt kanonický tvar (tj. UDNF, UKNF) formule?

- **UDNF**: disjunkce = 1, když alespoň jedna $UEK = 1$, tj. všechny literály v této $UEK = 1$.
- **UKNF**: konjunkce = 0, když alespoň jedna $UED = 0$, tj. všechny literály v této $UED = 0$.

Proto: UDNF (UKNF) sestojíme z pravdivostní funkce tak, že si všímáme řádků, kde je hodnota 1 (0) a „zajišťujeme správnou hodnotu literálů“ – 1 (0).

Nalezení UDNF, UKNF - tabulkou

Nalézt UDNF, UKNF formule: $\neg(p \supset q)$

p	q	$\neg(p \supset q)$	UEK	UED
1	1	0		$\neg p \vee \neg q$
1	0	1	$p \wedge \neg q$	
0	1	0		$p \vee \neg q$
0	0	0		$p \vee q$

UDNF: $p \wedge \neg q$

UKNF: $(\neg p \vee \neg q) \wedge (p \vee \neg q) \wedge (p \vee q)$

Nalezení UDNF, UKNF - úpravami

Metoda ekvivalentních úprav:

$$\begin{aligned} \neg(p \supset q) &\Leftrightarrow \neg(\neg p \vee q) \Leftrightarrow (p \wedge \neg q) \text{ UDNF} \Leftrightarrow \\ [p \vee (q \wedge \neg q)] \wedge [\neg q \vee (p \wedge \neg p)] &\Leftrightarrow \\ \Leftrightarrow (p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q) &\text{ UKNF} \end{aligned}$$

Pozn.: Využíváme zde **tautologie výrokové logiky**, viz předchozí prezentace.

Ve druhém řádku využíváme toho, že disjunkce libovolné formule A s kontradikcí (F) je ekvivalentní A : $A \vee F \Leftrightarrow A$

Ve třetím řádku jsou použity distributivní zákony.

*Každá formule, která není kontradikce, má UDNF a
Každá formule, která není tautologie, má UKNF*

Opačná úloha: k UDNF, UKNF nalézt jednodušší „původní“ formuli

- Alchymista je zavřen ve vězení a dostane 5 motáků s výroky:
 - p : Podaří se ti přeměna olova ve zlato
 - q : 1.4. bude tvůj švagr jmenován prokurátorem
 - r : Po 1.4. bude soud.

První moták zní: $p \wedge q \wedge r$

Druhý moták zní: $p \wedge q \wedge \neg r$

Třetí moták zní: $\neg p \wedge \neg q \wedge r$

Čtvrtý moták zní: $\neg p \wedge \neg q \wedge \neg r$

Pátý moták zní: Alespoň jeden z předchozích motáků je pravdivý.

- Otázka:** Co se vlastně nebohý alchymista dověděl?
- Řešení:** $(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$.
Máme tedy nalézt formuli, k níž je tato UDNF ekvivalentní. Za pomoci distributivních zákonů dostaneme:
$$(p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r) \Leftrightarrow$$
$$(p \wedge q) \wedge (r \vee \neg r) \vee (\neg p \wedge \neg q) \wedge (r \vee \neg r) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q) \Leftrightarrow (p \equiv q)$$
- Odpověď:** Podaří se ti přeměna olova ve zlato tehdy a jen tehdy, když bude 1.4. tvůj švagr jmenován prokurátorem.

Otázka: kolik binárních pravdivostních funkcí
(a tedy logických spojek) existuje?

p	q	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
			$\wedge$						$\vee$	$\downarrow$	$\equiv$				$\supset$	$\uparrow$	

NO
R

NAND

Kolik nejméně a které spojky potřebujeme?

- Dle věty o normálních tvarech stačí: $\neg, \vee, \wedge$
(**funkcionálně úplná soustava**)

- Ostatní vytvoříme skládáním funkcí

Následující soustavy pravdivostních funkcí jsou funkcionálně úplné:

1. pravdivostní funkce příslušející spojkám $\{\neg, \wedge, \vee\}$,
2. pravdivostní funkce příslušející spojkám $\{\neg, \wedge\}$ nebo $\{\neg, \vee\}$,
3. pravdivostní funkce příslušející spojkám $\{\neg, \supset\}$,
4. pravdivostní funkce příslušející spojce $\{\uparrow\}$ nebo $\{\downarrow\}$.

Tedy k vyjádření libovolné pravdivostní funkce, tj. libovolné formule ekvivalentním způsobem stačí jedna spojka!

Bud' Schefferova **NAND** $\uparrow$ nebo Pierceova **NOR** $\downarrow$.

Kolik nejméně a které spojky potřebujeme?

