Київський національний університет
імені Тараса Шевченка

В. В. Зубенко
С. С. Шкільняк

ОСНОВИ МАТЕМАТИЧНОЇ ЛОГІКИ

Навчальний посібник

КИЇВ – 2020

УДК 510.51(075.8)
ББК 22.12я73
Ш66

Рекомендовано вченою радою факультету комп'ютерних наук та кібернетики КНУТШ
(протокол № 9 від 22 квітня 2020 року)

Рецензенти:
Ю. В. Крак – член-кор. НАНУ, д-р фіз.-мат. наук,
А. Ю. Дорошенко – д-р фіз.-мат.наук,
С. О. Мащенко – д-р фіз.-мат.наук

Зубенко В.В., Шкільняк С.С.
Ш66 **Основи математичної логіка:** навчальний посібник. К.: НУБіП України, 2020. 102 с.

Викладено основи класичної математичної логіки. Наведено приклади розв'язків типових задач, запропоновано вправи для самостійного розв'язку. Посібник склали матеріали курсів лекцій з математичної логіки та теорії алгоритмів, які читають автори на факультеті комп'ютерних наук та кібернетики КНУ ім. Тараса Шевченка. Він може служити прелюдією для вивчення інших логік, зокрема неокласичної, яка розглядає функції і предикати на даних.

Для студентів освітніх програм «Прикладна математика» та «Системний аналіз».

ISBN 978-617-7878-13-0

ЗМІСТ

ВСТУП

Метою даного посібника є ознайомлення з основами математичної логіки. Якщо поглянути на логіку з загальних позицій, то вона вивчає зв'язки між предметами та явищами. При цьому її цікавить не природа і властивості цих зв'язків (це – предмет окремих наук), а сам факт їх наявності і те, як існування подібних фактів пов'язано між собою. Для відображення предметів та явищ навколишнього світу, а також зв'язків між ними людство створило природні та штучні мови. Для фіксації в них згаданих зв'язків використовуються спеціальні речення – висловлювання, характерні тим, що допускають свою оцінку. Це означає, що за певних умов таке речення можна оцінити, тобто з'ясувати чи має місце той чи інший зв'язок між предметами. Якщо має, то говорять, що воно істинне, якщо – ні, то що воно хибне. Якщо в даний момент (чи взагалі) не створені умови для оцінки висловлювання, то воно вважається невизначеним, беззмістовним. Хиба, істина та невизначеність є прикладом, так званих, істиннісних значень. На практиці зустрічаються логіки з двома, трьома і більшою кількістю істиннісних значень. Наприклад, скінченно-значні логіки з істиннісними значеннями – числами від 1 до n, де n- довільне натуральне число і навіть логіки з континуальною потужністю оцінок, як у випадку ймовірнісних логік. Таким чином, всяка логіка розпочинається з мови і засобів оцінки висловлювань.

Помічено, що між висловлюваннями існують певні відношення в контексті їхніх спільних оцінок. Наприклад, буває, які спільні оцінки не взяти для пари висловлювань, при істинності першого з них завжди і друге істинне, а при хибності першого оцінка другого вже немає значення – воно істинне. Це відношення між висловлюваннями отримало назву "імплікації" або "слідування". Найбільш важливі відношення між висловлюваннями у мовах представлені, так званими, "зв'язками" (з наголосом на першому складі). Ось деякі з них: "не …" (заперечення), "…або…" (диз'юнкція), "…і…" (кон'юнкція), "якщо …, то …" (імплікація), "тоді…і тільки тоді…" (еквіваленція). Враховуючи універсальний характер наведених зв'язок, у формальних мовах для них вводять спеціальні позначення. Ми будемо використовувати для них такі позначення: $\neg, \vee, \&, \rightarrow$ та $\leftrightarrow$ відповідно. Зв'язки можна розглядати як певні композиції на множині висловлювань, за допомогою яких утворюють з даних висловлювань нові, більш складні. Кожна з них фіксує певне відношення між даними висловлюваннями і новим. Так, заперечення висловлювання буде істинним при оцінках, коли воно саме – хибне, диз'юнкція двох висловлювань істина, якщо одне з них чи обидва істинні при спільній оцінці, тощо.

У більш складних випадках, висловлювання може стосуватись не просто окремих предметів, але і їхніх сукупностей. Такі висловлювання мають в своїй структурі загальні поняття (терміни), які представляють ту чи іншу сукупність предметів і щось стверджують про ці предмети. Наприклад, висловлювання "Люди – смертні" та "Всі люди – смертні" містять термін "люди", і означають, що кожна конкретна людина – смертна. Друге висловлювання містить зв'язку "всі люди". Візьмемо висловлювання "Існує дитина віком більше одного року", яке означає, що є принаймні одна конкретна дитина старша одного року. Істинність його залежить від контексту. А саме, від того, яка саме конкретна сукупність осіб пов'язана з терміном "дитина". Якщо мається на увазі все людство, то висловлювання істинне, а якщо мова тільки про дітей в межах певної конкретної молодої сім'ї чи в ясельній групі, то воно може бути хибним. Дане висловлювання містить зв'язку "існує дитина". Нові зв'язки називаються *кванторами* – загальності та підтвердження відповідно. Зазначимо суттєву відмінність кванторів від наведених раніше зв'язок. Оцінка висловлювання з квантором залежить від усіх оцінок конкретних предметів, пов'язаних з терміном. Сукупність цих оцінок може бути, наприклад, нескінченною, як у випадку зв'язки "для всіх натуральних чисел". Знайти оцінку висловлювання з такою зв'язкою емпіричним шляхом просто неможливо – потрібні спеціальні логічні методи[1].

Специфікою природних мов є те, що оцінка висловлювання може залежати від його контексту. Це пояснює, чому на практиці люди нерідко помиляються в своїх оцінках і чому логіка як наука потребує створення спеціальних штучних мов для своїх потреб, а якщо і задовольняється існуючою природною мовою, то не всією, а тільки тим чи іншим її спрощеним фрагментом .

Є ще одна серйозна причина для звернення логіки до штучних мов – це наявність у природних мовах такого явища, як софізми, паралогізми та парадокси. Про їх існування знали ще філософи Давньої Греції. *Софізми* – це міркування, які містять навмисну замасковану помилку. Ось три відомі приклади.

Софізм "Сидячий": "Сидячий встав. Хто встав, той стоїть. Отже сидячий стоїть."

Софізм "Вкритий": "Ти знаєш цього вкритого чоловіка, що спить під стіною ? Не знаю. Але ж це твій батько ! Отже ти не знаєш свого батька ?!"

Софізм "Рогатий": "Те, що ти не втратив, ти маєш. Ти не втратив роги. Отже, ти рогатий."

Звичайно, як і в давні часи, сьогодні теж не бракує не навмисних некоректних міркувань. Такі міркування називаються паралогізмами. Наприклад, "Якщо через дріт пропускають електричний струм, то він нагрівається. Дріт нагрівається. Отже, через нього пропускають

---

[1] Це може стосуватися і скінченних, але "надвеликих" сукупностей оцінок, як у випадку зв'язки "Всі люди".

електричний струм.” Зауважимо, що чіткого розмежування між софізмами і паралогізмами немає. Наприклад, до останніх можна віднести таке міркування:” Усі студенти складають іспити. Микола складає іспити. Отже, Микола – студент.” Ближче до софізму таке міркування:’’ Ссавці населяють сушу й океани. Миші – ссавці. Отже, миші населяють сушу й океани.’’ Про парадокси мова піде далі.

На сьогодні відомо сотні логік, які відрізняються своїми мовами, зв’язками та сукупністю істиннісних значень. Надалі ми будемо розглядати тільки, так звану, *класичну логіку*. Мова L в ній обмежується наведеними вище зв’язками і двозначними оцінками – хиба та істина. Ця логіка найбільш вивчена, охоплює значну частину математики і служить методологічною основою для решти логік.

Центральним відношенням між висловлюваннями з точки зору логіки є відношення семантичного логічного наслідку, яке дозволяє обґрунтовано отримувати з уже встановлених істинних фактів нові істинні факти (умовисновки в L).

Висловлювання B є *семантичним логічним наслідком* висловлювань $A_1,...,A_n$ ($A_1,...,A_n \models B$), якщо для всіх спільних оцінок висловлювань $A_1,...,A_n,B$ висловлювання B завжди істинне, при умові, що всі A_i істинні. Висловлювання A_i і B називаються тут відповідно *посилками* і *висновком,* Таким чином, якщо між деякими висловлюваннями має місце логічний наслідок, то істинність його посилок гарантує істинність і того факту, який представлено у висновку. У випадку, коли сукупність посилок – порожня, відношення $\varnothing \models B$ означає, що висловлювання B істинне при всіх оцінках. Цей факт записується $\models B$.Такі висловлювання називаються *всюди істинними* і є логічними наслідками будь-якої сукупності висловлювань.

Нехай S та R – певні сукупності висловлювань та усюди істинних висловлювань відповідно. Перші назвемо гіпотезами, а другі аксіомами і нехай B– довільне висловлювання. Ланцюжок висловлювань, який закінчується B і кожне з яких є або гіпотезою, або аксіомою, або семантичним логічним наслідком деяких попередніх висловлювань ланцюжка, називається *семантичним виведенням* висловлювання B з гіпотез та аксіом. Нескладно переконатись, що $S \models B$, тобто B є логічним наслідком гіпотез з S. Це випливає з того, що відношення логічного наслідку – транзитивне, тобто якщо $A_1,...,A_n \models B_i \quad i=\overline{1,k}$, і $B_1,...,B_k \models C$ то $A_1,...,A_n \models C$. Семантичні виведення з гіпотез та аксіом вказують шлях для отримання логічно обґрунтованих умовисновків у мові L.

Довільне відношення між висловлюваннями називається *коректним,* якщо воно гарантує наявність між ними семантичного логічного наслідку. Відразу зазначимо, що мова йде про формальне відношення між висловлюваннями як синтаксичними об’єктами. Вочевидь, конкретні коректні відношення можуть використовуватися для побудови семантичних виведень у мові L. Будемо називати їх *формальними правилами виведення*. Якщо семантичне логічне виведення висловлювання B з гіпотез S та аксіом R побудовано за участі тільки формальних правил виведення з певної їх сукупності P, то таке виведення будемо називати *формальним доведенням* і позначати $\vdash_P$ або $\vdash$, якщо сукупність P не суттєва чи зафіксована.

У зв'язку з формальними правилами виведення виникає ряд важливих питань. 1) Які конкретно формальні правила виведення існують у даній мові L? 2) Скільки їх, як їх можна описати ? 3) Як можна обґрунтувати даний логічний наслідок у мові L і чи завжди це можна зробити шляхом доведення з певних гіпотез та аксіом за допомогою тих чи інших формальних правил виведення? 4) Як обґрунтувати істинність висловлювання B, коли воно істинне тільки частково, тобто не при всіх оцінках? 5) Питання 1)-3) можна ставити не для однієї конкретної мови, а для усіх мов з однаковим синтаксисом, які відрізняються тільки своїми інтерпретаціями. Будемо називати такі мови *однотипними*. У цьому випадку семантичний наслідок між висловлюваннями буде мати місце, коли він має місце у кожній з однотипних мов. Це ж стосується і коректності формальних правил виведення. Вони мають бути коректними у кожній з мов. Подібні семантичні наслідки та правила виведення будемо називати *універсальними*. 6) Чи існує загальна ефективна процедура для обґрунтування: а) довільного семантичного наслідку у мові L, б) довільного універсального семантичного наслідку для мов типу L? Останні питання є важливими для розробки систем штучного інтелекту і інформаційних технологій.

Повні відповіді на дані та інші питання дає математична логіка – наука, яка вивчає формальні моделі логічних суджень, якими користуються математики і ми їх отримаємо далі. Але наявність зв'язок у мові L дозволяє сказати дещо суттєве вже наразі.

Візьмемо перше питання. Таких формальних правил виведення багато. Ось деякі з них. Правило розширення: $A \vdash B \vee A$, правило відокремлення (modus ponens): $A, A \rightarrow B \vdash B$, правило перетину: $A \vee B$, $\neg A \vee C \vdash B \vee C$ та інші. Нескладно перевірити, що ці правила коректні, тобто із істинності усіх висловлювань в лівих частини правил завжди випливає істинність висловлювань і в правих. Наприклад, візьмемо результат правила перетину $B \vee C$ і розглянемо перше з висловлювань зліва – $A \vee B$, припустивши, що воно істинне. Це означає, що або A істинне, або B, або вони обидва істинні. Нехай оцінка B істина, тоді результат перетину буде істинний, тому що B частиною його диз'юнкції. Візьмемо друге з висловлювань зліва $\neg A \vee C$ Нехай тепер A істинне. Тоді висловлювання $\neg A$ – хибне і щоб ця диз'юнкція була істинною необхідно, щоб висловлювання C було істинним. Тоді результат перетину знову буде істинним, тому що C

є його частиною. Зазначимо, що наведені правила виведення є універсальними.

Що стосується другого питання. Розглянемо довільне правило виведення $A_1,...,A_n \vdash B$. Воно коректне, тому що за означенням має місце логічний наслідок $A_1,...,A_n \models B$, який виконується тоді, і тільки тоді, коли імплікація $A_1 \wedge ... \wedge A_n \to B$ всюди істинна, тобто має місце $\models A_1 \wedge ... \wedge A_n \to B$. Таким чином, друге питання зводиться до третього. Якщо вдасться описати усі всюди істинні формули мови L, то залишиться вибрати серед них імплікації.

Щодо третього питання. У більшості мов L кількість оцінок, які потрібно розглянути для встановлення довільного логічного наслідку $A_1,...,A_n \models B$, якщо й скінченна, то надмірно велика, навіть для сучасних комп'ютерів. Як правило ж, вона нескінченна, тому емпіричні переборні методи обґрунтування логічного наслідку просто не працюють. Отже, природньо напрошується вихід – вибрати певну сукупністю достатньо простих аксіом і правил виведення і намагатися формально довести всюди істинність імплікації $\models A_1 \wedge ... \wedge A_n \to B$. Система аксіом разом з правилами виведення називається *численням*. Ідеально було б вибрати одне таке числення так, щоб можна було довести: а) будь-який логічний наслідок у мові L і б) будь-який універсальний логічний наслідок. Такі числення отримали назву *повних*. Є мови, в яких остання пропозиція не може бути реалізована, тобто не завжди можна довести довільний логічний наслідок, якщо зафіксувати ті чи інші розумні сукупності аксіом, правил виведення та допустимих оцінок. Тому на практиці використовуються неповні числення, але потужні настільки, що можна сподіватися на потрібні нам конкретні доведення. Про плідність такого аксіоматичного підходу свідчить багатий досвід математики.

Розглянемо четверте питання. План може бути наступним. Знайти умови для деяких (чи всіх!) оцінок, при якій висловлювання B істинне. Нехай ці умови задаються висловлювання $A_1,...,A_n$. Тоді має бути логічний наслідок $A_1 \vee ... \vee A_n \models B$, який слід обґрунтувати певним доведенням.

Що стосується п'ятого пункту, то відповідь на питання 1)-3) позитивна, тобто універсальні системи числення існують. Відповідь на питання пункту 6) негативна як і для більш-менш розвинених конкретних мов L, так і для універсальних систем. Щоб цю відповідь математично обгрунтувати, потрібно формалізувати як мови L певного типу, так і поняття ефективної процедури.

Перелік тільки вже наведених питань пояснює, чому відношення логічного наслідку та методи його обгрунтування є відправними пунктами багатьох досліджень класичної логіки та теорії алгоритмів.

Як ми вже сказали, метою нашого курсу є ознайомлення з основами математичної логіки (МЛ) і, зокрема, пошук відповідей на питання 1)-6).

Специфікою математичної логіки є не тільки те, що вона вивчає моделі математичного мислення, а й те, що вона спирається при цьому на математичні методи. Цим пояснюється і вибір мов для формулювання математичних висловлювань. Вони мають бути формальними. І вони не просто формальні, а ще й будуються індуктивним способом. Це означає, що спочатку вибирається алфавіт мови і вводиться кілька первинних понять, а всі інші поняття визначаються з них шляхом застосування деяких строгих правил (фактично операцій). Така індуктивна структура понять дозволяє зручно оперувати ними як математичними об'єктами. Зокрема, доводити їхні властивості методом загальної індукції. Центральне поняття формальних логічних мов – формула, яка представляє в них математичні висловлювання.

Об'єктом досліджень МЛ є *логічні системи*, які складаються з синтаксису формальної мови L, її семантики і числення. *Синтаксис* описує усі правильні конструкції мови, зокрема сукупність усіх формул. *Семантика* задає правила для оцінки формул і конкретизує поняття всюди істинної формули і відношення логічного наслідку. Для цього вводиться поняття інтерпретації мови. При інтерпретації кожна з синтаксичних конструкцій мови отримує певне конкретне значення, а формула – відповідне істиннісне значення. *Числення* задає певну аксіоматичну систему (сукупність аксіом і правил виведення) для формального доведення істинності формул і логічних наслідків в системі.

Основну увагу в посібнику ми приділимо двом класичним логікам – пропозиційній і логіці першого порядку. Ці логіки створюють підґрунтя для вивчення, зокрема, неокласичних логік, орієнтованих на представлення функцій і предикатів на даних [12-17].

З історії розвитку класичної математичної логіки

Поширення в соціумі софізмів та паралогізмів привернуло увагу до необхідності аналізу та вивчення правил логічних міркувань. Це зумовило суспільний запит на появу логіки як науки про закони мислення. Запит активно підживлювався з боку філософів, яких цікавив пошук універсальних методів обгрунтувань висловлювань. Слід враховувати, що на той час філософія (=натурфілософія) та математика співіснували в нерозривному взаємозв'язку.

