УВОД У ЛОГИКУ
први део

Мирјана Борисављевић

Универзитет у Београду
Саобраћајни факултет
Мај 2009

Предговор

Ова књига написана је као уџбеник за део основног курса математичке логике који се бави исказном логиком. Заснива се на предавањима проф. Косте Дошена из предмета Логика, која је држао на Одељењу за филозофију Филозофског факултета Универзитета у Београду почевши од 2002 године.

Трудила сам се да књига буде написана тако да за њено читање није потребно никакво посебно предзнање, осим познавања стандардне средњошколске математике и да буде штиво које ће читаоца упознати са исказном логиком.

Надам се да ће ова књига као помоћни уџбеник бити корисна за курсеве математике техничких факултета који садрже елементе математичке логике као и за курсеве дискретне математике.

Желим да поменем све оне који су ми помогли при раду на овој књизи и да им се захвалим. За свесрдну помоћ нарочиту захвалност дугујем проф. Кости Дошену чији се удео у овој књизи види од концепције курса који је основа ове књиге, до читања текста и драгоцених савета које ми је дао. Захваљујем се и студентима који су слушали курс Логика на Филозофском факултету и чије белешке су ми биле веома корисне. На веома пажљивом читању текста и бројним, изузетно корисним коментарима и сугестијама, најтоплије се захваљујем колеги др Зорану Петрићу. На помоћи и подршци веома сам захвална проф. Слободану Вујошевићу. Колеги др Предрагу Јаничићу захваљујем на коришћењу његовог програма GCLC и великој помоћи при изради слика. Захваљујем се лектору Сањи Миладиновић чије сугестије су ми помогле да побољшам читљивост овог текста, као и Гордани Марјановић која је књигу припремила за штампу.

Београд, 22. мај 2009. године *Аутор*

Садржај

Глава 1

Увод

Предмет логике

Шта је предмет логике, тј. чиме се логика бави? Најуопштенији одговор на ово питање је: логика се бави поступком (процесом) закључивања (расуђивања, извођења). У наставку ћемо, анализирајући шта је то поступак закључивања и које су његове карактеристике, доћи и до прецизнијег одговора на питање шта је предмет логике. Закључивање је један мисаони процес. Тај процес бисмо најједноставније могли објаснити овако. За почетак закључивања потребни су неки подаци (информације), а резултат тог процеса је нови податак. Сваки тај податак (и почетни и резултат) је написан (саопштен, о њему се мисли) на неком природном језику, тј. исказан је реченицом неког природног језика. У закључивањима користимо реченице за које има смисла питати да ли су истините (тачне) или неистините (нетачне). Реченице које имају то својство зову се искази. Дакле, полазимо од неких исказа и поступком закључивања изводимо нови исказ. Полазне исказе зовемо претпоставке (премисе), а резултат закључивања је закључак. Кажемо да из претпоставки следи закључак.

Логика се бави исправним (коректним) закључивањима. Шта су то исправна закључивања? То су закључивања којима се чува истинитост, тј. закључивања за која важи: ако су претпоставке истините, онда и закључак мора бити истинит. Ево примера исправног закључивања.

Пример 1

Пекинг је главни град Кине.

Кина је земља са највише становника на свету.

Дакле, Пекинг је главни град земље са највише становника на свету.

У овом закључивању обе претпоставке су истините и закључак је истинит. Али чување истинитости није једини критеријум за одређивање да ли је неко закључивање исправно. У исправним закључивањима закључак мора да нужно, неоспорно („без остатка") следи из претпоставки. Ево једног закључивања у коме су сви искази истинити, а очигледно је да закључак не следи нужно из претпоставки.

Пример 2

Лимун је воће.

Неке врсте воћа су жуте боје.

Дакле, лимун је жуте боје.

Сада погледајмо следећа закључивања и одговоримо на питање да ли су она исправна.

Пример 3

Иво Андрић је добио Нобелову награду.

Сви досадашњи добитници Нобелове награде били су Руси.

Дакле, Иво Андрић је био Рус.

Пример 4

Амазон је европска река.

Све европске реке се уливају у Јадранско море.

Дакле, Амазон се улива у Јадранско море.

Не дајмо да нас збуне истинитост, односно неистинитост претпоставки и закључка. Ми гледамо цео поступак закључивања и битна нам је само исправност тог поступка. У Примеру 3 имамо да је прва претпоставка тачна, друга је нетачна и закључак је нетачан. Али то јесте једно исправно закључивање. Пратимо само поступак закључивања: из тога да је Иво Андрић добио Нобелову награду и да су сви досадашњи добитници Нобелове награде били Руси, заиста следи да је Иво Андрић био Рус. У Примеру 4 обе претпоставке су нетачне, закључак је нетачан, а ипак имамо исправно закључивање!

Дакле, морамо бити веома опрезни у оценама исправности закључивања. Погледајмо следећи пример.

Пример 5

Пси не лете.

Птице нису пси.

Дакле, птице лете.

Сва три исказа су тачна, али закључак не следи нужно, „без остатка" из претпоставки. Наиме, не следи нужно да оно што има особину *нису пси* има особину *лети*. И мачке нису пси, али не лете!

Рекли смо да предмет логике јесу исправна (коректна) закључивања, али може се рећи да је њен посао и испитивање која закључивања су исправна, а која то нису. У том испитивању морамо раздвојити истинитост и неистинитост претпоставки и закључка од исправности самог поступка закључивања. Поједностављено речено, није битно из чега је закључак изведен и какав је тај закључак, већ је једино важно да ли је правилно изведен. У том поступку („путовању") од претпоставки ка закључку користимо нека правила или упутства. Управо тим „путовањем" од претпоставки до закључка, тј. правилима која чине закључивање, бави се логика. Дакле, задатак логике је да утврди и опише правила по којима се процес закључивања обавља. У процесу закључивања битна нам је исправност правила која се у њему користе, тј. исправност (коректност) правила закључивања. Та правила морају чувати истинитост и по њима закључак нужно, неоспорно мора следити из датих претпоставки. Оваква правила закључивања, која од истинитих претпоставки неоспорно, нужно дају истинити закључак, називају се дедуктивна правила. Закључивања која се састоје од дедуктивних правила су исправна закључивања и зовемо их дедуктивна закључивања (дедуктивна извођења) - дедукције.

Дакле, сада можемо прецизно рећи да су дедукције предмет истраживања логике.

Дедуктивно закључивање је било предмет још традиционалне логике. Аристотел је увео појам премисе и појам нужног следовања закључка из претпоставки. Осим тога, он је утврдио и класификовао разне начине извођења закључка. Али сва његова логичка разматрања и истраживања, као и истраживања настављача његовог дела, била су на неком природном језику, тачније, неком природном језику обогаћеном променљивама. Да бисмо добили бољу прецизност и строгост поступка дедукције, важан је језик на коме се формирају претпоставке, закључци и правила закључивања (дедуктивна правила).

Тек у другој половини XIX века почело је стварање језика логике који ми данас знамо као формални језик логике. У овој књизи ћемо се бавити тим језиком, а овде, у уводу, рецимо само оно најосновније о њему. У том језику постоје посебне речи са сталним значењем, логичке константе. Логичке константе су логички везници: ... *и* ...; ... *или* ...; *ако...*, *онда* ...; ... *ако и само ако...* (... *акко* ...); *не* .... који се изучавају у исказној логици. Логичке константе су и квантификатори (квантори): *сваки* и *неки* који се заједно са везницима изучавају у предикатској логици. Осим логичких константи важна су и дедуктивна правила која чине дедукције и која зовемо и логичка правила (правила

извођења). Свако логичко правило садржи логичке константе, а има и неке делове који су променљиви. Можемо говорити о посебним облицима логичких правила, тј. логичким формама тих правила. Зато се често истиче да се логика бави формалним дедукцијама. Поменућемо једно познато логичко правило, правило *modus ponens*. Нека су X и Y произвољни искази. Правило *modus ponens* је следећег облика:

прва претпоставка: X
друга претпоставка: *Ако је* X, *онда је* Y
закључак: Y

Логичка правила се најчешће записују овако:

$$\frac{P_1, ..., P_m}{Z}$$

где су P_1, ..., P_m претпоставке, а Z је закључак. Рецимо још да су у логици за везник *ако..., онда...* користи симбол $\Rightarrow$, па је правило *modus ponens* правило извођења следећег облика:

$$\frac{X, X \Rightarrow Y}{Y}$$

где X и Y могу бити било који искази.

Логика је добила једнозначан, строг и прецизан језик када се удружила са математиком. Оно што је најзначајнија карактеристика математике (што је потпуно одређује и разликује од других наука) је доказ. Сваки математички доказ је једно дедуктивно закључивање коме су претпоставке истините (или прихваћене као истините). Дакле, логика је повезивањем са математиком добила и плодно тло деловања, тј. почела је да се бави дедукцијама у оквиру математике. Прожимањем логике и математике створена је савремена логика чији почетак су означили радови Џорџа Була (George Boole), и посебно радови Готлоба Фрегеа (Gottlob Frege) у другој половини XIX века. Раздвајање од традиционалне логике представљено је променом имена логика у симболичка логика или математичка логика. Иако осликава важну карактеристику нове логике (рад са симболима новог језика), име симболичка логика није више у широкој употреби. Математика је постала главно поље деловања логике, а логика је постала значајна област математике. Повезивање логике и математике почело је као коришћење логике у математици, а довело је до тога да је логика постала област математике. Отуд и њено, опште прихваћено, име: математичка логика. Данас придев *математичка* постаје сувишан јер, усуђујемо се рећи, данас нема других врста логике осим математичке.

Математичка индукција

У овом одељку ћемо представити једну важну дедуктивну методу закључивања, методу математичке индукције. Природни бројеви и њихове особине имају важну улогу у математичкој индукцији. Скуп чији елементи су сви природни бројеви $0, 1, 2, 3, ...$ је скуп $\mathbf{N}$. Скуп $\mathbf{N}^+$ је скуп природних бројева $\mathbf{N}$ без нуле.

Претпоставимо да имамо исказе

$$I_0, \quad I_1, \quad I_2, \ . \ . \ . \ , \ I_k, \quad . \ . \ .$$

и да је наш задатак да докажемо да су сви ти искази тачни. Другим речима, наш задатак је да докажемо следеће:

За сваки природан број n исказ I_n је тачан.

На пример, нека је наш задатак да докажемо да за све природне бројеве n важи следећа особина: $2^n > n$. У овом конкретном примеру искази

$$I_0, \quad I_1, \quad I_2, \ . \ . \ . \ , \ I_k, \quad . \ . \ .$$

су редом

$$2^0 > 0, \quad 2^1 > 1, \ 2^2 > 2, \ . \ . \ . \ , \ 2^k > k, \quad . \ . \ .$$

и ми морамо да докажемо да су сви ти искази тачни.

Према расуђивању на којем се заснива метода математичке индукције за решавање тог задатка довољно је доказати следеће.
Прво: исказ I_0 је тачан.
Друго: сви искази

Ако I_0, онда I_1.
Ако I_1, онда I_2.
⋮
Ако I_k, онда I_{k+1}.
⋮

су тачни, тј.

за сваки природан број k тачан је исказ: *ако I_k, онда I_{k+1}*.

Ваљаност методе математичке индукције почива на следећем, очигледно исправном расуђивању. Најпре докажимо да је тачан први исказ, исказ I_0. Затим, користећи чињеницу да је тачан исказ I_0, и то да је тачан исказ *ако I_0, онда I_1*, добијамо да је тачан и исказ I_1. Из тачности исказа I_1 и из тачности исказа *ако I_1, онда I_2* закључимо да је тачан I_2. Настављамо, и из тачности исказа I_2 и *ако I_2, онда I_3* закључујемо да је тачан исказ I_3, и тако даље. Дакле, можемо закључити да је за сваки природан број n, исказ I_n тачан.

Расуђивање на којем се заснива метода математичке индукције описано је и следећим примером. Замислимо низ домина које стоје усправно у једном реду и знамо која домина је прва (тј. која домина одговара броју 0). Претпоставимо да знамо следеће: прво, да ће прва домина пасти (тј. да је исказ I_0 тачан) и друго, да ће кад год нека домина падне, онда пасти и домина после ње, њој суседна домина (тј. да је за сваки природан број k исказ *ако I_k, онда I_{k+1}* тачан). Онда исправно закључујемо да ће све домине пасти, без обзира на то колико их има (тј. да су сви искази I_0, I_1, I_2,..., I_k,... тачни).

Методу математичке индукције можемо записати и на следећи начин:

ако је тачан I_0 и за сваки природан број k тачан је исказ: *ако I_k, онда I_{k+1}*,
онда је тачан исказ I_n за сваки природан број n.

Део I_0 зове се база индукције, индукцијски корак је: *ако I_k, онда I_{k+1}*, а његов део I_k се зове индукцијска претпоставка.

Сваки индукцијски корак у овој основној врсти математичке индукције је следећег облика: из тачности исказа за природан број k следи тачност исказа

за природан број $k+1$. Зато ћемо рећи да је тај индукцијски корак прелаз са k на $k+1$.

Докажимо методом математичке индукције једну особину природних бројева.

Пример 1 За сваки природан број n важи:

$$0+1+2+3+...+n=\frac{n\cdot(n+1)}{2}.$$

База индукције. За $n=0$ имамо да је I_0 тачно: $0=\frac{0\cdot(0+1)}{2}$. Дакле, база индукције је тачна.

Сада доказујемо индукцијски корак: *ако* I_k, *онда* I_{k+1}.

У овом примеру индукцијска претпоставка,

I_k, је $\quad 0+1+2+3+...+k=\frac{k\cdot(k+1)}{2}$,

а I_{k+1} је $\quad 0+1+2+3+...+k+(k+1)=\frac{(k+1)\cdot((k+1)+1)}{2}$.

Претпоставимо да важи I_k. Тада је део $0+1+2+3+...+k$ израза $0+1+2+3+...+k+(k+1)$ једнак $\frac{k\cdot(k+1)}{2}$, па имамо

$$\begin{aligned}0+1+2+3+...+k+(k+1)&=\frac{k\cdot(k+1)}{2}+(k+1)\\&=\frac{(k+1)(k+2)}{2}=\frac{(k+1)((k+1)+1)}{2}.\end{aligned}$$

Дакле, важи I_{k+1}, тј. важи индукцијски корак: *ако* I_k, *онда* I_{k+1}.

На основу математичке индукције закључујемо да за сваки природан број n важи: $0+1+2+3+...+n=\frac{n\cdot(n+1)}{2}$.

Приметимо да постоје својства која не важе за неколико првих природних бројева, али важе за све друге природне бројеве, почев од неког природног броја. За нас је важно да се метода математичке индукције користи и за доказивање таквих својстава. У тим случајевима база индукције није I_0, него I_m, где је m први природан број од којег важи та особина.

Ево једног таквог примера.

Пример 2 За сваки природан број n, $n\geq 4$, важи: $3n^2>3n+19$.
Прво приметимо да неједнакост $3n^2>3n+19$ заиста не важи ако је n једнако 0, 1, 2 или 3. Зато је база индукције у овом примеру за $n=4$: $3\cdot 4^2>3\cdot 4+19$, тј. $48>31$ и она је тачна.
Индукцијски корак је:

ако важи $3k^2>3k+19$, онда важи $3(k+1)^2>3(k+1)+19$.

Претпоставимо I_k, тј. да је тачно $3k^2 > 3k + 19$. Тада имамо:

$$\begin{aligned} 3(k+1)^2 &= 3(k^2+2k+1) \qquad (\text{јер је } (a+b)^2 = a^2+2ab+b^2) \\ &= \underline{3k^2} + 6k + 3 \\ &> \underline{3k+19} + 6k + 3 \quad (\text{инд. претп. } 3k^2 > 3k+19) \\ &= 3k + 3 + 19 + 6k \\ &= 3(k+1) + 19 + 6k \\ &\geq 3(k+1) + 19 + 0 \quad (\text{јер је } 6k \geq 0 \text{ за сваки природан број } k) \end{aligned}$$

Дакле, важи: $3(k+1)^2 > 3(k+1)+19$, тј. доказали смо индукцијски корак.

Закључујемо да за сваки природан број n који је једнак или већи од 4 важи: $3n^2 > 3n + 19$.

Заменом n са $n+4$ у неједнакости $3n^2 > 3n + 19$ из Примера 2 добијамо неједнакост $3(n+4)^2 > 3(n+4) + 19$ која је тачна за сваки природан број n. Дакле, имамо својство: за сваки природан број n важи: $3(n+4)^2 > 3n + 31$ и то својство се доказује индукцијом чија база је за $n = 0$.

За правилну примену математичке индукције важно је истаћи међусобну независност следећих услова: (1) тачан је исказ I_0 и (2) за сваки природан број k тачан је исказ: *ако* I_k, *онда* I_{k+1}. Наиме, ниједан од тих услова није последица оног другог. Зато се у доказима у којима се користи математичка индукција морају доказати и база индукције и индукцијски корак. Уколико један део није тачан, онда не можемо да закључимо да је за сваки природан број n тачан исказ I_n. Навешћемо један пример у коме важи индукцијски корак, а не важи база индукције.

Пример 3 Тврђење: *за сваки природан број* n *важи да је број* $2n+1$ *дељив са* 2 није тачно. Међутим, индукцијски корак важи. Наиме, из индукцијске претпоставке: број $2k+1$ је дељив са 2, тј. постоји природан број l тако да је $2k+1 = 2 \cdot l$, следи да је број $2 \cdot (k+1)+1$ дељив са 2. Покажимо то.

$$\begin{aligned} 2 \cdot (k+1) + 1 = 2 \cdot k + 2 + 1 &= \underline{2 \cdot k + 1} + 2 \\ &= \underline{2 \cdot l} + 2 \quad (\text{инд. пр. } 2k+1 = 2 \cdot l) \\ &= 2(l+1). \end{aligned}$$

Дакле, број $2 \cdot (k+1) + 1$ је једнак производу броја 2 и броја $l+1$, тј. дељив је са 2. Тиме смо доказали индукцијски корак. Али шта је са базом? Број $2n+1$ за $n = 0$ је 1 и он сигурно није дељив са 2. Закључујемо да наше тврђење није тачно.

Дакле, мора се водити рачуна да се увек докажу и база индукције и индукцијски корак.

Математичку индукцију можемо посматрати као закључивање чије претпоставке су база индукције и индукцијски корак, а закључак је: *за сваки природан број* n, *исказ* I_n *је тачан.* Истакнимо да су претпоставке и закључак математичке индукције равноправни, тј. да и из њеног закључка можемо извести

њене претпоставке. Наиме, ако важи својство *за сваки природан број* n, I_n *је тачан*, онда:
– за n једнако 0 добијамо да је тачан I_0 и
– за произвољан природан број k и природан број $k+1$ добијамо да су тачни I_k и I_{k+1}, па је тачан и исказ: *ако* I_k, *онда* I_{k+1}.

То значи да важи следеће закључивање:

ако је за сваки природан број n тачан I_n,
онда важи: I_0 је тачан и
за сваки природан број k тачан је исказ: *ако* I_k, *онда* I_{k+1}.

Наравно да у пракси за доказивање разних својстава природних бројева немамо много користи од овог закључивања, јер ако знамо да нека особина важи за сваки природан број n нема потребе да закључујемо да та особина важи за $n = 0$ и да је за сваки природан број k тачно: *ако* I_k, *онда* I_{k+1}.

Сада можемо рећи да смо савладали основни облик математичке индукције и спремни смо да научимо неке врсте математичке индукције. Наиме, постоје тврђења која се доказују методом математичке индукције, али је лакше ако је индукцијски корак облика: из тога да особина важи за неколико бројева пре $k+1$, следи да важи и за $k+1$. Другачије речено, не правимо прелаз са k на $k+1$ већ је потребно направити прелаз са неколико бројева пре $k+1$ на $k+1$. Ево једног таквог примера.

Пример 4 Посматрајмо низ природних бројева дефинисан на следећи начин: $a_0 = 0$, $a_1 = 1$, и $a_{k+1} = 4a_k - 3a_{k-1}$, за $k \geq 1$. Наш задатак је да покажемо да за сваки природан број n важи: $a_n = \frac{3^n - 1}{2}$. Пошто база индукције и индукцијски корак међусобно не зависе, можемо прво да докажемо индукцијски корак. Да бисмо доказали да важи $a_{k+1} = \frac{3^{k+1} - 1}{2}$, довољно је да претпоставимо да важи $a_k = \frac{3^k - 1}{2}$ и $a_{k-1} = \frac{3^{k-1} - 1}{2}$. Тада добијамо:

$$a_{k+1} = 4a_k - 3a_{k-1} = 4 \cdot \frac{3^k - 1}{2} - 3 \cdot \frac{3^{k-1} - 1}{2} = \frac{4 \cdot 3^k - 4 - 3^k + 3}{2} = \frac{3^{k+1} - 1}{2}.$$

Веза $a_{k+1} = 4a_k - 3a_{k-1}$ важи за $k \geq 1$, тј. $k + 1 \geq 2$. То значи да доказани индукцијски корак важи за a_2, a_3,... Остаје нам још да докажемо базу индукције. У овом случају база индукције је провера да особина важи и за a_0 и за a_1: $a_0 = \frac{3^0 - 1}{2} = 0$ и $a_1 = \frac{3^1 - 1}{2} = 1$, што

је по поставци задатка тачно. Закључујемо да за сваки природан број n важи $a_n = \frac{3^n - 1}{2}$.

Овде смо употребили једну методу која на први поглед није иста као метода математичке индукције, али њена исправност почива на истим основама. Наиме, у Примеру 4 закључивање иде овако: *ако* I_0 *и* I_1, *онда* I_2; *ако* I_1 *и* I_2, *онда* I_3 и тако даље. Уопште, ако индукцијски корак има l претпоставки, где је l неки природан број већи од 1, ова метода се може записати на следећи начин:

ако је
база: тачни су $I_0,\ I_1,\ ...,\ I_{l-1}$
и индукцијски корак: за сваки k $(k \geq l - 1 > 0)$ је:
ако $I_{k-(l-1)}$ *и* I_{k-l} *и ... и* I_k, *онда* I_{k+1},
онда је тачан I_n за сваки природан број n.

Важно је истаћи да су за природне бројеве основна врста методе математичке индукције и ова врста математичке индукције међусобно еквивалентне, тј. све што можемо да докажемо једном методом можемо да докажемо и другом, и обрнуто. Међутим, ту еквивалентност није баш једноставно доказати и овде ћемо тај доказ изоставити.

Покажимо, на крају, још једну врсту математичке индукције, потпуну индукцију. Потпуна индукција има следећи облик:

ако је
база: тачан је I_0
и индукцијски корак: за сваки природан број k важи:
ако I_0 *и ... и* I_{k-1}, *онда* I_k,
онда је тачан I_n за сваки природан број n.

У наредном примеру ћемо користити потпуну индукцију.

Пример 5 Докажимо следеће тврђење.
За сваки природан број n *једнак или већи од* 2, *важи:* n *је или прост број или је производ простих бројева.*
База индукције, $n = 2$: број 2 је или прост или је производ простих бројева. Број 2 је прост, па имамо да је база индукције тачна.
Сада доказујемо индукцијски корак. Посматрамо произвољан природан број k и задатак нам је да покажемо да из претпоставке да за све бројеве мање од k важи да су или прости или производи простих бројева следи да је онда и сам број k или прост број или производ простих бројева. Ако је k прост, онда је посао завршен и индукцијски корак важи. Ако пак k није прост, онда је k производ нека два природна броја l_1 и l_2 који су сигурно мањи од k: $k = l_1 \cdot l_2$ и $l_1, l_2 < k$. Како су бројеви l_1 и l_2 мањи од k, то за њих важи индукцијска претпоставка, па су l_1 и l_2 или прости или производи простих бројева. То значи да је онда и број $k = l_1 \cdot l_2$ производ простих бројева. Тако је доказан индукцијски корак.

> Закључујемо, на основу потпуне индукције, да је сваки природан број n, који је једнак или већи од 2, или прост број или производ простих бројева.

Потпуна индукција подсећа на претходну врсту математичке индукције. У претходној врсти математичке индукције индукцијским кораком се (за $l > 1$) прелази са $k-(l-1)$, $k-l$,..., k на $k+1$, тј. индукцијска претпоставка је да особина важи за неколико бројева мањих од $k+1$, а у потпуној индукцији индукцијски корак је прелаз са 0, 1, 2,..., $k-1$ на k, тј. индукцијска претпоставка је да особина важи за све бројеве мање од k. Истакнимо (без доказивања те особине) да су потпуна индукција и раније представљене две врсте математичке индукције еквивалентне.

Рецимо на крају да ће потпуна индукција бити најчешћа метода за доказивање тврђења која ћемо представити у наредним одељцима ове књиге.

Дефиниције

Слободније речено, дефиницијом се уводе (кажемо, дефинишу) нови појмови неке теорије помоћу полазних или већ дефинисаних појмова те теорије. Најважније је истаћи да се у некој теорији поступком дефинисања не утврђују неке нове истине те теорије, већ се само уводе нови појмови, користећи познате (већ постојеће) појмове те теорије.

Погледајмо следеће реченице:

Квадрат је *правоугаоник чије су све четири странице једнаке.*

Паран број је *природан број који је дељив бројем 2.*

Ове реченице можемо сматрати типичним примерима дефиниција. Свака дефиниција садржи два истакнута дела, definiendum (део који се дефинише) и definiens (део којим се дефинише). Прва реченица је дефиниција појма *квадрат* у геометрији, а друга је дефиниција појма *паран број* у аритметици. У дефиницији квадрата ми претпостављамо да већ имамо дефинисан појам правоугаоника, појам странице правоугаоника, појам дужи и једнакост дужи. Слично је и са дефинисањем парног броја. Познат је појам природног броја и појам дељивости неког природног броја бројем 2.

Веома прецизан појам дефиниције ће се јавити у оквиру изучавања формалног језика логике. Међутим, нама ће већ за увођење тог формалног језика и његових формула бити потребне дефиниције. Због тога ћемо у овом одељку рећи само нешто најосновније о поступку прављења исправних (коректних) дефиниција.

Вратимо се дефиницији парног броја. Можемо рећи да реченица *број је паран* и реченица *број је природан и дељив бројем 2* саопштавају исто. Зато смо дефиницију парног броја могли записати на следећи начин:

Паран број је замена за *природан број који је дељив бројем 2.*

Уопште, сваку дефиницију можемо формулисати у облику

$$A \text{ је замена за } B,$$

где је A definiendum, а B definiens.

Али са дефинисањем морамо бити веома опрезни. Наведимо два услова која треба да испуњава исправна (коректна) дефиниција новог појма неке теорије.

(услов 1, Паскалов услов) Дефиниција мора бити отклоњива, тј. свака реченица у којој се појављује нови појам може бити замењена са више реченица (или само једном) у којима се појављују само стари појмови, тј. они који су полазни или већ дефинисани.

(услов 2) Дефиниција мора бити конзервативна (или некреативна), тј. не смеју се, користећи ту дефиницију, извести нека тврђења која се без ње иначе не би могла извести у тој теорији.

Ова правила значе да нови појам који се дефинише у некој теорији мора заиста да буде нов и само замена за већ постојеће (отклоњивост), као и да он ни на који начин не сме утицати на теореме које већ важе (конзервативност).

У одељку о предмету логике поменули смо логички везник *акко* (*ако и само ако*). Везник *акко* или једнакост користимо за повезивање definiendum-а са definiens-ом. Наиме, дефиницију парног броја можемо и овако формулисати.

Број је паран акко по дефиницији *тај број је природан и дељив са 2*.

У нашим дефиницијама ми ћемо део „акко по дефиницији" записивати: AKKO. Осим тога користићемо и „једнако по дефиницији" што ћемо записивати: $=_{def}$.

Представимо сада једну важну врсту дефиниција, индуктивне дефиниције. Прво погледајмо један пример.

Пример 1 Како можемо да дефинишемо степеновање неког реалног броја a произвољним бројем n из скупа $\mathbf{N}^+$, тј. a^n за произвољан број n из скупа $\mathbf{N}^+$? Имамо дефиницију следећег облика:
(1) $a^1 = a$;
(2) $a^{n+1} = a^n \cdot a$ и
(3) a^n се може дефинисати само коначном применом (1) и (2) ове дефиниције.

Ово је пример једне индуктивне дефиниције. Понекад је потребно дефинисати бесконачан скуп објеката исте врсте. Најопштије речено, ако је то такав скуп да се његови сложенији објекти граде помоћу једноставнијих, онда се користе индуктивне дефиниције. Индуктивна дефиниција неког бесконачног скупа S нових објеката има облик:
(1) Дефинишу се најједноставнији (полазни) објекти који припадају скупу S.
(2) Дефинише се поступак којим се помоћу објеката који су у скупу S праве нови објекти тог скупа.
(3) Одређује се да скупу S припадају само они објекти који се могу добити применом (1) и (2).

Погледајмо дефиницију из Примера 1 у светлу овог најопштијег облика индуктивне дефиниције. Потребно је дефинисати бесконачан скуп чији елементи су сви степени неког реалног броја a: a^1, a^2,... Прво смо дефинисали елемент a^1

тог скупа, степен броја a првим бројем скупа $\mathbf{N}^+$ (део (1)). Затим смо дефинисали како се помоћу a^n и a, који су већ у скупу S, прави његов нови елемент a^{n+1} (део (2)). Коначно, делом (3) одређујемо да се елементи скупа S могу направити само на начине представљене у деловима (1) и (2).

Истакнимо да ће у наредној глави ове књиге дефиниције веома важних појмова, на пример појма исказне формуле, бити индуктивне дефиниције.

Скупови, релације, функције и операције

У наредним одељцима ћемо, уз одређен степен строгости, увести следеће појмове: скуп, релацију, функцију и операцију, трудећи се да читалац задржи интуитивну слику коју је о тим појмовима стекао у досадашњем школовању.

Скупови

Колико год нама појам скупа и појам елемента неког скупа изгледали природни и колико нам се чинило да их је лако дефинисати, они се у математици сматрају основним појмовима који се не дефинишу. Наравно постоји опште прихваћена интуитивна слика скупа као груписања (окупљања) објеката са одређеним својством (особином) С. Ти објекти који формирају скуп су елементи тог скупа. Важно је рећи да у овом интуитивном поимању скупа ограничења за својство С и за објекте, који могу бити елементи неког скупа, просто не постоје. Дакле, појам скупа и појам елемента скупа схватамо веома слободно и широко. Та слобода нас доводи до тога да својство С може бити, на пример, *број дељив са 7*, па скуп чине сви цели бројеви дељиви са 7. Али С може бити и *број није дељив са 7*, тј. објекте можемо окупљати и по својству да немају неку особину. Исто тако С може бити својство *бити скуп*, па би ова малопре поменута два скупа била елементи скупа задатог тим својством. Дакле, то би био скуп чији елементи су скупови. Ако тако слободно хоћемо да дефинишемо скуп, онда то ствара парадоксе. Навешћемо Раселов парадокс.

Раселов парадокс

Видели смо да по овом интуитивном опису скупа елементи скупа могу бити и скупови. Посматрајмо зато скуп R чији су елементи сви скупови X који нису сами себи елементи, тј. сви скупови X који имају особину: X није елемент скупа X. Да ли има таквих скупова? Рећи ћемо: да, има. На пример, скуп F чији елементи су филозофи јесте један такав скуп. Наиме, сам скуп F није филозоф, па није елемент себе самог и припада скупу R. Да ли има скупова који не припадају скупу R? Опет ћемо рећи: има. Скуп M који окупља све што није књига и сам није књига, па је елемент себе самог и не припада скупу R. Намеће се следеће, као што ћемо видети, јако

опасно питање: шта је са самим скупом R, да ли је он елемент скупа R, тј. самог себе? Имамо две могућности: или R јесте елемент скупа R или R није елемент скупа R.
Ако скуп R јесте елемент скупа R, онда скуп R мора имати својство које имају сви елементи скупа R, а то је: R није елемент самога себе, тј. скуп R није елемент скупа R! Али ово је у супротности са нашом полазном претпоставком да скуп R јесте елемент скупа R.
Добро, онда мора важити да:
скуп R није елемент скупа R. Али то тачно значи да скуп R има својство на основу кога смо окупљали скупове и правили скуп R. Скуп R, као скуп са тим својством, мора да буде елемент скупа R и опет смо добили контрадикцију!
Дакле, слобода да било којим својством можемо формирати скуп довела нас је до тога да смо направили скуп R чије елементе не можемо да одредимо.

Видимо да не можемо допустити да је скуп свако груписање објеката са било којим својством и да елемент скупа може бити било шта, само да има то својство. Област математике која се бави скуповима, теорија скупова, појам скупа и појам елемента узима за основне појмове и заснована је строго формално као једна формална теорија са својим аксиомама и правилима извођења. (У одељку 3.1 ове књиге даћемо дефиницију формалне теорије, а у другом делу ове књиге, делу Увод у логику II, биће представљена аксиоматска теорија скупова).

Пример 1 Од скупова бројева већ смо помињали скуп природних бројева, скуп **N**. Имамо још скуп целих бројева **Z**; скуп рационалних бројева **Q**; скуп реалних бројева **R** и скуп комплексних бројева **C**.

У овом уводу о скуповима рецимо да реченицу *x је елемент скупа X* математички записујемо на следећи начин $x \in X$, а реченица *x није елемент скупа Y* има математички запис $x \notin Y$ што је скраћеница за *није да* $x \in Y$. На крају поменимо празан скуп као скуп који нема ниједан елемент. Празан скуп ћемо означавати са $\emptyset$.

Подскуп

Када говоримо о подскупу у ствари говоримо о односу нека два скупа. Посматрајмо два скупа, на пример скупове X и Y. Да би скуп Y био подскуп скупа X морају сви елементи скупа Y да буду елементи и скупа X. Скуп парних бројева је подскуп скупа природних бројева **N** јер је сваки паран број и природан број. Интересантно је посматрати случај када је Y баш скуп X и случај када је Y празан скуп. Имамо да сваки скуп X јесте подскуп самог себе, као и да за произвољан скуп X празан скуп јесте један његов подскуп.

Дакле, ако за елементе скупова X и Y важи да је сваки елемент скупа Y елемент и скупа X, онда кажемо да је скуп Y подскуп скупа X, у ознаци $Y \subseteq X$.

У наредном примеру ћемо указати на замку у коју можемо упасти са тако једноставним и природним појмовима као што су скуп и подскуп.

Пример 2 Посматрајмо скупове $A = \{1, 2\}$ и $B = \{\{1\}, \{2\}, \{3\}\}$. Да ли је скуп A подскуп скупа B? Ако смо брзоплети можемо размишљати овако: 1 је елемент скупа A и $\{1\}$ је елемент скупа B; даље, 2 је елемент скупа A и $\{2\}$ је елемент скупа B; и након тога на наше питање ћемо одговорити: ДА. Али ако пажљиво погледамо елементе ова два скупа видимо да је елемент скупа A број 1, а елемент скупа B је скуп $\{1\}$, а то није исто. Елементи скупа A су бројеви, а елементи скупа B су скупови! Закључујемо да скуп A није подскуп скупа B.

Два скупа X и Y су једнака, у ознаци $X = Y$, ако је скуп X подскуп скупа Y и скуп Y подскуп скупа X. Другим речима, два скупа X и Y су једнака ако и само ако имају исте елементе.

Сада знамо шта је подскуп и шта значи једнакост скупова, па можемо да уведемо и појам: бити прави подскуп. Ако је скуп Y подскуп скупа X и скуп Y није једнак скупу X, онда кажемо да је скуп Y прави подскуп скупа X. Прави подскуп Y скупа X означавамо $Y \subset X$. На пример, скуп природних бројева $\mathbf{N}$ је прави подскуп скупа целих бројева $\mathbf{Z}$.

Посматрајмо само коначне скупове, тј. скупове чији је број елемената неки природан број. Овде ћемо само за коначне скупове увести појмове: кардинални број и партитивни скуп.

Кардинални број скупа X је број његових елемената, а означаваћемо га са $card(X)$.

Када говоримо о подскуповима неког скупа X намеће се задатак да направимо све његове подскупове. Након тога, можемо посматрати скуп чији су елементи сви подскупови тог скупа X. Тај се скуп назива партитивни скуп скупа X, а обележава $\mathcal{P}X$. Погледајмо следећи једноставан пример.

Пример 3 Посматрајмо скуп $X = \{a, b, c\}$. Наведимо све његове подскупове. Прво, $\emptyset$ је подскуп од X. Подскупови скупа X који имају један елемент су: $\{a\}$, $\{b\}$ и $\{c\}$. Двочлани подскупови скупа X су: $\{a, b\}$, $\{a, c\}$ и $\{b, c\}$. На крају, скуп X има само један подскуп са три елемента, а то је сам скуп $X = \{a, b, c\}$. Дакле, имамо да је $\mathcal{P}X = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Интересантно је видети колико елемената има скуп $\mathcal{P}X$. Скуп $\mathcal{P}X$ има 8 елемената, тј. кардинални број скупа $\mathcal{P}X$ је 8, $card(\mathcal{P}X) = 8$. Приметимо да важи: $card(\mathcal{P}X) = 2^3 = 2^{card(X)}$.

Може се показати да ова веза кардиналних бројева из Примера 3 важи за сваки скуп X и његов партитивни скуп $\mathcal{P}X$. Дакле, за кардинални број неког скупа X, $card(X)$, и кардинални број његовог партитивног скупа $\mathcal{P}X$, $card(\mathcal{P}X)$, важи: $card(\mathcal{P}X) = 2^{card(X)}$.

Унија, пресек и разлика скупова. Декартов производ скупова

У овом одељку ћемо се подсетити добро познатих појмова: пресека, уније, разлике и Декартовог производа скупова.

Пресек скупова X и Y, у ознаци $X \cap Y$, јесте скуп свих елемената z из X и Y таквих да z припада скупу X и z припада скупу Y.

Пример 4 За скупове $X = \{a, \{b, c\}, \{d\}, \{b\}\}$ и $Y = \{\{a\}, \{b\}, \{c\}, \{d\}\}$, имамо да је $X \cap Y = \{\{d\}, \{b\}\}$.

Специјално, ако је пресек два скупа X и Y празан скуп, тј. $X \cap Y = \emptyset$, онда за скупове X и Y кажемо да су дисјунктни скупови. На пример, пресек скупа парних бројева и скупа непарних бројева је празан скуп. Та два скупа су дисјунктни скупови.

Унија скупова X и Y, у ознаци $X \cup Y$, јесте скуп свих елемената z из X и Y таквих да z припада скупу X или z припада скупу Y.

За X и Y из Примера 4, имамо да је $X \cup Y = \{a, \{b, c\}, \{d\}, \{b\}, \{a\}, \{c\}\}$.

Можемо посматрати унију и пресек више од два скупа, унију и пресек скупова $X_1, X_2, ..., X_n$, где је n неки природан број већи од 2. Пресек скупова $X_1, X_2, ..., X_n$ је скуп свих елемената z из тих скупова који припадају сваком од скупова $X_1, X_2, ..., X_n$. Тај пресек краће записујемо $\cap_{i=1}^{n} X_n$. Унија скупова $X_1, X_2, ..., X_n$ је скуп свих елемената z из тих скупова који припадају неком од скупова $X_1, X_2, ..., X_n$. Ту унију записујемо $\cup_{i=1}^{n} X_n$.

Погледајмо неке особине које важе за скупове и њихове уније и пресеке. Потпуно је јасно да су скупови $X \cup Y$ и $Y \cup X$ једнаки као скупови, тј. да важи: $X \cup Y = Y \cup X$. Такође важи: $X \cap Y = Y \cap X$. Имамо још да за било које скупове X, Y и Z важи следеће:

$$(X \cap Y) \cap Z = X \cap (Y \cap Z) \qquad (X \cup Y) \cup Z = X \cup (Y \cup Z)$$
$$(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z) \qquad (X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$$
$$X \cap X = X \qquad X \cup X = X$$
$$X \cap (Y \cup X) = X \qquad X \cup (Y \cap X) = X$$

Разлика скупова X и Y, у ознаци $X \setminus Y$, јесте скуп свих елемената из скупа X који не припадају скупу Y.

За скупове X и Y, из Примера 4, имамо скуп $X \setminus Y = \{a, \{b, c\}\}$ и скуп $Y \setminus X = \{\{a\}, \{c\}\}$.

Посебно ако је скуп Y подскуп скупа X, $Y \subseteq X$, онда се разлика $X \setminus Y$ зове комплемент скупа Y у односу на скуп X, и то ћемо означавати са $C_X Y$ (или $\overline{Y}$ ако је јасно о ком скупу X је реч).

Пример 5 Посматрајмо скуп природних бројева $\mathbf{N} = \{0, 1, 2, 3, ...\}$ и скуп целих бројева $\mathbf{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. Скуп $\mathbf{N}$ је подскуп скупа $\mathbf{Z}$, па је $\mathbf{N} \cup \mathbf{Z} = \mathbf{Z}$ и $\mathbf{N} \cap \mathbf{Z} = \mathbf{N}$. Разлика $\mathbf{N} \setminus \mathbf{Z}$ је наравно празан скуп. Како је $\mathbf{N} \subset \mathbf{Z}$, онда важи $\mathbf{Z} \setminus \mathbf{N} = C_{\mathbf{Z}}\mathbf{N}$ и тај скуп чине сви негативни цели бројеви, $C_{\mathbf{Z}}\mathbf{N} = \{-1, -2, -3, ...\}$.

Увели смо разлику скупова, па можемо навести још неке особине које важе за било које скупове X, Y и Z. ($\overline{X}$ и $\overline{Y}$ су комплементи редом скупова X и Y у односу на неки скуп X_1.)

$$X \setminus (Y \cap Z) = (X \setminus Y) \cup (X \setminus Z) \qquad X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z)$$
$$\overline{X \cap Y} = \overline{X} \cup \overline{Y} \qquad \overline{\overline{X}} = X \qquad \overline{X \cup Y} = \overline{X} \cap \overline{Y}$$

Сада ћемо увести још један веома важан појам теорије скупова и целе математике, појам уређеног пара. За два објекта a и b, уређени пар објеката a и b (или уређена двојка) је скуп $\{\{a\}, \{a, b\}\}$. Уређени пар објеката a и b означавамо (a, b), где је битно да је a први, а да је b други члан тог уређеног пара. На исти начин можемо увести уређену тројку (a, b, c), уређену четворку (a, b, c, d) и тако даље. За различите елементе a и b важи $\{a, b\} = \{b, a\}$, али за те различите елементе уређен пар (a, b) није једнак уређеном пару (b, a). Осим тога, ако су објекти a и b једнаки не говоримо о скупу $\{a, a\}$, али постоји уређен пар (a, a). Једнакост уређених парова дефинишемо на следећи начин:

$$(a, b) = (c, d) \qquad \text{АККО} \qquad a = c \text{ и } b = d.$$

Користећи појам уређеног пара, уводимо веома важну врсту скупова, Декартов производ два скупа.

Декартов производ скупова X и Y у ознаци $X \times Y$, јесте скуп свих уређених парова (x, y) таквих да x припада скупу X и y припада скупу Y.

За један скуп X Декартов производ $X \times X$ краће записујемо X^2. Одмах приметимо да из карактеристике уређеног пара, да је важан редослед његових чланова, добијамо следећу особину Декартовог производа: ако скупови X и Y нису једнаки, онда скупови $X \times Y$ и $Y \times X$ нису једнаки.

Као и за унију и пресек, постоји и Декартов производ скупова X_1, X_2,..., X_n, где је n неки природан број већи од 2. Правимо све могуће n-торке $(x_1, x_2, ..., x_n)$ у којима је први елемент из првог скупа, тј. $x_1 \in X_1$, други елемент је из другог скупа, тј. $x_2 \in X_2$, и тако даље све до $x_n \in X_n$. Скуп чији су елементи све n-торке $(x_1, x_2, ..., x_n)$, где је $x_1 \in X_1$, $x_2 \in X_2$, ..., $x_n \in X_n$, јесте Декартов производ скупова $X_1, X_2, ..., X_n$ у ознаци $X_1 \times X_2 \times ... \times X_n$. За неки скуп X Декартов производ $X \times X \times ... \times X$ (где се скуп X појављује n пута) краће записујемо X^n.

Релације

Излагање о релацијама почнимо примерима из обичног живота. На пример, реченицом *Јован је старији од Николе*, представљена је релација између два човека *...је старији од...*. Из овог записа се види да та релација тражи два објекта, па кажемо да је бинарна. Ево једне релације за коју нам треба три учесника: *... је град у држави ... на континенту ....* Питамо се: како правимо неку релацију? На пример, како ћемо из неког скупа људи L издвојити парове који су у релацији *...је старији од...*. Прво направимо све могуће уређене парове од људи из тог скупа L (тј. направимо скуп $L \times L$), а онда издвојимо оне парове које чине два човека, тако да је први из тог пара старији од другог. Сви ти

уређени парови праве један подскуп скупа $L \times L$, подскуп σ, за који кажемо да је једна бинарна релација на скупу L. Важно је рећи да смо могли, правећи подскуп скупа $L \times L$ по неком другом својству, на пример, *...је нижи од...*, да добијемо исти подскуп σ скупа $L \times L$. У поимању релације ми занемарујемо разлику између својстава која су нас довела до подскупа σ скупа $L \times L$ и говоримо о релацији σ на скупу L.

Дакле, подскуп Декартовог производа $X \times X$, скуп ρ, $\rho \subseteq X \times X$, назива се бинарна релација ρ на скупу X.

Једна од основних бинарних релација је релација једнакости: $=$. У математици имамо једнакост два броја и једнакост два скупа (о чему смо већ говорили). Како је свака бинарна релација неки скуп, онда је и релација $=$ један скуп. Међутим, за нека два објекта x и y који су једнаки никада не пишемо $(x, y) \in =$, него пишемо $x = y$. И за било коју бинарну релацију ρ, особину да су x и y у релацији ρ, тј. $(x, y) \in \rho$ записиваћемо и на следећи начин: $x \; \rho \; y$. У одељку о скуповима осим релације једнакости скупова, помињали смо и релације *...је подскуп од...* и *...је прави подскуп од...*.

Приметимо да наши примери релације *...је старији од...* и *...је подскуп од...* јесу подскупови Декартовог производа $X \times X$ неког скупа X. Наиме, те релације су бинарне и оба члана из пара су исте врсте: два човека, два скупа. Међутим, шта је са релацијом *... је град у држави... на континенту ...*? Сада ћемо представити и такву врсту релација и још неке друге врсте.

Бинарна релација између елемената скупа X и скупа Y Може се увести и бинарна релација између елемената скупова који нису једнаки. Подскуп Декартовог производа $X \times Y$ је бинарна релација између елемената скупа X и скупа Y.

> Пример 1 Имамо скуп $X = \{$Петроград, Београд, Лондон, Париз$\}$ и скуп $Y = \{$Ермитаж, Лувр$\}$. Једна бинарна релација ρ између елемената скупа X и скупа Y је дефинисана на следећи начин: $(x, y) \in \rho$ АККО *x је град у коме се налази музеј y*, тј. ρ је подскуп $\{$(Петроград, Ермитаж), (Париз, Лувр)$\}$ скупа $X \times Y$.

Релација дужине n ($n > 2$) на скупу X Може се на једном скупу, неком скупу X, осим бинарне увести и нека релација дужине 3, 4,... У општем случају за природан број n већи од 2 подскуп ρ скупа X^n, $\rho \subseteq X^n$, јесте релација дужине n на скупу X. Напоменимо да се за неку релацију ρ дужине веће од два и неку n-торку $(x_1, ..., x_n)$ која је у релацији ρ, осим записа $(x_1, ..., x_n) \in \rho$, користи и запис $\rho(x_1, ..., x_n)$.

> Пример 2 Имамо скуп $X = \{$Петроград, Београд, Лондон, Париз$\}$ из Примера 1. Једна релација дужине 3 на скупу X је подскуп скупа X^3 дефинисан на следећи начин: $(x_1, x_2, x_3) \in \rho$ АККО *град x_2 има више становника од града x_1, а мање од града x_3.*

Унарна релација на скупу X Било који подскуп ρ скупа X је релација дужине 1 на скупу X, унарна релација на скупу X. Свака унарна релација на неком

скупу X се у ствари односи на неко својство елемената скупа X (ако ништа друго на својство да припадају подскупу који чини ту релацију). Наиме, унарна релација разврстава елементе тог скупа на оне који имају неку особину, и оне друге који ту особину немају.

> Пример 3 Посматрамо скуп природних бројева $\mathbf{N}$ и особину природних бројева *бити паран*. Подскуп скупа $\mathbf{N}$ који окупља све парне бројеве је једна унарна релација на скупу природних бројева $\mathbf{N}$.

Релација дужине n ($n > 2$) између елемената скупова $X_1, ..., X_n$ Може се претпоставити у ком правцу води ово уопштавање појма релације. За неки природан број n већи од 2 подскуп ρ скупа $X_1 \times ... \times X_n$ (међу којима може бити и једнаких), $\rho \subseteq X_1 \times ... \times X_n$, јесте релација дужине n између елемената скупова $X_1, ..., X_n$.

> Пример 4 За скупове G = {Сремски Карловци, Пекинг, Лима}, D = {Србија, Француска, Перу, Кина} и K = {Азија, Европа, Јужна Америка, Аустралија} релација γ: *...је град државе... на континенту...*, коју смо већ помињали, јесте релација дужине 3 између елемената скупова G, D и K, тј. $\gamma \subseteq G \times D \times K$. Договор о запису за релацију дужине n ($n > 2$) на неком скупу X важи и за релације ове врсте. На пример, писаћемо (Сремски Карловци, Србија, Европа)$\in \gamma$ или γ(Сремски Карловци, Србија, Европа).

Особине бинарних релација

На почетку овог одељка даћемо два примера бинарних релација на неком скупу и користећи њихове особине представићемо важне особине бинарних релација.

> Пример 5 Имамо скуп кога чине неколико светских престоница: P = {Москва, Париз, Мадрид, Лисабон, Лима, Пекинг, Техеран, Хараре, Каиро}. Дефинишимо следеће две бинарне релације на скупу P:
>
> $p_1 \ \sigma \ p_2$ AKKO *град* p_1 *и град* p_2 *су на истом континенту*;
>
> $p_1 \ \varrho \ p_2$ AKKO p_1 *је у држави која је суседна држави у којој је град* p_2.

У Примеру 5 за сваки град p важи да је он заједно са самим собом на истом континенту, тј. за сваки град p важи да је у релацији σ са самим собом: $p \ \sigma \ p$. Што се тиче релације ϱ ниједан град p није у релацији ϱ са самим собом, тј. не важи $p \ \varrho \ p$. Особина коју има релација σ назива се рефлексивност, а релација која има ту особину је рефлексивна релација. Наиме, за бинарну релацију ρ на скупу X кажемо да је рефлексивна када за сваки елемент x скупа X важи $x \ \rho \ x$.

У математици постоји пуно рефлексивних релација: једнакост бројева, једнакост скупова, паралелност правих у равни, подударност (на пример, троуглова у некој равни), релација $\leq$ на неком скупу бројева (на пример, на скупу

природних бројева), релација подскуп $\subseteq$ на неком скупу чији елементи су скупови. Приметимо да само малом изменом релације $\leq$, изостављањем једнакости, добијамо релацију $<$ која није рефлексивна. Потпуно исто важи и за прелазак са релације $\subseteq$ на релацију прави подскуп $\subset$.

Која је следећа особина коју бисмо волели да има бинарна релација? То је особина да не морамо да водимо рачуна о редоследу навођења два елемента који су у тој релацији. Ако кажемо *x је у релацији ρ са y* да то одмах значи и да је *y у релацији ρ са x*, и просто можемо рећи *x и y су у релацији ρ*. Та особина се зове симетричност. За бинарну релацију ρ на скупу X кажемо да је симетрична када за свака два елемента x и y скупа X важи: ако је $x \,\rho\, y$, онда је $y \,\rho\, x$.

Погледајмо наше релације σ и ϱ на скупу P из Примера 5. Да ли су оне симетричне? Одговор је: да. Дефинишимо релацију τ на скупу P која није симетрична: $p_1 \,\tau\, p_2$ АККО *град p_1 има већи број становника од града p_2*. Очигледно τ није симетрична релација.

Каква је ситуација са нашим математичким релацијама по питању симетричности? Малопре помињане релације: једнакост бројева, једнакост скупова, паралелност правих у равни, подударност, осим што су рефлексивне оне су и симетричне. Међутим, релације $\leq$ и $\subseteq$ нису симетричне. На пример, за скуп природних бројева $\mathbf{N}$ и скуп реалних бројева $\mathbf{R}$ важи $\mathbf{N} \subseteq \mathbf{R}$, али не важи $\mathbf{R} \subseteq \mathbf{N}$.

Да бисмо представили још једну важну особину бинарних релација на неком скупу, останимо код примера релације једнакости. Познато је својство једнакости да ако утврдимо да је неки објекат x једнак објекту y и да је y једнак неком објекту z, онда закључујемо да је x једнак z, тј. важи: ако је $x = y$ и $y = z$, онда је $x = z$. Та особина назива се транзитивност. За бинарну релацију ρ на скупу X кажемо да је транзитивна када за свака три елемента x, y и z скупа X важи: ако је $x \,\rho\, y$ и $y \,\rho\, z$, онда је $x \,\rho\, z$.

Погледајмо сада наше релације σ и ϱ на скупу P из Примера 5. Да ли су оне транзитивне? Релација σ јесте транзитивна. Међутим, релација ϱ није транзитивна. Заиста, важи (Лисабон, Мадрид)$\in \varrho$ и (Мадрид, Париз)$\in \varrho$ (јер се градови које чине те парове налазе у суседним државама), али не важи (Лисабон, Париз)$\in \varrho$.

Од математичких релација које смо већ помињали транзитивне релације су и паралелност правих у равни, подударност, $\leq$, $<$, $\subseteq$ и $\subset$.

А сада представимо особину бинарне релације за коју можемо сликовито рећи да је супротна особини симетричности и тако ћемо је и звати антисиметричност. Наиме, та особина каже да ако је x у релацији ρ са y и x није y, онда нема симетричности, тј. онда y није у релацији ρ са x. Дакле, за бинарну релацију ρ на скупу X кажемо да је антисиметрична када за свака два елемента x и y скупа X важи: ако је $x \,\rho\, y$ и $y \,\rho\, x$, онда је $x = y$.

Погледајмо опет наше релације σ и ϱ из Примера 5. Ниједна од њих није антисиметрична. Ево образложења за релацију σ. За свака два града са једног континента p_1 и p_2 важи $p_1 \,\sigma\, p_2$ и $p_2 \,\sigma\, p_1$, али p_1 и p_2 могу бити два различита града и не мора да важи $p_1 = p_2$.

Две најпознатије математичке антисиметричне релације су релација $\leq$ и релација $\subseteq$. Очигледно је да ако за два броја x и y важи $x \leq y$ и $y \leq x$, онда мора да је $x = y$. Посматрајмо сада релацију $\subseteq$. Заиста, ако за два скупа X и Y важи $X \subseteq Y$ и $Y \subseteq X$, онда важи $X = Y$.

Врсте бинарних релација. Појам дрвета.

У овом одељку ћемо представити две најзначајније врсте бинарних релација на неком скупу X: релације еквиваленције и парцијалног уређења.

Бинарна релација ρ на скупу X која је рефлексивна, симетрична и транзитивна назива се релација еквиваленције.

Најчешће ознаке за релацију еквиваленције су $\sim$ или $\equiv$.

Које математичке релације су релације еквиваленције? То су, већ више пута помињане, једнакост, паралелност правих у равни и подударност (на пример, троуглова у некој равни). Шта је са релацијама σ, ϱ и τ на скупу P из Примера 5? Релација σ је релација еквиваленције, а ϱ и τ то нису. Останимо код релације σ и посматрајмо један елемент скупа P, неки град p_1. Природно је око града p_1 окупити све градове из P који су са градом p_1 у релацији σ, тј. све градове који су на истом континенту на коме и град p_1. Тај поступак, у општем случају за неки скуп X, један његов произвољан елемент x и релацију еквиваленције $\sim$ на скупу X изгледа овако: правимо скуп кога чине сви елементи скупа X који су у релацији $\sim$ са елементом x. Тај скуп се назива класа еквиваленције елемента x у односу на релацују $\sim$ и обележава се $[x]$ (или $\overline{C_x}$). Дакле, елемент скупа $[x]$ је сваки елемент y скупа X, за који важи $x \sim y$.

За релацију σ и наш град p_1 из скупа P, класа еквиваленције елемента p_1 у односу на релацују σ је скуп $[p_1]$, а чине га сви градови из P који су на истом континенту на коме је град p_1. На овај начин сваки град p из P добија своју класу еквиваленције, скуп $[p]$. Приметимо да, на пример, ако је град p_1 у Европи, онда $[p_1]$ чине сви градови из P који су у Европи.

Шта можемо да кажемо о особинама класа $[p]$ за градове p из скупа P. Прво, ниједна класа $[p]$ није празан скуп, јер бар град p припада својој класи $[p]$. Друго, ако посматрамо две класе еквиваленције, $[p_1]$ и $[p_2]$, оне могу да буду или једнаке или дисјунктне. Јасно је да су класе $[p_1]$ и $[p_2]$ једнаке када су p_1 и p_2 на истом континенту. Оне су дисјунктне када p_1 и p_2 нису на истом континенту. Наиме, ако би у том случају класе $[p_1]$ и $[p_2]$ имале заједнички елемент то би значило да је тај град на континенту на коме је град p_1 и на континенту на коме је град p_2, али то је немогуће јер се ниједан град из скупа P не налази на два континента. Треће, ако направимо унију класа еквиваленције свих градова из P: $[p_1] \cup ... \cup [p_9]$, где претпостављамо да су $p_1, ..., p_9$ сви градови из скупа P и тај скуп означимо $\bigcup_{p \in P}[p]$, онда имамо да је та унија једнака самом скупу P, тј. важи $\bigcup_{p \in P}[p] = P$.

Важно је рећи да ове три особине, које имају класе еквиваленције релације еквиваленције σ из Примера 5, имају и класе еквиваленције сваке релације еквиваленције $\sim$. Покажимо то.

Задатак 1 Нека је $\sim$ релација еквиваленције на неком скупу X. Покажимо да тада за класе еквиваленције релације $\sim$ важи:
(1) за сваки елемент x скупа X класа $[x]$ је непразан скуп, $[x] \neq \emptyset$;
(2) за сваке две класе еквиваленције $[x]$ и $[y]$ важи или да су једнаке, $[x] = [y]$, или да су дисјунктне, $[x] \cap [y] = \emptyset$;
(3) унија свих класа релације еквиваленције $\sim$, унија $\cup_{x \in X}[x]$, јесте једнака скупу X.
(1) Релација $\sim$ је релација еквиваленције, па је рефлексивна: $x \sim x$. Значи, $x \in [x]$, тј. $[x] \neq \emptyset$.
(2) За свака два елемента x и y скупа X важи: или су x и y у релацији $\sim$ (симетричност релације $\sim$ нам дозвољива да овако формулишемо однос ова два елемента) или x и y нису у релацији $\sim$. Ако су елементи x и y у релацији $\sim$, тј. $x \sim y$, онда покажимо да важи: $[x] = [y]$. Покажимо да је $[x] \subseteq [y]$. Нека је $z \in [x]$, тј. $x \sim z$. Из $x \sim y$, на основу симетричности релације $\sim$, добијамо $y \sim x$. Сада из $y \sim x$ и $x \sim z$, на основу транзитивности релације $\sim$ добијамо $y \sim z$, тј. $z \in [y]$. Дакле, важи $[x] \subseteq [y]$. На исти начин показује се да важи $[y] \subseteq [x]$, па имамо $[x] = [y]$. Ако елементи x и y нису у релацији $\sim$, онда би требало показати да су класе $[x]$ и $[y]$ дисјунктне. То ћемо показати тако што ћемо полазећи од претпоставке да класе $[x]$ и $[y]$ нису дисјунктне, добити контрадикцију. Значи наша претпоставка је: класе $[x]$ и $[y]$ нису дисјунктне. Тада, класе $[x]$ и $[y]$ имају бар један заједнички елемент, неки елемент z: $z \in [x]$ и $z \in [y]$. На основу дефиниције класе еквиваленције имамо да за елемент z важи: $x \sim z$ и $y \sim z$. Користимо симетричност релације $\sim$, па из $y \sim z$ закључујемо $z \sim y$. Сада користимо транзитивност релације $\sim$, па из $x \sim z$ и $z \sim y$ закључујемо да важи $x \sim y$. Али, то је немогуће јер је у супротности са нашом полазном претпоставком да x и y нису у релацији $\sim$. Дакле, наша претпоставка довела нас је до закључка који је нетачан. То значи да та претпоставка није тачна, тј. да је тачна њена негација: класе $[x]$ и $[y]$ су дисјунктне.
(3) Да бисмо показали једнакост скупова X и уније свих $[x]$, скупа $\cup_{x \in X}[x]$, треба показати да је X подскуп те уније и да је та унија подскуп скупа X. Прво показујемо $X \subseteq \cup_{x \in X}[x]$. Узмимо произвољан елемент скупа X, елемент y. Треба показати да је y елемент скупа $\cup_{x \in X}[x]$. Елемент y припада својој класи еквиваленције релације $\sim$, класи $[y]$, па тиме и скупу $\cup_{x \in X}[x]$ који је унија свих таквих класа, дакле, $X \subseteq \cup_{x \in X}[x]$. Сада још остаје да покажемо да је $\cup_{x \in X}[x]$ подскуп скупа X, мада је то очигледно. Наиме, скуп $\cup_{x \in X}[x]$ чине елементи скупа X, па је сваки елемент из $\cup_{x \in X}[x]$ очигледно и елемент скупа X. Дакле, из $X \subseteq \cup_{x \in X}[x]$ и $\cup_{x \in X}[x] \subseteq X$ добили смо да важи $X = \cup_{x \in X}[x]$.