- Soustava $\{\neg, \wedge, \vee\}$ stačí dle vět o normálních formách.
- Převod na soustavu $\{\neg, \wedge\}$ nebo $\{\neg, \vee\}$:

$$\begin{aligned} A \wedge B &\Leftrightarrow \neg(\neg A \vee \neg B), \\ A \vee B &\Leftrightarrow \neg(\neg A \wedge \neg B) \end{aligned}$$

- Převod na soustavu $\{\neg, \supset\}$:

$$\begin{aligned} A \vee B &\Leftrightarrow \neg A \supset B, \\ A \wedge B &\Leftrightarrow \neg(A \supset \neg B) \end{aligned}$$

- Převod na soustavu $\{\uparrow\}$ nebo $\{\downarrow\}$:

$$\begin{aligned} \neg A &\Leftrightarrow A \uparrow A, \quad A \wedge B \Leftrightarrow (A \uparrow B) \uparrow (A \uparrow B), \quad \text{kde } \uparrow \text{ značí NAND,} \\ \neg A &\Leftrightarrow A \downarrow A, \quad A \vee B \Leftrightarrow (A \downarrow B) \downarrow (A \downarrow B), \quad \text{kde } \downarrow \text{ značí NOR.} \end{aligned}$$

Sémantická tabla: metoda tvorby DNF, KNF

- Disjunktivní tablo: strom jehož listy jsou konjunkce literálů.
- Konjunktivní tablo: strom jehož listy jsou disjunkce literálů.
- $\models A$ (tautologie) $\Rightarrow$ všechny listy **konjunktivního** *tabla* musí být uzavřené, tj. obsahovat opačný pár literálů: $p, \neg p$: **$(p \vee \neg p)$ – tautologie**
- $A \not\models$ (kontradikce) $\Rightarrow$ všechny listy **disjunktivního** *tabla* musí být uzavřené, tj. obsahovat opačný pár literálů: $p, \neg p$: **$(p \wedge \neg p)$ – kontradikce**

Postup tvorby sémantického tabla

1. Formuli upravíme tak, aby negace byla všude „uvnitř“, tj. u jednotlivých proměnných (tedy provedeme ekvivalentní negace).
2. Tam, kde je nějaká podformule ve tvaru implikace nebo ekvivalence, převedeme na disjunkci resp. konjunkci s využitím logických zákonů:

$$(p \equiv q) \Leftrightarrow (p \supset q) \wedge (q \supset p) \Leftrightarrow (\neg p \vee q) \wedge (\neg q \vee p) \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q)$$

3. Konstruujeme tablo uplatňováním distributivního zákona.

Disjunktivní normální forma

- Větvení znamená disjunkci, čárka znamená konjunkci.
- Postupujeme zleva a jakmile narazíme na disjunkci, rozvětvíme. Levý disjunkt do levé větve + zbytek formule oddělený čárkami, pravý disjunkt do pravé větve + zbytek.
- Větvíme tak dlouho, až žádná podformule neobsahuje disjunkci a strom má v listech pouze seznamy literálů oddělené čárkami, které značí *elementární konjunkce*.

Konjunktivní normální forma: duální k disjunktivní

- Větvení znamená konjunkci, čárka znamená disjunkci.
- Postupujeme zleva a jakmile narazíme na konjunkci, rozvětvíme. Levý konjunkt do levé větve + zbytek formule oddělený čárkami, pravý do pravé + zbytek.
- Větvíme tak dlouho, až není nikde konjunkce a strom má v listech pouze seznamy literálů oddělené čárkami, které značí *elementární disjunkce*.

Důkaz, že formule je

a) tautologie, b) kontradikce

a) **Důkaz**, že formule **F** je kontradikce:

Zkonstruujeme **disjunktivní tablo**. Pokud se všechny větve uzavřely, tj. každý list sémantického stromu tvoří elementární konjunkce s dvojicí literálů s opačným znaménkem (např. $p, \neg p$, což znamená $p \wedge \neg p$), je formule **F** kontradikce.

a) **Důkaz**, že formule **F** je tautologie:

Zkonstruujeme **konjunktivní tablo**. Pokud se všechny větve uzavřely, tj. každý list sémantického stromu tvoří elementární disjunkce s dvojicí literálů s opačným znaménkem (např. $p, \neg p$, což znamená $p \vee \neg p$), je formule **F** tautologie.

Důkaz, co vyplývá z dané formule

- Disjunktivní sémantické tablo, které se neuzavřelo, doplníme takovou formulí (konjunkcí literálů), aby se *všechny* větve uzavřely.
- *Negace* toho, co jsme doplnili, vyplývá. Např. doplníme-li p , $\neg q$, pak jsme doplnili $p \wedge \neg q$, tedy vyplývá $\neg p \vee q$, tj. $p \supset q$.
- Duálním způsobem můžeme použít konjunktivní normální formu.

Úplné normální formy.

- Z tabla se dá snadno zdůvodnit, proč tautologie nemá úplnou konjunktivní normální formu (UKNF) a proč kontradikce nemá úplnou disjunktivní normální formu (UDNF):
- Je-li formule tautologie, pak se všechny větve konjunktivního tabla uzavřou, tj. v každé ED je dvojice literálů s opačným znaménkem ($p, \neg p$), resp. $p \vee \neg p$, což je vyloučeno v UED. Tedy neexistuje UKNF.
- Analogicky pro UDNF.

UDNF tautologie

o jedné (T1), dvou (T2) a třech (T3)
proměnných

$$T1: \quad p \vee \neg p$$

$$T2: \quad (p \wedge q) \vee (p \wedge \neg q) \vee (\neg p \wedge q) \vee (\neg p \wedge \neg q)$$

$$T3: \quad (p \wedge q \wedge r) \vee (p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee \\ (p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (\neg p \wedge q \wedge \neg r) \vee \\ (\neg p \wedge \neg q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$$

V každé možné valuaci musí být alespoň jedna
UEK pravdivá.

