Logikai algoritmusok

Mihálydeák Tamás

Számítógéptudományi Tanszék

March 10, 2019

Definíció

Klasszikus nulladrendű nyelven az

$$L^{(0)} = \langle LC, Con, Form \rangle$$

rendezett hármast értjük, ahol

1. $LC = \{\neg, \supset, \wedge, \vee, \equiv, (,)\}$ *(a nyelv logikai konstansainak halmaza).*
2. $Con \neq \emptyset$ *a nyelv nemlogikai konstansainak (állítás- vagy kijelentés-paramétereinek) legfeljebb megszámlálhatóan végtelen halmaza.*
3. *Az* $LC \cap Con = \emptyset$
4. *A nyelv formuláinak a halmazát, azaz a Form halmazt az alábbi induktív definíció adja meg:*

Definíció

- $Con \subseteq Form$
- *Ha* $A \in Form$*, akkor* $\neg A \in Form$.
- *Ha* $A, B \in Form$*, akkor*
  - $(A \supset B) \in Form$,
  - $(A \wedge B) \in Form$,
  - $(A \vee B) \in Form$,
  - $(A \equiv B) \in Form$.

Megjegyzés

A Con halmaz elemeit atomi formuláknak vagy prímformuláknak nevezzük.

Definíció

- *Ha A atomi formula, akkor nincs közvetlen részformulája;*
- *$\neg A$ egyetlen közvetlen részfomulája A;*
- *Az $(A \supset B), (A \wedge B), (A \vee B), (A \equiv B)$ formulák közvetlen részformulái az A és a B formulák.*

Definíció

Egy A formula részformuláinak halmaza az a legszűkebb halmaz [jelölés: $RF(A)$], amelyre teljesül, hogy

1. *$A \in RF(A)$,*
   (azaz az A formula részformulája önmagának);
2. *ha $A' \in RF(A)$ és B közvetlen részformulája A'-nek, akkor $B \in RF(A)$*
   (azaz, ha egy A' formula részformulája A-nak, akkor A' összes közvetlen részformulája is részformulája A-nak).

Definíció

Az A formula szerkezeti fáján egy olyan véges rendezett fát értünk, amelynek csúcsai formulák,

- *gyökere az A formula,*
- *$\neg B$ alakú csúcsának egyetlen gyermeke a B formula,*
- *$(B \supset C), (B \wedge C), (B \vee C), (B \equiv C)$ alakú csúcsainak két gyermekét a B, illetve a C formulák alkotják,*
- *levelei prímformulák (atomi formulák).*

Definíció

A ϱ függvényt az $L^{(0)}$ nyelv egy *interpretációjának nevezzük, ha*

1. $Dom(\varrho) = Con$
2. *Ha* $p \in Con$, *akkor* $\varrho(p) \in \{0, 1\}$.

Definíció

Legyen adott egy ϱ interpretáció. $|A|_\varrho$ jelöli az A formula ϱ interpretáció szerinti értékét.

1. *Ha* $p \in Con$, *akkor* $|p|_\varrho = \varrho(p)$
2. *Ha* $A \in Form$, *akkor* $|\neg A|_\varrho = 1 - |A|_\varrho$.
3. *Ha* $A, B \in Form$, *akkor*
   - $|(A \supset B)|_\varrho = \begin{cases} 0 & ha\ |A|_\varrho = 1,\ és\ |B|_\varrho = 0; \\ 1, & egyébként. \end{cases}$
   - $|(A \wedge B)|_\varrho = \begin{cases} 1 & ha\ |A|_\varrho = 1,\ és\ |B|_\varrho = 1; \\ 0, & egyébként. \end{cases}$
   - $|(A \vee B)|_\varrho = \begin{cases} 0 & ha\ |A|_\varrho = 0,\ és\ |B|_\varrho = 0; \\ 1, & egyébként. \end{cases}$
   - $|(A \equiv B)|_\varrho = \begin{cases} 1 & ha\ |A|_\varrho = |B|_\varrho; \\ 0, & egyébként. \end{cases}$

Definíció

Legyen $\Gamma \subseteq Form$ egy tetszőleges formulahalmaz! A ϱ interpretáció modellje a Γ formulahalmaznak, ha minden $A \in \Gamma$ esetén $|A|_\varrho = 1$

Definíció

Az A formula modelljén az $\{A\}$ egyelemű formulahalmaz modelljét értjük.

Definíció

Egy $\Gamma \subseteq Form$ fomulahalmaz kielégíthető, ha van modellje.
(Van olyan interpretáció, amelyben a formulahalmaz minden eleme igaz.)

Definíció

Egy $A \in Form$ formula kielégíthető, ha az $\{A\}$ formulahalmaz kielégíthető.

Megjegyzés

- *Kielégíthető formulahalmaz: nem tartalmaz logikai ellentmondást, azaz a formulahalmaz elemei lehetnek egyszerre igazak.*
- *Kielégíthető formula: a formula lehet igaz, azaz nem logikai hamisság.*
- *Ha egy formulahalmaz kielégíthető, akkor minden eleme kielégíthető.*
- *Az előző állítás megfordítása nem igaz. Pl.: a $\{p, \neg p\}$ formulahalmaz minden eleme kielégíthető, de maga a formulahalmaz nem kielégíthető.*

Tétel

Egy kielégíthető formulahalmaz minden részhalmaza kielégíthető. (A logikai ellentmondástalanság szűkítéssel nem rontható el.)

Proof.

- Legyen $\Gamma \subseteq Form$ egy tetszőleges kielégíthető formulahalmaz, és $\Delta \subseteq \Gamma$!
- Γ kielégíthetősége miatt a Γ formulahalmaznak van modellje, legyen Γ egy modellje a ϱ interpretáció.
- ϱ tulajdonsága: Ha $A \in \Gamma$, akkor $|A|_\varrho = 1$
- Mivel $\Delta \subseteq \Gamma$, ha $A \in \Delta$, akkor $A \in \Gamma$, s így $|A|_\varrho = 1$. Azaz a ϱ interpretáció modellje Δ-nak, tehát Δ kielégíthető.

$\square$

Definíció

Kielégíthetetlenség: Egy $\Gamma \subseteq Form$ formulahalmaz kielégíthetetlen, ha nem kielégíthető (ha nincs modellje).

Definíció

Egy $A \in Form$ formula kielégíthetetlen, ha az $\{A\}$ formulahalmaz kielégíthetetlen.

Megjegyzés

Kielégíthetetlen formulahalmaz: logikai ellentmondást tartalmaz, azaz a formulahalmaz elemei nem lehetnek egyszerre igazak.

Tétel

Egy kielégíthetetlen formulahalmaz minden bővítése kielégíthetetlen. (A logikai ellentmondás bővítéssel nem szüntethető meg.)

Proof.

- Indirekt bizonyítás:
- Tegyük fel, hogy $\Gamma \subseteq Form$ tetszőleges kielégíthetetlen formulahalmaz, $\Delta \subseteq Form$ pedig tetszőleges formulahalmaz.
- Indirekt feltétel: Γ kielégíthetetlen, és $\Gamma \cup \Delta$ kielégíthető.
- $\Gamma \subseteq \Gamma \cup \Delta$
- Az előző állítás miatt Γ kielégíthető, ez pedig ellentmondás.

$\square$

Definíció

A Γ formulahalmaznak logikai következménye *az A formula, ha a $\Gamma \cup \{\neg A\}$ formulahalmaz kielégíthetetlen. Jelölés: $(\Gamma \vDash A)$*

Definíció

$A \vDash B$, ha $\{A\} \vDash B$.

Definíció

Az A formula érvényes*, ha $\emptyset \vDash A$. Jelölés: $\vDash A$*

Definíció

Az A és a B formula logikailag ekvivalens*, ha $A \vDash B$ és $B \vDash A$. Jelölés: $A \Leftrightarrow B$*

Tétel

Legyen $\Gamma \subseteq Form$, és $A \in Form$. $\Gamma \models A$ akkor és csak akkor, ha a Γ formulahalmaz minden modellje modellje az a A formulának (azaz az $\{A\}$ egyelemű formulahalmaznak) is.

Proof.

$\rightarrow$ Indirekt feltétel: $\Gamma \models A$ és van olyan modellje a Γ formulahalmaznak, amely nem modellje az A formulának.
Legyen ez a modell a ϱ interpretáció!
A ϱ tulajdonságai:

1. minden $B \in \Gamma$ esetén $|B|_\varrho = 1$;
2. $|A|_\varrho = 0$, azaz $|\neg A|_\varrho = 1$

Ekkor a $\Gamma \cup \{\neg A\}$ formulahalmaz minden eleme igaz ϱ-ban, tehát $\Gamma \cup \{\neg A\}$ kielégíthető, azaz $\Gamma \not\models A$, ami ellentmondás.

$\square$

Proof.

$\leftarrow$ Indirekt feltétel: A Γ formulahalmaz minden modellje modellje az A formulának, de $\Gamma \not\models A$.
Ekkor a $\Gamma \cup \{\neg A\}$ formulahalmaz kielégíthető, azaz van modellje.
Legyen ez a modell a ϱ interpretáció!
A ϱ tulajdonságai:

1. minden $B \in \Gamma$ esetén $|B|_\varrho = 1$;
2. $|\neg A|_\varrho = 1$, azaz $|A|_\varrho = 0$

Tehát a Γ formulahalmaznak van olyan modellje, ami nem modellje az A formulának, s ez ellentmondás. $\square$

Corollary

Legyen $\Gamma \subseteq Form$, és $A \in Form$. $\Gamma \models A$ akkor és csak akkor, ha minden olyan interpretációban, amelyben a Γ formulahalmaz minden eleme igaz, igaz az A formula is.

Tétel

Ha A érvényes formula ($\vDash A$), akkor minden Γ formulahalmaz esetén $\Gamma \vDash A$. (Egy érvényes formula minden formulahalmaznak következménye.)

Proof.

- Ha A érvényes formula, akkor a definíció szerint $\emptyset \vDash A$.
- $\emptyset \cup \{\neg A\}$ $(= \{\neg A\})$ kielégíthetetlen, s így bővítései is kielégíthetetlenek.
- $\Gamma \cup \{\neg A\}$ bővítése $\{\neg A\}$-nak, így kielégíthetetlen, tehát $\Gamma \vDash A$.

$\square$

Tétel

Ha a Γ formulahalmaz kielégíthetetlen, akkor minden A formula esetén $\Gamma \vDash A$. (Egy kielégíthetetlen formulahalmaznak minden formula következménye.)

Proof.

- A már bizonyított állítás szerint: Ha a Γ formulahalmaz kielégíthetetlen, akkor Γ minden bővítése is kielégíthetetlen.
- $\Gamma \cup \{\neg A\}$ bővítése Γ-nak, így kielégíthetetlen, tehát $\Gamma \vDash A$.

$\square$

Tétel

Dedukció tétel: Ha $\Gamma \cup \{A\} \vDash B$, akkor $\Gamma \vDash (A \supset B)$.

Proof.