Зародження логіки відносять до 6 ст. до н.е. і пов'язують з діяльністю філософів іонiської школи, основоположником якої був *Фалес Мілетський* (625-547 рр. до н.е.). Він вперше довів деякі математичні твердження: діаметр ділить коло навпіл, кути при основі рівнобедреного трикутника – рівні.

Принципово новим було те, що для їхнього обгрунтування пропонувалися не дані емпіричних спостережень, а логічні доведення. Важливий крок в становленні логіки й математики зробив славнозвісний Піфагор (570-500 рр. до н.е.) та його учні, які вивели низку досить складних математичних тверджень суто логічним шляхом. Досить згадати теорему Піфагора, доведення існування ірраціональних чисел. Останній факт в принципі не може бути отриманий емпіричним шляхом. Загальні принципи логічних міркувань розвинув *Платон* (427-347 рр. до н.е.). Основоположником же логіки як цілісної науки, її батьком випало стати його учню – *Арістотелю* (384 – 322 рр. до н.е.). Саме він сформулював три основні закони логіки (тотожності, несуперечливості та виключення третього), розробив аксіоматичний метод, запропонував першу формально-аксіоматичну систему логіки – силогістику, заклав основи модальної логіки. Силогістика є піонерською роботою в галузі формальної логіки, яка базується на виведеннях за формальними правилами, які спираються тільки на структуру посилок, абстрагуючись від конкретного їхнього змісту. Після Аристотеля у розвитку логіки був затяжний період "затишку" (більше 1.5 тис. років). Перший з нових кроків був пов'язаний з іменем Р.Луллія (1235-1315), який запропонував ідею механізації виведення Арістотелевих силогізмів. І хоч йому не вдалося повністю реалізувати свою ідею – її можна вважати піонерською у галузі сучасного штучного інтелекту. З наступних зазначимо кроки зроблені Ф.Беконом (1561-1626) та Р.Декартом (1596-1650). Перший розвинув індуктивний метод обгрунтування математичних тверджень, а другий – дедуктивний метод. Ці роботи були в руслі пошуку універсальних методів доведень. Визначний крок у цьому напрямку зробив Г.Лейбніц (1646-1716), який запропонував ідею створення універсального логічного числення. Ця ідея далеко випередила свій час і саме вона фактично привела до виникнення МЛ як математичної дисципліни у 19 ст.

Першу завершену систему власне математичної логіки на базі строгої логіко-математичної мови (алгебри логіки) запропонував *Дж.Буль* (1815–1864). Основи МЛ закладали А. де Морган (1806-1873), Е.Шредер (1845-1902), П.Порецький (1846-1907), Ч.Пірс (1839-1914). Логіко-математичні мови і теорія їх смислу розвинуті в роботах *Г.Фреге* (1848–1925), який ввів поняття предикату і кванторів. Це дозволило застосувати логічні засоби для дослідження основ математики. Виклад цілих розділів математики мовою МЛ та аксіоматизація арифметики зроблені *Дж.Пеано* (1858–1932). Була навіть зроблена грандіозна спроба *Г.Фреге* та *Б.Рассела* (1872–1970) взагалі звести всю математику до МЛ. Вона не досягла основної мети, але привела до створення багатого логічного апарату, без якого оформлення МЛ в повноцінний розділ математики було б неможливе.

Величезним поштовхом для розвитку МЛ стало відкриття на межі 19–20 ст. парадоксів, пов'язаних з теорією множин. *Парадокс* – це логічно правильне міркування, яке приводить до суперечливих висновків. На той час вся математика стрімко переходила на теоретико-множинну платформу і ці парадокси спричинило великий переполох і навіть цілу “кризу” в середині математичної спільноти.

Парадокси як такі відомі ще з античних часів. Наприклад, парадокс “Брехуна” в стислій формі виглядає так: “Я брешу.” Якщо той, хто це проголошує, говорить правду, то він бреше, а коли він при цьому бреше, то говорить правду. Парадокс ”Перукара”: ”В одному селищі перукар зобов'язаний голити тих, і тільки тих, хто не голиться сам. Що йому робити з собою ? Якщо він поголить себе сам, то немає цього робити. Якщо ж він себе не поголить, то має це зробити.”

Найвідомішими парадоксами теорії множин є парадокси Г.Кантора та Б.Рассела. Перший полягає в наступному. Нехай M – множина всіх множин, а $B(M)$ – сукупність всіх його підмножин. Нехай $\overline{M}$ та $\overline{B(M)}$ – їхні потужності. За теоремою Кантора $\overline{M} < \overline{B(M)}$. З іншого боку, $B(M) \subseteq M$ і $\overline{B(M)}$ $\leq \overline{M}$. Маємо протиріччя. Другий парадокс пов’язаний з нормальними множинами. Множина нормальна, якщо вона не є елементом себе. Нехай S - множина усіх нормальних множин. Чи буде вона сама нормальною ? Якщо $S \notin S$, то вона нормальна і має належати S. Якщо ж $S \in S$, то вона не нормальна і не має належати S.

Для виходу математики з кризи *Л.Брауер* (1881–1966) висунув інтуїціоністську програму, в якій запропонував відмовитися від актуальної нескінченності та логічного закону виключеного третього, вважаючи допустимими в математиці тільки конструктивні доведення. Інший шлях запропонував німецький математик *Д.Гільберт* (1862–1943), який виступив з програмою обгрунтування математики на базі МЛ. Програма Гільберта передбачала побудову формально-аксіоматичних моделей у вигляді формальних систем для основних розділів математики та подальше доведення їх несуперечливості надійними фінітними засобами. Несуперечливість означає неможливість одночасного виведення деякого твердження та його заперечення. Математична теорія, несуперечливість якої хочемо довести, стає предметом вивчення певної математичної науки, яку Д.Гільберт назвав *метаматематикою*. На жаль, *К.Гьодель* (1906–1978) показав, що програма Гільберта не може бути реалізована сповна. Це випливає із його знаменитих теорем про неповноту, які засвідчують принципову обмеженість формально-аксіоматичного методу. Він довів, що несуперечливість кожної досить багатої формальної теорії не може бути доведена засобами самої теорії. Проте існують досить переконливі доведення несуперечливості багатьох теорій (наприклад, тієї ж формальної арифметики) іншими способами.

В науці, техніці та в повсякденному житті важливу роль відіграють дії “механічного” характеру, призначені для отримання за вхідними даними певного результату. Для опису подібних дій використовують спеціальні інструкції, які називають процедурами, протоколами або алгоритмами. Ми будемо розрізнювати ці поняття. Про *алгоритми* та *протоколи* будемо говорити, коли мова йде про певні конкретні відомі процедури чи протоколи (алгоритм Евкліда для знаходження найбільшого спільного дільника двох натуральних чисел, алгоритм поділу відрізка навпіл за допомогою циркуля і лінійки, протокол взяття аналізу на біохімію крові тощо) або більш загально, коли процедури описані в спеціальних формальних мовах. Описи алгоритмів в таких мовах обов'язково скінченні. Видатним досягненням МЛ було створення в 30-х роках 20 ст. перших спеціальних формальних мов для подання алгоритмів і математичне уточнення тим самим поняття алгоритму та алгоритмічно обчислюваної функції (АОФ). Першими формальними класами алгоритмів були машини Поста і Тьюрінга (1936-1937) (які виникли незалежно і були фактично однакові, але сьогодні відомі як машини Тюрінга), першими ж формально описаними класами АОФ – λ– обчислювані (А.Чорч,1936) та частково-рекурсивні (С.Кліні, 1936) функції.

Математичне уточнення поняття алгоритму дало можливість строго поставити питання про не існування алгоритму для розв'язку тих чи інших задач, що до цього було неможливо. Подібні задачі отримали назву *масових алгоритмічних проблем*. Для постановки такої проблеми потрібно конструктивно задати певну множину елементів M і певну її власну підмножину $M_0 \subset M$. Конструктивно означає, що має бути алгоритм для породження усіх елементів даної множини. Характеристичною функцією підмножини $M_0 \subset M$ називається функція $\chi_{M_0}(x) = \begin{cases} 1, x \in M_0, \\ 0, x \in M \setminus M_0. \end{cases}$

Множина M_0 називається *алгоритмічно розв'язною* (або просто розв'язною), якщо існує алгоритм для обчислення значень її характеристичної функції $\chi_{M_0}(x)$. Частковою характеристичною функцією множини $M_0 \subset M$ називається функція $\overline{\chi}_{M_0}(x)$, яка приймає значення 1 для $x \in M_0$ і невизначена для решти x. Множина M_0 називається *частково розв'язною,* якщо існує алгоритм для обчислення значення її часткової характеристичної функції $\overline{\chi}_{M_0}(x)$. Такий алгоритм за скінченну кількість кроків буде видавати результат 1 і працювати нескінченно на елементах, де часткова характеристична функція не визначена. Масові алгоритмічні проблеми пов'язані з питанням чи буде певна підмножина $M_0 \subset M$ розв'язною (не розв'язною) або частково розв'язною (частково нерозв'язною). Зазначимо, якщо відмовитись від конструктивності M_0, то існування алгоритмічно нерозв'язних проблем, очевидне, адже всіх алгоритмів (як скінченних об'єктів) тільки злічена кількість, а всіх підмножини, наприклад, множини N- континуум. Прикладами масових проблем є: 1) проблема розпізнавання чи буде трикутник зі сторонами a,b,c - натуральними числами – прямокутним, 2) чи буде довільне натуральне число n: а) простим, б) числом Гольдбаха тощо. Проблеми 1) та 2а) є розв'язними, проблема 2б) – відкрита. З останньою пов'язані, фактично, дві різні відкриті проблеми – масова і математична. У першій мова йде про існування алгоритму для пошуку двох простих чисел, які в сумі дадуть дане довільне натуральне число, а в другій – тільки про сам факт існування таких чисел для довільного натурального числа.

Однією з перших була математично доведена алгоритмічна нерозв'язність проблем самозастосовності та зупинки машин Тьюрінга. Потім була встановлена алгоритмічна нерозв'язність та часткова нерозв'язність великої кількості інших проблем математичної логіки, дискретної математики та алгебри. Наведемо три найбільш гучні алгоритмічно нерозв'язні проблеми: перевірка всюди істинності формул 1-го порядку (А. Чорч, 1936), проблема тотожності слів в групах (П.С. Новиков, 1955) та знаменита 10-та проблема Гільберта про розв'язність діофантових рівнянь в цілих числах (Ю.В. Матиясевич, 1970). Всі вони виявилися алгоритмічно не розв'язними (проте алгоритмічно розв'язними частково).

Сьогодні теорія алгоритмів під впливом конструктивної гілки математики та в зв'язку з бурхливим розвитком інформатики отримала нові виклики, відокремилась від МЛ і розвивається вже як окремий розділ математики.

І на завершення розділу зазначимо, що математична логіка та її методи лежать в основі формування сучасної наукової картини світу та наукового світогляду. У цьому полягає її світоглядне значення. Але що особливо важливо, надаючи потужні методи й засоби для наукового пізнання світу, математична логіка водночас досліджує і принципові обмеження цих можливостей в умовах існуючих парадигм. І в цьому її особлива цінність.

Розділ І. ПРОПОЗИЦІЙНА ЛОГІКА

Як ми вже сказали, метою нашого курсу є ознайомлення з основами математичної логіки (МЛ). Специфікою МЛ є не тільки те, що вона вивчає моделі математичного мислення, а й те, що вона спирається при цьому на математичні методи. Цим пояснюється і вибір мов для формулювання математичних висловлювань. Як зазначалося у Вступі, вони мають бути формальними і базуються на індуктивних означеннях. *Індуктивне означення* (ІО) множини M має наступну структуру:

(Б) База. Фіксується певна множина складових елементів. Деякі ж елементи апріорі покладаються такими, що належать M .

(І) Індуктивний перехід. Визначено коло індуктивних правил, які за елементами з M та складовими базовими елементами дозволяють будувати нові складені елементи цієї множини.

(П) Повнота. Множину M складають усі її базові та складені елементи і тільки вони.

За означенням, складові елементи з бази (Б) не належать M (не плутати їх з складеними елементами). У більшості випадків їхня сукупність порожня. Така структура елементів множини M дозволяє зручно оперувати ними як математичними об'єктами. Зокрема, доводити їхні властивості методом загальної (структурної) індукції:

(Б) Спочатку перевіряють, чи виконується дана властивість $P(x)$ для базових елементів, які належать множині M.
(І) Потім показують, що індуктивні правила зберігають властивість $P(x)$.
(П) Стверджується, що $P(x)$ виконується для всіх елементів множини M .

Більш детально про індуктивні означення та метод структурної індукції див. 2.2.

В класичній пропозиційної логіці (ПЛ) всі висловлювання розглядаються виключно на рівні структур, пов'язаних із уже згадуваними зв'язками – запереченням, імплікацією, диз'юнкцією, кон'юнкцією та еквівалентністю, а первинні висловлювання не структуруються і представлені просто певними абстрактними іменами. Елементи ПЛ присутні у всіх природних та більшості штучних мов різного призначення.

1.1. Синтаксис

Всяка формальна мова L починається з упорядкованого алфавіту $\mathrm{A} = \{a, b, ...\}$ і складається з синтаксично правильно побудованих слів у цьому алфавіті. *Словами* в алфавіті A називаються скінченні послідовності символів, тобто відображення вигляду $e : 1..n \to \mathrm{A}$, де $n \geq 0$ називається довжиною слова e і позначається $|e|$. Нехай $e(1) = a_1, ..., e(n) = a_n$, тоді слово

e подається як звичайно $a_1...a_n$. Наприклад, вираз $a \vee b$ представляє слово $e(1)=a, e(2)=\vee, e(3)=b$. Слово ε довжини 0 називається порожнім. Зазначимо, що при такому поданні слів символ a і однобуквене слово a подаються однаково, але це різні об'єкти. Сукупність всіх слів в алфавіті W позначається W^*. Отже, мова L є певною підмножиною слів з сукупності W^*. *Конкатенацією* $u \circ v$ слів u,v називається слово uv. Кожне слово однозначно розкладається на конкатенацію окремих однобуквених слів. Операція конкатенації є асоціативною, тому алгебра Fs $=(W^*, \circ, \varepsilon)$ є напівгрупою[2], в якій константа ε є одиницею. Визначимо на словах в алфавіті W відношення лексикографічного ($\prec$) та квазілексикографічного порядку ($\lhd$). Для слів u,v: (1) $\varepsilon \prec v$ для $v \neq \varepsilon$, (2) $xu \prec yv$ для $x,y \in A$ і $x<y$, (3) $xu \prec xv$ для $x \in A$ і $u \prec v$ та $u \lhd v$, якщо (1) $|u|<|v|$ або (2) $|u|=|v|$ і $u \prec v$.

Мова ПЛ дуже проста. Її алфавіт A складають пропозиційні змінні сукупності $V=\{x, y,...x_1, y_1,...\}$, зв'язки заперечення $\neg$ та диз'юнкції $\vee$, а також пара службових символів-дужок (,). Множина *пропозиційних формул* визначається індуктивно. (Б) Базові формули представлені пропозиційними змінними. Символи-зв'язки та дужки є базовими складовими формул. (І) Всі інші формули індуктивно задаються за допомогою зв'язок. А саме, якщо Φ і Ψ – формули, то слова $(\neg\Phi)$ і $(\Phi \vee \Psi)$ є формулами. (П) Інших пропозиційних формул немає. Формули Φ і Ψ називаються *підформулами* нових формул. Також підформулами нових формул будуть і всі їхні власні підформули. Таким чином, слова x і $(x \vee (\neg y))$ – пропозиційні формули, а слово $x \vee y$ – ні, тому що відсутні зовнішні дужки. У другій формулі підформулами є формули $x, (\neg y)$.

При вивченні мов (мов-об'єктів) використовують *метамови*. Їхня мета – спростити (скоротити) подання деяких конструкцій мови-об'єкту, а з іншого боку, ще й, можливо, придати їм певний особливий смисл. Головна вимога до метаконструкцій – простота й швидке та однозначне відновлення синтаксичного об'єкта, який вони представляють. В зв'язку з цим зробимо наступне зауваження. Труднощі, які виникають з розумінням того чи іншого математичного твердження чи його доведення, нерідко обумовлені нерозумінням до кінця системи первинних означень та позначень. Тому, коли виникає така проблема, потрібно спочатку повернутись до метамови та відповідних формальних означень, а вже потім до самої логіки доведення.

Означення деяких метамовних конструкцій будемо явно задавати в такому вигляді:

[2] Free semigroup (анл.) – вільна напівгрупа.

“метаконструкція”$\equiv$”конструкція мови-об’єкту”, де символ $\equiv$ означає синтаксичну рівність.

В метамові ПЛ у формулах опускаються зовнішні дужки, а поряд із основними зв’язками вводяться метазв’язки: *кон'юнкція* &, *імплікація* $\rightarrow$ та *еквіваленція* $\leftrightarrow$. Таким чином, запис $x \vee y$ у метамові є коректним. Для довільних формул Φ і Ψ їхня кон'юнкція $\Phi \& \Psi$, імплікація $\Phi \rightarrow \Psi$ та еквіваленція $\Phi \leftrightarrow \Psi$ визначаються наступним чином: $\Phi \& \Psi \equiv \neg(\neg\Phi \vee \neg\Psi)$, $\Phi \rightarrow \Psi \equiv (\neg\Phi \vee \Psi)$ та $\Phi \leftrightarrow \Psi \equiv (\Phi \rightarrow \Psi \& \Psi \rightarrow \Phi)$. Підформулами даних метаформул називаються формули Φ і Ψ і усі їхні власні підформули. В імплікації підформула Φ називається посилкою, а Ψ - висновком. Смислове навантаження введених метазв’язок стане зрозумілий із їхньої семантики.