За неку релацију еквиваленције $\sim$ на скупу X посматрајмо скуп чији су елементи класе еквиваленције релације $\sim$ свих елемената из X. Тај скуп се

означава $X/_\sim$ и назива се количнички скуп (или партиција) скупа X и његове релације еквиваленције $\sim$.

Количнички скуп скупа P из Примера 5 и његове релације еквиваленције σ, скуп $P/_\sigma$, чине класе еквиваленције од којих свака класа садржи градове једног континента. Стога је број елемената скупа $P/_\sigma$ број континената који имају бар један свој град у скупу P.

У наредном примеру показаћемо како се помоћу класа неке релације еквиваленције могу дефинисати важни појмови.

Пример 6 Већ смо рекли да је релација паралелности правих у једној равни рефлексивна, симетрична и транзитивна. Дакле, то је једна релација еквиваленције на скупу свих правих једне равни. Погледајмо шта су класе еквиваленције ове релације. Једну класу еквиваленције чине све међусобно паралелне праве те равни. Појам правца у равни се дефинише као једна класа еквиваленције релације паралелности (видети[14]).

Друга значајна врста бинарних релација на неком скупу X је релације парцијалног уређења. Бинарна релација ρ на скупу X која је рефлексивна, антисиметрична и транзитивна назива се парцијално уређење.

Најзначајније математичке релације парцијалног уређења су релација $\leq$ на неком скупу бројева, на пример на скупу природних бројева и релација $\subseteq$ на неком скупу чији су елементи скупови.

Поред релација еквиваленције и парцијалног уређења поменимо и предуређење. Бинарна релација ρ на скупу X која је рефлексивна и транзитивна назива се предуређење.

На крају овог одељка представићемо једну важну бинарну релацију на неком скупу, релацију дрво, коју ћемо у даљем излагању често користити.

Дрво

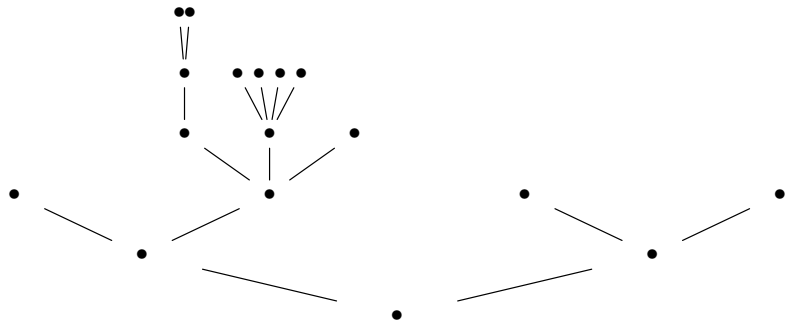
Посматрајмо произвољан непразан скуп X. Елементе скупа X зовемо чворови. Скуп X и бинарна релација δ на скупу X, $\delta \subseteq X \times X$, чине једно дрво δ ако сваки елемент (x_1, x_2) релације δ (чији први члан x_1 зовемо претходник, а други члан x_2 наследник) задовољава следеће услове:

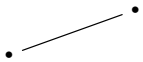
(1) Постоји тачно један чвор x_0 скупа X, такав да скуп δ нема елемент облика (y, x_0), тј. ниједан елемент скупа δ као други члан нема тај чвор x_0. Другачије речено, постоји тачно један чвор x_0 скупа X који нема претходника. Тај чвор x_0 зовемо корен.

(2) Ако важи $(x_1, y), (x_2, y) \in \delta$ тј. $x_1 \delta\, y$ и $x_2 \delta\, y$, онда је $x_1 = x_2$. Или другачије, сваки чвор y, који није корен x_0, има тачно једног претходника.

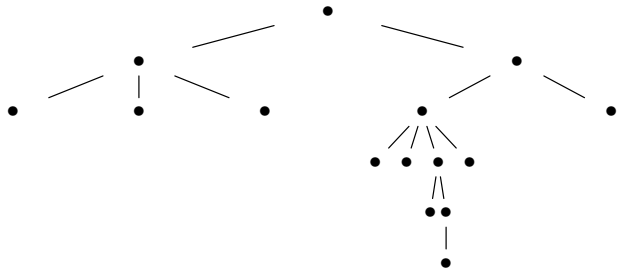
(3) За сваки чвор y, осим корена x_0, постоји јединствен низ чворова $x_0, ..., x_m$ (за неко $m \geq 0$) таквих да важи: $x_0\, \delta\, x_1$,..., $x_{m-1} \delta\, x_m$, $x_m \delta\, y$. Другачије речено, за сваки чвор y, осим корена x_0, постоји јединствена грана од корена x_0 до тог чвора y.

Ако скуп X има коначан број чворова, онда дрво δ зовемо коначно дрво. Коначно дрво се завршава чворовима који немају наследника и те чворове зовемо листови. Дрво графички може бити представљено на следећи начин:

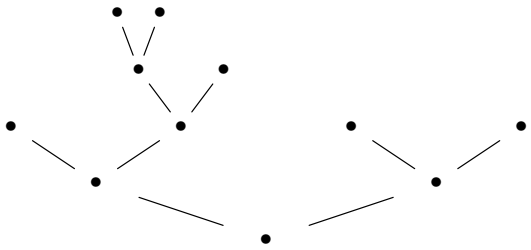


где су чланови једног пара из δ представљени овако  и претходник је доња тачка, а наследник горња. Једно гранање у дрвету δ на скупу X чине сви елементи (x_i, y_i) из δ ($1 \leq i \leq m$ за $m \geq 1$) који имају исти први члан, неки елемент x из скупа X, $x_i = x$, $1 \leq i \leq m$, тј. сви ти парови су облика (x, y_i), $1 \leq i \leq m$. Ако је дрво представљено као на овој слици, онда елемент x зовемо доњи чвор гранања, а све друге чланове тих парова, тј. све y_i, $1 \leq i \leq m$, зовемо горњи чворови гранања.

Дрво може бити представљено и на овај начин са кореном на врху.



Истакнимо и једну посебну врсту дрвета, бинарно дрво. Дрво чији сваки чвор, осим листова, има тачно два наследника зовемо бинарно дрво. Ево једног коначног бинарног дрвета.



Функције

У свим књигама елементарне математике излагање о функцијама почиње цртежом на коме су два облачка од којих један представља неки скуп X, а други скуп Y. У облачку X истакнута је тачка са именом x, у облачку Y истакнута је тачка која има име y. Једна закривљена линија полази из тачке x, а завршава се стрелицом у тачки y и изнад те линије пише f. Уз ту слику иде једно овакво објашњење: правило (договор, закон) f по коме се сваком елементу x скупа X додељује тачно један елемент y скупа Y назива се функција скупа X у скуп Y. Затим следи један пример којим се илуструју ови подвучени захтеви: сваком елементу из X додељује се тачно један елемент из Y. Овакав један пример.

Пример 1 Посматрајмо скупове $X = \{$Петроград, Београд, Лондон, Париз, Беч$\}$, $Y = \{$Лувр, Ермитаж, Британски музеј, Прадо, Музеј града Беча$\}$ и $Z = \{$Нева, Сава, Дунав, Темза, Сена, Волга$\}$.
(1) Питамо се да ли је договором *граду x додељујемо музеј у који се налази у том граду* дефинисана једна функција из скупа X у скуп Y? Одговор је: НЕ. Зашто? Таквим договором једном елементу скупа X (Београду) није додељен ниједан музеј у скупу Y, тј. није сваком елементу из X додељен неки елемент из Y. Да ли може да се нешто промени да би овај наш договор ипак био једна функција? Одговор је потврдан. Треба да мало променимо скупове. Наиме, можемо направити скуп X_1 избацивањем елемента Београд из скупа X, $X_1 = X \setminus \{$Београд$\} = \{$Петроград, Лондон, Париз, Беч$\}$. Придруживање елементима из X_1 елементе скупа Y по направљеном договору јесте једна функција из скупа X_1 у скуп Y. Могућа је и другачија промена. Можемо да не мењамо скуп X, али да проширимо скуп Y додавањем, на пример, Музеја Николе Тесле, $Y_1 = Y \cup \{$Музеј Николе Тесле$\}$. Опет је наш договор једна функција, али сада из X у скуп Y_1.
(2) Питамо се да ли је договором *граду x се додељује река z из скупа Z која кроз њега протиче* дефинисана једна функција скупа X у скуп Z? Проблем из (1) сада не постоји. Сваки од градова из скупа X лежи на некој реци из скупа Z. Али, Београд (опет Београд) лежи на две реке! Овим договором Београду се додељују и Сава и Дунав! То значи да се једном елементу скупа X (Београду) на тај начин додељују два елемента скупа Z, а не тачно један. Да ли и овде постоји могућност поправке? Да, треба само да прецизирамо договор. Наиме, договор треба да гласи *граду x се додељује најдужа река z из скупа Z која кроз њега протиче.* Овим договором Београду се додељује само Дунав. Штавише, и сваком другом граду из скупа X се додељује тачно једна река из скупа Z. Значи, овај нови договор јесте функција из скупа X у скуп Z.

Ми појам функције уводимо на следећи начин.

Посматрајмо скупове X и Y. Подскуп f Декартовог производа $X \times Y$, $f \subseteq X \times Y$, који задовољава следеће услове:
(1ф) скуп свих првих чланова уређених парова (x, y) из f једнак је скупу X;
(2ф) ако два уређена пара (x_1, y_1) и (x_2, y_2) из скупа f имају једнаке прве чланове, тј. ако је $x_1 = x_2$, онда и други чланови тих уређених парова морају бити једнаки, тј. мора бити $y_1 = y_2$;
назива се функција f из скупа X у скуп Y.

Шта је, дакле, функција из скупа X у скуп Y? То је подскуп Декартовог скупа $X \times Y$ који задовољава услове (1ф) и (2ф), или то је једна бинарна релација између елемената скупова X и Y која задовољава услове (1ф) и (2ф). Елементи функције f су уређени парови (x, y) код којих је први члан x оригинал (прва компонента, аргумент), а други члан је слика од x функцијом f (друга компонента, вредност функције f у тачки x) и пишемо $y = f(x)$. Скуп X је домен функције f, а скуп Y је њен кодомен.

> Пример 2 Посматрајмо скупове $A = \{a, b, c\}$ и $B = \{1, 2, 3, 4, 5\}$. Једна функција f из скупа A у скуп B је на пример следећи подскуп Декартовог производа $A \times B$: $f = \{(a, 3), (b, 1), (c, 4)\}$.

За функцију f из скупа X у скуп Y направимо подскуп скупа Y који чине други чланови свих уређених парова скупа f. Тај скуп се зове скуп вредности функције f и обележава се са $f(X)$. Дакле, скупу $f(X)$ припада сваки елемент y скупа Y за који постоји неки елемент x из скупа X, такав да је $y = f(x)$.

Наведимо један пример у коме ћемо користити и уобичајени запис реченице: f је функција из скупа X у скуп Y, $f : X \to Y$.

> Пример 3 Посматрајмо скуп реалних бројева $\mathbf{R}$ и дефинишимо функцију $f : \mathbf{R} \to \mathbf{R}$ следећим записом $f(x) = x^2$.
> Који елементи скупа $\mathbf{R}$ чине скуп $f(\mathbf{R})$? Елементи скупа $f(\mathbf{R})$ су реални бројеви z из скупа $\mathbf{R}$ који су једнаки квадрату неког реалног броја x, $z = f(x) = x^2$. Значи, имамо да је $f(\mathbf{R})$ скуп свих ненегативних (нуле и свих позитивних) реалних бројева који означавамо $\mathbf{R}^+$.

Одговоримо на питање: када су две функције f и g једнаке? Функције су скупови, зато њихову једнакост проверавамо тако што проверавамо једнакост тих скупова.

> Задатак 1 Покажимо да ако две функције f и g имају исти домен и за сваки елемент x тог домена важи $f(x) = g(x)$, онда су функције f и g једнаке. Задатак нам је да покажемо да су скупови f и g једнаки, тј. да је $f \subseteq g$ и $g \subseteq f$. Функције f и g имају исти домен и зато прве компоненте њихових елемената чине исти скуп. Сада прво покажимо да је $f \subseteq g$. Нека је $(x, y) \in f$. Тада је $y = f(x)$. Из $f(x) = g(x)$ имамо $(x, y) = (x, f(x)) = (x, g(x))$ и како $(x, g(x))$ припада g, закључујемо да $(x, y) \in g$. На сличан начин се показује да

је сваки елемент (x, y) из g елемент и f, тј. $g \subseteq f$, стога закључујемо да је $f = g$.

Покажимо које особине једна функција не мора да има. Погледајмо следећи пример.

Пример 4 Посматрајмо скупове X и Z из Примера 1. Дефинишимо бинарну релацију f за елементе тих скупова. За $x \in X$ и $z \in Z$: xfz АККО *најдужа река која протиче кроз* x *је* z. Ова релација је подскуп $f = \{$(Петроград, Нева), (Париз, Сена), (Београд, Дунав), (Беч, Дунав), (Лондон, Темза)$\}$ скупа $X \times Y$. Тај подскуп f јесте једна функција из скупа X у скуп Y јер су задовољена оба услова (1ф) и (2ф). Заиста, услов (1ф) јесте задовољен јер скуп који чине први чланови елемената овог скупа је читав скуп X. Али, приметимо да скуп који чине други чланови елемената овог скупа, скуп $f(X)$, није читав скуп Y. Наиме, $f(X) = Y \setminus \{$Сава, Волга$\}$. Закључујемо да за функцију не мора да важи: $f(X) = Y$. Услов (2ф) јесте задовољен јер f нема парова са истим првим, а различитим другим чланом. Међутим, погледајмо парове (Београд, Дунав) и (Беч, Дунав). Они имају различите прве чланове, а други чланови су им исти. Закључујемо да за елементе $(x_1, f(x_1))$ и $(x_2, f(x_2))$ из f не мора да важи: ако је $x_1 \neq x_2$, онда је $f(x_1) \neq f(x_2)$.

Одмах рецимо да неке функције могу имати особине које смо поменули у Примеру 4. Функција $f : X \to Y$ чији је скуп вредности, скуп $f(X)$, једнак скупу Y назива се сурјекција. Функција $f : X \to Y$ за чија свака два елемента $(x_1, f(x_1))$ и $(x_2, f(x_2))$ важи да ако је $x_1 \neq x_2$, онда је $f(x_1) \neq f(x_2)$ назива се инјекција. Приметимо да услов „ако је $x_1 \neq x_2$, онда је $f(x_1) \neq f(x_2)$" можемо да искажемо: „ако је $f(x_1) = f(x_2)$, онда је $x_1 = x_2$", па смо тако добили још један начин да запишемо особину функције: бити инјекција.

Пример 5 Погледајмо поново функцију из Примера 3, функцију $f : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2$. Да ли је функција f сурјекција, тј. да ли је $f(\mathbf{R}) = \mathbf{R}$? Већ смо показали да је $f(\mathbf{R}) = \mathbf{R}^+$, па је наш одговор на ово питање: НЕ. Да ли је функција f инјекција? Опет је одговор: НЕ. Да би f била инјекција, морале би слике различитих бројева из $\mathbf{R}$ да буду различити бројеви у $f(\mathbf{R})$. Али ми за функцију f имамо да су слике два различита броја, на пример 2 и -2, исти број, број 4: $f(-2) = (-2)^2 = 4$ и $f(2) = 2^2 = 4$.

Ако је нека функција $f : X \to Y$ и сурјекција и инјекција, онда она припада веома важној врсти функција, она је бијекција.

Посматрајмо начас само коначне скупове и сетимо се појма кардиналног броја неког скупа. Погледајмо шта добијамо једном бијекцијом $f : X \to Y$ између коначних скупова X и Y. Имамо да је f функција, зато је скуп првих компоненти њених парова једнак скупу X. Даље, функција f је инјекција,

па сви парови морају имати и различите друге компоненте, а оне су елементи скупа Y. Из овог можемо закључити да скуп Y мора имати елемената бар колико и X, а можда и више, тј. $card(X) \leq card(Y)$. Коначно функција f је сурјекција, зато $Y = f(X)$, тј. скуп X сигурно има елемената колико и скуп Y, а можда и више. Дакле, $card(X) \leq card(Y)$ и $card(Y) \leq card(X)$, па закључујемо: $card(X) = card(Y)$, тј. скупови X и Y имају исти број елемената. То значи да ако постоји бијекција $f : X \to Y$ између коначних скупова X и Y, онда ти скупови имају једнак број елемената, тј. $card(X) = card(Y)$. Желимо да истакнемо да се лепота и важност бијекције за одређивање кардиналног броја види тек међу бесконачним скуповима. Од бесконачних скупова овде ћемо поменути само пребројиве скупове, бесконачне скупове чији кардинални број је једнак кардиналном броју скупа природних бројева $\mathbf{N}$.

Свака функција f из скупа $\mathbf{N}$ у неки скуп X прави један бесконачан низ елемената скупа X. Наиме, функцијом $f : \mathbf{N} \to X$ добијамо следећи бесконачан низ елемената скупа X: $f(0)$, $f(1)$, $f(2)$,..., те елементе означавамо редом f_0, f_1, f_2,... и зовемо их чланови низа. Ако је функција f бијекција, онда ћемо за скуп X рећи да је пребројив. Сликовито речено, та бијекција нам говори да скуп X има исти број елемената као скуп $\mathbf{N}$. Напоменимо да нека константна функција $f : \mathbf{N} \to X$, која сваки природан број n слика у исти елемент x скупа X, прави један бесконачан низ x, x,... чији су сви чланови једнаки.

Уведимо и појам коначног низа елемената неког скупа. Посматрајмо неки скуп X и коначан подскуп скупа $\mathbf{N}^+$ облика $\{1, ..., n\}$ за неки $n \in \mathbf{N}^+$. Свака функција $g : \{1, ..., n\} \to X$ дефинише један коначан низ елемената скупа X, низ g_1,..., g_n, где је g_1 његов први члан, и тако даље до члана g_n који је последњи, n-ти, члан тог низа.

А сада поменимо још један појам везан за домен функције.

Нека је дата функција $f : X \to Y$ и један подскуп скупа X, скуп X_1. Дефинишемо функцију $g : X_1 \to Y$ на следећи начин: за сваки елемент x скупа X_1, $g(x)$ је по дефиницији једнака $f(x)$. Функција g се зове рестрикција функције f на скуп X_1 и то се записује $g = f\,|_{X_1}$.

Вратимо се сада функцији $f : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2$ (из Примера 3 и Примера 5) и посматрајмо подскуп $\mathbf{R}^+$ скупа $\mathbf{R}$ и рестрикцију функције f на тај скуп, функцију $g : \mathbf{R}^+ \to \mathbf{R}$, $g(x) = x^2$. Коју особину има функција g, а нема функција f? Функција g је инјекција, а функција f то није.

Композиција функција

Као и за појам функције постоји описно представљање шта је композиција две функције $f : X \to Y$ и $g : Y \to Z$. Произвољан елемент x скупа X има слику $f(x)$ у скупу Y. Затим, елемент $f(x)$ скупа Y има слику $g(f(x))$ у скупу Z. На тај начин добили смо једну функцију из скупа X у скуп Z, којом сваки елемент x скупа X добија слику $g(f(x))$ у скупу Z.

За три скупа X, Y и Z и две функције $f : X \to Y$ и $g : Y \to Z$ композиција функција f и g, у ознаци $g \circ f$, јесте функција из скупа X у скуп Z таква да за

сваки елемент x скупа X важи: $g \circ f(x) = g(f(x))$. Другачије речено, $g \circ f$ је подскуп скупа $X \times Z$ чији елементи су сви уређени парови облика $(x, g(f(x)))$, $x \in X$. Представимо то на једном примеру.

Пример 6 Посматрајмо скупове $L = \{a, b, c\}$, $B = \{1, 2, 3, 4, 5\}$ и $K = \{\text{A}, \text{B}, \text{C}, \text{D}\}$ и функције $f : L \to B$ и $g : B \to K$:

$$f = \{(a, 1), (b, 4), (c, 5)\} \text{ и } g = \{(1, \text{A}), (2, \text{C}), (3, \text{B}), (4, \text{A}), (5, \text{D})\}.$$

Композиција функција f и g је функција $g \circ f$ из скупа L у скуп K:

$$g \circ f(a) = g(f(a)) = g(1) = \text{A}$$
$$g \circ f(b) = g(f(b)) = g(4) = \text{A}$$
$$g \circ f(c) = g(f(c)) = g(5) = \text{D}$$

или другачије:

$$g \circ f = \{(a, \text{A}), (b, \text{A}), (c, \text{D})\}.$$

Приметимо да у Примеру 6 није могуће направити функцију $f \circ g$. Али ако посматрамо функције $f, g : X \to X$, онда постоје и композиција $f \circ g$ и композиција $g \circ f$. У том случају намеће се питање: да ли важи једнакост $f \circ g = g \circ f$? Погледајмо следећи пример.

Пример 7 Имамо скуп $K = \{\text{A}, \text{B}, \text{C}, \text{D}\}$ и функције $f : K \to K$ и $g : K \to K$:

$$f = \{(\text{A}, \text{C}), (\text{B}, \text{D}), (\text{C}, \text{B}), (\text{D}, \text{A})\} \text{ и } g = \{(\text{A}, \text{A}), (\text{B}, \text{A}), (\text{C}, \text{B}), (\text{D}, \text{D})\}.$$

У овом примеру постоје и функција $g \circ f$ и функција $f \circ g$:

$$g \circ f = \{(\text{A}, \text{B}), (\text{B}, \text{D}), (\text{C}, \text{A}), (\text{D}, \text{A})\} \text{ и } f \circ g = \{(\text{A}, \text{C}), (\text{B}, \text{C}), (\text{C}, \text{D}), (\text{D}, \text{A})\}.$$

Очигледно је да су $g \circ f$ и $f \circ g$ две различите функције.

На питање: да ли за произвољне функције $f, g : X \to X$ важи $g \circ f = f \circ g$ овим примером смо дали одговор. Одговор је: НЕ. Али, једна друга особина важи за композицију функција. Ако имамо три функције $h : A \to B$, $g : B \to C$ и $f : C \to D$, играјући се заградама можемо формирати две композиције: композицију $(f \circ g) \circ h$ и композицију $f \circ (g \circ h)$. Поставља се питање: да ли су ове две композиције једнаке као функције? Одговор је: ДА. То значи да се заграде могу избрисати и просто писати $f \circ g \circ h$.

Задатак 2 Посматрајмо три функције $h : A \to B$, $g : B \to C$ и $f : C \to D$. Показаћемо да су функције $(f \circ g) \circ h$ и $f \circ (g \circ h)$ једнаке. Први услов је да функције чију једнакост испитујемо морају имати исти домен. Тај услов је испуњен, домен и функције $(f \circ g) \circ h$ и функције $f \circ (g \circ h)$ је скуп A. Морамо показати да за сваки елемент x скупа A важи: $((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x)$. Узећемо произвољан елемент скупа A и показати да је његова слика функцијом $(f \circ g) \circ h$ једнака његовој слици функцијом $f \circ (g \circ h)$. Из особине да се те две функције поклапају на једном произвољном (било којем) елементу

скупа A, следи да се оне поклапају на сваком елементу скупа A. За произвољан елемент x скупа A имамо:

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))).$$

С друге стране имамо,

$$f \circ (g \circ h)(x) = f((g \circ h)(x)) = f(g(h(x))).$$

Показали смо да за произвољан елемент x скупа A важи:

$$((f \circ g) \circ h)(x) = (f \circ (g \circ h))(x).$$

Дакле, функције $(f \circ g) \circ h$ и $f \circ (g \circ h)$ су једнаке.

Погледајмо још једну врсту функција које су веома важне за композицију функција. За било који скуп X дефинишемо функцију $i_X : X \to X$ на следећи начин: $i_X(x) = x$. Функцију i_X називамо идентичка функција скупа X. За произвољну функцију $f : X \to Y$ и идентичку функцију $i_X : X \to X$ важи:

$$f \circ i_X = f.$$

Инверзна функција

Описно и не баш прецизно, појам инверзне функције за произвољну функцију $f : X \to Y$ би био представљен на следећи начин. Посматрајмо један оригинал, неки елемент x скупа X и његову слику функцијом f, елемент $f(x)$ скупа Y. Оригинал x је функцијом f отишао у $f(x)$. Намеће се питање о враћању слике у свој оригинал. Да ли постоји функција из скупа Y у скуп X која враћа $f(x)$ у x? Ако таква функција постоји, онда је она инверзна функција функције f. Другим речима, композиција функције f и ове функције било који елемент x скупа X слика у њега самог.

Посматрамо неку функцију $f : X \to Y$. Ако за ту функцију f постоји функција $g : Y \to X$, таква да је функција $g \circ f$ идентичка функција на скупу X и да је функција $f \circ g$ идентичка функција на скупу Y, тј. да важи:

$$g \circ f = i_X \quad \text{и} \quad f \circ g = i_Y,$$

тада је g инверзна функција функције f и њена ознака је f^{-1}.

Приметимо да се не тврди да све функције имају инверзну функцију. На питање које функције имају инверзну функцију, одговорићемо у следећем задатку.

Задатак 3 Ако је функција $f : X \to Y$ бијекција, онда она има јединствену инверзну функцију f^{-1}. Том функцијом сваки елемент y скупа Y има вредност x из скупа X за који важи $f(x) = y$, тј. њени парови су облика $(f(x), x)$.
Покажимо да важи ова особина. Посматрамо подскуп Декартовог производа $Y \times X$, који ћемо означити са f^{-1}, чији су елементи парови $(f(x), x)$ за све елементе x скупа X. Да ли је тај подскуп једна функција из Y у X? Да би био задовољен услов (1ф) мора скуп свих првих чланова уређених парова из f^{-1} бити једнак скупу Y.

Тај скуп је скуп $f(X)$, а како је f сурјекција имамо $f(X) = Y$ тј. услов (1ф) је задовољен. Што се тиче услова (2ф) посматрајмо два елемента тог скупа који имају исти први члан: (y, x_1) и (y, x_2). По дефиницији функције f^{-1} имамо $y = f(x_1)$ и $y = f(x_2)$, па добијамо да важи $f(x_1) = f(x_2)$. Функција f је инјекција, па из $f(x_1) = f(x_2)$ закључујемо да је $x_1 = x_2$. Дакле, посматрани подскуп задовољава и услов (2ф). Добијамо да f^{-1} јесте једна функција из скупа Y у скуп X. Посматрајмо сада функције $f^{-1} \circ f$ и $f \circ f^{-1}$. Домен функција $f^{-1} \circ f$ и i_X је скуп X, а за произвољан елемент x скупа X имамо: $f^{-1} \circ f(x) = f^{-1}(f(x)) = x = i_X(x)$. Дакле, функције $f^{-1} \circ f$ и i_X су једнаке. На потпуно исти начин се показује да су функције $f \circ f^{-1}$ и i_Y једнаке. Закључујемо да функција f^{-1} јесте једна инверзна функција функције f. Да бисмо показали јединственост функције f^{-1} претпоставимо да постоји још једна функција g, $g : Y \to X$, за коју важи $g \circ f = i_X$ и $f \circ g = i_Y$. Тада важи $f^{-1} \circ f = g \circ f = i_X$ и $f \circ f^{-1} = f \circ g = i_Y$ и добијамо:

$$\begin{aligned}
f^{-1} = f^{-1} \circ i_Y &= f^{-1} \circ (f \circ f^{-1}) && \text{(јер је } f \circ f^{-1} = i_Y\text{)} \\
&= (f^{-1} \circ f) \circ f^{-1} && \text{(особина композиције функција)} \\
&= (g \circ f) \circ f^{-1} && \text{(јер је } f^{-1} \circ f = g \circ f\text{)} \\
&= g \circ (f \circ f^{-1}) && \text{(особина композиције функција)} \\
&= g \circ i_Y = g && \text{(јер је } f \circ f^{-1} = i_Y\text{)}
\end{aligned}$$

Дакле, функција f^{-1} је једнака функцији g, па имамо јединственост инверзне функције f^{-1}.

Пример 8 Погледајмо опет функцију коју смо посматрали у Примеру 3 и Примеру 5, функцију $f : \mathbf{R} \to \mathbf{R}$, $f(x) = x^2$. У Примеру 5 смо показали да f није сурјекција нити инјекција. Дефинисали смо рестрикцију функције f на скупу $\mathbf{R}^+$ функцију $g : \mathbf{R}^+ \to \mathbf{R}$, $g(x) = x^2$ која је инјекција и $g(\mathbf{R}^+) = \mathbf{R}^+$. Сада посматрајмо функцију $h : \mathbf{R}^+ \to \mathbf{R}^+$, $h(x) = x^2$. Функција h је бијекција, дакле, постоји функција $h^{-1} : \mathbf{R}^+ \to \mathbf{R}^+$ за коју важи:

$$h^{-1} \circ h = i_{\mathbf{R}^+} \quad \text{и} \quad h \circ h^{-1} = i_{\mathbf{R}^+}.$$

То значи да за произвољан елемент x из $\mathbf{R}^+$ важи:

$$h^{-1} \circ h(x) = h^{-1}(h(x)) = h^{-1}(x^2) = x$$

и

$$h \circ h^{-1}(x) = h(h^{-1}(x)) = (h^{-1}(x))^2 = x.$$

Закључујемо да је h^{-1} позната корена функција, $h^{-1}(y) = \sqrt{y}$. (Ако хоћемо да поштујемо уобичајене ознаке, да се оригинал увек зове x, а слика y, онда добијамо да је инверзна функција функције h, функција $h^{-1} : \mathbf{R}^+ \to \mathbf{R}^+$, $h^{-1}(x) = \sqrt{x}$.)

Операције

Математика је јако богата примерима операција. Сабирање, одузимање, множење, дељење природних, целих, рационалних или реалних бројева, све су то примери операција. На примеру сабирања природних бројева, детаљније ћемо представити појам операције. Како природне бројеве сабирамо? Узмемо два природна броја, на пример 2 и 3, применимо операцију $+$ и као резултат те операције добијемо трећи природан број, број 5. Приметимо да су за обављање ове операције потребна два објекта (броја), па је она бинарна операција. Резултат операције сабирања два броја је објекат исте врсте као и објекти на које смо применили операцију. Наиме, сабирањем два природна броја као резултат добијамо трећи (тачно један) природан број. Процес сабирања јако подсећа на функцију: узели смо два објекта, тј. један пар објеката, и придружили смо им тачно један објекат (њихов збир). То значи да је сабирање природних бројева једна функција из скупа $\mathbf{N} \times \mathbf{N}$ у скуп $\mathbf{N}$.

Функција o из скупа $X \times X$ у скуп X, $o : X \times X \to X$, назива се бинарна операција o на скупу X.

Посматрање наших старих операција на овај начин доноси нам новости у њиховом записивању. Операција сабирања је сада функција $+ : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$, па уместо нашег старог записа $2+5 = 7$ имамо запис $+(2, 5) = 7$. Али, уобичајено је да за било коју бинарну операцију $*$ уместо записа $*(x, y)$ користимо природнији $x * y$. Сада ћемо признати да смо у одељку о скуповима намерно избегли да унију, пресек, разлику и Декартов производ два скупа назовемо операцијама. Чекали смо да се званично упознамо са операцијама. Сада можемо рећи да су то бинарне операције чији су полазни објекти два скупа (пар скупова), а резултат неки трећи скуп. Приметимо да, када се говори о операцијама пресек, унија, разлика и Декартов производ и сама операција и њен резултат имају исто име. Наиме, рећи ћемо операција пресек $\cap$, али и пресек $X \cap Y$, и исто за унију, разлику и Декартов производ.

Укажимо на неке детаље. Прво, подсетимо да су елементи скупа $X \times X$ уређени парови, тј. да је битан редослед чланова у сваком уређеном пару. На пример, операција одузимање на скупу целих бројева $\mathbf{Z}$ даје различите резултате за уређени пар $(5, 2)$: $5 - 2 = 3$ и за уређени пар $(2, 5)$: $2 - 5 = -3$. Друго, када кажемо да је операција функција, онда се под тим подразумева да за сваки елемент из $X \times X$ постоји резултат у X. На пример, за свака два цела броја x и y резултат одузимања $x - y$ је цео број. Али, ако одузимање хоћемо да дефинишемо на скупу природних бројева, онда имамо следећи проблем. Кажемо да је то функција $- : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ и потражимо $-(2, 5)$, тј. $2 - 5$. Резултат овог одузимања је негативан број -3, који није природан број, па не припада кодомену функције $-$, скупу $\mathbf{N}$! Нормално је да се запитамо да ли је онда одузимање операција на скупу $\mathbf{N}$? Заиста, није испуњен услов да сваки елемент скупа $\mathbf{N} \times \mathbf{N}$ има слику у скупу $\mathbf{N}$ операцијом $-$. Ми ћемо ипак рећи да одузимање јесте операција на скупу $\mathbf{N}$, и то једна парцијална операција на скупу $\mathbf{N}$. Та операција даје резултате само за неке парове из $\mathbf{N} \times \mathbf{N}$, парове (x, y), који задовољавају услов $x \geq y$. Дељење је парцијална операција на

скупу реалних бројева $\mathbf{R}$, јер само за парове (x, y) који задовољавају услов $y \neq 0$ постоји резултат $x : y$.

Операција дужине n ($n > 2$) на неком скупу X За природан број n већи од 2 функција $o : X^n \to X$ је једна операција o дужине n на скупу X.

> Пример 1 Као пример једне операције дужине 4 на скупу целих бројева $\mathbf{Z}$ дефинисаћемо операцију $\star$. За сваку четворку (x, y, z, t) из скупа $\mathbf{Z}^4$ операција $\star : \mathbf{Z}^4 \to \mathbf{Z}$ је: $\star(x, y, z, t) = (x + t) \cdot (y - z)$.

Унарна операција на скупу X Функција $o : X \to X$ је операција дужине 1 на скупу X, тј. унарна операција на скупу X. Може се посматрати и унарна операција на два различита скупа X и Y, а то је ништа друго него обична функција $f : X \to Y$.

> Пример 2 Посматрајмо неки скуп X и његов партитивни скуп $\mathcal{P}X$. За сваки подскуп Y скупа X прављење комплемента $\overline{Y}$ у односу на скуп X је једна унарна операција на том скупу $\mathcal{P}X$. Можемо је овако записати: $c : \mathcal{P}X \to \mathcal{P}X$, $c(Y) = \overline{Y}$, за $Y \in \mathcal{P}X$.

> Пример 3 Функција $f : \mathbf{R} \to \mathbf{R}$, $f(x) = \frac{1}{x}$ за све $x \neq 0$ је једна парцијална унарна операција на скупу $\mathbf{R}$. Ако посматрамо рестрикцију функције f на скуп $\mathbf{R} \setminus \{0\}$, функцију $g : \mathbf{R} \setminus \{0\} \to \mathbf{R}$, $g(x) = \frac{1}{x}$, онда је g унарна операција на скуповима $\mathbf{R} \setminus \{0\}$ и $\mathbf{R}$.

Нуларна операција на скупу X Неко издвајање једног елемента скупа X као посебног је операција дужине 0 на скупу X, тј. нуларна операција на скупу X.

> Пример 4 За неки скуп X и његов партитивни скуп $\mathcal{P}X$ издвајање, на пример, празног скупа $\emptyset$ као посебног елемента скупа $\mathcal{P}X$ је у ствари једна нуларна операција на $\mathcal{P}X$. Рецимо да смо на исти начин могли издвојити и било који други елемент тог скупа и тако дефинисати неку другу нуларну операцију на скупу $\mathcal{P}X$.

Бинарна операција на скуповима X, Y и Z Може се посматрати и бинарна операција на скуповима X, Y и Z који нису једнаки. Та бинарна операција је функција $o : X \times Y \to Z$.

> Пример 5 Пример бинарне операције на скуповима који нису једнаки може бити операција „прављење разломака" на скуповима целих, природних и рационалних бројева: $\mathbf{Z}$, $\mathbf{N}^+$ и $\mathbf{Q}$.
> То је операција $r : \mathbf{Z} \times \mathbf{N}^+ \to \mathbf{Q}$, $r(i, n) = \frac{i}{n}$.

Операција дужине n ($n > 2$) на скуповима $X_1, ..., X_n$ и Y За природан број n већи од 2 функција $o : X_1 \times ... \times X_n \to Y$ је операција o дужине n на скуповима X_1, ..., X_n и Y (међу којима може бити и једнаких).

Мада операције дужине n за $n > 2$ постоје, најчешће се срећемо и радимо са бинарним, унарним и нуларним операцијама.

Особине бинарних операција

Особине бинарних операција које ћемо представити у овом одељку, већ су познате особине које важе за, на пример, сабирање или множење два броја, а то су комутативност и асоцијативност.

За бинарну операцију $*$ на скупу X кажемо да је комутативна ако за свака два елемента x и y скупа X важи: $x * y = y * x$.

За бинарну операцију $*$ на скупу X кажемо да је асоцијативна ако за свака три елемента x, y и z скупа X важи: $(x * y) * z = x * (y * z)$.

Које комутативне и асоцијативне операције знамо? Сабирање и множење (на уобичајеној врсти бројева) су и комутативне и асоцијативне операције. Примећујемо да одузимање и дељење нису ни комутативне ни асоцијативне. Од операција на скуповима, унија и пресек су и комутативне и асоцијативне (видети особине тих операција у одељку о скуповима). Разлика скупова није ни комутативна ни асоцијативна операција. У одељку о функцијама показали смо да за две произвољне функције $f, g : X \to X$ не важи $g \circ f = f \circ g$, тј. да операција композиције функција није комутативна. Међутим, показали смо да композиција функција јесте асоцијативна операција.

На крају наведимо једну особину која се односи на везу две бинарне операције, особину дистрибутивности.

За бинарну операцију $*$ на скупу X кажемо да је дистрибутивна с десна у односу на бинарну операцију $\bullet$ на скупу X, ако за свака три елемента x, y и z скупа X важи:

$$(x \bullet y) * z = (x * z) \bullet (y * z).$$

Аналогно томе дефинише се и дистрибутивност с лева операције $*$ у односу на операцију $\bullet$: за свака три елемента x, y и z скупа X важи:

$$z * (x \bullet y) = (z * x) \bullet (z * y).$$

Приметимо да ако је операција $*$ комутативна, онда ако важи дистрибутивност с десна важи и дистрибутивност с лева и обрнуто.

Најпознатија дистрибутивност је дистрибутивност множења у односу на сабирање:

$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$ и $z \cdot (x + y) = (z \cdot x) + (z \cdot y)$

док не важи дистрибутивност сабирања у односу на множење:

$(x \cdot y) + z \neq (x + z) \cdot (y + z)$ $z + (x \cdot y) \neq (z + x) \cdot (z + y)$

У одељку о скуповима видели смо да је операција пресек дистрибутивна у односу на унију и да је унија дистрибутивна у односу на пресек.

О бројности операција

Одмах на почетку рецимо да ћемо овде разматрати бројност бинарних операција на неком коначном скупу. Пре него што кажемо нешто о њиховој бројности, покажимо још један начин представљања таквих операција.

Пример 6 Било коју бинарну операцију $*$ на неком коначном скупу $A = \{a, b, c, d\}$ можемо да представимо табелом:

$*$	a	b	c	d
a	a	b	b	c
b	c	d	b	c
c	d	b	d	c
d	c	a	b	a

Ако хоћемо да одредимо резултат $c * b$, онда пронађемо елемент c у првој колони (са леве стране вертикалне линије) и елемент b у првој врсти (изнад хоризонталне линије) и у пресеку врсте у којој се налази тај елемент c и колоне у којој се налази тај елемент b прочитамо резултат $c*b$, елемент b. Овакав једноставан и прегледан начин представљања бинарне операције на скупу A је замена за дугачак списак једнакости: $a * a = a$, $a * b = b$,...

Начин задавања бинарне операције на неком скупу X табелом је јако погодан ако скуп X има коначан број елемената.

Задавање бинарне операције на коначном скупу X табелом помоћи ће нам да одговоримо на питање: колико различитих бинарних операција можемо направити на неком коначном скупу X? Ако скуп X има m елемената правимо табелу, као у претходном примеру, са m елемената у врсти и m елемената у колони. Дакле, део табеле у коме бележимо резултат операције за два елемента (као пресек једне врсте и једне колоне) има $m \cdot m = m^2$ поља. (Конкретно у нашем Примеру 6 табела има $4^2 = 16$ поља за писање резултата.) Када та поља попунимо елементима посматраног скупа X на један начин, онда добијамо једну бинарну операцију на скупу X. У Примеру 6 на свако од 16 поља можемо ставити један од 4 елемента скупа A, тј. табелу можемо попунити на $4^{16} = 4^{4^2}$ начина. Дакле, на скупу A из Примера 6 постоји $4^{16} = 4^{4^2}$ различитих бинарних операција, а наша бинарна операција дефинисана у датој табели је само једна од њих. У општем случају, за скуп X са m елемената, на свако поље можемо да ставимо неки од m елемената скупа X, тј. имамо m могућности за попуњавање сваког поља. Дакле, начина за попуњавање табеле имамо m^{m^2}, па је број различитих бинарних операција на скупу X са m елемената једнак m^{m^2}. Рецимо и да различитих операција дужине n на скупу X са m елемената има m^{m^n}. Тако број бинарних операција на скупу X, број m^{m^2}, јесте у ствари број операција дужине 2, тј. случај када је $n = 2$.

Математичке структуре

Ако хоћемо да кажемо шта је то релација или операција потребно нам је да поменемо и неки скуп. Наиме, при дефинисању релације или операције прво имамо скуп, па затим на његовим елементима дефинишемо релацију, односно операцију. Ако имамо неки непразан скуп X и на елементима тог скупа неке различите операције (можда и само једну) $*$, $\star$, $\circ$ и $\bullet$, онда кажемо да тај скуп и те операције чине једну структуру, коју зовемо алгебарска структура

и означавамо $(X, *, \star, \circ, \bullet)$. Можемо направити и структуру коју чине скуп X, неке релације између његових елемената, на пример ρ и σ, и неке операције на његовим елиментима, на пример $*$, $\star$ и $\bullet$. Такву структуру зовемо релацијско-операцијска структура, $(X, \rho, \sigma, *, \star, \bullet)$. Често се скуп X зове носач алгебарске или релацијско-операцијске структуре. На пример, $(\mathbf{N}, >, +, \cdot)$ је једна релацијско-операцијска структура са носачем скупом природних бројева $\mathbf{N}$, бинарном релацијом $>$ и бинарним операцијама $+$ и $\cdot$.

Искази и везници. Истиносна вредност исказа.

Искази

У одељку о предмету логике поменули смо посебну врсту реченица, исказе. Искази су реченице које имају истиносну вредност, тј. за које има смисла питати да ли су истините или лажне (неистините). Напоменимо да је природније рећи да је исказ неистинит, али ми ћемо као технички термин, због краткоће, за неистините исказе говорити лажни.

Примери исказа природног језика су:

(1) *Никола Тесла је рођен у Смиљану.*
(2) *Број 7 је производ бројева 4 и 2.*
(3) *Матица српска је основана у Крушевцу.*
(4) *За сваки природан број важи да је већи од* -1.
(5) *Атеље 212 је најстарије српско позориште.*
(6) *Број 5 је већи од броја 43.*
(7) *Паја Јовановић је насликао слику „Сеоба Срба".*
(8) *Постоји цео број који је решење једначине* $x + 2 = 0$.
(9) *Књигу „Рани јади" написао је Данило Киш.*

Међу овим исказима истинити су искази (1), (4), (7), (8) и (9), а искази (2), (3), (5) и (6) су лажни.

Договоримо се да ради једноставнијег записивања исказе означавамо словима p, q, r,... Дакле, када напишемо слово p то значи да на његовом месту може стајати ма који конкретан исказ.

Везници

Од исказа правимо нове, сложеније исказе помоћу везника, које зовемо логички везници. Логички везници су: *...и...*; *...или...*; *ако ..., онда ...*; *не...*; *...ако и само ако....* Када имамо два исказа p и q, онда уз помоћ, на пример, везника *или* правимо нови исказ p *или* q. Чим формирамо нови исказ, у нашем случају исказ p *или* q, поставља се најважније питање: да ли је тај нови исказ истинит

или лажан? Истиносне вредности сложенијих исказа одређују се по принципу истиносне функционалности, тј. истиносна вредност сложенијих исказа зависи од исказа p и q, врсте логичког везника помоћу ког је формиран тај нови исказ (у нашем примеру везника *или*) и ни од чега другог.

Представимо сад логичке везнике и одговоримо на питања о истинитости исказа који се добијају помоћу тих везника.

1. Конјункција (везник *и*)

Погледајмо исказ:

Ђура Јакшић је био песник и сликар.

Оно што нам саопштава овај исказ можемо рећи и исказом који чине два исказа повезана везником *и*:

Ђура Јакшић је био песник и Ђура Јакшић је био сликар.

Конјункција исказа p и q је исказ:

$$p \text{ и } q.$$

За везник *и* користи се посебан симбол $\wedge$, који се зове и конјункција (као и сам исказ). Стога исказ p *и* q записујемо

$$p \wedge q.$$

Везник *и* је везник природних језика. У природном језику исказ p *и* q је истинит само ако су оба исказа p и q истинита. Исто ће важити и за исказ $p \wedge q$.

Исказ $p \wedge q$ је истинит ако је p истинит и q је истинит,
а лажан је ако:
(1) p је истинит и q је лажан,
(2) p је лажан и q је истинит,
(3) p је лажан и q је лажан.
Дакле, исказ $p \wedge q$ је истинит само у случају када су оба исказа p и q истинита, а лажан је ако је бар један од исказа p и q лажан.

2. Дисјункција (везник *или*)

Дисјункција исказа p и q је исказ:

$$p \text{ или } q.$$

За везник *или* користи се посебан симбол $\vee$, који се зове и дисјункција (као и сам исказ). Стога исказ p *или* q записујемо

$$p \vee q.$$

Исказ $p \vee q$ је истинит ако:
(1) p је истинит и q је истинит,
(2) p је истинит и q је лажан,
(3) p је лажан и q је истинит,

а лажан је ако p је лажан и q је лажан.
Дакле, исказ $p \vee q$ је истинит ако је бар један од исказа p и q истинит, а лажан једино у случају када су оба та исказа лажна.

Истакнимо да у природном језику постоје два начина коришћена везника *или*. Погледајмо исказ:

Никола има књигу или слику.

Овим исказом се саопштава исто што и исказом:

Никола има књигу или Никола има слику.

Дакле, имамо два исказа повезана везником *или*. Тај исказ је истинит ако је један од та два исказа истинит, и истинит је и ако су оба исказа истинита. Ова врста везника *или* зове се инклузивно (слабо) *или*. Постоји још један везник *или*, прецизније речено везник *или-или*, који се зове ексклузивно (јако) *или*. Наиме, ако кажемо:

Никола има или књигу или слику,

онда је овај исказ истинит само ако је истинит један од исказа:

Никола има књигу.

Никола има слику.

Ако су оба ова исказа истинита, он је лажан. Међутим, у природном језику понекад, кад контекст то омогућава, везник *или* се користи уместо везника *или-или*. Погледајмо следећи исказ:

Никола је у биоскопу или на фудбалској утакмици.

У овом исказу употребљено је само једно *или*, а саопшено нам је у ствари оно што се саопштава помоћу везника *или-или*. Дакле, овом реченицом је речено:

Никола је или у биоскопу или на фудбалској утакмици.

Логички везник $\vee$ који смо овде дефинисали је везник *или* из природних језика и зовемо га још инклузивна (која укључује, слаба) дисјункција.

Постоји и логички везник који одговара везнику *или-или* и зовемо га ексклузивна (која искључује, јака) дисјункција. Тај логички везник представићемо помоћу других везника (видети одељак 2.4.1), али за њега нећемо уводити посебан симбол.

3. Импликација (везник *ако..., онда...*)

Импликација исказа p са исказом q (тим редом) је исказ:

ако p, онда q.

За везник *ако..., онда...* користи се посебан симбол $\Rightarrow$, који се зове и импликација (као и сам исказ). Стога исказ *ако p, онда q* записујемо

$$p \Rightarrow q.$$

Истакнимо да је важан редослед навођења исказа p и q приликом формирања исказа $p \Rightarrow q$. У импликацији $p \Rightarrow q$ исказ p је антецеденс, а исказ q је консеквенс. Можемо говорити и о импликацији исказа q са исказом p која гласи: *ако* q, *онда* p. За импликације

ако p, *онда* q и *ако* q, *онда* p

кажемо да су једна другој обратне.

Важност исказа *ако* p, *онда* q је у томе што многа математичка тврђења имају тај облик. На пример, чувена Питагорина теорема се формулише у том облику:
ако је троугао правоугли, онда је површина квадрата над његовом хипотенузом једнака збиру површина квадрата над његовим катетама,

мада важи и обратна импликација. Рецимо да осим наведеног облика импликације: *ако* p, *онда* q са истим значењем се употребљавају и искази:

(1) q *је последица претпоставке* p

(2) p *повлачи* q

(3) *из* p *следи* q

(4) *да је* q, *довољно је да је* p

(5) p *имплицира* q

(6) p *је довољан услов за* q

(7) q *је нужан услов за* p

(8) q *је потребан услов за* p

(9) q *је неопходан услов за* p

(10) p, *само ако* q

(11) q, *ако* p

Што се тиче истинитости исказа $p \Rightarrow q$ имамо следеће.

> Исказ $p \Rightarrow q$ је истинит ако:
> (1) p је истинит и q је истинит,
> (2) p је лажан и q је истинит,
> (3) p је лажан и q је лажан;
> а лажан је ако p је истинит и q је лажан.
> Дакле, исказ $p \Rightarrow q$ је лажан само у случају када је исказ p истинит, а исказ q лажан. У свим осталим случајевима је истинит.

Имајући на уму везнике *и* и *или* природних језика истинитост конјункције $p \wedge q$ и дисјункције $p \vee q$ су, да тако кажемо, природне и очекиване. Међутим тако није са истинитошћу исказа $p \Rightarrow q$. Наиме, ми смо у природном језику навикли да у реченици облика *ако* p, *онда* q постоји нека веза (узрочно-последична) између претпоставке p и последице q, тј. да q заиста зависи од p. Али, у овом формалном начину грађења исказа, тако не мора да буде. На пример, могу се посматрати искази облика:

Ако је $1 = 0$*, онда је Сава притока Дунава.*

Ако је $1 \neq 0$*, онда је Сава притока Дунава.*

Ако је $1 = 0$*, онда је Дунав притока Саве.*

У овим исказима оно што саопштава исказ p нема никакве везе са садржајем исказа q. По ономе како смо ми увели истинитост импликације, сва три наведена исказа су истинита.

4. Негација (везник *не* (*није*))

У природном језику постоји много начина да се изрази негација неког исказа. Погледајмо исказ:

Ниш није главни град Србије.

Тај исказ је у ствари негација исказа:

Ниш је главни град Србије.

У природном језику рогобатно би изгледала негација тог исказа формулисана овако:

Није Ниш је главни град Србије.

Прихватљивије је то рећи овако:

Није тачно да је Ниш главни град Србије.

Формални начин негирања неког исказа је стављање речи *не* испред тог исказа.

Стога је негација исказа p исказ:

не p*.*

За везник *не* користи се посебан симбол $\neg$, који се зове и негација (као и сам исказ). Зато исказ *не* p записујемо

$$\neg p.$$

> Исказ $\neg p$ је истинит ако је исказ p лажан, а лажан ако је исказ p истинит.

5. Еквиваленција (везник *ако и само ако*)

Погледајмо исказе:

Ако је природан број дељив са 10, онда је он дељив и са 2 и са 5.

Ако је природан број дељив са 2 и са 5, онда је он дељив са 10.

А сада погледајмо исказ који има исто значење као ова два исказа заједно:

Природан број је дељив са 10 ако и само ако је дељив са 2 и са 5.

Еквиваленција исказа p и q је исказ:

p ако и само ако q,

или краће: *p акко q.*

За везник *ако и само ако* користи се посебан симбол $\Leftrightarrow$, који се зове и еквиваленција (као и сам исказ). Стога исказ p *ако и само ако* q записујемо

$$p \Leftrightarrow q.$$

Слично импликацији и за еквиваленцију p *акко* q постоје разни начини језичког изражавања као:

(1) *да је* p *потребно је и довољно да је* q

(2) p *је потребан и довољан услов за* q

(3) *да је* p *нужно је и довољно да је* q

(4) p *је нужан и довољан услов за* q

(5) *да је* p *неопходно је и довољно да је* q

(6) p *је неопходан и довољан услов за* q

(7) p *је еквивалентан са* q

(8) *ако је* p*, онда је* q *и обрнуто*

Исказ $p \Leftrightarrow q$ је истинит ако је:
(1) p истинит и q је истинит,
(2) p лажан и q је лажан,
а лажан је ако:
(1) p је истинит и q је лажан,
(2) p је лажан и q је истинит.
Дакле, исказ $p \Leftrightarrow q$ је истинит само у случајевима када су оба исказа p и q истинита или оба исказа p и q лажна.

6. Истина (везник $\top$) и лаж (везник $\bot$)

Везници $\wedge$, $\vee$, $\Rightarrow$ и $\Leftrightarrow$ су бинарни везници, тј. повезују два исказа. Везник $\neg$ је унарни, примењује се на један исказ. Постоје и нуларни везници: везник $\top$, тј. истина и $\bot$, тј. лаж (неистина).

Формални језици. Синтакса. Семантика.

У математици се срећемо са симболима операција $+$, $\cdot$, $-$,...; симболима релација: $<$, $=$,...; симболима за непознате: x, y,...; симболима за запис природних бројева: 0, 1, 2,... Кажемо, ти симболи припадају математичком језику. Тај језик се истиче својом јасноћом и прецизношћу. Други пример језика са тим карактеристикама је било који програмски језик. Ако је читалац у досадашњем школовању учио барем један програмски језик, приметио је са коликом прецизношћу су дефинисани облици наредбе, потпрограма, програма тог језика. Прецизност и јасноћа којим се ови језици одликују чине их, можемо рећи, различитим од природних језика. Наиме, богатство и сложеност природних језика

омогућавају да се на више начина (стилски лепше или мање лепо) саопшти једна информација. С друге стране, те особине понекад доводе до вишезначности и недоумица. Непрецизност и вишезначност не постоје у језицима које зовемо формални језици и којима припадају и математички језик и програмски језици. Најзначајнија карактеристика формалних језика је највећи могући степен прецизности у дефинисању речи тог језика (тј. форми које чине тај језик).

Као што смо већ поменули у одељку о предмету логике и логика има свој формални језик. У овој књизи изучаваћемо део логике који се зове исказна логика па ћемо упознати формални језик исказне логике. Формални језик предикатске логике је проширење формалног језика исказне логике.

Како градимо један формални језик? Прво изаберемо симболе, неке објекте које сматрамо недељивим. На пример, p_0 може бити симбол, при чему само p и само $_0$ не смеју бити симболи. Сви симболи чине скуп симбола, тј. алфабет. Сваки коначан низ симбола неког алфабета је једна реч над тим алфабетом. Низ симбола може бити и празан, тј. низ може да нема ниједан симбол, и онда је то празна реч. Следећи корак је дефиниција језика над тим алфабетом. Језик је неки скуп речи над посматраним алфабетом. Истакнимо да језик не морају да чине све речи над тим алфабетом већ само добро оформљене речи, назовимо их „добре" речи (д-речи). Дакле, језик је подскуп свих речи над тим алфабетом. За сваки алфабет прецизно дефинишемо које су то добре речи, тј. које речи чине језик над тим алфабетом. Погледајмо следећи пример.

Пример 1 Посматрајмо алфабет $A = \{в,\ е,\ л,\ о,\ с,\ т\}$. Речи над тим алфабетом градимо од симбола *в*, *е*, *л*, *о*, *с* и *т*. Сви ти симболи су речи и то дужине 1, над тим алфабетом. Имамо и празну реч са нула симбола. Ево још неколико речи над алфабетом A: *то, ел, твт, лето, тло, све, светлост, свет, весело, ссствее, тело, ооо, ооллтт, еееост, веселост, ссллл, светост*,... Међутим, језик над тим алфабетом чине само „добре" речи (д-речи): *то, лето, тло, све, светлост, свет, весело, веселост, светост, тело, во, ево, ово, вест, свест, осе, со*,...

У овом примеру поменимо још неке појмове везане за речи над неким алфабетом. Приметимо да се надовезивањем једне речи на другу (тј. дописивањем једне речи после друге) добија нова реч. На пример, ако на реч *ссллл* надовежемо реч *со* тим редом добијамо нову реч: *ссллсо* над истим алфабетом A. За речи *ссллл* и *со* рећи ћемо да су подречи речи *ссллсо*. Али и речи *с, л, о, сс, ссл, ллс, лсо* су подречи речи *ссллсо*. Уопште, нека реч r_1 је подреч друге речи r_2 ако постоје речи r_3 и r_4 тако да су r_2 и $r_3r_1r_4$ исти низ симбола, што записујемо $r_2 = r_3r_1r_4$. На пример, реч r_1: *ллс* је подреч речи r_2: *ссллсо* јер постоје речи r_3: *ссл* и r_4: *о* тако да је $r_3r_1r_4$ реч *ссллсо*. Исто тако и *ссл* је подреч речи *ссллсо*, где је r_3 празна реч, а r_4 је *лсо*. Јасно је да и д-речи имају своје подречи. Међу свим подречима неке д-речи важне су само оне које су и саме д-речи, тј.

> оне које припадају језику. На пример, реч *светлост* има подречи *свет, св, вет, све, лос, етло, светло, етлос, тло, светлост* ... али само су подречи *е, о, с, све, лос, тло, свет, светло, светлост* д-речи.
> Поменимо да је за неку реч важно забележити број јављања неких њених подречи. На пример, у речи *слотллоттт* њена подреч *лот* има два јављања. У општем случају, нека подреч r_1 речи r има више од једног јављања у r ако реч r можемо да рашчланимо на више различитих начина и да увек као једну подреч добијамо r_1, тј. да за реч r и њену подреч r_1 важи: $r = r_2r_1r_3 = r_4r_1r_5$ и $r_2 \neq r_4$. У нашем примеру, r је *слотллоттт*, њена подреч са два јављања r_1 је *лот* и имамо: r_2 је c и r_3 је *ллоттт*, али и r_4 је *слотл* и r_3 је m, па можемо r написати на два начина: $r_2r_1r_3$: *слотллоттт* и $r_4r_1r_5$: *слотллоттт* и $r_2 \neq r_4$. У д-речима важан је број јављања њених подречи које су д-речи. На пример, д-реч *светлосттт* има два јављања њене подречи c која је д-реч.

Изучавање формалног језика можемо упоредити са изучавањем неког страног језика, на пример грчког. У сваком таквом изучавању имамо два језика: један који изучавамо који се зове објект језик, и други језик на коме се објашњава, изучава тај објект језик и њега зовемо метајезик. Дакле, у нашем примеру грчки је објект језик, а српски је метајезик. Када смо у Примеру 1 говорили о језику над алфабетом $A = \{в, е, л, о, с, т\}$ тај језик је био објект језик, а наша разматрања су била на метајезику. Истакнимо да смо у представљању појма подреч користили симболе r, r_1, r_2, r_3, r_4 и r_5 који нису симболи објект језика (јер ти симболи не припадају алфабету A), него су симболи метајезика. Њих схватамо као променљиве или схеме на чија места стављамо различите речи над алфабетом A.