- Indirekt feltétel: Tegyük fel, hogy $\Gamma \cup \{A\} \vDash B$, és $\Gamma \nvDash (A \supset B)$.
- Így $\Gamma \cup \{\neg(A \supset B)\}$ kielégíthető, tehát van modellje. Legyen egy modellje a ϱ interpretáció!
- A ϱ tulajdonságai:
  1. Γ minden eleme igaz a ϱ interpretáció szerint.
  2. $|\neg(A \supset B)|_\varrho = 1$
- $|(A \supset B)|_\varrho = 0$, azaz $|A|_\varrho = 1$ és $|B|_\varrho = 0$. Így $|\neg B|_\varrho = 1$.
- $\Gamma \cup \{A\} \cup \{\neg B\}$ formulahalmaz minden eleme igaz a ϱ interpretáció szerint, tehát $\Gamma \cup \{A\} \nvDash B$, ami ellentmondás.

□

A klasszikus nulladrendű logika | Centrális logikai (szemantikai) fogalmak

Tétel

A dedukció tétel megfordítása: Ha $\Gamma \vDash (A \supset B)$, akkor $\Gamma \cup \{A\} \vDash B$.

Proof.

- Indirekt feltétel: Tegyük fel, hogy $\Gamma \vDash (A \supset B)$, és $\Gamma \cup \{A\} \nvDash B$.
- Így $\Gamma \cup \{A\} \cup \{\neg B\}$ kielégíthető, tehát van modellje. Legyen egy modellje a ϱ interpretáció!
- A ϱ tulajdonságai:
  1. Γ minden eleme igaz a ϱ interpretáció szerint.
  2. $|A|_\varrho = 1$
  3. $|\neg B|_\varrho = 1$, így $|B|_\varrho = 0$
- $|(A \supset B)|_\varrho = 0$, $|\neg(A \supset B)|_\varrho = 1$.
- $\Gamma \cup \{\neg(A \supset B)\}$ formulahalmaz minden eleme igaz a ϱ interpretáció szerint, tehát $\Gamma \nvDash (A \supset B)$.

□

Corollary

$A \vDash B$ akkor és csak akkor, ha $\vDash (A \supset B)$

Proof.

Bizonyítás: Az előző két tételben legyen $\Gamma = \emptyset$. $\square$

Tétel

Metszet tétel: Ha $\Gamma \cup \{A\} \vDash B$ és $\Delta \vDash A$, akkor $\Gamma \cup \Delta \vDash B$.

Proof.

Indirekt. $\square$

Az negáció igazságtáblázata:

$\neg$	$\neg p$
0	1
1	0

- A kettős negáció törvénye: $\neg\neg A \Leftrightarrow A$

A konjunkció igazságtáblázata:

$\wedge$	0	1	(q)
0	0	0	
1	0	1	
(p)			

- Felcserélhető (kommutatív): $(A \wedge B) \Leftrightarrow (B \wedge A)$ bármely $A, B \in Form$ esetén.
- Csoportosítható (asszociatív): $(A \wedge (B \wedge C)) \Leftrightarrow ((A \wedge B) \wedge C)$ bármely $A, B, C \in Form$ esetén.
- Idempotens: $(A \wedge A) \Leftrightarrow A$ bármely $A \in Form$ esetén.

- $(A \wedge B) \vDash A$, $(A \wedge B) \vDash B$
- Az ellentmondás törvénye: $\vDash \neg(A \wedge \neg A)$
- Az $\{A_1, A_2, \ldots, A_n\}$ formulahalmaz ($A_1, A_2, \ldots, A_n \in Form$) akkor és csak akkor kielégíthető, ha az $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ formula kielégíthető.
- Az $\{A_1, A_2, \ldots, A_n\}$ formulahalmaz ($A_1, A_2, \ldots, A_n \in Form$) akkor és csak akkor kielégíthetetlen, ha az $A_1 \wedge A_2 \wedge \cdots \wedge A_n$ formula kielégíthetetlen.
- Az $\{A_1, A_2, \ldots, A_n\} \vDash A$ ($A_1, A_2, \ldots, A_n, A \in Form$) akkor és csak akkor, ha az $A_1 \wedge A_2 \wedge \cdots \wedge A_n \vDash A$.
- Az $\{A_1, A_2, \ldots, A_n\} \vDash A$ ($A_1, A_2, \ldots, A_n, A \in Form$) akkor és csak akkor, ha az $((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \wedge \neg A)$ formula kielégíthetetlen.

Az diszjunkció igazságtáblázata:

$\vee$	0	1
0	0	1
1	1	1

- Felcserélhető (kommutatív): $(A \vee B) \Leftrightarrow (B \vee A)$ bármely $A, B \in Form$ esetén.
- Csoportosítható (asszociatív): $(A \vee (B \vee C)) \Leftrightarrow ((A \vee B) \vee C)$ bármely $A, B, C \in Form$ esetén.
- Idempotens: $(A \vee A) \Leftrightarrow A$ bármely $A \in Form$ esetén.
- $A \vDash (A \vee B)$ bármely $A, B \in Form$ esetén.
- $\{(A \vee B), \neg A\} \vDash B$
- A kizárt harmadik törvénye. $\vDash (A \vee \neg A)$

- A konjunkció és az diszjunkció kapcsolata:

$\wedge$	0	1
0	0	0
1	0	1

	1	0
1	1	1
0	1	0

$\vee$	0	1
0	0	1
1	1	1

- A fenti tulajdonság azt jelenti, hogy a konjunkció és a diszjunkció egymás duálisai.

- Kétoldali disztributivitás:
  - $(A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \vee C))$
  - $(A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C))$

- Elnyelési tulajdonság
  - $(A \wedge (B \vee A)) \Leftrightarrow A$
  - $(A \vee (B \wedge A)) \Leftrightarrow A$

De Morgan törvények

- Mit állítunk akkor, amikor egy konjunkciót tagadunk?
- Mit állítunk akkor amikor egy diszjunkció tagadunk?
- $\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$
- $\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$

- A De Morgan törvények bizonyítása.

A	B	$\neg A$	$\neg B$	$(\neg A \wedge \neg B)$	$(A \vee B)$	$\neg(A \vee B)$
0	0	1	1	1	0	1
0	1	1	0	0	1	0
1	0	0	1	0	1	0
1	1	0	0	0	1	0

- Az implikáció igazságtáblázata:

$\supset$	0	1
0	1	1
1	0	1

- $\models (A \supset A)$
- Modus ponens (leválasztási szabály): $\{(A \supset B), A\} \models B$
- Modus tollens (indirekt cáfolás sémája): $\{(A \supset B), \neg B\} \models \neg A$
- Láncszabály: $\{(A \supset B), (B \supset C)\} \models (A \supset C)$
- Redukció ad abszurdum: $\{(A \supset B), (A \supset \neg B)\} \models \neg A$

- $\neg A \models (A \supset B)$
- $B \models (A \supset B)$
- Áthelyezési törvény: $((A \wedge B) \supset C) \Leftrightarrow (A \supset (B \supset C))$
- Kontrapozíció: $(A \supset B) \Leftrightarrow (\neg B \supset \neg A)$
- $(A \supset \neg A) \models \neg A$
- $(\neg A \supset A) \models A$
- $(A \supset (B \supset C)) \Leftrightarrow ((A \supset B) \supset (A \supset C))$
- $\models (A \supset (\neg A \supset B))$
- $((A \vee B) \supset C) \Leftrightarrow ((A \supset C) \wedge (B \supset C))$
- Az $\{A_1, A_2, \ldots, A_n\} \models A$ $(A_1, A_2, \ldots, A_n, A \in Form)$ akkor és csak akkor, ha az $((A_1 \wedge A_2 \wedge \cdots \wedge A_n) \supset A)$ formula érvényes.

- Az ekvivalencia igazságtáblázata:

$\equiv$	0	1
0	1	0
1	0	1

- $\models (A \equiv A)$
- $\models \neg(A \equiv \neg A)$

Kifejezhetőség

- $(A \supset B) \Leftrightarrow \neg(A \wedge \neg B)$
- $(A \supset B) \Leftrightarrow (\neg A \vee B)$
- $(A \wedge B) \Leftrightarrow \neg(A \supset \neg B)$
- $(A \vee B) \Leftrightarrow (\neg A \supset B)$
- $(A \vee B) \Leftrightarrow \neg(\neg A \wedge \neg B)$
- $(A \wedge B) \Leftrightarrow \neg(\neg A \vee \neg B)$
- $(A \equiv B) \Leftrightarrow ((A \supset B) \wedge (B \supset A))$

Az igazságfunktorok elmélete

- A bázis fogalma: Igazságfunktorok egy olyan halmazát értjük bázison, amelynek elemeivel minden igazságfunktor kifejezhető.
  - Például: $\{\neg, \supset\}$,$\{\neg, \wedge\}$,
  - $\{\neg, \supset\}$:
    1. $(p \wedge q) \Leftrightarrow \neg(p \supset \neg q)$
    2. $(p \vee q) \Leftrightarrow (\neg p \supset q)$
  - Sheffer művelet: $(p|q) \Leftrightarrow_{def} \neg(p \wedge q)$
  - Sem–sem művelet: $(p \parallel q) \Leftrightarrow_{def} (\neg p \wedge \neg q)$
  - Megjegyzés: Mind a Sheffer, mind a sem–sem művelet önmagában bázist alkot.

Definíció

Ha $p \in Con$, akkor a $p, \neg p$ formulákat literálnak nevezzük (p a literál alapja).

Definíció

Ha az A formula literál vagy különböző alapú literálok konjunkciója, akkor A-t elemi konjunkciónak nevezzük.

Definíció

Ha az A formula literál vagy különböző alapú literálok diszjunkciója, akkor A-t elemi diszjunkciónak (vagy klóznak) nevezzük.

Definíció

Elemi konjunkciók diszjunkcióját diszjunktív normálformának nevezzük.

Definíció

Elemi diszjunkciók konjunkcióját konjunktív normálformának nevezzük.

Proposition

Az állításlogika minden formulájához létezik vele logikailag ekvivalens normálforma.

- A konvenciók célja az egyértelmű olvashatóság fenntartása mellett a formulákban előforduló zárójelek számának a csökkentése.
- A létrejött jelsorozatok betű szerint nem formulák, de egyértelműen előállítható belőlük egy formula.
- A továbbiakban az egyszerűség kedvéért az így létrejött jelsorozatokat is formuláknak nevezzük, s használatukkor mindig a belőlük egyértelműen előállítható formulákra gondolunk.

- A legkülső zárójelpár mindig elhagyható.
- A kétargumentumú logikai konstansok elsőbbségi sorrendje:

$$\wedge, \vee, \supset, \equiv$$

- A negáció erősebb bármely kétargumentumú logikai konstansnál.

- Az azonos kétargumentumú logikai konstansok egymás közötti elsőbbségét a balról jobbra szabály rendezi: először mindig a bal oldali formulát tekintjük külön műveleti komponensnek.

Megjegyzés

- *A szabálynak csak az implikációnál van jelentősége:*
  - *az $A \supset B \supset C$ "formula" egyértelműen zárójelezett alakja:*
    $(A \supset (B \supset C))$;
- *A konjunkció és a diszjunkció esetében a műveltek asszociativitása miatt a szabályt nem követő zárójelezések is logikailag ekvivalens formulát eredményeznek. Pl.: az $A \wedge B \wedge C$ "formula" egyértelműen zárójelezett alakja:* $(A \wedge (B \wedge C))[\Leftrightarrow ((A \wedge B) \wedge C)]$.