Для скорочення формул використовується наступний пріоритет зв’язок і метазв’язок: $\neg, \vee, \&, \rightarrow, \leftrightarrow$. Це означає, що відновлення пропущених дужок у словах розпочинається з підформул заперечення, потім – кон’юнкції і далі за списком. Наприклад, метаформула $\neg\, \Phi \rightarrow \Psi \& \Psi \vee \Phi$ скорочено представляє формулу $((\neg\, \Phi) \rightarrow ((\Psi \& \Psi) \vee \Phi))$.

У запис формул та в ланцюжки їхніх перетворень будемо вставляти *коментарі* вигляду “ --[коментар]”, які не впливають на інтерпретацію формул, але полегшують зрозуміти смисл формули чи її частини. Коментар відноситься до всього слова з початку поточного рядка тексту. Подібні коментарі не мають здивувати математиків та програмістів, знайомих з мовами програмування. Наприклад, коментар в записі метаформули $abd \prec ac \prec acc$:

$abd \prec ac \prec$ --[$b < c$]

$\prec acc$

містить факт, який пояснює, чому друге слово старше від першого .

1.2. Семантика

Щоб задати семантику ПЛ, потрібно спочатку проінтерпретувати основні символи її алфавіту. Істиннісні значення ПЛ – істину та хибу – будемо скорочено позначати 1 та 0. Покладемо $B = \{0,1\}$. *Інтерпретацію* пропозиційних символів задає відображення $I : V \rightarrow B$. Основні зв’язки трактуються як певні операції на істиннісних значеннях: $\neg 1 = 0, \neg 0 = 1, (0 \vee 0) = 0, (1 \vee 0) = (0 \vee 1) = (1 \vee 1) = 1$. Тоді з означення метазв’язок випливає, що кон'юнкція $(x \& y)$ істинна тільки у випадку $x = y = 1$, на решті наборах вона хибна. Імплікація $(x \rightarrow y)$ хибна тільки у випадку $x = 1$, $y = 0$, на решті наборах вона істинна. Еквіваленція $(x \leftrightarrow y)$ істинна тільки у випадку $x = y$, на решті наборах хибна.

Інтерпретація складених формул спирається на їхнє індуктивне означення. Позначимо Φ^I значення формули Φ при інтерпретації I. Тоді за означенням, для довільних формул Φ і Ψ: $(\neg\Phi)^I = \neg(\Phi^I)$, $(\Phi \vee \Psi)^I = \Phi^I \vee \Psi^I$, $(\Phi \& \Psi)^I = \Phi^I \& \Psi^I$, $(\Phi \to \Psi)^I = \Phi^I \to \Psi^I$, $(\Phi \leftrightarrow \Psi)^I = \Phi^I \leftrightarrow \Psi^I$.

Наприклад, знайдемо значення формули $\neg x \to x \vee y \leftrightarrow z$ при інтерпретації $I : x^I = 1, y^I = 0, z^I = 1$.

Маємо $(\neg x \to x \vee y \leftrightarrow z)^I = (((\neg x) \to (x \vee y)) \leftrightarrow z)^I =$ $= (((\neg x^I) \to (x^I \vee y^I)) \leftrightarrow z^I) = (((\neg 1) \to (1 \vee 0)) \leftrightarrow 1) = ((0 \to 1) \leftrightarrow 1) = (1 \leftrightarrow 1) = 1$.

Тепер подивимося, як виглядає в ПЛ центральне відношення для обґрунтування істинності формул – відношення *логічного наслідку* $\models$. Це відношення між формулами Φ і Ψ має місце ($\Phi \models \Psi$), якщо для будь-якої інтерпретації I: $(\Phi \to \Psi)^I = 1$, тобто , якщо посилка Φ^I при інтерпретації I істинна, то і висновок Ψ^I також істинний. Нагадаємо, що запис $\models \Psi$ означає всюди істинність Ψ. В ПЛ всюди істинні формули називаються *тавтологіями*. Таким чином, логічний наслідок $\Phi \models \Psi$ має місце тоді і тільки тоді**,** коли імплікація $(\Phi \to \Psi)$ є тавтологією. Формула є *суперечністю*, якщо її заперечення є тавтологією.

Лема 1.1. Проблеми тавтологічності та суперечливості довільної пропозиційної формули Φ є розв’язними.

►Для перевірки чи є формула Φ тавтологією існує проста процедура. Нехай в Φ n пропозиційних змінних. Кількість попарно різних інтерпретацій цих змінних дорівнює 2^n. Значення всіх інших пропозиційних змінних мови не впливає на значення формули Φ. Для кожної такої інтерпретації потрібно знайти значення формули і якщо всі вони істинні, то формула є тавтологією, якщо ж це не так, то формула – не тавтологія. Щоб ця процедура стала алгоритмом, її потрібно описати формально. На даному етапі нам достатньо і такого опису.

Розв’язність проблеми суперечливості зводиться до розв’язності проблеми тавтологічності формул.◄

Недоліком даної процедури є її експоненентна часова складність.

Метод редукції. Формула *спростовна*, якщо існує інтерпретація на якій вона хибна. Аналогічно, формула *виконувана*, якщо існує інтерпретація на якій вона істинна. Щоб перевірити чи є формула Φ тавтологією, достатньо з’ясувати чи є вона спростовною.

Для перевірки спростовності (виконуваності) формул нам знадобиться поняття, так званого, модифікованого дерева Канторовича для формул.

Звичайне *дерево Канторовича* $D(\Phi)$ для пропозиційної формули Φ визначається індуктивно. (Б) Пропозиційним змінним відповідає дерево, яке складається тільки з кореня, зваженого даною змінною. (І) Якщо формула має вигляд $\neg\Phi$, то в корені дерева міститься зв'язка $\neg$, а його єдиним піддеревом є дерево для підформули Φ. Якщо формула має вигляд $\Phi \vee \Psi$, то в корені дерева міститься зв'язка $\vee$ і у нього два піддерева – праве є деревом для підформули Φ, а ліве – деревом для Ψ. (П) Процес побудови дерева $D(\Phi)$ закінчиться за скінченну кількість кроків, тому що на кожному індуктивному кроці формули втрачають одну зв'язку.

Смисл дерева Канторовича полягає в тому, що його обхід дозволяє обчислити значення формули[3]. Модифікація дерева Канторовича полягає у зважуванні дуг істинніснісними значеннями і фарбуванні деяких піддерев.

Модифіковані дерева теж будується індуктивно. Будемо називати цей процес *розгортанням* формули Φ. Піддерева модифікованого дерева, як і самі дерева, діляться на дві категорії – позитивні і негативні. В корінь позитивного піддерева входить стрілка зважена 1, а негативного – 0. Процеси розгортання позитивного $D(\Phi)_+$ і негативного дерев $D(\Phi)_-$ взаємо пов'язані.

(Б) Формула $\Phi \equiv x$ є базовою. В корені дерева знаходиться змінна x_+ для позитивного дерева та x_- для негативного, він є листком і процес розгортання припиняється. Індуктивний перехід (І) для негативного дерева $D(\Phi)_-$.

Якщо $\Phi \equiv \neg\Psi$, то коренем $D(\Phi)_-$ є зв'язка $\neg_-$, в якого одне позитивне піддерево $D(\Psi)_+$.

Якщо $\Phi \equiv \text{E} \vee \Psi$, то коренем $D(\Phi)_-$ є зв'язка $\vee_-$, в якого два негативні піддерева $D(\text{E})_-$ і $D(\Psi)_-$.

Якщо $\Phi \equiv \text{E} \& \Psi$, то коренем $D(\Phi)_-$ є зв'язка $\&_-$, в якого два негативних і альтернативних піддерева $D(\text{E})_-$ і $D(\Psi)_-$, друге з яких пофарбоване в новий колір.

Якщо $\Phi \equiv \text{E} \to \Psi$,то коренем $D(\Phi)_-$є зв'язка $\to_-$, у якого піддерево $D(\text{E})_+$ є позитивним, а $D(\Psi)_-$ - негативним.

Індуктивний перехід (І) для позитивного дерева $D(\Phi)_+$.

Якщо $\Phi \equiv \neg\Psi$, то коренем $D(\Phi)_+$ є вузол $\neg_+$, у якого одне негативне піддерево $D(\Psi)_-$.

Якщо $\Phi \equiv \text{E} \vee \Psi$, то коренем $D(\Phi)_+$ є зв'язка $\vee_+$, у якого два позитивні альтернативні піддерева $D(\text{E})_-$ і $D(\Psi)_-$, друге з яких пофарбоване в новий колір.

Якщо $\Phi \equiv \text{E} \& \Psi$, то коренем $D(\Phi)_+$ є зв'язка $\&_+$, у якого два позитивних піддерева – $D(\text{E})_+$ і $D(\Psi)_+$.

---

[3] Дерева Канторовича вперше були застосовані для обчислення значень арифметичних виразів.

Якщо $\Phi \equiv \mathrm{E} \to \Psi$, то коренем $D(\Phi)_+$ є зв'язка $\to_+$, у якого два альтернативних піддерева – негативне $D(\mathrm{E})_-$ і позитивне $D(\Psi)_+$ з яких останнє пофарбоване в новий колір.

(П) Процес розгортання модифікованого дерева завершиться, коли в ньому не залишиться листків-зв'язок.

Виберемо стратегію розгортання дерев «зверху-вниз» і «зліва-направо». Тобто спочатку буде розгортатися піддерево для E, потім – для Ψ.

Якщо з кожної пари альтернативних піддерев модифікованого дерева вилучити одне з них, то отримане дерево будемо називати його редукційним варіантом (Р-варіантом). Зазначимо, що корені дерева і його Р-варіантів збігаються, а якщо в модифікованому дереві немає альтернативних піддерев, то Р-варіант дерева збігається з ним самим. Пара однакових листків Р-варіанта дерева називається контрарною, якщо в них ведуть дуги з протилежними мітками. Р-варіант "хороший", якщо серед його листків немає контрарних пар, у супротивному – він «нехороший». Для довільної інтерпретації I значення формули Φ^I може бути обчислена при обході певного її Р-варіанта, позитивність і негативність листків якого відповідає значенню змінних в даній інтерпретації.

Лема 1.2 (про редукцію). Формула Φ - спростовна (виконувана) $\Leftrightarrow$ існує принаймні один "хороший " Р-варіант модифікованого дерева $D(\Phi)_-$ ($D(\Phi)_+$).

► $(\Rightarrow)$ Індукція по структурі формули Φ.

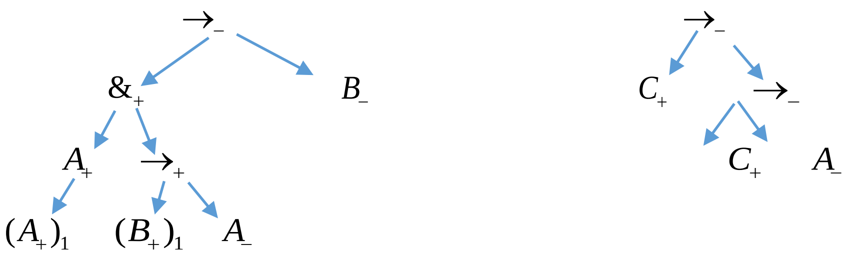
(Б) Нехай Φ - базова формула, тобто змінна і вона – спростовна (виконувана). Тоді дерево $D(\Phi)_-$ і($D(\Phi)_+$)складається з одного кореня-листка і воно «хороше».

(І) Нехай $\Phi \equiv \neg\Psi$ - а) спростовна (б) виконувана) і для підформули Ψ відповідні твердження леми вірні. Нехай $D(\Psi)_+$ – позитивне модифіковане дерево для Ψ. Візьмемо а). Якщо $\neg\Psi$ – спростовна, то Ψ - виконувана. За індуктивним припущенням, існує «хороший» Р-варіант дерева $D(\Psi)_+$. Якщо приєднати цей Р-варіант до кореня $\neg_-$, то тримаємо «хороший» Р-варіант дерева $D(\Phi)_-$. Аналогічно, доводиться і п. б).

Нехай формула $\Phi \equiv \mathrm{E} \vee \Psi$ - а) спростовна (б) виконувана) і для підформул E і Ψ відповідні твердження леми вірні. Візьмемо а). Маємо, якщо формула $\mathrm{E} \vee \Psi$ - спростосовна, то формули E і Ψ спростовні при певній спільній інтерпретації I і існують «хороші» Р-варіанти дерев $D(\mathrm{E})_-$ і $D(\Psi)_-$ для обчислення значення E^I і Ψ^I. В об'єднанні листків цих Р-варіантів не може бути контрарної пари, тому що у Р-варіанті листки узгоджені з інтерпретацією I, яка є спільною для обох Р-варіантів. Тому під'єднавши ці Р-варіанти до кореня $\vee_-$, отримаємо «хороший» Р-варіант дерева $D(\Phi)_-$. Аналогічно доводиться і п.б)..

($\Leftarrow$) За побудовою модифікованих дерев $D(\Phi)_-$ та $D(\Phi)_+$ (Вправа ???). За повнотою (П), доведення леми завершено.
◀
Розглянемо приклади розгортання формул.

Приклад 1.1. Розгорнемо формули 1) $\Phi \equiv (A \& (A \to B)) \to B$ та 2) $\Psi \equiv C \to (C \to A)$. На Рис. 1.1 представлені негативні модифіковані дерева для формул Φ та Ψ. В дереві $D(\Phi)_-$ є пара альтернативних піддерев з коренями $\&_+$ та B_- і обидва його Р-варіанти "нехороші". Числовий індекс у вершинах означає номер кольору, а символьний індекс вказує на позитивність чи негативність піддерева. В дереві $D(\Psi)$ немає альтернативних піддерев.



$D(\Phi)_-$ $D(\Psi)_-$

Рис. 1.1.

У першому дереві немає хороших Р-варіантів, тому формула – тавтологія. У другому є – саме дерево $D(\Psi)$. Інтерпретація $C^I = 1, A^I = 0$ спростовує формулу Ψ. ■

В подальшому ми побудуємо спеціальні числення для більш ефективного обгрунтування тавтологічності та суперечливості формул.

Закони ПЛ. В логіці тавтології називають *законами.* Вони носять універсальний характер і виконуються у всіх класичних логіках. Деякі тавтології мають власні назви.

Три основоположні закони логіки, зафіксовані ще Аристотелем, виражають такі тавтології:

а) закон тотожності: $P \leftrightarrow P$;

б) закон виключеного третього (*tertium non datur*): $(\neg P) \vee P$;

в) закон суперечливості (*lex contradictionis*): $\neg(P \& (\neg P))$.

До основних законів ПЛ належать властивості пропозиційних зв'язок. Нехай P, Q, R - довільні формули.

1) Закони комутативності для $\vee, \&$ та $\leftrightarrow$:

1.1 $P \vee Q \leftrightarrow Q \vee P$;

1.2 $P \& Q \leftrightarrow Q \& P$;

1.3 $(P \leftrightarrow Q) \leftrightarrow (Q \leftrightarrow P)$.

2) Закони асоціативності для $\vee, \&$ та $\leftrightarrow$

2.1 $(P \vee Q) \vee R \leftrightarrow P \vee (Q \vee R)$;

2.2 $(P \& Q) \& R \leftrightarrow P \& (Q \& R)$;

2.3 $((P \leftrightarrow Q) \leftrightarrow R) \leftrightarrow (P \leftrightarrow (Q \leftrightarrow R))$.

3) Закони дистрибутивності для $\vee, \&$:

3.1 $(P \vee Q) \& R \leftrightarrow (P \& R) \vee (Q \& R)$;

3.2 $(P \& Q) \vee R \leftrightarrow (P \vee R) \& (Q \vee R)$.

4) Закон зняття подвійного заперечення:

$\neg\neg P \leftrightarrow P$.

5) Закони ідемпотентності для $\vee, \&$:

4.1 $P \leftrightarrow P \vee P$;

4.2 $P \leftrightarrow P \& P$.

6) Закони де Моргана:

6.1 $\neg(P \vee Q) \leftrightarrow (\neg P \& \neg Q)$;

6.2 $\neg(P \& Q) \leftrightarrow (\neg P \vee \neg R)$.

7) Закони поглинання:

7.1 $P \to P \vee Q$;

7.2 $P \& Q \to P$.

8) Закон контрапозиції:

$(P \to Q) \leftrightarrow (\neg Q \to \neg P)$.

Наступна теорема створює основу для еквівалентних перетворень формул у семантичних виведеннях. Якщо у виведенні формулу (підформулу) замінити на еквівалентну, то результат виведення не зміниться.

Теорема 1.1 (про семантичну еквівалентність). Нехай формула Φ' отримана із формули Φ заміною деяких входжень формул $\Phi_1, ..., \Phi_n$ на Ψ_1, ..., Ψ_n відповідно. Якщо при цьому $\Phi_i \leftrightarrow \Psi_i, i = \overline{1,n}$, то $\Phi \leftrightarrow \Phi'$.

► Індукція по структурі формули Φ. (Б) Для базових формул твердження очевидне, тому що вони не містять власних підформул. (І) Нехай $\Phi \equiv \neg \mathrm{A}$ і для підформули A твердження теореми вірне. Враховуючи, що усі підформули Φ – це формула A і її власні підформули, то Φ' має вигляд $\neg(\mathrm{A}')$. Тоді за припущенням, $\mathrm{A} \leftrightarrow \mathrm{A}'$, а значить і $\neg\mathrm{A} \leftrightarrow \neg\mathrm{A}'$. Нехай $\Phi \equiv \mathrm{A} \vee \mathrm{B}$. За означенням, підформулами Φ є формули A, B та їхні власні підформули. Нехай для формул A і B твердження теореми вірне: $\mathrm{A} \leftrightarrow \mathrm{A}'$, $\mathrm{B} \leftrightarrow \mathrm{B}'$. Тоді Φ' збігається з $\mathrm{A}' \vee \mathrm{B}'$ і з припущень $\mathrm{A} \leftrightarrow \mathrm{A}', \mathrm{B} \leftrightarrow \mathrm{B}'$ випливає еквівалентність $\mathrm{A} \vee \mathrm{B} \leftrightarrow \mathrm{A}' \vee \mathrm{B}'$.