UDNF tautologie

Není-li formule tautologie, pak musí v UDNF nějaká z těchto UEK chybět.

Proto, konstruujeme-li **UDNF z tabulky**, vyjdeme z těch řádků pravdivostní funkce, ve kterých je **hodnota = 1** (hodnoty nepravda v disjunkci nehrají roli, neboť $A \vee F \Leftrightarrow A$) a konstruujeme UEK tak, aby byla při této valuaci pravdivá.

Zcela analogicky pro **UKNF - vyjdeme z 0.**

Dokažte, že formule F je
tautologie:

$$F: [(p \supset (q \vee r)) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r)] \supset (p \supset (s \vee t))$$

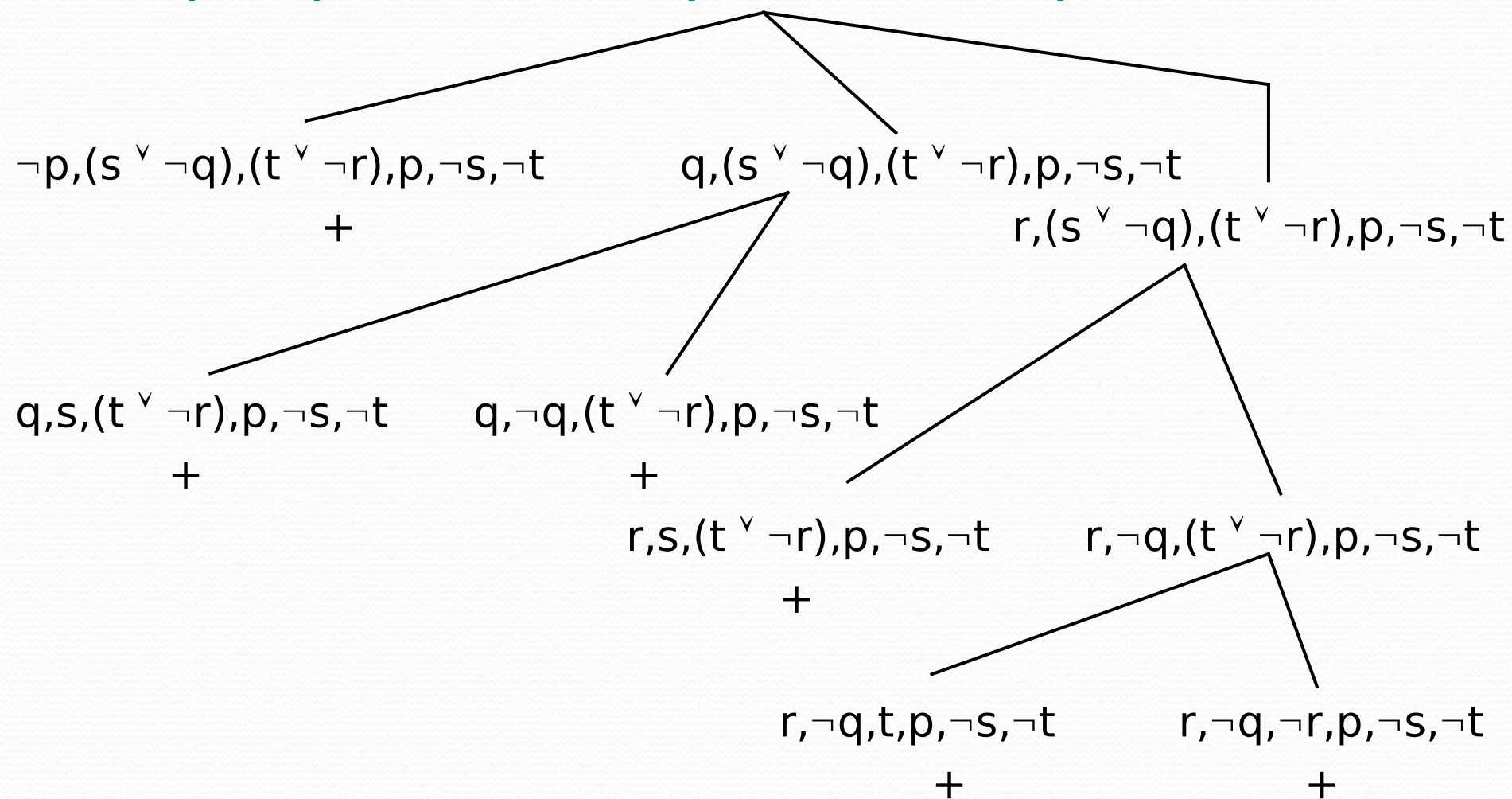
Nepřímý důkaz (sporem). Pomocí **disjunktivní** normální formy dokážeme, že formule $\neg F$ je **kontradikce**:

$$(p \supset (q \vee r)) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r) \wedge p \wedge \neg s \wedge \neg t \Leftrightarrow \\ (\neg p \vee q \vee r) \wedge (s \vee \neg q) \wedge (t \vee \neg r) \wedge p \wedge \neg s \wedge \neg t$$

Konstrukce disjunktivního tabla (větvení – disjunkce, čárka – konjunkce):

DokaŹte, Źe formule F je

tautologie:



Co vyplývá z formule G ?