Problémafelvetés

- Egy formula kielégíthetőségének eldöntése meghatározó szerepet játszik:
  - Véges formulahalmaz $\rightarrow$ formula;
  - Véges premisszás következtetés $\rightarrow$ formula

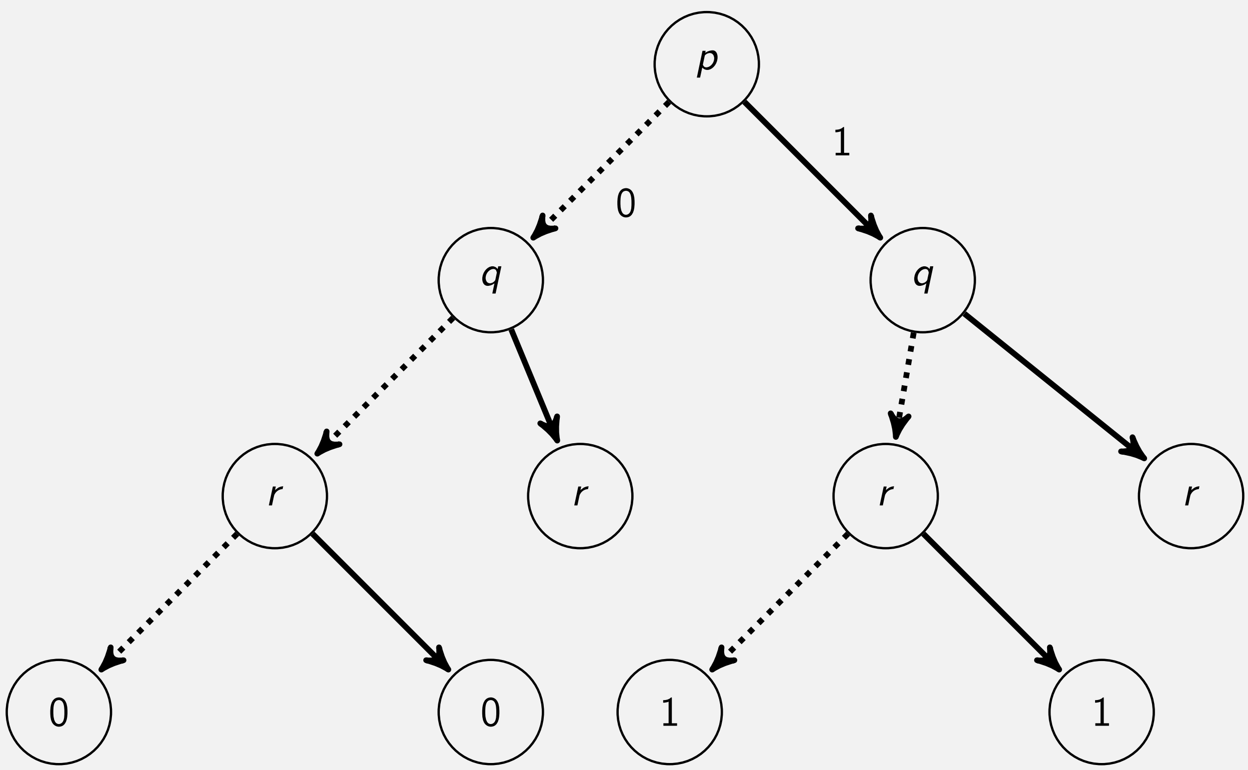
Igazságtáblák

	p	q	r	$p \vee (q \wedge r)$
1.	1	1	1	1
2.	1	1	0	1
3.	1	0	1	1
4.	1	0	0	1
5.	0	1	1	1
6.	0	1	0	0
7.	0	0	1	0
8.	0	0	0	0

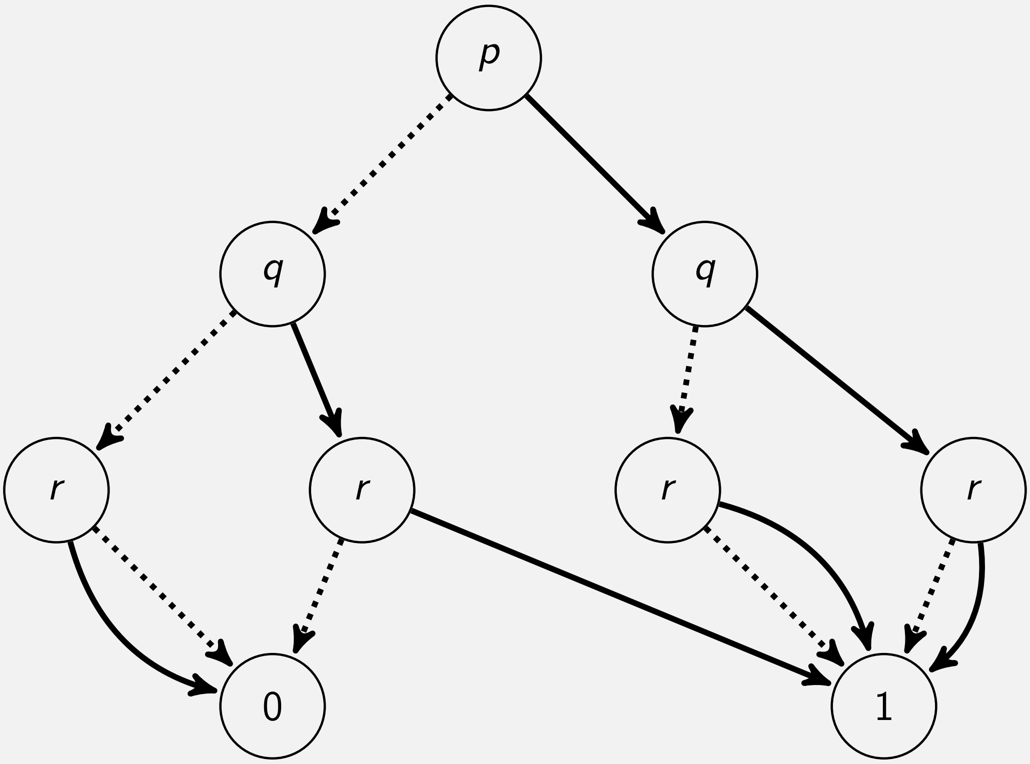
	p	q	r	$p \vee (q \wedge r)$
1.,2.	1	1	$\star$	1
3.,4.	1	0	$\star$	1
5.	0	1	1	1
6.	0	1	0	0
7.,8.	0	0	$\star$	0

	p	q	r	$p \vee (q \wedge r)$
1.,2., 3.,4.	1	$\star$	$\star$	1
5.	0	1	1	1
6.	0	1	0	0
7.,8.	0	0	$\star$	0

