

Úvod do TI - logika

Relace, zobrazení, spočetnost a nespočetnost množin,
opakování VL
(5. přednáška)

Marie Duží

marie.duzi@vsb.cz



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Intermezzo: Relace

- **Relace** mezi množinami A , B je podmnožina Kartézského součinu $A \times B$.
- **Kartézský součin** $A \times B$ je množina všech uspořádaných dvojic $\langle a, b \rangle$, kde $a \in A$, $b \in B$.
- (Binární) **relace** R^2 na množině M je podmnožina Kartézského součinu $M \times M$: $R^2 \subseteq M \times M$.
- **n -ární relace** R_n na množině M : $R_n \subseteq M \times \dots \times M$
 n -krát

Intermezzo: Relace

Pozor:

Dvojice $\langle a, b \rangle \neq \langle b, a \rangle$, ale množina $\{a, b\} = \{b, a\}$

$\langle a, a \rangle \neq \langle a \rangle$, ale $\{a, a\} = \{a\}$

U *n-tic* záleží na pořadí, prvky se mohou opakovat, na rozdíl od množin.

Notace: $\langle a, b \rangle \in R$ značíme také prefixně $R(a, b)$, nebo infixně $a R b$. Např. $1 \leq 3$.

Relace - příklad

Binární relace na $\mathbb{N}$: $<$ (ostře menší):

$\{\langle 0,1 \rangle, \langle 0,2 \rangle, \langle 0,3 \rangle, \dots, \langle 1,2 \rangle, \langle 1,3 \rangle, \langle 1,4 \rangle, \dots, \langle 2,3 \rangle, \langle 2,4 \rangle, \dots, \langle 3,4 \rangle, \dots, \langle 5,7 \rangle, \dots, \langle 115,119 \rangle, \dots\}$

Ternární relace na $\mathbb{N}$: množina trojic přirozených čísel takových, že 3. číslo je rozdíl 1. číslo minus 2. číslo:

$\{\langle 0,0,0 \rangle, \langle 1,0,1 \rangle, \langle 1,1,0 \rangle, \dots, \langle 2,0,2 \rangle, \langle 2,1,1 \rangle, \langle 2,2,0 \rangle, \dots, \langle 3,0,3 \rangle, \langle 3,1,2 \rangle, \langle 3,2,1 \rangle, \langle 3,3,0 \rangle, \dots, \langle 115,110,5 \rangle, \dots\}$

Relace „adresa osoby“:

$\{\langle \text{Jan Novák, Praha 5, Bellušova 1831} \rangle, \langle \text{Marie Duží, Praha 5, Bellušova 1827} \rangle, \dots, \}$

Intermezzo: Funkce (zobrazení)

n -ární funkce F na množině M je speciální zprava jednoznačná $(n+1)$ -ární relace $F \subseteq M \times \dots \times M$:

$$(n+1) \times \forall \underline{a} \forall b \forall c ([F(\underline{a}, b) \wedge F(\underline{a}, c)] \supset b = c).$$

Parciální F : ke každé n -tici prvků $\underline{a} \in M \times \dots \times M$ existuje **nanejvýš jeden** prvek $b \in M$.
Značíme $F: M \times \dots \times M \rightarrow M$, místo $F(\underline{a}, b)$ píšeme $F(\underline{a}) = b$.

Množinu $M \times \dots \times M$ nazýváme **definiční obor (doména)** funkce F , množinu M pak **obor hodnot (range)**.

Intermezzo: Funkce (zobrazení)

Příklad: Relace na $\mathbb{N}$:

$\{\langle\langle 1,1 \rangle, 1 \rangle, \langle\langle 2,1 \rangle, 2 \rangle, \langle\langle 2,2 \rangle, 1 \rangle, \dots, \langle\langle 4,2 \rangle, 2 \rangle, \dots, \langle\langle 9,3 \rangle, 3 \rangle, \dots, \langle\langle 27,9 \rangle, 3 \rangle, \dots\}$

je parciální funkce **dělení** beze zbytku.

Také relace *minus na $\mathbb{N}$* (viz předchozí slide) je na $\mathbb{N}$ parciální funkcí: např. dvojice $\langle 2,4 \rangle$ nemá v $\mathbb{N}$ obraz. Aby byla totální, museli bychom rozšířit její definiční obor na celá čísla.