G: $(p \supset (q \vee r)) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r)$

Řešení: Kdybychom udělali sémantické tablo formule G, pak ve všech listech předchozího sémantického stromu budou chybět literály $p, \neg s, \neg t$.

Doplníme-li je tedy do všech větví, všechny větve se uzavřou. Tedy formule $(G \wedge p \wedge \neg s \wedge \neg t)$ je kontradikce.

Proto: $\models G \supset \neg(p \wedge \neg s \wedge \neg t)$.

Tedy: $G \models \neg(p \wedge \neg s \wedge \neg t),$
 $G \models (\neg p \vee s \vee t),$
 $G \models (p \supset (s \vee t))$

Není divu, vždyť formule F (sl. 22) je tautologie !

Dokažte, že formule F je tautologie:

$$F: [(p \supset (q \vee r)) \wedge (\neg s \supset \neg q) \wedge (t \vee \neg r)] \supset (p \supset (s \vee t))$$

Přímý důkaz: Pomocí **konjunktivní** normální formy dokážeme, že formule F je **tautologie**:

Větvení – konjunkce, čárka – disjunkce.

$$F \Leftrightarrow (p \wedge \neg q \wedge \neg r) \vee (\neg s \wedge q) \vee (\neg t \wedge r) \vee \neg p \vee s \vee t$$

Atd., analogicky (duálně) k nepřímému důkazu disjunktivní normální formou.

Rezoluční metoda ve výrokové logice

- Sémantické tablo není výhodné z praktických důvodů.
- Chceme-li dokázat, že $P_1, \dots, P_n \models Z$, stačí dokázat, že $\models (P_1 \wedge \dots \wedge P_n) \supset Z$, tj. $P_1 \wedge \dots \wedge P_n \wedge \neg Z$ je kontradikce.
- Ale, pro důkaz sémantickým tablem potřebujeme formuli v **disjunktivní** normální formě. To znamená, že musíme převádět tuto formuli, která je téměř v konjunktivní formě, za použití distributivního zákona do disjunktivní formy.
- Použití sémantického tabla vede často k mnoha distributivním krokům.
- Jednodušší prakticky bude dokázat přímo spornost, tj. **nesplnitelnost**, formule $P_1 \wedge \dots \wedge P_n \wedge \neg Z$.

Rezoluční pravidlo dokazování ve výrokové logice

Nechť I je literál. Z formule $(A \vee I) \wedge (B \vee \neg I)$ odvod' $(A \vee B)$. Zapisujeme:

$$\frac{(A \vee I) \wedge (B \vee \neg I)}{(A \vee B)}$$

Toto pravidlo není přechodem **ekvivalentní** formulí, ale zachovává **splnitelnost**.

Důkaz: Nechť je formule $(A \vee I) \wedge (B \vee \neg I)$ splnitelná, tedy pravdivá při nějaké valuaci v . Pak při této valuaci musí být pravdivé oba disjunktivy (tzv. **klausule**):

$$(A \vee I) \text{ a } (B \vee \neg I).$$

Nechť je dále $v(I) = 0$. Pak $w(A) = 1$ a tedy $w(A \vee B) = 1$.

Nechť je naopak $v(I) = 1$. Pak $w(\neg I) = 0$ a musí být $w(B) = 1$, a tedy $w(A \vee B) = 1$.

V obou případech je tedy formule $A \vee B$ **pravdivá v modelu v** původní formule, a tedy **splnitelná**.

Rezoluční pravidlo dokazování ve výrokové logice

Uvědomme si, že důkaz byl proveden pro jakýkoli model, tj. valuaci v .

Jinými slovy platí, že pravidlo ***zachovává také pravdivost***:

$$(A \vee I) \wedge (B \vee \neg I) \models (A \vee B).$$

To nám poskytuje návod, jak řešit úlohu, **co vyplývá z** dané formule, resp. množiny formulí.

Navíc, platí že ***konjunktivní rozšíření*** formule o ***rezolventu*** $(A \vee B)$ nemění pravdivostní funkci formule:

$$(A \vee I) \wedge (B \vee \neg I) \Leftrightarrow (A \vee I) \wedge (B \vee \neg I) \wedge (A \vee B)$$

Klauzulární forma

- Konjunktivní normální forma formule se v rezoluční metodě nazývá **klauzulární forma**. Jednotlivé konjunktivy (tj. elementární disjunkce) se nazývají **klauzule**.
- Příklad: *Převod formule do klauzulární formy:*

$$\begin{aligned} & \neg [((p \supset q) \wedge (r \vee \neg q) \wedge \neg r) \supset \neg p] \Leftrightarrow \\ & ((p \supset q) \wedge (r \vee \neg q) \wedge \neg r) \wedge p \Leftrightarrow \\ & (\neg p \vee q) \wedge (r \vee \neg q) \wedge \neg r \wedge p \end{aligned}$$

- Formule má čtyři klauzule.