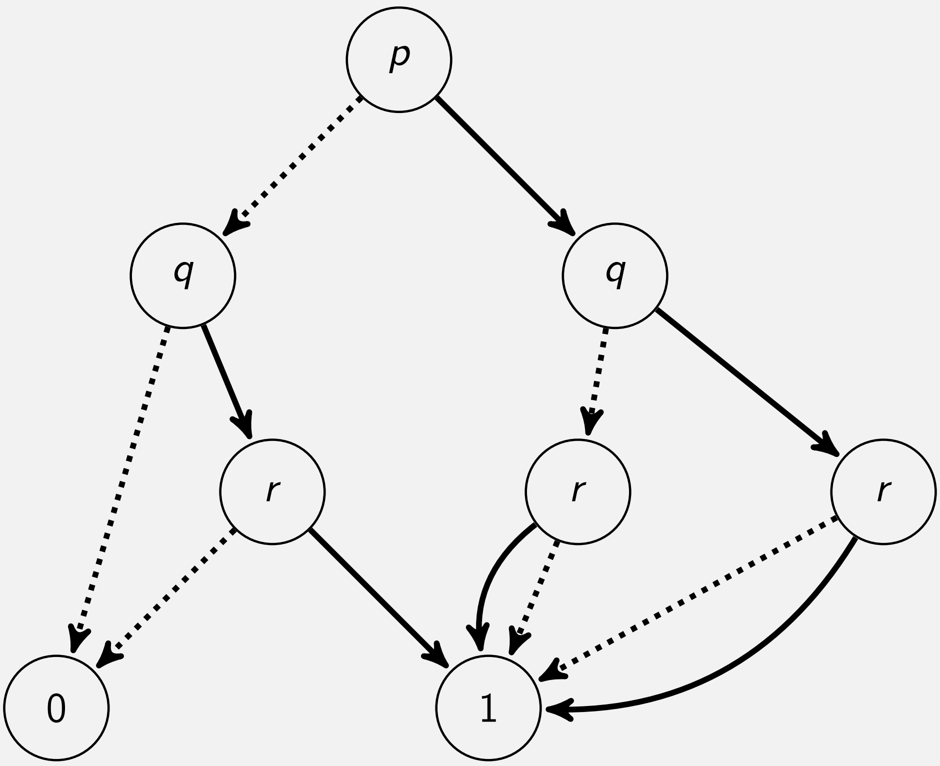
$p \vee (q \wedge r)$



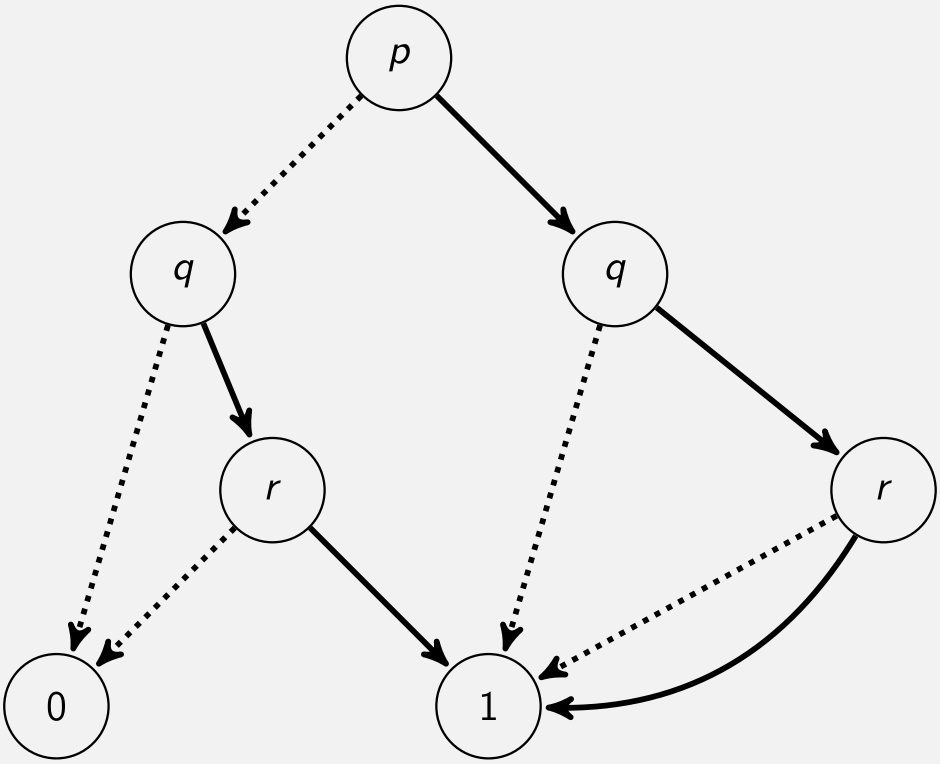
$p \vee (q \wedge r)$



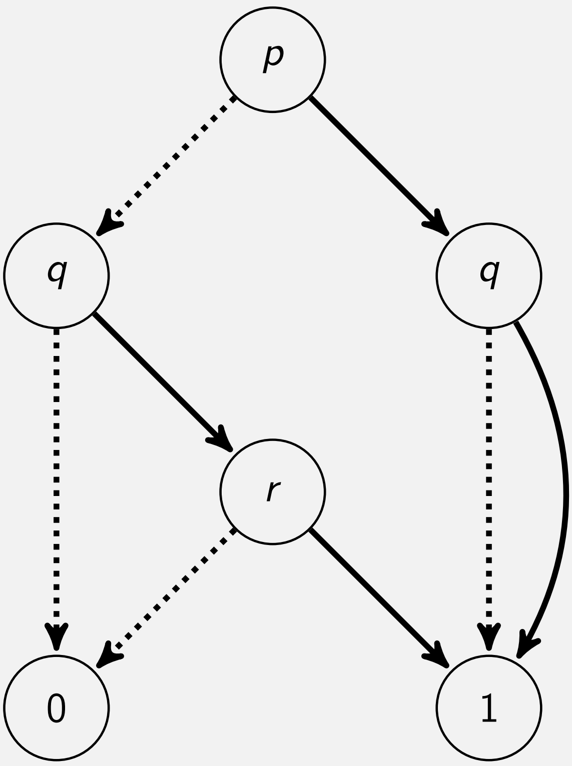
$p \vee (q \wedge r)$



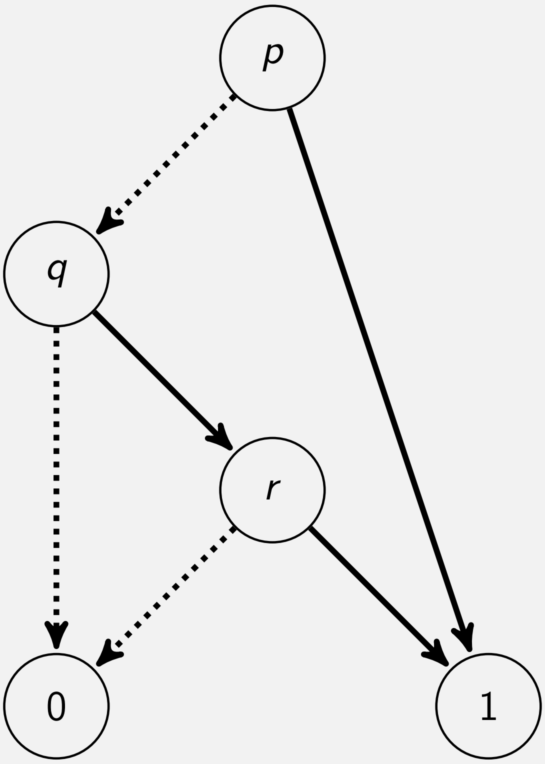
$p \lor (q \land r)$



$p \lor (q \land r)$



$p \vee (q \wedge r)$



Bináris döntési diagram (BDD)

- Egy olyan adatstruktúra, ami reprezentálja egy formula szemantikáját:
  - formula $\rightarrow$ irányított gráf $\rightarrow$ algoritmus $\rightarrow$ irányított redukált gráf;
  - logikailag ekvivalens formulák redukált irányított gráfja "tartalmilag" megegyezik;
  - egy formula érvényes, ha redukált bináris döntési diagramja (redukált irányított gráfja) megegyezik a verum triviális diagramjával $[\uparrow \Leftrightarrow_{def} (p \vee \neg p)]$;
  - egy formula kielégíthető, ha redukált bináris döntési diagramja (redukált irányított gráfja) nem egyezik meg a falsum triviális diagramjával $[\downarrow \Leftrightarrow_{def} (p \wedge \neg p)]$;

Definíció

Legyen $A \in Form$ (azaz A az állításlogika egy tetszőleges formulája). Az A formula bináris döntési diagramján a következő körmentes irányított gráfot értjük:

- Minden levélelem valamelyik igazságértéket tartalmazza.
- Minden belső (nem levélelem) csúcs egy A-beli paramétert tartalmaz és két kimenő éle van: egyik a "hamis él" (pontozással jelölt), a másik az "igaz él" (folytonos vonallal jelölt).
- Egy ágon egy paraméter legfeljebb egyszer fordulhat elő.

Megjegyzés

- Minden ág egy teljes vagy részleges interpretációt reprezentál.
- Egy ág által reprezentált interpretációban a formula értéke az ág levéleleme.

Redukáló algoritmus

- A következő lépéseket addig ismételjük, lehetséges:
  1. Ha egy bináris döntési diagramnak van két ugyanolyan tartalmú levéleleme, távolítsuk el a duplikált levélelem egyikét, és minden olyan élt irányítsunk át a megmaradó levélelemhez, amelyek az eltávolított levélelemhez mutattak.
  2. Ha a p_1-t tartalmazó csúcsnak mindkét kimenő éle a p_j-t tartalmazó csúcshoz vezet, akkor távolítsuk el a p_i-t tartalmazó csúcsot, a csúcs bemenő élét pedig irányítsuk át a p_j-t tartalmazó csúcshoz.
  3. Ha két p_i-t tartalmazó csúcs gyökere két azonos rész bináris döntési diagramnak, akkor távolítsuk el az egyiket, és az eltávolított rész bináris döntési diagram gyökeréhez mutató élet irányítsuk át a megtartott rész döntési diagram gyökeréhez.

Definíció

Ha egy bináris döntési diagram a redukáló algoritmus eredménye, akkor redukált bináris döntési diagramnak nevezzük.

Tétel

A redukált bináris döntési diagram logikailag ekvivalens a redukáló algoritmus bemeneteként fellépő bináris döntési diagrammal (abban az értelemben, hogy minden interpretációban ugyanazokat az igazságértékeket határozza meg).

Definíció

Legyen $L^{(0)} = \langle LC, Con, Form \rangle$ *a klasszikus állításlogika nyelve* ($LC = \{\neg, \supset, (,)\}$).
A klasszikus állításkalkulus axiómasémái (alapsémái):

- *(A1):* $A \supset (B \supset A)$
- *(A2):* $(A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$
- *(A3):* $(\neg A \supset \neg B) \supset (B \supset A)$

Definíció

- *Az alapsémák (axómasémák) szabályos behelyettesítésén olyan formulákat értünk, amelyek valamely alapsémából a benne szereplő betűk tetszőleges formulával való helyettesítése útján jönnek létre.*
- *A klasszikus állításkalkulus alapformulái (axiómái) az alapsémák (axiómasémák) szabályos behelyettesítései.*

Definíció

- *Az alapsémák (axómasémák) szabályos behelyettesítésén olyan formulákat értünk, amelyek valamely alapsémából a benne szereplő betűk tetszőleges formulával való helyettesítése útján jönnek létre.*
- *A klasszikus állításkalkulus alapformulái (axiómái) az alapsémák (axiómasémák) szabályos behelyettesítései.*

Definíció

A szintaktikai következményreláció strukturális induktív definíciója:

- *Legyen $\Gamma \subseteq Form, A \in Form$. A Γ formulahalmaznak szintaktikai következménye az A formula ($\Gamma \vdash A$), ha az alábbiak valamelyike teljesül:*
  1. *ha $A \in \Gamma$, akkor $\Gamma \vdash A$;*
  2. *ha A alapformula (axióma), akkor $\Gamma \vdash A$;*
  3. *ha $\Gamma \vdash B$, és $\Gamma \vdash B \supset A$, akkor $\Gamma \vdash A$.*

Definíció

Legyen $\Gamma \subset Form, A \in Form$. Ha az A formula szintaktikai következménye a Γ formulahalmaznak, akkor a '$\Gamma \vdash A$' jelsorozatot szekvenciának nevezzük.

A természetes levezetés technikájának alapvető szabálya a dedukciótételen alapul.

Tétel

Dedukciótétel: Ha $\Gamma \cup \{A\} \vdash B$, akkor $\Gamma \vdash A \supset B$.

Másként felírva:

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$$

Bizonyítás: gyakorlaton

Strukturális szabályok

Legyen a továbbiakban $\Gamma, \Delta \subseteq Form$, $A, B, C, \in Form$.

Az azonosság törvénye

$$\frac{\emptyset}{\Gamma, A \vdash A}$$

A bővítés szabálya

$$\frac{\Gamma \vdash A}{\Gamma, B \vdash A}$$

A szűkítés szabálya

$$\frac{\Gamma, B, B, \Delta \vdash A}{\Gamma, B, \Delta \vdash A}$$

Strukturális szabályok

A felcserélés (permutálás) szabálya

A felcserélés (permutálás) szabálya: $\dfrac{\Gamma, B, C, \Delta \vdash A}{\Gamma, C, B, \Delta \vdash A}$

A metszet szabály (vágás szabálya)

A metszet szabály (vágás szabálya): $\dfrac{\Gamma \vdash A \qquad \Delta, A \vdash B}{\Gamma, \Delta \vdash B}$

Logikai szabályok

Az implikáció (bevezető, illetve alkalmazó) szabályai

$(\supset\ 1.)\quad \dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$ $\qquad (\supset\ 2.)\quad \dfrac{\Gamma \vdash A \qquad \Gamma \vdash A \supset B}{\Gamma \vdash B}$

A konjunkció szabályai

$(\wedge\ 1.)\quad \dfrac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B}$ $\qquad (\wedge\ 2.)\quad \dfrac{\Gamma, A, B \vdash C}{\Gamma, A \wedge B \vdash C}$

A diszjunkció szabályai

$(\vee\ 1.)\quad \dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ $\qquad (\vee\ 2.)\quad \dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$

$(\vee\ 3.)\quad \dfrac{\Gamma, A \vdash C \qquad \Gamma, B \vdash C}{\Gamma, A \vee B \vdash C}$

Logikai szabályok

A negáció szabályai

$(\neg\ 1.)\quad \dfrac{\Gamma, A \vdash B \qquad \Gamma, A \vdash \neg B}{\Gamma \vdash \neg A}$ $\qquad (\neg\ 2.)\quad \dfrac{\Gamma \vdash \neg\neg A}{\Gamma \vdash A}$

A (materiális) ekvivalencia szabályai

$$(\equiv\ 1.)\quad \frac{\Gamma, A \vdash B \qquad \Gamma, B \vdash A}{\Gamma \vdash A \equiv B}$$

$$(\equiv\ 2.)\quad \frac{\Gamma \vdash A \qquad \Gamma \vdash A \equiv B}{\Gamma \vdash B}$$

$$(\equiv\ 3.)\quad \frac{\Gamma \vdash B \qquad \Gamma \vdash A \equiv B}{\Gamma \vdash A}$$