Када проучавамо неки формални језик, онда је објект језик тај формални језик. Зато ће и формални језик исказне логике, формални језик који је предмет нашег изучавања, бити објект језик. Метајезик ће бити српски језик и, ако хоћемо да будемо баш прецизни, њему ће бити додати још и неки технички и математички термини.

Вратимо се учењу грчког језика. То учење може бити организовано на следећи начин. Прво бисмо се упознали са симболима (то су слова грчког алфабета) помоћу којих се пишу (ако се задржимо само на писању речи) речи тог језика. Затим би нам саопштили како се од тих симбола праве добре речи, речи које чине језик. Слободније речено, као да добијамо неке шаблоне по којима правимо речи које припадају језику. За све природне језике део граматике посвећен изучавању правила образовања реченица у тим језицима назива се синтакса. Дакле, поменути начин бављења грчким језиком је изучавање синтаксе грчког језика. Пошто научимо да пишемо речи грчког језика, онда бисмо се бавили значењем тих речи. Када се у неком природном језику бавимо значењима његових речи и реченица, онда се бавимо семантиком тог језика. Нарав-

но, у процесу учења неког природног језика синтакса и семантика иду заједно, јер учењем записа речи и реченица одмах учимо и њихово значење.

Што се тиче неког формалног језика дефинисање алфабета и начина прављења речи тог језика припада његовој синтакси. Одређивање (додељивање) значења тим речима је семантика тог формалног језика. Прво се морају одредити значења симбола његовог алфабета или другачије речено ти симболи се морају интерпретирати. Када знамо значење симбола онда се дају прецизна правила како се одређује значење речи тог језика у зависности од интерпретације (значења) симбола који чине ту реч. Погледајмо следећи пример.

Пример 2 Посматрајмо алфабет B чији симболи су a, b и $*$ и имамо још и помоћне симболе леву и десну заграду. Неке речи над тим алфабетом су: a, b, $aba*$, $a**bba*$, $(a*b)$,... Језик над тим алфабетом чине д-речи које дефинишемо следећом индуктивном дефиницијом:

(1) a и b су д-речи;

(2) ако су R и P д-речи, онда је и $(R * P)$ д-реч;

(3) д-речи се могу градити само коначном применом делова (1) и (2) ове дефиниције.

Истакнимо да су R и P симболи метајезика уместо којих стављамо конкретне речи над посматраним алфабетом. Дакле, д-речи су: a, b, $(a * b)$, $(b * a)$, $((a * b) * a)$, $((a * b) * (b * b))$, $((b * (a * a)) * a)$,... Једна интерпретација овог језика је да симбол a значи цео број -1, симбол b има значење цео број 1, а симбол $*$ је бинарна операција множења на скупу $\{-1, 1\}$:

$\cdot$	-1	1
-1	1	-1
1	-1	1

Помоћни симболи леве и десне заграде имају искључиво синтаксну функцију и немају интерпретације као други симболи. У овој интерпретацији језика над алфабетом B значење неке д-речи добијамо овако. Значење д-речи a је -1, а д-речи b је 1. Ако имамо д-реч $(R * P)$ и број z_1 је значење д-речи R и број z_2 је значење д-речи P, онда значење д-речи $(R * P)$ је производ бројева z_1 и z_2: $z_1 \cdot z_2$. Сликовито речено, наше д-речи су интерпретиране као изрази у којима се множе бројеви -1 и 1 и значење сваке д-речи може бити или -1 или 1.

Јасно је да сваки језик може имати више интерпретација. Покажимо још једну интерпретацију језика над алфабетом B. Симбол a је 0, симбол b је 1 и симбол $*$ је бинарна операција минимума на скупу $\{0, 1\}$:

min	0	1
0	0	0
1	0	1

И у нашем изучавању формалног језика исказне логике ми ћемо се бавити синтаксом и семантиком тог језика. Симболе алфабета формалног језика исказне логике можемо поделити у две скупине. Једну скупину чине симболи са фиксним значењем, које смо поменули у одељку о предмету логике, логички везници $\wedge$ (конјункција), $\vee$ (дисјункција), $\Rightarrow$ (импликација), $\neg$ (негација), $\Leftrightarrow$ (еквиваленција), $\top$ (истина) и $\bot$ (лаж). Другу скупину чине симболи који су променљиви што се тиче значења.

Глава 2

Исказна логика

У овој глави изучаваћемо исказну логику. У првом делу представићемо формални језик исказне логике и строг и прецизан начин прављења исказних формула, тј. бавићемо се синтаксом формалног језика исказне логике. У другом делу представићемо семантику исказне логике. Наиме, говорићемо о значењу исказних формула, тј. представићемо главну интерпретацију формалног језика исказне логике. Свака исказна формула имаће само једно од два значења: истинита или лажна (неистинита). У трећем делу дефинисаћемо неколико значајних алгебарских структура, од којих истичемо Булове алгебре. На крају, у четвртом делу, изучаваћемо базе везника, представићемо важне форме исказних формула, конјунктивну и дисјунктивну нормалну форму, а показаћемо и неке везе између везника.

2.1 Синтакса исказне логике

2.1.1 Алфабет исказне логике

Алфабет формалног језика исказне логике је пребројив, непразан скуп симбола.

Дефиниција алфабета исказне логике

Алфабет $\mathcal{S}$ исказне логике састоји се од следећа три скупа:
$\diamond$ пребројивог скупа исказних слова, скупа $\mathcal{P}$, чији су елементи p_0, q_0, r_0, p_1, q_1, r_1,..., p_n, q_n, r_n,...;

◇ скупа логичких везника $\{\wedge, \vee, \Rightarrow, \bot\}$, где су $\wedge$, $\vee$ и $\Rightarrow$ бинарни везници, а $\bot$ нуларни везник;
◇ скупа помоћних симбола $\{(,)\}$.

2.1.2 Језик исказне логике

Од свих речи над алфабетом исказне логике, добро оформљене речи су исказне формуле. Дакле, језик исказне логике чине исказне формуле.

Дефиниција исказне формуле

(1) Исказна слова и логички везник $\bot$ су исказне формуле.
(2) Ако су A и B исказне формуле, онда су и $(A \wedge B)$, $(A \vee B)$ и $(A \Rightarrow B)$ исказне формуле.
(3) Исказне формуле се могу градити само коначном применом дела (1) и (2) ове дефиниције.

Приметимо да је ово индуктивна дефиниција. У њеном делу (1) дефинисане су најједноставније исказне формуле, исказна слова и нуларни логички везник $\bot$, и њих ћемо звати атомске исказне формуле. У делу (2) дефинисано је како се свака сложенија исказна формула добија повезивањем већ постојећих (већ направљених) исказних формула неким логичким везником $\wedge$, $\vee$ или $\Rightarrow$. Део (3) значи да је реч о једној индуктивној дефиницији. Свака индуктивна дефиниција ће имати један такав део, па ћемо га убудуће подразумевати.

Исказне формуле краће ћемо звати формуле или искази. Скуп свих формула исказне логике означаваћемо са $\mathcal{F}$.

Пример 1 Неке атомске исказне формуле су p_1, q_4, r_3, p_5, $\bot$ и r_{56}. Примери сложенијих исказних формула су: $((p_1 \vee \bot) \Rightarrow q_5)$, $(\bot \Rightarrow \bot)$, $(p_1 \vee p_2)$, $(r_1 \Rightarrow (p_{32} \wedge q_2))$ и $((p_4 \wedge q_1) \vee r_8)$. На крају, ево неколико низова симбола алфабета исказне логике који нису исказне формуле: $(p_1 \wedge \vee)$, $\Rightarrow$, $(p_5 \bot q_6)$ и $(p_1 q_1 \Rightarrow)$.

Напомена У дефиницији исказне формуле употребили смо слова A и B која припадају метајезику и нису симболи алфабета исказне логике. И надаље, слова A, B, C,..., F,..., A_1, A_2,..., B_1, B_2,..., C_1, C_2,..., F_1, F_2,... биће симболи метајезика, тј. схематска слова на место којих можемо ставити неку исказну формулу. На пример, да на месту слова F стоји формула $((p_1 \vee p_2) \Rightarrow q_1)$ записиваћемо: $F = ((p_1 \vee p_2) \Rightarrow q_1)$. Ако су формуле A и B синтаксно идентичне (једнаке као низови симбола алфабета исказне логике), онда ћемо то записати $A = B$. Даље, $A \wedge B$, $A \vee B$ и $A \Rightarrow B$ су схеме, у којима на место сваког симбола метајезика A и B стављамо неку исказну формулу и повезујући их редом везницима $\wedge$, $\vee$ и $\Rightarrow$ добијамо нову исказну формулу. Исто тако, често ћемо користити слова p, q, r,... из метајезика као схематска слова на место којих стављамо исказна слова алфабета исказне логике.

Када смо говорили о формалним језицима рекли смо да је важно дефинисати добро оформљене речи (назвали смо их д-речи) над алфабетом и да те речи чине језик. Важни појмови везани за неку д-реч су: подреч која је и сама д-реч и број јављања таквих подречи у тој д-речи (видети Пример 1 у одељку о формалним језицима). Наше д-речи су исказне формуле. Подречи једне исказне формуле, које су и саме исказне формуле, зваћемо потформуле, а биће нам важан и број њихових јављања у исказној формули.

Пример 2 Посматрајмо формулу $(((p_1 \vee p_2) \Rightarrow p_5) \vee (p_7 \wedge p_4))$. Приметимо да су неки њени делови, на пример $(p_1 \vee p_2)$, p_5, $(p_7 \wedge p_4)$ и $((p_1 \vee p_2) \Rightarrow p_5)$ и сами исказне формуле. Те формуле ћемо звати потформуле полазне формуле $(((p_1 \vee p_2) \Rightarrow p_5) \vee (p_7 \wedge p_4))$.

Дакле, ако сваку исказну формулу гледамо као једну реч језика исказне логике, онда је свака њена подреч, која је и сама исказна формула, једна потформула те формуле. А сада дефинишимо скуп свих потформула неке формуле.

Дефиниција скупа потформула неке формуле

Скуп свих потформула формуле F, скуп $P_f(F)$, индуктивно дефинишемо на следећи начин:
(1) сама формула F припада скупу $P_f(F)$;
(2) ако је $(A \wedge B) \in P_f(F)$, онда је $A \in P_f(F)$ и $B \in P_f(F)$;
ако је $(A \vee B) \in P_f(F)$, онда је $A \in P_f(F)$ и $B \in P_f(F)$;
ако је $(A \Rightarrow B) \in P_f(F)$, онда је $A \in P_f(F)$ и $B \in P_f(F)$.

Скуп потформула формуле из Примера 2 је скуп:

$\{p_1, p_2, p_4, p_5, p_7, (p_1 \vee p_2), (p_7 \wedge p_4), ((p_1 \vee p_2) \Rightarrow p_5), (((p_1 \vee p_2) \Rightarrow p_5) \vee (p_7 \wedge p_4))\}$.

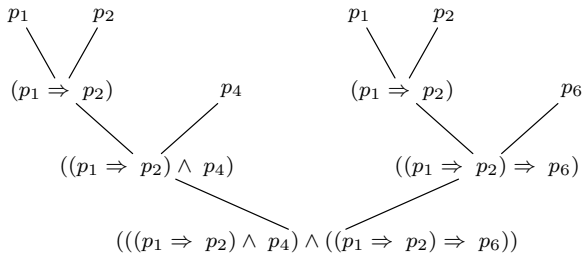
За неку формулу F и сваку њену потформулу A говорићемо и о јављању потформуле A у формули F. Исказне формуле су речи језика исказне логике, па више јављања потформуле A у некој формули F дефинише се као више јављања подречи A у речи F.

Погледајмо сада формулу у следећем примеру.

Пример 3 Имамо формулу $F = (((p_1 \Rightarrow p_2) \wedge p_4) \wedge ((p_1 \Rightarrow p_2) \Rightarrow p_6))$. Ова формула има два јављања њених потформула: $(p_1 \Rightarrow p_2)$, p_1 и p_2, а скуп свих њених потформула је скуп:
$\{p_1, p_2, p_4, p_6, (p_1 \Rightarrow p_2), ((p_1 \Rightarrow p_2) \wedge p_4), ((p_1 \Rightarrow p_2) \Rightarrow p_6), F\}$.

У Примеру 3 видимо да скуп свих потформула неке формуле F не даје информацију о томе колико пута се нека потформула јавља у формули F. Да бисмо могли да осим свих потформула неке формуле F забележимо и сва јављања тих потформула, правимо дрво те формуле F.

Дрво формуле F из Примера 3 је:

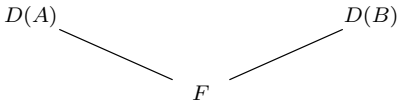


У дрвету формуле F забележена су сва јављања потформула $(p_1 \Rightarrow p_2)$, p_1 и p_2 у тој формули, као и сва јављања свих других потформула формуле F.

А ево и прецизне дефиниције дрвета неке формуле.

Дефиниција дрвета неке формуле

(1) Ако је F атомска формула (тј. F је неко исказно слово или $\bot$), онда је дрво формуле F, $\mathcal{D}(F)$, чвор у коме је сама формула F.
(2) Ако је формула F облика $(A \wedge B)$, $(A \vee B)$ или $(A \Rightarrow B)$, онда је дрво формуле F, $\mathcal{D}(F)$:



где је $\mathcal{D}(A)$ дрво потформуле A и $\mathcal{D}(B)$ дрво потформуле B.

Договоримо се да надаље, при прављењу сложених формула, не пишемо сасвим спољашње заграде. На пример, формуле $(A \wedge B)$, $(A \vee B)$ и $(A \Rightarrow B)$ писаћемо редом $A \wedge B$, $A \vee B$ и $A \Rightarrow B$.

Приметимо да алфабет исказне логике $\mathcal{S}$ не садржи све исказне везнике помоћу којих смо градили исказе. Недостају: бинарни везник $\Leftrightarrow$, унарни везник $\neg$ и нуларни везник $\top$. Те везнике дефинисаћемо помоћу везника који припадају алфабету $\mathcal{S}$ на следећи начин:

$$A \Leftrightarrow B =_{def} (A \Rightarrow B) \wedge (B \Rightarrow A)$$
$$\neg A =_{def} A \Rightarrow \bot$$
$$\top =_{def} \bot \Rightarrow \bot$$

2.2 Семантика исказне логике

У претходном одељку прецизно смо дефинисали поступак грађења исказних формула. У овом одељку ћемо говорити о значењу тих формула, тј. представићемо главну интерпретацију формалног језика исказне логике.

2.2.1 Истиносне вредности исказних формула

Исказне формуле су искази који имају само једну истиносну вредност, тј. имају само једно од следећа два значења: (1) истините или (2) лажне (неистините).

Везу између исказних формула $\mathcal{F}$ и њихових значења можемо да представимо као повезивање елемената следећа два скупа: скупа исказних формула $\mathcal{F}$ и скупа значења који чине само два елемента: 1 (истина) и 0 (лаж, неистина). Наиме, дефинисаћемо функције из скупа $\mathcal{F}$ у скуп $\{0,1\}$, функције $v : \mathcal{F} \to \{0,1\}$. Једном таквом функцијом свака исказна формула добија једну истиносну вредност: истинита је ако се слика у 1, а лажна је ако се слика у 0. Те функције задовољавају следећи принцип, принцип истиносне функционалности: истиносна вредност сложене формуле мора да зависи од истиносних вредности њених потформула, врсте логичког везника помоћу којег је формирана та формула и ни од чега другог. То значи да истиносна вредност неке формуле F, која има један од следећих облика: $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$ или $\neg A$, мора да зависи од истиносних вредности формула A и B као њених потформула и редом везника $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ и $\neg$. Одмах се намеће питање: да ли истиносне вредности формула $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$ и $\neg A$ зависе од истиносних вредности формула A и B исто као што истиносне вредности сложених исказа $p \wedge q$, $p \vee q$, $p \Rightarrow q$, $p \Leftrightarrow q$ и $\neg p$ зависе од истиносних вредности исказа p и q (видети одељак о везницима)? Одговор је: ДА. Да бисмо прецизно описали ту зависност, помоћи ће нам следеће операције на скупу $\mathbf{I} = \{0,1\}$.
Представимо прво четири бинарне операције на скупу $\mathbf{I} = \{0,1\}$:

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

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

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Приметимо да су ове бинарне операције редом следеће функције:

$$\wedge : \mathbf{I} \times \mathbf{I} \to \mathbf{I}, \qquad \wedge(a,b) = min(a,b);$$
$$\vee : \mathbf{I} \times \mathbf{I} \to \mathbf{I}, \qquad \vee(a,b) = max(a,b);$$
$$\Rightarrow : \mathbf{I} \times \mathbf{I} \to \mathbf{I}, \qquad \Rightarrow (a,b) = max(1-a,b);$$
$$\Leftrightarrow : \mathbf{I} \times \mathbf{I} \to \mathbf{I}, \qquad \Leftrightarrow (a,b) = \begin{cases} 1, & a = b \\ 0, & a \neq b. \end{cases}$$

Затим представимо унарну операцију:

	$\neg$
0	1
1	0

која је функција:

$$\neg : \mathbf{I} \to \mathbf{I}, \qquad \neg(a) = 1 - a.$$

На крају, представимо и две нуларне операције на $\mathbf{I} = \{0,1\}$:

($\bot$) нуларна операција на скупу $\mathbf{I}$ која издваја елемент 0;

($\top$) нуларна операција на скупу $\mathbf{I}$ која издваја елемент 1.

Дакле, за функције које повезују исказне формуле са њиховим истиносним вредностима, функције $v : \mathcal{F} \to \{0,1\}$, треба да важи следеће:

$$v(A \wedge B) = min(v(A), v(B))$$

$v(A \vee B) = max(v(A), v(B))$
$v(A \Rightarrow B) = max(1 - v(A), v(B))$
$v(\bot) = 0$
$v(\neg A) = 1 - v(A)$
$v(\top) = 1$
$v(A \Leftrightarrow B) = 1$ ако је $v(A) = v(B)$, иначе $v(A \Leftrightarrow B) = 0$.

Пример 1 Посматрајмо формулу $F = p_1 \wedge (p_2 \Rightarrow p_3)$. Одредимо истиносну вредност те формуле, вредност $v(p_1 \wedge (p_2 \Rightarrow p_3))$. На основу наведених својстава функције v имамо:

$$v(p_1 \wedge (p_2 \Rightarrow p_3)) = min(v(p_1), max(1 - v(p_2), v(p_3))).$$

Дакле, да бисмо одредили истиносну вредност наше формуле, вредност $v(p_1 \wedge (p_2 \Rightarrow p_3))$, морамо да знамо истиносне вредности њених исказних слова, тј. вредности $v(p_1)$, $v(p_2)$ и $v(p_3)$.

Из Примера 1 видимо да не можемо да одредимо истиносну вредност формуле F ако не знамо истиносну вредност њених исказних слова. Заиста, темељ сваке истиносне вредности неке исказне формуле су истиносне вредности свих исказних слова која се у њој појављују. Шире гледано темељ истиносних вредности свих исказних формула, свих елемената скупа $\mathcal{F}$, јесу истиносне вредности свих исказних слова, свих елемената скупа $\mathcal{P}$, подскупа скупа $\mathcal{F}$. Зато ћемо посматрати скуп исказних слова $\mathcal{P}$ и дефинисаћемо функције из $\mathcal{P}$ у $\{0, 1\}$ које ће исказним словима додељивати истиносне вредности.

Дефиниција валуације исказних слова

Функција $v_{\mathcal{P}}$ из скупа исказних слова $\mathcal{P}$ у скуп $\{0, 1\}$, $v_{\mathcal{P}}{:}\mathcal{P}{\to}\{0, 1\}$, назива се валуација исказних слова или краће базична валуација.

Свака базична валуација $v_{\mathcal{P}} : \mathcal{P} \to \{0, 1\}$ одређује тачно једну валуацију исказних формула v, $v : \mathcal{F} \to \{0, 1\}$, на следећи начин: за свако исказно слово p вредност $v(p)$ се поклапа са вредношћу тог слова базичном валуацијом $v_{\mathcal{P}}$, тј. $v(p) = v_{\mathcal{P}}(p)$, и постоји дефиниција како се одређују истиносне вредности сложенијих формула у зависности од истиносних вредности њихових потформула. Ево те дефиниције валуације.

Дефиниција валуације исказних формула

За неку валуацију исказних слова $v_{\mathcal{P}}$, $v_{\mathcal{P}} : \mathcal{P} \to \{0, 1\}$, дефинишемо функцију v, $v : \mathcal{F} \to \{0, 1\}$, на следећи начин:

- $v(p) = v_{\mathcal{P}}(p)$ за свако p из скупа исказних слова $\mathcal{P}$, $\mathcal{P} \subset \mathcal{F}$;
- $v(\bot) = 0$;
- $v(A \wedge B) = min(v(A), v(B))$;
- $v(A \vee B) = max(v(A), v(B))$;
- $v(A \Rightarrow B) = max(1 - v(A), v(B))$.

Овако дефинисана функција v је једна валуација исказних формула. За сваку исказну формулу F вредност $v(F)$ зваћемо истиносна вредност (или краће, вредност) формуле F валуацијом v.

Одмах покажимо како ћемо за неку валуацију v одредити истиносну вредност формула $\top$, $\neg A$ и $A \Leftrightarrow B$. Формула $\top$ је замена за формулу $\bot \Rightarrow \bot$, па користећи дефиницију валуације, добијамо:

$$v(\top) = v(\bot \Rightarrow \bot) = max(1 - v(\bot), v(\bot)) = max(1 - 0, 0) = 1.$$

С обзиром на то да је формула $\neg A$ замена за формулу $A \Rightarrow \bot$ имамо:

$$v(\neg A) = v(A \Rightarrow \bot) = max(1 - v(A), v(\bot)) = max(1 - v(A), 0) = 1 - v(A).$$

На сличан начин, користећи дефиницију валуације и дефиницију да је $A \Leftrightarrow B$ замена за формулу $(A \Rightarrow B) \wedge (B \Rightarrow A)$, може се показати да је:

$$v(A \Leftrightarrow B) = 1 \text{ ако је } v(A) = v(B), \text{ иначе } v(A \Leftrightarrow B) = 0.$$

Погледајмо сада нашу формулу $p_1 \wedge (p_2 \Rightarrow p_3)$ из Примера 1. Ако је валуација v_1 таква да је $v_1(p_1) = v_1(p_2) = 0$ и $v_1(p_3) = 1$, онда је:

$$\begin{aligned} v_1(p_1 \wedge (p_2 \Rightarrow p_3)) &= min(v_1(p_1), v_1(p_2 \Rightarrow p_3)) \\ &= min(v_1(p_1), max(1 - v_1(p_2), v_1(p_3))) \\ &= min(0, max(1 - 0, 1)) = min(0, 1) = 0. \end{aligned}$$

Ако узмемо валуацију v_2 такву да је $v_2(p_1) = v_2(p_2) = v_2(p_3) = 1$, онда вредност $v_2(p_1 \wedge (p_2 \Rightarrow p_3))$ рачунамо на исти начин као и $v_1(p_1 \wedge (p_2 \Rightarrow p_3))$, али са другим истиносним вредностима исказних слова, па имамо:

$$\begin{aligned} v_2(p_1 \wedge (p_2 \Rightarrow p_3)) &= min(v_2(p_1), v_2(p_2 \Rightarrow p_3)) \\ &= min(v_2(p_1), max(1 - v_2(p_2), v_2(p_3))) \\ &= min(1, max(1 - 1, 1)) = min(1, 1) = 1. \end{aligned}$$

Закључујемо да је за валуацију v_1 вредност $v_1(F)$ једнака 0, тј. формула F је лажна, а за валуацију v_2 вредност $v_2(F)$ једнака је 1, тј. формула F је истинита.

За сваку формулу F све валуације можемо разврстати на две стране: на једној страни имамо валуације за које је формула F истинита, а на другој страни валуације за које је формула F лажна. Поставља се следеће питање: да ли постоје формуле које су за сваку валуацију из скупа $\mathcal{F}$ у скуп $\{0, 1\}$ истините? Одговор је: ДА. Таква је на пример, формула $p_1 \Rightarrow p_1$. Имамо да се за сваку валуацију v вредност $v(p_1 \Rightarrow p_1)$ рачуна на следећи начин:

$$v(p_1 \Rightarrow p_1) = max(1 - v(p_1), v(p_1)).$$

Исказно слово p_1 неком валуацијом v може имати: или вредност 0 или вредност 1. Ако је $v(p_1) = 0$, онда је $v(p_1 \Rightarrow p_1) = max(1 - 0, 0) = 1$, а ако је $v(p_1) = 1$, онда је $v(p_1 \Rightarrow p_1)$ једнако $max(1-1, 1) = 1$. Закључујемо да је за све валуације формула $p_1 \Rightarrow p_1$ истинита. Формуле које имају ту особину зову се таутологије.

Дефиниција таутологије

Исказна формула F је таутологија АККО за сваку валуацију v вредност $v(F)$ је 1. Да је формула F таутологија записујемо $\models F$.

С друге стране, постоје и формуле које су лажне за све валуације. Те формуле зовемо контрадикције (или противречности). На пример, формула

$p_2 \wedge (p_2 \Rightarrow \bot)$ је контрадикција. Ако се сетимо да је замена за формулу $p_2 \Rightarrow \bot$ формула $\neg p_2$, онда је формула $p_2 \wedge (p_2 \Rightarrow \bot)$ у ствари $p_2 \wedge \neg p_2$ и она је увек лажна. Потврдимо то одређивањем вредности $v(p_2 \wedge (p_2 \Rightarrow \bot))$. Исказно слово p_2 неком валуацијом v може да има или вредност 1 или вредност 0. Ако је $v(p_2) = 1$, онда је $v(p_2 \wedge (p_2 \Rightarrow \bot)) = min(1, max(1–1, 0)) = min(1, 0) = 0$. Ако је пак, $v(p_2) = 0$, онда је $v(p_2 \wedge (p_2 \Rightarrow \bot)) = min(0, max(1 - 0, 0)) = min(0, 1) = 0$. Дакле, за све валуације формула $p_2 \wedge (p_2 \Rightarrow \bot)$ је лажна.

Дефиниција контрадикције (противречности)

Исказна формула F је контрадикција (противречност) АККО за сваку валуацију v вредност $v(F)$ је 0.

Наравно, скуп формула $\mathcal{F}$ исказне логике не чине само таутологије и контрадикције. На пример, наша формула $p_1 \wedge (p_2 \Rightarrow p_3)$ из Примера 1 није ни таутологија ни контрадикција. Дакле, скуп исказних формула $\mathcal{F}$ чине таутологије, контрадикције и трећа врста формула које нису ни таутологије ни контрадикције. Ипак, централно место заузимају таутологије. Можемо рећи да је наш најважнији задатак да установимо да ли је нека формула F, коју посматрамо, таутологија или није. Решавање тог задатка зависи од одговора на следеће питање: да ли постоји бар једна метода којом можемо утврдити за произвољну формулу F да ли је таутологија или није? Одговор на ово питање је: ДА, постоји више таквих метода. Можда најпознатија од свих тих метода је метода истиносних таблица. Ту методу ћемо представити у следећем примеру.

Пример 2 Дата је формула $F = (p \wedge (p \Rightarrow q)) \Rightarrow q$. За формулу F правимо истиносну таблицу на следећи начин. Прво за све потформуле формуле F направимо колоне, а затим за потформуле које су исказна слова (тј. за сва исказна слова која се појављују у тој формули) записујемо све могуће валуације (у нашем примеру имамо четири врсте различитих валуација):

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

У свакој врсти (тј. сваком реду таблице), користећи дефиницију валуације, одређујемо вредности осталих потформула посматране формуле F. На пример у првом реду имамо $v_1(p) = 1$ и $v_1(q) = 1$, па користећи дефиницију валуације добијамо:
$v_1(p \Rightarrow q) = max(1 - v_1(p), v_1(q)) = max(1 - 1, 1) = max(0, 1) = 1$,
$v_1(p \wedge (p \Rightarrow q)) = min(v_1(p), v_1(p \Rightarrow q)) = min(1, 1) = 1$.
На крају, одређујемо вредност $v_1((p \wedge (p \Rightarrow q)) \Rightarrow q)$:
$max(1 - v_1(p \wedge (p \Rightarrow q)), v_1(q)) = max(1 - 1, 1) = 1$.
На исти начин попуњавамо и све друге редове направљене таблице и добијамо попуњену таблицу:

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

Одговор на питање: да ли је посматрана формула F таутологија, читамо из таблице у колони која одговара тој формули. Ако су у тој колони само јединице, онда је формула F таутологија. Дакле, наша формула $(p \wedge (p \Rightarrow q)) \Rightarrow q$ јесте таутологија. Напоменимо да контрадикцију препознајемо тако што на свим местима у целој колони формуле F добијамо 0, а формула која није ни таутологија ни контрадикција у својој колони има и јединице и нуле.

А сада размотримо питање броја различитих (битних) валуација. Ако погледамо истиносну таблицу коју смо направили у нашем Примеру 2, видимо да смо испитивали вредност формуле F за четири валуације. Природно је запитати се: како смо знали да за формулу F постоје четири битне валуације v_j, $1 \leq j \leq 4$, и да ће за сваку другу валуацију $v : \mathcal{F} \to \{0,1\}$ вредност $v(F)$ бити једнака некој од $v_j(F)$, $1 \leq j \leq 4$? Потпуно је јасно да за одређивање вредности $v(F)$ уопште нису важне вредности валуацијом v исказних слова која се не појављују у формули F. За неку валуацију v нама су потребне само истиносне вредности исказних слова која се појављују у тој формули F. Нека су p_1,..., p_n $(n \geq 1)$ сва исказна слова (међусобно различита) која се појављују у формули F. За сваку валуацију v нама је потребна само рестрикција те валуације v на подскуп $\{p_1, ..., p_n\}$ скупа $\mathcal{P}$, рестрикција $v|_{\{p_1,...,p_n\}}$. Погледајмо све могуће валуације $v : \mathcal{F} \to \{0,1\}$. Јасно је да ако се две валуације v_1 и v_2 поклапају на скупу $\{p_1, ..., p_n\}$, онда су и вредности формуле F валуацијама v_1 и v_2 једнаке, тј.

ако је $v_1|_{\{p_1,...,p_n\}} = v_2|_{\{p_1,...,p_n\}}$, онда важи $v_1(F) = v_2(F)$.

Зато за произвољну формулу F све могуће валуације разврставамо по томе да ли имају једнаке рестрикције на скупу исказних слова која се појављују у формули F.

Напомена Формирање различитих врста свих могућих валуација, које смо сада представили, намеће нам следеће питање: да ли можда тим поступком правимо класе неке релације еквиваленције? Одговор је: ДА. Те различите врсте валуација су класе еквиваленције следеће релације еквиваленције ρ на скупу свих валуација:

$$v_1 \ \rho \ v_2 \ \text{АККО} \ v_1|_{\{p_1,...,p_n\}} = v_2|_{\{p_1,...,p_n\}}.$$

Јасно је да су сваке две овакве класе валуација или једнаке или немају заједничких елемената. Питамо се: колико таквих класа валуација има за произвољну формулу F? То зависи од броја различитих исказних слова која се појављују у посматраној формули F. Ако се у формули F појављује n $(n \geq 1)$ исказних слова, p_1,..., p_n, онда је број тражених класа валуација 2^n. Покажимо то за конкретне вредности броја исказних слова. Нека се у формули F појављује само једно исказно слово, исказно слово p, тј. $n = 1$. Било којом

валуацијом v исказно слово p може добити или вредност 0 или вредност 1. То значи да све валуације можемо разврстати у две класе, јер је $2^n = 2^1 = 2$. У једној класи су оне за које је вредност слова p једнака 1, а у другој су оне за које је вредност слова p једнака 0.

Пример 3 Погледајмо формулу $p \vee (p \Rightarrow (p \Rightarrow \bot))$ која има једно исказно слово. Све могуће валуације разврставамо у две класе и истиносна таблица те формуле има само две валуације, и то једну из прве класе $v_1(p) = 1$, и једну из друге класе $v_2(p) = 0$:

p	$\bot$	$p \Rightarrow \bot$	$p \Rightarrow (p \Rightarrow \bot)$	$p \vee (p \Rightarrow (p \Rightarrow \bot))$
1	0	0	0	1
0	0	1	1	1

Приметимо да је формула $p \vee (p \Rightarrow (p \Rightarrow \bot))$ таутологија.

Следећи случај је када се у формули F појављују два различита исказна слова као у Примеру 2 и онда имамо $2^2 = 4$ класе валуација са својим представницима које смо навели у том примеру.

Ако формула F има три различита исказна слова, на пример p_1, p_2 и p_3 (као у Примеру 1), онда имамо $2^3 = 8$ класа валуација са својим представницима које наводимо у редовима таблице испод исказних слова. Истиносна таблица формуле $p_1 \wedge (p_2 \Rightarrow p_3)$ из Примера 1 је:

p_1	p_2	p_3	$p_2 \Rightarrow p_3$	$p_1 \wedge (p_2 \Rightarrow p_3)$
1	1	1	1	1
1	1	0	0	0
1	0	1	1	1
1	0	0	1	1
0	1	1	1	0
0	1	0	0	0
0	0	1	1	0
0	0	0	1	0

Из ње видимо да формула $p_1 \wedge (p_2 \Rightarrow p_3)$ није ни таутологија ни контрадикција.

Дакле, у општем случају, ако се у некој формули F појављује n ($n \geq 1$) различитих исказних слова, на пример $p_1, ..., p_n$, онда се скуп свих могућих валуација дели на 2^n класе. Из сваке те класе узимамо једну валуацију као њеног представника и онда за сваку од тих валуација одређујемо вредност формуле F. То значи да истиносна таблица формуле F, у којој се појављују n различитих исказних слова, има 2^n редова, тј. свакој од поменутих валуација, представнику једне класе валуација, одговара један ред у таблици.

Овај одељак ћемо завршити једним списком таутологија. Корисна вежба за учење методе истиносних таблица је да се том методом покаже да свака од формула из тог списка јесте таутологија. Ове таутологије ћемо користити у методи чишћења, још једној методи за испитивање да ли је нека формула таутологија, коју ћемо представити у одељку 2.2.3. Напоменимо и то да ћемо у таутологијама које следе користити формулу $\top$ као замену за формулу $\bot \Rightarrow \bot$, формулу $\neg p$ као замену за формулу $p \Rightarrow \bot$ и формулу $A \Leftrightarrow B$ (за неке формуле A и B) као замену за формулу $(A \Rightarrow B) \wedge (B \Rightarrow A)$.

Таутологије

(1) $(p \wedge \top) \Leftrightarrow p$ (2) $(\top \wedge p) \Leftrightarrow p$ (3) $(p \wedge \bot) \Leftrightarrow \bot$ (4) $(\bot \wedge p) \Leftrightarrow \bot$

(5) $(p \vee \top) \Leftrightarrow \top$ (6) $(\top \vee p) \Leftrightarrow \top$ (7) $(p \vee \bot) \Leftrightarrow p$ (8) $(\bot \vee p) \Leftrightarrow p$

(9) $(p \Rightarrow \top) \Leftrightarrow \top$ (10) $(\top \Rightarrow p) \Leftrightarrow p$ (11) $(p \Rightarrow \bot) \Leftrightarrow \neg p$ (12) $(\bot \Rightarrow p) \Leftrightarrow \top$

(13) $(p \Leftrightarrow \top) \Leftrightarrow p$ (14) $(\top \Leftrightarrow p) \Leftrightarrow p$ (15) $(p \Leftrightarrow \bot) \Leftrightarrow \neg p$ (16) $(\bot \Leftrightarrow p) \Leftrightarrow \neg p$

(17) $\neg\top \Leftrightarrow \bot$ (18) $\neg\bot \Leftrightarrow \top$

И у наредном излагању нећемо посматрати само формуле које су изграђене помоћу логичких везника из скупа везника алфабета исказне логике, скупа $\{\wedge, \vee, \Rightarrow, \bot\}$, већ и формуле направљене помоћу других логичких везника, имајући на уму њихове дефиниције помоћу везника из скупа $\{\wedge, \vee, \Rightarrow, \bot\}$.

2.2.2 Замена еквивалената

У овом одељку дефинисаћемо поступак униформне замене (супституције) у исказним формулама и доказати нека својства која ћемо користити за представљање методе чишћења.

Пример 4 Посматрајмо формулу $F = (((p \wedge q) \vee r) \wedge p) \Rightarrow p$. Шта значи униформно заменити исказно слово p формулом C у формули F? То значи да се свако јављање исказног слова p у посматраној формули F замени формулом C. Резултат те замене је формула $F_1 = (((C \wedge q) \vee r) \wedge C) \Rightarrow C$.

Дефинишимо сада поступак униформне замене, прецизно.

Дефиниција униформне замене (супституције)

Униформна замена (супституција) исказног слова p исказном формулом C у некој исказној формули из скупа исказних формула $\mathcal{F}$ је једна функција $\overset{p}{C} : \mathcal{F} \to \mathcal{F}$ индуктивно дефинисана на следећи начин:

(1) (1.1) за неко исказно слово q: $q^p_C = \begin{cases} C, & q = p \\ q, & q \neq p \end{cases}$

(1.2) за нуларни везник $\bot$: $\bot^p_C = \bot$

(2) (2.1) за неку исказну формулу $A \wedge B$:

$$(A \wedge B)^p_C = A^p_C \wedge B^p_C$$

(2.2) за неку исказну формулу $A \vee B$:

$$(A \vee B)^p_C = A^p_C \vee B^p_C$$

(2.3) за неку исказну формулу $A \Rightarrow B$:

$$(A \Rightarrow B)^p_C = A^p_C \Rightarrow B^p_C$$

Пример 5 Посматрајмо поново формулу из Примера 4, формулу $F = (((p \wedge q) \vee r) \wedge p) \Rightarrow p$, и урадимо овакав задатак: заменимо формулом C само нека јављања исказног слова p у формули F, на пример његово прво и друго јављање с лева на десно. Резултат те замене је формула $F_2 = (((C \wedge q) \vee r) \wedge C) \Rightarrow p$.

Питамо се: да ли ову замену само неких јављања исказног слова p можемо описати помоћу униформне замене? Одговор је: ДА. Тај поступак покажимо за формулу F из Примера 4. Пре поступка замене само првог и другог (с лева на десно) јављања исказног слова p у формули F вратимо се „корак назад" на формулу $\overline{F} = (((s \wedge q) \vee r) \wedge s) \Rightarrow p$ у којој су јављања исказног слова p из формуле F која хоћемо да заменимо формулом C представљена исказним словом које се не јавља у F, словом s, а она јављања исказног слова p из формуле F која нећемо да заменимо су остала исказно слово p. Формулу $\overline{F}$ можемо сликовито да назовемо претходница формуле F за примену замене само неких јављања исказног слова p. Сада посматрамо формулу $\overline{F}$. Имамо да је наша полазна формула F резултат једне униформне замене у формули $\overline{F}$, тј. F је $\overline{F}^s_p$, а тражена формула F_2 је резултат опет једне униформне замене у формули $\overline{F}$, тј. F_2 је $\overline{F}^s_C$. Дакле, у некој формули F замена произвољном формулом C само неких јављања изабраног исказног слова p је у ствари једна униформна замена у формули претходници формуле F, формули $\overline{F}$, у којој су јављања исказног слова p, која треба да буду замењена, названа новим исказним словом.

Сада ћемо дефинисати важно својство које може повезивати исказне формуле, еквивалентност формула, и које има веома значајну улогу у поступцима замене.

Дефиниција еквивалентних формула

Две исказне формуле A и B су логички еквивалентне (или краће, еквивалентне) АККО је формула $A \Leftrightarrow B$ таутологија, тј. $\models A \Leftrightarrow B$.

А ево и неких својстава еквивалентних формула.

Задатак 1 Покажимо следеће својство еквивалентних формула: формуле A и B су еквивалентне ако и само ако за сваку валуацију v важи $v(A) = v(B)$.
Претпоставимо да су формуле A и B еквивалентне. То значи да је $A \Leftrightarrow B$ таутологија, тј. за сваку валуацију v важи $v(A \Leftrightarrow B) = 1$. На основу дефиниције валуације, из $v(A \Leftrightarrow B) = 1$, следи $v(A) = v(B)$. С друге стране, ако за сваку валуацију v важи $v(A) = v(B)$, онда по дефиницији валуације за сваку валуацију v имамо: $v(A \Leftrightarrow B) = 1$. Дакле, формула $A \Leftrightarrow B$ је таутологија, тј. формуле A и B су еквивалентне.

Задатак 2 На скупу свих исказних формула $\mathcal{F}$ дефинишемо бинарну релацију $\equiv$ на следећи начин:

$A \equiv B$ АККО формуле A и B су еквивалентне.

Покажимо да је $\equiv$ једна релација еквиваленције на скупу $\mathcal{F}$.
Рефлексивност. Формула $A \Leftrightarrow A$ је таутологија, па важи: $A \equiv A$.
Симетричност. Да ли важи особина: ако је $A \equiv B$, онда је $B \equiv A$? По дефиницији релације $\equiv$ требало би да проверимо да ли важи следећа особина: ако је $\models A \Leftrightarrow B$, онда је $\models B \Leftrightarrow A$, тј. да за сваку валуацију v важи: ако је $v(A) = v(B)$, онда је $v(B) = v(A)$. То важи на основу симетричности релације једнакости, па закључујемо да је релација $\equiv$ симетрична.
Транзитивност. Да ли важи: ако је $A \equiv B$ и $B \equiv C$, онда је $A \equiv C$? По дефиницији релације $\equiv$ то значи да испитујемо да ли важи следећа особина: ако је $\models A \Leftrightarrow B$ и $\models B \Leftrightarrow C$, онда је $\models A \Leftrightarrow C$, тј. да за сваку валуацију v: из $v(A) = v(B)$ и $v(B) = v(C)$ следи $v(A) = v(C)$. То важи на основу транзитивности релације једнакости, па закључујемо да је релација $\equiv$ транзитивна.
Дакле, релација еквивалентности формула $\equiv$ јесте једна релација еквиваленције на скупу свих исказних формула $\mathcal{F}$.

Надаље ћемо често за неке еквивалентне формуле A и B говорити и A је еквивалентна формули B. Истакнимо две најинтересантније класе еквиваленције релације $\equiv$. Једна је класа формуле $\top$ коју чине све формуле еквивалентне формули $\top$. Дакле, класу формуле $\top$ чине све таутологије. Друга класа је класа формуле $\bot$, класа којој припадају све контрадикције.

Покажимо сада неке важне особине које имају еквивалентне формуле.

ЛЕМА 1 (ЛЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА)

(1) Ако је $\models A \Leftrightarrow B$, онда је $\models \neg A \Leftrightarrow \neg B$.

(2) Ако је $\models A \Leftrightarrow B$, онда за произвољну формулу C важи:

($\wedge$1)	$\models (C \wedge A) \Leftrightarrow (C \wedge B)$	и	($\wedge$2)	$\models (A \wedge C) \Leftrightarrow (B \wedge C)$;
($\vee$1)	$\models (C \vee A) \Leftrightarrow (C \vee B)$	и	($\vee$2)	$\models (A \vee C) \Leftrightarrow (B \vee C)$;
($\Rightarrow$1)	$\models (C \Rightarrow A) \Leftrightarrow (C \Rightarrow B)$	и	($\Rightarrow$2)	$\models (A \Rightarrow C) \Leftrightarrow (B \Rightarrow C)$;
($\Leftrightarrow$1)	$\models (C \Leftrightarrow A) \Leftrightarrow (C \Leftrightarrow B)$	и	($\Leftrightarrow$2)	$\models (A \Leftrightarrow C) \Leftrightarrow (B \Leftrightarrow C)$.

ДОКАЗ

Из таутологије $\models A \Leftrightarrow B$ добијамо да су формуле A и B еквивалентне. Стога за сваку валуацију v важи: $v(A) = v(B)$.
(1) Потребно је показати да је за сваку валуацију v вредност $v(\neg A)$ једнака вредности $v(\neg B)$. По дефиницији валуације за сваку валуацију v имамо:

$$v(\neg A) = 1 - v(A) \quad \text{и} \quad v(\neg B) = 1 - v(B).$$

Како за сваку валуацију v важи $v(A) = v(B)$, онда имамо:

$$v(\neg A) = 1 - v(A) = 1 - v(B) = v(\neg B).$$

Добили смо да за сваку валуацију v важи:

$$v(\neg A) = v(\neg B).$$

Дакле, формуле $\neg A$ и $\neg B$ су еквивалентне, тј. важи:

$$\models \neg A \Leftrightarrow \neg B.$$

(2) Доказаћемо делове ($\wedge$1) и ($\Leftrightarrow$1). Делови ($\wedge$2), ($\vee$1), ($\vee$2), ($\Rightarrow$1) и ($\Rightarrow$2) се доказују аналогно као део ($\wedge$1), а део ($\Leftrightarrow$2) као део ($\Leftrightarrow$1). Нека је C произвољна формула.

($\wedge$1) По дефиницији валуације за сваку валуацију v имамо:

$$v(C \wedge A) = min(v(C), v(A)) \quad \text{и} \quad v(C \wedge B) = min(v(C), v(B)).$$

Пошто за сваку валуацију v важи $v(A) = v(B)$, онда добијамо:

$$v(C \wedge A) = min(v(C), v(A)) = min(v(C), v(B)) = v(C \wedge B).$$

Дакле, за сваку валуацију важи: $v(C \wedge A) = v(C \wedge B)$. Стога су формуле $C \wedge A$ и $C \wedge B$ еквивалентне, тј. важи:

$$\models (C \wedge A) \Leftrightarrow (C \wedge B).$$

($\Leftrightarrow$1) Све валуације можемо поделити у две скупине. У једној су валуације v за које су вредности $v(A)=v(B)$ и $v(C)$ једнаке, а у другој су валуације v за које су вредности $v(A)=v(B)$ и $v(C)$ различите. За валуације v за које су вредности $v(A) = v(B)$ и $v(C)$ једнаке, по дефиницији валуације имамо:

$$v(C \Leftrightarrow A) = 1 \quad \text{и} \quad v(C \Leftrightarrow B) = 1.$$

За валуације v за које су вредности $v(A) = v(B)$ и $v(C)$ различите, по дефиницији валуације имамо:

$$v(C \Leftrightarrow A) = 0 \quad \text{и} \quad v(C \Leftrightarrow B) = 0.$$

Дакле, у оба случаја смо добили:

$$v(C \Leftrightarrow A) = v(C \Leftrightarrow B),$$

па закључујемо да су за сваку валуацију v вредности $v(C \Leftrightarrow A)$ и $v(C \Leftrightarrow B)$ једнаке, тј. важи:

$$\models (C \Leftrightarrow A) \Leftrightarrow (C \Leftrightarrow B).$$

♢

Сада ћемо формулисати веома важну теорему, теорему о замени еквивалената, која најјасније показује важност еквивалентних формула у поступку замене.

ТЕОРЕМА 1 (ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА)
За произвољне формуле C, D и F и неко исказно слово p важи:

$$\text{ако је } \models C \Leftrightarrow D, \text{ онда је } \models F_C^p \Leftrightarrow F_D^p.$$

Пре него што докажемо ТЕОРЕМУ О ЗАМЕНИ ЕКВИВАЛЕНАТА, погледајмо шта нам она даје. Имамо формулу F, неко исказно слово p и међусобно еквивалентне формуле C и D. Од формуле F униформном заменом исказног слова p формулом C добијамо формулу F_C^p и униформном заменом истог слова p формулом D добијамо формулу F_D^p. Питамо се: у каквој су вези формуле F_C^p и F_D^p? На основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА имамо да су те две формуле еквивалентне. Другачије речено, еквивалентност формула C и D се униформном заменом пренела на формуле F_C^p и F_D^p.

ДОКАЗ ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА

Посматрајмо произвољну формулу F. Теорему ћемо доказати индукцијом по броју бинарних логичких везника у формули F.

База индукције, F има 0 бинарних везника, тј. F је или $\bot$ или неко исказно слово.
Ако је F формула $\bot$, онда је $F_C^p = \bot_C^p = \bot$ и $F_D^p = \bot_D^p = \bot$, па важи $\models F_C^p \Leftrightarrow F_D^p$.
Ако је F исказно слово q различито од p, онда је $F_C^p = q_C^p = q$ и $F_D^p = q_D^p = q$. Дакле, формула $F_C^p \Leftrightarrow F_D^p$ је таутологија $q \Leftrightarrow q$, па важи $\models F_C^p \Leftrightarrow F_D^p$.
Ако је F баш исказно слово p, тада имамо да је $F_C^p = p_C^p = C$ и $F_D^p = p_D^p = D$. Како важи $\models C \Leftrightarrow D$, то значи да важи: $\models F_C^p \Leftrightarrow F_D^p$.

Индукцијска претпоставка: теорема важи за сваку формулу F која има мање од n бинарних логичких везника.

Докажимо да теорема важи и за формулу која има n везника.
Посматрајмо формулу F која има n бинарних везника. Формула F може имати један од следећих облика:

$$A \wedge B, \qquad A \vee B \qquad \text{или} \qquad A \Rightarrow B.$$

Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка, тј. имамо таутологије:

$$\models A_C^p \Leftrightarrow A_D^p \qquad \text{и} \qquad \models B_C^p \Leftrightarrow B_D^p.$$

$\triangleleft$ Претпоставимо да је формула F облика $A \wedge B$.
На основу дефиниције функције униформне замене имамо:

$$F_C^p \text{ је формула } A_C^p \wedge B_C^p \quad \text{и} \quad F_D^p \text{ је формула } A_D^p \wedge B_D^p.$$

За таутологију $\models B_C^p \Leftrightarrow B_D^p$ и формулу A_C^p важи део ($\wedge$1) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \wedge B_C^p) \Leftrightarrow (A_C^p \wedge B_D^p),$$

па су формуле $A_C^p \wedge B_C^p$ и $A_C^p \wedge B_D^p$ еквивалентне. Исто тако, за таутологију $\models A_C^p \Leftrightarrow A_D^p$ и формулу B_D^p важи део ($\wedge 2$) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \wedge B_D^p) \Leftrightarrow (A_D^p \wedge B_D^p),$$

па су формуле $A_C^p \wedge B_D^p$ и $A_D^p \wedge B_D^p$ еквивалентне. На основу транзитивности релације $\equiv$ из еквивалентности формула $A_C^p \wedge B_C^p$ и $A_C^p \wedge B_D^p$ и еквивалентности формула $A_C^p \wedge B_D^p$ и $A_D^p \wedge B_D^p$ добијамо еквивалентност формула $A_C^p \wedge B_C^p$ и $A_D^p \wedge B_D^p$.
Дакле, имамо таутологију $\models (A_C^p \wedge B_C^p) \Leftrightarrow (A_D^p \wedge B_D^p)$, тј. таутологију $\models F_C^p \Leftrightarrow F_D^p$.

◁ Претпоставимо да је формула F облика $A \vee B$.
На основу дефиниције функције униформне замене имамо:

$$F_C^p \text{ је формула } A_C^p \vee B_C^p \quad \text{и} \quad F_D^p \text{ је формула } A_D^p \vee B_D^p.$$

За таутологију $\models B_C^p \Leftrightarrow B_D^p$ и формулу A_C^p важи део ($\vee 1$) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \vee B_C^p) \Leftrightarrow (A_C^p \vee B_D^p),$$

па су формуле $A_C^p \vee B_C^p$ и $A_C^p \vee B_D^p$ еквивалентне. За таутологију $\models A_C^p \Leftrightarrow A_D^p$ и формулу B_D^p важи део ($\vee 2$) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \vee B_D^p) \Leftrightarrow (A_D^p \vee B_D^p),$$

па су формуле $A_C^p \vee B_D^p$ и $A_D^p \vee B_D^p$ еквивалентне. На основу транзитивности релације $\equiv$ из еквивалентности формула $A_C^p \vee B_C^p$ и $A_C^p \vee B_D^p$ и еквивалентности формула $A_C^p \vee B_D^p$ и $A_D^p \vee B_D^p$ добијамо еквивалентност формула $A_C^p \vee B_C^p$ и $A_D^p \vee B_D^p$.
Дакле, имамо таутологију $\models (A_C^p \vee B_C^p) \Leftrightarrow (A_D^p \vee B_D^p)$, тј. таутологију $\models F_C^p \Leftrightarrow F_D^p$.

◁ Претпоставимо да је формула F облика $A \Rightarrow B$.
На основу дефиниције функције униформне замене имамо:

$$F_C^p \text{ је формула } A_C^p \Rightarrow B_C^p \quad \text{и} \quad F_D^p \text{ је формула } A_D^p \Rightarrow B_D^p.$$

За таутологију $\models B_C^p \Leftrightarrow B_D^p$ и формулу A_C^p важи део ($\Rightarrow 1$) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \Rightarrow B_C^p) \Leftrightarrow (A_C^p \Rightarrow B_D^p),$$

па су формуле $A_C^p \Rightarrow B_C^p$ и $A_C^p \Rightarrow B_D^p$ еквивалентне. Исто тако за таутологију $\models A_C^p \Leftrightarrow A_D^p$ и формулу B_D^p важи део ($\Rightarrow 2$) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА:

$$\models (A_C^p \Rightarrow B_D^p) \Leftrightarrow (A_D^p \Rightarrow B_D^p),$$

па су формуле $A_C^p \Rightarrow B_D^p$ и $A_D^p \Rightarrow B_D^p$ еквивалентне. На основу транзитивности релације $\equiv$ из еквивалентности формула $A_C^p \Rightarrow B_C^p$ и $A_C^p \Rightarrow B_D^p$ и еквивалентности формула $A_C^p \Rightarrow B_D^p$ и $A_D^p \Rightarrow B_D^p$ добијамо еквивалентност формуле $A_C^p \Rightarrow B_C^p$ и формуле $A_D^p \Rightarrow B_D^p$.

Дакле, имамо таутологију $\models (A^p_C \Rightarrow B^p_C) \Leftrightarrow (A^p_D \Rightarrow B^p_D)$, тј. таутологију $\models F^p_C \Leftrightarrow F^p_D$.

Доказавши да особина важи за сваку формулу F са n бинарних везника, ми смо доказали да важи индукцијски корак, па закључујемо да за произвољну формулу F (тј. формулу са произвољним бројем n бинарних везника) и исказно слово p из $\models C \Leftrightarrow D$ следи $\models F^p_C \Leftrightarrow F^p_D$.

$\diamondsuit$

После доказа ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА наводимо један типичан пример примене те теореме.

Пример 6 Посматрајмо формулу F:

$$(r \Rightarrow (p \wedge \top)) \Rightarrow (q \vee (\neg(p \wedge \top))),$$

њену потформулу $p \wedge \top$ и њој еквивалентну формулу p (на основу таутологије (1) $(p \wedge \top) \Leftrightarrow p$ из одељка 2.2.1). Приметимо да се потформула $p \wedge \top$ јавља два пута у формули F, тј. има два јављања у формули F. Само једно јављање потформуле $p \wedge \top$ у F, прво с лева, замењујемо њој еквивалентном формулом p и добијамо формулу F_1: $(r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top)))$. Расуђујемо овако: формуле $p \wedge \top$ и p су еквивалентне, па на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА

формуле F и $(r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top)))$ су еквивалентне,

тј. формула $F \Leftrightarrow ((r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top))))$ је таутологија.

Слично закључивање ће се често појављивати у нашем даљем излагању и тада нећемо улазити у детаљно објашњавање и оправдавање тог закључивања. Овде ћемо анализирати и детаљније оправдати овакво закључивање. Шта смо ми у ствари урадили? Користећи еквивалентност формула $p \wedge \top$ и p, једно јављање формуле $p \wedge \top$ у формули F смо заменили формулом p. Тврдимо да на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА можемо закључити да је тако добијена формула, формула $F_1 = (r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top)))$, еквивалентна формули F. Иза замене потформуле $p \wedge \top$ формуле F њој еквивалентном формулом p стоји, како смо је звали, претходница формула F и F_1, формула

$$(r \Rightarrow s) \Leftrightarrow (q \vee (\neg(p \wedge \top)))$$

у којој је јављање потформуле $p \wedge \top$ које хоћемо да заменимо „названо" посебним исказним словом s. Дакле, ми у ствари посматрамо формулу $(r \Rightarrow s) \Leftrightarrow (q \vee (\neg(p \wedge \top)))$, њено исказно слово s и таутологију $\models (p \wedge \top) \Leftrightarrow p$, па на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА добијамо:

$$\models ((r \Rightarrow s) \Rightarrow (q \vee (\neg(p \wedge \top))))^s_{p \wedge \top} \Leftrightarrow ((r \Rightarrow s) \Rightarrow (q \vee (\neg(p \wedge \top))))^s_p$$

тј. добијамо:

$$\models F \Leftrightarrow ((r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top)))).$$

Дакле, наш закључак да су формуле F и $(r \Rightarrow p) \Rightarrow (q \vee (\neg(p \wedge \top)))$ еквивалентне је исправан и јесте заснован на ТЕОРЕМИ О ЗАМЕНИ ЕКВИВАЛЕНАТА.

У излагању које следи ми ћемо у случајевима као што је овај описан у Примеру 6 говорити о примени ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, а у ствари то ће бити примена следеће њене последице.

ПОСЛЕДИЦА 1 (ПОСЛЕДИЦА ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА)
Нека је F произвољна формула, а формула A једна њена потформула. Ако се у формули F нека јављања потформуле A замене неком формулом B еквивалентном формули A, добија се формула F_1 која је еквивалентна формули F, тј. важи:

$$\models F \Leftrightarrow F_1.$$

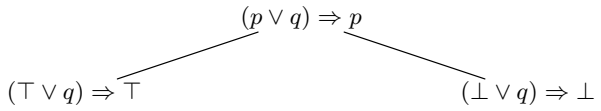
Како се особина из ПОСЛЕДИЦЕ 1 добија из ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, описано је у Примеру 6 за конкретну формулу F.

2.2.3 Метода чишћења

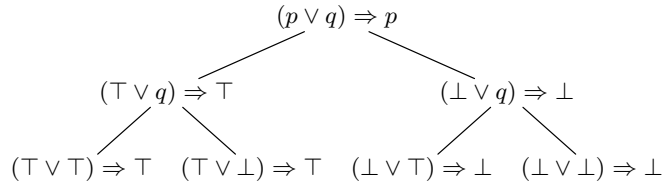
Одмах на почетку одељка представимо методу чишћења на једном једноставном примеру.

Пример 7 Методом чишћења испитајмо да ли је формула $(p \vee q) \Rightarrow p$ таутологија. Метода чишћења је следећи поступак. Полазимо од формуле $(p \vee q) \Rightarrow p$, бирамо једно исказно слово које се појављује у тој формули, на пример p, правимо следеће формуле:

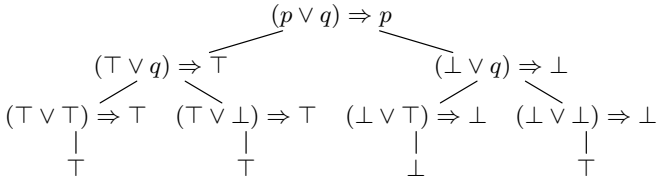
$((p \vee q) \Rightarrow p)^p_\top = (\top \vee q) \Rightarrow \top$ и $((p \vee q) \Rightarrow p)^p_\bot = (\bot \vee q) \Rightarrow \bot$
и формирамо дрво:



У наредном кораку посматрамо формулу $(\top \vee q) \Rightarrow \top$ и формулу $(\bot \vee q) \Rightarrow \bot$ и опет бирамо неко исказно слово тих формула. Оне имају само једно исказно слово, слово q, па можемо изабрати једино то исказно слово. Свака од тих формула се грана на две формуле такве да је у једној q замењено са $\top$, а у другој је q замењено са $\bot$ и добијамо дрво:

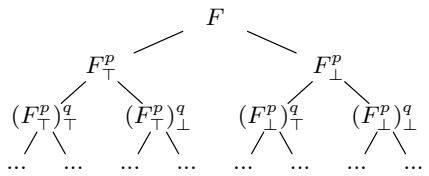


На листовима овог дрвета добили смо формуле у којима нема исказних слова. У последњем кораку сваку од тих формула повезујемо са њој еквивалентном формулом, једном од формула $\bot$ или $\top$. Резултат тог поступка је дрво:



Овим кораком поступак прављења дрвета је завршен и сада посматрамо листове овог дрвета. Да смо на свим листовима добили формулу $\top$, закључили бисмо да је наша полазна формула $(p \vee q) \Rightarrow p$ таутологија. Међутим, на једном листу је формула $\bot$, па закључујемо да формула $(p \vee q) \Rightarrow p$ није таутологија.