Důkaz, že je to kontradikce provedeme tak, že postupně přidáváme rezolventy, až dojdeme ke sporné klauzuli ($\neg p \wedge p$), značíme:

- $(\neg p \vee q) \wedge (r \vee \neg q) \wedge (\neg p \vee r) \wedge \neg r \wedge \neg p \wedge p$

Důkazy rezoluční metodou

- $R(F)$ - **konjunktivní rozšíření** formule F o všechny rezolventy.
- $R_0(F) = F$, $R_i(F) = R(R_{i-1}(F))$ - **rezoluční uzávěr** formule F . Platí, že $R_i(F) \Leftrightarrow F$
- Důkaz, že **A je kontradikce** (nesplnitelná): existuje n takové, že $R_n(A)$ obsahuje prázdnou klausuli:
- Důkaz, že **A je tautologie**: $\neg A$ je kontradikce.
- Důkaz, že **množina formulí $\{A_1, \dots, A_n\}$ je nesplnitelná**: dokážeme, že $A_1 \wedge \dots \wedge A_n$ je kontradikce. formule
- Odvodit, co vyplývá z $\{A_1, \dots, A_n\}$ znamená odvodit všechny rezolventy.
- Důkaz správnosti úsudku $A_1, \dots, A_n \models Z$
 - **Přímý**: postupným vytvářením rezolvent odvodíme, že z $A_1, \dots, A_n$ vyplývá Z
 - **Nepřímý**: dokážeme, že $A_1 \wedge \dots \wedge A_n \supset Z$ je tautologie, neboli $A_1 \wedge \dots \wedge A_n \wedge \neg Z$ je kontradikce, neboli množina $\{A_1, \dots, A_n, \neg Z\}$ je nesplnitelná.

Příklady, postup

- Jednotlivé klausule napíšeme pod sebe a odvozujeme rezolventy (které vyplývají). Při nepřímém důkazu se snažíme dojít k prázdné klauzuli.
- Důkaz nesplnitelnosti formule:

$$(\neg q \supset p) \wedge (p \vee r) \wedge (q \supset \neg r) \wedge \neg p$$

1. $q \vee p$
2. $p \vee r$
3. $\neg q \vee \neg r$
4. $\neg p$
5. $p \vee \neg r$ rezoluce 1, 3
6. p rezoluce 2, 5
7. $\blacksquare$ spor 4, 6

Dotaz: Co vyplývá z formule $(\neg q \supset p) \wedge (p \vee r) \wedge (q \supset \neg r)$?
Formule **p**.

Příklady, postup

- **Přímý** důkaz platnosti úsudku:

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \models p \supset (s \vee t)$$

$$1. \quad \neg p \vee q \vee r$$

$$2. \quad s \vee \neg q$$

$$3. \quad t \vee \neg r$$

$$\square. \quad \neg p \vee s \vee r$$

$$\square. \quad \neg p \vee s \vee t$$

$$\square. \quad \neg p \vee s \vee t \Leftrightarrow p \supset (s \vee t)$$

rezoluce 1, 2

rezoluce 3, 4

Q.E.D.

Příklady

- **Nepřímý** důkaz platnosti úsudku:

$$p \supset q \vee r, \neg s \supset \neg q, t \vee \neg r \vdash p \supset (s \vee t)$$

$$\square \quad \neg p \vee q \vee r$$

$$\square \quad s \vee \neg q$$

$$\square \quad t \vee \neg r$$

$$\square \quad \neg p \vee s \vee r \quad \text{rezoluce 1, 2}$$

$$\square \quad \neg p \vee s \vee t \quad \text{rezoluce 3, 4}$$

$$\square \quad p \quad \text{Negovaný}$$

$$\square \quad \neg s \quad \text{Závěr}$$

$$\square \quad \neg t \quad (\text{řádky 6.,7.,8.})$$

$$\square \quad \neg p \vee s \vee t, p, \neg s, \neg t \vdash s \vee t, \neg s, \neg t \vdash t, \neg t \vdash \square \vdash$$

Logické programování

- Strategie generování rezolvent.
- Rezoluční uzávěr – generujeme **všechny** rezolventy – strategie generování do **šířky**
 - Může být implementačně neefektivní – kombinatorická exploze rezolvent
- Proto v logickém programování se používá strategie generování **do hloubky**: není úplná – může uvíznout v nekonečné větvi, i když řešení existuje.

Příklad neúplnosti strategie **do hloubky**

$$d \wedge e \wedge (b \supset a) \wedge (e \supset b) \wedge (d \supset a) \not\models a (?)$$

- Logický program (strategie do hloubky, řízená cílem):

□D. *fakt*
□E. *fakt*
□A :- B. *pravidlo (A pokud B)*
□B :- E. *pravidlo (B pokud E)*
□A :- D. *pravidlo (A pokud D)*
□?A *dotaz, cíl*