◄

КНФ та ДНФ. Формули ПЛ мають канонічні стандартні форми – кон'юнктивну та диз'юнктивну нормальні форми (скорочено КНФ та ДНФ). Пропозиційну змінну та її заперечення назвемо літерами, а диз'юнкцію (кон'юнкцію) літер – *диз'юнктом* (*кон'юнктом*). Кон'юнкція кількох диз'юнктів називається *КНФ*, а диз'юнкція кількох кон'юнктів – *ДНФ*. На практиці, для отримання КНФ та ДНФ даної формули буває достатньо застосувати закони зняття подвійного заперечення, Де Моргана та дистрибутивності.

Приклад 1.1. Побудуємо КНФ для формули $\neg((\mathrm{A} \vee \mathrm{B}) \& (C \vee D))$, де A, B, C, D - літери.

$\neg((\mathrm{A} \vee \mathrm{B}) \& (C \vee D)) \leftrightarrow$

$\neg(A \vee B) \vee \neg(C \vee D) \quad \leftrightarrow$ Де Моргана 6.2

$(\neg A \& \neg B) \vee (\neg C \& \neg D) \leftrightarrow$ Де Моргана 6.2 для підформул

$(\neg A \vee (\neg C \& \neg D)) \wedge (\neg B \vee (\neg C \& \neg D)) \leftrightarrow$ дистрибутивність 3.2

$(\neg C \vee \neg A) \& (\neg D \vee \neg A) \& (\neg C \vee \neg B) \& (\neg D \vee \neg B)$ комутативність 1.1 та дистрибутивність 3.2 для підформул

Щоб диз'юнкції в дужках стали диз'юнктами, залишилося за законом 4) усунути, де це потрібно, подвійне заперечення.■

Загальний метод отримання КНФ та ДНФ для заданої формули надає наступна

Теорема 1.2 (про існування КНФ та ДНФ). Для будь-якої формули Φ існують еквівалентні КНФ Φ' та ДНФ Φ''.

► Нехай $x_1,...,x_n$ – всі пропозиційні змінні формули Φ. Випишемо усі кортежі значень цих змінних, при яких формула Φ хибна і назвемо їх виділеними. Кожному виділеному кортежу поставимо у відповідність диз'юнкт $X_1 \vee ... \vee X_n$, де X_i є змінна x_i, якщо її значення у даному кортежі хибне і літера $\neg x_i$, якщо це значення – істинне. Позначимо ці диз'юнкти $D_1,...,D_m$. За побудовою, кожний з диз'юнктів хибний на своєму виділеному кортежі, а на усіх решти кортежах значень змінних x_i – істинний. Тоді КНФ для формули Φ буде кон'юнкція $\Phi' = D_1 \wedge ... \wedge D_m$, яка хибна на всіх виділених кортежах і істинна на усіх невиділених, де $\wedge \equiv \&$.

Для побудови ДНФ виділеними назвемо кортежі, на яких формула Φ істинна. Кожному виділеному кортежу поставимо у відповідність кон'юнкт $X_1 \wedge ... \wedge X_n$, де X_i є змінна x_i, якщо її значення у даному кортежі істинне і літера $\neg x_i$, якщо це значення – хибне. Позначимо ці кон'юнкти $K_1,...,K_l$. За побудовою, кожний з кон'юнктів істинний на своєму виділеному кортежі, а на усіх решти кортежах значень змінних – хибний. Тоді ДНФ для формули Φ буде диз'юнкція $\Phi'' = K_1 \vee ... \vee K_l$, яка істинна на всіх виділених кортежах і хибна на усіх невиділених.

◀

Сукупність зв'язок називається *повною*, якщо їх достатньо для побудови з точністю до еквівалентності будь-якої пропозиційної формули.

Наслідок 1. Як показує теорема 1.2, сукупність зв'язок $\{\neg,\vee\}$ є повною, тому що кон'юнкція є їхньою похідною. Повними будуть також пари зв'язок $\{\neg,\wedge\}$ та $\{\neg,\rightarrow\}$. Для першої пари це випливає з закону Де Моргана 6.1. а для другої – з еквіваленції $x \vee y \leftrightarrow \neg x \rightarrow y$.■

Приклад 1.2. Побудуємо КНФ і ДНФ для формули $\Phi = \neg((\mathrm{A} \vee \mathrm{B}) \wedge (C \vee D))$ з прикладу 1.1., коли літери A, B, C – змінні x_1, x_2, x_3, а літера $D = \neg x_4$. Побудуємо таблицю, в якій представлено а) усі кортежі значень цих змінних, б) значення на них формули Φ та в) диз'юнкти D_i та кон'юнкти K_i, які відповідають виділеним кортежам для КНФ та ДНФ

x_1	x_2	x_3	x_4	Φ	Диз'юнкти	Кон'юнкти
0	0	0	0	1		$K_1 = \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4$
0	1	0	0	1		$K_2 = \neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4$
0	0	1	0	1		$K_3 = \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4$
0	0	0	1	1		$K_4 = \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4$
0	1	1	0	0	$D_1 = x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg x_4$	
0	1	0	1	0	$D_2 = x_1 \vee \neg x_2 \vee x_3 \vee \neg\neg x_4$ $= x_1 \vee \neg x_2 \vee x_3 \vee x_4$	
0	0	1	1	1		$K_5 = \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4$
0	1	1	1	0	$D_3 = x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg\neg x_4$ $= x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4$	
1	0	0	0	1		$K_6 = x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4$
1	0	1	0	0	$D_4 = \neg x_1 \vee x_2 \vee x_3 \vee \neg\neg x_4$	
1	0	0	1	0	$D_5 = \neg x_1 \vee x_2 \vee x_3 \vee \neg\neg x_4$ $= \neg x_1 \vee x_2 \vee x_3 \vee x_4$	
1	1	0	0	1		$K_7 = x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4$
1	1	0	1	0	$D_6 = \neg x_1 \vee \neg x_2 \vee x_3 \vee \neg\neg x_4$ $= \neg x_1 \vee \neg x_2 \vee x_3 \vee x_4$	
1	1	1	0	0	$D_7 = \neg x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg\neg x_4$ $= \neg x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4$	
1	0	1	1	0	$D_8 = \neg x_1 \vee x_2 \vee \neg x_3 \vee \neg\neg x_4$ $= \neg x_1 \vee x_2 \vee \neg x_3 \vee x_4$	
1	1	1	1	0	$D_9 = \neg x_1 \vee \neg x_2 \vee \neg x_3 \vee \neg\neg x_4$ $= \neg x_1 \vee \neg x_2 \vee \neg x_3 \vee x_4$	

Тоді кон'юнкція $\Phi' = \bigwedge_{i=1}^{9} D_i$ є КНФ, а диз'юнкція $\Phi'' = \bigvee_{i=1}^{7} K_i$ – ДНФ формули Φ .■

1.3. Секвенційне пропозиційне числення

Нехай $\Delta = \{\Psi_1,...,\Psi_m\}$. Будемо говорити, що множина формул Δ є *семантичним (тавтологічним) наслідком* множини формул $\Gamma = \{\Phi_1,...,\Phi_n\}$ і позначати це $\Gamma \models \Psi$, якщо $\Phi_1 \& ... \& \Phi_n \models \Psi_1 \vee ,..., \vee \Psi_m$. Це відношення має наступні важливі властивості. За означенням, відношення $\Gamma \models \varnothing$ хибне для будь-якого Γ.

Лема 1.3. Нехай Γ, Δ – довільні сукупності формул. Тоді

G1) Якщо $\Gamma \cap \Delta \neq \varnothing \models \Delta$, то $\Gamma \models \Delta$.

G1) Якщо $\Gamma \models \Delta$ і $\Delta \subseteq \Delta' \models \Delta$, то $\Gamma \models \Delta'$.

R1) $\neg\Phi, \Gamma \models \Delta. \Leftrightarrow \Gamma \models \Delta, \Phi$.

R2) $\Gamma \models \Delta, \neg\Phi \Leftrightarrow \Phi, \Gamma \models \Delta$

R3) $\Phi \vee \Psi, \Gamma \models \Delta \Leftrightarrow \Phi, \Gamma \models \Delta$ та $\Psi, \Gamma \models \Delta$.

R4) $\Gamma \models \Delta, \Phi \vee \Psi \Leftrightarrow \Gamma \models \Delta, \Phi, \Psi$.

R5) $\Phi \& \Psi, \Gamma \models \Delta \Leftrightarrow \Phi, \Psi, \Gamma$.

R6) $\Gamma \models \Delta, \Phi \& \Psi \Leftrightarrow \Gamma \models \Delta, \Phi$ та $\Gamma \models \Delta, \Psi$.

R7) $\Phi \to \Psi, \Gamma \models \Delta \Leftrightarrow \Gamma \models \Delta, \Phi$ та $\Psi, \Gamma \models \Delta$.

R8$\Gamma \models \Delta, \Phi \to \Psi \Leftrightarrow \Phi, \Gamma \models \Delta, \Psi$.

R9$\Phi \leftrightarrow \Psi, \Gamma \models \Delta \Leftrightarrow \Phi, \Psi, \Gamma \models \Delta$ та $\Gamma \models \Delta, \Phi, \Psi$.

R10$\Gamma \models \Delta, \Phi \leftrightarrow \Psi \Leftrightarrow \Phi, \Gamma \models \Delta, \Psi$ та $\Psi, \Gamma \models \Delta, \Phi$.

► Перші два твердження очевидні. Візьмемо R1) . $(\Rightarrow)$ Нехай $\neg\Phi, \Gamma \models \Delta$. Тоді для довільної інтерпретації I при $(\neg\Phi \wedge \Gamma)^I = 1$ $\Phi^I = 0, \Gamma^I = 1$ і $\Delta^I = 1$. Розглянемо значення правої сторони $(\Delta \vee \Phi)^I$ відношення $\Gamma \models \Delta, \Phi$. для даної інтерпретації. Вона істинна, тому що $\Delta^I = 1$. $(\Leftarrow)$ Нехай тепер $\Gamma \models \Delta, \Phi$ і для інтерпретації I $\Gamma^I = 1$ і $(\Delta \vee \Phi)^I = 1$. Тоді нехай а) $\Delta^I = 1$, $\Phi^I = 0$ і б) $\Delta^I = 0, \Phi^I = 1$. Розглянемо ліву сторону і її значення $(\neg\Phi \wedge \Gamma)^I$ для випадку а). Вона істинна, тому що $\Gamma^I = (\neg\Phi)^I = 1$. У випадку б) маємо, що $\neg\Phi^I = 0$, а значить і $(\neg\Phi \wedge \Gamma)^I = 0$ і він не впливає на відношення $\neg\Phi, \Gamma \models \Delta$.

Візьмемо R3). $(\Rightarrow)$ Нехай $\Phi \vee \Psi, \Gamma \models \Delta$. Тоді для довільної інтерпретації I при $(\Phi \vee \Psi)^I \wedge \Gamma^I = 1$ маємо $(\Phi \vee \Psi)^I = \Gamma^I = 1$ і $\Delta^I = 1$. Розглянемо значення першого відношення $\Phi, \Gamma \models \Delta$ для даної інтерпретації, коли $\Phi^I = 1$ і $\Phi^I = 0$. У першому випадку $\Phi^I = \Gamma^I = 1$ і $\Delta^I = 1$, що і потрібно, у другому – $\Phi^I \wedge \Gamma^I = 0$ і це не впливає на виконання відношення. Тому $\Phi, \Gamma \models \Delta$ має місце. Аналогічно і $\Psi, \Gamma \models \Delta$ теж має місце. $(\Leftarrow)$ Нехай тепер $\Phi, \Gamma \models \Delta$ та $\Psi, \Gamma \models \Delta$ і нехай $\Phi^I = 0$ і $\Psi^I = 0$. Тоді $(\Delta \vee \Phi)^I = 0$ і інтерпретація I не впливає на відношення $\Phi \vee \Psi, \Gamma \models \Delta$. Якщо, принаймні, одне з Δ^I, Φ^I істинне і $\Gamma^I = 1$, то за умовою $\Delta^I = 1$. Тоді маємо $(\Delta \vee \Phi)^I =$ $\Gamma^I =$ $\Delta^I = 1$, що і потрібно для виконання $\Phi \vee \Psi, \Gamma \models \Delta$.

Доведення тверджень R2) і R4) аналогічні і винесені у вправи. Твердження R5)- R8) випливають з R1) – R4), тому що заперечення і диз’юнкція є повною системою зв’язок.

◄

Еквіваленції з Леми 1.3 дозволяють звести питання про виконання логічного наслідку між сукупностями формул до аналогічних питань щодо підформул цих формул. Це створює основу для побудови, так званого, секвенційного пропозиційного числення.

Нехай $\Gamma \models \Delta$ довільний тавтологічний наслідок і $\Gamma = \{\Phi_1, ..., \Phi_n\}$, $\Delta = \{\Psi_1, ..., \Psi_m\}$. Секвенцією називається слово $[\Gamma \Rightarrow \Delta]$ ($[\Rightarrow \Delta]$), яке представляє імплікацію $\Phi_1 \wedge ... \wedge \Phi_n \rightarrow \Psi_1 \vee, ..., \vee \Psi_m$ (формулу $\Psi_1 \vee, ..., \vee \Psi_m$). Квадратні дужки – це метасимволи, які підкреслюють, що секвенція формально не є імплікацією чи формулою, вона тільки синтаксично представляє їх. Секвенція $[\Gamma \Rightarrow \Delta]$ *виконується*, якщо її імплікація є тавтологією, тобто має місце тавтологічний наслідок $\Gamma \models \Delta$. Секвенції, в яких ліва і права частини мають не порожній перетин, називаються замкненими. За *G*1) вони завжди виконуються.

Г. Генцен запропонував спеціальне повне *секвенційне числення* (СЧ) для секвенцій, що виконуються (а значить і для логічних наслідків !). Тому його іноді називають – генценівським. Аксіомами числення виступають замкнені секвенції вигляду $[\{\Phi\} \cup \Gamma \Rightarrow \Delta \cup \{\Phi\}]$, формули яких не містять зв’язок, а правила виведення ПВ1-ПВ10 відповідають властивостям R1) – R10). А саме, відповідні секвенції справа від еквівалентності “$\Leftrightarrow$” є аргументами правил, а секвенція зліва – їхнім результатом. Повнота числення означає, що з аксіом можна довести (вивести) будь-яку секвенцію, що виконується. Насправді, для повноти числення достатньо і перших чотирьох правил ПВ1-ПВ4. Секвенція – вивідна в СЧ, якщо вона має доведення з аксіом.

Домовимося, як і в Лемі 1.3, об'єднання в секвенціях записувати через кому. Наприклад, писати $[\Phi, \Gamma \Rightarrow \Delta, \Phi]$замість $[\{\Phi\} \cup \Gamma \Rightarrow \Delta \cup \{\Phi\}]$. Правилами виведення (ПВ) в СЧ є наступні чотири правила:

ПВ1 $[\Gamma \Rightarrow \Delta, \Phi] \vdash [\neg\Phi, \Gamma \Rightarrow \Delta]$

ПВ2) $[\Phi, \Gamma \Rightarrow \Delta] \vdash [\Gamma \Rightarrow \Delta, \neg\Phi]$

ПВ3) $[\Phi, \Gamma \Rightarrow \Delta]$, $[\Psi, \Gamma \Rightarrow \Delta] \vdash [\Phi \vee \Psi, \Gamma \Rightarrow \Delta]$

ПВ4 $[\Gamma \Rightarrow \Delta, \Phi, \Psi] \vdash [\Gamma \Rightarrow \Delta, \Phi \vee \Psi]$.

Як бачимо, тільки правило П3 має два аргументи.

Лема 1.4. Секвенційне числення є коректним.

► Секвенції в аксіомах виконуються, а правила ПВ1- ПВ4 зберігають виконуваність секвенцій. Це випливає з Леми 1.3 ◄

Доведення теорем в СЧ будуються методом «зверху-вниз», тобто з кінця. Спочатку кінцеву секвенцію намагаємося подати як результат застосування підходящого правила виведення з числа ПВ1- ПВ4 і певних секвенцій-аргументів. Потім аналогічно діємо стосовно вибраних секвенцій-аргументів і так до тих пір, поки не дістанемося замкнених секвенцій або секвенцій без зв'язок. Це трапиться обов'язково, тому що секвенції-аргументи мають завжди на одну зв'язку менше. Подібні доведення зручно представляти *секвенційними деревами.* Це бінарні дерева, вузли яких зважені секвенціями так, що секвенції у вузлах-предках є результатами застосування одного з правил виведення ПВ1-ПВ4 до секвенцій вузлів-нащадків. Секвенційне дерево називається 1) термінальним, якщо в його листках немає пропозиційних зв'язок, тобто ліва і права частина секвенцій складається виключно з базових формул – пропозиційних змінних і 2) замкненим, якщо всі його листки – замкнені.

Якщо взяти секвенцію $[\Gamma \Rightarrow \Delta]$, то основна роль стрілки в ній – розділити формули лівої і правої частин. Цього можна досягти, якщо приписати всім формулам зліва і справа спеціальні префікси – відповідно $\vdash$ та $\dashv$. Тоді сукупність таких розмічених формул однозначно подає секвенцію $[\Gamma \Rightarrow \Delta]$. Таке подання має свої переваги, тому що порядок формул в сукупності перестає бути важливим, відпадає необхідність в символі $\Rightarrow$ і в квадратних дужках. Надалі секвенції будемо зображати як $\vdash \Gamma \dashv \Delta$.

Щоб краще зрозуміти введені поняття, розглянемо наступний приклад.