Како метода чишћења изгледа за произвољну формулу F? Полазимо од формуле F, бирамо једно исказно слово које се појављује у тој формули, на пример p, и вршимо гранање од формуле F (као у Примеру 7), тј. правимо формулу $F^p_\top$ (тако што у формули F свако јављање исказног слова p замењујемо формулом $\top$) и формулу $F^p_\bot$ (тако што у формули F свако јављање исказног слова p замењујемо формулом $\bot$). Затим бирамо следеће исказно слово формуле F, на пример q, и вршимо гранање сваке од формула $F^p_\top$ и $F^p_\bot$ тј. користећи формулу $F^p_\top$ правимо формуле $(F^p_\top)^q_\top$ и $(F^p_\top)^q_\bot$, а користећи формулу $F^p_\bot$ правимо формуле $(F^p_\bot)^q_\top$ и $(F^p_\bot)^q_\bot$. Поступак настављамо избором новог исказног слова формуле F (различитог од p и q) и гранањем формула $(F^p_\top)^q_\top$, $(F^p_\top)^q_\bot$, $(F^p_\bot)^q_\top$ и $(F^p_\bot)^q_\bot$. Графички то можемо да представимо следећим дрветом:

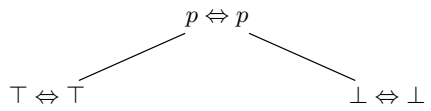


Поступак гранања се завршава када се (примењујући замене исказних слова формулама $\top$ и $\bot$) добију формуле у којима нема исказних слова. Последњи

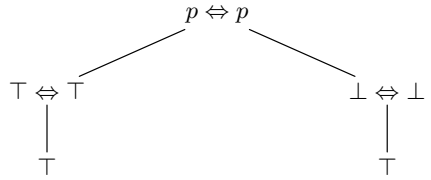
корак је да направимо листове, тј. да сваку од тих формула повежемо са оном од формула $\top$ или $\bot$ којој је та формула еквивалентна. Дакле, на листовима дрвета које добијамо описаним поступком могу се налазити само формуле $\top$ и $\bot$. Подсетимо се да том методом испитујемо да ли је нека формула F, која нам је дата, таутологија. Зато када направимо овакво дрво, онда у зависности од тога које формуле се налазе на његовим листовима, закључујемо да ли је полазна формула F таутологија или није. Ако се на свим листовима налази формула $\top$, онда је полазна формула F таутологија. Ако се на свим листовима налази формула $\bot$, онда је формула F контрадикција. Ако се на листовима појављују обе формуле и $\top$ и $\bot$, онда та формула није ни таутологија ни контрадикција.

Пре него што докажемо да је овакво закључивање исправно, погледајмо још два једноставна примера.

Пример 8 Покажимо да је формула $p \Leftrightarrow p$ таутологија. У тој формули појављује се само исказно слово p, зато правимо формуле $(p \Leftrightarrow p)^p_\top = \top \Leftrightarrow \top$ и $(p \Leftrightarrow p)^p_\bot = \bot \Leftrightarrow \bot$:

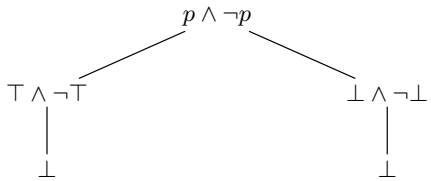


У овом једноставном примеру већ смо првим кораком гранања добили формуле у којима нема исказних слова. Преостаје нам да направимо листове, тј. формулу $\top \Leftrightarrow \top$ повежемо са њој еквивалентном формулом $\top$ и исто тако формулу $\bot \Leftrightarrow \bot$ повежемо са њој еквивалентном формулом $\top$:



На свим листовима смо добили формулу $\top$ и закључујемо да је формула $p \Leftrightarrow p$ таутологија.

Пример 9 Покажимо да је формула $p \wedge \neg p$ контрадикција. Као и у претходном примеру исказно слово p замењујемо формулама $\top$ и $\bot$ и добијамо дрво:



На свим листовима смо добили формулу $\bot$ и закључујемо да је формула $p \wedge \neg p$ контрадикција.

После ових једноставних примера погледајмо на чему се заснива метода чишћења. Полазимо од неке формуле F и показаним поступком правимо дрво на чијим листовима могу бити само $\bot$ или $\top$. Ако смо на свим листовима добили формуле $\top$, ми тврдимо да је полазна формула таутологија. То закључивање оправдавамо следећим својством за произвољну формулу E (које ћемо убрзо доказати): формула E је таутологија ако и само ако су формуле $E^r_\top$ и $E^r_\bot$ таутологије. Дакле, ако су на листовима тог дрвета таутологије $\top$, почињемо да се од листова враћамо ка нашој полазној формули F. У сваком кораку враћања ми прелазимо са неких формула $E^r_\top$ и $E^r_\bot$ на формулу E и користимо овај део поменутог својства: ако су формуле $E^r_\top$ и $E^r_\bot$ таутологије, онда је и формула E таутологија. У последњем кораку враћања користимо то својство и прелазимо са таутологија $F^p_\top$ и $F^p_\bot$ на формулу F и закључујемо да је наша полазна формула F таутологија.

Да поменуто својство важи тврди наредна теорема.

ТЕОРЕМА 2
Формула F је таутологија ако и само ако су формуле $F^p_\top$ и $F^p_\bot$ таутологије.

Пре него што докажемо ову теорему погледајмо један пример.

Пример 10 Посматрајмо формулу F из Примера 2, формулу $(p \wedge (p \Rightarrow q)) \Rightarrow q$. За било коју валуацију v вредност $v(F)$ рачунамо на следећи начин:

$$\begin{aligned} v(F) &= max(1 - v(p \wedge (p \Rightarrow q)), v(q)) \\ &= max(1 - min(v(p), v(p \Rightarrow q)), v(q)) \\ &= max(1 - min(v(p), max(1 - v(p), v(q))), v(q)). \end{aligned}$$

А сада погледајмо формуле

$$F^p_\top = (\top \wedge (\top \Rightarrow q)) \Rightarrow q \quad \text{и} \quad F^p_\bot = (\bot \wedge (\bot \Rightarrow q)) \Rightarrow q.$$

За било коју валуацију v вредност $v(F^p_\top)$ рачунамо на исти начин као $v(F)$ само што уместо $v(p)$ стављамо $v(\top)$:

$$v(F^p_\top) = max(1 - min(v(\top), max(1 - v(\top), v(q))), v(q)).$$

Исто тако, вредност $v(F^p_\bot)$ рачунамо на исти начин као $v(F)$ само што уместо $v(p)$ стављамо $v(\bot)$:

$$v(F^p_\bot) = max(1 - min(v(\bot), max(1 - v(\bot), v(q))), v(q)).$$

Наш први задатак је да за произвољну валуацију v користећи формулу F, одредимо $v(F^p_\top)$ и $v(F^p_\bot)$. Ако хоћемо да одредимо $v(F^p_\top)$, онда узимамо произвољну валуацију v_1 са особином да се њом исказно слово p слика у 1, тј. $v_1(p) = 1 = v(\top)$, а на осталим исказним словима формуле F та валуација се поклапа са v. У нашем примеру

формула F осим p има још само исказно слово q, па узимамо валуацију v_1 за коју је $v_1(p) = 1$ и $v_1(q) = v(q)$ и добијамо:

$$v(F^p_\top) = max(1 - min(v(\top), max(1 - v(\top), v(q))), v(q))$$
$$= max(1 - min(v_1(p), max(1 - v_1(p), v_1(q))), v_1(q)) = v_1(F).$$

Аналогно томе, када рачунамо вредност $v(F^p_\bot)$ можемо узети произвољну валуацију v_2 са особином да p слика у 0, а на осталим исказним словима се поклапа са v и за њу важи:

$$v(F^p_\bot) = v_2(F).$$

Други задатак је да за неку валуацију v израчунамо вредност $v(F)$, користећи вредности $v(F^p_\top)$ и $v(F^p_\bot)$. Важна је вредност слова p том валуацијом v. Ако је $v(p) = 1$, онда је $v(p) = v(\top)$ и имамо:

$$v(F) = max(1 - min(v(p), max(1 - v(p), v(q))), v(q))$$
$$= max(1 - min(v(\top), max(1 - v(\top), v(q))), v(q)) = v(F^p_\top).$$

А ако је $v(p) = 0$, онда је $v(p) = v(\bot)$ и имамо:

$$v(F) = max(1 - min(v(p), max(1 - v(p), v(q))), v(q))$$
$$= max(1 - min(v(\bot), max(1 - v(\bot), v(q))), v(q)) = v(F^p_\bot).$$

Особина коју смо показали у Примеру 10 важи и у општем случају. Посматрамо произвољну валуацију v и формулу F у којој се осим исказног слова p појављују још и исказна слова p_1, ..., p_n, где број тих слова може бити и нула. Ако је v_1 валуација таква да слово p слика у 1, тј. $v_1(p) = 1$, а на свим осталим исказним словима формуле F (ако та слова постоје), исказним словима p_1,...,p_n, се поклапа са валуацијом v, тј. $v_1(p_i) = v(p_i)$, $1 \leq i \leq n$, онда имамо:

$$v(F^p_\top) = v_1(F).$$

Ако је v_2 валуација таква да исказно слово p слика у 0, тј. $v_2(p) = 0$, а на свим осталим исказним словима формуле F (ако та слова постоје), исказним словима p_1, ..., p_n, се поклапа са валуацијом v, тј. $v_2(p_i) = v(p_i)$, $1 \leq i \leq n$, онда имамо:

$$v(F^p_\bot) = v_2(F).$$

С друге стране, за произвољну валуацију v вредност $v(F)$ рачунамо овако:

ако је $v(p) = 1$, онда је $v(F) = v(F^p_\top)$;
ако је $v(p) = 0$, онда је $v(F) = v(F^p_\bot)$.

Користећи ова својства, докажимо ТЕОРЕМУ 2.

ДОКАЗ ТЕОРЕМЕ 2

Нека се у формули F осим исказног слова p јављају и исказна слова p_1,..., p_n, где број тих слова може бити и нула.
Доказ дела: Ако је F таутологија, онда су и $F^p_\top$ и $F^p_\bot$ таутологије.
Ако за произвољну валуацију v:$\mathcal{F} \to \{0, 1\}$ покажемо да је $v(F^p_\top) = 1$ и $v(F^p_\bot) = 1$ то ће значити да су те формуле таутологије. Докажимо да је $v(F^p_\top) = 1$. Узмимо валуацију v_1 која исказно слово p слика у 1, тј. $v_1(p) = 1$, а на свим исказним словима p_1,..., p_n (ако та слова

постоје) се поклапа са валуацијом v, тј. $v_1(p_i) = v(p_i)$, $1 \leq i \leq n$. Имамо (као у Примеру 10) да важи:

$$v(F^p_\top) = v_1(F).$$

Формула F је таутологија, па је и за валуацију v_1 истинита, тј. важи $v_1(F) = 1$. Стога из $v(F^p_\top) = v_1(F)$ и $v_1(F) = 1$ добијамо $v(F^p_\top) = 1$. Дакле, показали смо да за произвољну валуацију v важи $v(F^p_\top) = 1$. То значи да је формула $F^p_\top$ таутологија. (Доказ да је формула $F^p_\bot$ таутологија је аналоган овом доказу.)

Доказ дела: Ако су $F^p_\top$ и $F^p_\bot$ таутологије, онда је и F таутологија.

Све валуације можемо разврстати на оне које исказно слово p сликају у 1 и оне које p сликају у 0.

$\lhd_1$ За сваку валуацију v којом се исказно слово p слика у 1, тј. $v(p) = 1$ (као у Примеру 10), важи:

$$v(F) = v(F^p_\top).$$

Формула $F^p_\top$ је таутологија, па имамо $v(F^p_\top) = 1$. Из $v(F) = v(F^p_\top)$ и $v(F^p_\top) = 1$ добијамо $v(F) = 1$.

$\lhd_2$ За сваку валуацију v којом се исказно слово p слика у 0, тј. $v(p) = 0$ (као у Примеру 10), важи:

$$v(F) = v(F^p_\bot).$$

Формула $F^p_\bot$ је таутологија, па имамо $v(F^p_\bot) = 1$. Из $v(F) = v(F^p_\bot)$ и $v(F^p_\bot) = 1$ добијамо $v(F) = 1$.

Дакле, за сваку валуацију v важи: $v(F) = 1$. Закључујемо да је формула F таутологија.

♢

ТЕОРЕМА 3

Ако је p произвољно исказно слово неке формуле F и формула F је таутологија, онда је за произвољну формулу C и формула F^p_C таутологија.

ДОКАЗ

Ако за сваку валуацију $v : \mathcal{F} \to \{0, 1\}$ покажемо да је формула F^p_C истинита, тј. да је $v(F^p_C) = 1$, то ће значити да је та формула таутологија. Вредност $v(C)$ може бити или 1 или 0.

$\lhd_1$ Ако је $v(C) = 1$, онда је $v(C) = v(\top)$, па имамо да је $v(F^p_C)$ једнако $v(F^p_\top)$. Формула F је таутологија, па на основу ТЕОРЕМЕ 2 и формула $F^p_\top$ је таутологија, тј. $v(F^p_\top) = 1$. Из тога следи да је $v(F^p_C) = 1$.

$\lhd_2$ Ако је $v(C) = 0$, онда је $v(C) = v(\bot)$, па имамо да је $v(F^p_C)$ једнако $v(F^p_\bot)$. Опет на основу тога што је формула F таутологија користећи ТЕОРЕМУ 2, добијамо да је формула $F^p_\bot$ таутологија, па је опет $v(F^p_C) = 1$.

Дакле, добили смо да је формула F^p_C истинита за сваку валуацију v, па закључујемо да је формула F^p_C таутологија.

♢

Овом теоремом свака таутологија постаје, сликовито речено, једна схема за прављење нових таутологија тако да у њој свако исказно слово може бити замењено произвољном исказном формулом и том заменом се добија нова таутологија. На пример, таутологија $p \Rightarrow p$ и ТЕОРЕМА 3 нам омогућавају прављење следећих таутологија:

$A \Rightarrow A$, где је p замењено са A;

$(A \Rightarrow C) \Rightarrow (A \Rightarrow C)$, где је p замењено са $A \Rightarrow C$, и тако даље.

Исто тако, таутологија $(p \wedge (p \Rightarrow q)) \Rightarrow q$, на основу ТЕОРЕМЕ 3, даје таутологију:

$$((p \wedge (p \Rightarrow q)) \Rightarrow q)^p_A = (A \wedge (A \Rightarrow q)) \Rightarrow q.$$

Та нова таутологија на основу исте теореме даје таутологију:

$$((A \wedge (A \Rightarrow q)) \Rightarrow q)^q_B = (A \wedge (A \Rightarrow B)) \Rightarrow B.$$

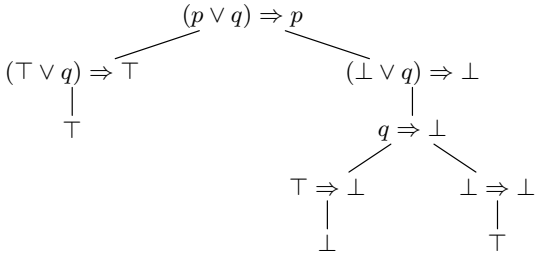
Приметимо да је таутологија $(A \wedge (A \Rightarrow B)) \Rightarrow B$ у ствари формула добијена из таутологије $(p \wedge (p \Rightarrow q)) \Rightarrow q$, када су два исказна слова p и q замењена редом формулама A и B, тј. $(A \wedge (A \Rightarrow B)) \Rightarrow B$ је формула $(((p \wedge (p \Rightarrow q)) \Rightarrow q)^p_A)^q_B$. То својство је представљено следећом последицом ТЕОРЕМЕ 3.

ПОСЛЕДИЦА 2 (ПОСЛЕДИЦА ТЕОРЕМЕ 3)
Ако је формула F таутологија и $p_1, ..., p_n$ $(n \geq 1)$ њена исказна слова, онда за произвољне формуле $C_1, ..., C_n$ и формула $F^{p_1 \dots p_n}_{C_1 \dots C_n}$ је таутологија.

У наредним примерима применићемо методу чишћења на неколико, да их тако назовемо, познатих таутологија. Пре тога погледајмо поново формулу из Примера 7. На овом примеру покажимо како поступак чишћења, који смо већ описали, можемо скратити, користећи таутологије из списка у одељку 2.2.1 и ТЕОРЕМУ 3. Након првог гранања добили смо формуле $(\top \vee q) \Rightarrow \top$ и $(\bot \vee q) \Rightarrow \bot$. Уместо да наставимо гранање заменама исказног слова q са $\top$ и $\bot$, урадићемо следеће. Користећи таутологију (9) $(p \Rightarrow \top) \Leftrightarrow \top$ и таутологију (8) $(\bot \vee p) \Leftrightarrow p$, на основу ТЕОРЕМЕ 3, добијамо редом таутологије:

$((p \Rightarrow \top) \Leftrightarrow \top)^p_{\top \vee q} = ((\top \vee q) \Rightarrow \top) \Leftrightarrow \top$ и $((\bot \vee p) \Leftrightarrow p)^p_q = (\bot \vee q) \Leftrightarrow q$.

Из таутологије $((\top \vee q) \Rightarrow \top) \Leftrightarrow \top$ следи да је формула $(\top \vee q) \Rightarrow \top$ на левој грани еквивалентна формули $\top$. Из таутологије $(\bot \vee q) \Leftrightarrow q$, на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, добијамо да је формула $(\bot \vee q) \Rightarrow \bot$ на десној грани еквивалентна формули $q \Rightarrow \bot$. Зато дрво продужавамо тако што $(\top \vee q) \Rightarrow \top$ повезујемо са $\top$, а $(\bot \vee q) \Rightarrow \bot$ са $q \Rightarrow \bot$. Остаје нам још гранање формуле $q \Rightarrow \bot$ и добијамо дрво које је једноставније од дрвета из Примера 7:

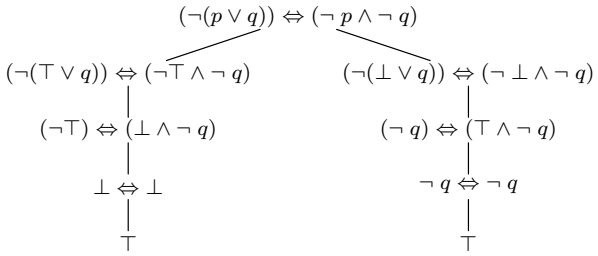


И у свим наредним примерима, при преласку са формуле у једном чвору (претходнику) на формулу у неком његовом наследнику, урадићемо следеће:

неке потформуле формуле из претходника замењујемо њима еквивалентним формулама и добијамо формулу у наследнику. Еквивалентност сваке те потформуле и оне формуле којом је замењујемо оправдано је неком од таутологија, најчешће оних наведених у одељку 2.2.1 (некад и ТЕОРЕМОМ 3 чију примену нећемо истицати). Формула у наследнику, која је резултат тих замена, еквивалентна је формули у претходнику на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА. Када будемо за неко дрво са две гране говорили о левој и десној грани тог дрвета то ће се односити на леву и десну грану од корена до листа тог дрвета.

Пример 11 Де Морганов закон: $(\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q)$.

Правимо дрво:



Првим гранањем направили смо формуле:

$$((\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q))^p_\top = (\neg(\top \vee q)) \Leftrightarrow (\neg\top \wedge \neg q)$$
$$((\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q))^p_\bot = (\neg(\bot \vee q)) \Leftrightarrow (\neg\bot \wedge \neg q).$$

Детаљно ћемо образложити како смо направили остале чворове леве гране овог дрвета. (Прављење његове десне гране и грана у наредним примерима неће бити тако детаљно образложено.)

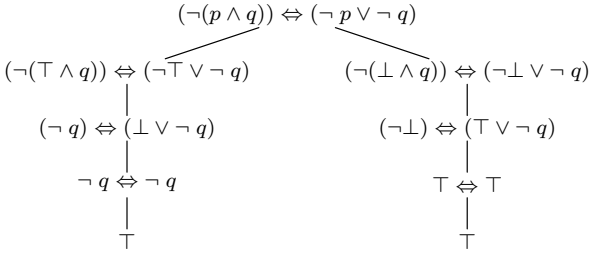
Први корак: из $(\neg(\top \vee q)) \Leftrightarrow (\neg\top \wedge \neg q)$ добијање $(\neg\top) \Leftrightarrow (\bot \wedge \neg q)$. На основу таутологије (6) и ТЕОРЕМЕ 3 формула $\top \vee q$ је еквивалентна формули $\top$, па је на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула $(\neg(\top \vee q)) \Leftrightarrow (\neg\top \wedge \neg q)$ еквивалентна $(\neg\top) \Leftrightarrow (\neg\top \wedge \neg q)$. На основу таутологије (17) формула $\neg\top$ је еквивалентна $\bot$, па је на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула $(\neg\top) \Leftrightarrow (\neg\top \wedge \neg q)$ еквивалентна формули $(\neg\top) \Leftrightarrow (\bot \wedge \neg q)$.

Други корак: из чвора $(\neg\top) \Leftrightarrow (\bot \wedge \neg q)$ добијање чвора $\bot \Leftrightarrow \bot$. На основу таутологије (17) формула $\neg\top$ је еквивалентна $\bot$, па је на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула $(\neg\top) \Leftrightarrow (\bot \wedge \neg q)$ еквивалентна формули $\bot \Leftrightarrow (\bot \wedge \neg q)$. На основу таутологије (4) и ТЕОРЕМЕ 3 формула $\bot \wedge \neg q$ је еквивалентна формули $\bot$, па је на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула $\bot \Leftrightarrow (\bot \wedge \neg q)$ еквивалентна формули $\bot \Leftrightarrow \bot$.

Трећи корак: из чвора $\bot \Leftrightarrow \bot$ добијање листа $\top$. На основу таутологије из Примера 8 и ТЕОРЕМЕ 3 формула $\bot \Leftrightarrow \bot$ је еквивалентна формули $\top$.

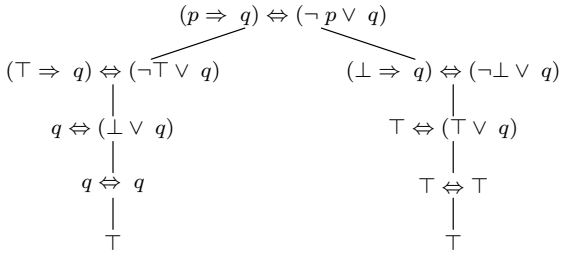
У десној грани овог дрвета користили смо редом, по корацима, таутологије: (8) и (18); (2); из Примера 8.

Пример 12 Де Морганов закон: $(\neg(p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$.
Правимо дрво:



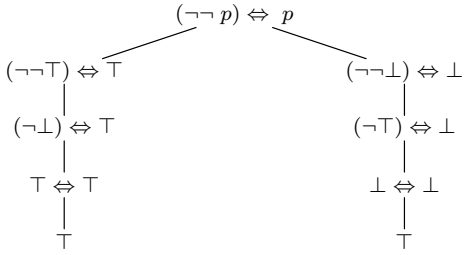
У левој грани овог дрвета користили смо редом, по корацима, тауто-логије: (2) и (17); (8); из Примера 8, а у његовој десној грани користили смо редом, по корацима, таутологије: (4) и (18); (18) и (6); (13).

Пример 13 Закон замене импликације: $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$.
Правимо дрво:



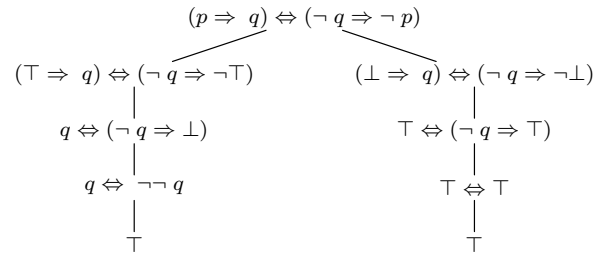
У левој грани овог дрвета користили смо редом, по корацима, тауто-логије: (10) и (17); (8); из Примера 8, а у његовој десној грани користили смо редом, по корацима, таутологије: (12) и (18); (6); (13).

Пример 14 Закон двојне негације: $(\neg\neg p) \Leftrightarrow p$.
Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, тауто-логије: (17); (18); (13), а у његовој десној грани користили смо редом, по корацима, таутологије: (18); (17); из Примера 8.

Пример 15 Закон контрапозиције: $(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$.
Правимо дрво:

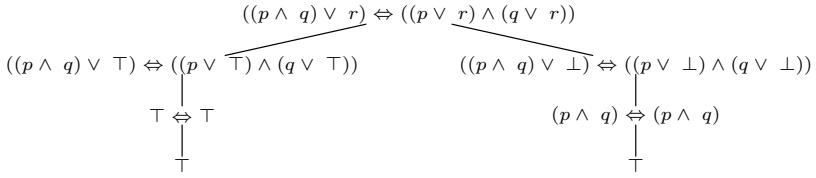


У левој грани овог дрвета користили смо редом, по корацима, тауто-логије: (10) и (17); (11); из Примера 14. У десној грани дрвета користили смо редом, по корацима, таутологије: (12) и (18); (9); (13).

Пример 16 Закон дистрибутивости $\vee$ у односу на $\wedge$:

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

Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, тауто-логије: (5) и (1); (13); а у његовој десној грани користили смо редом, по корацима, таутологије: (7); из Примера 8.

Сада дајемо списак таутологија у коме се поред већ поменутих таутологија налазе још неке значајне таутологије које ћемо користити у даљем излагању.

Закон рефлексивности за импликацију:	$p \Rightarrow p$
Закон искључења трећег:	$p \vee \neg p$
Закон непротивречности:	$\neg(p \wedge \neg p)$
Закон двојне негације:	$\neg\neg p \Leftrightarrow p$
Персов закон:	$((p \Rightarrow q) \Rightarrow p) \Rightarrow p$
Закон замене импликације:	$(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$
Закон замене еквиваленције:	$(p \Leftrightarrow q) \Leftrightarrow ((p \Rightarrow q) \wedge (q \Rightarrow p))$
Закон транзитивности за импликацију:	$(p \Rightarrow q) \Rightarrow ((q \Rightarrow r) \Rightarrow (p \Rightarrow r))$
Закон транзитивности за еквиваленцију:	$((p \Leftrightarrow q) \wedge (q \Leftrightarrow r)) \Rightarrow (p \Leftrightarrow r)$
Закон негирања импликације:	$(\neg(p \Rightarrow q)) \Leftrightarrow (p \wedge \neg q)$
Закон јаког свођења на противречност:	$((\neg p) \Rightarrow (q \wedge \neg q)) \Rightarrow p$

Закони комутативности за $\wedge$ и $\vee$:	$(p \wedge q) \Leftrightarrow (q \wedge p)$ и $(p \vee q) \Leftrightarrow (q \vee p)$
Закон асоцијативности за $\wedge$:	$((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$
Закон асоцијативности за $\vee$:	$((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$
Закони апсорпције:	$(p \vee (q \wedge p)) \Leftrightarrow p$ и $(p \wedge (q \vee p)) \Leftrightarrow p$
Закон дистрибутивности $\wedge$ у односу на $\vee$:	$((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (q \wedge r))$
Закон дистрибутивности $\vee$ у односу на $\wedge$:	$((p \wedge q) \vee r) \Leftrightarrow ((p \vee r) \wedge (q \vee r))$
Модус поненс (modus ponens):	$(p \wedge (p \Rightarrow q)) \Rightarrow q$
Де Морганов закон:	$(\neg(p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$
Де Морганов закон:	$(\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q)$
Закон контрапозиције:	$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$

У наредној теореми представићемо још једну везу која постоји између формуле F и формула $F^p_\top$ и $F^p_\bot$, где је p неко исказно слово формуле F.

ТЕОРЕМА 4

За произвољну формулу F и неко исказно слово p важи да је F еквивалентна формули $(p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot)$, тј. формула $F \Leftrightarrow ((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ је таутологија.

ДОКАЗ

Треба показати да је за сваку валуацију $v : \mathcal{F} \to \{0,1\}$ вредност $v(F \Leftrightarrow ((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot)))$ једнака 1. На основу дефиниције v за формулу облика $A \Leftrightarrow B$, то значи да треба показати да је $v(F)$ једнако $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$. По дефиницији валуације v вредност $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ рачунамо као минимум $v(p \Rightarrow F^p_\top)$ и $v(\neg p \Rightarrow F^p_\bot)$, а те вредности рачунамо овако:

$$v(p \Rightarrow F^p_\top) = max(1 - v(p), v(F^p_\top))$$
$$v(\neg p \Rightarrow F^p_\bot) = max(1 - v(\neg p), v(F^p_\bot)).$$

За даље рачунање неопходна нам је вредност исказног слова p валуацијом v. За сваку валуацију v вредност $v(p)$ је или 1 или 0.

$\lhd_1$ Ако је $v(p) = 1$, онда имамо да је $v(F) = v(F^p_\top)$.
Одредимо још $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$. Имамо:

$v(p \Rightarrow F^p_\top) = max(1 - 1, v(F^p_\top)) = max(0, v(F^p_\top)) = v(F^p_\top)$
и
$v(\neg p \Rightarrow F^p_\bot)) = max(1 - 0, v(F^p_\bot)) = max(1, v(F^p_\bot)) = 1.$

Из тога следи: $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot)) = min(v(F^p_\top), 1) = v(F^p_\top)$.
Добили смо да су обе вредности $v(F)$ и $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ једнаке $v(F^p_\top)$, па су једнаке међусобно.

$\lhd_2$ Ако је $v(p) = 0$, онда имамо да је $v(F) = v(F^p_\bot)$.
На исти начин као у $\lhd_1$ добијамо да је $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ једнако $v(F^p_\bot)$.

Дакле, имамо да су обе вредности $v(F)$ и $v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ једнаке $v(F^p_\bot)$, па су једнаке међусобно.

Из $\lhd_1$ и $\lhd_2$ закључујемо да за сваку валуацију v важи:

$$v(F) = v((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot)),$$

тј.

$$v(F \Leftrightarrow ((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))) = 1.$$

Дакле, формула $F \Leftrightarrow ((p \Rightarrow F^p_\top) \wedge (\neg p \Rightarrow F^p_\bot))$ је таутологија.

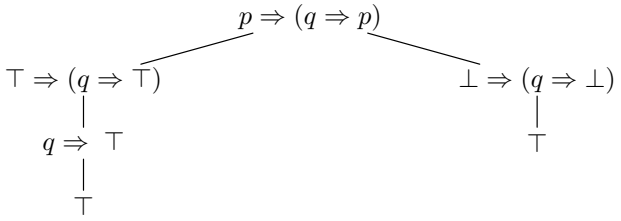
$\Diamond$

У наредном задатку ћемо за десет формула показати да су таутологије и то методом чишћења.

Задатак 3

(1.1) Показати да је формула $p \Rightarrow (q \Rightarrow p)$ таутологија.

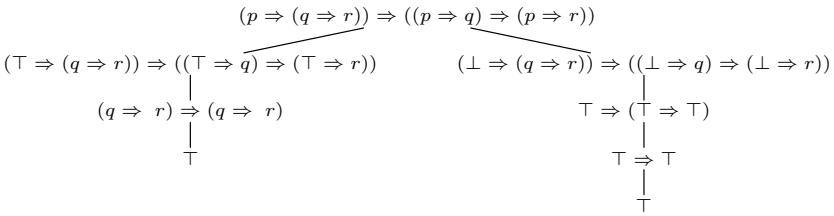
Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, таутологије: (10) и (9), а у његовој десној грани користили смо таутологију (12).

(1.2) Показати да је $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$ таутологија.

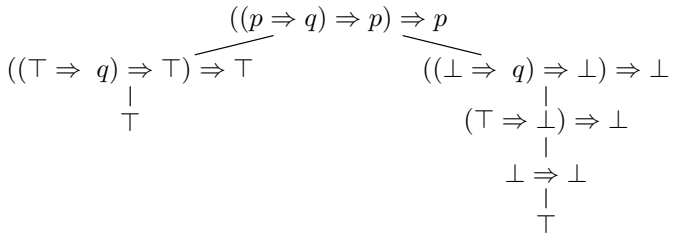
Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, таутологије: (10) и рефлексивност импликације, а у његовој десној грани користили смо редом, по корацима, таутологије: (12); (10) и (9).

(1.3) Показати да је формула $((p \Rightarrow q) \Rightarrow p) \Rightarrow p$ таутологија.

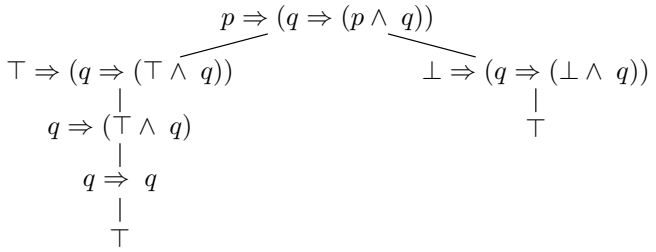
Правимо дрво:



У левој грани овог дрвета користили смо таутологију (9), а у десној грани редом, по корацима, таутологије: (12); (10) и (12).

(1.4) Показати да је формула $p \Rightarrow (q \Rightarrow (p \wedge q))$ таутологија.

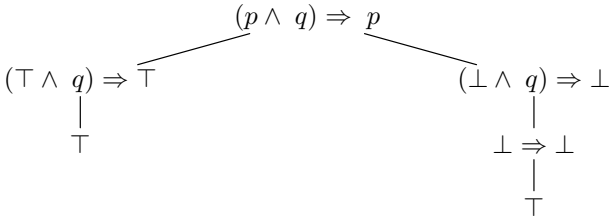
Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, таутологије: (10); (2) и рефлексивност импликације, а у десној таутологију (12).

(1.5) Показати да је формула $(p \wedge q) \Rightarrow p$ таутологија.

Правимо дрво:

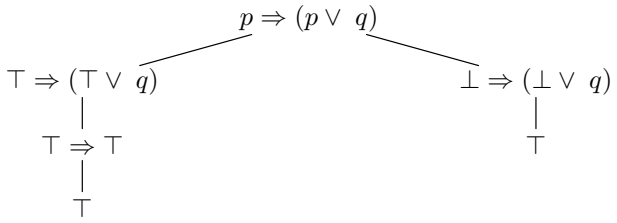


У десној грани овог дрвета користили смо редом, по корацима, таутологије: (4) и (12), а у левој таутологију (9).

(1.6) Показати да је формула $(p \wedge q) \Rightarrow q$ таутологија. Поступамо аналогно као у (1.5).

(1.7) Показати да је формула $p \Rightarrow (p \vee q)$ таутологија.

Правимо дрво:

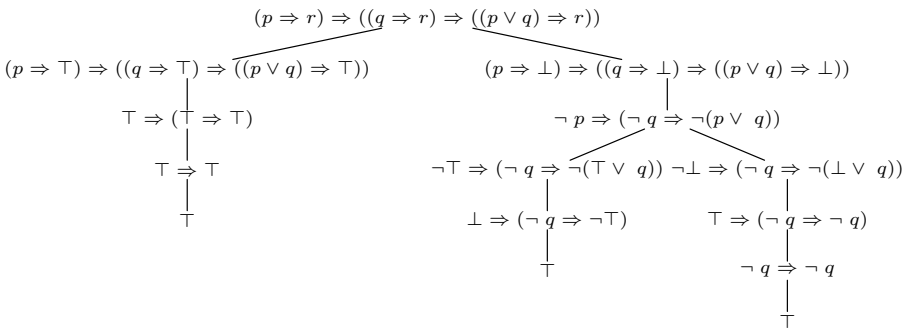


У левој грани овог дрвета користили смо редом, по корацима, таутологије: (6) и (10), а у десној таутологију (12).

(1.8) Показати да је формула $q \Rightarrow (p \vee q)$ таутологија. Поступамо аналогно као у (1.7).

(1.9) Показати да је $(p \Rightarrow r) \Rightarrow ((q \Rightarrow r) \Rightarrow ((p \vee q) \Rightarrow r))$ таутологија.

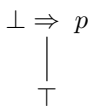
Правимо дрво:



У левој грани овог дрвета користили смо редом, по корацима, таутологије: (9); (10); (9). У грани од корена до чвора у коме је формула $\neg p \Rightarrow (\neg q \Rightarrow \neg(p \vee q))$ користили смо таутологију (11). У грани у чијем чвору је формула $\neg\top \Rightarrow (\neg q \Rightarrow \neg(\top \vee q))$ користили смо редом, по корацима, таутологије: (17) и (6); (12); а у грани у чијем чвору је формула $\neg\bot \Rightarrow (\neg q \Rightarrow \neg(\bot \vee q))$ користили смо редом, по корацима, таутологије: (18) и (8); (10); рефлексивност импликације.

(1.10) Показати да је формула $\bot \Rightarrow p$ таутологија.

Правимо дрво:



Користили смо таутологију (12).

Задатак 4 Посматрајмо таутологије из Задатка 3. Из тих таутологија, на основу ТЕОРЕМЕ 3, добијамо редом следеће таутологије:
(1.1) $A \Rightarrow (B \Rightarrow A)$
(1.2) $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$
(1.3) $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$
(1.4) $A \Rightarrow (B \Rightarrow (A \wedge B))$
(1.5) $(A \wedge B) \Rightarrow A$
(1.6) $(A \wedge B) \Rightarrow B$
(1.7) $A \Rightarrow (A \vee B)$
(1.8) $B \Rightarrow (A \vee B)$
(1.9) $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))$
(1.10) $\bot \Rightarrow A$

где су A, B и C произвољне формуле.

За неке формуле F_1,..., F_n $(n \geq 1)$ уопштену конјункцију, $\bigwedge_{i=1}^{n} F_i$, дефинишемо индуктивно на следећи начин:

(1) $\bigwedge_{i=1}^{1} F_i = F_1$

(2) $\bigwedge_{i=1}^{n+1} F_i = (\bigwedge_{i=1}^{n} F_i \wedge F_{n+1})$

На потпуно исти начин се дефинише уопштена дисјункција $\bigvee_{i=1}^{n} F_i$. На пример за неке формуле F_1, F_2, F_3 и F_4 имамо $\bigvee_{i=1}^{4} F_i = (((F_1 \vee F_2) \vee F_3) \vee F_4)$ и како код писања формула занемарујемо скроз спољне заграде та уопштена дисјункција је формула $((F_1 \vee F_2) \vee F_3) \vee F_4$.

Користећи дефиниције уопштене конјункције и дисјункције, формулишемо уопштене законе дистрибутивности и уопштене Де Морганове законе који су таутологије.

Задатак 5 Показати да су следеће формуле $(n \geq 2)$:

уопштени закон дистрибутивности $\wedge$ у односу на $\vee$:

$$((\bigvee_{i=1}^{n} A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^{n} (A_i \wedge C))$$

уопштени закон дистрибутивности $\vee$ у односу на $\wedge$:

$$((\bigwedge_{i=1}^{n} A_i) \vee C) \Leftrightarrow (\bigwedge_{i=1}^{n} (A_i \vee C))$$

и уопштени Де Морганови закони:

$$(\neg(\bigvee_{i=1}^{n} A_i)) \Leftrightarrow (\bigwedge_{i=1}^{n} \neg A_i)$$

$$(\neg(\bigwedge_{i=1}^{n} A_i)) \Leftrightarrow (\bigvee_{i=1}^{n} \neg A_i)$$

таутологије. (За $n = 1$ све ово формуле су облика $F \Leftrightarrow F$, па су таутологије.)

Индукцијом по броју формула $A_1, ..., A_n$ покажимо да уопштени закон дистрибутивности $\wedge$ у односу на $\vee$ јесте таутологија. (И са другим формулама се поступа аналогно.)
База индукције, $n = 2$, посматрана формула је облика

$$((A_1 \vee A_2) \wedge C) \Leftrightarrow ((A_1 \wedge C) \vee (A_2 \wedge C)),$$

а то је таутологија закон дистрибутивности $\wedge$ у односу на $\vee$.
Индукцијска претпоставка је да формула

$$((\bigvee_{i=1}^{n} A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^{n} (A_i \wedge C))$$

јесте таутологија.
Покажимо да је таутологија и формула

$$((\bigvee_{i=1}^{n+1} A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^{n+1} (A_i \wedge C))$$

На основу дефиниције уопштене дисјункције имамо
$\bigvee_{i=1}^{n+1} A_i = (\bigvee_{i=1}^{n} A_i \vee A_{n+1})$, зато је формула

$$((\bigvee_{i=1}^{n+1} A_i) \wedge C) \Leftrightarrow ((\bigvee_{i=1}^{n} A_i \vee A_{n+1}) \wedge C)$$

таутологија. На основу закона дистрибутивности $\wedge$ у односу на $\vee$:

$$((B \vee D) \wedge C) \Leftrightarrow ((B \wedge C) \vee (D \wedge C)),$$

где је B формула $\bigvee_{i=1}^{n} A_i$, а D формула A_{n+1} имамо таутологију:

$$((\bigvee_{i=1}^{n} A_i \vee A_{n+1}) \wedge C) \Leftrightarrow (((\bigvee_{i=1}^{n} A_i) \wedge C) \vee (A_{n+1} \wedge C)).$$

На крају, за формулу која је таутологија по индукцијској претпоставци и формулу $A_{n+1} \wedge C$, на основу дела ($\vee$2) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, имамо да је формула

$$(((\bigvee_{i=1}^{n} A_i) \wedge C) \vee (A_{n+1} \wedge C)) \Leftrightarrow ((\bigvee_{i=1}^{n} (A_i \wedge C)) \vee (A_{n+1} \wedge C))$$

таутологија. Посматрајмо све наведене таутологије. Свака од њих даје еквивалентност формула које су у њој повезане везником $\Leftrightarrow$. Стога на основу транзитивности еквивалентности имамо да је формула $(\bigvee_{i=1}^{n+1} A_i) \wedge C$ из прве таутологије еквивалентна формули из последње, формули $(\bigvee_{i=1}^{n} (A_i \wedge C)) \vee (A_{n+1} \wedge C)$. На основу дефиниције уопштене дисјункције за ту формулу важи:

$$(\bigvee_{i=1}^{n} (A_i \wedge C)) \vee (A_{n+1} \wedge C) = \bigvee_{i=1}^{n+1} (A_i \wedge C).$$

Дакле, формуле $(\bigvee_{i=1}^{n+1} A_i) \wedge C$ и $\bigvee_{i=1}^{n+1} (A_i \wedge C)$ су еквивалентне, тј. имамо таутологију:

$$((\bigvee_{i=1}^{n+1} A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^{n+1} (A_i \wedge C)).$$

2.2.4 Још о замени еквивалената

Погледајмо таутологију modus ponens,

$$\models (A \wedge (A \Rightarrow B)) \Rightarrow B$$

и прочитајмо је као да она представља један поступак закључивања:

ако је истинито A и ако је истинито да из A следи B,
онда закључујемо да је и B истинито.

Користећи тај начин закључивања можемо од познатих таутологија да правимо нове таутологије. То својство ћемо доказати у наредној теореми, коју ћемо (због modus ponensa) назвати ТЕОРЕМА *MP*.

ТЕОРЕМА 5 (ТЕОРЕМА *MP*)
Ако су формуле A и $A \Rightarrow B$ таутологије, онда је и формула B таутологија.
ДОКАЗ

Формуле A и $A \Rightarrow B$ су таутологије, па за сваку валуацију v важи: $v(A) = 1$ и $v(A \Rightarrow B) = 1$. С друге стране, на основу дефиниције v, вредност $v(A \Rightarrow B)$ рачунамо овако:
$max(1 - v(A), v(B))$=$max(1 - 1, v(B))$=$max(0, v(B))$=$v(B)$. Дакле, имамо да је $v(A \Rightarrow B) = 1$ и $v(A \Rightarrow B) = v(B)$, па закључујемо да је $v(B)$ једнако 1 за сваку валуацију v, тј. формула B је таутологија.

$\diamondsuit$

Одмах покажимо једну примену ТЕОРЕМЕ *MP*. Наиме, веома једноставно ћемо доказати ЛЕМУ О ЗАМЕНИ ЕКВИВАЛЕНАТА као последицу ТЕОРЕМЕ *MP*. Прво проширимо наш списак познатих таутологија новим таутологијама за које можемо рећи да повезују везник $\Leftrightarrow$ са осталим везницима.

Задатак 6 Покажимо да за произвољне формуле A, B и C важи:

(Т1$\neg$) $\models (A \Leftrightarrow B) \Rightarrow (\neg A \Leftrightarrow \neg B)$;

(Т2$\wedge$) $\models (A \Leftrightarrow B) \Rightarrow ((C \wedge A) \Leftrightarrow (C \wedge B))$ и
$\models (A \Leftrightarrow B) \Rightarrow ((A \wedge C) \Leftrightarrow (B \wedge C))$;

(Т3$\vee$) $\models (A \Leftrightarrow B) \Rightarrow ((C \vee A) \Leftrightarrow (C \vee B))$ и
$\models (A \Leftrightarrow B) \Rightarrow ((A \vee C) \Leftrightarrow (B \vee C))$;

(Т4$\Rightarrow$) $\models (A \Leftrightarrow B) \Rightarrow ((C \Rightarrow A) \Leftrightarrow (C \Rightarrow B))$ и
$\models (A \Leftrightarrow B) \Rightarrow ((A \Rightarrow C) \Leftrightarrow (B \Rightarrow C))$;

(Т5$\Leftrightarrow$) $\models (A \Leftrightarrow B) \Rightarrow ((C \Leftrightarrow A) \Leftrightarrow (C \Leftrightarrow B))$ и
$\models (A \Leftrightarrow B) \Rightarrow ((A \Leftrightarrow C) \Leftrightarrow (B \Leftrightarrow C))$.

Показаћемо само да је друга формула из дела (Т2$\wedge$) таутологија.
За било коју валуацију v вредност $v(A \Leftrightarrow B)$ може бити или 1 или 0. Када је $v(A \Leftrightarrow B)$ једнако 1, онда важи $v(A) = v(B)$, па добијамо: $v(A \wedge C) = min(v(A), v(C)) = min(v(B), v(C)) = v(B \wedge C)$. Дакле,

$v((A \Leftrightarrow B) \Rightarrow ((A \wedge C) \Leftrightarrow (B \wedge C))) = 1$. Ако је $v(A \Leftrightarrow B) = 0$, онда одмах, на основу дефиниције валуације v, добијамо да је вредност $v((A \Leftrightarrow B) \Rightarrow ((A \wedge C) \Leftrightarrow (B \wedge C)))$ једнака 1. Дакле, показали смо да је формула $(A \Leftrightarrow B) \Rightarrow ((A \wedge C) \Leftrightarrow (B \wedge C))$ таутологија. Са осталим формулама поступамо слично као са овом формулом.

А сада ево доказа ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА.

ДОКАЗ ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА КАО ПОСЛЕДИЦЕ ТЕОРЕМЕ *MP*

Имамо да је претпоставка ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА таутологија $\models A \Leftrightarrow B$ и још посматрамо произвољну формулу C.
Докажимо део (1). Из таутологије $\models A \Leftrightarrow B$ и таутологије (T1$\neg$) $\models (A \Leftrightarrow B) \Rightarrow (\neg A \Leftrightarrow \neg B)$ из Задатка 6, на основу ТЕОРЕМЕ *MP*, добијамо таутологију $\models \neg A \Leftrightarrow \neg B$.
Што се тиче дела (2), доказаћемо само случај ($\wedge$2), а остали случајеви се доказују аналогно. Из таутологије $\models A \Leftrightarrow B$ и таутологије $\models (A \Leftrightarrow B) \Rightarrow ((A \wedge C) \Leftrightarrow (B \wedge C))$ из Задатка 6, на основу ТЕОРЕМЕ *MP*, добијамо таутологију $\models (A \wedge C) \Leftrightarrow (B \wedge C)$.

$\diamondsuit$

На крају овог одељка, покажимо још једну последицу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА. То је особина која говори о вези еквивалентних формула и бинарних везника.

Задатак 7 Ако је $\models A \Leftrightarrow B$ и $\models C \Leftrightarrow D$,

онда је
$(1\wedge)$ $\models (A \wedge C) \Leftrightarrow (B \wedge D)$;
$(2\vee)$ $\models (A \vee C) \Leftrightarrow (B \vee D)$;
$(3\Rightarrow)$ $\models (A \Rightarrow C) \Leftrightarrow (B \Rightarrow D)$;
$(4\Leftrightarrow)$ $\models (A \Leftrightarrow C) \Leftrightarrow (B \Leftrightarrow D)$.

Наравно да ову особину можемо доказати на следећи начин: користећи претпоставке $\models A \Leftrightarrow B$ и $\models C \Leftrightarrow D$, утврдићемо да свака од наведених формула за сваку валуацију v има вредност 1. Али ми ћемо ту особину доказати као последицу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА. Тачније, показаћемо само део ($2\vee$), тј. да важи $\models (A \vee C) \Leftrightarrow (B \vee D)$, а остали случајеви се доказују аналогно.
За формулу $p \vee C$ и таутологију $\models A \Leftrightarrow B$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје следећу таутологију: $\models (p \vee C)^p_A \Leftrightarrow (p \vee C)^p_B$, тј. $\models (A \vee C) \Leftrightarrow (B \vee C)$. За формулу $B \vee p$ и таутологију $\models C \Leftrightarrow D$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје: $\models (B \vee p)^p_C \Leftrightarrow (B \vee p)^p_D$, тј. таутологију $\models (B \vee C) \Leftrightarrow (B \vee D)$.
Из таутологија $\models (A \vee C) \Leftrightarrow (B \vee C)$ и $\models (B \vee C) \Leftrightarrow (B \vee D)$ добијамо редом: $A \vee C \equiv B \vee C$ и $B \vee C \equiv B \vee D$. На крају, користећи транзитивност релације $\equiv$, добијамо $A \vee C \equiv B \vee D$, тј. $\models (A \vee C) \Leftrightarrow (B \vee D)$.

2.3 Булове алгебре

У овом одељку представићемо неколико веома важних алгебарских структура. Полазиште нам је један непразан скуп B са својим елементима. Посматраћемо неке операције над тим скупом, захтеваћемо различите особине за те операције и на тај начин градити различите структуре. Одмах рецимо да ће инспирација за прављење тих структура бити партитивни скуп неког непразног скупа X, скуп $\mathcal{P}(X)$, са својим елементима: подскуповима од X, добро познате операције на скуповима: пресек, унија, комплемент и особине неких од тих операција: комутативност, асоцијативност и др. Ту везу која увек постоји између дефиниције неке структуре и конкретног примера те структуре представићемо у наредном једноставном примеру.

Пример 1 Дефинишемо једну структуру на следећи начин: свака алгебарска структура са комутативном операцијом $\star$ на њеном носачу је једна к-структура. Одмах се питамо: да ли постоји пример такве структуре? И одговор је: постоји. За неки скуп X, његов партитивни скуп $\mathcal{P}(X)$ и операција пресек скупова чине једну к-структуру $(\mathcal{P}(X), \cap)$. Има још примера: скуп природних бројева и операција сабирање, $(\mathbf{N}, +)$, па скуп целих бројева и операција множење, $(\mathbf{Z}, \cdot)$ и др. Сада посматрамо пример к-структуре $(\mathcal{P}(X), \cap)$ и питамо се: коју још особину има операција пресек скупова? На пример за произвољан елемент Y из $\mathcal{P}(X)$ важи: $Y \cap Y = Y$. Та особина операције $\cap$ нам је инспирација да дефинишемо нову врсту структуре, структуру са скупом B, бинарном операцијом $\cap$ за коју важи комутативност и за сваки елемент b из B важи $b \cap b = b$. Одмах знамо да је један пример те нове структуре $(\mathcal{P}(X), \cap)$. Да ли су $(\mathbf{N}, +)$ и $(\mathbf{Z}, \cdot)$ примери и те нове структуре? Одговор је: НЕ. Образложење за структуру $(\mathbf{N}, +)$ је следеће: сабирање јесте комутативна операција, али за произвољан природан број n не важи $n + n = n$.

Сада када смо упознали ту везу између дефиниција различитих структура и конкретних примера тих структура представићемо неке веома значајне алгебарске структуре.

2.3.1 Мреже

Пре него што дамо дефиницију структуре коју ћемо звати мрежа, погледајмо прво један пример.

Пример 2 Посматрајмо произвољан коначан непразан скуп X и његов партитивни скуп $\mathcal{P}(X)$. Затим на скупу $\mathcal{P}(X)$ посматрајмо познате операције унију и пресек. Јасно је да за било која два подскупа A и B скупа X, тј. елемента скупа $\mathcal{P}(X)$ важи: $A \cup B$ и $A \cap B$

су подскупови скупа X и припадају скупу $\mathcal{P}(X)$. Осим тога, за било која три елемента A, B и C скупа $\mathcal{P}(X)$ важе и следеће особине:

$$(A \cap B) \cap C = A \cap (B \cap C) \quad \text{и} \quad (A \cup B) \cup C = A \cup (B \cup C)$$
$$A \cap B = B \cap A \quad \text{и} \quad A \cup B = B \cup A$$
$$A \cap A = A \quad \text{и} \quad A \cup A = A$$
$$A \cap (B \cup A) = A \quad \text{и} \quad A \cup (B \cap A) = A$$

Структура која се састоји од непразног скупа и две бинарне операције на том скупу са наведеним особинама је једна мрежа. Дакле, $(\mathcal{P}(X), \cap, \cup)$ је пример једне мреже.

Наведимо сада дефиницију мреже.

Дефиниција мреже

Нека је B произвољан непразан скуп и $\cap$ и $\cup$ две бинарне операције дефинисане на том скупу. Структура $\mathcal{B} = (B, \cap, \cup)$ је мрежа АККО за операције $\cap$ и $\cup$ и произвољне елементе a, b и c скупа B важе следеће особине:

асоцијативност:	$(a \cap b) \cap c = a \cap (b \cap c)$	$(a \cup b) \cup c = a \cup (b \cup c)$
комутативност:	$a \cap b = b \cap a$	$a \cup b = b \cup a$
идемпотентност:	$a \cap a = a$	$a \cup a = a$
закони апсорпције:	$a \cap (b \cup a) = a$	$a \cup (b \cap a) = a$

Можемо над неким скупом B посматрати само једну бинарну операцију са особинама наведеним у дефиницији мреже. Таква структура назива се полумрежа.

Дефиниција полумреже

Нека је B произвољан скуп и $\cap$ бинарна операција дефинисана на том скупу. Структура $\mathcal{B} = (B, \cap)$ је полумрежа АККО за операцију $\cap$ важи асоцијативност, комутативност и идемпотентност.

Приметимо да сваку мрежу $\mathcal{B} = (B, \cap, \cup)$ чине две полумреже $\mathcal{B}_1 = (B, \cap)$ и $\mathcal{B}_2 = (B, \cup)$ и још имамо додатна својства која повезују операције $\cap$ и $\cup$, тј. за те операције важе закони апсорпције.

Задатак 1 Посматрајмо једну мрежу $\mathcal{B} = (B, \cap, \cup)$. Покажимо да је бинарна релација $\leq$ на скупу B дефинисана на следећи начин:

$$a \leq b \qquad \text{АККО} \qquad a \cap b = a \qquad (*)$$

једна релација парцијалног уређења.
Да ли је релација $\leq$ рефлексивна, тј. да ли је $a \leq a$? У ствари питање је: да ли важи $a \cap a = a$? Одговор је ДА. Дакле, важи рефлексивност.
Да ли је релација $\leq$ транзитивна, тј. да ли важи: ако је $a \leq b$

и $b \leq c$, онда је $a \leq c$? По дефиницији релације $\leq$ то значи да испитујемо да ли важи следећа особина: ако је $a \cap b = a$ и $b \cap c = b$, онда је $a \cap c = a$. По првој претпоставци имамо: $a = a \cap b$. У тој једнакости, користећи другу претпоставку, b замењујемо са $b \cap c$ и добијамо $a = a \cap (b \cap c)$. Затим користимо асоцијативност операције $\cap$ и добијамо $a = (a \cap b) \cap c$. На основу прве претпоставке $a \cap b$ је једнако a, па у $(a \cap b) \cap c$ део $a \cap b$ замењујемо са a и добијамо: $a = a \cap c$. Дакле, важи $a \leq c$, тј. релација $\leq$ је транзитивна.
Да ли је релација $\leq$ антисиметрична, тј. да ли важи: ако је $a \leq b$ и $b \leq a$, онда је $a = b$? По дефиницији релације $\leq$ то значи да испитујемо да ли важи следећа особина: ако је $a \cap b = a$ и $b \cap a = b$, онда је $a = b$. На основу комутативности $\cap$ имамо $a \cap b = b \cap a$. Дакле, $a = b$. То значи да је релација $\leq$ антисиметрична.
Дакле, релација $\leq$ је једно парцијално уређење на скупу B.

Погледајмо још један начин дефинисања релације $\leq$ на скупу B за неку мрежу $\mathcal{B} = (B, \cap, \cup)$:

$$a \leq b \qquad \text{AKKO} \qquad a \cup b = b \qquad (**)$$

У следећем задатку видећемо да релација дата дефиницијом (**) и релација дата дефиницијом (*) у Задатаку 1 представљају исту релацију парцијалног уређења.

Задатак 2 Покажимо да у свакој мрежи $\mathcal{B} = (B, \cap, \cup)$ за произвољне елементе a и b важи: $a \cap b = a$ ако и само ако $a \cup b = b$.
Ако је $a \cap b = a$, онда полазећи од $a \cup b$ елемент a замењујемо са $a \cap b$ и добијамо $a \cup b = (a \cap b) \cup b$. Сада, користећи комутативност операције $\cup$, имамо $a \cup b = b \cup (a \cap b)$. Коначно, закон апсорпције $b \cup (a \cap b) = b$, даје $a \cup b = b$. С друге стране, ако је $a \cup b = b$, користећи редом ту особину, комутативност операције $\cup$ и закон апсорпције, добијамо: $a \cap b = a \cap (a \cup b) = a \cap (b \cup a) = a$.

Особине операција уније и пресека скупова, које важе за елементе скупа $\mathcal{P}(X)$ мреже $(\mathcal{P}(X), \cap, \cup)$, биће нам инспирација за дефинисање и других структура богатијих од мреже. Зато се вратимо нашем примеру мреже $(\mathcal{P}(X), \cap, \cup)$ и подсетимо се да за операције пресека и уније скупова, операције $\cap$ и $\cup$, важе и закони дистрибутивности. Стога и у произвољној мрежи $(B, \cap, \cup)$ можемо испитати да ли за њене операције $\cap$ и $\cup$ важе дистрибутивни закони. Ако важе, онда ћемо такву мрежу звати дистрибутивна мрежа.

Дефиниција дистрибутивне мреже

Мрежа $\mathcal{B} = (B, \cap, \cup)$ је дистрибутивна мрежа AKKO за операције $\cap$ и $\cup$ поред особина које за њих важе у мрежи, важе и закони дистрибутивности:
$(a \cap b) \cup c = (a \cup c) \cap (b \cup c)$ и $(a \cup b) \cap c = (a \cap c) \cup (b \cap c)$
за произвољне елементе a, b и c скупа B.

Тако је за произвољан непразан скуп X структура $(\mathcal{P}(X), \cap, \cup)$ једна дистрибутивна мрежа.

2.3.2 Булове алгебре

Посматрамо произвољан непразан скуп X и његов партитивни скуп $\mathcal{P}(X)$. Ако хоћемо да дефинишемо алгебарску структуру која као свој пример има партитивни скуп $\mathcal{P}(X)$, све скуповне операције (пресек, унија и комплемент) и да буду истакнута два важна елемента тог скупа, празан скуп и цео скуп X, онда ту структуру дефинишемо на следећи начин.

Дефиниција Булове алгебре

Нека је $\mathcal{B} = (B, \cap, \cup)$ једна дистрибутивна мрежа. На скупу B имамо још и једну унарну операцију $^-$ и две нуларне операције: истакнуте елементе 0 и 1. Ако за произвољан елемент a скупа B и операције $\cap, \cup, ^-, 0$ и 1 важе следеће особине:

$$a \cap 0 = 0 \qquad a \cup 1 = 1$$
$$a \cap \overline{a} = 0 \qquad a \cup \overline{a} = 1$$

онда је структура $\mathcal{B} = (B, \cap, \cup, ^-, 0, 1)$ Булова алгебра.

Пре него што дамо примере Булових алгебри, покажимо одмах још неке особине које важе за операције Булове алгебре.