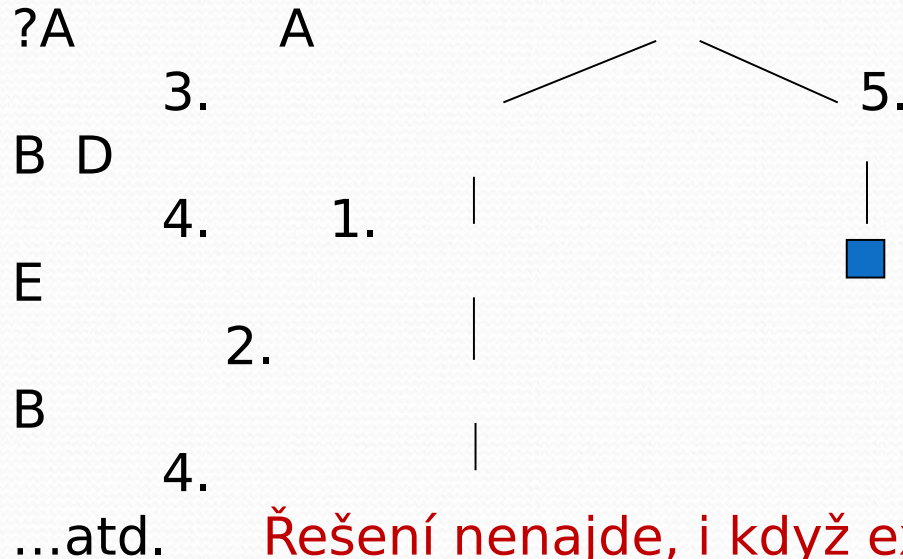
- snaží se splnit cíl A, prohledává program **shora dolů** a hledá klauzuli s A vlevo - najde klauzuli 3. - generuje nový cíl B - najde klauzuli 4. - nový cíl E - je splněn klauzulí 2. - **ANO.**

- **nebo** generuje **proces navracení: znovu ?A** - klauzule 5 - cíl D - klauzule 1. - **ANO.**

Příklad neúplnosti strategie *do hloubky, zleva*

Malá úprava programu:

1. D.
2. E :- B.
3. A :- B.
4. B :- E.
5. A :- D.
6. ?A



Opakování výroková logika

- Nejdůležitější pojmy a metody výrokové logiky.

Tabulka pravdivostních funkcí

A	B	$\neg A$	$A \vee B$	$A \wedge B$	$A \supset B$	$A \equiv B$
1	1	0	1	1	1	1
1	0	0	1	0	0	0
0	1	1	1	0	1	0
0	0	1	0	0	1	1

Pozor na implikaci $p \supset q$. Je nepravdivá pouze v jednom případě: $p = 1, q = 0$. Je to jako slib:

„Budeš-li hodný, dostaneš lyže“ ($p \supset q$). „Byl jsem hodný, ale lyže jsem nedostal“. ($p \wedge \neg q$) Byl slib splněn?

Kdyby nebyl hodný ($p = 0$), pak slib k ničemu nezavazuje.

Shrnutí

- Typické úlohy:
 - Ověření *platnosti úsudku*.
 - *Co vyplývá* z daných předpokladů ?
 - Doplňte chybějící předpoklady tak, aby *úsudek* byl *platný*.
 - Je daná formule *tautologie, kontradikce, splnitelná* ?
 - Najděte *modely* formule, najděte *model množiny* formulí.
- Umíme zatím řešit:
 - Tabulkovou metodou.
 - Úvahou a ekvivalentními úpravami.
 - Sporem, nepřímým důkazem – sémanticky.
 - Rezoluční metodou.
 - Sémantickým tablem.

Příklad: Důkaz tautologie

$$\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r)$$

Tabulkou:

A

p	q	r	$(p \supset q)$	$(\neg p \supset r)$	A	$(\neg q \supset r)$	$A \supset (\neg q \supset r)$
1	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	0	0	0	1

Důkaz tautologie - sporem

$$\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r)$$

Formule **A je tautologie**, právě když negovaná formule $\neg A$ je **kontradikce**:

$$\models A, \text{ právě když } \neg A \models$$

- Předpokládáme tedy, že negovaná formule může být pravdivá.
- **Negace implikace:** $\neg(A \supset B) \Leftrightarrow (A \wedge \neg B)$
- $(p \supset q) \wedge (\neg p \supset r) \wedge \neg q \wedge \neg r$

 $q = 0, r = 0, \text{ tedy } p \supset 0, \neg p$
 $\text{proto: } p = 0, \neg p = 0, \text{ tj. } p = 1$

spor

- negovaná formule nemá model, je to kontradikce, tedy původní formule je tautologie.

Důkaz tautologie - úpravami

Potřebné zákony:

- $(A \supset B) \Leftrightarrow (\neg A \vee B) \Leftrightarrow (\neg(A \wedge \neg B))$
- $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$ de Morgan
- $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$ de Morgan
- $\neg(A \supset B) \Leftrightarrow (A \wedge \neg B)$ negace implikace
- $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$ distributivní zákony
- $(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$ distributivní zákony
- $1 \vee A \Leftrightarrow 1$ $1 \Leftrightarrow$ tautologie, např. $(p \vee \neg p)$
- $1 \wedge A \Leftrightarrow A$
- $0 \wedge A \Leftrightarrow 0$ $0 \Leftrightarrow$ kontradikce, např. $(p \wedge \neg p)$
- $0 \vee A \Leftrightarrow A$