Példák

$$\frac{\Gamma, A \vdash B}{\Gamma, \neg B \vdash \neg A} \tag{1}$$

Bizonyítás:

$$\begin{array}{r} (\text{Bővítés}) \\ (\text{Felcserélés}) \\ (\neg\ 1.) \end{array} \quad \dfrac{\dfrac{\dfrac{\Gamma, A \vdash B}{\Gamma, A, \neg B \vdash B}}{\Gamma, \neg B, A \vdash B} \qquad \dfrac{\dfrac{\emptyset}{\Gamma, A, \neg B \vdash \neg B}}{\Gamma, \neg B, A \vdash \neg B}}{\Gamma, \neg B \vdash \neg A} \quad \begin{array}{l} (\text{Azonosság}) \\ (\text{Felcserélés}) \end{array}$$

Példák

$$\frac{\Gamma, A \vdash \neg B}{\Gamma, B \vdash \neg A} \tag{2}$$

Bizonyítás:

$$\begin{array}{r} (\text{Azonosság}) \\ (\text{Felcserélés}) \\ (\neg\ 1.) \end{array} \quad \dfrac{\dfrac{\dfrac{\emptyset}{\Gamma, A, B \vdash B}}{\Gamma, B, A \vdash B} \qquad \dfrac{\dfrac{\Gamma, A \vdash \neg B}{\Gamma, A, B \vdash \neg B}}{\Gamma, B, A \vdash \neg B}}{\Gamma, B \vdash \neg A} \quad \begin{array}{l} (\text{Bővítés}) \\ (\text{Felcserélés}) \end{array}$$

$$\frac{\Gamma, \neg A \vdash B}{\Gamma, \neg B \vdash A} \tag{3}$$

Bizonyítás:

$$\cfrac{\cfrac{\cfrac{\Gamma, \neg A \vdash B}{\Gamma, \neg A, \neg B \vdash B}\ (\text{Bővítés})}{\Gamma, \neg B, \neg A \vdash B}\ (\text{Felcserélés}) \qquad \cfrac{\cfrac{\emptyset}{\Gamma, \neg A, \neg B \vdash \neg B}\ (\text{Azonosság})}{\Gamma, \neg B, \neg A \vdash \neg B}\ (\text{Felcserélés})}{\cfrac{\Gamma, \neg B \vdash \neg\neg A}{\Gamma, \neg B \vdash A}\ (\neg\ 2.)}\ (\neg\ 1.)$$

Példák

$$\frac{\Gamma, \neg A \vdash \neg B}{\Gamma, B \vdash A} \tag{4}$$

Bizonyítás:

$$\cfrac{\cfrac{\cfrac{\emptyset}{\Gamma, \neg A, B \vdash B}\ (\text{Azonosság})}{\Gamma, B, \neg A \vdash B}\ (\text{Felcserélés}) \qquad \cfrac{\cfrac{\Gamma, \neg A \vdash \neg B}{\Gamma, \neg A, B \vdash \neg B}\ (\text{Bővítés})}{\Gamma, B, \neg A \vdash \neg B}\ (\text{Felcserélés})}{\cfrac{\Gamma, B \vdash \neg\neg A}{\Gamma, B \vdash A}\ (\neg\ 2.)}\ (\neg\ 1.)$$

$$\vdash A \supset A \tag{5}$$

Bizonyítás:

$$\begin{array}{rc} (\text{Azonosság}) & \dfrac{\emptyset}{A \vdash A} \\ (\supset 1.) & \overline{\vdash A \supset A} \end{array}$$

Példák

$$A, A \supset B \vdash B \tag{6}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\emptyset}{A \supset B, A \vdash A}}{A,\ A \supset B \vdash A} \qquad \dfrac{\emptyset}{A, A \supset B \vdash A \supset B}}{A, A \supset B \vdash B}$$

$$A \vdash B \supset A \tag{7}$$

Bizonyítás:

$$\begin{array}{rc} & \emptyset \\ \text{(Azonosság)} & \overline{B, A \vdash A} \\ \text{(Felcserélés)} & \overline{A, B \vdash A} \\ (\supset 1.) & \overline{A \vdash B \supset A} \end{array}$$

Példák

$$A, \neg A \vdash B \tag{8}$$

$$\neg A \vdash A \supset B \tag{9}$$

Bizonyítás (8), (9):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A, \neg B, \neg A \vdash \neg A}}{A, \neg A, \neg B \vdash \neg A} \qquad \dfrac{\dfrac{\dfrac{\emptyset}{\neg A, \neg B, A \vdash A}}{\neg A, A, \neg B \vdash A}}{A, \neg A, \neg B \vdash A}}{A, \neg A \vdash \neg\neg B}}{A, \neg A \vdash B}}{\neg A, A \vdash B}}{\neg A \vdash A \supset B}$$

Példák

$$B \vdash A \supset B \tag{10}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\emptyset}{B \vdash B}}{B, A \vdash B}}{B \vdash A \supset B}$$

A természetes levezetés rendszere

$$\vdash A \supset B \equiv \neg A \vee B \tag{11}$$

Bizonyítás: Először lássuk be, hogy

$$A \supset B \vdash \neg A \vee B \tag{12}$$

$$\dfrac{\dfrac{\dfrac{\emptyset}{A \supset B \vdash A \supset B}}{A \supset B, \neg(\neg A \vee B) \vdash A \supset B} \qquad \dfrac{(3)\ \dfrac{\dfrac{\dfrac{\emptyset}{\neg A \vdash \neg A}}{\neg A \vdash \neg A \vee B}}{\neg(\neg A \vee B) \vdash A}}{A \supset B, \neg(\neg A \vee B) \vdash A}}{A \supset B, \neg(\neg A \vee B) \vdash B}$$

Példák

$$(1)\ \cfrac{\cfrac{\cfrac{\cfrac{\emptyset}{B \vdash B}}{B \vdash \neg A \vee B}}{\neg(\neg A \vee B) \vdash \neg B}}{A \supset B, \neg(\neg A \vee B) \vdash \neg B}$$

$$\cfrac{\cfrac{A \supset B, \neg(\neg A \vee B) \vdash B \qquad A \supset B, \neg(\neg A \vee B) \vdash \neg B}{A \supset B \vdash \neg\neg(\neg A \vee B)}}{A \supset B \vdash \neg A \vee B}$$

Példák

(11) bizonyításához lássuk be, hogy

$$\neg A \vee B \vdash A \supset B \tag{13}$$

$$\cfrac{\cfrac{(9)}{\neg A \vdash A \supset B} \qquad \cfrac{(10)}{B \vdash A \supset B}}{\neg A \vee B \vdash A \supset B}$$

$$A \supset B, \neg B \vdash \neg A \tag{14}$$

$$A \supset B \vdash \neg B \supset \neg A \tag{15}$$

Bizonyítás (14), (15):

$$\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A \supset B, \neg B, A \vdash \neg B}}{A \supset B, \neg B, A \vdash \neg B} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A, A \supset B \vdash B}}{A \supset B, A \vdash B}}{A \supset B, A, \neg B \vdash B}}{A \supset B, \neg B, A \vdash B}}{A \supset B, \neg B \vdash \neg A}}{A \supset B \vdash \neg B \supset \neg A}$$

$$\neg B \supset \neg A \vdash A \supset B \tag{16}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{\neg B \supset \neg A, \neg B, A \vdash A} \qquad \dfrac{\dfrac{\emptyset}{\neg B \supset \neg A, \neg B \vdash \neg A}}{\neg B \supset \neg A, \neg B, A \vdash \neg A}}{\neg B \supset \neg A, A \vdash \neg\neg B}}{\neg B \supset \neg A, A \vdash B}}{\neg B \supset \neg A \vdash A \supset B}$$

Példák

(15), (16) alapján:

$$\vdash A \supset B \equiv \neg B \supset \neg A \tag{17}$$

Bizonyítás:

$$\frac{A \supset B \vdash \neg B \supset \neg A \qquad \neg B \supset \neg A \vdash A \supset B}{\vdash A \supset B \equiv \neg B \supset \neg A}$$

$$\vdash (A \vee \neg A) \tag{18}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\emptyset}{A, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)}}{\neg(A \vee \neg A), A \vdash \neg(A \vee \neg A)} \qquad \dfrac{\dfrac{\emptyset}{\neg(A \vee \neg A), A \vdash A}}{\neg(A \vee \neg A), A \vdash A \vee \neg A}}{\neg(A \vee \neg A) \vdash \neg A}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{\neg A, \neg(A \vee \neg A) \vdash \neg(A \vee \neg A)}}{\neg(A \vee \neg A), \neg A \vdash \neg(A \vee \neg A)} \qquad \dfrac{\dfrac{\emptyset}{\neg(A \vee \neg A), \neg A \vdash \neg A}}{\neg(A \vee \neg A), \neg A \vdash A \vee \neg A}}{\neg(A \vee \neg A) \vdash \neg\neg A}}{\neg(A \vee \neg A) \vdash A}$$

Példák

$$\dfrac{\dfrac{\neg(A \vee \neg A) \vdash \neg A \qquad \neg(A \vee \neg A) \vdash A}{\vdash \neg\neg(A \vee \neg A)}}{\vdash (A \vee \neg A)}$$

$$A \wedge B \vdash B \wedge A \tag{19}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\emptyset}{A, B \vdash B} \qquad \dfrac{\dfrac{\emptyset}{B, A \vdash A}}{A, B \vdash A}}{A, B \vdash B \wedge A}}{A \wedge B \vdash B \wedge A}$$

$$A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C) \tag{20}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{B, A \vdash A}}{A, B \vdash A} \quad \dfrac{\emptyset}{A, B \vdash B}}{A, B \vdash A \wedge B}}{A, B \vdash (A \wedge B) \vee (A \wedge C)} \quad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{C, A \vdash A}}{A, C \vdash A} \quad \dfrac{\emptyset}{A, C \vdash C}}{A, C \vdash A \wedge C}}{A, C \vdash (A \wedge B) \vee (A \wedge C)}}{\dfrac{A, B \vee C \vdash (A \wedge B) \vee (A \wedge C)}{A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)}}$$

$$(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C) \tag{21}$$

Bizonyítás:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{B, A \vdash A}}{A, B \vdash A}}{A \wedge B \vdash A} \quad \dfrac{\dfrac{\dfrac{\emptyset}{C, A \vdash A}}{A, C \vdash A}}{A \wedge C \vdash A}}{(A \wedge B) \vee (A \wedge C) \vdash A} \quad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A, B \vdash B}}{A \wedge B \vdash B}}{A \wedge B \vdash B \vee C} \quad \dfrac{\dfrac{\dfrac{\emptyset}{A, C \vdash C}}{A \wedge C \vdash C}}{A \wedge C \vdash B \vee C}}{(A \wedge B) \vee (A \wedge C) \vdash B \vee C}}{(A \wedge B) \vee (A \wedge C) \vdash A \wedge (B \vee C)}$$

(20) és (21) alapján:

$$\vdash A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C) \tag{22}$$

$$\vdash A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C) \tag{23}$$

Bizonyítás: Először lássuk be, hogy

$$A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C) \tag{24}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A \vdash A}}{A \vdash A \vee B} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{B \vdash B}}{B, C \vdash B}}{B, C \vdash A \vee B}}{B \wedge C \vdash A \vee B}}{A \vee (B \wedge C) \vdash A \vee B} \qquad \dfrac{\dfrac{\dfrac{\emptyset}{A \vdash A}}{A \vdash A \vee C} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{C \vdash C}}{C \vdash A \vee C}}{B, C \vdash A \vee C}}{B \wedge C \vdash A \vee C}}{A \vee (B \wedge C) \vdash A \vee C}}{A \vee (B \wedge C) \vdash (A \vee B) \wedge (A \vee C)}$$

Most lássuk be, hogy

$$(A \vee B) \wedge (A \vee C) \vdash A \vee (B \wedge C) \tag{25}$$

$$\dfrac{\dfrac{\dfrac{\emptyset}{A \vdash A}}{A \vdash A \vee (B \wedge C)}}{A \vee B, A \vdash A \vee (B \wedge C)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A \vdash A}}{A \vdash A \vee (B \wedge C)}}{A, C \vdash A \vee (B \wedge C)} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{B \vdash B}}{B, C \vdash B} \qquad \dfrac{\dfrac{\emptyset}{C \vdash C}}{B, C \vdash C}}{B, C \vdash B \wedge C}}{B, C \vdash A \vee (B \wedge C)}}{A \vee B, C \vdash A \vee (B \wedge C)}$$

$$\frac{\dfrac{A \vee B, A \vdash A \vee (B \wedge C) \qquad A \vee B, C \vdash A \vee (B \wedge C)}{A \vee B, A \vee C \vdash A \vee (B \wedge C)}}{(A \vee B) \wedge (A \vee C) \vdash A \vee (B \wedge C)}$$

Példák

$$\vdash (A \supset B) \supset (B \supset C) \supset (A \supset C) \tag{26}$$

Bizonyítás: Használjuk fel már bizonyított (6) szekvenciát.