Приклад 1.3. Побудуємо термінальне секвенційне дерево для секвенції $[\Rightarrow (\neg B \lor C \to \neg(\neg A \lor B) \lor (\neg A \lor C))]$ без лівої частини.

$\dashv (\neg B \lor C \to \neg(\neg A \lor B) \lor (\neg A \lor C))$

$\vdash \neg B \lor C, \dashv \neg(\neg A \lor B) \lor (\neg A \lor C)$ [19]

$\vdash \neg B, \dashv \neg(\neg A \lor B) \lor (\neg A \lor C)$ [9] $\quad$ $\vdash C, \dashv \neg(\neg A \lor B) \lor (\neg A \lor C)$ [18]

$\dashv B, \dashv \neg(\neg A \lor B) \lor (\neg A \lor C)$ [8] $\quad$ $\vdash C, \dashv \neg(\neg A \lor B), \dashv (\neg A \lor C)$ [17]

$\dashv B, \dashv \neg(\neg A \lor B), \dashv (\neg A \lor C)$ [7] $\quad$ $\vdash C, \dashv \neg(\neg A \lor B), \dashv \neg A, \dashv C$ [16]

$\dashv B, \vdash (\neg A \lor B), \dashv (\neg A \lor C)$ [6] $\quad$ $\vdash C, \vdash (\neg A \lor B), \dashv \neg A, \dashv C$ [15]

$\dashv B, \vdash (\neg A \lor B), \dashv \neg A, \dashv C$ [5] $\quad$ $\vdash C, \vdash \neg A, \dashv \neg A, \dashv C$ [12] $\quad$ $\vdash C, \vdash B, \dashv \neg A, \dashv C$ [14]

$\dashv B, \vdash \neg A, \dashv \neg A, \dashv C$ [3] $\quad$ $\dashv B, \vdash B, \dashv \neg A, \dashv C \times$ [4] $\quad$ $\vdash C, \dashv A, \dashv \neg A, \dashv C$ [11] $\quad$ $\vdash C, \vdash B, \vdash A, \dashv C \times$ [13]

$\dashv B, \dashv A, \dashv \neg A, \dashv C$ [2] $\quad$ $\vdash C, \dashv A, \vdash A, \dashv C \times$ [10]

$\dashv B, \dashv A, \vdash A, \dashv C \times$ [1]

Рис. 1.2

Як бачимо, дерево є замкненим, тому що всі листки в ньому (відмічені ×) замкнені (є аксіомами). Тепер щоб довести секвенцію $[\Rightarrow(\neg B\vee C\rightarrow\dashv\neg(\neg A\vee B)\vee(\neg A\vee C))]$ в СЧ, достатньо обійти дане дерево знизу-вверх і зліва-направо і взяти відповідні секвенції. При цьому спочатку будемо обходити ліве піддерево, потім – праве, а потім корінь піддерева. На кожному кроці обходу у батьківському вузлі знаходиться результат застосування певного правила з числа ПВ1- ПВ4 до секвенцій його безпосередніх нащадків. На останньому кроці застосовано правило ПВ3 до секвенцій $\vdash\neg B$, $\dashv\neg(\neg A\vee B)\vee(\neg A\vee C)$ та $\vdash C$, $\dashv\neg(\neg A\vee B)\vee(\neg A\vee C)$, при цьому $\Phi=\neg B,\Psi=C,\Gamma=\varnothing,\Delta=\{\ \dashv(\neg A\vee B)\vee(\neg A\vee C)$ }. Послідовність обходу вершин показана в дереві номерами в квадратних дужках. Таке доведення є доведенням з аксіом і свідчить, що має місце логічний наслідок $\neg B\vee C\ \models\ \dashv(\neg A\vee B)\vee(\neg A\vee C)$], тому що правила ПВ1- ПВ4 зберігають виконуваність результату. ■

Теорема 1.3 (про повноту СЧ). Секвенційне числення є повним.

► Візьмемо довільну секвенцію $\vdash\Gamma\dashv\Delta$ і припустимо, що вона виконується. Спочатку покажемо, що 1) термінальне секвенційне дерево для неї є обов'язково замкненим, а потім, що 2) вона має доведення в СЧ. Для доведення п. 1) застосуємо індукцію по числу зв'язок n в секвенції $\vdash\Gamma\dashv\Delta$.

(Б). Нехай $n=0$. Тоді секвенційне дерево складається з одного кореня $\vdash\Gamma\dashv\Delta$ і є термінальним, тому що сукупності Γ і Δ складаються тільки з пропозиційних змінних. Щоб така секвенція виконувалася, умова її замкненості ($\Gamma\cap\Delta\neq\varnothing$) стає і необхідною. Дійсно, якщо $\Gamma\cap\Delta=\varnothing$, то тоді достатньо взяти інтерпретацію, в якій усі змінні з Γ істинні, а з Δ – хибні і на ній секвенція виконуватися не буде. Таким чином, секвенція $\vdash\Gamma\dashv\Delta$ як і все дерево є замкненими.

(І). Нехай для всіх секвенцій, що виконуються, з числом зв'язок менше довільного n, всі термінальні секвенційні дерева замкнені. Покажемо, що і всі термінальні дерева для секвенції $\vdash\Gamma\dashv\Delta$ з числом зв'язок n замкнені. Розглянемо довільне термінальне секвенційне дерево D для секвенції $\vdash\Gamma\dashv\Delta$ з числом зв'язок n. Його коренем є $\vdash\Gamma\dashv\Delta$. Нехай $\vdash\Gamma_1\dashv\Delta_1$ або $\vdash\Gamma_1\dashv\Delta_1$ і $\vdash\Gamma_2\dashv\Delta_2$ (якщо декомпозиція секвенції розпочиналася за допомогою правила ПВ3 – безпосередні нащадки кореня. За побудовою, число зв'язок в них $n-1$ і ці секвенції виконуються, тому що правила виведення СЧ спираються на властивості R1) – R4) Леми 1.3 , кожна з яких є еквівалентністю і виконання правих їхніх частин гарантує виконання і лівих. Розглянемо піддерева дерева D з коренями у вузлах $\vdash\Gamma_1\dashv\Delta_1$ і $\vdash\Gamma_2\dashv\Delta_2$. Вони є теж термінальними і за індуктивним припущенням – замкненими. (П). Значить і дерево D – замкнене і доведення п.1) завершено.

Щодо п.2) побудови доведення в ГЧ секвенції $\vdash\Gamma\dashv\Delta$, то як і в Прикладі 1.3, достатньо обійти дерево D знизу-вверх і зліва – направо і взяти відповідні секвенції. Отримана послідовність секвенцій завершується $\vdash\Gamma \dashv\Delta$ і є її доведенням з аксіом.

◀

Для зменшення висоти секвенційних дерев і скорочення відповідних доведень, доповнимо СЧ додатковими правилами виведення, які відповідають решті зв'язок $\wedge,\rightarrow,\leftrightarrow$ згідно правил R5) – R10). Покладемо

ПВ5) $[\Phi,\Psi,\Gamma\Rightarrow\Delta] \vdash [\Phi\wedge\Psi,\Gamma\Rightarrow\Delta]$

ПВ6) $[\Phi,\Gamma\Rightarrow\Delta],\ [\Psi,\Gamma\Rightarrow\Delta] \vdash [\Phi\wedge\Psi,\Gamma\Rightarrow\Delta]$

ПВ7) $[\Gamma\Rightarrow\Delta,\Phi],\ [\Psi,\Gamma\Rightarrow\Delta] \vdash [(\Phi\rightarrow\Psi),\Gamma\Rightarrow\Delta]$

ПВ8) $[\Psi,\Gamma\Rightarrow\Delta,\Psi] \vdash [\Gamma\Rightarrow\Delta,(\Phi\rightarrow\Psi)]$.

ПВ9) $[\Phi,\Psi,\Gamma\rightarrow\Delta],[\Gamma\Rightarrow\Delta\ \Phi,\Psi] \vdash [\Phi\leftrightarrow\Psi,\Gamma\Rightarrow\Delta]$.

ПВ10) $[\Phi,\Gamma\Rightarrow\Delta,\Psi],[\Psi,\Gamma\Rightarrow\Delta,\Phi] \vdash [\Gamma\Rightarrow\Delta,\ \Phi\leftrightarrow\Psi]$.

В правилах ПВ7-ПВ8, щоб уникнути колізії з використанням символа $\rightarrow$ – в круглих дужках він означає імплікацію, в квадратних – секвенцію.

Приклад 1.4. З'ясувати, чи є формула $\Phi\equiv(A\rightarrow C)\rightarrow(B\vee C\rightarrow A\vee B\rightarrow C)$ тавтологією. Побудуємо термінальне секвенційне дерево для секвенції $\dashv(A\rightarrow C)\rightarrow(B\vee C\rightarrow A\vee B\rightarrow C)$ з порожньою лівою стороною і перевіримо чи воно замкнене.

$\dashv(A\rightarrow C)\rightarrow(B\vee C\rightarrow(A\vee B\rightarrow C))$

$\vdash A\rightarrow C,\ \dashv B\vee C\rightarrow(A\vee B\rightarrow C)$ [ПВ8]

$\vdash A\rightarrow C,\ \vdash B\vee C,\ \dashv A\vee B\rightarrow C$ [ПВ8]

$\dashv A,\ \vdash B\vee C,\ \dashv A\vee B\rightarrow C$ $\qquad$ $\vdash C,\ \vdash B\vee C,\ \dashv A\vee B\rightarrow C$ [ПВ7]

$\dashv A,\ \vdash B,\ \dashv A\vee B\rightarrow C$ $\qquad$ $\dashv A,\ \vdash C,\ \dashv A\vee B\rightarrow C$ [ПВ3]

$\dashv A,\ \vdash B,\ \vdash A\vee B,\ \dashv C$ [ПВ8]

$\dashv A,\ \vdash B,\ \vdash A,\ \dashv C$ $\qquad$ $\dashv A,\ \vdash B,\ \dashv C*$ [ПВ3]

Рис. 1.3

Ми побудували секвенційне дерево з термінальним незамкненим листком (*). Цього достатньо, адже заключне термінальне дерево теж буде незамкненим, а значить за теоремою про повноту секвенція в корені не виконується і формула Φ - не тавтологія. Листок дерева (*) вказує на одну із інтерпретацій, при якій секвенція в корені не виконується. Дійсно, при інтерпретації I, коли $B^I=1,\ A^I=C^I=0$, секвенція (*) не виконується, а і значення формули Φ^I в корені хибне. ■

1.4. Резолюційне пропозиційне числення

Нагадаємо, що формула Φ називається суперечністю, якщо її заперечення $(\neg\Phi)$ є тавтологією. Суперечність хибна при всіх інтерпретаціях. Метою резолюційного числення (R-числення) є перевірка формул на суперечність. Щоб застосувати R-числення, формулу потрібно попередньо перетворити до КНФ. В R-численні КНФ представляється сукупністю її диз'юнктів. Об'єктами R-числення є сукупності диз'юнктів. Його єдиним правилом виведення є правило резолюцій (R-правило). Пару літер $x, \neg x$ називають *контрарною*.

Нехай D_1 і D_2 довільні диз'юнкти, які мають контрарну пару літер: $D_1 = x \vee D_1', D_2 = \neg x \vee D_2'$. Тоді результатом *правила резолюцій* $R(D_1, D_2)$ є диз'юнкт $D_1' \vee D_2'$, який називається *резольвентою* диз'юнктів D_1 і D_2. Резольвента у даних диз'юнктів може бути не одна – для кожної контрарної пари своя. Підкреслимо, що резольвента утворюється викреслюванням тільки однієї контрарної пари. Вона також може не існувати, коли в диз'юнктах відсутні контрарні пари. Зазначимо, у випадку, коли $D_1 = x, D_2 = \neg x$ резольвентою є порожній диз'юнкт $D_{\varnothing}$. R-правило може застосовуватись і до *сукупності* диз'юнктів. Для цього в сукупності вибирається довільна пара диз'юнктів, знаходиться їхня резольвента і долучається до сукупності замість вибраних диз'юнктів.

Покажемо, що R-правило зберігає суперечність сукупності диз'юнктів.

Лема 1.5. Сукупність диз'юнктів $\{D_1, D_2\}$ є суперечністю, тоді і тільки тоді, коли резольвента $R(D_1, D_2)$ є суперечністю.

► $(\Rightarrow)$ Нехай сукупність $\{D_1, D_2\}$- суперечність. Це означає, що кон'юнкція $D_1 \& D_2$ є суперечністю. Нехай $D_1 = x \vee D_1', D_2 = \neg x \vee D_2'$. Потрібно показати, що резольвента $D_1' \vee D_2'$ є суперечністю. Нехай I - довільна інтерпретація. Маємо, що $(x \vee D_1' \& \neg x \vee D_2')^I = 0$. Якщо $I(x) = 1$, тоді $\neg x = 0$ і $D_2'^I = 0$. Візьмемо таку інтерпретацію $\bar{I}$, що $\bar{I}(x) = 0, \bar{I}(y) = I(y)$. Тоді $(x \vee D_1' \& \neg x \vee D_2')^{\bar{I}} = 0$ і $\neg x = 1$. Значить $(x \vee D_1')^{\bar{I}} = 0$ і $D_1'^{\bar{I}} = 0$. Але $D_1'^{\bar{I}} = D_1'^I$, тому що в інтерпретаціях I і $\bar{I}$ значення всіх змінних $y \neq x$ збігаються , а змінна x не входить до D_1'. Таким чином, $(D_1' \vee D_2')^I = D_1'^I \vee D_2'^I = 0$ і резольвента є суперечністю.

$(\Leftarrow)$ Нехай резольвента $D_1' \vee D_2'$ – суперечність. Це значить, що для довільної інтерпретації I $(D_1' \vee D_2')^I = 0$. Тоді і кон'юнкція $(x \vee D_1' \& \neg x \vee D_2')^I = 0$, а значить і кон'юнкція $D_1 \& D_2$, тобто сукупність $\{D_1, D_2\}$, є суперечністю.

◄

Лема 1.5 має місце і коли два диз'юнкти замінити на їхню сукупність. Адже $D_1 \& D_2 \& \Phi$ - суперечність, тоді і тільки тоді, коли кон'юнкція $R(D_1, D_2)$ $\& \Phi$ є суперечність.

В R-численні аксіоми відсутні. Всі виведення здійснюються з гіпотез. Нехай S – довільна сукупність диз'юнктів. *Виведенням* сукупності S' з S називається послідовність сукупностей диз'юнктів $S_0,\ S_1, ..., S_n$ така, що $S_0 = S, S_n = S'$ і $S_i = R(S_{i-1})$, $i = \overline{1, n}$.

Теорема 1.4 (про повноту R-числення). Сукупність S є суперечністю, тоді і тільки тоді, коли з неї можна вивести сукупність з порожнім диз'юнктом.

► $(\Leftarrow)$ Нехай $S_0 = S,\ S_1, ..., S_n$ виведення таке, що $D_\varnothing \in S_n$. Тоді S_{n-1} є суперечністю, адже містить два диз'юнкти, які складають контрарну пару, з якої був отриманий порожній диз'юнкт в S_n. Тоді за Лемою 1.5 КНФ S_{n-2} теж суперечність. І так далі прийдемо, що $S_0 = S$ – суперечність.

$(\Rightarrow)$ Нехай S суперечність. Розглянемо усі виведення з S. Їх скінченна кількість, тому що резольвента сумарно містить на дві літери менше ніж два диз'юнкти, з яких вона отримана. Таким чином, на кожному кроці виведення відбувається спрощення поточної сукупності. Виведення назвемо тупиковим, якщо в диз'юнктах S_n немає жодної контрарної пари і $D_\varnothing \notin S_n$. Тоді нескладно підібрати інтерпретацію, при якій S_n буде істинним. Продемонструємо це на прикладі. Нехай $S_n = \{\ D_1, D_2, D_3\}$, $D_1 = x \vee \neg y \vee z, D_2 = u \vee \neg y, D_3 = z.$ На інтерпретації $I(z) = 1, I(y) = 0$ $(D_1 \& D_2 \& D_3)^i = 1$ і сукупність S_n - не суперечність, а з нею і S (Лема 1.3). Якщо всі виведення тупикові, то сукупність S - не суперечність. Випливає з $(\Leftarrow)$.

◄

Нехай потрібно з'ясувати чи має місце логічний наслідок $A_1, ..., A_n \models B$. Це еквівалентно тому, щоб з'ясувати чи формула $\neg(A_1 \& ... \& \to B_n)$ є суперечністю.

Враховуючи, що $\neg(A_1 \& ... \& \to B_n) \leftrightarrow \neg(\neg(A_1 \& ... \&) \vee B_n) \leftrightarrow$ $(A_1 \& ... \& A_n \& \neg B_n)$, питання зводиться до суперечливості останньої кон'юнкції. Залишилося перетворити усі $A_1, ..., A_n, \neg B$ до КНФ і спробувати вивести з неї порожній – $D_\varnothing$.

Приклад 1.5. З'ясувати чи буде мати місце логічний наслідок

$A \vee B \to C \to D, \neg A \& \neg B \models C \& \neg D.$ Перетворимо всі формули і заперечення останньої до КНФ:

$A \vee B \to C \to D = \neg(A \vee B) \vee (\neg C \vee D) \leftrightarrow \neg A \& \neg B \vee \neg C \vee D \leftrightarrow$
$\leftrightarrow (\neg A \vee \neg C \vee D) \& (\neg B \vee \neg C \vee D)$. (правила де Моргана 6.2 та дистрибутивності 3.2),

$\neg(C \& \neg D) \leftrightarrow \neg C \vee \neg D$ (правило де Моргана 6.2).