Задатак 3 У дефиницији Булове алгебре имамо да је $a \cap 0 = 0$, а онда се поставља питање чему је једнако $a \cup 0$? Користећи $a \cap \overline{a} = 0$ у $a \cup 0$ нулу замењујемо са $a \cap \overline{a}$ и добијамо $a \cup 0 = a \cup (a \cap \overline{a})$. На основу комутативности $\cap$ и апсорпције имамо: $a \cup (a \cap \overline{a}) = a \cup (\overline{a} \cap a) = a$. Дакле, $a \cup 0 = a$.
У дефиницији Булове алгебре имамо да важи $a \cup 1 = 1$, а питање је чему је једнако $a \cap 1$? Користећи једнакост $a \cup \overline{a} = 1$ у $a \cap 1$ јединицу замењујемо са $a \cup \overline{a}$ и добијамо $a \cap 1 = a \cap (a \cup \overline{a})$, а на основу комутативности операције $\cup$ и закона апсорпције израз са десне стране једнакости је једнак a. Дакле, $a \cap 1 = a$.
Покажимо да је $\overline{0} = 1$ и $\overline{1} = 0$. За $a = \overline{0}$ једнакост $a \cup 0 = a$ је $\overline{0} \cup 0 = \overline{0}$. Осим тога, за $a = 0$ једнакост $a \cup \overline{a} = 1$ је $0 \cup \overline{0} = 1$. Дакле, $\overline{0} = 1$. Исто тако, $a \cap 1 = a$ за $a = \overline{1}$ и $a \cap \overline{a} = 0$ за $a = 1$ дају $\overline{1} = 0$.

А ево и неколико примера Булових алгебри са партитивним скупом неког скупа X и операцијама на том скупу $\mathcal{P}(X)$.

Пример 3 Имамо скуп $\{\emptyset\}$ и његов партитивни скуп $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. Ако су операције $\cap$ и $\cup$ уобичајене скуповне операције редом пресек и унија, а унарна операција $^-$ је операција комплемент скупа: $\overline{\emptyset} = \{\emptyset\}$ и $\overline{\{\emptyset\}} = \emptyset$, тада је структура $(\mathcal{P}(\{\emptyset\}), \cap, \cup, ^-, \emptyset, \{\emptyset\})$ једна

Булова алгебра. Истакнимо да је структура $(\mathcal{P}(\{\emptyset\}), \cap, \cup, ^-, \emptyset, \{\emptyset\})$ најмања могућа Булова алгебра која има само два елемента, па се зове Булова алгебра 2.

Пример 4 Посматрајмо скуп од два елемената, скуп $\{0,1\}$. Његов партитивни скуп $\mathcal{P}(\{0,1\}) = \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ има четири елемента. Опет имамо уобичајене операције пресека и уније на скупу $\mathcal{P}(\{0,1\})$, а на следећи начин дефинишемо резултате операције комплемент: $\overline{\{0\}} = \{1\}$, $\overline{\{1\}} = \{0\}$, $\overline{\emptyset} = \{0,1\}$ и $\overline{\{0,1\}} = \emptyset$. Добијамо да је структура $(\mathcal{P}(\{0,1\}), \cap, \cup, ^-, \emptyset, \{0,1\})$ једна Булова алгебра и то Булова алгебра 4 (јер има четири елемента).

Пример 5 Посматрајмо произвољан скуп X и његов партитивни скуп $\mathcal{P}(X)$. Већ смо видели да је структура $(\mathcal{P}(X), \cap, \cup)$ једна дистрибутивна мрежа. Штавише, структура $(\mathcal{P}(X), \cap, \cup, ^-, \emptyset, X)$ је једна Булова алгебра. Ако скуп X има n елемената, онда знамо да скуп $\mathcal{P}(X)$ има 2^n елемената.

Сада ћемо на један, можемо рећи, необичан начин посматрати исказне формуле и представити веома значајан пример Булове алгебре.

Пример 6 **Линденбаумова алгебра**

Посматрамо скуп свих формула исказне логике, скуп $\mathcal{F}$. Показали смо да је еквивалентност формула, релација $\equiv$, једна релација еквиваленције на скупу $\mathcal{F}$. Та релација разбија скуп $\mathcal{F}$ на класе еквиваленције. Произвољна класа еквиваленције те релације, класа неке формуле A, садржи све формуле C еквивалентне формули A, $A \equiv C$, тј. све формуле C за које важи $\models A \Leftrightarrow C$. Класу еквиваленције формуле A означаваћемо $[A]$. Знамо да за класе еквиваленције неке релације еквиваленције ρ над неким скупом X и два различита елемента x и y тог скупа важи: ако су x и y у релацији ρ, онда су њихове класе једнаке, а ако x и y нису у релацији ρ, онда су њихове класе дисјунктне. У нашем случају то значи да за две произвољне формуле A и B скупа $\mathcal{F}$ важи:

ако је $\models A \Leftrightarrow B$, онда је $[A] = [B]$ и

ако не важи $\models A \Leftrightarrow B$, онда је $[A] \cap [B] = \emptyset$.

Сетимо се и да смо посебно издвојили класе еквиваленције формула $\top$ и $\bot$. Класа $[\top]$ је скуп свих таутологија, а класу формуле $\bot$, класу $[\bot]$, чине све контрадикције.

Сада посматрајмо скуп $[\mathcal{F}]$ чији су елементи класе еквиваленције свих исказних формула скупа $\mathcal{F}$. На том скупу дефинишимо бинарне операције $\wedge$ и $\vee$ и унарну операцију $\neg$. Ако су $[A]$ и $[B]$ произвољни елементи скупа $[\mathcal{F}]$, онда:

$$[A] \wedge [B] \quad =_{def} \quad [A \wedge B]$$

$$[A] \vee [B] \quad =_{def} \quad [A \vee B]$$
$$\neg[A] \quad =_{def} \quad [\neg A]$$

где је јасно да класе $[A \wedge B]$, $[A \vee B]$ и $[\neg A]$ чине све формуле C за које важи редом $\models (A \wedge B) \Leftrightarrow C$, $\models (A \vee B) \Leftrightarrow C$ и $\models (\neg A) \Leftrightarrow C$.
Треба проверити да ли су ове дефиниције коректне. Проверићемо коректност само дефиниције

$$[A] \wedge [B] \quad =_{def} \quad [A \wedge B],$$

а провера коректности друге две дефиниције се ради слично. Морамо показати да за било коју формулу C из $[A]$ и било коју формулу D из $[B]$ важи $[A \wedge B] = [C \wedge D]$, тј. да вредност операције $\wedge$ на класама $[A]$ и $[B]$ не зависи од избора елемената из тих класа. Из $C \in [A]$ и $D \in [B]$ редом имамо $\models A \Leftrightarrow C$ и $\models B \Leftrightarrow D$. Одатле, на основу дела $(1\wedge)$ Задатка 7 из одељка 2.2.4, добијамо $\models (A \wedge B) \Leftrightarrow (C \wedge D)$, тј. $[A \wedge B] = [C \wedge D]$.

Структура $([\mathcal{F}], \wedge, \vee, \neg, [\bot], [\top])$ је једна Булова алгебра, и та се структура зове Линденбаумова алгебра.
Покажимо да $([\mathcal{F}], \wedge, \vee, \neg, [\bot], [\top])$ стварно јесте Булова алгебра, тј. проверимо да ли за елементе скупа $[\mathcal{F}]$ и операције $\wedge$, $\vee$, $\neg$, $[\bot]$ и $[\top]$ дефинисане на том скупу, важе особине из дефиниције Булове алгебре.
Асоцијативност: За произвољне исказне формуле A, B и C, по дефиницији операције $\wedge$ на $[\mathcal{F}]$, класа $([A]\wedge[B])\wedge[C]$ је класа $[(A\wedge B)\wedge C]$. Формула $(A \wedge B) \wedge C$ је еквивалентна формули $A \wedge (B \wedge C)$, тј. $\models ((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[(A \wedge B) \wedge C] = [A \wedge (B \wedge C)]$. С друге стране, по дефиницији операције $\wedge$ на скупу $[\mathcal{F}]$, имамо да је $[A] \wedge ([B] \wedge [C])$ класа $[A \wedge (B \wedge C)]$. Дакле, $([A] \wedge [B]) \wedge [C] = [A] \wedge ([B] \wedge [C])$. Особина $([A] \vee [B]) \vee [C] = [A] \vee ([B] \vee [C])$ се доказује аналогно.
Комутативност: За произвољне исказне формуле A и B, по дефиницији операције $\wedge$ на скупу $[\mathcal{F}]$, класа $[A] \wedge [B]$ је класа $[A \wedge B]$. Формуле $A \wedge B$ и $B \wedge A$ су еквивалентне, тј. $\models (A \wedge B) \Leftrightarrow (B \wedge A)$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[A \wedge B] = [B \wedge A]$. С друге стране, по дефиницији операције $\wedge$ на скупу $[\mathcal{F}]$ имамо да је $[B]\wedge[A]$ класа $[B\wedge A]$. Дакле, $[A]\wedge[B] = [B]\wedge[A]$. Особина $[A]\vee[B] = [B]\vee[A]$ се доказује аналогно.
Идемпотентност: За произвољну исказну формулу A, по дефиницији операције $\wedge$ на скупу $[\mathcal{F}]$, класа $[A] \wedge [A]$ је класа $[A \wedge A]$. Формула $A \wedge A$ је еквивалентна формули A, тј. $\models (A \wedge A) \Leftrightarrow A$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[A \wedge A] = [A]$. Дакле, $[A] \wedge [A] = [A]$. Особина $[A] \vee [A] = [A]$ се доказује аналогно.
Закони апсорпције: За произвољне исказне формуле A и B, по дефиницијама операција $\wedge$ и $\vee$ на скупу $[\mathcal{F}]$, класа $[A] \vee ([B] \wedge [A])$ је класа $[A \vee (B \wedge A)]$. Формула $A \vee (B \wedge A)$ је еквивалентна формули

A, тј. $\models (A \vee (B \wedge A)) \Leftrightarrow A$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[A \vee (B \wedge A)] = [A]$. Дакле, $[A] \vee ([B] \wedge [A]) = [A]$. Особина $[A] \wedge ([B] \vee [A]) = [A]$ се доказује аналогно.
Дистрибутивност: За произвољне исказне формуле A, B и C, по дефиницијама операција $\wedge$ и $\vee$ на $[\mathcal{F}]$, класа $([A] \wedge [B]) \vee [C]$ је класа $[(A \wedge B) \vee C]$. Формула $(A \wedge B) \vee C$ је еквивалентна формули $(A \vee C) \wedge (B \vee C)$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[(A \wedge B) \vee C] = [(A \vee C) \wedge (B \vee C)]$. С друге стране, по дефиницијама операција $\wedge$ и $\vee$ на скупу $[\mathcal{F}]$, имамо да је $([A] \vee [C]) \wedge ([B] \vee [C])$ класа $[(A \vee C) \wedge (B \vee C)]$. Дакле, $([A] \wedge [B]) \vee [C] = ([A] \vee [C]) \wedge ([B] \vee [C])$. Особина $([A] \vee [B]) \wedge [C] = ([A] \wedge [C]) \vee ([B] \wedge [C])$ се доказује аналогно.
Остале особине Булове алгебре:
По дефиницији операције $\wedge$ на скупу $[\mathcal{F}]$ класа $[A] \wedge [\bot]$ је $[A \wedge \bot]$. Формула $A \wedge \bot$ је еквивалентна $\bot$, тј. $\models (A \wedge \bot) \Leftrightarrow \bot$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[A \wedge \bot] = [\bot]$. Дакле, $[A] \wedge [\bot] = [\bot]$. Особина $[A] \vee [\top] = [\top]$ се доказује аналогно.
По дефиницији операција $\wedge$ и $\neg$ на скупу $[\mathcal{F}]$ класа $[A] \wedge \neg[A]$ је $[A \wedge \neg A]$. Формула $A \wedge \neg A$ је еквивалентна $\bot$, тј. $\models (A \wedge \neg A) \Leftrightarrow \bot$, па на основу дефиниције класа из $[\mathcal{F}]$ имамо $[A \wedge \neg A] = [\bot]$. Дакле, $[A] \wedge \neg[A] = [\bot]$. Особина $[A] \vee \neg[A] = [\top]$ се доказује аналогно.
Закључујемо да структура $([\mathcal{F}], \wedge, \vee, \neg, [\bot], [\top])$ јесте једна Булова алгебра.

2.4 О везницима

2.4.1 Базе везника

Наша дефиниција алфабета исказне логике из одељка 2.1.1 је везнике $\wedge$, $\vee$, $\Rightarrow$ и $\bot$ одредила као основне, а преостали везници, везници $\Leftrightarrow$, $\neg$ и $\top$, дефинисани су помоћу основних следећим дефиницијама:

$$p \Leftrightarrow q =_{def} (p \Rightarrow q) \wedge (q \Rightarrow p), \qquad \neg p =_{def} p \Rightarrow \bot \quad \text{и} \quad \top =_{def} \bot \Rightarrow \bot.$$

У овим дефиницијама низови симбола са леве стране $=_{def}$ (међу којима је нови симбол за везник) су замена за низ симбола са десне стране $=_{def}$ који чине симболи алфабета исказне логике и који је исказна формула. Можемо поставити питање: зашто смо везнике $\Leftrightarrow$, $\neg$ и $\top$ представили помоћу основних везника баш тим формулама? Одговор је да су ове дефиниције инспирисане семантиком исказне логике. Наиме, када смо дефинисали алфабет исказне логике ми смо могли да за основне везнике изаберемо све познате везнике, тј. да за скуп логичких везника алфабета исказне логике узмемо цео скуп $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$. Тада не бисмо имали потребу да дефинишемо везнике $\Leftrightarrow$, $\neg$ и $\top$, али бисмо морали у интерпретацији језика да одредимо које операције на скупу $\mathbf{I} = \{0, 1\}$ одговарају тим везницима. Наравно да би то биле баш

одговарајуће операције $\Leftrightarrow$, $\neg$ и $\top$ на скупу $\mathbf{I} = \{0, 1\}$ представљене у одељку 2.2.1. Том интерпретацијом формуле $p \Leftrightarrow q$, $\neg p$ и $\top$ би биле еквивалентне редом формулама $(p \Rightarrow q) \wedge (q \Rightarrow p)$, $p \Rightarrow \bot$ и $\bot \Rightarrow \bot$. Еквивалентност тих формула је разлог за наведене дефиниције везника $\Leftrightarrow$, $\neg$ и $\top$.

Вратимо се алфабету са основним везницима $\wedge$, $\vee$, $\Rightarrow$ и $\bot$ и рецимо нешто о облику датих дефиниција везника $\Leftrightarrow$, $\neg$ и $\top$. Дефинисање нових везника подразумева следеће: прављење новог низа симбола, у коме се појављује нови везник и исказна слова које он повезује, као замену за неку исказну формулу у којој се појављују везници $\wedge$, $\vee$, $\Rightarrow$ и $\bot$ и исказна слова. На пример, у дефиницији:

$$p \Leftrightarrow q =_{def} (p \Rightarrow q) \wedge (q \Rightarrow p)$$

формула $p \Leftrightarrow q$ са новим везником $\Leftrightarrow$ и исказним словима p и q замењује формулу $(p \Rightarrow q) \wedge (q \Rightarrow p)$ у којој се појављују иста исказна слова p и q и везници $\Rightarrow$ и $\wedge$.

Намеће се питање: да ли скуп $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ има још неки прави подскуп (осим $\{\wedge, \vee, \Rightarrow, \bot\}$) са особином да се остали његови везници могу дефинисати помоћу везника тог подскупа и то тако да те дефиниције повезују међусобно еквивалентне формуле? Одговор је: да. У наредним задацима представићемо подскупове скупа $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ са том особином.

Задатак 1 Покажимо да је везнике скупа $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ могуће дефинисати помоћу везника скупа $\{\vee, \neg\}$. (Приметимо да како смо $\Leftrightarrow$ и $\top$ већ дефинисали помоћу везника скупа $\{\wedge, \vee, \Rightarrow, \bot\}$, онда би било довољно да само $\wedge$, $\Rightarrow$ и $\bot$ дефинишемо помоћу $\vee$ и $\neg$.)
(везник $\wedge$) Користећи особину да ако је формула $C \Leftrightarrow D$ таутологија, онда је и $\neg C \Leftrightarrow \neg D$ таутологија, из $\models (\neg(p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$ (Де Морганов закон), добијамо таутологију: $\models (\neg\neg(p \wedge q)) \Leftrightarrow (\neg(\neg p \vee \neg q))$, тј. важи: $\neg\neg(p \wedge q) \equiv \neg(\neg p \vee \neg q)$. Из $\models (\neg\neg(p \wedge q)) \Leftrightarrow (p \wedge q)$ (закон двојне негације), добијамо: $\neg\neg(p \wedge q) \equiv p \wedge q$. Дакле, на основу симетричности и транзитивности $\equiv$ добијамо: $\neg(\neg p \vee \neg q) \equiv p \wedge q$. Стога везник $\wedge$ дефинишемо на следећи начин:

$$p \wedge q =_{def} \neg(\neg p \vee \neg q) \qquad (\wedge_{def})$$

(везник $\Rightarrow$) Таутологијом $\models (p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ (закон замене импликације), везник $\Rightarrow$ је представљен помоћу $\vee$ и $\neg$. Дакле, везник $\Rightarrow$ дефинишемо на следећи начин:

$$p \Rightarrow q =_{def} \neg p \vee q \qquad (\Rightarrow_{def})$$

(везник $\Leftrightarrow$) Формула $p \Leftrightarrow q$ је замена за $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Везнике $\Rightarrow$ и $\wedge$ смо већ дефинисали помоћу везника $\vee$ и $\neg$. Користећи те дефиниције, добијамо:

$$p \Leftrightarrow q =_{def} \neg((\neg(\neg p \vee q)) \vee (\neg(\neg q \vee p))) \qquad (\Leftrightarrow_{def})$$

(везник $\top$) На основу закона искључења трећег, $\models p \vee \neg p$, формула $p \vee \neg p$ је таутологија, тј. еквивалентна је формули $\top$. Зато везник $\top$ дефинишемо на следећи начин:

$$\top =_{def} p \vee \neg p \qquad (\top_{def})$$

(везник $\bot$) Имамо да су формуле $p \vee \neg p$ и $\top$ еквивалентне. Као што смо показали, онда су и њихове негације, формуле $\neg(p \vee \neg p)$ и $\bot$, еквивалентне: $\neg(p \vee \neg p) \equiv \bot$. Дакле, дефиниција везника $\bot$ је:

$$\bot =_{def} \neg(p \vee \neg p) \qquad (\bot_{def})$$

Задатак 2 Покажимо сада да је помоћу везника скупа $\{\wedge, \neg\}$ могуће дефинисати остале везнике.
(везник $\vee$) Знамо да ако је формула $C \Leftrightarrow D$ таутологија, онда је и $\neg C \Leftrightarrow \neg D$ таутологија, па из $\models (\neg(p \vee q)) \Leftrightarrow (\neg p \wedge \neg q)$ (Де Морганов закон), добијамо таутологију: $\models (\neg\neg(p \vee q)) \Leftrightarrow (\neg(\neg p \wedge \neg q))$, тј. $\neg\neg(p \vee q) \equiv \neg(\neg p \wedge \neg q)$. Из $\models (\neg\neg(p \vee q)) \Leftrightarrow (p \vee q)$ (закон двојне негације), добијамо: $\neg\neg(p \vee q) \equiv p \vee q$. Затим, на основу симетричности и транзитивности $\equiv$, имамо: $\neg(\neg p \wedge \neg q) \equiv p \vee q$. Дакле, везник $\vee$ дефинишемо:

$$p \vee q =_{def} \neg(\neg p \wedge \neg q) \qquad (\vee_{def})$$

(везник $\Rightarrow$) Имамо таутологију $\models (p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ (закон замене импликације). Везник $\vee$ смо већ дефинисали помоћу везника $\wedge$ и $\neg$. Користећи ту дефиницију, добијамо: $\models (p \Rightarrow q) \Leftrightarrow (\neg(\neg\neg p \wedge \neg q))$. Из таутологије $\models \neg\neg p \Leftrightarrow p$ (закон двојне негације) на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА добијамо $\models (p \Rightarrow q) \Leftrightarrow (\neg(p \wedge \neg q))$, тј. $p \Rightarrow q \equiv \neg(p \wedge \neg q)$. Дакле, везник $\Rightarrow$ дефинишемо на следећи начин:

$$p \Rightarrow q =_{def} \neg(p \wedge \neg q) \qquad (\Rightarrow_{def})$$

(везник $\Leftrightarrow$) Формула $p \Leftrightarrow q$ је замена за $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Везник $\Rightarrow$ смо већ дефинисали помоћу везника $\wedge$ и $\neg$. Користећи ту дефиницију, добијамо:

$$p \Leftrightarrow q =_{def} (\neg(p \wedge \neg q)) \wedge (\neg(q \wedge \neg p)) \qquad (\Leftrightarrow_{def})$$

(везник $\bot$) Формула $p \wedge \neg p$ је контрадикција, па имамо:

$$\bot =_{def} p \wedge \neg p \qquad (\bot_{def})$$

(везник $\top$) Везник $\top$ дефинишемо на следећи начин:

$$\top =_{def} \neg(p \wedge \neg p) \qquad (\top_{def})$$

На реду је скуп $\{\Rightarrow, \neg\}$.

Задатак 3 Покажимо да је помоћу везника скупа $\{\Rightarrow, \neg\}$ могуће дефинисати остале везнике.
(везник $\wedge$) Користимо особину да ако је формула $C \Leftrightarrow D$ таутологија, онда је и формула $\neg C \Leftrightarrow \neg D$ таутологија, па из Де Моргановог закона $\models (\neg(p \wedge q)) \Leftrightarrow (\neg p \vee \neg q)$ добијамо: $\models (\neg\neg(p \wedge q)) \Leftrightarrow (\neg(\neg p \vee \neg q))$, тј. еквивалентност формула: $\neg\neg(p \wedge q) \equiv \neg(\neg p \vee \neg q)$. На основу исте особине, из таутологије $\models (p \Rightarrow \neg q) \Leftrightarrow (\neg p \vee \neg q)$ (закона замене

импликације), добијамо: $\models (\neg(p \Rightarrow \neg q)) \Leftrightarrow (\neg(\neg p \vee \neg q))$, па важи $\neg(p \Rightarrow \neg q) \equiv \neg(\neg p \vee \neg q)$. Закон двојне негације $\models (\neg\neg(p \wedge q)) \Leftrightarrow (p \wedge q)$ нам даје еквивалентност формула $\neg\neg(p \wedge q)$ и $p \wedge q$: $\neg\neg(p \wedge q) \equiv p \wedge q$. Из $\neg\neg(p \wedge q) \equiv \neg(\neg p \vee \neg q)$, $\neg(p \Rightarrow \neg q) \equiv \neg(\neg p \vee \neg q)$ и $\neg\neg(p \wedge q) \equiv p \wedge q$, користећи симетричност и транзитивност релације $\equiv$, добијамо: $\neg(p \Rightarrow \neg q) \equiv p \wedge q$. Дакле, дефиниција $\wedge$ је:

$$p \wedge q =_{def} \neg(p \Rightarrow \neg q) \qquad (\wedge_{def})$$

(везник $\vee$) У $\models (\neg p \Rightarrow q) \Leftrightarrow (\neg\neg p \vee q)$ (закон замене импликације) формулу $\neg\neg p$ замењујемо њој еквивалентном формулом p и на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА добијамо таутологију: $\models (\neg p \Rightarrow q) \Leftrightarrow (p \vee q)$. Дакле, везник $\vee$ дефинишемо:

$$p \vee q =_{def} (\neg p \Rightarrow q) \qquad (\vee_{def})$$

(везник $\Leftrightarrow$) Формула $p \Leftrightarrow q$ је замена за $(p \Rightarrow q) \wedge (q \Rightarrow p)$. Везник $\wedge$ смо већ дефинисали помоћу везника $\Rightarrow$ и $\neg$. Користећи ту дефиницију, добијамо:

$$p \Leftrightarrow q =_{def} \neg((p \Rightarrow q) \Rightarrow (\neg(q \Rightarrow p))) \qquad (\Leftrightarrow_{def})$$

(везник $\bot$) Везник $\bot$ дефинишемо на следећи начин:

$$\bot =_{def} \neg(p \Rightarrow p) \qquad (\bot_{def})$$

(везник $\top$) Везник $\top$ дефинишемо на следећи начин:

$$\top =_{def} p \Rightarrow p \qquad (\top_{def})$$

На крају имамо скуп $\{\Rightarrow, \bot\}$.

Задатак 4 Користећи претходни задатак, Задатак 3, у коме смо помоћу везника $\Rightarrow$ и $\neg$ дефинисали остале везнике, и користећи дефиницију везника $\neg$ да је формула $\neg p$ замена за $p \Rightarrow \bot$ добијамо:

$$p \wedge q =_{def} (p \Rightarrow (q \Rightarrow \bot)) \Rightarrow \bot \qquad (\wedge_{def})$$
$$p \vee q =_{def} (p \Rightarrow \bot) \Rightarrow q \qquad (\vee_{def})$$
$$p \Leftrightarrow q =_{def} ((p \Rightarrow q) \Rightarrow ((q \Rightarrow p) \Rightarrow \bot)) \Rightarrow \bot \qquad (\Leftrightarrow_{def})$$
$$\neg p =_{def} p \Rightarrow \bot \qquad (\neg_{def})$$
$$\top =_{def} p \Rightarrow p \qquad (\top_{def})$$

После неколико двочланих скупова помоћу чијих везника дефинишемо остале везнике скупа $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$, намеће се следеће питање: да ли сви везници тог скупа могу бити дефинисани само помоћу једног везника? Одговор је: ДА, али то није ниједан од везника из тог скупа. То ћемо моћи да урадимо помоћу следећа два нова везника, које зовемо шеферовски везници. Ове везнике интерпретирамо следећим бинарним операцијама на скупу $\mathbf{I} = \{0, 1\}$:

$\uparrow$	0	1
0	1	1
1	1	0

$\downarrow$	0	1
0	1	0
1	0	0

а можемо их и дефинисати помоћу познатих везника на следећи начин:

$$p \uparrow q =_{def} \neg(p \wedge q)$$
$$p \downarrow q =_{def} \neg(p \vee q)$$

Тврдимо да сви везници скупа $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ могу бити представљени само помоћу једног од везника $\uparrow$ и $\downarrow$. Како ћемо то показати? Довољно је да све веснике једног од скупова из Задатака 1-4 представимо помоћу везника $\uparrow$, односно везника $\downarrow$.

Задатак 5 Покажимо да се везници скупа $\{\wedge, \neg\}$ могу представити помоћу везника $\uparrow$.
Истиносне таблице за формуле $p \uparrow p$ и $(p \uparrow q) \uparrow (p \uparrow q)$ су редом:

p	$p \uparrow p$
1	0
0	1

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

Дакле, имамо $\neg p \equiv p \uparrow p$ и $p \wedge q \equiv (p \uparrow q) \uparrow (p \uparrow q)$. Зато имамо следеће дефиниције везника $\neg$ и $\wedge$ помоћу везника $\uparrow$:

$$\neg p =_{def} p \uparrow p \qquad (\neg_{def})$$
$$p \wedge q =_{def} (p \uparrow q) \uparrow (p \uparrow q) \qquad (\wedge_{def})$$

У Задатку 2 смо показали да везнике $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\bot$ и $\top$ можемо представити помоћу $\wedge$ и $\neg$, па користећи ове дефиниције, све везнике из $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ можемо представити само помоћу везника $\uparrow$.

Задатак 6 Покажимо да се везници скупа $\{\vee, \neg\}$ могу представити помоћу везника $\downarrow$.
Истиносне таблице за формуле $p \downarrow p$ и $(p \downarrow q) \downarrow (p \downarrow q)$ су редом:

p	$p \downarrow p$
1	0
0	1

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

Дакле, имамо $\neg p \equiv p \downarrow p$ и $p \vee q \equiv (p \downarrow q) \downarrow (p \downarrow q)$. Зато имамо следеће дефиниције везника $\neg$ и $\vee$ помоћу везника $\downarrow$:

$$\neg p =_{def} p \downarrow p \qquad (\neg_{def})$$
$$p \vee q =_{def} (p \downarrow q) \downarrow (p \downarrow q) \qquad (\vee_{def})$$

Из Задатка 1 имамо да се везници $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\bot$ и $\top$ могу представити помоћу $\vee$ и $\neg$, стога све везнике из $\{\wedge, \vee, \Rightarrow, \Leftrightarrow, \neg, \top, \bot\}$ можемо представити само помоћу везника $\downarrow$.

На скупу $\mathbf{I} = \{0, 1\}$, осим операција из одељка 2.2.1 и операција $\uparrow$ и $\downarrow$, постоје и друге операције. Свака од њих може бити интерпретација неког логичког

везника који можемо додати постојећем скупу везника алфабета исказне логике. Дакле, за сваку операцију дужине n на $\mathbf{I} = \{0,1\}$ (за неки природан број n) можемо дефинисати један везник дужине n који додајемо скупу везника алфабета исказне логике и чија интерпретација је та операција. Питамо се, да ли постоји скуп који чине само неки логички везници (не сви) такав да има следеће својство: помоћу везника тог скупа могу се дефинисати сви могући везници, тј. везници свих дужина? Одговор је: ДА, постоје такви скупови везника. Такве скупове везника зовемо функционално потпуни скупови везника или базе везника, а то њихово својство је функционална потпуност. Одговоримо одмах и на питање: да ли су скупови везника које смо посматрали у претходним задацима базе везника? Одговор је: ДА. Да бисмо то показали довољно је да за један од тих скупова покажемо да је база везника. То ћемо урадити за скуп $\{\Rightarrow, \bot\}$. Пре тога у наредном задатку покажимо шта су то сви могући везници.

Задатак 7 Пре свега подсетимо се да на скупу $\mathbf{I} = \{0,1\}$, који има два елемента, свих операција дужине n (за неки природни број n) има 2^{2^n}. А сада представимо логичке везнике чије интерпретације су операције на скупу $\mathbf{I} = \{0,1\}$.

Прво су на реду нуларни везници, везници дужине 0. Нуларних операција на скупу $\mathbf{I} = \{0,1\}$ има 2^{2^0}=2. То су две операције које на скупу $\mathbf{I} = \{0,1\}$ издвајају елемент 0 и елемент 1 и оне су интерпретације већ познатих нуларних логичких везника редом $\bot$ и $\top$.

Следећи су на реду унарни везници, везници дужине 1. Операција дужине 1 на скупу $\mathbf{I} = \{0,1\}$ има четири, $2^{2^1} = 4$, од којих је једна нама већ позната, а то је $\neg$. Дакле, на скупу $\mathbf{I} = \{0,1\}$ имамо $\neg$ и још три унарне операције α_1^1, α_2^1 и α_3^1 (где горњи индекс говори о дужини операције):

	$\neg$
0	1
1	0

	α_1^1
0	1
1	1

	α_2^1
0	0
1	1

	α_3^1
0	0
1	0

Алфабет исказне логике можемо проширити са три унарна везника α_1^1, α_2^1 и α_3^1, чије су интерпретације редом операције α_1^1, α_2^1 и α_3^1 на скупу $\mathbf{I} = \{0,1\}$. Да ли можемо те везнике да дефинишемо помоћу познатих везника? Потребне су нам неке формуле у којима се појављују познати везници и једно исказно слово, а чија истиносна таблица се поклапа са таблицом операција α_1^1, α_2^1 и α_3^1. То су редом формуле $p \vee \neg p$, p и $p \wedge \neg p$. Стога дефинишимо унарне логичке везнике α_1^1, α_2^1 и α_3^1 на следећи начин:

$$\alpha_1^1 p =_{def} p \vee \neg p \qquad \alpha_2^1 p =_{def} p \qquad \alpha_3^1 p =_{def} p \wedge \neg p$$

Сада су на реду бинарни везници. Бинарних операција, операција дужине 2, на скупу $\mathbf{I} = \{0,1\}$ има $2^{2^2} = 16$. Те операције представљамо таблицом која може имати један од следећа два облика:

	α	
1		1
1		0
0		1
0		0

α	0	1
1		
0		

Од бинарних операција су нам познате: $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, $\uparrow$ и $\downarrow$. Истакнимо да све бинарне операције можемо поделити у две скупине. У једној скупини је 8 операција, а другу чине преосталих 8 операција, при чему је свака од њих негација неке операције из прве скупине. Представимо то следећом табелом.

α_1^2	$\vee$	α_3^2	$\Rightarrow$	$\uparrow$	α_6^2	α_7^2	α_8^2
1	1	1	1	0	1	1	0
1	1	1	0	1	1	0	1
1	1	0	1	1	0	1	1
1	0	1	1	1	0	0	0
α'^2_1	$\downarrow$	α'^2_3	α'^2_4	$\wedge$	α'^2_6	α'^2_7	$\Leftrightarrow$
0	0	0	0	1	0	0	1
0	0	0	1	0	0	1	0
0	0	1	0	0	1	0	0
0	1	0	0	0	1	1	1

Нове бинарне логичке везнике дефинишемо на следећи начин:

$$p\ \alpha_1^2\ q \quad =_{def} \quad (p \Rightarrow p) \wedge (q \Rightarrow q) \qquad (\alpha_1^2)$$
$$p\ \alpha_3^2\ q \quad =_{def} \quad q \Rightarrow p \qquad (\alpha_3^2)$$
$$p\ \alpha_6^2\ q \quad =_{def} \quad p \wedge (q \Rightarrow q) \qquad (\alpha_6^2)$$
$$p\ \alpha_7^2\ q \quad =_{def} \quad q \wedge (p \Rightarrow p) \qquad (\alpha_7^2)$$
$$p\ \alpha_8^2\ q \quad =_{def} \quad \neg(p \Leftrightarrow q) \qquad (\alpha_8^2)$$
$$p\ \alpha'^2_1\ q \quad =_{def} \quad \neg(p\ \alpha_1^2\ q) \qquad (\alpha'^2_1)$$
$$p\ \alpha'^2_3\ q \quad =_{def} \quad \neg(p\ \alpha_3^2\ q) \qquad (\alpha'^2_3)$$
$$p\ \alpha'^2_4\ q \quad =_{def} \quad \neg(p \Rightarrow q) \qquad (\alpha'^2_4)$$
$$p\ \alpha'^2_6\ q \quad =_{def} \quad \neg(p\ \alpha_6^2\ q) \qquad (\alpha'^2_6)$$
$$p\ \alpha'^2_7\ q \quad =_{def} \quad \neg(p\ \alpha_7^2\ q) \qquad (\alpha'^2_7)$$

Приметимо да је везник α_8^2 ексклузивана (јака) дисјункција коју смо помињали у одељку о везницима.

До сада смо показали да је све везнике дужине 0, 1 и 2 могуће представити помоћу, да тако кажемо, познатих логичких везника. То значи да везнике $\top$, $\bot$, $\neg$, α_i^1 $(i \in \{1,2,3\})$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$, α_j^2 $(j \in \{1,3,6,7,8\})$ и α'^2_j $(j \in \{1,3,4,6,7\})$ можемо дефинисати помоћу везника алфабета исказне логике: $\wedge, \vee$, $\Rightarrow$ и $\bot$.

На реду су тернарни везници, везници дужине 3. Тернарних операција на скупу $\mathbf{I} = \{0, 1\}$ има $2^{2^3} = 2^8 = 256$. Овде се већ појављује проблем навођења свих тих операција и проблем проверавања да ли се сваки тернарни везник може представити помоћу познатих везника.

Потврду да се сваки везник произвољне дужине n (за сваки природан број n) може представити помоћу познатих везника даје нам следећа теорема.

ТЕОРЕМА 1 (ТЕОРЕМА О ФУНКЦИОНАЛНОЈ ПОТПУНОСТИ СКУПА $\{\Rightarrow, \bot\}$)
За сваки везник α^n дужине n, где је n природан број, постоји формула F у којој се јављају само симболи $p_1, ..., p_n$, $\Rightarrow$ и $\bot$, таква да је еквивалентна формули $\alpha^n(p_1, ..., p_n)$, тј. да важи:

$$\models \alpha^n(p_1, ..., p_n) \Leftrightarrow F.$$

ДОКАЗ

Доказ ће бити индукцијом по дужини n везника α^n.

База индукције: α^n је нуларни везник: $n = 0$.
Посматрамо све нуларне везнике, а то су везници $\top$ и $\bot$. За сваки од тих везника тражимо еквивалентну формулу F на алфабету исказне логике чији скуп везника је скуп $\{\Rightarrow, \bot\}$. За формулу $\bot$ тражена формула F је сама формула $\bot$. Знамо да важи: $\models \top \Leftrightarrow (\bot \Rightarrow \bot)$, па је за формулу $\top$ тражена формула F формула $\bot \Rightarrow \bot$.

Индукцијска претпоставка: теорема важи за сваки везник дужине n: за сваки везник α^n дужине n постоји формула F у којој се јављају само симболи $p_1, ..., p_n$, $\Rightarrow$ и $\bot$, таква да је:

$$\models \alpha^n(p_1, ..., p_n) \Leftrightarrow F.$$

Докажимо сада да теорема важи и за везник дужине $n + 1$.
Дакле, за произвољан везник α^{n+1} дужине $n + 1$, треба показати да постоји формула F у којој се јављају само симболи $p_1, ..., p_n, p_{n+1}$, $\Rightarrow$ и $\bot$, таква да је:

$$\models \alpha^{n+1}(p_1, ..., p_n, p_{n+1}) \Leftrightarrow F.$$

Било којом валуацијом v исказно слово p_{n+1} може имати или вредност 0 или вредност 1. То значи да се његова вредност сваком валуацијом v поклапа или са истиносном вредношћу формуле $\top$ (ако је $v(p_{n+1}) = 1$) или са истиносном вредношћу формуле $\bot$ (ако је $v(p_{n+1}) = 0$). Ако у формули $\alpha^{n+1}(p_1, ..., p_n, p_{n+1})$ исказно слово p_{n+1} заменимо са $\top$ и $\bot$, добијамо редом формуле $\alpha^{n+1}(p_1, ..., p_n, \top)$ и $\alpha^{n+1}(p_1, ..., p_n, \bot)$, чија исказна слова су $p_1, ..., p_n$. Помоћу тих формула дефинишемо два везника дужине n:

$$\beta^n(p_1, ..., p_n) =_{def} \alpha^{n+1}(p_1, ..., p_n, \top)$$

и

$$\gamma^n(p_1, ..., p_n) =_{def} \alpha^{n+1}(p_1, ..., p_n, \bot).$$

За сваки везник дужине n, па и за везнике $\beta^n(p_1,...,p_n)$ и $\gamma^n(p_1,...,p_n)$, важи индукцијска претпоставка, тј. постоје формуле F' и F'' у којима се јављају само симболи $p_1,...,p_n$, $\Rightarrow$ и $\bot$ и за њих важи:

$$\models \beta^n(p_1,...,p_n) \Leftrightarrow F'$$

и

$$\models \gamma^n(p_1,...,p_n) \Leftrightarrow F''$$

тј. на основу дефиниција везника β^n и γ^n, важи:

$$\models \alpha^{n+1}(p_1,...,p_n,\top) \Leftrightarrow F'$$

и

$$\models \alpha^{n+1}(p_1,...,p_n,\bot) \Leftrightarrow F''.$$

Дакле, имамо еквивалентност формула $\alpha^{n+1}(p_1,...,p_n,\top)$ и F', и еквивалентност формула $\alpha^{n+1}(p_1,...,p_n,\bot)$ и F'':

$$\alpha^{n+1}(p_1,...,p_n,\top) \equiv F' \qquad \text{и} \qquad \alpha^{n+1}(p_1,...,p_n,\bot) \equiv F''.$$

С друге стране, на основу ТЕОРЕМЕ 4 (одељак 2.2.3), за формулу $\alpha^{n+1}(p_1,...,p_n,p_{n+1})$ и њено исказно слово p_{n+1} имамо следећу таутологију:

$$\alpha^{n+1}(p_1,...,p_n,p_{n+1}) \Leftrightarrow ((p_{n+1} \Rightarrow \alpha^{n+1}(p_1,...,p_n,\top)) \wedge (\neg p_{n+1} \Rightarrow \alpha^{n+1}(p_1,...,p_n,\bot))).$$

Ако у тој таутологији формуле $\alpha^{n+1}(p_1,...,p_n,\top)$ и $\alpha^{n+1}(p_1,...,p_n,\bot)$ заменимо њима еквивалентним формулама редом F' и F'', онда на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА добијамо еквивалентну формулу тој таутологији. Дакле, добијамо таутологију:

$$\models \alpha^{n+1}(p_1,...,p_n,p_{n+1}) \Leftrightarrow ((p_{n+1} \Rightarrow F') \wedge (\neg p_{n+1} \Rightarrow F'')).$$

Посматрајмо формулу $(p_{n+1} \Rightarrow F') \wedge (\neg p_{n+1} \Rightarrow F'')$. У њеним потформулама F' и F'' се јављају само симболи $p_1,...,p_n$, $\Rightarrow$ и $\bot$, па треба још везнике $\neg$ и $\wedge$ (које видимо у запису формуле) представити помоћу $\Rightarrow$ и $\bot$. Користимо дефиницију везника $\neg$ помоћу $\Rightarrow$ и $\bot$ и добијамо да је $\neg p_{n+1} \Rightarrow F''$ замена за $(p_{n+1} \Rightarrow \bot) \Rightarrow F''$, па из последње таутологије добијамо таутологију:

$$\models \alpha^{n+1}(p_1,...,p_n,p_{n+1}) \Leftrightarrow ((p_{n+1} \Rightarrow F') \wedge ((p_{n+1} \Rightarrow \bot) \Rightarrow F'')).$$

Остаје још да везник $\wedge$ представимо помоћу $\Rightarrow$ и $\bot$. Имамо да је формула $A \wedge B$ замена за $(A \Rightarrow (B \Rightarrow \bot)) \Rightarrow \bot$, па је формула $(p_{n+1} \Rightarrow F') \wedge ((p_{n+1} \Rightarrow \bot) \Rightarrow F'')$, а тиме и $\alpha^{n+1}(p_1,...,p_n,p_{n+1})$, еквивалентна формули

$$((p_{n+1} \Rightarrow F') \Rightarrow (((p_{n+1} \Rightarrow \bot) \Rightarrow F'') \Rightarrow \bot)) \Rightarrow \bot.$$

Дакле, тражена формула F за коју важи

$$\models \alpha^{n+1}(p_1,...,p_n,p_{n+1}) \Leftrightarrow F$$

и у којој се појављују само симболи $p_1,...,p_n,p_{n+1}$, $\Rightarrow$ и $\bot$ је формула:

$$((p_{n+1} \Rightarrow F') \Rightarrow (((p_{n+1} \Rightarrow \bot) \Rightarrow F'') \Rightarrow \bot)) \Rightarrow \bot.$$

На овај начин смо доказали да важи индукцијски корак, па закључујемо да се сваки везник α^n произвољне дужине n може дефинисати помоћу везника $\Rightarrow$ и $\bot$.

$\diamondsuit$

Овом теоремом смо доказали функционалну потпуност скупа $\{\Rightarrow, \bot\}$, тј. показали смо да је скуп $\{\Rightarrow, \bot\}$ једна база везника. Пошто смо за све друге скупове које смо овде представили, скупове $\{\wedge, \vee, \Rightarrow, \bot\}$, $\{\vee, \neg\}$, $\{\wedge, \neg\}$, $\{\Rightarrow, \neg\}$, $\{\downarrow\}$ и $\{\uparrow\}$, показали да се помоћу њихових везника могу дефинисати везници базе $\{\Rightarrow, \bot\}$ закључујемо да су сви ти скупови базе везника.

2.4.2 Дисјунктивна и конјунктивна нормална форма

Овај одељак о облицима исказних формула који се зову дисјунктивна и конјунктивна нормална форма почећемо једним примером.

Пример 1 Посматрајмо формулу $F = (\neg((p \Rightarrow q) \wedge p)) \vee q$. Наш циљ је да направимо формулу која је еквивалентна формули F, а која је у дисјунктивној нормалној форми, тј. начињена је од неких формула $A_1, ..., A_m$ $(m \geq 1)$, које су повезане дисјункцијама, док је свака од формула $A_1, ..., A_m$ начињена од исказних слова и негација исказних слова повезаних конјункцијама. У поступку којим долазимо до такве формуле први корак је да направимо формулу која је еквивалентна нашој формули F, а у којој се појављују само везници $\wedge$, $\vee$ и $\neg$. Зато у формули F потформулу $p \Rightarrow q$ замењујемо њој еквивалентном формулом $\neg p \vee q$ и добијамо формулу $F_1 = (\neg((\neg p \vee q) \wedge p)) \vee q$. На основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формуле F и F_1 су еквивалентне формуле. Следећи корак је да формулу F_1 заменимо еквивалентном формулом у којој везник $\neg$ стоји само уз исказна слова. На основу Де Моргановог закона, $\models (\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$, потформула $\neg((\neg p \vee q) \wedge p)$ формуле F_1 је еквивалентна формули $(\neg(\neg p \vee q)) \vee \neg p$, а опет на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула F_1 је еквивалентна формули $F_2 = ((\neg(\neg p \vee q)) \vee \neg p) \vee q$. Сада користимо други Де Морганов закон, $\models (\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$, и добијамо да је потформула $\neg(\neg p \vee q)$ формуле F_2 еквивалентна формули $\neg\neg p \wedge \neg q$, па је на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула F_2 еквивалентна формули $F_3 = ((\neg\neg p \wedge \neg q) \vee \neg p) \vee q$. На крају, закон о двојној негацији, $\models \neg\neg A \Leftrightarrow A$, даје еквивалентност формула $\neg\neg p$ и p, а ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје формули F_3 (а тиме и полазној формули F) еквивалентну формулу F_4:

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

Формула F_4 је облика $(A_1 \vee A_2) \vee A_3$, где је A_1 потформула $p \wedge \neg q$, A_2 је $\neg p$ и A_3 је q. Дакле, формула F_4 јесте у дисјунктивној нормалној форми.

Сада ћемо да наведемо и дефиницију формуле у дисјунктивној нормалној форми, али пре тога уведимо појам литерала. Литерал је исказна формула која је или исказно слово или негација исказног слова. Са $\overline{p}$ ћемо означавати литерале p и $\neg p$, где је p неко исказно слово.

Дефиниција дисјунктивне нормалне форме

Нека је свака од формула $A_1, ..., A_m$ $(m \geq 1)$ начињена од литерала повезаних конјункцијама. Формула коју чине формуле $A_1, ..., A_m$ повезане дисјункцијама је формула у дисјунктивној нормалној форми (ДНФ) и ту формулу означавамо:

$$A_1 \vee ... \vee A_m,$$

а формуле $A_1, ..., A_m$ зовемо дисјункти. Ако су $\overline{p_1}, ..., \overline{p_n}$ $(n \geq 1)$ литерали од којих је начињена нека од формула A_i, $1 \leq i \leq m$, ту формулу A_i ћемо означавати: $\overline{p_1} \wedge ... \wedge \overline{p_n}$.

Дуално се дефинише формула у конјунктивној нормалној форми. Наиме, таква формула је начињена од формула које су повезане конјункцијама, а сваку од тих формула чине литерали повезани дисјункцијама.

Пример 2 Поставимо захтев да направимо формулу која је у конјунктивној нормалној форми и која је еквивалентна формули из Примера 1, формули $F = (\neg((p \Rightarrow q) \wedge p)) \vee q$. Да бисмо то урадили можемо посматрати формулу из Примера 1 еквивалентну формули F, формулу $F_4 = ((p \wedge \neg q) \vee \neg p) \vee q$, тачније њој еквивалентну формулу (на основу асоцијативности за $\vee$): $(p \wedge \neg q) \vee (\neg p \vee q)$. На основу закона дистрибутивности $\vee$ у односу на $\wedge$ имамо да је та формула еквивалентна формули $F_5 = (p \vee (\neg p \vee q)) \wedge (\neg q \vee (\neg p \vee q))$. Дакле, формула F је еквивалентна формули F_5. Формула F_5 је у конјунктивној нормалној форми, тј. та формула је облика $A_1 \wedge A_2$, где је A_1 потформула $p \vee (\neg p \vee q)$ и A_2 је потформула $\neg q \vee (\neg p \vee q)$.

А сада дајемо дефиницију формула у конјунктивној нормалној форми.

Дефиниција конјунктивне нормалне форме

Нека је свака од формула $A_1, ..., A_m$ $(m \geq 1)$ начињена од литерала повезаних дисјункцијама. Формула коју чине формуле $A_1, ..., A_m$ повезане конјункцијама је формула у конјунктивној нормалној форми (КНФ) и ту формулу означавамо:

$$A_1 \wedge ... \wedge A_m,$$

а формуле $A_1, ..., A_m$ зовемо конјункти. Ако су $\overline{p_1}, ..., \overline{p_n}$ $(n \geq 1)$ литерали од којих је начињена нека од формула A_i, $1 \leq i \leq m$, ту формулу A_i ћемо означавати: $\overline{p_1} \vee ... \vee \overline{p_n}$.

Посматрајмо формуле $A_1, ..., A_m$ начињене од литерала повезаних конјункцијама, где је m веће од 2. Појаснимо везу између записа уопштене дисјункције и записа формуле у ДНФ. На пример за $m = 4$ и формуле A_1, A_2, A_3 и A_4 имамо да је уопштена дисјункција $\bigvee_{i=1}^{4} A_i = ((A_1 \vee A_2) \vee A_3) \vee A_4$, тј. заграде су у тој формули асоциране налево. На основу закона асоцијативности за $\vee$ та формула је еквивалентна формулама $(A_1 \vee A_2) \vee (A_3 \vee A_4)$ и $A_1 \vee ((A_2 \vee A_3) \vee A_4)$ у којима су заграде другачије распоређене. Ми смо ДНФ дефинисали тако да нам није

битан распоред заграда и за све наведене, међусобно еквивалентне формуле, кажемо да су начињене од формула A_1, A_2, A_3, A_4 повезаних дисјункцијама, тј. за њих можемо да користимо ознаку $A_1 \vee A_2 \vee A_3 \vee A_4$. Исто важи и за уопштену конјункцију и КНФ. А сада погледајмо следећи пример.

Пример 3 Имамо формулу

$$F = (p \wedge (\neg q \wedge r)) \vee ((p \wedge \neg q) \vee (\neg r \wedge (q \wedge s))).$$

Формула F је у ДНФ, тј. формула F је облика $A_1 \vee (A_2 \vee A_3)$, за формуле: $A_1 = p \wedge (\neg q \wedge r)$, $A_2 = p \wedge \neg q$ и $A_3 = \neg r \wedge (q \wedge s)$. Посматрајмо формулу $B_1 = (p \wedge \neg q) \wedge r$, која је уопштена конјункција и има исте литерале као формула A_1 и то поређане истим редом, тј. B_1 је добијена од A_1 само премештањем заграда. Исто важи за формуле $B_2 = p \wedge \neg q$ и A_2 (оне су идентичне); и формуле $B_3 = (\neg r \wedge q) \wedge s$ и A_3. На основу закона асоцијативности за $\wedge$ имамо:

$$\models A_1 \Leftrightarrow B_1, \qquad \models A_2 \Leftrightarrow B_2 \qquad \text{и} \qquad \models A_3 \Leftrightarrow B_3.$$

Из тих таутологија, на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, добијамо таутологију:

$$\models (A_1 \vee (A_2 \vee A_3)) \Leftrightarrow (B_1 \vee (B_2 \vee B_3)),$$

па важи $A_1 \vee (A_2 \vee A_3) \equiv B_1 \vee (B_2 \vee B_3)$. На основу закона асоцијативности за $\vee$ имамо:

$$\models (B_1 \vee (B_2 \vee B_3)) \Leftrightarrow ((B_1 \vee B_2) \vee B_3),$$

тј. $B_1 \vee (B_2 \vee B_3) \equiv (B_1 \vee B_2) \vee B_3$, па транзитивност релације $\equiv$ даје:

$$\models (A_1 \vee (A_2 \vee A_3)) \Leftrightarrow ((B_1 \vee B_2) \vee B_3).$$

Добили смо да је F еквивалентна формули $F_1 = (B_1 \vee B_2) \vee B_3$. Формула F_1 је у ДНФ, има три дисјункта као и формула F и за свако i, $1 \leq i \leq 3$, одговарајући дисјункти формула F и F_1, дисјункти A_i и B_i, су начињени од истих литерала наведених истим редом, само су у њима заграде различито постављене. Формула F_1 је специфична по томе што је уопштена дисјункција и сви њени дисјункти су уопштене конјункције.

И за произвољну формулу која је у ДНФ, неку формулу $F = A_1 \vee ... \vee A_m$ ($m \geq 1$), постоји еквивалентна формула која је у ДНФ и уопштена дисјункција, а чији дисјункти су уопштене конјункције који се од A_1,...,A_m разликују само по распореду заграда. Исто важи и за неку формулу у КНФ, неку формулу $F = A_1 \wedge ... \wedge A_m$ ($m \geq 1$). Наиме, на основу закона асоцијативности за $\vee$ свака формула A_i, $1 \leq i \leq m$, еквивалентна је формули B_i, која је уопштена дисјункција литерала те формуле A_i поређаних истим редом као у A_i. На основу закона асоцијативности за $\wedge$ формула F је еквивалентна уопштеној конјункцији формула B_i, $1 \leq i \leq m$ која је исто једна формула у КНФ.

Покажимо сада важне особине формула у КНФ и ДНФ. Ако је формула у КНФ онда можемо веома једноставно да проверимо да ли је она таутологија. Погледајмо формулу у КНФ, формулу $A_1 \wedge ... \wedge A_m$ ($m \geq 1$), где су све формуле

$A_1, ..., A_m$ начињене од литерала повезаних дисјункцијама. Да би формула $A_1 \wedge ... \wedge A_m$ била истинита мора бити истинита свака од формула $A_1, ..., A_m$. Питамо се: ког облика треба да буду те формуле $A_1, ..., A_m$ да би биле истините за било које истиносне вредности њихових исказних слова, тј. за било коју валуацију? Довољно је да се у свакој од тих формула $A_1, ..., A_m$ јави неко исказно слово p и његова негација $\neg p$. За сваку валуацију v једна од вредности $v(p)$ и $v(\neg p)$ мора бити 1, па како су формуле $A_1, ..., A_m$ начињене од литерала повезаних дисјункцијама, имамо да је истиносна вредност сваке од $A_1, ..., A_m$ једнака 1 за сваку валуацију. Стога ако имамо формулу $A_1 \wedge ... \wedge A_m$ у КНФ и у свакој од формула $A_1, ..., A_m$ се јавља неко исказно слово и његова негација, онда знамо да је формула $A_1 \wedge ... \wedge A_m$ таутологија. Важи и обрнуто: ако је формула $A_1 \wedge ... \wedge A_m$ $(m \geq 1)$ у КНФ таутологија, онда се у свакој формули A_i, $1 \leq i \leq m$, јавља неко исказно слово и његова негација, и то ћемо показати у наредном задатку, Задатку 8.

Формула $F_5 = (p \vee (\neg p \vee q)) \wedge (\neg q \vee (\neg p \vee q))$ из Примера 2 је пример формуле у КНФ и она је облика $A_1 \wedge A_2$. У формули A_1 јавља се исказно слово p и његова негација $\neg p$, а у формули A_2 јавља се исказно слово q и његова негација $\neg q$. Дакле, формула F_5 јесте таутологија. Формула $F = (\neg((p \Rightarrow q) \wedge p)) \vee q$ је еквивалентна формули F_5, па закључујемо да је и формула F таутологија.

Задатак 8 Покажимо да важи следећа особина:
формула $A_1 \wedge ... \wedge A_m$ $(m \geq 1)$ у КНФ је таутологија ако и само ако се у свакој A_i $(1 \leq i \leq m)$ јавља неко исказно слово и његова негација.
Део да формула описаног облика јесте таутологија већ смо доказали. Остаје да докажемо други део тврђења: да свака таутологија у КНФ мора бити описаног облика. Претпоставимо да међу формулама A_1,..., A_m постоји нека формула A_l са особином да се у њој не појављују неко исказно слово и његова негација. Посматрајмо скуп свих исказних слова која су литерали формуле A_l, скуп $\{p_1, ..., p_k\}$, и скуп свих исказних слова чије негације су литерали формуле A_l, скуп $\{q_1, ..., q_j\}$, где неки од тих скупова може бити и празан. Јасно је да на основу особине формуле A_l скупови $\{p_1, ..., p_k\}$ и $\{q_1, ..., q_j\}$ немају заједничких елемената. Сада посматрамо валуацију v такву да је $v(p_i) = 0$, $1 \leq i \leq k$ и $v(q_i) = 1$, $1 \leq i \leq j$. Имамо да је формула A_l сачињена од литерала p_1,..., p_k, $\neg q_1$,..., $\neg q_j$ повезаних дисјункцијама, а истиносна вредност валуацијом v сваког тог литерала је 0. Дакле, $v(A_l) = 0$. Одатле, на основу дефиниције v, добијамо да је $v(A_1 \wedge ... \wedge A_m) = 0$, што је немогуће јер је формула $A_1 \wedge ... \wedge A_m$ таутологија. Закључујемо да се у свакој формули A_i, $1 \leq i \leq m$, мора јављати неко исказно слово и његова негација.

А сада погледајмо шта нам даје ДНФ. Ако је формула у ДНФ, онда се врло једноставно проверава да ли је она контрадикција. Погледајмо формулу у ДНФ, формулу $A_1 \vee ... \vee A_m$ $(m \geq 1)$, где су све формуле $A_1, ..., A_m$ начињене од литерала повезаних конјункцијама. Да би формула $A_1 \vee ... \vee A_m$ била неистинита, мора бити неистинита свака од формула $A_1, ..., A_m$. Вредност сваке од

формула $A_1, ..., A_m$ је увек 0 ако се у њој јавља неко исказно слово, на пример p, и његова негација $\neg p$. За сваку валуацију v једна од вредности $v(p)$ и $v(\neg p)$ мора бити 0, па како су формуле $A_1, ..., A_m$ начињене од литерала повезаних конјункцијама, имамо да је истиносна вредност сваке од $A_1, ..., A_m$ једнака 0 за сваку валуацију. Када је истиносна вредност сваке од формула $A_1, ..., A_m$ једнака 0 онда је и истиносна вредност формуле $A_1 \vee ... \vee A_m$ једнака 0.

Дакле, за формулу у КНФ лако је проверити да ли је таутологија, а за формулу у ДНФ да ли је контрадикција. Због тих својстава постављамо питање: да ли за сваку исказну формулу F постоји формула у ДНФ и формула у КНФ које су њој еквивалентне? Одговор је: ДА, а то ћемо и доказати.

ТЕОРЕМА 2 (ТЕОРЕМА О ДНФ И КНФ)
За сваку формулу F постоји бар једна формула F^k у конјунктивној нормалној форми и бар једна формула F^d у дисјунктивној нормалној форми, такве да је:

$$\models F \Leftrightarrow F^k \quad \text{и} \quad \models F \Leftrightarrow F^d.$$

ДОКАЗ

Посматрајмо произвољну формулу F. Ако се у формули F појављују везници који нису из скупа $\{\wedge, \vee, \neg\}$, онда користећи познате везе између логичких везника правимо формулу еквивалентну формули F у којој се појављују само везници из тог скупа. Стога смемо да претпоставимо да је F формула већ таквог облика, тј. у формули F се појављују само везници $\wedge$, $\vee$ и $\neg$. Теорему доказујемо индукцијом по броју везника формуле F, броју n.

База индукције, формула F нема везника, $n = 0$. То значи да је формула F неко исказно слово, на пример исказно слово p. Тражене формуле F^k и F^d су само исказно слово p.

Индукцијска претпоставка: теорема важи за сваку формулу F која има мање од n логичких везника.

Докажимо да теорема важи и за формулу која има n везника.
Посматрајмо формулу F која има n везника. Формула F може имати један од следећих облика:

$$A \wedge B, \qquad A \vee B \qquad \text{или} \qquad \neg A.$$

Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка: постоје формуле A^k и B^k у конјунктивној нормалној форми и формуле A^d и B^d у дисјунктивној нормалној форми, такве да је:

$$\models A \Leftrightarrow A^k, \quad \models A \Leftrightarrow A^d \quad \text{и} \quad \models B \Leftrightarrow B^k, \quad \models B \Leftrightarrow B^d.$$

На основу закона о асоцијативности за $\wedge$ и $\vee$ и транзитивности релације еквивалентности формула, можемо претпоставити да су у формулама A^k, B^k, A^d и B^d све заграде асоциране налево. Дакле, формуле A^k и B^k су уопштене конјункције редом $D_1 \wedge ... \wedge D_m$ $(m \geq 1)$ и $D'_1 \wedge ... \wedge D'_l$ $(l \geq 1)$ за неке формуле $D_1, ..., D_m, D'_1, ..., D'_l$, које су

уопштене дисјункције литерала. Формуле A^d и B^d су уопштене дисјункције редом $C_1 \vee ... \vee C_k$ $(k \geq 1)$ и $C'_1 \vee ... \vee C'_j$ $(j \geq 1)$ за неке формуле $C_1, ..., C_k, C'_1, ..., C'_j$ које су уопштене конјункције литерала. Користећи ове формуле, направимо формуле F^k и F^d.