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{A \supset B, A \vdash B \qquad B, B \supset C \vdash C}{A \supset B, A, B \supset C \vdash C}}{A \supset B, B \supset C, A \vdash C}}{A \supset B, B \supset C \vdash A \supset C}}{A \supset B \vdash (B \supset C) \supset (A \supset C)}}{\vdash (A \supset B) \supset (B \supset C) \supset (A \supset C)}$$

$$\vdash (A \supset B) \supset (A \supset (B \supset C)) \supset (A \supset C) \tag{27}$$

Bizonyítás: Használjuk fel már bizonyított (6) szekvenciát.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A, A \supset B \vdash B}{A, A \supset B, A \supset (B \supset C) \vdash B} \quad \dfrac{A, A \supset (B \supset C) \vdash B \supset C}{A, A \supset B, A \supset (B \supset C) \vdash B \supset C}}{A, A \supset B, A \supset (B \supset C) \vdash C}}{A \supset B, A \supset (B \supset C) \vdash A \supset C}}{A \supset B \vdash (A \supset (B \supset C)) \supset (A \supset C)}}{\vdash (A \supset B) \supset (A \supset (B \supset C)) \supset (A \supset C)}$$

A természetes levezetés rendszere

A De Morgan azonosságok:

$$\vdash \neg(A \wedge B) \equiv (\neg A \vee \neg B) \tag{28}$$

$$\vdash \neg(A \vee B) \equiv (\neg A \wedge \neg B) \tag{29}$$

Példák

A (28) bizonyításához először lássuk be, hogy

$$\neg(A \land B) \vdash (\neg A \lor \neg B) \qquad (30)$$

$$\begin{array}{c}(3)\ \dfrac{\dfrac{(3)\ \dfrac{\dfrac{\dfrac{\emptyset}{\neg A \vdash \neg A}}{\neg A \vdash \neg A \lor \neg B}}{\neg(\neg A \lor \neg B) \vdash A} \qquad (3)\ \dfrac{\dfrac{\dfrac{\emptyset}{\neg B \vdash \neg B}}{\neg B \vdash \neg A \lor \neg B}}{\neg(\neg A \lor \neg B) \vdash B}}{\neg(\neg A \lor \neg B) \vdash A \land B}}{\neg(A \land B) \vdash \neg A \lor \neg B}\end{array}$$

A (28) bizonyításához most lássuk be, hogy

$$\neg A \lor \neg B \vdash \neg(A \land B) \qquad (31)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{A \vdash A}}{A, B \vdash A}}{A \land B \vdash A}}{\neg A \lor \neg B, A \land B \vdash A} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\emptyset}{\neg A \vdash \neg A}}{B, \neg A \vdash \neg A} \qquad \dfrac{(8)}{B, \neg B \vdash \neg A}}{B, \neg A \lor \neg B \vdash \neg A}}{\neg A \lor \neg B, B \vdash \neg A}}{\neg A \lor \neg B, A, B \vdash \neg A}}{\neg A \lor \neg B, A \land B \vdash \neg A}}{\neg A \lor \neg B \vdash \neg(A \land B)}$$

A (29) bizonyításához először lássuk be, hogy

$$\neg(A \vee B) \vdash \neg A \wedge \neg B \tag{32}$$

$$\cfrac{(1)\ \cfrac{\cfrac{\cfrac{\emptyset}{A \vdash A}}{A \vdash A \vee B}}{\neg(A \vee B) \vdash \neg A} \qquad (1)\ \cfrac{\cfrac{\cfrac{\emptyset}{B \vdash B}}{B \vdash A \vee B}}{\neg(A \vee B) \vdash \neg B}}{\neg(A \vee B) \vdash \neg A \wedge \neg B}$$

Példák

A (29) bizonyításához most lássuk be, hogy

$$\neg A \wedge \neg B \vdash \neg(A \vee B) \tag{33}$$

$$(2)\ \cfrac{\cfrac{(2)\ \cfrac{\cfrac{\cfrac{\cfrac{\emptyset}{\neg A \vdash \neg A}}{\neg A, \neg B \vdash \neg A}}{\neg A \wedge \neg B \vdash \neg A}}{A \vdash \neg(\neg A \wedge \neg B)} \qquad (2)\ \cfrac{\cfrac{\cfrac{\cfrac{\emptyset}{\neg B \vdash \neg B}}{\neg A, \neg B \vdash \neg B}}{\neg A \wedge \neg B \vdash \neg B}}{B \vdash \neg(\neg A \wedge \neg B)}}{A \vee B \vdash \neg(\neg A \wedge \neg B)}}{\neg A \wedge \neg B \vdash \neg(A \vee B)}$$

Értelmezések

- Klóz: literálok egy halmaza.
- Egy klózt úgy lehet tekinteni, mint literáljainak diszjunkcióját.
- Az egység klóz pontosan egy literált tartalmaz.
- Ha egy klóz egyetlen literált sem tartalmaz, akkor üres klózról beszélünk, jele: $\square$.
- Egy formula klóz formája klózok egy halmaza. Ekkor maga a formula a klózokból képzett diszjunkciók konjunkciója.
- Ha egy formula klóz formája egyetlen klózt sem tartalmaz, akkor a formula jele $\emptyset$.

- Az ábrázolás csak logikailag nem releváns különbséget jelent: $p \Leftrightarrow p \vee p$

Tétel

- Az állításlogika minden formulája klóz formában reprezentálható: a klóz forma által reprezentált formula logikailag ekvivalens az eredeti formulával.

- Egy klózt triviálisnak nevezünk, ha tartalmaz ugyanazon alapú pozitív és negatív literált.
- Legyen S klózoknak egy halmaza (azaz egy klózforma), és $C \in S$ egy triviális klóz. Ekkor a $S \setminus \{C\}$ klózforma logikailag ekvivalens az S klózformával (azaz a nekik megfeleltetett formulák logikailag ekvivalensek).

Lemma

- Az üres klóz ($\square$) kielégíthetetlen. (Az üres klóznak megfelelő formula kielégíthetetlen.)
- Az üres klózforma (az egyetlen klózt sem tartalmazó klózforma, azaz $\emptyset$) érvényes. (Az üres klózformának megfelelő formula érvényes.)

- Ahhoz, hogy egy klóz (azaz a neki megfeleltetett formula) kielégíthető legyen legalább egy literáljának igaznak kell lennie. (Ha nem tartalmaz literált, akkor nem lehet kielégíthető.)
- Ahhoz, hogy a klózforma (azaz a neki megfeleltetett formula) érvényes legyen, minden elemének érvényes kell lennie.

Definíció

- Legyen l egy literál. Az l komplementerén l^c-n a következő literált értjük:
  - ha $l = p$, akkor $l^c = \neg p$;
  - ha $l = \neg p$, akkor $l^c = p$.

Rezolúció szabály: állításlogika

Legyen C_1, C_2 két klóz úgy, hogy $l \in C_1$ és $l^c \in C_2$.

- A C klóz a C_1 és C_2 klózok rezolvense, ha $C = Res(C_1, C_2) = (C_1 \setminus \{l\}) \cup (C_2 \setminus \{l^c\})$
- a C_1 és C_2 klózok a C klóz szülő klózai.
- a C_1 és C_2 klózok "ütköző" klózok, (az l, l^c kiegészítő literálok miatt).

Megjegyzés

- A halmazelméleti kivonás miatt két klóz rezolvense lehet az üres klóz ($\square$), ami kielégíthetetlen.

Lemma

Ha a C_1 és C_2 több mint egy kiegészítő literálpárt tartalmaz, (azaz $l_1, l_2 \in C_1$ és $l_1^c, l_2^c \in C_2$), akkor rezolvensük a triviális klóz ($l_2, l_2^c \in Res(C_1, C_2)$).

Megjegyzés

- Nincs egyszerre több lépés: $Res(\{p, q\}, \{\bar{p}, \bar{q}\}) = \{q, \bar{q}\}$, azaz $Res(\{p, q\}, \{\bar{p}, \bar{q}\}) \neq \square$.
- Ha a C_1 és C_2 több mint egy kiegészítő literálpárt tartalmaznak, akkor törölhetjük őket a klózhalmazból, és utána kell végrehajtani a rezolúciót.

Tétel

Legyen C_1, C_2 két klóz úgy, hogy $l \in C_1$ és $l^c \in C_2$ és $C = Res(C_1, C_2$. A C klóz akkor és csak akkor kielégíthető, ha C_1, C_2 klózok kielégíthetőek. (A rezolvens akkor és csak akkor kielégíthető, ha szülő klózai kielégíthetőek.)

Definíció

Egy konjunktív normálformájú formula 3CNF alakú, ha minden eelemi diszjunkció pontosan 3 literált tartalmaz.

Megjegyzés

A CNF és a 3CNF létrehozása NP-teljes probléma (3CNF nem "kerül többe").

CNF→ 3CNF

- Input: egy CNF alakú formula
- Output: a bemenettel logikailag ekvivalens 3CNF alakú formula
- Minden $C_i = l_i^1 \vee l_i^2 \vee \cdots \vee l_i^{n_i}$ az n_i értékétől függő átalakítások végrehajtása:
  - Ha $n_i = 1$, akkor C_i a következő taggal helyettesítendő: $(l_i^1 \vee p_i^1 \vee p_i^2) \wedge (l_i^1 \vee \neg p_i^1 \vee p_i^2) \wedge (l_i^1 \vee p_i^1 \vee \neg p_i^2) \wedge (l_i^1 \vee \neg p_i^1 \vee \neg p_i^2)$, ahol p_i^1, p_i^2 új állításparaméterek.
  - Ha $n_i = 2$, akkor C_i a következő taggal helyettesítendő: $(l_i^1 \vee l_i^2 \vee p_i^1) \wedge (l_i^1 \vee l_i^2 \vee \neg p_i^1)$, ahol p_i^1 új állításparaméter.
  - Ha $n_i = 3$, akkor nincs teendő.
  - Ha $n_i > 3$, akkor C_i a következő taggal helyettesítendő: $(l_i^1 \vee l_i^2 \vee p_i^1) \wedge (\neg p_i^1 \vee l_i^3 \vee p_i^2) \wedge \cdots \wedge (\neg p_i^{n-3} \vee l_i^{n-1} \vee l_i^n)$, ahol $p_i^1, p_i^2, \ldots, p_i^{n-3}$ új állításparaméterek.