Маємо сукупність диз'юнктів: $\{(\neg A \vee \neg C \vee D), (\neg B \vee \neg C \vee D), \neg A, \neg B, \neg C \vee \neg D\}$. Як бачимо, є тільки два варіанти контрарних пар – обидва з парою $(D, \neg D)$. Це значить, що всі інші літери не можуть бути усунені з диз'юнктів в процесі виведень і виведення порожнього диз'юнкту неможливе. Значить логічний наслідок в умові задачі не виконується. ■

Приклад 1.6. З'ясувати чи буде формула $\Phi = ((B \to C) \to (A \vee B) \to C)$ тавтологією. Побудуємо КНФ для заперечення Φ.

$\neg(\neg B \vee C) \vee \neg(A \vee B) \vee C) \leftrightarrow$

$(B \& \neg C) \vee (\neg A \vee C) \& (\neg B \vee C) \leftrightarrow$

$(B \vee (\neg A \vee C) \& (\neg B \vee C)) \& (\neg C \vee (\neg A \vee C) \& (\neg B \vee C) \leftrightarrow$

$(B \vee \neg A \vee C) \& (B \vee \neg B \vee C) \& (\neg C \vee (\neg A \vee C) \& (\neg C \vee \neg B \vee C) \leftrightarrow$

$(B \vee \neg A \vee C)$.

КНФ складається тільки з одного диз'юнкту, а для застосування R-правила потрібно два, тому з даного КНФ не можна вивести порожній диз'юнкт. Значить Φ - не тавтологія.■

1.5. Пропозиційне числення

Якщо секвенційне і резолюційне числення визначенні відповідно на секвенційних деревах та сукупностях диз'юнктів, то класичне *пропозиційне числення* (далі просто пропозиційне числення або скорочено ПЧ) визначено безпосередньо на пропозиційних формулах. Воно дозволяє прямо формально проводити доведення теорем ПЛ і напряму обгрунтовувати логічний наслідок між пропозиційними формулами. Ми розглянемо наступний варіант ПЧ. Воно має одну схему аксіом $\neg A \vee A$, де A – довільна формула і чотири правила виведення:

П1 $A \vdash B \vee A$ (правило розширення)

П2 $A \vee A \vdash A$ (правило поглинання)

П3 $A \vee (B \vee C) \vdash (A \vee B) \vee C$ (права асоціативність)

П4 $A \vee B, \neg A \vee C \vdash B \vee C$ (правило перетину)

Зазначимо, що аксіоми є тавтологіями, а усі правила коректні – між лівими і правими частинами має місце логічний наслідок. З приводу незалежності правил виведення П1-П4 див. Вправи до розділу II.

Нехай Γ - певна сукупність формул, які будемо називати *гіпотезами*. Доведенням формули Φ з гіпотез Γ називається послідовність формул

$\Phi_0,\dots,\Phi_n=\Phi$ така, що для кожного $0\le i\le n$ Φ_i є аксіомою, або гіпотезою, або результатом застосування одного з правил виведення 1)-4) до певних формул з числа $\Phi_0,\dots,\Phi_{i-1}$. Факт існування такого доведення будемо записувати $\Gamma\vdash\Phi$. Нагадаємо, що теоремами в численні називаються формули, для яких існує виведення тільки з аксіом. Записуємо цей факт $\vdash\Phi$.

Розглянемо кілька важливих доведень формул з гіпотез.

Лема 1.5а. Мають місце наступні доведення:

$A\vee B\vdash B\vee A$ (правило комутативності (ПК))

$A, A\to B\vdash B$ (правило відокремлення (МР))

$(A\vee B)\vee C\vdash A\vee(B\vee C)$ (ліва асоціативність (ЛА))

$A\vee B\vdash\neg\neg A\vee B$ ($\neg\neg-$введення)

$\neg\neg A\vee B\vdash A\vee B$ ($\neg\neg-$усунення)

$A\vee(B\vee B)\vdash A\vee B$ (внутрішнє поглинання)

$A\vee(B\vee C)\vdash A\vee(C\vee B)$ (внутрішня комутативність)

$A\to B,\ B\to C\vdash A\to C$ (правило транзитивності)

$A\to B\vdash\neg B\to\neg A$ (правило контрапозиції)

$A_1,\dots,A_n,\ A_1\to\dots\to A_n\to B\vdash B$

►Доведення для 1) : $A\vee B$ (гіпотеза), $\neg A\vee A$ (аксіома), $B\vee A$ (перетин).

Доведення для 2) : $A, \neg A\vee B$ (гіпотези), $B\vee A$ (розширення A), $A\vee B$ (ПК), $B\vee B$ (П4, B (П4.

Доведення для 3) : $(A\vee B)\vee C$, $C\vee(A\vee B)$ (ПК), $(C\vee A)\vee B$ (П3, $B\vee(C\vee A)$ (ПК), $(B\vee C)\vee A$ (П3, $A\vee(B\vee C)$ (ПК).

Доведення для 4) : $A\vee B$, $\neg\neg A\vee\neg A$ (ах.), $\neg A\vee\neg\neg A$ (ПК), $B\vee\neg\neg A$ (П4, $\neg\neg A\vee B$ (ПК).

Доведення для 5) : $\neg\neg A\vee B$, $\neg A\vee A$ (ах.), $A\vee B$ (П4).

Доведення для 6) : $A\vee(B\vee B)$, $(A\vee B)\vee B$ (асоц.), $B\vee(A\vee B)$ (ПК), $A\vee(B\vee(A\vee B))$ (П1, $(A\vee B)\vee(A\vee B)$ (асоц.), $A\vee B$ (П2).

Доведення для 7) : $A\vee(B\vee C)$, $(A\vee B)\vee C$ (асоц.), $((A\vee B)\vee C)\vee B$ (П1+ПК), $(A\vee B)\vee(C\vee B)$ (асоц.), $(C\vee B)\vee(A\vee B)$ (ПК), $A\vee((C\vee B)\vee(A\vee B))$ (П1, $(A\vee(C\vee B))\vee(A\vee B)$ (асоц.), $B\vee((A\vee(C\vee B))\vee A)$ (асоц. + ПК), $(B\vee(A\vee(C\vee B)))\vee A$ (асоц.), $(B\vee(A\vee(C\vee B)))\vee A\vee C$ (П1+ПК), $((A\vee(C\vee B)))\vee A\vee C)\vee B$ (асоц.+ ПК), $((A\vee(C\vee B))\vee A)\vee(C\vee B)$ (асоц.), $(A\vee(C\vee B)\vee(A\vee(C\vee B)$ (П2), $A\vee(C\vee B)$.

Доведення для 8) : $\neg A\vee B, \neg B\vee C$ (гіпотези), $B\vee\neg A$ (ПК), $A\to C$ (П4.

Доведення для 9) : $\neg A\vee B$, $B\vee\neg A$ (ПК), $\neg\neg B\vee\neg A$ ($\neg\neg-$введення), $\neg B\to\neg A$.

Доведення для 10) : $A_1,\dots,A_n, (A_1\to(\dots\to(A_n\to B)\dots)$ (гіпотези), $(A_2\to(\dots\to(A_n\to B)\dots)$, …, $A_n\to B$, B (n разів відокремлення п.2).

◄

Надалі властивості 1)-10) будуть використовуватися як додаткові правила виведення ПЧ.

Теорема 1.5 (повноти для ПЧ). Будь-яка тавтологія Φ є теоремою ПЧ.

► Як правило, для доведення теореми повноти для ПЧ використовують індуктивне означення формул ПЧ та доведення з Леми 1.5а чи їм подібні. Ми підемо іншим шляхом. Скористаємося теоремою про повноту секвенційного числення. Побудуємо термінальне секвенційне дерево D з коренем $\dashv \Phi$. Будемо говорити, що вершина цього дерева має доведення в ПЧ, якщо формула, яка відповідає її секвенції $\vdash \Gamma \dashv \Delta$, є теоремою ПЧ. Нехай $\Gamma = \{\Phi_1,...,\Phi_n\}, \Delta = \{\Psi_1,...,\Psi_m\}$. Нагадаємо, що мова йде про імплікацію $\Phi_1 \wedge ... \wedge \Phi_n \to \Psi_1 \vee ,..., \vee \Psi_m$ (*) або формулу $\Psi_1 \vee ,..., \vee \Psi_m$ (**), якщо $\Gamma = \varnothing$. Теорема буде доведена, якщо ми покажемо, що усі вершини нашого секвенційного дерева мають доведення в ПЧ. Спочатку покажемо, що це справедливо для листків. Оскільки формула Φ є тавтологією, то за теоремою повноти дерево D є замкненим, тобто всі його листки термінальні і замкнені. Перше означає, що Γ і Δ в них складаються тільки з пропозиційних змінних, а друге – що в них обов'язково присутня якась спільна змінна x. Значить $\Gamma \neq \varnothing$.

Нехай в імплікації (*) $\Phi_1 = \Psi_1 = x$. Щоб довести $\vdash x \wedge \Phi_2 \wedge ... \wedge \Phi_n \to x \vee \Psi_2 \vee ,..., \vee \Psi_m$, зазначимо, що маємо аксіому $x \to x$ і достатньо показати, що в ПЧ для будь-яких формул A, B, C існують доведення: (1) $A \to B \vdash A \& C \to B$ та (2) $A \to B \vdash A \to B \vee C$.

Доведення (1). $\neg A \vee B$, $\neg C \vee \neg A \vee B$ (П1), $(\neg C \vee \neg A) \vee B$(асоц.), $(\neg A \vee \neg C) \vee B$(внутрішня комут. 7)), $\neg\neg(\neg A \vee \neg C) \vee B$ ($\neg\neg-$введення), $\neg(A \& C) \vee B$ (озн. кон'юнкції), $A \& C \to B$.

Доведення (2). $\neg A \vee B$, $(\neg A \vee B) \vee C$ (П1+ПК), $\neg A \vee (B \vee C)$ (асоц.), $A \to B \vee C$.

Властивість (1) дозволяє довільно кон'юнктивно розширювати посилку в імплікації, а властивість (2) – те саме робити з висновком тільки диз'юнктивно. Таким чином, всі листки дерева D мають доведення.

Секвенції решти вершин пов'язані з секвенціями безпосередніх вершин-нащадків правилами виведення ПВ1- ПВ4. Покажем, якщо вершини-нащадки мають доведення, то це справедливо і для їхньої батьківської вершини.

Нехай батьківська вершина отримана за правилом ПВ1: $[\Gamma \to \Delta, \Phi] \vdash [\neg\Phi, \Gamma \to \Delta]$. Покажемо, що в ПЧ існують доведення (3) $\Gamma \to \Delta \vee \Phi \vdash \neg\Phi \& \Gamma \to \Delta$ та $\Gamma \to \Phi \vee \Delta \vdash \Gamma \& \neg\Phi \to \Delta$.

Розглянемо перше. $\Gamma \to \Delta \vee \Phi$, $\Phi \vee (\neg\Gamma \vee \Delta)$, $\neg\neg\Phi \vee (\neg\Gamma \vee \Delta)$, $(\neg\neg\Phi \vee \neg\Gamma) \vee \Delta$, $(\neg\neg\Phi \vee \neg\Gamma) \vee \Delta$, $\neg\neg(\neg\neg\Phi \vee \neg\Gamma) \vee \Delta$, $\neg(\neg\Phi \& \Gamma) \vee \Delta = \neg\Phi \& \Gamma \to \Delta$.
Друге доведення аналогічне.

Візьмемо ПВ2: $[\Phi,\Gamma\to\Delta]$ $\vdash$ $[\Gamma\to\Delta,\neg\Phi]$. Покажемо, що (4) $\Phi\&\Gamma\to\Delta\vdash\Gamma\to\Delta\vee\neg\Phi$.

$\Phi\&\Gamma\to\Delta$, $\neg(\Phi\&\Gamma)\vee\Delta$, $\neg\neg(\neg\Phi\vee\neg\Gamma)\vee\Delta$, $(\neg\Phi\vee\neg\Gamma)\vee\Delta$, $\neg\Phi\vee(\neg\Gamma\vee\Delta)$, $(\neg\Gamma\vee\Delta)\vee\neg\Phi$, $\neg\Gamma\vee(\Delta\vee\neg\Phi)$, $\Gamma\to\Delta\vee\neg\Phi$.

Візьмемо ПВ3: $[\Phi,\Gamma\to\Delta]$, $[\Psi,\Gamma\to\Delta]$ $\vdash$ $[\Phi\vee\Psi,\Gamma\to\Delta]$. Покажемо, що

(5) $\Phi\&\Gamma\to\Delta$, $\Psi\&\Gamma\to\Delta\vdash(\Phi\vee\Psi)\&\Gamma\to\Delta$.

$\Phi\&\Gamma\to\Delta$, $\Psi\&\Gamma\to\Delta$, $\neg(\Phi\&\Gamma)\vee\Delta$, $\neg\neg(\neg\Phi\vee\neg\Gamma)\vee\Delta$, $(\neg\Phi\vee\neg\Gamma)\vee\Delta$, $\neg\Phi\vee(\neg\Gamma\vee\Delta)$, $\neg(\Psi\&\Gamma)\vee\Delta$, $\neg\neg(\neg\Psi\vee\neg\Gamma)\vee\Delta$, $(\neg\Psi\vee\neg\Gamma)\vee\Delta$, $\neg\Psi\vee(\neg\Gamma\vee\Delta)$, $\neg(\Phi\vee\Psi)\vee\Phi\vee\Psi$, $\Psi\vee\neg(\Phi\vee\Psi)\vee\Phi$, $\neg(\Phi\vee\Psi)\vee\Phi\vee(\neg\Gamma\vee\Delta)$, $\neg(\Phi\vee\Psi)\vee(\neg\Gamma\vee\Delta)\vee\Phi$, $\Phi\vee\neg(\Phi\vee\Psi)\vee(\neg\Gamma\vee\Delta)$, $\neg(\Phi\vee\Psi)\vee(\neg\Gamma\vee\Delta)\vee(\neg\Gamma\vee\Delta)$, $\neg(\Phi\vee\Psi)\vee(\neg\Gamma\vee\Delta)$, $(\neg(\Phi\vee\Psi)\vee\neg\Gamma)\vee\Delta$, $\neg\neg(\neg(\Phi\vee\Psi)\vee\neg\Gamma)\vee\Delta$, $\neg((\Phi\vee\Psi)\&\Gamma)\vee\Delta$, $(\Phi\vee\Psi)\&\Gamma\to\Delta$.

Візьмемо ПВ4: $[\Gamma\to\Delta,\Phi,\Psi]\vdash[\Gamma\to\Delta,\Phi\vee\Psi]$. Покажемо, що

(6) $\Gamma\to\Delta\vee\Phi\vee\Psi\vdash\Gamma\to\Delta\vee(\Phi\vee\Psi)$. Випливає з правила асоціативності.

Таким чином, всі вершини дерева D мають доведення. А значить і тавтологія Φ в його корені.

◀

Теорему про повноту ПЧ називають ще *теоремою тавтології* (ТТ). Вона має кілька важливих наслідків.

Наслідок 1. Існують і інші повні варіанти ПЧ. Ми фактично довели, що система числення з аксіомою $A\to A$ та правилами виведення (1)-(6) є повним ПЧ. У Вправах наведено приклади інших відомих повних ПЧ. ■

Наслідок 2. Щоб довільне ПЧ було повним необхідно й достатньо, щоб в ньому мали місце: теорема $\vdash A\to A$ та виведення (1)-(6). ■

Наслідок 3. Щоб довести, що в ПЧ має місце виведення з гіпотез $\Gamma\vdash\Psi$ (Ψ є теоремою), $\Gamma=\{\Phi_1,...,\Phi_n\}$ достатньо обгрунтувати, що імплікація $\Phi_1\wedge...\wedge\Phi_n\to\Psi$ (формула Ψ) є тавтологією. ■

Приклад 1.7. а) $\Gamma\vdash\Phi\&\Psi\Leftrightarrow\Gamma\vdash\Phi$, $\Gamma\vdash\Psi$, б) $\Gamma\vdash\Phi\leftrightarrow\Psi\Leftrightarrow\Gamma\vdash\Phi\to\Psi$, $\Gamma\vdash\Psi\to\Phi$.■

Найбільш важливим наслідком ТТ є наступна теорема. Для числень з розв'язною сукупністю аксіом існує загальна стратегія для доведення теорем. Для цього необхідно організувати ефективний перелік усіх доведень в численні і вибрати необхідне. Але ця перебірна стратегія немає практичного сенсу, не кажучи вже про те, що вона часткова.

Теорема 1.6. Існує загальний, відмінний від переборної процедури, метод пошуку доведення будь-якої пропозиційної теореми $\vdash\Psi$.

►Спочатку будується термінальне секвенційне дерево для Ψ і перевіряється чи воно замкнене. Далі достатньо обійти його вершин зліва-направо і знизу-вверх. Отримана в процесі такого обходу послідовність формул вигляду (*) або (**) і є необхідним доведенням. Дійсно, листкам відповідають теореми ПЧ (див. доведення ТТ), а формули усіх інших вершин є результатом застосування правил (3)-(6) з доведення ТТ до деяких попередніх формул у цьому обході. Звертаємо увагу, що з урахуванням комутативності кон'юнкції й диз'юнкції листкам секвенційного дерева можуть відповідати різні теореми.