◁ Претпоставимо да је формула F облика $A \wedge B$.
Направимо прво формулу F^k.
Из $\models A \Leftrightarrow A^k$ и $\models B \Leftrightarrow B^k$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје:

$$\models (A \wedge B) \Leftrightarrow (A^k \wedge B^k),$$

где су формуле A^k и B^k у конјунктивној нормалној форми. Стога је и формула $A^k \wedge B^k$ у конјунктивној нормалној форми, па је тражена формула F^k баш формула $A^k \wedge B^k$.
Направимо сада формулу F^d.
Из $\models A \Leftrightarrow A^d$ и $\models B \Leftrightarrow B^d$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје:

$$\models (A \wedge B) \Leftrightarrow (A^d \wedge B^d),$$

тј. F је еквивалентна формули $A^d \wedge B^d$: $F \equiv A^d \wedge B^d$, где је формула $A^d \wedge B^d$ облика $(C_1 \vee ... \vee C_k) \wedge (C'_1 \vee ... \vee C'_j)$. Ако потформулу $C'_1 \vee ... \vee C'_j$ формуле $A^d \wedge B^d$ означимо са C', онда је формула $A^d \wedge B^d$ облика: $(C_1 \vee ... \vee C_k) \wedge C'$. На основу уопштеног закона дистрибутивности $\wedge$ у односу на $\vee$ имамо таутологију:

$$\models ((C_1 \vee ... \vee C_k) \wedge C') \Leftrightarrow ((C_1 \wedge C') \vee ... \vee (C_k \wedge C')),$$

где је формула десно од $\Leftrightarrow$, формула F_1:

$$(C_1 \wedge (C'_1 \vee ... \vee C'_j)) \ \vee \ ... \ \vee \ (C_k \wedge (C'_1 \vee ... \vee C'_j))$$

уопштена дисјункција формула $C_i \wedge (C'_1 \vee ... \vee C'_j)$, $\quad 1 \leq i \leq k$. Дакле, формула $A^d \wedge B^d$ је еквивалентна тој формули F_1. Користећи закон комутативности за $\wedge$ и уопштени закон дистрибутивности $\wedge$ у односу на $\vee$ добијамо таутологију:

$$\models (C \wedge (C'_1 \vee ... \vee C'_j)) \Leftrightarrow ((C \wedge C'_1) \vee ... \vee (C \wedge C'_j)),$$

па имамо: $C \wedge (C'_1 \vee ... \vee C'_j) \equiv (C \wedge C'_1) \vee ... \vee (C \wedge C'_j)$. Стога за сваку од већ истакнутих потформула формуле F_1, $1 \leq i \leq k$, имамо:

$$C_i \wedge (C'_1 \vee ... \vee C'_j) \equiv (C_i \wedge C'_1) \vee ... \vee (C_i \wedge C'_j).$$

Сада у формули F_1 сваку њену потформулу $C_i \wedge (C'_1 \vee ... \vee C'_j)$, $1 \leq i \leq k$, замењујемо њој еквивалентном формулом и добијамо формулу F_2:

$$((C_1 \wedge C'_1) \ \vee ... \vee \ (C_1 \wedge C'_j)) \ \vee ... \vee \ ((C_k \wedge C'_1) \ \vee ... \vee \ (C_k \wedge C'_j)),$$

где све формуле C_1,..., C_k, C'_1,..., C'_j чине литерали који су повезани конјункцијама. То значи да је формула F_2 у дисјунктивној нормалној форми. На основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА формула F_1 (а тиме и $A^d \wedge B^d$) је еквивалентна формули F_2. Дакле, тражена формула F^d је формула F_2.

◁ Претпоставимо да је формула F облика $A \vee B$.
У овом случају је једноставније формирати формулу F^d.
Из $\models A \Leftrightarrow A^d$ и $\models B \Leftrightarrow B^d$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје:

$$\models (A \vee B) \Leftrightarrow (A^d \vee B^d)$$

и формуле A^d и B^d су у дисјунктивној нормалној форми. Стога је и формула $A^d \vee B^d$ у дисјунктивној нормалној форми, па је тражена формула F^d баш формула $A^d \vee B^d$.
За налажење формуле F^k за формулу $A \vee B$ поступамо аналогно као у случају налажења формуле F^d за формулу $A \wedge B$.

◁ Претпоставимо да је формула F облика $\neg A$.
Из $\models A \Leftrightarrow A^k$ и $\models A \Leftrightarrow A^d$ ТЕОРЕМА О ЗАМЕНИ ЕКВИВАЛЕНАТА даје:

$$\models (\neg A) \Leftrightarrow (\neg A^k) \quad \text{и} \quad \models (\neg A) \Leftrightarrow (\neg A^d),$$

тј. $F \equiv \neg A^k$ и $F \equiv \neg A^d$. Направимо формулу F^d.
За то ћемо користити формулу A^k која је у конјунктивној нормалној форми. Формула A^k је облика $D_1 \wedge ... \wedge D_m$, па је формула $\neg A^k$ облика $\neg(D_1 \wedge ... \wedge D_m)$. На основу уопштеног Де Моргановог закона имамо таутологију:

$$\models (\neg(D_1 \wedge ... \wedge D_m)) \Leftrightarrow (\neg D_1 \vee ... \vee \neg D_m),$$

где је формула $\neg D_1 \vee ... \vee \neg D_m$ уопштена дисјункција формула $\neg D_i$, $1 \leq i \leq m$. Дакле, $\neg A^k \equiv \neg D_1 \vee ... \vee \neg D_m$, тј. $F \equiv \neg D_1 \vee ... \vee \neg D_m$.
Свака формула D_i, за $1 \leq i \leq m$, јесте уопштена дисјункција литерала и свака формула D_i има s_i литерала, за $s_i \geq 1$. Дакле, произвољна формула D_i, за $1 \leq i \leq m$, јесте уопштена дисјункција $\overline{p}_1^i \vee ... \vee \overline{p}_{s_i}^i$, где су $\overline{p}_1^i$,..., $\overline{p}_{s_i}^i$ неки литерали. Стога је свака формула $\neg D_i$ $(1 \leq i \leq m)$ облика $\neg(\overline{p}_1^i \vee ... \vee \overline{p}_{s_i}^i)$. Опет користећи уопштени Де Морганов закон, имамо таутологију:

$$\models (\neg(\overline{p}_1^i \vee ... \vee \overline{p}_{s_i}^i)) \Leftrightarrow (\neg\overline{p}_1^i \wedge ... \wedge \neg\overline{p}_{s_i}^i)$$

и добијамо да је свака формула $\neg D_i$ $(1 \leq i \leq m)$ еквивалентна формули $\neg\overline{p}_1^i \wedge ... \wedge \neg\overline{p}_{s_i}^i$. (Напоменимо да ако је у $\neg\overline{p}_1^i \wedge ... \wedge \neg\overline{p}_{s_i}^i$ неки литерал $\overline{p}_t^i$ облика $\neg r$ за неко исказно слово r, онда $\neg\overline{p}_t^i$ постаје (због двојне негације) литерал r.) Ако у формули $\neg D_1 \vee ... \vee \neg D_m$ сваку формулу $\neg D_i$ $(1 \leq i \leq m)$ заменимо њој еквивалентном формулом $\neg\overline{p}_1^i \wedge ... \wedge \neg\overline{p}_{s_i}^i$ добијамо формулу F_2 која је у дисјунктивној нормалној форми и за коју, на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, важи: $\neg D_1 \vee ... \vee \neg D_m \equiv F_2$. Већ имамо да је $F \equiv \neg D_1 \vee ... \vee \neg D_m$, па на основу транзитивности релације $\equiv$, имамо $F \equiv F_2$, тј. формула F_2 је тражена формула F^d за коју важи:

$$\models F \Leftrightarrow F^d.$$

За налажење формуле F^k користимо формулу A^d и поступамо аналогно као у случају налажења формуле F^d.
Дакле, доказали смо индукцијски корак, па закључујемо да за произвољну формулу F постоје формуле у КНФ и ДНФ, редом формуле F^k и F^d, које су њој еквивалентне.

♢

2.4.3 Дуалност везника $\wedge$ и $\vee$

У овом одељку говорићемо о својствима која повезују везнике $\wedge$ и $\vee$.

Подсетимо се закона дистрибутивности.

Закон дистрибутивности $\wedge$ у односу на $\vee$:

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

и закон дистрибутивности $\vee$ у односу на $\wedge$:

$$\models ((p \wedge q) \vee r) \Leftrightarrow ((p \vee r) \wedge (q \vee r)).$$

Видимо да су формуле $(p \wedge q) \vee r$ и $(p \vee r) \wedge (q \vee r)$ које се појављују у другом дистрибутивном закону добијене од формула које се појављују у првом дистрибутивном закону, редом формула $(p \vee q) \wedge r$ и $(p \wedge r) \vee (q \wedge r)$, тако што су везници $\wedge$ и $\vee$ заменили места. Можемо рећи да је првим дистрибутивним законом дата еквивалентност две формуле, формула $(p \vee q) \wedge r$ и $(p \wedge r) \vee (q \wedge r)$, а да други дистрибутивни закон даје еквивалентност формула које су добијене од те две формуле тако што су везници $\wedge$ и $\vee$ заменили места, еквивалентност формула $(p \wedge q) \vee r$ и $(p \vee r) \wedge (q \vee r)$.

Ту замену везника $\wedge$ и $\vee$ прецизније ћемо дефинисати функцијом $^\delta$ на скупу свих исказних формула $\mathcal{F}$. Само у овом одељку уместо скупа логичких везника $\{\wedge, \vee, \Rightarrow, \bot\}$ у алфабету исказне логике користићемо скуп $\{\wedge, \vee, \neg\}$. На основу нашег излагања о базама везника јасно је да за сваку исказну формулу F можемо да направимо еквивалентну формулу на алфабету чији је скуп везника скуп $\{\wedge, \vee, \neg\}$.

Функцијом $^\delta$ произвољна формула F слика се у формулу која је добијена тако што у полазној формули F уместо везника $\wedge$ ставимо $\vee$, а уместо $\vee$ ставимо $\wedge$. Дефинишемо функцију $^\delta : \mathcal{F} \to \mathcal{F}$ индуктивно на следећи начин:

(1) за неко исказно слово p: $p^\delta = p$;

(2) (2.1) за неку исказну формулу $A \wedge B$: $(A \wedge B)^\delta = A^\delta \vee B^\delta$;

(2.2) за неку исказну формулу $A \vee B$: $(A \vee B)^\delta = A^\delta \wedge B^\delta$;

(2.3) за неку исказну формулу $\neg A$: $(\neg A)^\delta = \neg A^\delta$.

Када пођемо од формуле F и применимо поступак замене $\wedge$ са $\vee$, и $\vee$ са $\wedge$ добијемо формулу F^δ. Ако сада на формулу F^δ применимо исти поступак и направимо формулу $(F^\delta)^\delta$, вратићемо се на почетак, тј. формула $(F^\delta)^\delta$ је полазна формула F. То је и показано у наредном задатку.

Задатак 9 Покажимо индукцијом по броју везника у формули да за сваку исказну формулу F важи: $(F^\delta)^\delta = F$.
Ако је F неко исказно слово p, онда је $(F^\delta)^\delta = (p^\delta)^\delta = p^\delta = p = F$. Ако је формула F облика $A \wedge B$, $A \vee B$ или $\neg A$, онда формуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка: $(A^\delta)^\delta = A$ и $(B^\delta)^\delta = B$. Покажимо да особина важи у случају када је формула F облика $A \wedge B$. Имамо: $(F^\delta)^\delta = ((A \wedge B)^\delta)^\delta = (A^\delta \vee B^\delta)^\delta = (A^\delta)^\delta \wedge (B^\delta)^\delta$. С обзиром на то да је $(A^\delta)^\delta = A$ и $(B^\delta)^\delta = B$, закључујемо да је $(F^\delta)^\delta$ једнако $A \wedge B$, тј. $(F^\delta)^\delta = F$. Исто се поступа и у другим случајевима.

Користећи функцију $^\delta$ и закон дистрибутивности $\wedge$ у односу на $\vee$,
$$\models ((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (q \wedge r)),$$
закон дистрибутивности $\vee$ у односу на $\wedge$ можемо записати овако:
$$\models ((p \vee q) \wedge r)^\delta \Leftrightarrow ((p \wedge r) \vee (q \wedge r))^\delta.$$

Приметимо да се, користећи познате таутологије, лако може доказати да важи:
ако је $((p \vee q) \wedge r) \Leftrightarrow ((p \wedge r) \vee (q \wedge r))$ таутологија,
онда је и $((p \vee q) \wedge r)^\delta \Leftrightarrow ((p \wedge r) \vee (q \wedge r))^\delta$ таутологија.
Питамо се: да ли та особина важи за произвољне формуле? Одговор је: ДА.
То управо тврди наредна теорема, теорема о дуалности везника $\wedge$ и $\vee$.

ТЕОРЕМА 3 (ТЕОРЕМА О ДУАЛНОСТИ ВЕЗНИКА $\wedge$ И $\vee$)
Нека су D и E произвољне формуле.
Ако је формула $D \Leftrightarrow E$ таутологија, онда је и формула $D^\delta \Leftrightarrow E^\delta$ таутологија.

Да бисмо доказали ову теорему морамо пре тога да докажемо неколико лема. Осим тога потребно је дефинисати још једну функцију на скупу свих исказних формула $\mathcal{F}$. Функција $^* : \mathcal{F} \to \mathcal{F}$ је индуктивно дефинисана на следећи начин:

(1) за неко исказно слово p: $p^* = \neg p$;
(2) (2.1) за неку исказну формулу $A \wedge B$: $(A \wedge B)^* = A^* \vee B^*$;
(2.2) за неку исказну формулу $A \vee B$: $(A \vee B)^* = A^* \wedge B^*$;
(2.3) за неку исказну формулу $\neg A$: $(\neg A)^* = \neg A^*$.

ЛЕМА 1
За сваку формулу F формула $\neg F \Leftrightarrow F^*$ је таутологија.

ДОКАЗ
Лему ћемо доказати индукцијом по броју везника формуле F.

База индукције: број везника је 0, тј. формула F је неко исказно слово p. У том случају формула $\neg F$ је $\neg p$ и формула $F^* = p^*$ је $\neg p$, па пошто важи $\models \neg p \Leftrightarrow \neg p$, то важи: $\models \neg F \Leftrightarrow F^*$.

Индукцијска претпоставка: за сваку F са мање од n везника важи:
$$\models \neg F \Leftrightarrow F^*.$$

Докажимо да лема важи и за формулу која има n везника.
Посматрамо формулу F која има n везника. Формула F може имати један од следећих облика:
$$A \wedge B, \qquad A \vee B \qquad \text{или} \qquad \neg A.$$
Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају мањи број везника него формула F, стога за њих важи индукцијска претпоставка:
$$\models \neg A \Leftrightarrow A^* \qquad \text{и} \qquad \models \neg B \Leftrightarrow B^*.$$

$\triangleleft$ Претпоставимо да је формула F облика $A \wedge B$.
Имамо да је $\neg F = \neg(A \wedge B)$ и $F^* = (A \wedge B)^* = A^* \vee B^*$. На основу индукцијске претпоставке и ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, имамо:
$$\models (\neg A \vee \neg B) \Leftrightarrow (A^* \vee B^*),$$

па добијамо: $\neg A \vee \neg B \equiv A^* \vee B^*$. На основу Де Моргановог закона, $\models (\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$, добијамо још један пар еквивалентних формула: $\neg F \equiv \neg A \vee \neg B$. Сада, на основу транзитивности релације $\equiv$, имамо $\neg F \equiv A^* \vee B^*$, тј. имамо таутологију:

$$\models \neg F \Leftrightarrow F^*.$$

◁ Претпоставимо да је формула F облика $A \vee B$.
На потпуно исти начин као у претходном случају добијамо да важи $\models (\neg(A \vee B)) \Leftrightarrow (A^* \wedge B^*)$. Дакле, $\models \neg F \Leftrightarrow F^*$.

◁ Претпоставимо да је формула F облика $\neg A$.
Формула $\neg F$ је $\neg\neg A$, а формула F^* је $\neg A^*$. На основу индукцијске претпоставке имамо $\models \neg A \Leftrightarrow A^*$. Сетимо се дела (1) ЛЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА: из $\models C \Leftrightarrow D$ следи $\models \neg C \Leftrightarrow \neg D$. Применом тог својства из $\models \neg A \Leftrightarrow A^*$ добијамо:

$$\models \neg\neg A \Leftrightarrow \neg A^*, \qquad \text{тј.} \qquad \models \neg F \Leftrightarrow F^*.$$

♢

ЛЕМА 2
Нека је F произвољна формула и нека је скуп исказних слова која се појављују у тој формули подскуп скупа $\{p_1, ..., p_m\}$. Тада важи да је формула $(F^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m} \Leftrightarrow F^\delta$ таутологија.

ДОКАЗ

Лему ћемо доказати индукцијом по броју везника формуле F.

База индукције: број везника је 0, тј. формула F је неко исказно слово p. Тада је:

$$F^* = \neg p, \;\; (F^*)^p_{\neg p} = (\neg p)^p_{\neg p} = \neg\neg p \quad \text{и} \quad F^\delta = p^\delta = p.$$

Како важи $\models \neg\neg p \Leftrightarrow p$, добијамо $\models (F^*)^p_{\neg p} \Leftrightarrow F^\delta$.

Индукцијска претпоставка: за сваку F са мање од n везника важи:

$$\models (F^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m} \Leftrightarrow F^\delta.$$

Докажимо да лема важи и за формулу која има n везника.
Посматрамо формулу F која има n везника. Формула F може имати један од следећих облика:

$$A \wedge B, \quad A \vee B \quad \text{или} \quad \neg A.$$

Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка:

$$\models (A^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m} \Leftrightarrow A^\delta \quad \text{и} \quad \models (B^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m} \Leftrightarrow B^\delta.$$

◁ Претпоставимо да је формула F облика $A \wedge B$.
Из индукцијске претпоставке, на основу ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА, добијамо таутологију:

$$\models ((A^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m} \vee (B^*)^{p_1 \dots p_m}_{\neg p_1 \dots \neg p_m}) \Leftrightarrow (A^\delta \vee B^\delta).$$

Покажимо да је то таутологија $\models (F^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \Leftrightarrow F^\delta$. На основу дефиниције униформне замене и дефиниција функција * и $^\delta$ за формулу $F = A \wedge B$ имамо:

$$(F^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} = ((A \wedge B)^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} = (A^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \vee (B^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m}$$
$$\text{и } F^\delta = (A \wedge B)^\delta = A^\delta \vee B^\delta.$$

Дакле, заиста имамо таутологију:

$$\models (F^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \Leftrightarrow F^\delta.$$

$\triangleleft$ Случајеви када је F облика $A \vee B$ и $\neg A$ доказују се аналогно.

$\diamondsuit$

Сада докажимо теорему о дуалности $\wedge$ и $\vee$.

ДОКАЗ ТЕОРЕМЕ О ДУАЛНОСТИ ВЕЗНИКА $\wedge$ И $\vee$

Претпоставимо да је формула $D \Leftrightarrow E$ таутологија. Онда из те таутологије, на основу својства да ако важи $\models A \Leftrightarrow B$, следи да важи $\models \neg A \Leftrightarrow \neg B$, добијамо таутологију:

$$\models \neg D \Leftrightarrow \neg E,$$

па важи $\neg D \equiv \neg E$. Још имамо, на основу ЛЕМЕ 1, да за формуле D и E важи:

$$\models \neg D \Leftrightarrow D^* \quad \text{и} \quad \models \neg E \Leftrightarrow E^*,$$

тј. $\neg D \equiv D^*$ и $\neg E \equiv E^*$. Из тих еквивалентности и еквивалентности $\neg D \equiv \neg E$, симетричност и транзитивност релације $\equiv$ дају $D^* \equiv E^*$, тј. таутологију:

$$\models D^* \Leftrightarrow E^*.$$

Из ове таутологије за формулу $D^* \Leftrightarrow E^*$, њена исказна слова $p_1, ..., p_m$ и за формуле $\neg p_1, ..., \neg p_m$, на основу ПОСЛЕДИЦЕ ТЕОРЕМЕ 3 из одељка 2.2.3, добијамо таутологију:

$$\models (D^* \Leftrightarrow E^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m},$$

а то је, на основу дефиниције униформне замене и веза између везника, таутологија:

$$\models (D^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \Leftrightarrow (E^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m},$$

тј. важи $(D^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \equiv (E^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m}$. С друге стране, ЛЕМА 2 даје:

$$\models (D^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \Leftrightarrow D^\delta \quad \text{и} \quad \models (E^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \Leftrightarrow E^\delta,$$

па важи $(D^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \equiv D^\delta$ и $(E^*)^{p_1\dots p_m}_{\neg p_1\dots\neg p_m} \equiv E^\delta$. Сада опет користећи симетричност и транзитивност $\equiv$, добијамо $D^\delta \equiv E^\delta$, тј. добијамо таутологију:

$$\models D^\delta \Leftrightarrow E^\delta.$$

$\diamondsuit$

У наредној леми показаћемо да важи и обрнуто од оног што тврди ТЕОРЕМА О ДУАЛНОСТИ ВЕЗНИКА $\wedge$ И $\vee$, тј. да важи: ако је формула $D^\delta \Leftrightarrow E^\delta$ таутологија, онда је и формула $D \Leftrightarrow E$ таутологија.

ЛЕМА 3
Нека су D и E произвољне формуле.
Ако је формула $D^\delta \Leftrightarrow E^\delta$ таутологија, онда је и формула $D \Leftrightarrow E$ таутологија.

ДОКАЗ

Како је $D^\delta \Leftrightarrow E^\delta$ таутологија, на основу ТЕОРЕМЕ О ДУАЛНОСТИ ВЕЗНИКА $\wedge$ И $\vee$ имамо да је и формула $(D^\delta)^\delta \Leftrightarrow (E^\delta)^\delta$ таутологија. Међутим, на основу особине функције $^\delta$ из Задатка 9 имамо да је, $(D^\delta)^\delta = D$ и $(E^\delta)^\delta = E$, па је та таутологија у ствари таутологија $D \Leftrightarrow E$.

$\diamondsuit$

Из ТЕОРЕМЕ О ДУАЛНОСТИ ВЕЗНИКА $\wedge$ И $\vee$ и ЛЕМЕ 3 имамо следећи закључак.

ПОСЛЕДИЦА 1
Нека су D и E произвољне формуле.
Формула $D \Leftrightarrow E$ је таутологија ако и само ако је формула $D^\delta \Leftrightarrow E^\delta$ таутологија.

Глава 3

Формалне теорије

3.1 Шта је то формална теорија?

Пре него што одговоримо на питање шта је то формална теорија, истакнимо главну карактеристику неке формалне теорије, тачније читаве математике. Доказ, тј. доказивање јесте најважнија карактеристика математике. На сваку констатацију облика: *Важи то и то*, „математика ће рећи": *Докажи!*

Сваки математички доказ је једно дедуктивно закључивање и почива на полазним претпоставкама и правилима по којима се из тих претпоставки изводе нова тврђења. Користећи симболе математичког језика и језика логике, имамо могућност да уместо са нејасним појмовима, као што су реченице природног језика, радимо са формулама. На тај начин доказ неког математичког тврђења можемо да сведемо на поступак којим се од неких полазних формула, користећи нека правила закључивања, добијају нове формуле. Погледајмо један једноставан пример.

Пример 1 Поставимо следеће питање: да ли из $a \leq b$, $b \leq c$ и $c \leq d$ следи $a \leq d$? Ево једног доказа:
1. $a \leq b$ је претпоставка;
2. $b \leq c$ је претпоставка;
3. $a \leq c$ закључујемо из претпоставки 1. и 2. користећи особину да је релација $\leq$ транзитивна, тј. да ако је $x \leq y$ и $y \leq z$, онда је $x \leq z$;
4. $c \leq d$ је претпоставка;
5. $a \leq d$ закључујемо из 3. и 4. опет користећи особину да је релација $\leq$ транзитивна.

Задатак формалног језика логике је да одређену математичку теорију преведе на језик формула, дефинише полазне формуле и дефинише правила извођења помоћу којих ће се изводити (добијати) нове формуле.

Свака математичка област има своје полазне појмове. Осим тога, има неке основне, једноставне особине за које не тражимо никакав доказ. Једноставност и очигледност тих особина су критеријуми по којима оне постају полазне истине те области. На основу полазних истина, користећи поступак дедуктивног закључивања, доказују (изводе, дедукују) се нова својства која важе у тој математичкој области. Затим, користећи већ доказана својства, доказујемо нова својства и на тај начин грађевина, која се зове резултати те области, расте и обогаћује се. Може се поставити питање шта је у тој изградњи математичких области узето као основна конструкција од које се онда, у зависности од тога који се материјал користи за наставак градње, могу направити тако различита здања као што су геометрија, алгебра, информатика и др. Та полазна конструкција, конструкција која је заједничка за све математичке теорије, јесте појам формалне теорије или формалног система. Појам формалне теорије је постављен веома широко тако да свака строго заснована математичка теорија јесте једна посебна формална теорија.

Када кажемо формална теорија $\mathcal{T}$, шта под тим подразумевамо? Прво, имамо скуп основних симбола (алфабет) те теорије $\mathcal{T}$, скуп $\mathcal{S}(\mathcal{T})$. Од тих симбола праве се све могуће речи (коначни низови симбола) над тим алфабетом. Из тог скупа речи издвајамо речи одређеног облика које зовемо формуле. Формуле чине други важан део те формалне теорије: скуп формула теорије $\mathcal{T}$, скуп $\mathcal{F}(\mathcal{T})$. Затим из скупа свих формула издвајамо један његов подскуп чије елементе зовемо аксиоме формалне теорије $\mathcal{T}$, скуп $\mathcal{A}(\mathcal{T})$, и то је трећи део. На крају, као четврти део, имамо коначан број правила извођења теорије $\mathcal{T}$ помоћу којих из аксиома и из већ доказаних тврђења изводимо (доказујемо) нова тврђења. Та правила извођења чине скуп $\mathcal{R}(\mathcal{T})$. Свако правило извођења је једна релација на скупу формула скоро у свим формалним теоријама. Наиме, ако је ρ једно правило извођења дужине $n+1$, онда ма какве биле формуле $A_1, ..., A_n, B$ постоји ефективан поступак за одлучивање да ли су редом формуле A_1,...,A_n, B у релацији ρ или нису. Ако су редом формуле $A_1, ..., A_n, B$ у релацији ρ, онда пишемо

$$\frac{A_1, ..., A_n}{B}\ \rho$$

и кажемо да су формуле $A_1, ..., A_n$ премисе (или горње формуле), а формула B закључак (или доња формула) тог правила извођења ρ.

Пре дефиниције формалне теорије, дајемо један пример.

Пример 2 Представимо једну формалну теорију, теорију $\mathcal{T}_1$.
Скуп основних симбола је $\mathcal{S}(\mathcal{T}_1) = \{0, 1, 2, 3, 4, 5\}$.
Скуп формула $\mathcal{F}(\mathcal{T}_1)$ чине све могуће речи над скупом симбола $\mathcal{S}(\mathcal{T}_1)$. Примери речи су: 4, 005, 55, 0345, 123451,...
Речи 1, 2, 3, 4 и 5 су аксиоме те теорије, па је скуп аксиома $\mathcal{A}(\mathcal{T}_1)$ скуп $\{1, 2, 3, 4, 5\}$.

На крају, формална теорија $\mathcal{T}_1$ има само једно правило извођења: $\frac{a \quad b}{a0b} R_0$. Правило R_0 од две формуле a и b прави трећу тако што на прву формулу надовезује другу, стављајући између њих симбол 0. Строго говорећи, правило R_0 је једна релација дужине 3 и то правило је једини елемент скупа правила извођења $\mathcal{R}(\mathcal{T}_1)$.
Са ова четири скупа формална теорија $\mathcal{T}_1$ је потпуно одређена.

А ево и дефиниције формалне теорије (формалног система).

Дефиниција формалне теорије (формалног система) $\mathcal{T}$

Формална теорија (формални систем) $\mathcal{T}$ је једна четворка објеката $(\mathcal{S}(\mathcal{T}), \mathcal{F}(\mathcal{T}), \mathcal{A}(\mathcal{T}), \mathcal{R}(\mathcal{T}))$, где је:

◇ $\mathcal{S}(\mathcal{T})$ скуп основних симбола или алфабет;
◇ $\mathcal{F}(\mathcal{T})$ скуп формула, који је подскуп скупа свих речи над алфабетом $\mathcal{S}(\mathcal{T})$, тј. скупа свих коначних низова симбола из $\mathcal{S}(\mathcal{T})$;
◇ $\mathcal{A}(\mathcal{T})$ скуп аксиома;
◇ $\mathcal{R}(\mathcal{T})$ скуп правила извођења.

Сада дајемо дефиницију најзначајније карактеристике формалне теорије, дефиницију доказа (извођења, дедукције) у некој формалној теорији $\mathcal{T}$.

Дефиниција доказа (извођења, дедукције) у формалној теорији $\mathcal{T}$

◇ Доказ (извођење, дедукција) у формалној теорији $\mathcal{T}$ је једно коначно дрво, на чијим листовима се налазе аксиоме, а свако гранање тог дрвета је оправдано неким правилом извођења, тако што се у горњим чворовима тог гранања налазе премисе правила, а у његовом доњем чвору је закључак тог правила. Ако се у корену тог дрвета налази формула F, онда је то доказ формуле F. (Приметимо да је доказ аксиоме дрво са једним чвором (корен и лист) у коме је сама та аксиома.)

◇ Осим као дрво доказ (извођење, дедукција) се може дефинисати и као коначан низ формула ($n \geq 1$)

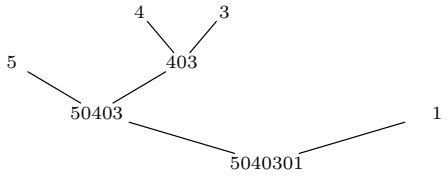
$$F_1, \ldots, F_n,$$

где за сваку формулу F_i, $1 \leq i \leq n$, важи:
или F_i је аксиома
или F_i је закључак неког правила извођења теорије $\mathcal{T}$, а премисе тог правила извођења су неке од формула из низа F_1,..., F_n, индекса мањег од i.
За доказ $F_1, ..., F_n$ кажемо да је доказ формуле F_n.

Ако имамо један доказ дат као низ формула $F_1, \ldots, F_n$ ($n \geq 1$), онда тај доказ можемо представити коначним дрветом у чијем корену се налази формула F_n, а на његовим листовима су све аксиоме из низа $F_1, ..., F_n$. Свако гранање у том дрвету је оправдано неким правилом извођења, тако што се у доњем чвору

налази закључак тог правила, који је нека формула F_i из низа $F_1, ..., F_n$, а у горњим чворовима тог гранања су премисе тог правила, које су формуле из низа $F_1, ..., F_n$ са индексом мањим од i.

Пример 3 Погледајмо дрво у чијим чворовима су формуле формалне теорије $\mathcal{T}_1$ из Примера 2:



Да ли је ово дрво један доказ у теорији $\mathcal{T}_1$? На листовима тог дрвета су аксиоме 4, 3, 5 и 1. Имамо три гранања и сва три су по једином правилу извођења теорије $\mathcal{T}_1$, правилу R_0. На пример, погледајмо гранање у чијем доњем чвору је формула 50403. У горњим чворовима тог гранања су формуле 5 и 403, а 50403 јесте закључак правила $\mathcal{R}_0$ из премиса 5 и 403. Дакле, посматрано дрво јесте један доказ у теорији $\mathcal{T}_1$ и то је доказ формуле која је у његовом корену, формуле 5040301. На доказу формуле 5040301 покажимо да дрво доказа можемо записати и на следећи начин:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{4}\quad\dfrac{}{3}}{403}\quad\dfrac{}{5}}{50403}\quad\dfrac{}{1}}{5040301}$$

Овај доказ можемо представити и коначним низом формула: $F_1 = 4$, $F_2 = 3$, $F_3 = 403$, $F_4 = 5$, $F_5 = 50403$, $F_6 = 1$ и $F_7 = 5040301$. Формуле F_1, F_2, F_4 и F_6 су аксиоме теорије $\mathcal{T}_1$; F_3 је закључак правила R_0, где су премисе тог правила формуле F_1 и F_2; F_5 је закључак правила R_0, где су премисе тог правила формуле F_3 и F_4; и F_7 је закључак правила R_0, а премисе тог правила су формуле F_5 и F_6.

Пошто смо се упознали са појмом доказа, можемо дати дефиницију теореме формалне теорије $\mathcal{T}$.

Дефиниција теореме формалне теорије $\mathcal{T}$

У формалној теорији $\mathcal{T}$ формула F је теорема АККО постоји бар један доказ формуле F у теорији $\mathcal{T}$. Да је формула F теорема теорије $\mathcal{T}$ означавамо са $\vdash_{\mathcal{T}} F$ (или $\vdash F$ ако знамо о којој формалној теорији је реч), а за тај доказ формуле F кажемо да је један доказ теореме F у теорији $\mathcal{T}$.

Доказ формуле F из скупа хипотеза Φ у формалној теорији $\mathcal{T}$ је једно коначно дрво у чијем корену је формула F, а на свим његовим листовима налазе

се или аксиоме или формуле скупа Φ. Свако гранање тог дрвета је оправдано неким правилом извођења те теорије, тако што се у доњем чвору тог гранања налази закључак правила, а у његовим горњим чворовима су премисе тог правила. Другачије речено, постоји низ формула које су или аксиоме или формуле скупа Φ или закључци правила извођења чије премисе су неке већ наведене формуле тог низа, а последња формула је формула F. Формуле скупа Φ зовемо хипотезама тог доказа. Да постоји доказ формуле F из скупа хипотеза Φ у формалној теорији $\mathcal{T}$ означавамо са $\Phi \vdash_{\mathcal{T}} F$ (или $\Phi \vdash F$) и кажемо да је формула F последица скупа формула Φ.

У оквиру овог уводног излагања о формалним теоријама представимо и два важна својства формалних теорија: одлучивост и непротивречност. Ако постоји ефективан поступак (процедура) помоћу којег за сваку формулу из скупа формула теорије $\mathcal{T}$, скупа $\mathcal{F}(\mathcal{T})$, можемо утврдити да ли је теорема теорије $\mathcal{T}$ или није, онда за теорију $\mathcal{T}$ кажемо да је одлучива. Формална теорија $\mathcal{T}$ је непротивречна ако постоји бар једна формула те теорије која није теорема. У противном, теорија $\mathcal{T}$ је противречна.

Напомена. Истакнимо да се у изграђивању неке формалне теорије појављују две врсте теорема. Постоје теореме које су део формалне теорије изведене из њених аксиома уз помоћ њених правила извођења и постоје теореме на метајезику, метатеореме, у којима се говори о својствима посматране формалне теорије.

3.2 Исказна логика као формална теорија

У одељцима 2.1, 2.2 и 2.4 изучавали смо исказну логику као једну целину коју образују њена синтакса и њена семантика. У тим изучавањима смо синтаксу користили као алат који нам даје симболе и који нам омогућава да прецизно (од тих симбола) формирамо исказне формуле. У главној улози је пак била семантика где смо се бавили значењима исказних формула (или истините или лажне). У овом одељку ћемо исказну логику представити као једну формалну теорију. Посматрати исказну логику као формалну теорију значи за тежиште изабрати њену синтаксу. Централно место заузимају теореме те теорије које су резултат формалног закључивања (доказа) из посебних формула (аксиома) на основу неких правила извођења. У тим процесима прављења теорема исказне логике нећемо се бавити истинитошћу тих формула. Ипак, на крају одељка ћемо повезати теореме исказне логике, као формуле које су производ правила извођења из аксиома, и таутологије, као формуле исказне логике које су увек истините. Показаћемо да су скуп теорема исказне логике и скуп таутологија једнаки скупови.

Али пре тога морамо представити исказну логику као формалну теорију и то ћемо урадити на два начина. Наиме, представићемо формални систем природне дедукције, формални систем $\mathcal{N}$, и хилбертовски формални систем, формални систем $\mathcal{L}$.

3.2.1 Правила извођења природне дедукције

Може се рећи да су докази у природној дедукцији најближи интуитивном схватању доказа и доказивања. У природној дедукцији доказ је у облику дрвета на чијим листовима су хипотезе (претпоставке) од којих полазимо, а свако његово гранање је по неком правилу извођења, тако што су у његовим горњим чворовима премисе, а у доњем чвору је закључак тог правила. То дрво се назива и извођењем формуле која је у његовом корену. Важна карактеристика природне дедукције је да у поступку извођења неке хипотезе могу бити избрисане (кажемо прецртане). Када будемо представили правила извођења то ћемо детаљно објаснити, а сада дајемо само скицу тог поступка. Наиме, ми полазимо од неких хипотеза, примењујемо неко правило извођења, добијамо његов закључак, опет примењујемо неко правило извођења и тако градимо једно извођење. У природној дедукцији постоје правила извођења која, да би у неком извођењу била примењена, користе неке од хипотеза тог извођења. Када се такво правило примени и изведе његов закључак, хипотезе које су искоришћене прецртају се. Ако имамо једно извођење неке формуле F, онда кажемо да је формула F изведена из хипотеза које су на листовима тог извођења и при прављењу тог извођења нису прецртане, тј. из непрецртаних хипотеза.

Истакнимо сада једну заједничку карактеристику правила извођења природне дедукције. Упрошћено речено, правила извођења природне дедукције показују нам како се од постојећих доказа уз помоћ логичких везника прави нови доказ. Везници $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ и $\neg$ који се виде редом у формулама $A \wedge B$, $A \vee B$, $A \Rightarrow B$, $A \Leftrightarrow B$ и $\neg A$ су главни везници тих формула. За сваки логички везник постоје два правила извођења природне дедукције: правило увођења и правило елиминације. У свим правилима увођења везник, на који се правило односи, јесте главни везник закључка тог правила увођења, тачније закључак је направљен помоћу тог везника и премиса правила. На пример, правило увођења везника $\wedge$ каже да ако постоји неки доказ D_1 за формулу A и неки доказ D_2 за формулу B, онда постоји доказ (начињен од D_1 и D_2) за формулу $A \wedge B$:

$$\dfrac{\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2\\ A & B\end{array}}{A \wedge B}$$

У овом правилу везник $\wedge$ се уводи у закључак правила, у формулу $A \wedge B$, тј. закључак је направљен помоћу везника $\wedge$ и премиса тог правила (формула A и B). Што се тиче неког правила елиминације, везник на који се правило односи је главни везник у једној од његових премиса, а закључак је нека потформула те премисе или нека друга формула. Као пример једног правила елиминације везника, навешћемо правило елиминације везника $\Rightarrow$. Инспирација за ово правило је таутологија modus ponens: ако постоји неки доказ D_1 за формулу $A \Rightarrow B$ и постоји неки доказ D_2 за формулу A, онда постоји доказ (начињен од D_1 и D_2) за формулу B:

$$\dfrac{\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2\\ A \Rightarrow B & A\end{array}}{B}$$

У правилу елиминације везника $\Rightarrow$, тај везник је главни везник у премиси, формули $A \Rightarrow B$, а закључак правила је потформула те формуле, формула B.

У наредном одељку дајемо дефиницију система природне дедукције и дефиницију доказа у том систему. Сада ћемо само неформално представити правила извођења природне дедукције. Прво наведимо аксиоматско правило.

Аксиоматско правило

Ако је A формула, онда је

$$A$$

доказ за A и његова непрецртана хипотеза је A.

А сада представимо правила извођења за везнике.

1. Правила увођења и елиминације везника $\wedge$

Погледајмо пример доказа једне очигледне истине.

Пример 1 Докажимо да важи: $1 < \sqrt{2} < 2$.
Записом $1 < \sqrt{2} < 2$ дате су две неједнакости: $1 < \sqrt{2}$ и $\sqrt{2} < 2$. Зато морамо да докажемо да важе обе неједнакости.
Докажимо да је $1 < \sqrt{2}$. Знамо да важи $1 < 2$. Корена функција $f(x) = \sqrt{x}$ је растућа функција, па за бројеве 1 и 2 корен мањег броја, $\sqrt{1}$, је мањи од корена већег броја, $\sqrt{2}$, тј. $\sqrt{1} < \sqrt{2}$.
Сада докажимо да је $\sqrt{2} < 2$. Из $2 < 4$, опет користећи да је функција $f(x) = \sqrt{x}$ растућа, добијамо: $\sqrt{2} < \sqrt{4}$, тј. $\sqrt{2} < 2$.
Резултат спајања доказа $1 < \sqrt{2}$ и доказа $\sqrt{2} < 2$ је доказ тврђења: $1 < \sqrt{2}$ и $\sqrt{2} < 2$.

Одмах рецимо да је овим доказом описано природнодедукцијско правило увођења везника $\wedge$. Ако $1 < \sqrt{2}$ означимо са A, а $\sqrt{2} < 2$ означимо са B онда је задатак из Примера 1: доказати $A \wedge B$. У Примеру 1 смо тај задатак решили на следећи начин: направили смо доказ за A, направили смо доказ за B и закључили смо да та два доказа спојена, јесу доказ за $A \wedge B$.

Правило увођења везника $\wedge$

Ако су

$$\begin{array}{c} \mathrm{D}_1 \\ A \end{array} \quad \text{и} \quad \begin{array}{c} \mathrm{D}_2 \\ B \end{array}$$

докази редом за A и за B, онда је

$$\dfrac{\begin{array}{c} \mathrm{D}_1 \\ A \end{array} \qquad \begin{array}{c} \mathrm{D}_2 \\ B \end{array}}{A \wedge B}(\wedge U)$$

доказ за $A \wedge B$ и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D_1 и D_2.

Иако знамо само једно природнодедукцијско правило, можемо правити природнодедукцијске доказе. Навешћемо два природнодедукцијска доказа у којима ћемо представити неке карактеристике таквих доказа.

Пример 2 Нека су и доказ D_1 и доказ D_2 из дефиниције правила $(\wedge U)$ само формула A, онда правилом $(\wedge U)$ добијамо доказ

$$\dfrac{\begin{array}{cc}A & A\end{array}}{A \wedge A}\wedge U$$

за формулу $A \wedge A$. Формуле A које се појављују у овом доказу су хипотезе тог доказа и рећи ћемо да је то доказ из скупа хипотеза $\{A\}$. Приметимо да, пошто говоримо о скупу хипотеза, не наводимо двапут хипотезу A, већ само једанпут.

Истакнимо да у прављењу сложенијег доказа можемо користити један исти доказ више пута. У прављењу доказа за $A \wedge A$ у Примеру 2 два пута је коришћен доказ кога чини сама формула A, и морао је бити наведен два пута. Већ смо поменули да постоје нека правила извођења природне дедукције (на пример, увођење $\Rightarrow$, елиминација $\vee$, увођење $\neg$) са следећом особином: када се у доказу примени једно од тих правила, онда се неке од постојећих хипотеза бришу, тј. приликом примене тог правила неке хипотезе у том доказу буду прецртане. Зато у сваком доказу разликујемо прецртане и непрецртане хипотезе тог доказа. Непрецртана хипотеза доказа из Примера 2 је формула A. Погледајмо још један пример.

Пример 3 Нека су докази D_1, D_2 и D_3 редом формуле A, B и C, онда правимо доказ:

$$\dfrac{\dfrac{\begin{array}{cc}A & B\end{array}}{A \wedge B}\wedge U \qquad \begin{array}{c}C\end{array}}{(A \wedge B) \wedge C}\wedge U$$

Непрецртане хипотезе доказа D_1, D_2 и D_3 су редом A, B и C, па је $\{A, B, C\}$ скуп непрецртаних хипотеза овог доказа.

Представимо сада правило елиминације везника $\wedge$. То правило се заснива на следећем исправном закључивању: ако постоји доказ D за формулу $A \wedge B$, онда је могуће доказати и само формулу A и само формулу B.

Правило елиминације везника $\wedge$

Ако је

$$\begin{array}{c}\mathrm{D}\\ A \wedge B\end{array}$$

доказ за $A \wedge B$, онда су

$$\dfrac{\begin{array}{c}\mathrm{D}\\ A \wedge B\end{array}}{A}(\wedge E_1) \qquad \dfrac{\begin{array}{c}\mathrm{D}\\ A \wedge B\end{array}}{B}(\wedge E_2)$$

докази редом за A и за B и непрецртане хипотезе оба та доказа су непрецртане хипотезе доказа D.

2. Правила увођења и елиминације везника $\Rightarrow$

Представимо и правила увођења и елиминације везника $\Rightarrow$. То представљање почнимо једним примером.

Пример 4 Докажимо да важи особина:
ако је x реалан број, онда је $x^2 + 2x \geq -1$.

Претпоставимо да је x реалан број. Стога је и $x+1$ реалан број. За сваки реалан број важи да је његов квадрат већи од нуле или једнак нули. Зато је $(x+1)^2 \geq 0$, тј. $x^2+2x+1 \geq 0$. Одузимањем јединице са обе стране неједнакости добијамо: $x^2 + 2x \geq -1$. Дакле, важи тврђење: *ако је x реалан број, онда је* $x^2+2x \geq -1$. Приметимо да овај доказ можемо посматрати као један главни доказ у оквиру кога се налази још један, мањи доказ. Мањи доказ има хипотезу *x је реалан број* и закључује: $x^2 + 2x \geq -1$. У главном доказу користи се тај мањи доказ и добија се: *ако је x реалан број, онда је* $x^2 + 2x \geq -1$, и *x је реалан број* није хипотеза главног доказа.

Ако у овом нашем примеру *x је реалан број* означимо са A, а $x^2+2x \geq -1$ са B, онда мали доказ доказује B из хипотезе A и он се користи у главном доказу, који је доказ за $A \Rightarrow B$, а који нема хипотезу A. Ово је опис правила увођења везника $\Rightarrow$.

Правило увођења везника $\Rightarrow$

Ако је

$$\begin{array}{c} \\ \mathrm{D} \\ B \end{array}$$

доказ за B и A је нека формула, онда је

$$\frac{\begin{array}{c} \not{A} \\ \mathrm{D} \\ B \end{array}}{A \Rightarrow B}(\Rightarrow U)$$

доказ за $A \Rightarrow B$ и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D, осим можда A.

Прво рецимо да у доказу D формуле B не мора да постоји хипотеза A.

Ознака $\not{A}$ значи да је хипотеза A, ако она постоји, искоришћена, тј. прецртана, и формула A није хипотеза доказа формуле $A \Rightarrow B$. Појаснимо шта у наведеној дефиницији значи: осим можда A. Приликом једне примене правила $(\Rightarrow U)$ можемо прецртати једну или неколико хипотеза A, али можемо и да не прецртамо ниједну хипотезу A и да, без обзира на то колико смо хипотеза A прецртали правилом $(\Rightarrow U)$, закључимо формулу $A \Rightarrow B$. Сада ћемо навести неколико доказа у којима се појављује правило $(\Rightarrow U)$. У првом доказу ћемо представити једну примену правила $(\Rightarrow U)$

која нема прецртане хипотезе и једну примену правила $(\Rightarrow U)$ која има прецртане хипотезе. Ево тог доказа:

$$\dfrac{\dfrac{\not{B}^{1}}{A \Rightarrow B} \Rightarrow U}{B \Rightarrow (A \Rightarrow B)} 1 \Rightarrow U$$

Рецимо да у доказу природне дедукције истим природним бројем n повезујемо све формуле, које су прецртане хипотезе ($\not{A}^{n}$), са правилом ρ чијом применом су те хипотезе прецртане ($n\rho$). У нашем доказу прво правило $(\Rightarrow U)$ нема прецртаних хипотеза A и његов закључак је $A \Rightarrow B$. Део тог доказа који се завршава формулом $A \Rightarrow B$ има једну непрецртану хипотезу B. Затим се тај доказ наставља другим правилом $(\Rightarrow U)$ које има једну прецртану хипотезу, формулу B, и то правило је са прецртаном хипотезом повезано бројем 1. Дакле, цео наш доказ нема непрецртаних хипотеза. У наредном доказу представићемо још једну могућност коју пружа правило $(\Rightarrow U)$. Посматрајмо доказ:

$$\dfrac{\dfrac{\not{A}^{1}}{A \Rightarrow A} \Rightarrow U}{A \Rightarrow (A \Rightarrow A)} 1 \Rightarrow U$$

Применом првог правила $(\Rightarrow U)$ нисмо прецртали ниједну хипотезу A, мада таква хипотеза постоји. Њу смо као прецртану хипотезу искористили у другом правилу $(\Rightarrow U)$. Приметимо да смо у овом доказу могли да бирамо у коме од два правила $(\Rightarrow U)$ ћемо искористити формулу A као хипотезу, док оно друго правило онда нема прецртаних хипотеза, тј. постоји и следећи доказ формуле $A \Rightarrow (A \Rightarrow A)$:

$$\dfrac{\dfrac{\not{A}^{1}}{A \Rightarrow A} 1 \Rightarrow U}{A \Rightarrow (A \Rightarrow A)} \Rightarrow U$$

Сада је на реду правило елиминације везника $\Rightarrow$ које смо већ поминьали.

Правило елиминације везника $\Rightarrow$

Ако су

$$\begin{array}{ccc} \mathrm{D}_1 & & \mathrm{D}_2 \\ A \Rightarrow B & \text{и} & A \end{array}$$

докази редом за $A \Rightarrow B$ и за A, онда је

$$\dfrac{\begin{array}{cc} \mathrm{D}_1 & \mathrm{D}_2 \\ A \Rightarrow B & A \end{array}}{B} (\Rightarrow E)$$

доказ за B и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D_1 и D_2.

Ево једног доказа природне дедукције у коме се користе само правила увођења и елиминације везника $\Rightarrow$:

$$\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow (\cancel{A}^{2} \Rightarrow B) \qquad \cancel{A}^{1}}{A \Rightarrow B} \Rightarrow E \qquad \cancel{A}^{1}}{B} \Rightarrow E}{A \Rightarrow B} 1 \Rightarrow U}{(A \Rightarrow (A \Rightarrow B)) \Rightarrow (A \Rightarrow B)} 2 \Rightarrow U$$

Овај доказ формуле $(A \Rightarrow (A \Rightarrow B)) \Rightarrow (A \Rightarrow B)$ нема непрецртаних хипотеза. Две хипотезе, две формуле A, прецртане су применом првог правила $(\Rightarrow U)$ и њих са тим правилом повезује број 1. Друго правило $(\Rightarrow U)$ има само једну прецртану хипотезу, формулу $A \Rightarrow (A \Rightarrow B)$, и то правило је са прецртаном хипотезом повезано бројем 2.
Сада, знајући четири правила извођења, можемо правити и сложеније природнодедукцијске доказе.

Задатак 1 Направимо доказ без непрецртаних хипотеза за формулу $(A \wedge B) \Rightarrow (B \wedge A)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{A \wedge \cancel{B}^{1}}{B} \wedge E_2 \qquad \dfrac{A \wedge \cancel{B}^{1}}{A} \wedge E_1}{B \wedge A} \wedge U}{(A \wedge B) \Rightarrow (B \wedge A)} 1 \Rightarrow U$$

Аналогно овом доказу, може се направити доказ без непрецртаних хипотеза за формулу $(B \wedge A) \Rightarrow (A \wedge B)$.

Задатак 2 Направимо доказ без непрецртаних хипотеза за формулу $(A \wedge (B \wedge C)) \Rightarrow ((A \wedge B) \wedge C)$.

$$\dfrac{\dfrac{\dfrac{A \wedge (\cancel{B}^{1} \wedge C)}{A} \wedge E_1 \qquad \dfrac{\dfrac{A \wedge (\cancel{B}^{1} \wedge C)}{B \wedge C} \wedge E_2}{B} \wedge E_1}{A \wedge B} \wedge U \qquad \dfrac{\dfrac{A \wedge (\cancel{B}^{1} \wedge C)}{B \wedge C} \wedge E_2}{C} \wedge E_2}{(A \wedge B) \wedge C} \wedge U$$
$$\dfrac{}{(A \wedge (B \wedge C)) \Rightarrow ((A \wedge B) \wedge C)} 1 \Rightarrow U$$

Аналогно овом доказу, може се направити доказ без непрецртаних хипотеза за формулу $((A \wedge B) \wedge C) \Rightarrow (A \wedge (B \wedge C))$.

3. Правила увођења и елиминације везника $\vee$

Прво ћемо представити правило увођења везника $\vee$. Ако постоји доказ за A, онда наравно постоји доказ за $A \vee B$, и исто тако, ако постоји доказ за B, онда постоји доказ за $A \vee B$. То расуђивање представљено је правилом увођења везника $\vee$.

Правило увођења везника $\vee$

Ако су

$$\begin{array}{cc} \mathrm{D}_1 & \mathrm{D}_2 \\ A & B \end{array}$$

докази редом за A и за B, онда су

$$\begin{array}{cc} \mathrm{D}_1 & \mathrm{D}_2 \\ \dfrac{A}{A \vee B}\ (\vee U_1) & \dfrac{B}{A \vee B}\ (\vee U_2) \end{array}$$

два доказа за $A \vee B$ и непрецртане хипотезе тих доказа су редом непрецртане хипотезе доказа D_1 и D_2.

Правило елиминације $\vee$ ћемо објаснити доказом у следећем примеру.

Пример 5 Докажимо да важи особина:
за сваки реалан број x различит од нуле важи: $\frac{x^2-2|x|+1}{|x|} \geq 0$.

Претпоставимо да је x реалан број различит од нуле. То значи да за реалан број x важи: $x > 0$ или $x < 0$ (у ствари важи или $x > 0$ или $x < 0$ али та прецизност нам за овај пример није корисна). Зато ћемо у доказу ове особине посматрати два случаја, када је $x > 0$ и када је $x < 0$.
Први случај: претпоставимо да је $x > 0$. Тада је $|x| = x$, па имамо $x^2 - 2|x| + 1 = x^2 - 2 \cdot x + 1 = (x-1)^2 \geq 0$. Дакле, из $x^2 - 2|x| + 1 \geq 0$ и $|x| > 0$ добијамо: $\frac{x^2-2|x|+1}{|x|} \geq 0$.
Други случај: претпоставимо да је $x < 0$. Тада је $|x| = -x$, па имамо $x^2 - 2|x| + 1 = x^2 - 2 \cdot (-x) + 1 = (x+1)^2 \geq 0$. Дакле, из $|x| > 0$ и $x^2 - 2|x| + 1 \geq 0$ добијамо: $\frac{x^2-2|x|+1}{|x|} \geq 0$.
Пошто у оба случаја важи $\frac{x^2-2|x|+1}{|x|} \geq 0$, закључујемо да та особина важи за сваки реалан број x различит од нуле.

Начин размишљања који је коришћен у доказу из Примера 5 је у духу правила елиминације везника $\vee$. Наиме, ако имамо доказ за формулу $A \vee B$ и ако постоје два доказа, такви да се можда међу хипотезама једног од њих налази формула A, а међу хипотезама другог налази формула B и оба имају исти закључак C, онда спајајући та три доказа можемо закључити C. Ево правила елиминације везника $\vee$.

Правило елиминације везника $\vee$

Ако су

$$\begin{array}{ccc} \mathrm{D}_1 & \mathrm{D}_2 & \qquad\qquad \mathrm{D}_3 \\ A \vee B & C & \text{и} \qquad\qquad C \end{array}$$

докази редом за $A \vee B$ и два доказа за C, онда је

$$\dfrac{\begin{array}{ccc} & \not{A} & \not{B} \\ \mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 \\ A \vee B & C & C \end{array}}{C}(\vee E)$$

један доказ за C и непрецртане хипотезе тог доказа су: непрецртане хипотезе доказа D_1, непрецртане хипотезе доказа D_2, осим можда A, и непрецртане хипотезе доказа D_3, осим можда B.

Применом овог правила (као и правила увођења везника $\Rightarrow$) можемо прецртати неке хипотезе. Наиме, ако докази D_2 и D_3 имају редом хипотезе A и B, онда те хипотезе могу бити прецртане применом правила $(\vee E)$. Истакнимо да једном применом овог правила можемо прецртати ниједну, једну или неколико хипотеза A и B.
Сада знамо правила извођења природне дедукције за везнике $\wedge$, $\Rightarrow$ и $\vee$, па наводимо један природнодедукцијски доказ у коме се користе та правила.

Задатак 3 Направимо доказ без непрецртаних хипотеза за формулу $((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))$.

$$\dfrac{\dfrac{(A \vee \not{B}) \vee \not{C}^{\,3} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\not{A}^{\,1}}{A \vee (B \vee C)} \vee U_1 \quad \dfrac{\dfrac{\not{B}^{\,1}}{B \vee C} \vee U_1}{A \vee (B \vee C)} \vee U_2}{A \vee (B \vee C)} 1 \vee E \quad \dfrac{\dfrac{\not{C}^{\,2}}{B \vee C} \vee U_2}{A \vee (B \vee C)} \vee U_2}{A \vee (B \vee C)} 2 \vee E}{((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))} 3 \Rightarrow U$$

Аналогно овом доказу, може се направити доказ без непрецртаних хипотеза за формулу $(A \vee (B \vee C)) \Rightarrow ((A \vee B) \vee C)$.

4. Правило елиминације везника $\bot$

Из наше базе везника исказне логике $\{\wedge, \vee, \Rightarrow, \bot\}$ остаје нам још да представимо правила извођења за везник $\bot$. За тај везник постоји само једно правило извођења, правило елиминације везника $\bot$.

Правило елиминације везника $\bot$

Ако је

$$\begin{array}{c} \mathrm{D} \\ \bot \end{array}$$

доказ за $\bot$, онда је

$$\dfrac{\begin{array}{c} \mathrm{D} \\ \bot \end{array}}{A}(\bot E)$$

доказ за A, где је A произвољна формула.

Дакле, овим правилом из $\bot$ закључујемо произвољну формулу A.

5. Правила увођења и елиминације везника $\Leftrightarrow$

Осим за везнике базе $\{\wedge, \vee, \Rightarrow, \bot\}$ у природној дедукцији постоје правила увођења и елиминације за остале логичке везнике. Сетимо се дефиниције да је $A \Leftrightarrow B$ замена за $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Зато ће правила увођења и елиминације за $\Leftrightarrow$ бити редом увођење и елиминација за $\wedge$ када је A баш $A \Rightarrow B$, а B баш $B \Rightarrow A$. Погледајмо следећи једноставан пример.

Пример 6 Доказати: $x = 2$ ако и само ако $x - 2 = 0$.
Доказ се састоји од два дела.
Доказ с лева на десно: ако је $x = 2$, онда је $x - 2 = 2 - 2 = 0$, тј. важи $x - 2 = 0$.
Доказ с десна на лево: ако је $x - 2 = 0$, онда, додавањем 2 са обе стране једнакости, добијамо: $x - 2 + 2 = 0 + 2$, тј. $x = 2$.

Правило увођења везника $\Leftrightarrow$ је представљено доказом у Примеру 6.

Правило увођења везника $\Leftrightarrow$
Ако су

$$\begin{array}{c}\mathrm{D}_1\\ A \Rightarrow B\end{array} \quad \text{и} \quad \begin{array}{c}\mathrm{D}_2\\ B \Rightarrow A\end{array}$$

докази редом за $A \Rightarrow B$ и за $B \Rightarrow A$, онда је

$$\dfrac{\begin{array}{c}\mathrm{D}_1\\ A \Rightarrow B\end{array} \qquad \begin{array}{c}\mathrm{D}_2\\ B \Rightarrow A\end{array}}{A \Leftrightarrow B}(\Leftrightarrow U)$$

доказ за $A \Leftrightarrow B$ и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D_1 и D_2.

А ево и правила елиминације везника $\Leftrightarrow$.