Intermezzo: Funkce (zobrazení)

Jako interpretace funkčních symbolů formulí PL1 používáme pouze *totální* funkce:

Totální funkce $F: A \rightarrow B$:

Ke každému prvku $a \in A$ existuje ***právě jeden*** prvek $b \in B$ takový, že:

$$F(a)=b: \forall a \exists b F(a)=b \wedge \forall a \forall b \forall c [(F(a)=b \wedge F(a)=c) \supset b=c]$$

Zavádíme někdy **speciální kvantifikátor $\exists!$** s významem „existuje právě jedno“ a píšeme:

$$\forall a \exists! b F(a)=b$$

Intermezzo: Funkce (zobrazení)

Příklady:

Relace $+$ $\{ \langle 0,0,0 \rangle, \langle 1,0,1 \rangle, \langle 1,1,2 \rangle, \langle 0,1,1 \rangle, \dots \}$ je na $\mathbb{N}$ **(totální binární) funkce**. Každým dvěma číslům přiřadí **právě jedno**, jejich součet.

Místo $\langle 1,1,2 \rangle \in +$ píšeme $1+1=2$

Relace $\geq$ není funkce: $\exists x \exists y \exists z [(x \geq y) \wedge (x \geq z) \wedge (y \neq z)]$

Relace $\{ \langle 0,0 \rangle, \langle 1,1 \rangle, \langle 2,4 \rangle, \langle 3,9 \rangle, \langle 4,16 \rangle, \dots \}$ je na $\mathbb{N}$ **totální funkce druhá mocnina** (x^2).

Surjekce, injekce, bijekce

- Zobrazení $f : A \rightarrow B$ je **surjekce** (zobrazení *A na B*), jestliže k libovolnému $b \in B$ existuje $a \in A$ takový, že $f(a)=b$.

$$\forall b [B(b) \supset \exists a (A(a) \wedge f(a)=b)].$$

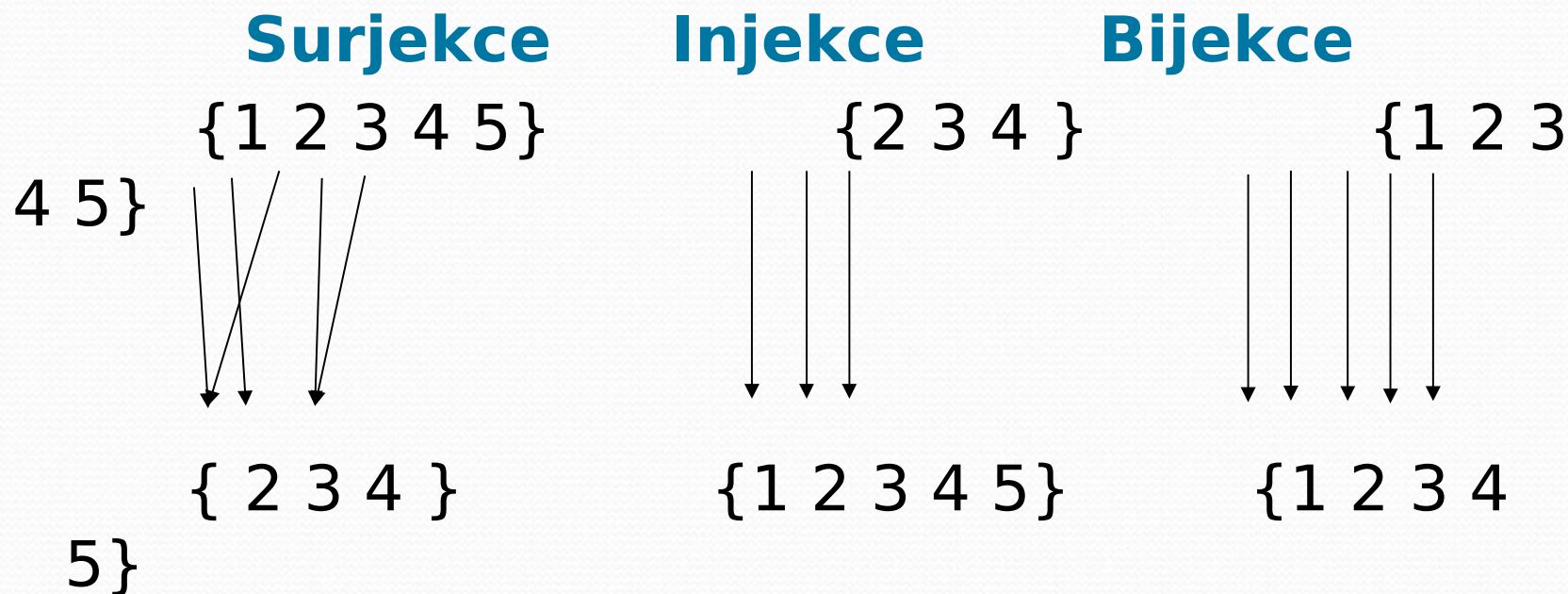
- Zobrazení $f : A \rightarrow B$ je **injekce** (*prosté zobrazení A do B*), jestliže pro všechna $a \in A$, $b \in A$ taková, že $a \neq b$ platí, že $f(a) \neq f(b)$.