◄

Приклад 1.8. Повернемося до прикладу 1.3 і побудуємо для тавтології $\neg B\vee C\to\neg(\neg A\vee B)\vee(\neg A\vee C)$ її доведення в ПЧ за процедурою з Теореми 1.6. Відповідне термінальне секвенційне дерево вже побудоване (див. Рис.1.2), тому залишилося лише здійснити його обхід

$A\to A\vee B\vee C$ (аксіома СЧ), $A\vee B\vee C\vee\neg A$ (4), $\neg A\to B\vee C\vee\neg A$ (3), $B\to B\vee C\vee\neg A$ (аксіома СЧ), $(\neg A\vee B)\to B\vee C\vee\neg A$ (5), $(\neg A\vee B)\to B\vee(C\vee\neg A)$ (6), $B\vee(C\vee\neg A)\vee\neg(\neg A\vee B)$ (4), $B\vee((C\vee\neg A)\vee\neg(\neg A\vee B))$ (6), $\neg B\to((C\vee\neg A)\vee\neg(\neg A\vee B))$ (3), $C\&A\to A\vee C$ (аксіома СЧ), $C\to A\vee C\vee\neg A$ (4), $\neg A\&C\to C\vee\neg A$ (3), $C\&B\&A\to C$ (аксіома СЧ), $C\&B\to C\vee\neg A$ (3), $(\neg A\vee B)\&C\to C\vee\neg A$ (5), $C\to C\vee\neg A\vee\neg(\neg A\vee B)$ (3), $C\to(C\vee\neg A)\vee\neg(\neg A\vee B)$ (6), $\neg B\vee C\to(C\vee\neg A)\vee\neg(\neg A\vee B)$ (5).

Зауважимо, що замість аксіоми $A\to A\vee B\vee C$ доведення могло розпочинатися з аксіоми $A\to B\vee A\vee C$ чи $A\to C\vee A\vee B$ з відповідним корегування всього доведення. І друге – загальний метод доведення не є самим коротким та ефективним, але важливо, що він існує і його завжди можна реалізувати. Пряме доведення даної теореми коротше:

$\neg(\neg B\vee C)\vee(\neg B\vee C)$ (аксіома), $\neg(\neg A\vee B)\vee(\neg A\vee B)$ (аксіома), $\neg(\neg B\vee C)\vee(C\vee\neg B)$ (внутр. комут.), $\neg B\vee(\neg(\neg B\vee C)\vee C)$ (асоц.+ ПК),$\neg(\neg A\vee B)\vee(B\vee\neg A)$ (внутр. комут.), $B\vee(\neg(\neg A\vee B)\vee\neg A)$ (асоц.+ ПК),$(\neg(\neg A\vee B)\vee\neg A)\vee(\neg(\neg B\vee C)\vee C)$ (перетин П4), $(\neg(\neg A\vee B)\vee\neg A)\vee$ $(C\vee(\neg(\neg B\vee C))$ (внутр.комут.) $((\neg(\neg A\vee B)\vee\neg A)\vee C)\vee(\neg(\neg B\vee C))$ (асоц.), $(\neg(\neg B\vee C))\vee(\neg(\neg A\vee B)\vee\neg A)\vee C$ (ПК), $\neg(\neg B\vee C)\vee\neg(\neg A\vee B)\vee(\neg A\vee C)$ (асоц.). ■

Наступна теорема дозволяє зводити доведення з гіпотез до доведень теорем ПЧ.

Теорема 1.7 (дедукції для ПЧ).

Для довільних формул A, B $A\vdash B\Leftrightarrow\vdash A\to B$.

► $(\Rightarrow)$ Нехай $A\vdash B$. Індукція за довжиною n виведення $A=B_0,...,B_n=B$. Нехай B - аксіома. Тоді $T\ \vdash B$ і $T\ \vdash A\to B$ за П1. Нехай $B\equiv A$. Тоді $\vdash A\to A$ і $T\ \vdash A\to A$.

Нехай B на останньому кроці виведення в $T[A]$ отримана з формули C за допомогою правил П1-П3. Тоді за ТТ $T\ |\!-C\to B$. За індуктивним припущенням, $T\ |\!-A\to C$ і $T\ |\!-A\to B$ за правилом транзитивності. Нехай B на останньому кроці отримана з формул C та D за допомогою правила П4. Тоді за ТТ $T\ |\!-C\&D\to B$. За індуктивним припущенням, $T\ |\!-A\to C$ і $T\ |\!-A\to D$. Тоді за ТТ $T\ |\!-A\to C\&D$ і $T\ |\!-A\to B$ за правилом транзитивності. ◄

Наслідок 1. Для довільної сукупності гіпотез $\Gamma=\{A_1,...,A_n\}$ і довільної формули $B:\Gamma\,|\!-B \Leftrightarrow |\!-A_1\to...\to A_n\to B$.■

І на завершення розділу 1 зазначимо, що методи доведення теорем ПЛ і обгрунтування логічних наслідків носять універсальний характер і можуть бути застосовані у всіх логічних системах, які містять елементи пропозиційних структур. Ми побачимо як це працює в наступних розділах, присвячених класичній логіці першого порядку.

Відмітимо також, що в ПЛ вивчались і часткові ПЧ, основані на неповних системах зв'язок та з тими чи іншими обмеженнями на сукупності теорем ПЧ. До перших належать, наприклад, імплікативне ПЧ та позитивне ПЧ Гільберта [1,20] до других – різні варіанти інтуїціоністських ПЧ. В останніх не діють, зокрема, такі закони ПЛ як подвійного заперечення та виключення третього [20].

ВПРАВИ

1. Доведіть, що має місце логічний наслідок:

1) $A \models A\vee B$;
2) $A\&B \models A$;
3
) 4) $\{A\to B, C\to D\} \models A\vee C\to B\vee D$;
5) $\{A\to B, C\to D\} \models A\&C\to B\&D$.

∨ 2. Встановіть, чи має місце логічний наслідок:

B 1
)¬ 2
)A 3) $\neg A, A\to B \models \neg B$
∨→B ⊨ B 4) $\neg B, A\to B \models \neg A$
→B ⊨ A 5) $A\to B, C\to D, A\vee D \models B\vee C$
6) $A\vee B, B\to C, \neg A\vee\neg C \models \neg A\vee D$
7) $A\vee B\to C\to D, \neg A\&\neg B \models C\&\neg D$
8) $A\to C, B\to D, A\vee B \models D\&C$
9) $A\to B, C\to D, \neg B\vee\neg D \models \neg A\vee\neg C$

10) $A \to B,\ C \to D \models A \lor C \to B \& D$

11) $A \to B,\ C \to D \models A \& C \to B \lor D$;

12) $A \& D \to B \lor C \models (A \to B) \lor (A \to C) \lor (D \to B)$.

3. Доведіть в пропозиційному численні без використання ТТ:

–

–B→A∨B;

A 3) $\vdash A \to \neg A \to B$;

→ 4) $\vdash (\neg A \to B) \lor \neg A$;

–A∨A→A;

–

(7) $A \to C \vdash A \to B \lor C$;

8) $A \lor B \vdash \neg A \to C \lor B$;

A

A ∨

A

B A

B →

A∨(B→C), B |–A∨C;

A→B→C, B |–A→C;

A→B→C , A→B |–A→C.

B 4. Використовуючи пропозиційне секвенційне числення, встановіть, чи вірно:

1

) 2) $A \to B,\ C \to D \models A \lor C \to B \lor D$

3) $A \to B,\ C \to D \models A \& C \to B \& D$

∨ 4) $A \to B,\ C \to D,\ A \lor D \models B \lor C$

B 5) $A \lor B,\ B \to C,\ \neg A \lor \neg C \models \neg A \lor D$

¬ 6) $A \lor B \to C \to D,\ \neg A \& \neg B \models C \& \neg D$

A 7) $A \to C,\ B \to D,\ A \lor B \models D \& C$

∨ 8) $A \to B,\ C \to D,\ \neg B \lor \neg D \models \neg A \lor \neg C$

9) $A \to B,\ C \to D \models A \lor C \to B \& D$

10) $A \to B,\ C \to D\} \models A \& C \to B \lor D$

11) $A \& D \to B \lor C \models (A \to B) \lor (A \to C) \lor (D \to B)$?

5. Розв’язати Впр.4 за допомогою методу резолюцій.

6. Довести повноту наступних варіантів ПЧ з системою аксіом та правилом МР (див. Лема 1.5а):

a) $A \to (A \& A), A \& B \to A, (A \to B) \to (\neg(B \& C) \to \neg(C \& A))$ (Россер)

b) $A \to (A \lor B), A \lor A \to A, (A \lor B) \to (B \lor A), (B \to C) \to ((A \lor B) \to (A \lor C))$ (Гільберт-Аккерман)

Розділ ІІ. ЛОГІКА ПЕРШОГО ПОРЯДКУ

В класичній логічній системі першого порядку або логіці першого порядку (ЛПП), на відміну від пропозиційної логіки, базові висловлювання структуруються, а до системи зв'язок долучаються квантори. Вона лежить в основі більшості математичних теорій від арифметики натуральних чисел до загальних алгебраїчних систем.

2.1. Синтаксис

Алфавіт мови першого порядку L включає алфавіт символів ПЛ і наступні символи:

- сигнатура функціональних символів $\sigma_f = \{f_i^{n_i} : i \geq 0\}$;
- сигнатура предикатних символів $\sigma_p = \{p_j^{m_j} : j \geq 0\}$;
- символ рівності "=";
- сигнатура констант $\sigma_0 = \{c_i : i \in I\}$, де I – довільна множина індексів;
- сукупність кванторів підтвердження $\{\exists x : x \in V\}$;
- службовий символ ",".

Він потребує коментарів. Нагадаємо, що алфавіт ПЛ складають пропозиційні змінні алфавіту $V = \{x, y, \ldots x_1, y_1, \ldots\}$, зв'язки $\neg, \vee$ та круглі дужки. Пропозиційні змінні ПЛ в ЛПП перейменовуються у предметні і у них тепер зовсім інша роль – вони служать іменами не висловлювань, а довільних елементів предметних областей при інтерпретації мови L. Кожний функціональний та предикатний символи сигнатур σ_f та σ_p має арність – натуральне число $n_i > 0$ та $m_j > 0$, яке пов'язує з символами f_i та p_j відповідну кількість аргументів при їхній інтерпретації як операцій та предикатів. Метасимволи f^n та p^m будуть надалі представляти довільний функціональний та предикатний символи вказаних сигнатур. В метамові арності конкретних символів будуть опускатися, якщо сигнатура фіксована чи відомо, про яку саме конкретну сигнатуру йдеться. Ми будемо розглядати ЛПП з рівністю =, яка представлена окремо від інших предикатних символів. Буває зручно оперувати об'єднаними сигнатурами 1) $\sigma = \sigma_f \cup \sigma_p \cup \sigma_0$ та 2) $\sigma = \sigma_f \cup \sigma_0$. Останній пункт стосується алгебр.

Щоб визначити множину формул ЛПП, необхідно спочатку визначити, що таке терм. Терми – це слова для подання елементів предметних областей, складених функцій та алгебраїчних виразів.

ІО сукупності *термів* T_σ сигнатури σ :

(Б) Всі предметні змінні та константи алфавіту ЛПП є базовими термами, інші символи алфавіту мови (за виключенням предикатних символів) є складовими термів. (І) Для функціонального символу f^n і термів $t_1,...,t_n$ слово $f^n(t_1,...,t_n)$ є термом. (П) Інших термів немає.

Терми з бінарними функціональними символами будемо записувати у звичній інфіксній формі $t_1 f_i^2 t_2$ без зовнішніх дужок.

ІО сукупності F_σ *формул* сигнатури σ :

(Б) Всі вирази вигляду $p^m(t_1,...,t_m)$, де $p^m \in \sigma$, а $t_1,...,t_m \in T_\sigma$, $t_1 = t_2$, а також логічні константи **0** та **1** є базовими формулами. (І) Для формул Φ і Ψ та предметних змінних $x \in \Sigma$ слова $(\neg\Phi)$, $(\Phi \vee \Psi)$ та $(\exists x\Phi)$ є формулами. (П) Інших формул немає.

Формули, утворені за пунктом (І), називаються складеними. В них формули Φ і Ψ називаються підформулами. Також підформулами нових формул будуть і всі власні підформули Φ і Ψ.

Всі елементи метамови ПЛ переносяться і до метамови ЛПП. З'являються й нові: $x \neq y \equiv \neg(x = y)$, універсальний квантор $\forall x\Phi \equiv \neg(\exists x(\neg\Phi))$. В ЛПП діє наступний *пріоритет символів*: $f_i, p_j, Qx, \neg, \&, \vee, \rightarrow$ та $\leftrightarrow$, де $Q \in \{\exists, \forall\}$. Квантори мають однаковий пріоритет. Візьмемо, наприклад, метаформулу $\exists x\ x + z = y \rightarrow x = x \,\&\, \forall z x \neq z + 1$. Вона скорочено представляє формулу $\exists x\,(\neg\,(\exists x((x+z)=y) \rightarrow (x = x \,\&(\neg(\exists z(\neg(x=(z+1)))))))$ (*) . Надалі і формули, і метаформули будемо називати просто формулами. З контексту завжди буде зрозуміло про що йдеться.

Зробимо кілька зауважень, пов'язаних зі структурою формул з F_σ. Нехай формули $\exists x\Phi$ та $\forall x\Psi$ є підформулами формули E. Тоді Φ та Ψ називаються областю дії в E відповідних кванторів. Усі входження змінної x в цих підформулах, як і самі змінні, називаються *зв'язаними* у формулі E . Змінні, які не є зв'язаними у формулі E називаються *вільними*. Це означає, що існують їхні входження в формулу E, які не знаходяться в області дії жодного зі своїх кванторів. У формулі (*) перше й друге входження x є зв'язаним, а решта – вільні, друге й третє входження z – зв'язане, а перше – вільне, змінна y має тільки одне входження і воно вільне. Якщо $x_1,..., x_n$ - всі змінні терму t чи всі вільні змінні формули E, то ці факти будемо записувати так – $t(x_1,...,x_n)$ та $\mathrm{E}(x_1,...,x_n)$. Формула – *замкнена*, якщо вона не має вільних змінних. Терм є замкненим, якщо не містить змінних, тобто побудований тільки з предметних констант.

Далі поговоримо про утворення часткових випадків термів та формул. Часткові випадки утворюються шляхом підстановки в терм або формулу замість змінних тих чи інших термів. При одночасній підстановці в терм t замість змінних x_i термів t_i отримуємо його *частковий випадок* – терм $t_{x_1,...x_n}[t_1,...,t_n]$. З формулами питання складніше. Зв'язані імена можна замінювати на інші тільки, якщо не приводить до колізії – ситуації, коли після такої заміни вільні змінні стають зв'язаними. Наприклад, із формули

$\exists z\ (x+z=y)$ заміною z на u та x можна отримати дві формули $\exists u((x+u)=y)$ і $\exists x((x+x)=y)$. При першій заміні не виникає колізії і формула визначає, як і до заміни, існування різниці $u=y-x$, при другій – колізія має місце і змінює зміст формули – тепер вона визначає існування частки x від ділення y на 2. Якщо заміна успішна, то нова формула називається *варіантою* старої. Вільні входження змінних можна не тільки переіменовувати, а й замінювати на довільний терм, але після цього в новій формулі теж не повинно виникати колізій – змінні терму не повинні зв'язуватися при такій підстановці. Якщо колізія не виникає, то такий терм називається *допустимим* для підстановки. До чого може привести підстановка не допустимого терму, показує наступний приклад: підставимо у формулу $\forall z(x=z)$ замість вільної змінної x терм z. Отримаємо в результаті колізію і всюди істинну формулу $\forall z(z=z)$. Стара ж формула, як побачимо далі, навпаки буде хибною для всіх інтерпретацій, за виключенням одноелементних. Зміст формули перевертається навпаки. Формулу, яка є результатом одночасної підстановки у формулу $\mathrm{E}(x_1,...,x_n)$ замість змінних x_i допустимих термів t_i, позначимо $\mathrm{E}_{x_1,...,x_n}[t_1,...,t_n]$.

Наведемо кілька прикладів мов першого порядку.

Приклад 2.1. 1) *Мова арифметики* L_{ar} має об'єднану сигнатуру $\sigma_{ar}=\{+^2,\times^2,0,1\}$ з двома функціональними символами і двома арифметичними константами (при цьому не забуваємо про рівність =). Всі терми та формули мови арифметики інфіксні. Будемо називати їх *арифметичними*. Для спрощення подання арифметичних термів вважається, що множення є старшим по відношенню до додавання. Тому вираз $b\times x+c$ подає терм $(b\times x)+c$. Вираз $\overbrace{x\times x\times ...\times x}^{n}$ подається степенем x^n. І найбільш радикальне спрощення – символ множення $\times$ між термами може опускатися: вираз t_1t_2 означає $t_1\times t_2$.

Формула (*) є прикладом арифметичної формули Інший приклад – запис квадратного рівняння $ax^2+bx+c=0$.

2) Мова *теорії множин* L_{set} має сигнатуру $\sigma_{set}=\{\in^2\}$ **.** Тоді $x\in z$ – базова формула. а $\forall x\ (x\in z\to x\in y)$ та $\forall x\ (x\notin z)$ – складені формули. Останні в теорії множин виражають відповідно включення "$z\subseteq y$" та рівність"$z=\varnothing$" .■

Зазначимо, що мови ЛПП можуть відрізнятися сигнатурою, базовими пропозиційними зв'язками та способом подання термів і формул. Наприклад, існують бездужкові записи термів і формул – прямий та обернений польські записи: $ft_1...t_n$, $p^m t_1...t_m$, $\neg\Phi$, $\vee\Phi\Psi$, $\exists x\Phi$ (прямий) та обернений – $t_1...t_n f^n$, $t_1...t_m p^m$, $\Phi\neg$, $\Phi\Psi\vee$, $\Phi\exists x$. Мова 1-го порядку L' сигнатури σ' називається *розширенням мови* 1-го порядку L сигнатури σ, якщо їхні алфавіти відрізняються тільки сигнатурами і $\sigma \subset \sigma'$. У цьому разі мова L є *звуженням* мови L'.

Також відмітимо, що особливістю мов 1-го порядку є те, що квантори стосуються тільки предметних змінних. Окремих функціональних і предикатних змінних, значення яких могли б пробігати ті чи інші сукупності функцій в межах однієї інтерпретації у цих мовах немає. Такі змінні з'являються вже у мовах вищих порядків.

2.2. Семантика

Семантику класичних мов першого порядку задають алгебраїчні системи.