A rezolúció eljárása

- Input: Egy S klózhalmaz.
- Output: S kielégíthető vagy kielégíthetetlen.
  - $S_0 \leftarrow S$
  - Egy eddig nem választott ütköző klózpár kiválasztása: $\{C_1, C_2\} \subseteq S_i$
  - $C \leftarrow Res(C_1, C_2)$
  - Ha C nem egy triviális klóz, akkor $S_{i+1} = S_i \cup \{C\}$, különben $S_{i+1} = S_i$
- Az eljárás leáll, ha
  - $C = \Box$
  - Az ütköző párok mindegyike sorra került (nem létezik nem rezolvált ütköző pár).

Tétel (helyesség)

Legyen S egy klózhalmaz. Ha létezik rezolúció általi cáfolata S-nek, akkor S kielégíthetetlen.

Tétel (teljesség)

Legyen S egy klózhalmaz. Ha S kielégíthetetlen, akkor a rezolúció eljárásának eredménye az üres klóz ($\Box$).

- Van-e igazán hatékony módszer annak eldöntésére, hogy az állításlogika valamely formulája kielégíthető?
- Az igazságtábla nem igazán hatékony.
- Egy nem teljes algoritmus (a gyakorlatban) alkalmas lehet a probléma megoldására:
  - ha egy formula kielégíthető (azaz van modellje), akkor gyorsan talál egy modellt;
  - de: nem alkalmas a kielégíthetetlenség megállapítására.
- SAT solver: olyan program, ami az állításlogika egy formulájának a modelljét adja meg.
- Hasznos: sok problémát lehet állításlogikai eszközökkel kódolni.

Értelmezések

- Klóz: literálok egy halmaza.
- Egy klózt úgy lehet tekinteni, mint literáljainak diszjunkcióját.
- Az egység klóz pontosan egy literált tartalmaz.
- Ha egy klóz egyetlen literált sem tartalmaz, akkor üres klózról beszélünk, jele: $\Box$.
- Egy formula klóz formája klózok egy halmaza. Ekkor maga a formula a klózokból képzett diszjunkciók konjunkciója.
- Ha egy formula klóz formája egyetlen klózt sem tartalmaz, akkor a formula jele $\emptyset$.

- Az ábrázolás csak logikailag nem releváns különbséget jelent: $p \Leftrightarrow p \vee p$

Tétel

- Az állításlogika minden formulája klóz formában reprezentálható: a klóz forma által reprezentált formula logikailag ekvivalens az eredeti formulával.

- Egy klózt triviálisnak nevezünk, ha tartalmaz ugyanazon alapú pozitív és negatív literált.
- Legyen S klózoknak egy halmaza (azaz egy klózforma), és $C \in S$ egy triviális klóz. Ekkor a $S \setminus \{C\}$ klózforma logikailag ekvivalens az S klózformával (azaz a nekik megfeleltetett formulák logikailag ekvivalensek).

Az állításlogika SAT problémája

Lemma

- Az üres klóz ($\square$) kielégíthetetlen. (Az üres klóznak megfelelő formula kielégíthetetlen.)
- Az üres klózforma (az egyetlen klózt sem tartalmazó klózforma, azaz $\emptyset$) érvényes. (Az üres klózformának megfelelő formula érvényes.)

- Ahhoz, hogy egy klóz (azaz a neki megfeleltetett formula) kielégíthető legyen legalább egy literáljának igaznak kell lennie. (Ha nem tartalmaz literált, akkor nem lehet kielégíthető.)
- Ahhoz, hogy a klózforma (azaz a neki megfeleltetett formula) érvényes legyen, minden elemének érvényes kell lennie.

Definíció

Legyen S és S' két klózhalmaz (azaz két klózfroma). $S \approx S'$ ha S akkor és csak akkor kielégíthető, ha S' kielégíthető (azaz a klózformáknak megfeleltetett formulák kielégíthetőségének feltételei megegyeznek).

Megjegyzés

$S \approx S'$ nem jelenti azt, hogy a két klózforma (és így a nekik megfeletetett formulák) ekvivalensek lennének.

- $S = \{pq\bar{r}, p\bar{q}, \bar{p}q\}$, $S' = \{p\bar{q}, \bar{p}q\}$
- $\varrho(p) = 0, \varrho(q) = 0, \varrho(r) = 1$

Definíció

- Legyen l egy literál. Az l komplementerén l^c-n a következő literált értjük:
  - ha $l = p$, akkor $l^c = \neg p$;
  - ha $l = \neg p$, akkor $l^c = p$.
- Legyen S klózok egy halmaza (azaz egy klózforma). Az l literál S egy tiszta literálja, ha az l literál előfordul S legalább egy klózában, de az l komplementer literálja (azaz l^c) S egyetlen klózában sem fordul elő.

Tétel

Legyen S klózok egy halmaza (azaz egy klózforma), és az l literál S egy tiszta literálja. Legyen S' az a klózforma, amelyet az S klózformából úgy kapunk, hogy az összes olyan klózt töröljük S-ből, amelyben l előfordul. Ekkor $S \approx S'$.

Tétel (Egység klóz)

Legyen $\{l\} \in S$ egy egység klóz. Legyen S' az a klózforma, amelyet az S klózformából úgy kapunk, hogy

- egyrészt töröljük az összes olyan klózt S-ből, amelyben l előfordul,
- másrészt a fennmaradó klózhalmaz minden eleméből töröljük az l^c komplementer literált.

Ekkor $S \approx S'$.

Bizonyítás

- A klózforma értelmezése alapján triviális.
- $S = \{r, pq\bar{r}, p\bar{q}, \bar{p}q\}$, $S' = \{pq, p\bar{q}, \bar{p}q\}$

Következmény

$\square$ kielégíthetetlen.

Az $S = \{\{p\}, \{\bar{p}\}\}$ a kielégíthetetlen $p \wedge \neg p$ formula klózformája. A két lépés után $S' = \{\{\}\} = \{\square\}$.
A tétel alapján $S \approx S'$, így $\square$ kielégíthetetlen.

Definíció

Legyen C_1 és C_2 két klóz. Ha $C_1 \subseteq C_2$, akkor a a C_1 klóz szubszummálja a C_2 klózt.

Tétel

Legyen $C_1, C_2 \in S$, C_1 szubszummálja C_2-t, $S' = S \setminus \{C_2\}$. Ekkor $S \approx S'$.

Példa

$S = \{pr, \bar{p}q\bar{r}, q\bar{r}\}$, $S' = \{pr, q\bar{r}\}$

Definíció

Legyen S egy klózforma (azaz klózok egy halmaza), U pedig állításparaméterek egy halmaza. Az S U elemeivel való átnevezését, $R_U(S)$-t úgy kapjuk meg, hogy minden olyan literált, amelynek alapja U eleme, a literál komplementerével helyettesítjük.

Tétel

$S \approx R_U(S)$

Davis-Putnam algoritmus

1. Input: Egy klózformájú A formula
2. Output: A kielégíthető; A kielégíthetetlen
   1. Egységliterál szabály: ha $\{l\} \in A$ (azaz l egy egységkóz A-ban), akkor töröljük az összes olyan klóz A-ból, amelynek eleme l, és töröljük l^c összes előfordulását a fennmaradó klózokból;
   2. Tiszta literál szabály: ha l tiszta literál, akkor töröljünk minden olyan klózt, amely tartalmazza az l literált;
   3. Állításparaméterek rezolúció általi eliminációja: válasszunk egy p állításparamétert és végezzük el az összes lehetséges rezolúciót azokon a klózokon, amelyek tartalmazzák a $p, \bar{p}$ literálokat. Az eredményül kapott rezolvenseket adjuk hozzá a klózhalmazhoz, majd töröljük az összes olyan klózt, amely tartalmazza a p vagy a $\bar{p}$ literálokat.
3. Az algoritmus leáll, ha
   1. eljutott az üres klózig ($\square$), ekkor a formulát kielégíthetetlennek minősíti;
   2. ha nincs alkalmazható szabály, akkor a formulát kielégíthetőnek minősíti.

Az algoritmus szükségképpen leáll:

- egy formula állításparamétereinek halmaza véges;
- a rezolúció által előállított lehetséges klózok száma véges.

Az algoritmus helyességét az alábbiak biztosítják:

- az egység klózokra vonatkozó tétel;
- a tiszta klózokra vonatkozó tétel;
- a rezolúcióra vonatkozó tétel.

Rezolúció szabály: állításlogika

Legyen C_1, C_2 két klóz úgy, hogy $l \in C_1$ és $l^c \in C_2$.

- A C klóz a C_1 és C_2 klózok rezolvense, ha $C = Res(C_1, C_2) = (C_1 \setminus \{l\}) \cup (C_2 \setminus \{l^c\})$
- a C_1 és C_2 klózok a C klóz szülő klózai.
- a C_1 és C_2 klózok "ütköző" klózok, (az l, l^c kiegészítő literálok miatt).

Megjegyzés

- A halmazelméleti kivonás miatt két klóz rezolvense lehet az üres klóz ($\square$), ami kielégíthetetlen.
- Ha a C_1 és C_2 több mint egy kiegészítő literálpárt tartalmaz, (azaz $l_1, l_2 \in C_1$ és $l_1^c, l_2^c \in C_2$), akkor rezolvensük a triviális klóz ($l_2, l_2^c \in Res(C_1, C_2)$).
- De nincs egyszerre több lépés: $Res(\{p, q\}, \{\bar{p}, \bar{q}\}) = \{q, \bar{q}\}$, azaz $Res(\{p, q\}, \{\bar{p}, \bar{q}\}) \neq \square$

Definíció

Az egységliterál szabály ismételt alkalmazását (addig amíg ez lehetséges) egység propagálásnak vagy Boole kényszer propagálásnak nevezik.

- A Davis-Putnam algoritmus: egy állításparaméterhez kötődően az össze lehetséges rezolvens előállítása nem igazán hatékony.
- A DPLL algoritmus a paramétereliminációt helyettesíti a formula egy modelljének a keresésével.

Definíció

Legyen A egy klózforma, azaz klózoknak egy halmaza, és ϱ egy parciális interpretációja A-nak és $C \in A$.

- Ha $|C|_\varrho = 1$, akkor a ϱ interpretáció kielégíti C-t.
- Ha $|C|_\varrho = 0$, akkor C egy konfliktusklóz a ϱ interpretációra nézve.