Důkaz tautologie - úpravami

$$\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r)$$

$$[(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r) \Leftrightarrow$$

$$\neg[(p \supset q) \wedge (\neg p \supset r)] \vee (\neg q \supset r) \Leftrightarrow$$

$$(p \wedge \neg q) \vee (\neg p \wedge \neg r) \vee q \vee r \Leftrightarrow$$

$$[p \vee (\neg p \wedge \neg r) \vee q \vee r] \wedge [\neg q \vee (\neg p \wedge \neg r) \vee q \vee r] \Leftrightarrow$$

$$(p \vee \neg p \vee q \vee r) \wedge (p \vee \neg r \vee q \vee r) \wedge (\neg q \vee \neg p \vee q \vee r) \wedge (\neg q \vee \neg r \vee q \vee r)$$

$$\Leftrightarrow 1 \wedge 1 \wedge 1 \wedge 1 \Leftrightarrow 1 - \text{tautologie}$$

Pozn.: Obdrželi jsme *konjunktivní normální formu*,
KNF.

Důkaz tautologie – rezoluční metodou

$$\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r)$$

Negovanou formuli převedeme do klauzulární formy (KNF), důkaz sporem:

$$(p \supset q) \wedge (\neg p \supset r) \wedge \neg q \wedge \neg r \Leftrightarrow (\neg p \vee q) \wedge (p \vee r) \wedge \neg q \wedge \neg r$$

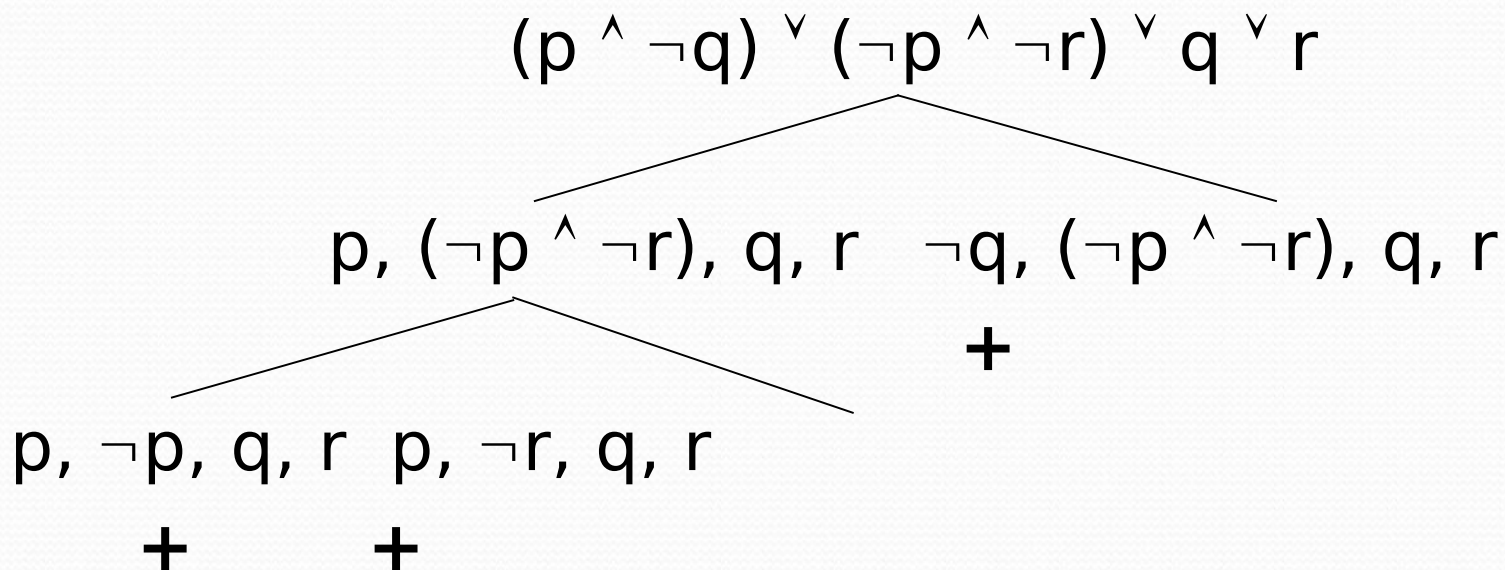
1. $\neg p \vee q$
2. $p \vee r$
3. $\neg q$
4. $\neg r$
5. $q \vee r$ rezoluce 1, 2
6. r rezoluce 3, 5
7. $\blacksquare$ rezoluce 4, 6 – spor

Důkaz tautologie – sémantickým tablem

$$\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r)$$

Přímý důkaz: sestrojíme KNF

(‘^’: větvení, ‘v’: , - ve všech větvích 1: ‘p v ¬p’)