Правило елиминације везника $\Leftrightarrow$
Ако је

$$\begin{array}{c}\mathrm{D}\\ A \Leftrightarrow B\end{array}$$

доказ за $A \Leftrightarrow B$, онда су

$$\dfrac{\begin{array}{c}\mathrm{D}\\ A \Leftrightarrow B\end{array}}{A \Rightarrow B}(\Leftrightarrow E_1) \qquad \dfrac{\begin{array}{c}\mathrm{D}\\ A \Leftrightarrow B\end{array}}{B \Rightarrow A}(\Leftrightarrow E_2)$$

докази редом за $A \Rightarrow B$ и за $B \Rightarrow A$ и непрецртане хипотезе тих доказа су непрецртане хипотезе доказа D.

Користећи доказе из Задатака 1-3 и правило увођења везника $\Leftrightarrow$, направићемо доказ без непрецртаних хипотеза за формуле:

$$(A \wedge B) \Leftrightarrow (B \wedge A)$$
$$((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$$
$$((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C)).$$

Задатак 4 Доказ за $(A \wedge B) \Rightarrow (B \wedge A)$ из Задатка 1 означимо са D_1 и доказ за $(B \wedge A) \Rightarrow (A \wedge B)$ (за који смо рекли да је аналоган доказу D_1) означимо са D_2. Користећи доказе D_1 и D_2 и правило $(\Leftrightarrow U)$, добијамо следећи природнодедукцијски доказ:

$$\dfrac{\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2 \\ (A \wedge B) \Rightarrow (B \wedge A) & (B \wedge A) \Rightarrow (A \wedge B)\end{array}}{(A \wedge B) \Leftrightarrow (B \wedge A)} \Leftrightarrow U$$

Како докази D_1 и D_2 немају непрецртаних хипотеза, то и овај доказ нема непрецртаних хипотеза.

Доказ за $(A \wedge (B \wedge C)) \Rightarrow ((A \wedge B) \wedge C)$ из Задатка 2 означимо са D_3 и доказ за $((A \wedge B) \wedge C) \Rightarrow (A \wedge (B \wedge C))$ (за који смо рекли да је аналоган доказу D_3) означимо са D_4. Користећи доказе D_3 и D_4 и правило $(\Leftrightarrow U)$, добијамо природнодедукцијски доказ:

$$\dfrac{\begin{array}{cc}\mathrm{D}_4 & \mathrm{D}_3 \\ ((A \wedge B) \wedge C) \Rightarrow (A \wedge (B \wedge C)) & (A \wedge (B \wedge C)) \Rightarrow ((A \wedge B) \wedge C)\end{array}}{((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))} \Leftrightarrow U$$

Како докази D_3 и D_4 немају непрецртаних хипотеза, то и овај доказ нема непрецртаних хипотеза.

На потпуно исти начин, користећи доказе из Задатка 3 и правило увођења везника $\Leftrightarrow$, прави се доказ без непрецртаних хипотеза за формулу $((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$.

6. Правила увођења и елиминације везника $\neg$

Питамо се како можемо користити негацију у процесима закључивања? Сетимо се да смо негацију дефинисали помоћу везника $\Rightarrow$ и $\bot$ на следећи начин: $\neg A$ је замена за $A \Rightarrow \bot$. Сликовито речено, када хоћемо да кажемо да нешто није тачно (да *није* A) кажемо да ако то важи, онда следи нека општепозната неистина (да *ако* A, *онда* $\bot$). Ево примера: општепознато је да је $0 = 1$ неистина. Зато је реченицом: *ако је* $\sqrt{2}$ *природан број, онда је* $0 = 1$ на другачији начин саопштена особина: $\sqrt{2}$ *није природан број.* Овај начин закључивања је представљен у правилу увођења $\neg$.

Правило увођења везника $\neg$

Ако је

$$\begin{array}{c}\mathrm{D} \\ \bot\end{array}$$

доказ за $\bot$ и A је нека формула, онда је

$$\dfrac{\begin{array}{c}\not{A} \\ \mathrm{D} \\ \bot\end{array}}{\neg A}(\neg U)$$

доказ за $\neg A$ и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D, осим можда A.

И за ово правило важи да доказ D не мора да има хипотезе A и да једном применом овог правила можемо прецртати ниједну, једну или неколико хипотеза A. Рецимо да се ово правило, правило увођења везника $\neg$, назива и правило свођења на противречност (reductio ad absurdum). Приметимо да ако у правилу увођења везника $\neg$ формулу $\neg A$ заменимо са $A \Rightarrow \bot$, онда добијамо правило увођења $\Rightarrow$ када је формула B баш $\bot$:

$$\dfrac{\begin{array}{c}\not{A}\\ \mathrm{D}\\ \bot\end{array}}{A \Rightarrow \bot} \Rightarrow U$$

Исто тако, правило елиминације везника $\neg$ ће бити у ствари правило елиминације везника $\Rightarrow$ када је формула B баш $\bot$:

$$\dfrac{\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2\\ A \Rightarrow \bot & A\end{array}}{\bot} \Rightarrow E$$

Ево правила елиминације везника $\neg$.

Правило елиминације везника $\neg$

Ако су

$$\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2\\ A & \neg A\end{array}$$

доказ редом за A и за $\neg A$, онда је

$$\dfrac{\begin{array}{cc}\mathrm{D}_1 & \mathrm{D}_2\\ A & \neg A\end{array}}{\bot}(\neg E)$$

доказ за $\bot$ и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D_1 и D_2.

Сада смо дефинисали правила природне дедукције за све везнике, па направимо још неки природнодедукцијски доказ.

Задатак 5 Направимо доказ без непрецртаних хипотеза за тautологију $(\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$ (Де Морганов закон). Прво направимо доказ за формулу $(\neg(A \vee B)) \Rightarrow (\neg A \wedge \neg B)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\not{A}^{1}}{A \vee B} \vee U_1 \quad \neg(A \vee B)^{3}}{\bot} \neg E}{\neg A} 1\neg U \quad \dfrac{\dfrac{\dfrac{\not{B}^{2}}{A \vee B} \vee U_2 \quad \neg(A \vee B)^{3}}{\bot} \neg E}{\neg B} 2\neg U}{\neg A \wedge \neg B} \wedge U}{(\neg(A \vee B)) \Rightarrow (\neg A \wedge \neg B)} 3 \Rightarrow U$$

Ево сада доказа за формулу $(\neg A \wedge \neg B) \Rightarrow (\neg(A \vee B))$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\not{A}^{1} \quad \dfrac{\neg A \not\wedge \neg B^{3}}{\neg A} \wedge E_1}{\bot}\neg E \quad \dfrac{\not{B}^{1} \quad \dfrac{\neg A \not\wedge \neg B^{3}}{\neg B} \wedge E_2}{\bot}\neg E}{\bot}1 \vee E \quad A \not\vee B^{2}}{\bot}2\neg U}{\neg(A \vee B)}}{(\neg A \wedge \neg B) \Rightarrow (\neg(A \vee B))}3 \Rightarrow U$$

Ако доказ за формулу $(\neg(A \vee B)) \Rightarrow (\neg A \wedge \neg B)$ означимо са D_1, а доказ за формулу $(\neg A \wedge \neg B) \Rightarrow (\neg(A \vee B))$ означимо са D_2, онда добијамо следећи природнодедукцијски доказ:

$$\dfrac{\begin{matrix}\mathrm{D}_1 \\ (\neg(A \vee B)) \Rightarrow (\neg A \wedge \neg B)\end{matrix} \qquad \begin{matrix}\mathrm{D}_2 \\ (\neg A \wedge \neg B) \Rightarrow (\neg(A \vee B))\end{matrix}}{(\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)} \Leftrightarrow U$$

који је доказ за формулу $(\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$ без непрецртаних хипотеза.

Аналогно овом доказу, може се направити доказ без непрецртаних хипотеза за таутологију $(\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$.

7. Персово правило

Формални систем природне дедукције који представља исказну логику, осим правила увођења и елиминације за логичке везнике, има још једно правило извођења, Персово правило.

Персово правило

Ако је

$$\begin{matrix} A \Rightarrow B \\ \mathrm{D} \\ A \end{matrix}$$

доказ за A, онда је

$$\dfrac{\begin{matrix} A \not\Rightarrow B \\ \mathrm{D} \end{matrix}}{A}(Pers)$$

доказ за A и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D осим формуле $A \Rightarrow B$.

Истакнимо да за Персово правило важи да хипотезе $A \Rightarrow B$ не морају постојати. У тим случајевима Персово правило је тривијално, тј. из $\begin{matrix}\mathrm{D} \\ A\end{matrix}$ доказа A закључујемо опет A.

Дакле, представили смо сва правила извођења система природне дедукције за исказну логику. На крају представимо још једно правило које је, сликовито речено, исте јачине као Персово правило, правило јаког свођења

на противречност. Наиме, важи да ако скупу кога чине правила извођења за логичке везнике додамо било које од та два правила добићемо исти формални систем, формални систем исказне логике.

Правило јаког свођења на противречност (јака reductio ad absurdum)

Ако је

$$\begin{array}{c}\neg A\\ \mathrm{D}\\ \bot\end{array}$$

доказ за $\bot$, онда је

$$\dfrac{\begin{array}{c}\not{\neg A}\\ \mathrm{D}\\ \bot\end{array}}{A}(RAA)$$

доказ за A и непрецртане хипотезе тог доказа су непрецртане хипотезе доказа D осим формуле $\neg A$.

И за ово правило важи да хипотезе $\neg A$ не морају да постоје. У тим случајевима правило јаког свођења на противречност је правило $(\bot E)$. А сада покажимо да су Персово правило и правило RAA исте јачине, или друкчије речено, да су међусобно еквивалентна.

Задатак 6 Персово правило и RAA су међусобно еквивалентна правила.

Имамо доказ $\begin{array}{c}A \Rightarrow B\\ \mathrm{D}\\ A\end{array}$. Применом Персовог правила на последњу формулу овог доказа, формулу A, добили бисмо као закључак формулу A и формула $A \Rightarrow B$ би била прецртана хипотеза. Ми имамо на располагању правила извођења за све везнике и правило RAA и морамо да направимо доказ са истим закључком и са истим скупом непрецртаних хипотеза као да смо на доказ D применили Персово правило. Ево тог доказа:

$$\dfrac{\dfrac{\dfrac{\dfrac{\not{A}^{1} \qquad \not{\neg A}^{2}}{\bot}\,\neg E}{B}\,\bot E}{A \Rightarrow B}\,1 \Rightarrow U \qquad \begin{array}{c}\mathrm{D}\\ A\end{array} \qquad \not{\neg A}^{2}}{\dfrac{\bot}{A}\,2RAA}\,\neg E$$

Дакле, овај доказ је замена за Персово правило. Кажемо да смо Персово правило извели из правила RAA зато што су остала правила извођења стално ту, њих увек имамо на располагању. Остаје да правило RAA изведемо из Персовог правила. Имамо

$$\begin{array}{c}\neg A\\ \mathrm{D}\\ \bot\end{array}$$

доказ $\bot$. Применом правила RAA на последњу формулу овог доказа, формулу $\bot$, добили бисмо формулу A и формула $\neg A$ би била прецртана хипотеза. Ми формулу $\neg A$ замењујемо са $A \Rightarrow \bot$, имамо на располагању тај доказ, сва правила извођења за логичке везнике и Персово правило и правимо доказ са истим закључком и са истим скупом непрецртаних хипотеза као да смо на доказ D применили правило RAA:

$$\dfrac{\dfrac{\begin{array}{c}\not{A \Rightarrow \bot}^{1}\\ \mathrm{D}\\ \bot\end{array}}{A}\,\bot E}{A}\,1Pers$$

На тај начин смо показали да се правило RAA може извести из Персовог правила.

Дакле, из Задатка 6 следи да су Персово правило и правило јаког свођења на противречност међусобно еквивалентна правила, тј. ако скупу који чине правила извођења за све логичке везнике додамо било које од та два правила добијамо исти формални систем (формални систем исказне логике).
На крају овог одељка представимо доказ за формулу $A \vee \neg A$ у коме се користи правило јаког свођења на противречност. Јасно је, на основу Задатка 6, да се може направити доказ за ту формулу у коме се користи Персово правило.

Задатак 7 За формулу $A \vee \neg A$ постоји доказ без непрецртаних хипотеза.
Ево једног таквог доказа:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\not{\neg A}^{1}}{A \vee \neg A}\vee U_2 \qquad \neg(A \vee \not{\neg A}^{2})}{\bot}\neg E}{A}\,1RAA}{A \vee \neg A}\vee U_1 \qquad \neg(A \vee \not{\neg A}^{2})}{\bot}\neg E}{A \vee \neg A}\,2RAA$$

3.2.2 Природна дедукција, систем $\mathcal{N}$

Сада ћемо дефинисати један формални систем природне дедукције, формални систем $\mathcal{N}$. Као и сваки формални систем и систем $\mathcal{N}$ потпуно је одређен са своја четири дела: скупом основних симбола $\mathcal{S}(\mathcal{N})$, скупом исказних формула $\mathcal{F}(\mathcal{N})$, скупом аксиома $\mathcal{A}(\mathcal{N})$ и скупом правила извођења $\mathcal{R}(\mathcal{N})$. Скуп основних

симбола система $\mathcal{N}$, скуп $\mathcal{S}(\mathcal{N})$, јесте алфабет исказне логике дефинисан у одељку 2.1.1 са додатим помоћним симболом $\vdash$.

Скуп основних симбола система $\mathcal{N}$, скуп $\mathcal{S}(\mathcal{N})$

Скуп основних симбола система $\mathcal{N}$, скуп $\mathcal{S}(\mathcal{N})$, састоји се од следећа три скупа:
$\diamond$ пребројивог скупа исказих слова, скупа $\mathcal{P}$, чији елементи су p_0, q_0, r_0, p_1, q_1, r_1,..., p_n, q_n, r_n,...;
$\diamond$ скупа логичких везника $\{\wedge, \vee, \Rightarrow, \bot\}$, где су $\wedge, \vee$ и $\Rightarrow$ бинарни везници, а $\bot$ нуларни везник;
$\diamond$ скупа помоћних симбола $\{(,), \vdash\}$.

Исказне формуле система $\mathcal{N}$ су исказне формуле дефинисане у одељку 2.1.2, али ипак поновимо њихову дефиницију.

Дефиниција исказне формуле система $\mathcal{N}$

(1) Исказна слова и везник $\bot$ су исказне формуле система $\mathcal{N}$.
(2) Ако су A и B исказне формуле система $\mathcal{N}$, онда су и $(A \wedge B)$, $(A \vee B)$ и $(A \Rightarrow B)$ исказне формуле тог система.

Везници $\Leftrightarrow$, $\neg$ и $\top$ су дефинисани као у одељку 2.1.2.
И у систему $\mathcal{N}$ поштујемо договор да при писању исказних формула изостављамо сасвим спољашње заграде.

Скуп формула система $\mathcal{N}$, скуп $\mathcal{F}(\mathcal{N})$

Скуп формула система $\mathcal{N}$, скуп $\mathcal{F}(\mathcal{N})$, чине исказне формуле тог система $\mathcal{N}$.

Коначне скупове исказних формула означаваћемо са Γ, Δ, Λ,..., Γ_1, Δ_1, Λ_1,..., Γ', Δ', Λ',... За дефинисање скупа аксиома и скупа правила извођења система $\mathcal{N}$, скупова $\mathcal{A}(\mathcal{N})$ и $\mathcal{R}(\mathcal{N})$, користићемо секвенте, које правимо од елемената скупа симбола $\mathcal{S}(\mathcal{N})$. Секвент је израз следећег облика: $\Gamma \vdash A$, где је Γ коначан скуп формула који може бити и празан скуп. За коначан скуп Γ, на пример $\Gamma = \{B, C, D\}$, писаћемо $B, C, D \vdash A$, а ако је Γ празан скуп, онда ћемо изостављати $\emptyset$ и писаћемо само $\vdash A$.

Важно је рећи да скуп аксиома система $\mathcal{N}$ неће чинити неке формуле, нити ће правила извођења бити релације између формула. У систему $\mathcal{N}$ ће, да тако кажемо, у главној улози бити секвенти. Ево трећег дела формалног система $\mathcal{N}$, скупа аксиома.

Скуп аксиома система $\mathcal{N}$, скуп $\mathcal{A}(\mathcal{N})$

Аксиоме система $\mathcal{N}$ су секвенти посебног облика. Тачније, аксиоматски секвент система $\mathcal{N}$ је облика

$A \vdash A$, где је A произвољна формула.

Аксиоматски секвент одговара аксиоматском правилу које смо представили у неформалном опису природне дедукције. Истакнимо да смо дефиницијом аксиоматског секвента $A \vdash A$ у ствари дали једну схему за прављење аксиоматских секвената, тако што на месту A може бити произвољна формула. На пример, секвенти $C \vdash C$, $A \Rightarrow C \vdash A \Rightarrow C$, $C \vee (A \wedge D) \vdash C \vee (A \wedge D)$ и $B \wedge D \vdash B \wedge D$ су аксиоматски секвенти.

Четврти део формалног система $\mathcal{N}$ је скуп правила извођења тог система. Та правила смо већ представили у неформалном опису природне дедукције као правила увођења и елиминације логичких везника.

Скуп правила извођења система $\mathcal{N}$, скуп $\mathcal{R}(\mathcal{N})$

Правила извођења у систему $\mathcal{N}$ ће бити релације између секвената. Скуп правила извођења система $\mathcal{N}$, скуп $\mathcal{R}(\mathcal{N})$, чине правило елиминације и правило увођења за сваки од бинарних везника $\wedge$, $\Rightarrow$ и $\vee$; правило елиминације за нуларни везник $\bot$; и Персово правило. Дакле, скуп $\mathcal{R}(\mathcal{N})$ чине следећа правила извођења:

правила елиминације

$$(\wedge E_1)\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad (\wedge E_2)\frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$(\Rightarrow E)\ \frac{\Gamma \vdash A \Rightarrow B \qquad \Delta \vdash A}{\Gamma \cup \Delta \vdash B}$$

$$(\vee E)\ \frac{\Gamma \vdash A \vee B \qquad \Delta_1 \vdash C \qquad \Theta_1 \vdash C}{\Gamma \cup \Delta \cup \Theta \vdash C}$$

$$(\bot E)\ \frac{\Gamma \vdash \bot}{\Gamma \vdash A}$$

правила увођења

$$(\wedge U)\ \frac{\Gamma \vdash A \qquad \Delta \vdash B}{\Gamma \cup \Delta \vdash A \wedge B}$$

$$(\Rightarrow U)\ \frac{\Gamma_1 \vdash B}{\Gamma \vdash A \Rightarrow B}$$

$$(\vee U_1)\ \frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \qquad (\vee U_2)\frac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$$

Персово правило

$$(Pers)\ \frac{\Gamma \cup \{A \Rightarrow B\} \vdash A}{\Gamma \vdash A}$$

У правилу $(\Rightarrow U)$ скуп Γ може бити скуп Γ_1 или скуп $\Gamma_1 \setminus \{A\}$. У правилу $(\vee E)$ скуп Δ може бити скуп Δ_1 или скуп $\Delta_1 \setminus \{A\}$, а скуп Θ може бити скуп Θ_1 или скуп $\Theta_1 \setminus \{B\}$.

Као и аксиоматске секвенте и правила извођења сматрамо схемама.

Напомена Приметимо да у систему $\mathcal{N}$ немамо правила извођења за везнике $\Leftrightarrow$ и $\neg$, али на основу веза између везника, та правила можемо извести из правила система $\mathcal{N}$.

Сада, пошто смо дефинисали сва четири дела формалног система $\mathcal{N}$, дефинишемо појам доказа у том систему. У систему $\mathcal{N}$ ћемо доказивати секвенте, тј. правићемо доказе за секвенте. Зато дефинишемо доказ у систему $\mathcal{N}$ као дрво које чине секвенти.

Дефиниција доказа секвента у систему $\mathcal{N}$

У систему $\mathcal{N}$ доказ секвента $\Gamma \vdash F$ је једно коначно дрво у чијем корену је баш тај секвент $\Gamma \vdash F$, на сваком листу је један аксиомат-

ски секвент, а свако гранање је оправдано неким правилом извођења система $\mathcal{N}$. (Приметимо да је доказ аксиоматског секвента дрво са једним чвором (корен и лист) у коме је сам тај секвент.)

Ако постоји доказ у чијем корену је секвент $\Gamma \vdash F$, онда кажемо да је секвент $\Gamma \vdash F$ доказив у систему $\mathcal{N}$. Неки доказ $\mathcal{D}$ секвента $\Gamma \vdash F$ записиваћемо $\begin{matrix}\mathcal{D}\\ \Gamma \vdash F\end{matrix}$.

Повежимо сада доказе у нашем неформалном опису природне дедукције из одељка 3.2.1 и доказе у систему $\mathcal{N}$. Доказ у неформалном опису природне дедукције у чијем је корену формула F, а све непрецртане хипотезе на листовима тог дрвета чине скуп Γ је доказ секвента $\Gamma \vdash F$. Доказ у неформалном опису природне дедукције који нема непрецртаних хипотеза, а у чијем корену је формула F је доказ секвента $\vdash F$. Правила извођења система $\mathcal{N}$ су правила извођења за везнике $\wedge$, $\Rightarrow$, $\vee$ и $\bot$ и Персово правило које смо представили у одељку 3.2.1, само записани другачије. На пример, правилу увођења везника $\Rightarrow$ из неформалног описа одговара правило $(\Rightarrow U)$ система $\mathcal{N}$. Наиме, у одељку 3.2.1 у правилу увођења везника $\Rightarrow$ имали смо доказ формуле B чији је скуп непрецртаних хипотеза скуп Γ_1, доказ $\begin{matrix}\mathrm{D}\\ B\end{matrix}$. У систему $\mathcal{N}$ то је доказ секвента $\Gamma_1 \vdash B$. Применом правила увођења везника $\Rightarrow$ на доказ D добијамо доказ формуле $A \Rightarrow B$, чији скуп непрецртаних хипотеза је скуп Γ_1, осим можда формуле A. То значи да скуп Γ_1 може али и не мора да садржи формулу A и више, да иако Γ_1 садржи формулу A та формула не мора да буде прецртана хипотеза применом правила увођења везника $\Rightarrow$. Све те могућности дате су и правилом $(\Rightarrow U)$ система $\mathcal{N}$. У систему $\mathcal{N}$ применом правила $(\Rightarrow U)$ на доказ секвента $\Gamma_1 \vdash B$ добијамо доказ секвента $\Gamma \vdash A \Rightarrow B$ и имамо:
(1) Ако скуп непрецртаних хипотеза Γ_1 доказа D садржи формулу A, онда имамо два случаја: ако A јесте прецртана хипотеза правила увођења везника $\Rightarrow$ добијамо доказ формуле $A \Rightarrow B$ са скупом непрецртаних хипотеза $\Gamma_1 \setminus \{A\}$, и то је у систему $\mathcal{N}$ доказ секвента $\Gamma \vdash A \Rightarrow B$ у коме је $\Gamma = \Gamma_1 \setminus \{A\}$; ако A није прецртана хипотеза правила увођења везника $\Rightarrow$, онда имамо доказ формуле $A \Rightarrow B$ са скупом непрецртаних хипотеза Γ_1, а у систему $\mathcal{N}$ је то доказ секвента $\Gamma \vdash A \Rightarrow B$ у коме је $\Gamma = \Gamma_1$.
(2) Ако скуп непрецртаних хипотеза Γ_1 доказа D не садржи формулу A, онда применом правила увођења везника $\Rightarrow$ добијамо доказ формуле $A \Rightarrow B$ са скупом непрецртаних хипотеза Γ_1, а у систему $\mathcal{N}$ то је опет доказ секвента $\Gamma \vdash A \Rightarrow B$ у коме је $\Gamma = \Gamma_1$.

Пример 7 Направимо доказ таутологије $(A \wedge (A \Rightarrow B)) \Rightarrow B$ (modus ponens) записујући га на неформални начин показан у одељку 3.2.1.

$$\dfrac{\dfrac{\dfrac{A \wedge (\cancel{A} \overset{1}{\Rightarrow} B)}{A \Rightarrow B}\wedge E_2 \qquad \dfrac{A \wedge (\cancel{A} \overset{1}{\Rightarrow} B)}{A}\wedge E_1}{B}\Rightarrow E}{(A \wedge (A \Rightarrow B)) \Rightarrow B}1 \Rightarrow U$$

Ово је доказ без непрецртаних хипотеза. А сада направимо доказ секвента $\vdash (A \wedge (A \Rightarrow B)) \Rightarrow B$ у систему $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{A \wedge (A \Rightarrow B) \vdash A \wedge (A \Rightarrow B)}{A \wedge (A \Rightarrow B) \vdash A \Rightarrow B} \wedge E_2 \qquad \dfrac{A \wedge (A \Rightarrow B) \vdash A \wedge (A \Rightarrow B)}{A \wedge (A \Rightarrow B) \vdash A} \wedge E_1}{A \wedge (A \Rightarrow B) \vdash B} \Rightarrow E}{\vdash (A \wedge (A \Rightarrow B)) \Rightarrow B} \Rightarrow U$$

На листовима су аксиоматски секвенти $A \wedge (A \Rightarrow B) \vdash A \wedge (A \Rightarrow B)$, а свако гранање је оправдано неким правилом извођења система $\mathcal{N}$. У корену је секвент $\vdash (A \wedge (A \Rightarrow B)) \Rightarrow B$, па кажемо да је тај секвент доказив у систему $\mathcal{N}$.

Наредна дефиниција ће нам рећи шта су то теореме система $\mathcal{N}$.

Дефиниција теореме система $\mathcal{N}$

Формула F је теорема система $\mathcal{N}$ АККО је секвент $\vdash F$ доказив у систему $\mathcal{N}$.

Дакле, таутологија modus ponens, $(A \wedge (A \Rightarrow B)) \Rightarrow B$, из Примера 7 је теорема система $\mathcal{N}$.

Пример 8 Користећи доказе из Задатака 1-5 и Задатка 7 из одељка 3.2.1 лако се у систему $\mathcal{N}$ могу направити докази за секвенте:

(1) $\vdash (A \wedge B) \Leftrightarrow (B \wedge A)$,

(2) $\vdash ((A \wedge B) \wedge C) \Leftrightarrow (A \wedge (B \wedge C))$

(3) $\vdash ((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$

(4) $\vdash (\neg(A \vee B)) \Leftrightarrow (\neg A \wedge \neg B)$

(5) $\vdash (\neg(A \wedge B)) \Leftrightarrow (\neg A \vee \neg B)$

(6) $\vdash A \vee \neg A$

На основу дефиниције теореме система $\mathcal{N}$ добијамо да су формуле у наведеним секвентима теореме система $\mathcal{N}$.

Приметимо да су теореме система $\mathcal{N}$ из Примера 7 и Примера 8 таутологије. У наредним задацима ћемо за још неколико таутологија (таутологије из Задатка 4 у одељку 2.2.3 и дистрибутивне законе) доказати да су теореме система $\mathcal{N}$.

Задатак 8 Формула $A \Rightarrow (B \Rightarrow A)$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{A \vdash A}{A \vdash B \Rightarrow A} \Rightarrow U}{\vdash A \Rightarrow (B \Rightarrow A)} \Rightarrow U$$

Задатак 9 Формула $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \Rightarrow (B \Rightarrow C) \vdash A \Rightarrow (B \Rightarrow C) \qquad A \vdash A}{A \Rightarrow (B \Rightarrow C), A \vdash B \Rightarrow C} \Rightarrow E \qquad \dfrac{A \Rightarrow B \vdash A \Rightarrow B \quad A \vdash A}{A \Rightarrow B, A \vdash B} \Rightarrow E}{A \Rightarrow (B \Rightarrow C), A \Rightarrow B, A \vdash C} \Rightarrow E}{A \Rightarrow (B \Rightarrow C), A \Rightarrow B \vdash A \Rightarrow C} \Rightarrow U}{A \Rightarrow (B \Rightarrow C) \vdash (A \Rightarrow B) \Rightarrow (A \Rightarrow C)} \Rightarrow U}{\vdash (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))} \Rightarrow U$$

Задатак 10 Формула $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{(A \Rightarrow B) \Rightarrow A \vdash (A \Rightarrow B) \Rightarrow A \qquad A \Rightarrow B \vdash A \Rightarrow B}{(A \Rightarrow B) \Rightarrow A, A \Rightarrow B \vdash A} \Rightarrow E}{(A \Rightarrow B) \Rightarrow A \vdash A} Pers}{\vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A} \Rightarrow U$$

Задатак 11 Формула $A \Rightarrow (B \Rightarrow (A \wedge B))$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{A \vdash A \qquad B \vdash B}{A, B \vdash A \wedge B} \wedge U}{A \vdash B \Rightarrow (A \wedge B)} \Rightarrow U}{\vdash A \Rightarrow (B \Rightarrow (A \wedge B))} \Rightarrow U$$

Задатак 12 Формуле $(A \wedge B) \Rightarrow A$ и $(A \wedge B) \Rightarrow B$ су теореме система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash A} \wedge E_1}{\vdash (A \wedge B) \Rightarrow A} \Rightarrow U \qquad \dfrac{\dfrac{\dfrac{A \wedge B \vdash A \wedge B}{A \wedge B \vdash B} \wedge E_2}{\vdash (A \wedge B) \Rightarrow B} \Rightarrow U$$

Задатак 13 Формуле $A \Rightarrow (A \vee B)$ и $B \Rightarrow (A \vee B)$ су теореме система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash A \vee B} \vee U_1}{\vdash A \Rightarrow (A \vee B)} \Rightarrow U \qquad \dfrac{\dfrac{\dfrac{B \vdash B}{B \vdash A \vee B} \vee U_2}{\vdash B \Rightarrow (A \vee B)} \Rightarrow U$$

Задатак 14 Формула $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{A \vee B \vdash A \vee B \qquad \dfrac{B \Rightarrow C \vdash B \Rightarrow C \quad B \vdash B}{B, B \Rightarrow C \vdash C} \Rightarrow E \quad \dfrac{A \Rightarrow C \vdash A \Rightarrow C \quad A \vdash A}{A, A \Rightarrow C \vdash C} \Rightarrow E}{A \Rightarrow C, B \Rightarrow C, A \vee B \vdash C} \vee E}{A \Rightarrow C, B \Rightarrow C \vdash (A \vee B) \Rightarrow C} \Rightarrow U}{A \Rightarrow C \vdash (B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)} \Rightarrow U}{\vdash (A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))} \Rightarrow U$$

Задатак 15 Формула $\bot \Rightarrow A$ је теорема система $\mathcal{N}$.

$$\dfrac{\dfrac{\dfrac{}{\bot \vdash \bot}}{\bot \vdash A}\bot E}{\vdash \bot \Rightarrow A} \Rightarrow U$$

Задатак 16 Формула $((A \vee B) \wedge C) \Leftrightarrow ((A \wedge C) \vee (B \wedge C))$ је теорема система $\mathcal{N}$.

Доказаћемо да су секвенти $\vdash ((A \vee B) \wedge C) \Rightarrow ((A \wedge C) \vee (B \wedge C))$ и $\vdash ((A \wedge C) \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge C)$ доказиви у систему $\mathcal{N}$.

Прво представимо доказ за $\vdash ((A \vee B) \wedge C) \Rightarrow ((A \wedge C) \vee (B \wedge C))$, доказ $\mathcal{D}_1$, у коме је са F означена формула $(A \vee B) \wedge C$.

$$\dfrac{\dfrac{\dfrac{\dfrac{F \vdash F}{F \vdash A \vee B} \wedge E_1 \quad \dfrac{\dfrac{A \vdash A \qquad \dfrac{\dfrac{F \vdash F}{F \vdash C} \wedge E_2}{}}{A, F \vdash A \wedge C} \wedge U}{A, F \vdash (A \wedge C) \vee (B \wedge C)} \vee U_1 \quad \dfrac{\dfrac{B \vdash B \qquad \dfrac{\dfrac{F \vdash F}{F \vdash C} \wedge E_2}{}}{B, F \vdash B \wedge C} \wedge U}{B, F \vdash (A \wedge C) \vee (B \wedge C)} \vee U_2}{(A \vee B) \wedge C \vdash (A \wedge C) \vee (B \wedge C)} \vee E}{\vdash ((A \vee B) \wedge C) \Rightarrow ((A \wedge C) \vee (B \wedge C))} \Rightarrow U$$

А сада ево доказа за секвент $\vdash ((A \wedge C) \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge C)$, доказ $\mathcal{D}_2$, у коме је са E означена формула $(A \wedge C) \vee (B \wedge C)$.

$$\dfrac{\dfrac{\dfrac{E \vdash E \quad \dfrac{\dfrac{\dfrac{A \wedge C \vdash A \wedge C}{A \wedge C \vdash A} \wedge E_1}{A \wedge C \vdash A \vee B} \vee U_1 \quad \dfrac{\dfrac{\dfrac{B \wedge C \vdash B \wedge C}{B \wedge C \vdash B} \wedge E_1}{B \wedge C \vdash A \vee B} \vee U_2}{(A \wedge C) \vee (B \wedge C) \vdash (A \vee B)} \vee E \quad E \vdash E \quad \dfrac{\dfrac{A \wedge C \vdash A \wedge C}{A \wedge C \vdash C} \wedge E_2 \quad \dfrac{B \wedge C \vdash B \wedge C}{B \wedge C \vdash C} \wedge E_2}{(A \wedge C) \vee (B \wedge C) \vdash C} \vee E}{(A \wedge C) \vee (B \wedge C) \vdash (A \vee B) \wedge C} \wedge U}{\vdash ((A \wedge C) \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge C)} \Rightarrow U$$

У систему $\mathcal{N}$, користећи $\mathcal{D}_1$ и $\mathcal{D}_2$ и правило $\wedge U$, правимо доказ:

$$\dfrac{\overset{\mathcal{D}_1}{\vdash ((A \vee B) \wedge C) \Rightarrow ((A \wedge C) \vee (B \wedge C))} \qquad \overset{\mathcal{D}_2}{\vdash ((A \wedge C) \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge C)}}{\vdash (((A \vee B) \wedge C) \Rightarrow ((A \wedge C) \vee (B \wedge C))) \wedge (((A \wedge C) \vee (B \wedge C)) \Rightarrow ((A \vee B) \wedge C))} \wedge U.$$

Дакле, на основу познатих веза између везника, имамо да је ово доказ за формулу $((A \vee B) \wedge C) \Leftrightarrow ((A \wedge C) \vee (B \wedge C))$, тј. да је дистрибутивни закон $\wedge$ у односу на $\vee$ теорема система $\mathcal{N}$.

3.2.3 Хилбертовски систем, систем $\mathcal{L}$

У овом одељку дефинисаћемо још један формални систем исказне логике, хилбертовски систем, систем $\mathcal{L}$.

Скуп основних симбола система $\mathcal{L}$, скуп $\mathcal{S}(\mathcal{L})$

Скуп основних симбола система $\mathcal{L}$ је скуп основних симбола система $\mathcal{N}$ без помоћног симбола $\vdash$.

Исказне формуле система $\mathcal{L}$ су исказне формуле система $\mathcal{N}$.

Скуп формула система $\mathcal{L}$, скуп $\mathcal{F}(\mathcal{L})$

Скуп формула система $\mathcal{L}$, скуп $\mathcal{F}(\mathcal{L})$, чине исказне формуле тог система $\mathcal{L}$, тј. скуп $\mathcal{F}(\mathcal{L})$ је једнак скупу $\mathcal{F}(\mathcal{N})$.

Коначне скупове формула система $\mathcal{L}$ означаваћемо као у систему $\mathcal{N}$. Сада, са скупом аксиома и скупом правила извођења, испољиће се разлике између система $\mathcal{N}$ и $\mathcal{L}$. Аксиоме система $\mathcal{L}$ су посебни елементи скупа $\mathcal{F}(\mathcal{L})$, тј. неке исказне формуле, а правило извођења система $\mathcal{L}$ је једна релација дужине 3 на скупу $\mathcal{F}(\mathcal{L})$.

Скуп аксиома система $\mathcal{L}$, скуп $\mathcal{A}(\mathcal{L})$

$(A1)$ $A \Rightarrow (B \Rightarrow A)$

$(A2)$ $(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$

$(A3)$ $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$

$(A4)$ $A \Rightarrow (B \Rightarrow (A \wedge B))$

$(A5)$ $(A \wedge B) \Rightarrow A$

$(A6)$ $(A \wedge B) \Rightarrow B$

$(A7)$ $A \Rightarrow (A \vee B)$

$(A8)$ $B \Rightarrow (A \vee B)$

$(A9)$ $(A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C))$

$(A10)$ $\bot \Rightarrow A$

где су A, B и C произвољне формуле.

Важно је истаћи да смо напоменом да A, B и C могу бити произвољне формуле у ствари рекли да наведене аксиоме представљају схеме аксиоме. На пример, ако у тој схеми $(A1)$ на место формуле A ставимо формулу $B \Rightarrow C$, а на место формуле B ставимо формулу $A \wedge D$, тада добијамо аксиому система $\mathcal{L}$: $(B \Rightarrow C) \Rightarrow ((A \wedge D) \Rightarrow (B \Rightarrow C))$.

Скуп правила извођења система $\mathcal{L}$, скуп $\mathcal{R}(\mathcal{L})$

Систем $\mathcal{L}$ има једно правило извођења, правило modus ponens:

$$\frac{A \qquad A \Rightarrow B}{B} \quad MP$$

где су A и B произвољне формуле.

Дефиниција доказа у систему $\mathcal{L}$

Доказ у систему $\mathcal{L}$ је коначан низ формула $(n \geq 1)$

$$F_1, ..., F_n,$$

где за сваку формулу F_i, $1 \leq i \leq n$, важи:
или F_i је аксиома
или је F_i закључак правила MP (modus ponens) чије премисе су неке од формула из низа $F_1, ..., F_n$ индекса мањег од i.
За доказ $F_1, ..., F_n$ ћемо рећи да је доказ формуле F_n. Број формула које се појављују у том доказу, број n, зваћемо дужином тог доказа.

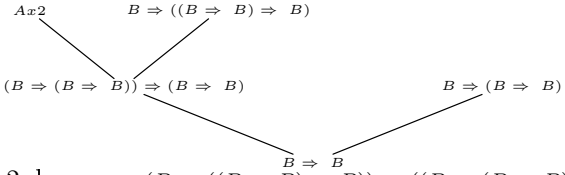
Ми ћемо доказе система $\mathcal{L}$ представљати и у облику дрвета. Наиме, сваки доказ F_1,...,F_n у систему $\mathcal{L}$ можемо представити једним дрветом у чијем корену је формула F_n, на листовима су све формуле тог доказа (низа F_1,...,F_n) које су аксиоме, а свако гранање тог дрвета је оправдано правилом извођења MP тако што се у доњем чвору тог гранања налази закључак правила, нека формула F_i, а у горњим чворовима су премисе тог правила, неке формуле из низа $F_1, ..., F_n$ индекса мањег од i.

Дефиниција теореме система $\mathcal{L}$

У систему $\mathcal{L}$ формула F је теорема АККО постоји бар један доказ формуле F у систему $\mathcal{L}$. Да је формула F теорема означаваћемо са $\vdash_{\mathcal{L}} F$ или $\vdash F$, а тај доказ је један доказ теореме F у систему $\mathcal{L}$.

У наредном примеру представићемо један доказ теореме у систему $\mathcal{L}$.

Пример 9 Покажимо да је таутологија рефлексивност импликације, $B \Rightarrow B$, једна теорема система $\mathcal{L}$. Правимо следеће дрво:



где је $Ax2$ формула $(B \Rightarrow ((B \Rightarrow B) \Rightarrow B)) \Rightarrow ((B \Rightarrow (B \Rightarrow B)) \Rightarrow (B \Rightarrow B))$.

Ево тог доказа у облику низа.

1. $(B \Rightarrow ((B \Rightarrow B) \Rightarrow B)) \Rightarrow ((B \Rightarrow (B \Rightarrow B)) \Rightarrow (B \Rightarrow B))$

   (ово је аксиома (A2) где: A је B, B је $B \Rightarrow B$ и C је B)

2. $B \Rightarrow ((B \Rightarrow B) \Rightarrow B)$

   (ово је аксиома (A1) где: A је B и B је $B \Rightarrow B$)

3. $(B \Rightarrow (B \Rightarrow B)) \Rightarrow (B \Rightarrow B)$

   (закључак правила MP из 1. и 2.)

4. $B \Rightarrow (B \Rightarrow B)$

   (ово је аксиома (A1) где: A је B и B је B)

5. $B \Rightarrow B$

   (закључак правила MP из 3. и 4.)

Дакле, формула $B \Rightarrow B$ је теорема система $\mathcal{L}$, тј. $\vdash_{\mathcal{L}} B \Rightarrow B$.

Сада ћемо показати нека својства доказа у систему $\mathcal{L}$.

ТЕОРЕМА 1

У систему $\mathcal{L}$ важи:

(1) Ако је $\Gamma \vdash A$ и $\Gamma \subseteq \Delta$, онда је $\Delta \vdash A$.

(2) Важи $\Gamma \vdash A$ ако и само ако постоји коначан подскуп Δ скупа Γ такав да важи $\Delta \vdash A$.

(3) Ако је $\Gamma \vdash A$ и за сваку формулу B из скупа Γ важи $\Delta \vdash B$, онда важи $\Delta \vdash A$.

ДОКАЗ

$\Gamma \vdash A$ значи да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Γ (одељак 3.1), тј. да постоји низ формула F_1,..., F_n такав да је F_n формула A, а за сваку формулу F_i, $1 \leq i \leq n$, важи: или је F_i аксиома или је F_i из скупа Γ, или је F_i закључак правила MP чије премисе су неке две претходне формуле тог низа.

(1) Како важи $\Gamma \subseteq \Delta$, одмах имамо да је свака формула из низа F_1,..., F_n или аксиома или формула из скупа Δ (јер је $\Gamma \subseteq \Delta$) или закључак правила MP из неке две претходне формуле тог низа. Дакле, имамо један доказ формуле A из скупа хипотеза Δ, тј. $\Delta \vdash A$.

(2) Први део: претпоставимо да важи $\Gamma \vdash A$. Нека је Δ скуп начињен од свих формула из низа F_1,..., F_n које припадају скупу Γ. Добијамо да је Δ коначан подскуп скупа Γ, а свака формула из низа F_1,..., F_n је или аксиома, или припада скупу Δ или је закључак правила MP, тј. важи: $\Delta \vdash A$. Други део: претпоставимо да постоји коначан подскуп скупа Γ, скуп Δ, за који важи $\Delta \vdash A$. Стога на основу особине из дела (1) добијамо $\Gamma \vdash A$.

(3) Пошто за сваку формулу B из скупа Γ важи $\Delta \vdash B$, то значи да за сваку ту формулу постоји доказ из скупа хипотеза Δ. Ако у доказу формуле A из скупа хипотеза Γ, доказу F_1,..., F_n, сваку формулу B која припада скупу Γ заменимо њеним доказом из скупа хипотеза Δ (који је неки низ формула), онда добијамо низ формула који се завршава формулом A и у коме је свака формула или аксиома или формула скупа Δ или закључак правила MP из неке две претходне формуле тог низа. То значи да је то један доказ формуле A из скупа хипотеза Δ, тј. важи $\Delta \vdash A$.

♢

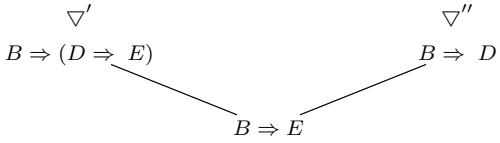
На крају овога одељка, у коме је представљен систем $\mathcal{L}$, доказаћемо значајну особину система $\mathcal{L}$, теорему дедукције.

ТЕОРЕМА 2 (ТЕОРЕМА ДЕДУКЦИЈЕ)

За произвољне формуле A и B и неки скуп формула Φ важи:

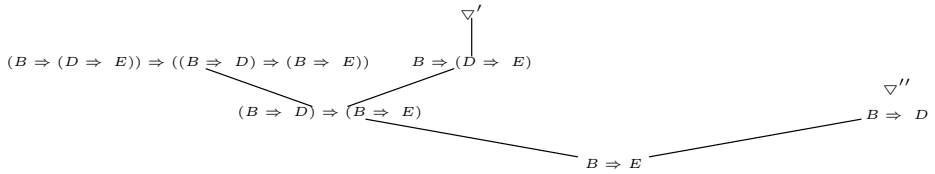
ако је $\Phi \cup \{B\} \vdash A$, онда је $\Phi \vdash B \Rightarrow A$.

Пре строгог доказа ТЕОРЕМЕ ДЕДУКЦИЈЕ дађемо један, мање формалан, доказ те теореме у коме су докази представљени као коначна дрвета.
Доказ формуле A из скупа хипотеза $\Phi \cup \{B\}$ је један низ формула. Нека су формуле $A_1, ..., A_k$ све аксиоме које се појављују у том доказу, формуле $F_1, ..., F_m$ све формуле из скупа Φ које се појављују у том доказу (где k и m могу бити и 0) и још формула B се појављује у том доказу. Од тог доказа можемо направити једно коначно дрво $\bigtriangledown$ на следећи начин. Корен тог дрвета је формула A. На листовима су формуле $A_1, ..., A_k$, $F_1, ..., F_m$ и B, а свако гранање је оправдано правилом MP, тј. у сваком чвору који није лист је нека формула E и у чворовима одмах изнад ње су формуле облика D и $D \Rightarrow E$, за неку формулу D. Сада вршимо следеће трансформације тог дрвета $\bigtriangledown$.
Први корак: сваку формулу F која се појављује у дрвету $\bigtriangledown$ замењујемо формулом $B \Rightarrow F$. То значи да је у корену новог дрвета формула $B \Rightarrow A$. На његовим листовима може се појавити једна од следећих формула: или $B \Rightarrow A_j$, $1 \leq j \leq k$, ако је на листу старог дрвета била аксиома A_j; или $B \Rightarrow F_i$, $1 \leq i \leq m$, ако је на листу старог дрвета била хипотеза F_i из скупа Φ; или $B \Rightarrow B$, ако је на листу старог дрвета била хипотеза B. На крају, свако гранање (из старог дрвета) у чијем доњем чвору је нека формула E после трансформације има облик:

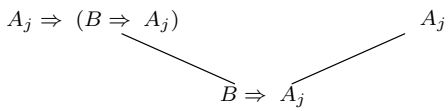


(*)

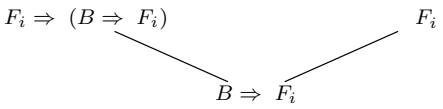
где су $\bigtriangledown'$ и $\bigtriangledown''$ делови новог дрвета изнад редом формуле $B \Rightarrow (D \Rightarrow E)$ и формуле $B \Rightarrow D$.
Други корак: у сваком чвору који није лист гранање је облика (*) и није оправдано правилом MP, зато тај део исецамо и на његово место стављамо:



где је формула $(B \Rightarrow (D \Rightarrow E)) \Rightarrow ((B \Rightarrow D) \Rightarrow (B \Rightarrow E))$ аксиома система $\mathcal{L}$ и сва гранања су оправдана правилом MP. На сваки од листова дрвета $\bigtriangledown$, у зависности од формуле која је на том листу, калемимо неко дрво. На сваки лист $B \Rightarrow A_j$, $1 \leq j \leq k$, одозго калемимо следеће дрво:



на чијим листовима су аксиоме A_j и $A_j \Rightarrow (B \Rightarrow A_j)$, а гранање је оправдано правилом MP. На сваки лист $B \Rightarrow F_i$, $1 \leq i \leq m$, одозго калемимо следеће дрво:



на чијим листовима су хипотеза F_i из скупа Φ и аксиома $F_i \Rightarrow (B \Rightarrow F_i)$, а гранање је оправдано правилом MP. На сваки лист $B \Rightarrow B$ одозго калемимо доказ теореме $B \Rightarrow B$ из Примера 9 на чијим листовима су аксиоме, а сва гранања су оправдана правилом MP. Процес трансформисања полазног дрвета доказа формуле A из скупа хипотеза $\Phi \cup \{B\}$ је завршен. Добили смо дрво у чијем корену је формула $B \Rightarrow A$, сва гранања су оправдана правилом MP и на листовима тог дрвета су или аксиоме система $\mathcal{L}$ или формуле скупа Φ. Дакле, то дрво је доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ у систему $\mathcal{L}$.

А сада ево и строгог доказа.

ДОКАЗ ТЕОРЕМЕ ДЕДУКЦИЈЕ

Теорему ћемо доказати индукцијом по дужини доказа формуле A из скупа хипотеза $\Phi \cup \{B\}$.

База индукције: доказ формуле A из скупа хипотеза $\Phi \cup \{B\}$ је дужине 1. То значи да се тај доказ састоји само из једне формуле и то мора бити формула A.
Ако је A из скупа Φ или ако је A аксиома система $\mathcal{L}$, онда користећи тај доказ, који чини формула A, и аксиому $A \Rightarrow (B \Rightarrow A)$ правимо следећи доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ:
1. A (или хипотеза из скупа Φ или аксиома)
2. $A \Rightarrow (B \Rightarrow A)$ (аксиома)
3. $B \Rightarrow A$ (закључак MP из 1. и 2.)
Ако је A формула B, онда је потребно показати да постоји доказ формуле $B \Rightarrow B$ из скупа хипотеза Φ. У Примеру 9 смо показали да је формула $B \Rightarrow B$ теорема система $\mathcal{L}$, тј. важи $\vdash B \Rightarrow B$, па из $\emptyset \subseteq \Phi$, на основу дела (1) ТЕОРЕМЕ 1, важи $\Phi \vdash B \Rightarrow B$.

Индукцијска претпоставка: за произвољне формуле A и B и скуп формула Φ: ако постоји доказ A из скупа хипотеза $\Phi \cup \{B\}$ дужине мање од n, онда постоји доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ.

Докажимо да теорема важи и за произвољне формуле A и B и скуп формула Φ и доказ формуле A из скупа хипотеза $\Phi \cup \{B\}$ дужине n: ако постоји доказ A из скупа хипотеза $\Phi \cup \{B\}$ дужине n, онда постоји доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ.
Нека је $C_1,...,C_n$ један доказ формуле A из скупа хипотеза $\Phi \cup \{B\}$ дужине n. Како је то доказ формуле A, онда је формула C_n у ствари A, тј. тај доказ је низ: $C_1,...,C_{n-1}$, A. За формулу A, као формулу која се појављује у том доказу, постоје следеће четири могућности:
(1) A је аксиома;
(2) A је нека хипотеза из скупа $\Phi \cup \{B\}$ која није B;
(3) A је хипотеза B из скупа $\Phi \cup \{B\}$;

(4) A је закључак правила MP, тј. постоје формуле C_i и C_j тог доказа (где су i и j мањи од n) такве да је C_j облика $C_i \Rightarrow A$.

У случајевима (1), (2) и (3) поступамо слично као у бази индукције и добијамо да постоји доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ.
У случају (4) посматрамо следеће делове доказа C_1,...,C_{n-1}, A: део C_1,..., C_i и део C_1,..., C_j. Све формуле тих делова су аксиоме, хипотезе из скупа $\Phi \cup \{B\}$ или закључци MP, тј. ти делови су докази редом формула C_i и C_j из скупа хипотеза $\Phi \cup \{B\}$. Дужине тих доказа су редом i и j, тј. њихове дужине су мање од n. Примењујемо индукцијску претпоставку на формуле C_i и C_j које имају доказ из скупа хипотеза $\Phi \cup \{B\}$ дужине мање од n: постоје докази из скупа хипотеза Φ за формуле $B \Rightarrow C_i$ и $B \Rightarrow C_j$, где је C_j облика $C_i \Rightarrow A$, тј. постоје докази: D_1, ..., $D_m = B \Rightarrow C_i$ и E_1, ..., $E_l = B \Rightarrow (C_i \Rightarrow A)$ (за $m, l > 0$). Надовезивањем тих доказа добијамо низ: D_1,..., D_{m-1}, $B \Rightarrow C_i$, E_1,..., E_{l-1}, $B \Rightarrow (C_i \Rightarrow A)$ чије формуле су или аксиоме или формуле из Φ или закључци правила MP. Тај низ настављамо, додајући следеће формуле: $(B \Rightarrow (C_i \Rightarrow A)) \Rightarrow ((B \Rightarrow C_i) \Rightarrow (B \Rightarrow A))$ (аксиома), затим закључак правила MP из те аксиоме и из формуле $B \Rightarrow (C_i \Rightarrow A)$: формулу $(B \Rightarrow C_i) \Rightarrow (B \Rightarrow A)$ и на крају закључак MP из те формуле и из формуле $B \Rightarrow C_i$: формулу $B \Rightarrow A$. Направљени низ формула чине формуле од којих је свака или аксиома или хипотеза из скупа Φ или је закључак правила MP из претходних формула низа, тј. то је један доказ формуле $B \Rightarrow A$ из скупа хипотеза Φ у систему $\mathcal{L}$.

$\diamondsuit$

3.2.4 Еквивалентност система $\mathcal{N}$ и $\mathcal{L}$

У овом одељку ћемо доказати да су систем $\mathcal{N}$ и систем $\mathcal{L}$ еквивалентни, тј. свака формула која је теорема система $\mathcal{N}$ она је теорема и система $\mathcal{L}$ и обрнуто. То значи да су та два система два еквивалентна начина задавања (представљања) исказне логике као формалне теорије. Прво ћемо доказати једну везу између доказа секвената система $\mathcal{N}$ и доказа из хипотеза система $\mathcal{L}$.

ТЕОРЕМА 3
Ако је секвент $\Gamma \vdash A$ доказив у систему $\mathcal{N}$, онда у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Γ.
ДОКАЗ

На почетку прихватимо следећи договор: када будемо говорили о томе да постоји неки доказ формуле C из скупа хипотеза Λ у систему $\mathcal{L}$ онда ћемо дрво тог доказа представити $\begin{matrix}\nabla_\Lambda \\ C\end{matrix}$ или $\begin{matrix}\nabla_\Lambda \\ | \\ C\end{matrix}$.

Теорему ћемо доказати индукцијом по дужини доказа $\mathcal{D}$ секвента $\Gamma \vdash A$ у систему $\mathcal{N}$, где дужину доказа дефинишемо као број правила извођења у том доказу.

База индукције, доказ секвента $\Gamma \vdash A$ има дужину 0, тј. тај доказ нема ни једно правило извођења. То значи да је секвент $\Gamma \vdash A$ аксиоматски секвент $A \vdash A$. У систему $\mathcal{L}$ то је доказ формуле A из скупа хипотеза $\{A\}$ и њега чини сама формула A.

Индукцијска претпоставка: теорема важи за сваки доказив секвент система $\mathcal{N}$ чији доказ има дужину мању од n.

Покажимо да теорема важи за секвент чији доказ је дужине n.
Посматрамо доказ $\mathcal{D}$ секвента $\Gamma \vdash A$ који је дужине n. Последње правило тог доказа може бити било које правило извођења ρ система $\mathcal{N}$, тј. доказ $\mathcal{D}$ је облика:

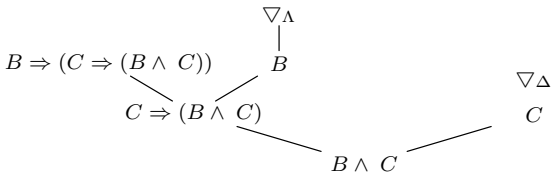
$$\dfrac{\begin{array}{ccc}\mathcal{D}' & \mathcal{D}'' & \mathcal{D}''' \\ \Gamma' \vdash A' & \Gamma'' \vdash A'' & \Gamma''' \vdash A'''\end{array}}{\Gamma \vdash A}\ \rho$$

где неки од доказа $\mathcal{D}'$, $\mathcal{D}''$, или $\mathcal{D}'''$, могу да не постоје. Горњи секвенти правила ρ, секвенти $\Gamma' \vdash A'$, $\Gamma'' \vdash A''$ и $\Gamma''' \vdash A'''$, су доказиви у систему $\mathcal{N}$ и њихови докази имају једно правило извођења мање него доказ секвента $\Gamma \vdash A$. Стога ће за њих важити индукцијска претпоставка. Имамо више случајева у зависности од тога које је последње правило извођења доказа $\mathcal{D}$ секвента $\Gamma \vdash A$.

◁ Последње правило доказа $\mathcal{D}$ је увођење $\wedge$, па је доказ $\mathcal{D}$:

$$\dfrac{\begin{array}{cc}\mathcal{D}' & \mathcal{D}'' \\ \Lambda \vdash B & \Delta \vdash C\end{array}}{\Lambda \cup \Delta \vdash B \wedge C}\ \wedge U$$

а секвент $\Gamma \vdash A$ је $\Lambda \cup \Delta \vdash B \wedge C$. Треба показати да у систему $\mathcal{L}$ постоји доказ формуле $B \wedge C$ из скупа хипотеза $\Lambda \cup \Delta$. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле B из скупа хипотеза Λ и постоји доказ формуле C из скупа хипотеза Δ. Користећи те доказе у систему $\mathcal{L}$ правимо дрво:



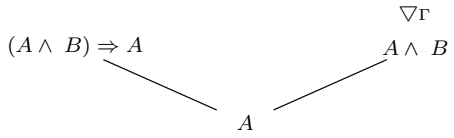
Листови овог дрвета су листови дрвета $\overset{\nabla\Lambda}{B}$ и дрвета $\overset{\nabla\Delta}{C}$ (на којима су или аксиоме или формуле из скупа Λ, односно Δ) и лист на коме је аксиома $B \Rightarrow (C \Rightarrow (B \wedge C))$. Остали чворови новог дрвета су

чворови (који нису листови) дрвета $\overset{\nabla\Lambda}{B}$ и дрвета $\overset{\nabla\Delta}{C}$ и два чвора у којима су формуле $B \wedge C$ и $C \Rightarrow (B \wedge C)$, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, ово ново дрво јесте један доказ у систему $\mathcal{L}$ формуле $B \wedge C$ из скупа хипотеза $\Lambda \cup \Delta$.

$\triangleleft$ Последње правило доказа $\mathcal{D}$ је елиминација $\wedge$, на пример $(\wedge E_1)$. Дакле, доказ $\mathcal{D}$ је:

$$\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma \vdash A \wedge B\end{array}}{\Gamma \vdash A} \wedge E_1$$

Треба показати да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Γ. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле $A \wedge B$ из скупа хипотеза Γ. Користећи тај доказ правимо дрво:



Листови овог дрвета су листови дрвета $\overset{\nabla\Gamma}{A \wedge B}$ (на којима су или аксиоме или формуле из Γ) и лист на коме је аксиома $(A \wedge B) \Rightarrow A$. Остали чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla\Gamma}{A \wedge B}$ и чвор у коме је формула A, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, то ново дрво јесте један доказ у систему $\mathcal{L}$ формуле A из скупа хипотеза Γ. У случају када је $(\wedge E_2)$ последње правило доказа $\mathcal{D}$ поступамо аналогно.

$\triangleleft$ Последње правило доказа $\mathcal{D}$ је увођење $\Rightarrow$, па је доказ $\mathcal{D}$:

$$\dfrac{\begin{array}{c}\mathcal{D}'\\ \Gamma_1 \vdash C\end{array}}{\Gamma \vdash B \Rightarrow C} \Rightarrow U$$

а секвент $\Gamma \vdash A$ је $\Gamma \vdash B \Rightarrow C$. Треба показати да у систему $\mathcal{L}$ постоји доказ формуле $B \Rightarrow C$ из скупа хипотеза Γ. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле C из скупа хипотеза Γ_1. Стога на основу дела (1) ТЕОРЕМЕ 1, постоји доказ формуле C из скупа хипотеза $\Gamma_1 \cup \{B\}$. Из дефиниције правила $(\Rightarrow U)$ за скуп Γ имамо: $\Gamma = \Gamma_1$ или $\Gamma = \Gamma_1 \backslash \{B\}$. Дакле, у оба случаја имамо да у систему $\mathcal{L}$ постоји доказ формуле C из скупа хипотеза $\Gamma \cup \{B\}$. Дакле, на основу ТЕОРЕМЕ ДЕДУКЦИЈЕ, у систему $\mathcal{L}$ постоји доказ формуле $B \Rightarrow C$ из скупа хипотеза Γ.