$$\forall a \forall b [(A(b) \wedge A(a) \wedge (a \neq b)) \supset (f(a) \neq f(b))].$$

- Zobrazení $f : A \rightarrow B$ je **bijekce** (*prosté zobrazení A na B*), jestliže f je surjekce a injekce

Funkce (zobrazení)

- *Příklad:*



Existuje-li mezi množinami A , B bijekce, pak říkáme, že mají stejnou *kardinalitu* (počet prvků).

Kardinalita, spočetné množiny

- Množina A , která má stejnou kardinalitu jako množina N přirozených čísel, se nazývá **spočetná**.
- Příklad: množina sudých čísel S je spočetná. Prosté zobrazení f množiny S na N je dáno například předpisem:

$$f(n) = 2n.$$

Tedy $0 \rightarrow 0, 1 \rightarrow 2, 2 \rightarrow 4, 3 \rightarrow 6, 4 \rightarrow 8, \dots$

Jeden z **paradoxů Cantorovy teorie** množin:

$S \subset N$ (vlastní podmnožina) a přitom počet prvků obou množin je stejný:

$$\text{Card}(S) = \text{Card}(N)!$$

Kardinalita, spočetné množiny

Množina racionálních čísel R je rovněž spočetná.

Důkaz: Provedeme ve dvou krocích.

- a) **$\text{Card}(N) \leq \text{Card}(R)$** ,
neboť každé přirozené číslo je racionální: $N \subseteq R$.
- b) Sestrojíme **zobrazení N na R** (tedy surjekci N na R), čímž dokážeme, že **$\text{Card}(R) \leq \text{Card}(N)$** :

1	2	3	4	5	6	...
1/1	2/1	1/2	3/1	2/2	1/3	...

1/1	1/2	1/3	1/4	1/5	1/6	...
2/1	2/2	2/3	2/4	2/5	2/6	...
3/1	3/2	3/3	3/4	3/5	3/6	...
4/1	4/2	4/3	4/4	4/5	4/6	...
5/1	5/2	5/3	5/4	5/5	5/6	...
6/1	6/2	6/3	6/4	6/5	6/6	...
...	...	...	...	...	...	...

Ale v tabulce se nám racionální čísla opakují, tedy toto zobrazení není prosté. Nicméně, žádné racionální číslo nevynecháme, je to zobrazení **na R (surjekce)**.

Kardinalita, nespočetné množiny

- Existují však **nespočetné** množiny: nejmenší z nich je **množina reálných čísel $\mathbb{R}$** .
- Již v intervalu $\langle 0,1 \rangle$ je reálných čísel více než je všech přirozených, ale stejně mnoho jako všech $\mathbb{R}$!
- **Cantorův diagonální důkaz:** Kdyby bylo v tomto intervalu čísel $\mathbb{R}$ spočetně mnoho, pak by šly uspořádat do posloupnosti první (1.), druhé (2.), třetí (3.),..., a každé z nich je tvaru $0,i_1i_2i_3\dots$, kde $i_1i_2i_3\dots$ je desetinný rozvoj čísla.
- Racionální čísla mají desetinný rozvoj konečný, iracionální čísla jej mají nekonečný.
- V posloupnosti desetinných míst $i_1i_2i_3\dots$ přičteme ke každému n -tému číslu i_n v jeho rozvoji číslo 1_{i_n} . Dostaneme čísla, která v původní uspořádané

Cantorův diagonální důkaz nespočetnosti reálných čísel v intervalu $\langle 0,1 \rangle$.