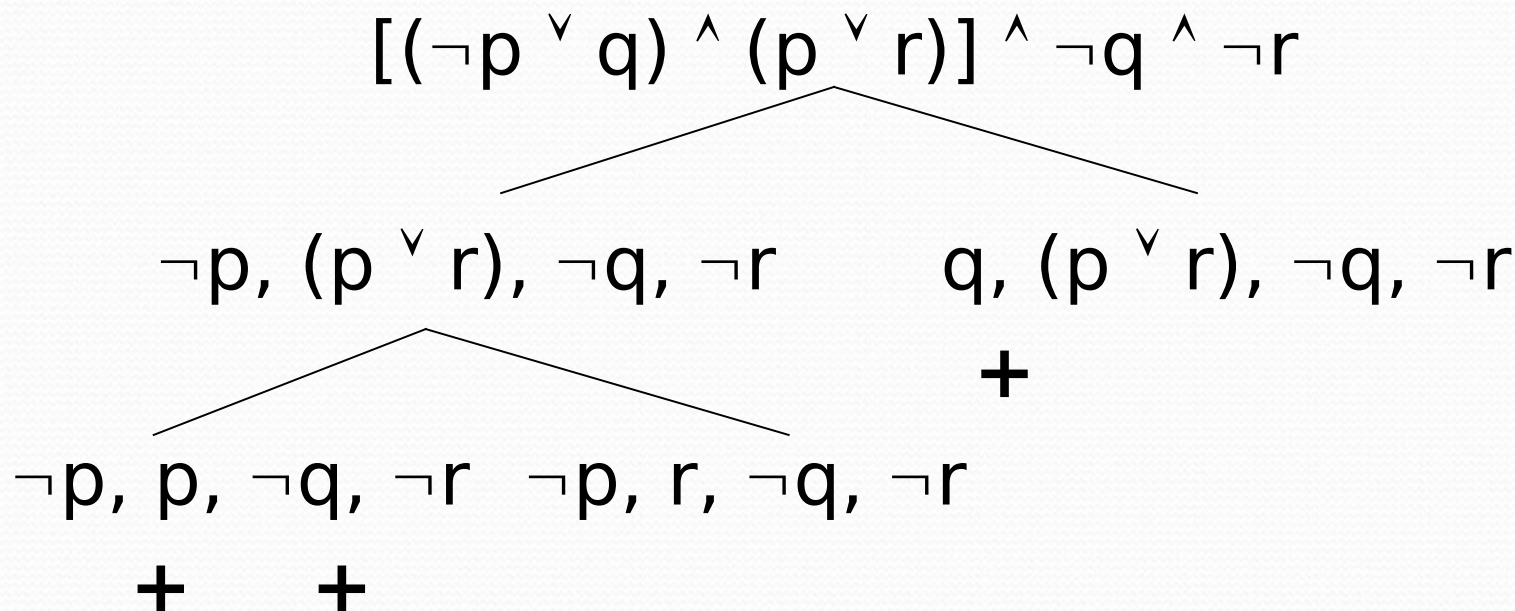


Důkaz tautologie – sémantickým tablem

$$\models [(\mathbf{p} \supset \mathbf{q}) \wedge (\neg \mathbf{p} \supset \mathbf{r})] \supset (\neg \mathbf{q} \supset \mathbf{r})$$

Nepřímý důkaz: sestrojíme DNF *negované* formule.

(‘ $\vee$ ’: větvení, ‘ $\wedge$ ’: , - a ve všech větvích 0: ‘ $p \wedge \neg p$ ’)



Důkaz platnosti úsudku

$$\begin{aligned} &\models [(p \supset q) \wedge (\neg p \supset r)] \supset (\neg q \supset r) \quad \text{iff} \\ &[(p \supset q) \wedge (\neg p \supset r)] \models (\neg q \supset r) \text{ iff} \\ &(p \supset q), (\neg p \supset r) \models (\neg q \supset r) \end{aligned}$$

p : Program funguje.

q : Systém je v pořádku.

r : Je nutno volat systémového inženýra.

Funguje-li program, je systém v pořádku.

Nefunguje-li program, je nutno volat syst. Inženýra

—————
Není-li systém v pořádku, je nutno volat syst. inženýra.

Důkaz platnosti úsudku

$$(p \supset q), (\neg p \supset r) \models (\neg q \supset r)$$

Nepřímý důkaz:

- musí být sporná množina formulí $\{(p \supset q), (\neg p \supset r), (\neg q \wedge \neg r)\}$

1. $\neg p \vee q$

2. $p \vee r$

3. $\neg q$

4. $\neg r$

5. $q \vee r$ rezoluce 1, 2

6. r rezoluce 3, 5

7. rezoluce 4, 6, spor

Důkaz platnosti úsudku

$$(p \supset q), (\neg p \supset r) \models (\neg q \supset r)$$

Přímý důkaz: Co vyplývá z předpokladů?

Pravidlo rezoluce zachovává pravdivost:

$$\begin{array}{ccc} \neg p \vee q & , & p \vee r \\ 1 & & 1 \end{array} \vdash \begin{array}{c} q \vee r \\ 1 \end{array}$$

V libovolné valuaci v , jsou-li pravdivé předpoklady, je pravdivá i rezolventa.

Důkaz:

$$\text{a) } p = 1 \Rightarrow \neg p = 0 \Rightarrow q = 1 \Rightarrow (q \vee r) = 1$$

$$\text{b) } p = 0 \Rightarrow r = 1 \Rightarrow (q \vee r) = 1$$

$$\begin{array}{l} \square \quad \neg p \vee q \\ \square \quad p \vee r \\ \square \quad q \vee r \end{array}$$

rezoluce 1, 2 - důsledek: $(q \vee r) \Leftrightarrow (\neg q \supset r)$