◁ Последње правило доказа $\mathcal{D}$ је елиминација $\Rightarrow$, па је доказ $\mathcal{D}$:

$$\dfrac{\begin{matrix}\mathcal{D}' & \mathcal{D}'' \\ \Lambda \vdash B \Rightarrow A & \Delta \vdash B\end{matrix}}{\Lambda \cup \Delta \vdash A} \Rightarrow E$$

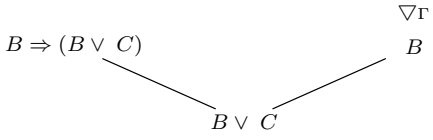
а секвент $\Gamma \vdash A$ је $\Lambda \cup \Delta \vdash A$. Морамо показати да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза $\Lambda \cup \Delta$. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле B из скупа хипотеза Δ и постоји доказ формуле $B \Rightarrow A$ из скупа хипотеза Λ. Користећи те доказе правимо ново дрво:

Листови овог дрвета су листови дрвета $\overset{\nabla\Delta}{B}$ и дрвета $\overset{\nabla\Lambda}{B \Rightarrow A}$ (на којима су или аксиоме или формуле из скупа Δ, односно Λ). Сви остали чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla\Delta}{B}$ и дрвета $\overset{\nabla\Lambda}{B \Rightarrow A}$ и чвор у коме је формула A, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, то ново дрво јесте један доказ у систему $\mathcal{L}$ формуле A из скупа хипотеза $\Lambda \cup \Delta$.

◁ Последње правило доказа $\mathcal{D}$ је увођење $\vee$, на пример $(\vee U_1)$. Дакле, доказ $\mathcal{D}$ је:

$$\dfrac{\begin{matrix}\mathcal{D}' \\ \Gamma \vdash B\end{matrix}}{\Gamma \vdash B \vee C} \vee U_1$$

а секвент $\Gamma \vdash A$ је $\Gamma \vdash B \vee C$. Остаје да покажемо да у систему $\mathcal{L}$ постоји доказ формуле $B \vee C$ из скупа хипотеза Γ. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле B из скупа хипотеза Γ. Користећи тај доказ правимо ово дрво:

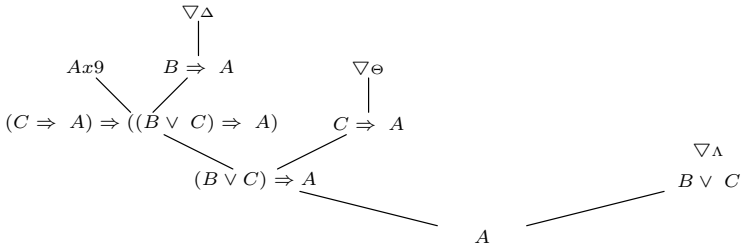


Листови овог дрвета су листови дрвета $\overset{\nabla\Gamma}{B}$ (на којима су или аксиоме или формуле из скупа Γ) и лист на коме је аксиома $B \Rightarrow (B \vee C)$. Сви остали чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla\Gamma}{B}$ и чвор у коме је формула $B \vee C$, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, то ново дрво јесте један доказ у систему $\mathcal{L}$ формуле $B \vee C$ из скупа хипотеза Γ. У случају када је $(\vee U_2)$ последње правило у $\mathcal{D}$ поступамо аналогно.

◁ Последње правило доказа $\mathcal{D}$ је елиминација $\vee$, па је доказ $\mathcal{D}$:

$$\dfrac{\begin{array}{ccc}\mathcal{D}' & \mathcal{D}'' & \mathcal{D}''' \\ \Lambda \vdash B \vee C & \Delta_1 \vdash A & \Theta_1 \vdash A\end{array}}{\Lambda \cup \Delta \cup \Theta \vdash A} \vee E$$

а секвент $\Gamma \vdash A$ је $\Lambda \cup \Delta \cup \Theta \vdash A$. Треба показати да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза $\Lambda \cup \Delta \cup \Theta$. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле $B \vee C$ из скупа хипотеза Λ, постоји доказ формуле A из скупа хипотеза Δ_1 и постоји доказ формуле A из скупа хипотеза Θ_1. Стога на основу дела (1) ТЕОРЕМЕ 1, постоји доказ формуле A из скупа хипотеза $\Delta_1 \cup \{B\}$ и постоји доказ формуле A из скупа хипотеза $\Theta_1 \cup \{C\}$. Из дефиниције правила $(\vee E)$ за скупове Δ и Θ имамо: $\Delta = \Delta_1$ или $\Delta = \Delta_1 \backslash \{B\}$; и $\Theta = \Theta_1$ или $\Theta = \Theta_1 \backslash \{C\}$. Дакле, у свим тим случајевима имамо да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза $\Delta \cup \{B\}$ и постоји доказ формуле A из скупа хипотеза $\Theta \cup \{C\}$. Из та два доказа, на основу ТЕОРЕМЕ ДЕДУКЦИЈЕ, имамо да у систему $\mathcal{L}$ постоји доказ формуле $B \Rightarrow A$ из скупа хипотеза Δ и постоји доказ формуле $C \Rightarrow A$ из скупа хипотеза Θ. Користећи те доказе, правимо дрво:



где је $Ax9 : (B \Rightarrow A) \Rightarrow ((C \Rightarrow A) \Rightarrow ((B \vee C) \Rightarrow A))$ (аксиома (A9)). Листови овог дрвета су листови дрвета $\overset{\nabla_\Delta}{B \Rightarrow A}$, дрвета $\overset{\nabla_\Theta}{C \Rightarrow A}$ и дрвета $\overset{\nabla_\Lambda}{B \vee C}$ (на којима су или аксиоме или формуле из скупа $\Delta \cup \Theta \cup \Lambda$) и лист на коме је аксиома $(B \Rightarrow A) \Rightarrow ((C \Rightarrow A) \Rightarrow ((B \vee C) \Rightarrow A))$. Сви остали чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla_\Delta}{B \Rightarrow A}$, дрвета $\overset{\nabla_\Theta}{C \Rightarrow A}$ и дрвета $\overset{\nabla_\Lambda}{B \vee C}$ и чворови у којима су формуле: $(C \Rightarrow A) \Rightarrow ((B \vee C) \Rightarrow A)$, $(B \vee C) \Rightarrow A$ и A, и у сваком од тих чворова је закључак једне примене правила MP. Стога, то ново дрво јесте доказ формуле A из скупа хипотеза $\Delta \cup \Theta \cup \Lambda$ у $\mathcal{L}$.

◁ Последње правило доказа $\mathcal{D}$ је елиминација $\bot$, па је доказ $\mathcal{D}$:

$$\dfrac{\begin{array}{c}\mathcal{D}' \\ \Gamma \vdash \bot\end{array}}{\Gamma \vdash A} \bot E$$

Треба показати да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Г. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле $\bot$ из скупа хипотеза Г. Користећи тај доказ правимо ново дрво:

$$\begin{array}{ccc} \bot \Rightarrow A & & \overset{\nabla_\Gamma}{\bot} \\ & \searrow \quad \swarrow & \\ & A & \end{array}$$

Листови овог дрвета су листови дрвета $\overset{\nabla_\Gamma}{\bot}$ (на којима су или аксиоме или формуле из скупа Г) и лист на коме је аксиома $\bot \Rightarrow A$. Сви други чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla_\Gamma}{\bot}$ и чвор у којем је формула A, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, то дрво јесте један доказ у систему $\mathcal{L}$ формуле A из скупа хипотеза Г.

◁ Последње правило доказа $\mathcal{D}$ је Персово правило, тј. доказ $\mathcal{D}$ је:

$$\dfrac{\begin{array}{c}\mathcal{D}' \\ \Gamma \cup \{A \Rightarrow B\} \vdash A\end{array}}{\Gamma \vdash A} Pers$$

Треба показати да у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Г. На основу индукцијске претпоставке у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза $\Gamma \cup \{A \Rightarrow B\}$. Из овог последњег доказа, на основу ТЕОРЕМЕ ДЕДУКЦИЈЕ, имамо да у систему $\mathcal{L}$ постоји доказ формуле $(A \Rightarrow B) \Rightarrow A$ из скупа хипотеза Г. Користећи тај доказ правимо ново дрво:

$$\begin{array}{ccc} ((A \Rightarrow B) \Rightarrow A) \Rightarrow A & & \overset{\nabla_\Gamma}{(A \Rightarrow B) \Rightarrow A} \\ & \searrow \quad \swarrow & \\ & A & \end{array}$$

Листови овог дрвета су листови дрвета $\overset{\nabla_\Gamma}{(A \Rightarrow B) \Rightarrow A}$ (на којима су или аксиоме или формуле из Г) и аксиома $((A \Rightarrow B) \Rightarrow A) \Rightarrow A$. Остали чворови новог дрвета су чворови (који нису листови) дрвета $\overset{\nabla_\Gamma}{(A \Rightarrow B) \Rightarrow A}$ и чвор у којем је формула A, и у сваком од тих чворова је закључак једне примене правила MP. Дакле, то ново дрво јесте један доказ у систему $\mathcal{L}$ формуле A из скупа хипотеза Г.

Закључујемо: за сваки доказив секвент система $\mathcal{N}$, неки секвент $\Gamma \vdash A$, у систему $\mathcal{L}$ постоји доказ формуле A из скупа хипотеза Г.

$\diamondsuit$

ТЕОРЕМА 4

Формула F је теорема система $\mathcal{L}$ ако и само ако је F теорема система $\mathcal{N}$.

ДОКАЗ

ПРВИ ДЕО:

Ако је формула F теорема система $\mathcal{L}$, онда је F теорема система $\mathcal{N}$.

ДОКАЗ

Прво треба доказати да су све аксиоме система $\mathcal{L}$ теореме система $\mathcal{N}$. Другачије речено, за сваку аксиому A система $\mathcal{L}$ треба показати да је секвент $\vdash A$ доказив у систему $\mathcal{N}$. То смо ми већ показали у Задацима 8-15 одељка 3.2.2. Дакле, све аксиоме система $\mathcal{L}$ су теореме система $\mathcal{N}$. Остаје још да, користећи ту особину, покажемо да је и произвољна теорема система $\mathcal{L}$ теорема система $\mathcal{N}$. Нека је формула F теорема система $\mathcal{L}$. У систему $\mathcal{L}$ постоји доказ формуле F. Ако тај доказ представимо као дрво, онда је то коначно дрво у чијем корену је формула F, на сваком листу тог дрвета је нека аксиома система $\mathcal{L}$ и свако гранање је оправдано правилом извођења MP. На том дрвету направимо следеће измене:
(1) на сваком листу затечену аксиому A заменимо дрветом доказа секвента $\vdash A$ из система $\mathcal{N}$ који смо направили у Задацима 8-15 и
(2) у сваком чвору затечену формулу D заменимо секвентом облика $\vdash D$, па и у корену тог дрвета формулу F заменимо секвентом $\vdash F$. Добили смо ново дрво. Питамо се да ли је то дрво један доказ у систему $\mathcal{N}$? Прво, сви листови тог дрвета су листови доказа система $\mathcal{N}$ из Задатака 8-15, значи на њима су аксиоматски секвенти. Остаје још да проверимо чиме су оправдана гранања у том дрвету. Ако је то гранање у делу дрвета који се завршава секвентом $\vdash A$, где је A нека аксиома система $\mathcal{L}$ (то је гранање неког од доказа представљених у Задацима 8-15), онда је оно оправдано неким правилом извођења система $\mathcal{N}$. Ако је то гранање у делу дрвета које је постојало у дрвету доказа формуле F у систему $\mathcal{L}$ (и тамо оправдано правилом MP), онда је у систему $\mathcal{N}$ то гранање оправдано правилом елиминације везника $\Rightarrow$, правилом $(\Rightarrow E)$. Закључујемо да су на листовима новог дрвета аксиоматски секвенти, а свако његово гранање је оправдано неким правилом извођења система $\mathcal{N}$, па то дрво јесте један доказ у систему $\mathcal{N}$ у чијем је корену секвент $\vdash F$. Стога закључујемо да је секвент $\vdash F$ доказив у систему $\mathcal{N}$, тј. формула F јесте теорема система $\mathcal{N}$.

ДРУГИ ДЕО:

Ако је формула F теорема система $\mathcal{N}$, онда је F теорема система $\mathcal{L}$.

ДОКАЗ

Како је формула F теорема система $\mathcal{N}$, то значи да је секвент $\vdash F$ доказив у систему $\mathcal{N}$. На основу ТЕОРЕМЕ 3, у систему $\mathcal{L}$ постоји

доказ формуле F из скупа хипотеза који је празан скуп. То значи да је формула F теорема система $\mathcal{L}$.

$\Diamond$

Еквивалентност формалних система $\mathcal{N}$ и $\mathcal{L}$ значи да надаље можемо једноставно говорити о исказној логици и теоремама исказне логике не прецизирајући да ли мислимо на систем $\mathcal{N}$ или систем $\mathcal{L}$. Осим тога, сваки пут када хоћемо да утврдимо да ли је нека исказна формула F теорема исказне логике то можемо урадити тако што направимо доказ те формуле у систему $\mathcal{L}$ или доказ секвента $\vdash F$ у систему $\mathcal{N}$.

3.2.5 Потпуност исказне логике

У Примерима 7-9 и Задацима 8-16 из одељка 3.2.2 показали смо да су неке таутологије теореме система $\mathcal{N}$, тј. система $\mathcal{L}$. Намеће се следеће питање: да ли и за друге таутологије важи да су теореме исказне логике? Одговор је: ДА. Важи и више, а то је да нема других теорема исказне логике осим таутологија, тј. свака теорема исказне логике мора бити таутологија и обрнуто, свака таутологија је теорема исказне логике. Другачије речено, важи следећа особина:

формула F је теорема исказне логике ако и само ако је формула F таутологија,

тј. за сваку формулу F исказне логике важи:

$$\vdash F \text{ ако и само ако } \models F.$$

Ова особина се зове потпуност у ширем смислу. Део:

ако је формула F теорема исказне логике, онда је F и таутологија,

тј.

$$\text{ако је} \quad \vdash F, \quad \text{онда је} \quad \models F$$

је особина ваљаности, а део

ако је формула F таутологија, онда је F теорема исказне логике,

тј.

$$\text{ако је} \quad \models F, \quad \text{онда је} \quad \vdash F$$

је особина потпуности, тј. потпуност у ужем смислу.

Докажимо прво да важи особина ваљаности.

ТЕОРЕМА 5 (ВАЉАНОСТ)
Ако је формула F теорема исказне логике, онда је формула F и таутологија.

ДОКАЗ

У доказу особине ваљаности исказну логику ћемо представити системом $\mathcal{L}$. У претходним одељцима показали смо следеће:
(1) У Задатку 4 одељка 2.2.3 за сваку аксиому система $\mathcal{L}$ показали

смо да је таутологија. Дакле, важи да су све аксиоме система $\mathcal{L}$ таутологије.
(2) У одељку 2.2.4 доказали смо ТЕОРЕМУ *MP* која нам показује да правило MP чува таутологије, тј. да важи: ако су A и $A \Rightarrow B$ таутологије, онда је и B таутологија.
Из ових резултата следи особина ваљаности. Наиме, ако је формула F теорема исказне логике, тј. система $\mathcal{L}$, онда у том систему постоји доказ у облику дрвета на чијим листовима су аксиоме система $\mathcal{L}$, а у свим осталим чворовима су закључци правила MP. Из (1) имамо да су на свим листовима тог дрвета таутологије, а из (2) да су и у свим осталим чворовима таутологије. Дакле, у свим чворовима доказа формуле F су таутологије, па и формула у његовом корену, формула F. Закључујемо да свака теорема исказне логике мора бити таутологија, тј. да важи особина ваљаности:

$$\text{ако је} \quad \vdash F, \quad \text{онда је} \quad \models F.$$

♢

Остаје да докажемо да важи особина потпуности.

ТЕОРЕМА 6 (ПОТПУНОСТ)

Ако је формула F таутологија, онда је формула F и теорема исказне логике.

Прво докажимо неке једноставне особине које важе за теореме исказне логике, а које олакшавају рад са њима.

ТЕОРЕМА 7

За теореме исказне логике важи:
(1) ако је формула $A \wedge B$ теорема, онда су и формуле A и B теореме;
(2) ако су формуле A и B теореме, онда је и $A \wedge B$ теорема;
(3) ако је A теорема, онда су (за неку формулу C) и $A \vee C$ и $C \vee A$ теореме;
(4) ако је формула $A \vee B$ теорема, онда је и $B \vee A$ теорема;
(5) формула $A \Leftrightarrow B$ је теорема ако и само ако су $A \Rightarrow B$ и $B \Rightarrow A$ теореме;
(6) $(A \vee B) \vee C$ је теорема ако и само ако је $A \vee (B \vee C)$ теорема;
(7) ако су формуле $A \Leftrightarrow B$ и $B \Leftrightarrow C$ теореме, онда је и $A \Leftrightarrow C$ теорема.

ДОКАЗ

Све ове особине је лакше доказати у систему $\mathcal{N}$. Користимо дефиницију да је C теорема АККО у систему $\mathcal{N}$ постоји доказ секвента $\vdash C$.
(1) У систему $\mathcal{N}$ постоји доказ $\mathcal{D}$ секвента $\vdash A \wedge B$. Користећи тај доказ, правимо следеће доказе: $\dfrac{\begin{matrix}\mathcal{D}\\ \vdash A \wedge B\end{matrix}}{\vdash A} \wedge E_1$ и $\dfrac{\begin{matrix}\mathcal{D}\\ \vdash A \wedge B\end{matrix}}{\vdash B} \wedge E_2$. Дакле, формуле A и B су теореме исказне логике.

(2) У систему $\mathcal{N}$ постоје докази $\mathcal{D}_1$ и $\mathcal{D}_2$ редом секвента $\vdash A$ и $\vdash B$. Користећи те доказе, правимо следећи доказ: $\dfrac{\overset{\mathcal{D}_1}{\vdash A} \quad \overset{\mathcal{D}_2}{\vdash B}}{\vdash A \wedge B} \wedge U$. Дакле, формула $A \wedge B$ је теорема исказне логике.

(3) У систему $\mathcal{N}$ постоји доказ $\mathcal{D}$ секвента $\vdash A$. Користећи тај доказ, правимо следеће доказе: $\dfrac{\overset{\mathcal{D}}{\vdash A}}{\vdash A \vee C} \vee E_1$ и $\dfrac{\overset{\mathcal{D}}{\vdash A}}{\vdash C \vee A} \vee E_2$. Дакле, формуле $A \vee C$ и $C \vee A$ су теореме исказне логике.

(4) У систему $\mathcal{N}$ постоји доказ $\mathcal{D}$ секвента $\vdash A \vee B$. Користећи тај доказ, правимо доказ:

$$\dfrac{\overset{\mathcal{D}}{\vdash A \vee B} \quad \dfrac{A \vdash A}{A \vdash B \vee A} \vee U_2 \quad \dfrac{B \vdash B}{B \vdash B \vee A} \vee U_1}{\vdash B \vee A} \vee E.$$

Дакле, формула $B \vee A$ је теорема исказне логике.

(5) Када $A \Leftrightarrow B$ запишимо $(A \Rightarrow B) \wedge (B \Rightarrow A)$, онда је овај део последица делова (1) и (2). Наиме, ако је $(A \Rightarrow B) \wedge (B \Rightarrow A)$ теорема исказне логике, онда у систему $\mathcal{N}$ постоји доказ $\mathcal{D}$ секвента $\vdash (A \Rightarrow B) \wedge (B \Rightarrow A)$. Користећи тај доказ, правимо доказе: $\dfrac{\overset{\mathcal{D}}{\vdash (A \Rightarrow B) \wedge (B \Rightarrow A)}}{\vdash A \Rightarrow B} \wedge E_1$ и $\dfrac{\overset{\mathcal{D}}{\vdash (A \Rightarrow B) \wedge (B \Rightarrow A)}}{\vdash B \Rightarrow A} \wedge E_2$ Дакле, формуле $A \Rightarrow B$ и $B \Rightarrow A$ су теореме исказне логике. С друге стране, ако су формуле $A \Rightarrow B$ и $B \Rightarrow A$ теореме, онда у систему $\mathcal{N}$ постоје докази секвената $\vdash A \Rightarrow B$ и $\vdash B \Rightarrow A$, редом $\mathcal{D}_1$ и $\mathcal{D}_2$. Од њих правимо доказ: $\dfrac{\overset{\mathcal{D}_1}{\vdash A \Rightarrow B} \quad \overset{\mathcal{D}_2}{\vdash B \Rightarrow A}}{\vdash (A \Rightarrow B) \wedge (B \Rightarrow A)} \wedge U$. Дакле, $A \Leftrightarrow B$ јесте теорема.

(6) Формула $((A \vee B) \vee C) \Leftrightarrow (A \vee (B \vee C))$ је теорема исказне логике (Пример 8 из одељка 3.2.2), па на основу (5), добијамо да су теореме и $((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))$ и $(A \vee (B \vee C)) \Rightarrow ((A \vee B) \vee C)$, тј. у $\mathcal{N}$ постоје докази секвената $\vdash ((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))$ и $\vdash (A \vee (B \vee C)) \Rightarrow ((A \vee B) \vee C)$, редом $\mathcal{D}_1$ и $\mathcal{D}_2$. Ако је формула $(A \vee B) \vee C$ теорема, онда у систему $\mathcal{N}$ постоји доказ $\mathcal{D}$ секвента $\vdash (A \vee B) \vee C$. Користећи тај доказ и доказ $\mathcal{D}_1$, правимо доказ:

$$\dfrac{\overset{\mathcal{D}_1}{\vdash ((A \vee B) \vee C) \Rightarrow (A \vee (B \vee C))} \qquad \overset{\mathcal{D}}{\vdash (A \vee B) \vee C}}{\vdash A \vee (B \vee C)} \Rightarrow E$$

Дакле, $A \vee (B \vee C)$ је теорема исказне логике. С друге стране, ако је формула $A \vee (B \vee C)$ теорема, онда у $\mathcal{N}$ постоји доказ $\mathcal{D}'$ секвента $\vdash A \vee (B \vee C)$. Слично претходном случају, користећи доказе $\mathcal{D}'$ и $\mathcal{D}_2$ и правило $(\Rightarrow E)$, правимо доказ секвента $\vdash (A \vee B) \vee C$. Дакле, $(A \vee B) \vee C$ је теорема исказне логике.

(7) Ако су формуле $A \Leftrightarrow B$ и $B \Leftrightarrow C$ теореме, онда су, на основу дела (5), теореме и формуле $A \Rightarrow B$, $B \Rightarrow A$, $B \Rightarrow C$ и $C \Rightarrow B$. То значи да за секвенте $\vdash A \Rightarrow B$, $\vdash B \Rightarrow A$, $\vdash B \Rightarrow C$ и $\vdash C \Rightarrow B$ постоје докази у систему $\mathcal{N}$. Користећи доказе секвената $\vdash A \Rightarrow B$ и $\vdash B \Rightarrow C$ редом $\mathcal{D}_1$ и $\mathcal{D}_2$, правимо доказ секвента $\vdash A \Rightarrow C$:

$$\dfrac{\dfrac{\mathcal{D}_2}{\vdash B \Rightarrow C} \qquad \dfrac{\dfrac{\mathcal{D}_1}{\vdash A \Rightarrow B} \qquad \dfrac{}{A \vdash A}\Rightarrow E}{A \vdash B}\Rightarrow E}{\dfrac{A \vdash C}{\vdash A \Rightarrow C}\Rightarrow U}$$

На сличан начин, користећи доказе секвената $\vdash B \Rightarrow A$ и $\vdash C \Rightarrow B$, можемо направити доказ секвента $\vdash C \Rightarrow A$. Дакле, имамо да су формуле $A \Rightarrow C$ и $C \Rightarrow A$ теореме, па на основу дела (5) добијамо да је и формула $A \Leftrightarrow C$ теорема исказне логике.

♢

Особине теорема исказне логике које сада следе су сличне особинама тautологија доказаним у претходним одељцима. Другачије речено, ми смо већ доказали семантичку верзију неких особина исказних формула, а сада ћемо доказати и синтаксну верзију тих особина. Прва таква особина је особина представљена у ТЕОРЕМИ MP у одељку 2.2.4. Синтаксна верзија ТЕОРЕМЕ MP је следеће тврђење.

ТЕОРЕМА 8

Ако су A и $A \Rightarrow B$ теореме исказне логике, онда је и B теорема исказне логике.

ДОКАЗ

С обзиром на то да су формуле A и $A \Rightarrow B$ теореме исказне логике, закључујемо да постоје неки докази $A_1,\ldots,A_m = A$ и $C_1,\ldots,C_n = A \Rightarrow B$. Доказ формуле B у систему $\mathcal{L}$ правимо надовезивањем постојећих доказа: $A_1,\ldots,A_m = A$, $C_1,\ldots,C_n = A \Rightarrow B$ и додавањем формуле B, као закључак правила MP, чије премисе су формуле $C_n = A \Rightarrow B$ и $A_m = A$. Дакле, формула B има доказ у систему $\mathcal{L}$, па је формула B теорема исказне логике.

♢

Следећа теорема одговара ЛЕМИ О ЗАМЕНИ ЕКВИВАЛЕНАТА из одељка 2.2.2.

ТЕОРЕМА 9

У исказној логици ако је $A \Leftrightarrow B$ теорема и C произвољна формула, онда важи:

(1) формула $\neg A \Leftrightarrow \neg B$ је теорема;
(2) формуле $(A \wedge C) \Leftrightarrow (B \wedge C)$ и $(C \wedge A) \Leftrightarrow (C \wedge B)$ су теореме;
(3) формуле $(A \vee C) \Leftrightarrow (B \vee C)$ и $(C \vee A) \Leftrightarrow (C \vee B)$ су теореме;
(4) формуле $(A \Rightarrow C) \Leftrightarrow (B \Rightarrow C)$ и $(C \Rightarrow A) \Leftrightarrow (C \Rightarrow B)$ су теореме;
(5) формуле $(A \Leftrightarrow C) \Leftrightarrow (B \Leftrightarrow C)$ и $(C \Leftrightarrow A) \Leftrightarrow (C \Leftrightarrow B)$ су теореме.

ДОКАЗ

Покажимо само да је формула $(A \wedge C) \Leftrightarrow (B \wedge C)$ из дела (2) теорема. На основу дела (5) ТЕОРЕМЕ 7 пошто је формула $A \Leftrightarrow B$ теорема, онда су и формуле $A \Rightarrow B$ и $B \Rightarrow A$ теореме. То значи да у систему $\mathcal{N}$ постоје неки докази $\mathcal{D}_1$ и $\mathcal{D}_2$ редом секвента $\vdash A \Rightarrow B$ и секвента $\vdash B \Rightarrow A$. Користећи доказ $\mathcal{D}_1$, правимо следећи доказ:

$$\dfrac{\dfrac{\dfrac{\mathcal{D}_1}{\vdash A \Rightarrow B} \quad \dfrac{A \wedge C \vdash A \wedge C}{A \wedge C \vdash A} \wedge E_1}{A \wedge C \vdash B} \Rightarrow E \qquad \dfrac{A \wedge C \vdash A \wedge C}{A \wedge C \vdash C} \wedge E_2}{\dfrac{A \wedge C \vdash B \wedge C}{\vdash (A \wedge C) \Rightarrow (B \wedge C)} \Rightarrow U} \wedge U$$

На сличан начин, користећи доказ $\mathcal{D}_2$, можемо направити доказ секвента $\vdash (B \wedge C) \Rightarrow (A \wedge C)$. Дакле, формула $(A \wedge C) \Rightarrow (B \wedge C)$ и формула $(B \wedge C) \Rightarrow (A \wedge C)$ су теореме исказне логике, па на основу дела (5) ТЕОРЕМЕ 7, и формула $(A \wedge C) \Leftrightarrow (B \wedge C)$ је теорема исказне логике. Докази за све друге формуле праве се на сличан начин.

♢

Следећа теорема је синтаксна верзија ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА из одељка 2.2.2. За доказ те теореме можемо сликовито рећи да је доказ ТЕОРЕМЕ О ЗАМЕНИ ЕКВИВАЛЕНАТА у коме је реч таутологија замењена речју теорема. Ту теорему ћемо формулисати за систем $\mathcal{L}$ исказне логике.

ТЕОРЕМА 10

У систему $\mathcal{L}$ за произвољне формуле C, D и F и исказно слово p важи:

ако је $\vdash C \Leftrightarrow D$, онда је $\vdash F^p_C \Leftrightarrow F^p_D$.

ДОКАЗ

Посматрајмо произвољну формулу F. Теорему ћемо доказати индукцијом по броју бинарних логичких везника у формули F.

База индукције, формула F има 0 бинарних везника, тј. F је или $\bot$ или неко исказно слово. Ако је F баш $\bot$, онда је $F^p_C = \bot^p_C = \bot$ и $F^p_D = \bot^p_D = \bot$. Дакле, формула $F^p_C \Leftrightarrow F^p_D$ је теорема. Ако је F исказно слово q и q је различито од p, онда је $F^p_C = q^p_C = q$ и $F^p_D = q^p_D = q$. Дакле, формула $F^p_C \Leftrightarrow F^p_D$ је теорема $q \Leftrightarrow q$, па важи $\vdash F^p_C \Leftrightarrow F^p_D$. Ако је формула F баш исказно слово p, тада имамо да је формула $F^p_C = p^p_C = C$ и формула $F^p_D = p^p_D = D$. Како важи $\vdash C \Leftrightarrow D$, имамо и $\vdash F^p_C \Leftrightarrow F^p_D$.

Индукцијска претпоставка: теорема важи за сваку формулу F која има мање од n бинарних логичких везника.

Докажимо да теорема важи и за формулу која има n везника.
Посматрајмо формулу F која има n везника. Формула F може имати један од следећих облика:

$$A \wedge B, \qquad A \vee B \qquad \text{или} \qquad A \Rightarrow B.$$

Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка, тј. имамо теореме:

$$\vdash A^p_C \Leftrightarrow A^p_D \qquad \text{и} \qquad \vdash B^p_C \Leftrightarrow B^p_D.$$

Ми ћемо доказати само случај када је формула F облика $A \wedge B$. Случајеви када је F облика $A \vee B$ или $A \Rightarrow B$ доказују се аналогно. Претпоставимо да је формула F облика $A \wedge B$. На основу дефиниције функције униформне замене имамо:

$$F^p_C \text{ је формула } A^p_C \wedge B^p_C \quad \text{и} \quad F^p_D \text{ је формула } A^p_D \wedge B^p_D.$$

За $\vdash B^p_C \Leftrightarrow B^p_D$ и формулу A^p_C важи део (2) ТЕОРЕМЕ 9:

$$\vdash (A^p_C \wedge B^p_C) \Leftrightarrow (A^p_C \wedge B^p_D).$$

Исто тако, за $\vdash A^p_C \Leftrightarrow A^p_D$ и формулу B^p_D важи део (2) ТЕОРЕМЕ 9:

$$\vdash (A^p_C \wedge B^p_D) \Leftrightarrow (A^p_D \wedge B^p_D).$$

Формуле $(A^p_C \wedge B^p_C) \Leftrightarrow (A^p_C \wedge B^p_D)$ и $(A^p_C \wedge B^p_D) \Leftrightarrow (A^p_D \wedge B^p_D)$ су теореме, па на основу дела (7) ТЕОРЕМЕ 7, добијамо да је и формула $(A^p_C \wedge B^p_C) \Leftrightarrow (A^p_D \wedge B^p_D)$ теорема, тј.

$$\vdash F^p_C \Leftrightarrow F^p_D.$$

♢

Наравно, као и у семантичкој верзији најчешћа примена ТЕОРЕМЕ 10 је следећег облика:

ако је формула $C \Leftrightarrow D$ теорема исказне логике, тј. $\vdash C \Leftrightarrow D$,
и у некој формули F неко јављање њене потформуле C заменимо са D,
тада добијемо формулу F' такву да је $F \Leftrightarrow F'$ теорема тј. $\vdash F \Leftrightarrow F'$.

У наредном задатку представићемо особину да су таутологије уопштени закони дистрибутивности као и уопштени Де Морганови закони теореме исказне логике.

Задатак 17 Формуле
уопштени закони дистрибутивности:

$$((\bigvee_{i=1}^n A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^n (A_i \wedge C)) \quad \text{и} \quad ((\bigwedge_{i=1}^n A_i) \vee C) \Leftrightarrow (\bigwedge_{i=1}^n (A_i \vee C))$$

и уопштени Де Морганови закони:

$$(\neg(\bigvee_{i=1}^n A_i)) \Leftrightarrow (\bigwedge_{i=1}^n \neg A_i) \qquad \text{и} \qquad (\neg(\bigwedge_{i=1}^n A_i)) \Leftrightarrow (\bigvee_{i=1}^n \neg A_i)$$

су теореме исказне логике.
Доказ за прву формулу је аналоган доказу да је та формула таутологија (из Задатка 5 у одељку 2.2.3). База индукције: закон дистрибутивности $\wedge$ у односу на $\vee$ је теорема (Задатак 16 из одељка 3.2.2.) Индукцијска претпоставка: $((\bigvee_{i=1}^n A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^n (A_i \wedge C))$ је теорема. На основу особине да је закон дистрибутивности $\wedge$ у односу на $\vee$ теорема, имамо теорему

$$((\bigvee_{i=1}^{n} A_i \vee A_{n+1}) \wedge C) \Leftrightarrow (((\bigwedge_{i=1}^{n} A_i) \wedge C) \vee (A_{n+1} \wedge C)).$$

Формула која је теорема по индукцијској претпоставци и формула $A_{n+1} \wedge C$, на основу дела (3) ТЕОРЕМЕ 9, дају теорему

$$(((\bigvee_{i=1}^{n} A_i) \wedge C) \vee (A_{n+1} \wedge C)) \Leftrightarrow ((\bigvee_{i=1}^{n} (A_i \wedge C)) \vee (A_{n+1} \wedge C)).$$

Из ових теорема, на основу дела (7) ТЕОРЕМЕ 7, добијамо теорему

$$((\bigvee_{i=1}^{n+1} A_i) \wedge C) \Leftrightarrow (\bigvee_{i=1}^{n+1} (A_i \wedge C)).$$

Слично се поступа и у доказима за остале уопштене законе.

Потребна нам је и синтаксна верзија ТЕОРЕМЕ О ДНФ И КНФ. Та особина ће бити формулисана за систем $\mathcal{L}$ исказне логике јер ће тада доказ те особине бити доказ ТЕОРЕМЕ О ДНФ И КНФ у коме се уместо таутологија пише теорема, тј. уместо знака $\models$ пишемо $\vdash$ и уместо особине да су уопштени закони дистрибутивности и уопштени Де Морганови закони таутологије користимо особине из Задатка 17 да су они теореме.

ТЕОРЕМА 11

У систему $\mathcal{L}$ за сваку формулу F постоји бар једна формула F^k у конјунктивној нормалној форми и бар једна формула F^d у дисјунктивној нормалној форми, такве да важи:

$$\vdash F \Leftrightarrow F^k \quad \text{и} \quad \vdash F \Leftrightarrow F^d.$$

ДОКАЗ

Посматрајмо произвољну формулу F. Ако се у формули F појављују везници који нису из скупа $\{\wedge, \vee, \neg\}$, онда их користећи дефиниције везника замењујемо, везницима из скупа $\{\wedge, \vee, \neg\}$. Стога смемо да претпоставимо да је F формула већ таквог облика, тј. у њој се појављују само везници $\wedge$, $\vee$ и $\neg$. Теорему доказујемо индукцијом по броју везника формуле F, броју n.

База индукције, формула F нема везника, $n = 0$. То значи да је формула F неко исказно слово, на пример исказно слово p. Тражене формуле F^k и F^d су само исказно слово p.

Индукцијска претпоставка: теорема важи за сваку формулу F која има мање од n логичких везника.

Докажимо да теорема важи и за формулу која има n везника.
Посматрајмо формулу F која има n везника. Формула F може имати један од следећих облика:

$$A \wedge B, \qquad A \vee B \qquad \text{или} \qquad \neg A.$$

Без обзира на то који од три наведена облика има формула F њене потформуле A и B имају бар један везник мање од формуле F, па за њих важи индукцијска претпоставка: постоје формуле A^k и B^k у конјунктивној нормалној форми и формуле A^d и B^d у дисјунктивној нормалној форми, такве да:

$$\vdash A \Leftrightarrow A^k, \ \vdash A \Leftrightarrow A^d \quad \text{и} \quad \vdash B \Leftrightarrow B^k, \quad \vdash B \Leftrightarrow B^d.$$

Ми ћемо овде дати доказ теореме само у случају када је формула F облика $A \wedge B$. Претпоставимо да је формула F облика $A \wedge B$ и одредимо прво формулу F^k.
Из $\vdash A \Leftrightarrow A^k$ и $\vdash B \Leftrightarrow B^k$, на основу ТЕОРЕМЕ 10, имамо:

$$\vdash (A \wedge B) \Leftrightarrow (A^k \wedge B^k),$$

где су формуле A^k и B^k у конјунктивној нормалној форми. Стога је и формула $A^k \wedge B^k$ у конјунктивној нормалној форми, па је тражена формула F^k баш формула $A^k \wedge B^k$.
Одредимо сада формулу F^d.
Од формула A^d и B^d у дисјунктивној нормалној форми, користећи законе асоцијативности за $\wedge$ и $\vee$ (тј. премештајући заграде), можемо формирати формуле A_1^d и B_1^d у дисјунктивној нормалној форми које су редом уопштетне дусјункције $C_1 \vee ... \vee C_k$ $(k \geq 1)$ и $C_1' \vee ... \vee C_j'$ $(j \geq 1)$, где је свака формула C_i, $1 \leq i \leq k$, и свака формула C_i', $1 \leq i \leq j$, уопштена конјункција. Како су закони асоцијативности за $\wedge$ и $\vee$ теореме (видети Пример 8), онда на основу дела (7) ТЕОРЕМЕ 7 важи:

$$\vdash A^d \Leftrightarrow A_1^d \qquad \text{и} \qquad \vdash B^d \Leftrightarrow B_1^d,$$

а одатле, на основу ТЕОРЕМЕ 10, имамо:

$$\vdash (A^d \wedge B^d) \Leftrightarrow (A_1^d \wedge B_1^d).$$

Из $\vdash A \Leftrightarrow A^d$ и $\vdash B \Leftrightarrow B^d$, на основу ТЕОРЕМЕ 10, имамо:

$$\vdash (A \wedge B) \Leftrightarrow (A^d \wedge B^d).$$

Дакле, на основу дела (7) ТЕОРЕМЕ 7 имамо:

$$\vdash (A \wedge B) \Leftrightarrow (A_1^d \wedge B_1^d).$$

Формула $A_1^d \wedge B_1^d$ је $(C_1 \vee ... \vee C_k) \wedge (C_1' \vee ... \vee C_j')$. Ако потформулу $C_1' \vee ... \vee C_j'$ формуле $A_1^d \wedge B_1^d$ означимо са C', онда је $A_1^d \wedge B_1^d$ формула: $(C_1 \vee ... \vee C_k) \wedge C'$. На основу теореме уопштени закон дистрибутивности $\wedge$ у односу на $\vee$ (видети Задатак 17), имамо теорему:

$$\vdash ((C_1 \vee ... \vee C_k) \wedge C') \Leftrightarrow ((C_1 \wedge C') \vee ... \vee (C_k \wedge C')).$$

Формула са десне стране везника $\Leftrightarrow$ у овој теореми је облика:

$$(C_1 \wedge (C_1' \vee ... \vee C_j')) \ \vee \ ... \ \vee \ (C_k \wedge (C_1' \vee ... \vee C_j'))$$

(јер је C' формула $C_1' \vee ... \vee C_j'$) и ту формулу ћемо означити са F_1. Имамо да се формула F_1 састоји од потформула

$$C_i \wedge (C_1' \vee ... \vee C_j'), \quad 1 \leq i \leq k,$$

повезаних дисјункцијама. Из теореме уопштени закон дистрибутивности $\wedge$ у односу на $\vee$, на основу закона комутативности за $\wedge$, имамо следећу теорему:

$$\vdash (C_i \wedge (C_1' \vee ... \vee C_j')) \Leftrightarrow ((C_i \wedge C_1') \vee ... \vee (C_i \wedge C_j'))$$

за свако i, $1 \leq i \leq k$. У F_1 сваку потформулу $C_i \wedge (C_1' \vee ... \vee C_j')$, $1 \leq i \leq k$, замењујемо формулом $(C_i \wedge C_1') \vee ... \vee (C_i \wedge C_j')$ и добијамо формулу F_2:

$$((C_1 \wedge C_1') \vee ... \vee (C_1 \wedge C_j')) \vee ... \vee ((C_k \wedge C_1') \vee ... \vee (C_k \wedge C_j'))$$

и та формула је у дисјунктивној нормалној форми. На основу ТЕОРЕМЕ 10, имамо:

$$\vdash F_1 \Leftrightarrow F_2.$$

Сада из $\vdash (A \wedge B) \Leftrightarrow (A_1^d \wedge B_1^d)$, $\vdash (A_1^d \wedge B_1^d) \Leftrightarrow F_1$ и $\vdash F_1 \Leftrightarrow F_2$, на основу дела (7) ТЕОРЕМЕ 7, добијамо теорему:

$$\vdash (A \wedge B) \Leftrightarrow F_2.$$

Дакле, тражена формула F^d је формула F_2.

Када је F облика $A \vee B$ или $\neg A$ доказ је аналоган овом доказу.

♢

На крају ево синтаксне верзије ТЕОРЕМЕ 3 из одељка 2.2.3.

ТЕОРЕМА 12

Ако је формула F теорема система $\mathcal{L}$, онда за неко исказно слово p формуле F и произвољну исказну формулу C и формула F_C^p је теорема система $\mathcal{L}$.

ДОКАЗ

Ако је формула F теорема система $\mathcal{L}$, онда постоји доказ формуле F у том систему: F_1,..., F_n $(n \geq 1)$, где је F_n формула F. Ако у свакој од формула F_i, $1 \leq i \leq n$, исказно слово p заменимо формулом C, онда добијамо низ формула ${F_1}_C^p$,..., ${F_n}_C^p$ и формула ${F_n}_C^p$ је F_C^p. Лако се види да је тај низ један доказ у систему $\mathcal{L}$ са последњом формулом F_C^p. Дакле, формула F_C^p јесте теорема система $\mathcal{L}$.

♢

У доказу особине потпуности, тј. да је свака таутологија теорема исказне логике, користићемо особину да је свака таутологија у КНФ теорема исказне логике.

ТЕОРЕМА 13

Нека је формула F у КНФ.

Ако је формула F таутологија, онда је F теорема исказне логике.

ДОКАЗ

Исказну логику ћемо представити системом $\mathcal{L}$. Пошто је формула F у КНФ она је облика $A_1 \wedge ... \wedge A_m$, за неки природан број $m \geq 1$, где су све формуле A_i, $1 \leq i \leq m$, сачињене од литерала повезаних дисјункцијама. Формула F је таутологија, па на основу Задатка 8 из одељка 2.4.2, у свакој од формула A_i, $1 \leq i \leq m$, мора да се јавља неко исказно слово p и његова негација $\neg p$. То значи да од сваке формуле A_i, $1 \leq i \leq m$, можемо премештањем њених литерала (коришћењем закона комутативности и асоцијативности за $\vee$) добити формулу A_i', $1 \leq i \leq m$, облика $(p \vee \neg p) \vee A_i''$, где је p исказно слово које се заједно са својом негацијом $\neg p$ јавља у A_i и формула A_i'' је начињена од преосталих литерала формуле A_i повезаних дисјункцијама. У

Примеру 8 из одељка 3.2.2 показали смо да је произвољна формула облика $A \vee \neg A$ теорема исказне логике. Дакле, формула $p \vee \neg p$ је теорема исказне логике, тј. $\vdash_{\mathcal{L}} p \vee \neg p$. Стога свака од формула A_i', $1 \leq i \leq m$, јесте дисјункција једне теореме и неке формуле A_i'', па на основу дела (3) ТЕОРЕМЕ 7, добијамо да је свака од тих формула A_i', $1 \leq i \leq m$, теорема система $\mathcal{L}$. Како смо за свако i, $1 \leq i \leq m$, формулу A_i' добили из A_i применом закона комутативности и асоцијативности за $\vee$ то, на основу делова (4) и (6) ТЕОРЕМЕ 7, имамо да је и свака формула A_i, $1 \leq i \leq m$, теорема система $\mathcal{L}$:

$$\vdash_{\mathcal{L}} A_1, \quad . \quad . \quad . \quad , \quad \vdash_{\mathcal{L}} A_m.$$

Користећи ове теореме, на основу дела (2) ТЕОРЕМЕ 7 добијамо да је формула $A_1 \wedge ... \wedge A_m = F$ теорема система $\mathcal{L}$, тј. $\vdash_{\mathcal{L}} F$.

♢

ДОКАЗ ТЕОРЕМЕ 6 (ДОКАЗ ПОТПУНОСТИ)

У доказу особине потпуности исказну логику ћемо представити системом $\mathcal{L}$. Претпоставимо да је формула F таутологија, тј. $\models F$. Потребно је доказати да је формула F теорема исказне логике. За формулу F, на основу ТЕОРЕМЕ 11, постоји формула F^k у КНФ за коју важи:

$$\vdash_{\mathcal{L}} F \Leftrightarrow F^k \qquad (*)$$

На основу ТЕОРЕМЕ 5, тј. особине ваљаности, теорема $F \Leftrightarrow F^k$ је и таутологија:

$$\models F \Leftrightarrow F^k.$$

Дакле, имамо да су формуле F и F^k еквивалентне, $F \equiv F^k$, и да је формула F таутологија, па закључујемо да је F^k таутологија. Стога на основу ТЕОРЕМЕ 13, добијамо да је формула F^k теорема исказне логике:

$$\vdash_{\mathcal{L}} F^k.$$

Из $(*)$ на основу дела (5) ТЕОРЕМЕ 7, имамо теорему $\vdash_{\mathcal{L}} F^k \Rightarrow F$.

Коначно, из $\vdash_{\mathcal{L}} F^k$ и $\vdash_{\mathcal{L}} F^k \Rightarrow F$, на основу ТЕОРЕМЕ 8, добијамо $\vdash_{\mathcal{L}} F$, тј. формула F је теорема исказне логике. Закључујемо да свака таутологија мора бити теорема исказне логике, тј. важи особина потпуности:

$$\text{ако је} \quad \models F, \quad \text{онда је} \quad \vdash F.$$

♢

3.2.6 Одлучивост и непротивречност исказне логике

Користећи особину да је исказна формула теорема исказне логике ако и само ако је таутологија, доказаћемо да је исказна логика одлучива и непротивречна формална теорија.

ТЕОРЕМА 14

Формални систем исказне логике, систем $\mathcal{L}$, је одлучив.

ДОКАЗ

За сваку исказну формулу F може се ефективно проверити да ли је таутологија (на пример, методом чишћења). Како је исказна формула теорема исказне логике ако и само ако је таутологија, следи да се за сваку исказну формулу F може ефективно проверити да ли је теорема система $\mathcal{L}$. Дакле, систем $\mathcal{L}$ је одлучив.

♢

ТЕОРЕМА 15

Формални систем исказне логике, систем $\mathcal{L}$, је непротивречан.

ДОКАЗ

Како је исказна формула теорема исказне логике ако и само ако је таутологија, следи да свака формула која није таутологија није ни теорема система $\mathcal{L}$. Дакле, пошто има формула које нису таутологије, онда те формуле нису ни теореме система $\mathcal{L}$, тј. систем $\mathcal{L}$ је непротивречан.

♢

3.2.7 Синтактичка потпуност исказне логике

Можемо се питати следеће: какав систем добијамо ако проширимо систем исказне логике $\mathcal{L}$ неком формулом, тј. ако направимо систем који као аксиоме има аксиоме система $\mathcal{L}$ и још неку формулу која није теорема система $\mathcal{L}$? Одговор на ово питање је да су у тако добијеном систему (без обзира на то која је та додата формула) све исказне формуле теореме.

Опишимо прво потпуно прецизно шта значи проширити неки формални систем $\mathcal{S}$ неком његовом формулом F. То значи да формирамо нови систем $\mathcal{S}'$ са истим скупом симбола, формула и правила извођења као и систем $\mathcal{S}$ само је скуп аксиома система $\mathcal{S}'$, скуп $\mathcal{A}(\mathcal{S}')$, скуп аксиома система $\mathcal{A}(\mathcal{S})$ са додатом формулом F, тј. $\mathcal{A}(\mathcal{S}') = \mathcal{A}(\mathcal{S}) \cup \{F\}$. Важно је истаћи да се под овим додавањем формуле F подразумева да је F једна схема аксиома. Ако, на пример, систем $\mathcal{L}$ проширимо формулом $F = (A \vee B) \Rightarrow (A \Rightarrow B)$, где су A и B произвољне формуле, онда је и $((D \wedge A) \vee (A \Rightarrow C)) \Rightarrow ((D \wedge A) \Rightarrow (A \Rightarrow C))$ једна аксиома система $\mathcal{L}'$ јер је то формула истог облика као F у којој је A формула $D \wedge A$, а B формула $A \Rightarrow C$. Формални систем $\mathcal{S}'$ који је на описани начин направљен од система $\mathcal{S}$ зваћемо проширење система $\mathcal{S}$ формулом F.

Да ли је неки формални систем $\mathcal{S}$ синтактички потпун зависи од његових проширења различитим формулама. Ево дефиниције синтактички потпуног система.

Дефиниција синтактички потпуног формалног система

Нека је $\mathcal{S}$ један формални систем. Ако за сваку формулу F система $\mathcal{S}$, која није теорема тог система, важи да су у проширењу система $\mathcal{S}$ том формулом F, систему $\mathcal{S}_F$, све формуле теореме, онда је систем $\mathcal{S}$ синтактички потпун систем.

Показаћемо да је систем исказне логике $\mathcal{L}$ синтактички потпун систем. Посматрајмо формални систем исказне логике, систем $\mathcal{L}$. Направимо систем $\mathcal{L}'$ који је проширење система $\mathcal{L}$ формулом A која није теорема система $\mathcal{L}$. За системе $\mathcal{L}$ и $\mathcal{L}'$ важи следеће:
(i) Све теореме система $\mathcal{L}$ морају бити теореме система $\mathcal{L}'$. Наиме, ако је нека формула F теорема система $\mathcal{L}$, онда постоји доказ те формуле чија свака формула је или аксиома система $\mathcal{L}$ или закључак правила MP из претходних формула. Аксиоме које се појављују у том доказу су аксиоме и система $\mathcal{L}'$ и MP је правило извођења тог система. Зато тај доказ јесте доказ и у систему $\mathcal{L}'$, па је формула F теорема и система $\mathcal{L}'$.
(ii) Особине које су представљене у ТЕОРЕМАМА 7-12 за систем $\mathcal{L}$ важе и за систем $\mathcal{L}'$. У доказима ТЕОРЕМА 7-12 најважнији аргумент је да од постојећих теорема посматраног формалног система уз помоћ правила извођења правимо нове теореме тог формалног система, а системи $\mathcal{L}$ и $\mathcal{L}'$ имају исто правило извођења.

Користећи ова својства докажимо да је систем $\mathcal{L}$ синтактички потпун.

ТЕОРЕМА 16

Формални систем исказне логике, систем $\mathcal{L}$, је синтактички потпун.

ДОКАЗ

Посматрамо формулу A која није теорема система $\mathcal{L}$. Нека је систем $\mathcal{L}'$ проширење система $\mathcal{L}$ формулом A. У систему $\mathcal{L}$, на основу ТЕОРЕМЕ 11, за формулу A постоји формула A^k у конјунктивној нормалној форми таква да важи:

$$\vdash_{\mathcal{L}} A \Leftrightarrow A^k.$$

Формула A^k је облика $B_1 \wedge ... \wedge B_m$, за неки природан број $m \geq 1$, где су све формуле B_i, $1 \leq i \leq m$, сачињене од литерала повезаних дисјункцијама. Формула A није теорема система $\mathcal{L}$, па на основу особине потпуности, није таутологија. Формула $A \Leftrightarrow A^k$ јесте теорема система $\mathcal{L}$, па је и таутологија: $\models A \Leftrightarrow A^k$. Дакле, имамо да су формуле A и A^k еквивалентне и да A није таутологија, па закључујемо да формула A^k није таутологија. То значи, на основу Задатка 8 из одељка у 2.4.2, да међу формулама $B_1, ..., B_m$ постоји нека формула у којој се не јављају литерали q и $\neg q$ ни за једно исказно слово q (тј. ако се јавља неко исказно слово q, онда се не јавља $\neg q$, и обрнуто). Нека је то формула B_j, за неко j између 1 и m.
Вратимо се сада у систем $\mathcal{L}'$. У сваком формалном систему аксиоме тог система су и његове теореме, стога је и аксиома A система $\mathcal{L}'$ теорема тог система: $\vdash_{\mathcal{L}'} A$. Имамо да је формула $A \Leftrightarrow A^k$ теорема

система $\mathcal{L}$, па је тиме (на основу (i)) теорема и система $\mathcal{L}'$, тј. важи: $\vdash_{\mathcal{L}'} A \Leftrightarrow A^k$. Из те теореме, на основу дела (5) ТЕОРЕМЕ 7 (за систем $\mathcal{L}'$), добијамо теорему: $\vdash_{\mathcal{L}'} A \Rightarrow A^k$. Сада из $\vdash_{\mathcal{L}'} A \Rightarrow A^k$ и $\vdash_{\mathcal{L}'} A$ на основу ТЕОРЕМЕ 8 (за систем $\mathcal{L}'$), добијамо да је A^k теорема система $\mathcal{L}'$:

$$\vdash_{\mathcal{L}'} A^k.$$

Из тога што је A^k теорема система $\mathcal{L}'$, на основу дела (1) ТЕОРЕМЕ 7 (за систем $\mathcal{L}'$) добијамо да је свака формула B_i $(1 \leq i \leq m)$ теорема система $\mathcal{L}'$. Дакле, и формула B_j је теорема система $\mathcal{L}'$:

$$\vdash_{\mathcal{L}'} B_j.$$

Наш циљ је да покажемо да за било које исказно слово p важи: $\vdash_{\mathcal{L}'} p$.
Да бисмо то показали потребно је доказати да важи: $\vdash_{\mathcal{L}'} B_j \Leftrightarrow p$.
На основу особине формуле B_j, скуп исказних слова која су литерали у формули B_j и скуп исказних слова чије негације су литерали у формули B_j су дисјунктни скупови. Зато у формули B_j можемо извршити овакве замене: сваки литерал који је неко исказно слово замењујемо исказним словом p, а у сваком литералу који је негација неког исказног слова то исказно слово замењујемо са $\neg p$. (Да постоји заједнички елемент r поменутих скупова, тј. да се и r и $\neg r$ јављају у B_j, не бисмо могли да урадимо те замене, јер бисмо морали да r заменимо и са p и са $\neg p$.) Резултат тих замена је формула B начињена од p и $\neg\neg p$ повезаних дисјункцијама.
(На пример, ако је формула B_j облика $(s \vee \neg q) \vee (r \vee \neg p)$, тада исказна слова s и r замењујемо исказним словом p, а q и p замењујемо са $\neg p$ и резултат је формула B: $(p \vee \neg\neg p) \vee (p \vee \neg\neg p)$.)
Користећи својство да у $\mathcal{L}$ (а по (i) и у систему $\mathcal{L}'$) важи $\vdash \neg\neg p \Leftrightarrow p$ и $\vdash (p \vee p) \Leftrightarrow p$, вршимо следеће замене.
У формули B сваку њену потформулу $\neg\neg p$ замењујемо са p и добијамо формулу C. Формулу C чине јављања исказног слова p повезана дисјункцијама (l јављања слова p за неко l, $l \geq 1$).
(У нашем примеру формула C је $(p \vee p) \vee (p \vee p)$ и $l = 4$.)
Сада у формули C једну њену потформулу $p \vee p$ замењујемо са p. На тај начин добијамо формулу истог облика као формула C која има $l - 1$ јављања исказног слова p. Наставимо да правимо такве замене (има их укупно $l - 1$) све док не добијемо формулу са једним јављањем исказног слова p, формулу p.
(У нашем примеру првом заменом $p \vee p$ са p у формули C добијамо формулу $(p \vee p) \vee p$, затим $p \vee p$ и на крају p. Имамо три корака замене, тј. $l - 1 = 4 - 1 = 3$.)
На основу ТЕОРЕМЕ 10 (за систем $\mathcal{L}'$), имамо: $\vdash_{\mathcal{L}'} B_j \Leftrightarrow B, \vdash_{\mathcal{L}'} B \Leftrightarrow C$ и $\vdash_{\mathcal{L}'} C \Leftrightarrow p$, па на основу дела (7) ТЕОРЕМЕ 7 (за систем $\mathcal{L}'$), имамо $\vdash_{\mathcal{L}'} B_j \Leftrightarrow p$. Дакле, на основу дела (5) ТЕОРЕМЕ 7 (за систем $\mathcal{L}'$), добијамо $\vdash_{\mathcal{L}'} B_j \Rightarrow p$. Коначно из $\vdash_{\mathcal{L}'} B_j$ и $\vdash_{\mathcal{L}'} B_j \Rightarrow p$, на основу ТЕОРЕМЕ 8 (за систем $\mathcal{L}'$), добијамо:

$$\vdash_{\mathcal{L}'} p.$$

Из $\vdash_{\mathcal{L}'} p$ за произвољну исказну формулу D, на основу ТЕОРЕМЕ 12 (за систем $\mathcal{L}'$), добијамо $\vdash_{\mathcal{L}'} p^p_D$, тј.

$$\vdash_{\mathcal{L}'} D.$$

Дакле, произвољна исказна формула D је теорема система $\mathcal{L}'$. Закључујемо да је формални систем $\mathcal{L}$ синтактички потпун.

$\diamondsuit$

Литература

[1] Баркер, С. *Филозофија математике*, Нолит, Београд, 1973.

[2] Божић, М., Вујић, С. *Математичка логика са елементима опште логике*, Научна књига, Београд, 1980.

[3] Вујошевић, С. *Математичка логика*, ЦИД, Подгорица, 1996.

[4] Gentzen, G. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift* 39, 176-210, 405-431 (English translation in *The Collected Papers of Gerhard Gentzen*, Szabo, M.E. (ed.), North-Holland, 1969)

[5] Дошен, К. *Logic*, у: The Language of Science, Polimetrica, Monza, биће објављено (http://www.mi.sanu.ac.rs/ kosta/Logic.pdf)

[6] Zach, R. *Completeness before Post: Bernays, Hilbert, and the development of propositional logic*, The Bulletin of Symbolic Logic, vol. 5, no. 3, (1999), pp. 331-366.

[7] Јаничић, П. *Математичка логика у рачунарству*, Математички факултет у Београду (Skripta Internacional), Београд, 2004.

[8] Крон, А. *Логика*, Универзитет у Београду (Завод за графичку технику Технолошко-металушког факултета), Београд, 1998.

[9] Mendelson, E. *Introduction to Mathematical Logic*, Van Nostrand Reinho Co., 1964.

[10] Мијајловић, Ж., Марковић, З. и Дошен, К. *Хилбертови проблеми и логика*, Завод за уџбенике и наставна средства, Београд, 1986.

[11] Prawitz, D. *Natural Deduction*, Almquist and Wiksell, Stockholm, 1965.

[12] Прешић, С. *Елементи математичке логике*, Научна књига, Београд, 1980.

[13] Прешић, С. и М. *Увод у математичку логику*, Математички институт, Београд, 1979.

[14] Frege, G. *The Foundations of Arithmetic*, translated by Austin, J. L., Harper and Brothers, New York 1953.

[15] Chiswell, I. and Hodges, W. *Mathematical Logic*, Oxford University Press, 2007.

Индекс појмова

Белешка о аутору

Мирјана Борисављевић дипломирала је на Математичком факултету Универзитета у Београду на смеру математичке структуре и примене. Од јануара до јула 1992. године боравила је на Универзитету у Амстердаму (Institute for Logic, Language and Computation, University of Amsterdam). На Математичком факултету Универзитета у Београду магистрирала је 1994. године, а докторирала 1997. године.

Од 1990. године ради на Саобраћајном факултету у Београду. У марту 2004. године изабрана је у звање ванредног професора Саобраћајног факултета за ужу научну област Математика. Од октобра 2002. године на Економском факултету у Београду ангажована је као наставник на предмету *Математика*. Од јануара 2003. године на Филозофском факултету у Београду, на Одељењу за филозофију, ангажована је за изборни предмет *Математика* (*Историја и филозофија математике*). На истом одељењу академске године 2008/09 држала је курс *Логика*. На смеру Информатика Војне Академије од септембра 2003. до септембра 2007. године предавала је предмет *Математика 5* (*Дискретна математика*). Коаутор је две збирке задатака.

Од 1991. године ангажована је као истраживач-сарадник на научним пројектима Математичког института САНУ. У оквиру научне области математичка логика, бави се теоријом доказа. Са научним саопштењима учествовала је на више домаћих и међународних научних скупова. У домаћим и међународним часописима објавила је више научних радова.