	1	2	3	4	5	6	7
1	i_{11}	i_{12}	i_{13}	i_{14}	i_{15}	i_{16}	i_{17}
2	i_{21}	i_{22}	i_{23}	i_{24}	i_{25}	i_{26}	i_{27}
3	i_{31}	i_{32}	i_{33}	i_{34}	i_{35}	i_{36}	i_{37}
4	i_{41}	i_{42}	i_{43}	i_{44}	i_{45}	i_{46}	i_{47}
5	i_{51}	i_{52}	i_{53}	i_{54}	i_{55}	i_{56}	i_{57}

....

Nové číslo, které v tabulce není:

$$0, i_{11}+1 \ i_{22}+1 \ i_{33}+1 \ i_{44}+1 \ i_{55}+1 \ ...$$

Opakování: výroková logika

- Příští týden se koná zápočtová písemka:
- maximálně 15 bodů, minimálně 5 bodů
- Nebude opravný termín !

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:** $\neg(A \supset B) \Leftrightarrow (A \wedge \neg B)$

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

$$\begin{array}{ccccccc} & 1 & & 1 & 10 & 10 & q = 0, r = 0, \text{ tedy } p \supset 0, \neg p \supset 0 \\ \swarrow & & \downarrow & & & & \\ 0 & 0 & 0 & 0 & & & \text{proto: } p = 0, \neg p = 0, \text{ tj. } p = 1 \\ & 1 & & & & & \end{array}$$