DPLL algoritmus

A DPLL algoritmus egy parciális interpretációt terjeszt ki:

- olyan paraméterekre, amelyek eddig még nem kaptak értéket;
- a klózhalmazt kiértékeli az új parciális interpretációra támaszkodva;
- a klózhalmazt egyszerűsíti az egység propagálás által;
- ha a klózhalmaz konfliktus klózt tartalmaz az adott parciális interpretációra nézve, akkor a parciális interpretációt nem lehet úgy kiterjeszteni, hogy minden klóz igaz legyen: ekkor egy új parciális interpretációból kell kiindulni.

- A DPLL algoritmus nem determinisztikus:
  - az új paraméter választásában;
  - az új paraméterhez rendelt érték meghatározásában.

Heurisztikák

- Válasszuk azt a literált (és ezáltal az alapját mint paramétert), amely leggyakrabban fordul elő a klózhalmazban. (Mintha egységliterálnak tekintenénk, azaz törtölni lehet az összes olyan klóz, amely tartalmazza a literált, valamint a literál komplementerének előfordulását a fennmaradó klózokból.)
- Válasszuk azt a paramétert, amely a legrövidebb klózokban leggyakrabban fordul elő.

α klasszifikáció

α	α_1	α_2
$\neg\neg A_1$	A_1	
$A_1 \wedge A_2$	A_1	A_2
$\neg(A_1 \vee A_2)$	$\neg A_1$	$\neg A_2$
$\neg(A_1 \supset A_2)$	A_1	$\neg A_2$
$(A_1 \equiv A_2)$	$(A_1 \supset A_2)$	$(A_2 \supset A_1)$

β klasszifikáció

β	β_1	β_2
$\neg(B_1 \wedge B_2)$	$\neg B_1$	$\neg B_2$
$(B_1 \vee B_2)$	B_1	B_2
$(B_1 \supset B_2)$	$\neg B_1$	B_2
$\neg(B_1 \equiv B_2)$	$\neg(B_1 \supset B_2)$	$\neg(B_2 \supset B_1)$

Szemantikai tablók algoritmusa

1. Input: az állításlogika egy A formulája.
2. Output: az A formula T szemantikai tablója (jelölt levélelemekkel)
3. Kezdő állapot: a T szemantikai tablónak egyetlen csúcspontja van (a gyökere), a csúcs címkéje $\{A\}$, a csúcs nem jelölt
4. Legyen l egy nem jelölt csúcspont a $\mathcal{A}(l)$ címkével. Ekkor
    1. ha $\mathcal{A}(l)$ egy literálhalmaz, akkor
        - jelölje $\times$ a csúcspontot, ha $\mathcal{A}(l)$ tartalmaz kiegészítő literálpárt (zárt),
        - jelölje $\circ$ a csúcspontot, ha $\mathcal{A}(l)$ nem tartalmaz kiegészítő literálpárt (nyílt).
    2. ha $\mathcal{A}(l)$ nem egy literálhalmaz, és $C \in \mathcal{A}(l)$ nem literál, akkor a klasszifikáció vezérli a következő lépést.
    3. ha C α-formula, akkor l' az l egyetlen gyermeke és $\mathcal{A}(l') = (\mathcal{A}(l) \setminus \{C\}) \cup \{C_1, C_2\}$
    4. ha C β-formula, akkor l' és l'' az l két gyermeke úgy, hogy $\mathcal{A}(l') = (\mathcal{A}(l) \setminus \{C\}) \cup \{C_1\}$ és $\mathcal{A}(l'') = (\mathcal{A}(l) \setminus \{C\}) \cup \{C_2\}$.

Elsőrendű kiterjesztés

- Literál: zárt atomi formula, valamint zárt atomi formula negációja.
- Klasszifikáció kiterjesztése:
- γ klasszifikáció:

γ	$\gamma(a)$
$\forall x A(x)$	$A(a)$
$\neg\exists x A(x)$	$\neg A(a)$

- δ klasszifikáció:

δ	$\delta(a)$
$\exists x A(x)$	$A(a)$
$\neg\forall x A(x)$	$\neg A(a)$

Herbrand modell

- Függvényszimbólumok használata esetén nehéz megadni/jellemezni a lehetséges interpretációkat.
- Klózok halmazához azonban rendelhetők kanonikus interpretációk: a Herbrand modellek.
- Fő tulajdonság: ha egy klózhalmaznak van modellje, akkor van Herbrand modellje is.
- A Herbrand modellek kulcsszerepet játszanak az elsőrendű rezolúcióban.

Definíció (Herbrand univerzum)

Legyen S egy klózhalmaz, $\mathfrak{A}$ az S-ben előforduló névparaméterek halmaza, $\mathfrak{F}$ az S-ben előforduló függvényszimbólumok halmaza. S Herbrand univerzumát (H_S-t) a következő induktív definíció adja meg:

- Ha $a_i \in \mathfrak{A}$, akkor $a_i \in H_S$;
- Ha $f_i^0 \in \mathfrak{F}$, akkor $f_i^0 \in H_S$;
- Ha $f_i^n \in \mathfrak{F}(n \geq 1)$, $t_j \in H_S$, akkor $f_i^n(t_1, \ldots, t_n) \in H_S$;

Megjegyzés

- Ha S-ben nincs névparaméter vagy 0-argumentumú függvényszimbólum, akkor az induktív definícióban legyen $a \in H_S$ egy tetszőleges névparaméterre.
- A Herbrand univerzum azokat az alapterminusokat tartalmazza, amelyeket az S elemeiből lehet képezni.
- Ha van legalább egy nem 0-argumentumú függvényszimbólum S-ben, akkor a Herbrand univerzum végtelen.

- A rezolúció az automatikus tételbizonyítás alapvető eszközeként jött létre.
- Kiderült, hogy a rezolúció egy megszorított módozata alkalmas programozási feladatok ellátására: ezt valósítja meg a logikai programozás:
  - A program klózok halmazaként jelenik meg.
  - A lekérdezés egy klóz, amely ellentmondhat egy vagy több program klóznak. (Ennek kiderítése a cél.)
  - A lekérdezés valójában a program eredményének a tagadása.
  - Ha a cáfolási eljárás sikeres, akkor a lekérdezés tagadása logikai következménye a programnak.

Logikai háttér

- Program klóz:
  - a megfelelő formula klózformája (azaz az összes változó univerzális kvantifikáció változója);
  - egyetlen pozitív literál ($P(x)$, ez megfelel a $\forall x P(x)$) formulának;
  - $l_1 \wedge l_2 \wedge \cdots \wedge l_n \subset l$ formula univerzális lezártjának megfelelő klózforma, ahol $l_1, \ldots, l_n$ és l pozitív literálok: egyetlen klózt tartalmaz: $\{\neg l_1, \neg l_2, \ldots, \neg l_n, l\}$
- Cél klóz: tegyük fel, hogy be akarjuk bizonyítani, hogy a $g_1 \wedge g_2 \wedge \cdots \wedge g_k$ formula logikai következménye programklózok egy halmazának (ahol g_i pozitív literál).
- Azaz: be kell látni, hogy a programklózok halmaza kiegészítve a $\neg(g_1 \wedge g_2 \wedge \cdots \wedge g_k)$ formulával kielégíthetetlen
- Ez utóbbi formula viszont egy tiszta negatív literálokból álló klóz: $\{\neg g_1, \neg g_2, \ldots, \neg g_k\}$

- Mivel a cél klóz csak negatív literált tartalmaz, így ütközés csak valamely programklózzal lehet.
- A rezolúció elvezethet az üres klózig, ami az eredeti halmaz kielégíthetetlenségét jelenti.
- Első rendben fontos eszköz az unifikáció.

Definíció (Horn klóz)

A legfeljebb egy pozitív literált tartalmazó klózt Horn klóznak nevezzük.

- A pozitív literál a klóz feje.
- A negatív literálok alkotják a klóz testét.
- Tény: a pozitív egység klóz.
- Cél klóz: a pozitív literált nem tartalmazó Horn klóz.
- Program klóz: a pozitív literált és egy vagy több negatív literált tartalmazó Horn klóz

Jelölés

- $B_1 \wedge \cdots \wedge B_n \supset A$ helyett $A \leftarrow B_1, \ldots, B_n$
- Tény: $A \leftarrow$
- Cél klóz: $\leftarrow B_1, \ldots, B_n$
- Kiolvasás:
  - A bizonyításához bizonyítsd be $B_1, \ldots, B_n$-t.
  - A bizonyítása $B_1, \ldots, B_n$ bizonyítását jelenti.
  - A kiszámításához számold ki $B_1, \ldots, B_n$-t.
  - A kiszámítása $B_1, \ldots, B_n$ kiszámítását jelenti.

Definíció

- Az eljárás olyan nem cél Horn klózok halmaza, amelyek fejében ugyanaz a predikátumparaméter szerepel.
- A logikai program eljárások egy halmaza.
- Az adatbázis olyan eljárás, amely csak alaptényekből áll (változókat nem tartalmazó pozitív literálokból).

SLD rezolúció: (Selective Linear Definite (SLD) Resolution)

SLD rezolúció,példa, cél: $\leftarrow Q(y,b), Q(b,z)$

1. $Q(x,y) \leftarrow P(x,y)$
2. $Q(x,y) \leftarrow P(x,z), Q(z,y)$

3.	P(b,a)	5.	P(d,b)	7.	P(f,b)	9.	P(i,h)
4.	P(c,a)	6.	P(e,b)	8.	P(h,g)	10.	P(j,h)

- $Q(y,b)$, klóz 1: $\leftarrow P(y,b), Q(b,z)$
- $P(y,b)$, klóz 5.: $\leftarrow Q(b,z)$, helyettesítés: $\{y \to d\}$
- csak egy literál van, a klóz 1. után: $\leftarrow P(b,z)$
- csak egy literál van, klóz 3. után $\square$, helyettesítés: $\{z \to a\}$

Azaz van egy cáfolatunk a $\leftarrow Q(y,b), Q(b,z)$ cél klózra a $\{y \to d, z \to a\}$ helyettesítéssel. A rezolúció helyessége alapján $Q(d,b) \wedge Q(b,a)$ igaz a P bármely modelljében.

- A cél klóz egy literáljának a kiválasztását meghatározó szabály a számítási szabály.
- Az alkalmazott program klóz kiválasztását meghatározó szabály a keresési szabály.

- Az SLD rezolúció teljes a Horn klózok halmazára nézve (de nem teljes általános esetben).
- Az SLD cáfolat érzéketlen a a számítási szabályok választására.
- Az SLD cáfolat nem vezet mindig eredményre a keresési szabály tetszőleges választása esetén.

Cáfolatok mint számítások?

- Ha adott program klózoknak egy halmaza és egy lekérdezés (egy pozitív literált nem tartalmazó cél klóz formájában), akkor a sikeres cáfolat eredménye egy válasz, amit a megfelelő helyettesítés (unifikáció) ad meg.
- A szokásos programnyelvekben a számítási folyamatot a programozó a program részeként alkotja meg explicit módon.
- A logikai programozás esetén deklaratív formulákat ír a programozó, amelyben az input és output viszonyát rögzíti.
- A rezolúciós következtetési motor egy egységes implicit felügyelő struktúra (azaz a programozónak nem kell explicit módon megadnia).
- A logikai programozás elvonatkoztat a felügyelő struktúrától (pont úgy, ahogy a programozási nyelvek elvonatkoztatnak az explicit memória és regiszter allokációktól, amelyeket meg kell tenni az assembler esetén).

Köszönöm a figyelmet!