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. ■ rezoluce 4, 6 – spor

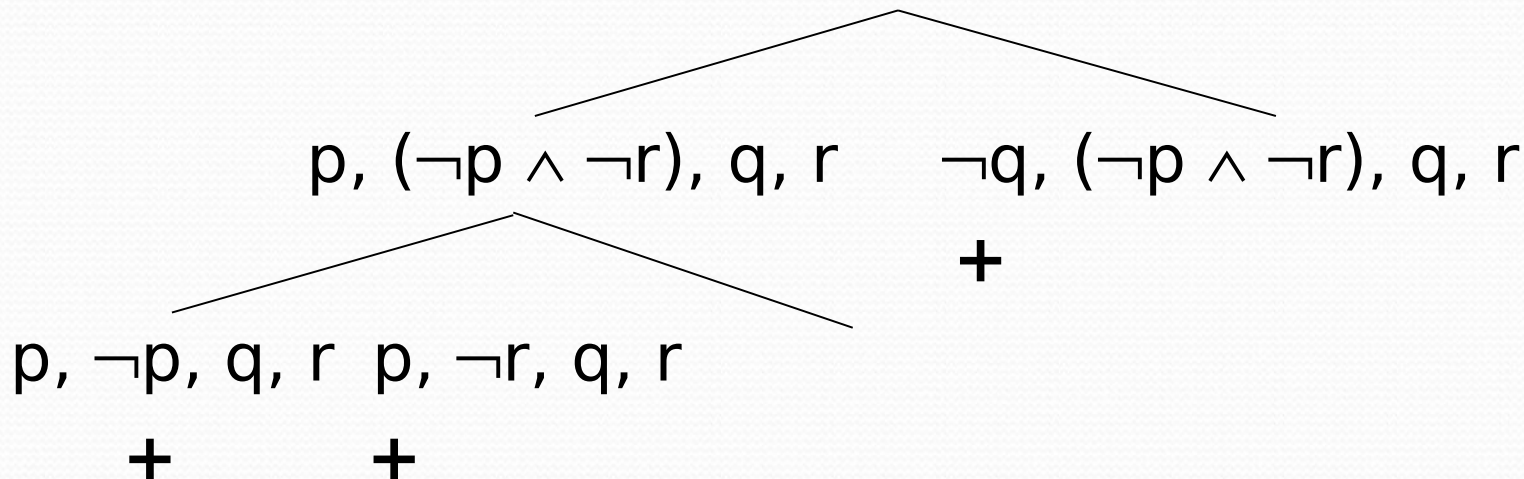
Důkaz tautologie – sémantickým tablem

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

Přímý důkaz: sestrojíme KNF

(‘ $\wedge$ ’: větvení, ‘ $\vee$ ’: , - ve všech větvích 1: ‘ $p \vee \neg p$ ’)

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

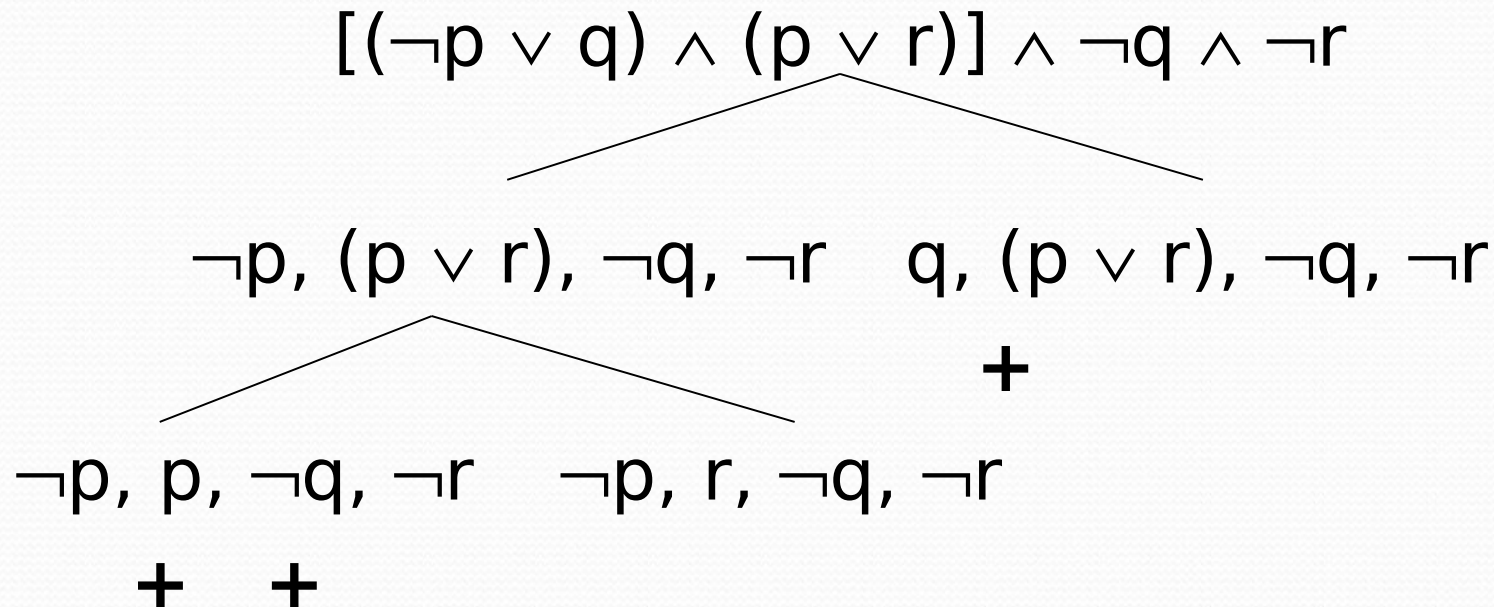


Důkaz tautologie – sémantickým tablem

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

Nepřímý důkaz: sestrojíme DNF *negované* formule.

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



Důkaz platnosti úsudku

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

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

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

Přímý důkaz: Co vyplývá z předpokladů?

Pravidlo rezoluce zachovává pravdivost:

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

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

Důkaz:

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

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

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

$$2. \quad p \vee r$$

$$3. \quad q \vee r \quad \text{rezoluce 1, 2 - důsledek: } (q \vee r) \Leftrightarrow (\neg q \supset r)$$