Алгебричні системи. Алгебричні системи (АС) – це структури з певними сукупностями об'єктів та всюдивизначених операцій і предикатів на них. Нехай A – довільна множина, $Bool \equiv \{0,1\}$. n*-арною операцією на* A (m*-арним предикатом на* A) називається відображення вигляду $F^n : A^n \to A$ (відображення вигляду $P^m : A^m \to Bool$). Число n (m) визначає арність операції (предиката).

Нехай $\sigma = \sigma_f \cup \sigma_p \cup \sigma_0$- довільна об'єднана сигнатура функціональних, предикатних символів та констант. Кожному функціональному символу $f^n \in \sigma_f$ і кожному предикатному символу сигнатури $p^m \in \sigma_p$, а також кожній константі $c \in \sigma_0$ поставимо у відповідність n - арну операцію f_A^n на A, m -арний предикат p_A^m на A та певний елемент $c_A \in A$. Позначимо σ_A отриману сукупність операцій, предикатів та констант.

Алгебричною системою сигнатури σ називається двійка $A_\sigma = (A;\sigma_A)$.

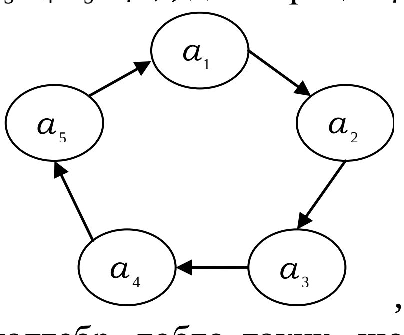
Не порожня множина A називається *носієм* АС, а трійка $(n_1, n_2, ...; m_1, m_2, ...; 0,0,...,0)$, яка утворена з арностей її операцій, предикатів та констант – *типом* τ *АС*. Константи трактуються як 0-арні функціональні символи. Алгебрична система називається: 1) *алгеброю*, якщо сигнатура $\sigma_p = \varnothing$ і 2) *реляційною системою*, якщо сигнатура $\sigma_f = \varnothing$ – порожня.

Арифметика сигнатури $\sigma_{ar} = \{+^2, \times^2, 0, 1\}$ це АС $N_{ar} = (N; +_N, \times_N, 0_N, 1_N\}$ типу $(2,2;0,0)$ з операціями додавання, множення та константами 0 та 1. Надалі будемо опускати індекси в арифметичних операціях і константах, а також і в загальному випадку, коли з контексту буде зрозуміло, що мова йде не про сигнатурні символи, а про їхню інтерпретацію. Одним із найпростіших класів алгебр є *напівгрупи.* Вони мають тип (2). Сигнатура їх складається з єдиної асоціативної бінарної операції – множення. Напівгрупами є натуральні числа відносно операцій додавання та множення, вже згадувана вільна півгрупа слів у певному алфавіті з операцією конкатенації.

Кожну алгебричну систему A_σ можна подати у вигляді певної реляційної системи R_A, якщо операції замінити предикатами, що відповідають їхнім графікам. Наприклад, натуральну арифметику N_{ar} подає реляційна система $R_{ar} = (N; P_1^3, P_2^3, 0_N, 1_N)$, де $P_1^3(x,y,z) \Leftrightarrow x + y = z$, $P_2^3(x,y,z) \Leftrightarrow x \times y = z$.

Підсистеми. Зупинимось тепер на важливому питанні опису (поданні) носія АС за допомогою її операцій. Нехай $A_\sigma = (A, \sigma_A)$ – довільна алгебра. Непорожня підмножина $B \subseteq A$ називається *замкненою* в алгебрі A_σ, якщо вона містить всі константи і замкнена відносно кожної операції системи, тобто якщо результат кожної операції на елементах із B теж належить B. Алгебра $B_\sigma = (B, \sigma_B)$, де σ_B – сукупність операцій алгебри A_σ, обмежених на замкнену підмножину B, називається *підалгеброю* алгебри A_σ. Щоб не ускладнювати позначення, будемо там, де це можливо, обходитися без нових позначень для основних операцій підалгебр і їхніх сукупностей. Із контекста завжди буде зрозуміло про яку операцію – алгебри чи підалгебри йдеться.

Алгебра $\boldsymbol{C} = (\{a_1, a_2, a_3, a_4, a_5\}, f^1)$, де операція f^1 задана графом:



,

не має *власних* підалгебр, тобто таких, що не збігаються із самою алгеброю, а алгебра $N_+ = (N - \{0\}, +)$ має зліченну кількість власних підалгебр, наприклад вигляду $(\{k, k+1, \ldots\}, +), k > 1$.

Має місце

Лема 2.0. Перетин M носіїв всіх непорожніх власних підалгебр даної алгебри A_σ або порожній, або замкнений відносно операцій алгебри.

► Нехай $M \neq \varnothing$, $f_A^n \in \sigma_A$ - довільна операція алгебри і $a_1, \ldots, a_n \in M$. Тоді елемент $f_A^n(a_1, \ldots, a_n)$ належить кожній з підалгебр, а значить і перетину M .◄

Підалгебра $M_\sigma = (M, \sigma_A)$ з Леми 2.1, якщо вона існує, є найменшою (головною) підалгеброю алгебри A_σ. До речі, якщо в сигнатурі алгебри є константи, то найменша підалгебра завжди існує. А в алгебрі N_+ не має головної підалгебри.

Нехай $B \subseteq A$. Серед підалгебр A_σ обов'язково є й надалгебри множини B (напр., сама алгебра A_σ). Нехай $\Re$ – сукупність усіх підалгебр алгебри A_σ, що включають B. Тоді перетин B^* усіх підалгебр з $\Re$ є найменшою підалгеброю алгебри A_σ, що містить усі елементи B. Система $B^*_\sigma = (B^*, \sigma_A)$ називається *підалгеброю* алгебри A_σ, *породженою множиною* B, множина B^* – *замкненням множини* B відносно операцій із σ_A, а елементи множини B – *твірними елементами* замкнення B^*.

Якщо $B^* = A$, то множина B називається *множиною твірних* алгебри A_σ. Алгебра може мати не одну множину твірних. Наприклад, в алгебрі ***C*** кожен елемент a_i є твірним алгебри. Множина твірних називається *незалежною,* якщо вона мінімальна. Отже, щоб визначити довільну алгебру, достатньо описати її основні операції й вибрати одну з незалежних множин твірних. Наприклад, для означення алгебри N_+ достатньо взяти за твірну число 1 і описати операцію додавання. Усі її елементи містяться серед значень: $1,(1+1),((1+1)+1),\ldots$ тощо[4].

Приклад 2.2. Натуральна арифметика $N_{ar} = (N;+,\times,0,1\}$ породжується своїми константами 0 та 1. Це означає, що власних підалгебр ця система немає. ■

Структурна індукція. Поняття алгебричного замкнення лежить в основі індуктивних означень і методу структурної індукції. Важливою властивістю замкнень алгебричної системи є те, що вони припускають доведення методом структурної індукції. Нехай $P(x)$ – певний предикат на замкненні B^* алгебри $\boldsymbol{A}_\sigma$.

Правило *структурної індукції* для замкнення B^*:

(Б) База індукції: $\forall x (x \in B \to P(x))$.

(І) Індуктивний перехід: для всіх основних операцій $f^n_A \in \sigma_A$ і для всіх

$a_1,\ldots,a_n \in B^*$: $\mathop{\&}\limits_{k=1}^{n_i} P(a_k) \to P(f_A(a_1,\ldots,a_n))$.

(П) Повнота: $\forall x (x \in B^* \to P(x))$.

Лема 2.1 (про структурну індукцію). З бази індукції та індуктивного переходу випливає істинність пункту Повнота.

[4] Насправді достатньо часткового випадку додавання – збільшення числа на 1.

►Дійсно, нехай $R=\{x\in B^*:P(x)\}$, тоді з бази індукції випливає $B\subseteq R$, а за індуктивним переходом – $B^*\subseteq R$. Однак $R\subseteq B^*$, отже, $R=B^*$.◄

Таким чином, щоб установити повноту, достатньо перевірити базу індукції та з'ясувати чи виконується індуктивний перехід. Звичайна математична індукція для натуральних чисел є частковим випадком структурної.

Мови ПЛ і ЛПП використовують індуктивні означення основних понять – термів і формул. Це означає, що для доведення їхніх властивостей в багатьох випадках може бути застосована структурна індукція. Ми вже скористалися нею для доведення лем і теорем в Розділі І.

Для доведення тверджень про слова часто використовують звичайну математичну індукцію за довжиною слів. Покажемо, як подібні твердження можуть доводитися за допомогою структурної індукції. Для цього необхідно задати множину слів A^* індуктивно. Нехай A - довільний алфавіт, а $pre:A\times A^*\to A^*$ - операція приписування ліворуч літери до слова: $pre(a,u)=au$. Нехай ε - порожнє слово. Очевидно, що множина всіх слів є замкненням множини $B=\{\varepsilon\}$ відносно операції pre.

Тоді структурна індукція для слів в алфавіті A має вигляд:

(Б) $P(\varepsilon)$;

(І) $\forall a\forall u(a\in A\,\&\,u\in A^*\,\&\,P(u)\to P(au))$;

(П) $\forall u(u\in A^*\to P(u))$.

Нагадаємо, конкатенацією слів u і v називається слово $u\circ v=uv$.

Приклад 2.3. Довести асоціативність операції конкатенації.

► Покладемо $P(u)\equiv\ \forall v\forall w((u\circ v)\circ w=u\circ(v\circ w))$. (Б). Нехай v,w – довільні слова з A^*. Тоді з означення порожнього слова випливає, що $(\varepsilon\circ v)\circ w=v\circ w=vw$ (1) і $\varepsilon\circ(v\circ w)=\varepsilon\circ vw=vw$ (2). Отже, $(1)=(2)$ і $P(\varepsilon)$ виконується. (І). Нехай u,v,w – довільні слова з A^*, $a\in A$ і $P(u)$ виконується. Розглянемо $P(au):(au\circ v)\circ w=au\circ(v\circ w)$. З означень операцій pre та конкатенації і індуктивного припущення, випливає: $(au\circ v)\circ w=pre(a,(u\circ v))\circ w=pre(a,(u\circ v)\circ w))=pre(a,u\circ(v\circ w))=pre(a,u)\circ(v\circ w)=au\circ(v\circ w)$. Отже, (І) виконується, а з ним і повнота (П) ◄.

Інтерпретація мов першого порядку. Щоб задати *інтерпретацію* ***I*** мови 1-го порядку L сигнатури σ, потрібно вибрати певну АС $A_\sigma=(A,\sigma_A)$ сигнатури σ і задати відображення вигляду $I:V\to A$. Тоді алфавітні символи мови L набувають наступних значень:

- пропозиційні зв'язки трактуються як і в ПЛ;
- значення предметних змінних задає відображення I;

* значення сигнатурних символів задають операції, предикати та константи АС A_σ.

Для алфавітного символу s нехай $\boldsymbol{I}(s)$ – його значення при інтерпретації $\boldsymbol{I}$. Тоді для сигнатурних символів маємо: $\boldsymbol{I}(c)=c_A$, $\boldsymbol{I}(f_i)=f_{i_A}$, $\boldsymbol{I}(p_j)=p_{j_A}$. Інтерпретації змінних $I:\Sigma\to A$ та $I':\Sigma\to A$ називаються x-*аналогом* одне одного, якщо вони відрізняються хіба що тільки своїми значенням для x. Інтерпретації $\boldsymbol{I}_1$ і $\boldsymbol{I}_2$ називаються x-*аналогом* одне одного для певного $\boldsymbol{x}\in\boldsymbol{V}$, якщо їхні АС збігаються, а інтерпретації змінних є x-аналогом одне одного.

Терми і формули набувають *значення* індуктивно:

(Б) $\boldsymbol{I}(x_i)=I(x_i)$,

(І) $\boldsymbol{I}(f_i^{n_i}(t_1,...,t_{n_i}))=f_{i_A}(I(t_1),...,I(t_{n_i}))$, $\boldsymbol{I}(p_j^{m_j}(t_1,...,t_{m_j}))=p_{j_A}(I(t_1),...,I(t_{m_j}))$,

$\boldsymbol{I}(\neg\Phi)=\neg\boldsymbol{I}(\Phi)$, $\boldsymbol{I}(\Phi\vee\Psi)=\boldsymbol{I}(\Phi)\vee\boldsymbol{I}(\Psi)$ та $\boldsymbol{I}(\exists x\Phi)=1$, якщо $\boldsymbol{I}_1(\Phi)=1$ для деякого x-аналога $\boldsymbol{I}_1$ інтерпретації $\boldsymbol{I}$.

Значення $\boldsymbol{I}(t)$ і $\boldsymbol{I}(\Phi)$ будемо скорочено позначати t_A^I та Φ_A^I.

При обчисленні значень термів і формул в інтерпретації $\boldsymbol{I}$ зручно вважати всі елементи носія A додатковими константами, які можна підставлятися в терми.

Приклад 2.4. Знайдемо в цілій арифметиці $Z_{ar}=(Z;+,\times,=,0,1)$ значення формули $\Psi(a,b,c)\equiv\exists x(ax^2+bx+c=0)$ при інтерпретаціях I та J таких, що $I(a)=2, I(b)=-2, I(c)=-4$, $J(a)=J(b)=2, J(c)=1$. Формула стверджує, що існує цілочисловий розв'язок квадратного рівняння $ax^2+bx+c=0$. В Ψ змінні a,b,c – вільні, а x- зв'язана. При обчисленні значення термів у формулах, значення вільних змінних просто підставляються в них. Нехай $t=t(x,a,b,c)$ – терм з лівої частини рівняння. Тоді $t_Z^I(x,a,b,c)=(2\times x\times x+(-2)\times x+(-4))_Z^I$. Візьмемо x-аналог I' відображення I такий, що $I'(x)=2$. Тоді $t_Z^{I'}(x,a,b,c)=(2\times 2\times 2+(-2)\times 2+(-4))_Z=0$. За означенням, формула $\Psi(a,b,c)$ в арифметиці Z_{ar} при інтепретації I істинна.

Тепер розглянемо інтерпретацію J і довільний її x-аналог J', $J'(x)=d$. Тоді $t_Z^{J'}(x,a,b,c)=(2\times d\times d+2\times d+1)_Z=(d^2+(d+1)^2)_Z\neq 0$ для будь-якого $d\in Z$. За означенням, формула $\Psi(a,b,c)$ в арифметиці Z_{ar} при інтепретації J хибна. ■

Надалі сигнатуру σ вважаємо фіксованою і там, де це можливо, будемо опускати символ σ. Кожен терм $t(x_1,...,x_n, y_1,...,y_m)$ формули $\Phi(x_1,...,x_n)$ з вільними змінними $x_1,...,x_n$ та зв'язаними $y_1,...,y_m$ представляє при інтерпретації в АС A_σ певну n-арну складену функцію $t_A(x_1,...,x_n)$ на A, в якій зв'язані його змінні виступають як параметри, сама формула представляє n-арний предикат $\Phi_A(x_1,...,x_n)$ на A, а кожна замкнена формула – 0-арний предикат, тобто логічну константу – **0** чи **1**. Значення замкненої формули не залежить від інтерпретації змінних I.

Якщо повернутися до Прикладу 2.4, то терм $t = t(x,a,b,c)$ представляє в Z_{ar} тернарну арифметичну, параметричну відносно x, функцію $t = t_Z^x(a,b,c)$ зі значенням ax^2+bx+c, а формула $\Psi\ (a,b,c)$ – тернарний предикат $\Psi_Z\ (a,b,c)$ на Z, такий що $\Psi_Z\ (a,b,c)=1$ тоді, і тільки тоді, коли існує цілочисловий розв'язок квадратного рівняння $ax^2+bx+c=0$.

Формулу Φ назвемо *істинною* на АС A_σ, якщо предикат Φ_A є істинним, тобто істинним для всіх значень змінних $x_1,...,x_n$ в A. Те, що формула Φ істинна на A_σ, позначатимемо $A_\sigma \models \Phi$.

Формула Φ називається *всюди істинною*, якщо вона істинна на кожній АС сигнатури σ. Всюди істинність формули Φ, як і в ПЛ, будемо позначати $\models \Phi$. Формулу Φ будемо називати *виконуваною* на АС A_σ, якщо предикат Φ_A є виконуваним, тобто істинним принаймні на одному наборі значень змінних.

Приклад 2.5. а) Формула $x = x$ – всюди істинна, в) формула $\forall x \forall y (x = y)$ істинна на всіх 1-елементних АС і тільки на них, с) формула $\neg \forall x \forall y (x = y)$ істинна на всіх АС з двома і більше елементами в носії, d) формула $\Phi_x[t] \to \exists x \Phi$ – всюди істинна. Нехай $(\Phi_x[t])_A^I = 1$ в довільній інтерпретації (A_σ, I) і нехай $t_A^I = a$. Тоді на x – аналозі I' інтерпретації I $I'(x) = a$ маємо $\Phi_A^{I'} = 1$, а значить $\exists x \Phi_A^I = 1$ і $(\Phi_x[t] \to \exists x \Phi)_A^I = 1$.■

Замиканням формули $\Phi\ (x_1,...,x_n)$, де $x_1,...,x_n$ – усі її вільні змінні, називається формула $\overline{\Phi} \equiv \forall x_1 ... \forall x_n\ \Phi\ (x_1,...,x_n)$.

Лема 2.2. Для довільної АС A_σ та формули Φ: $A_\sigma \models \Phi \Leftrightarrow A_\sigma \models \overline{\Phi}$.

►Випливає з означень. Див. Вправи. ◄

Окремим випадком всюди істинних формул є тавтології, тобто формули, які мають структуру тавтології ПЛ. Формуло назвемо пропозиційно нерозкладною, якщо вона атомарна або є підтвердженням $\exists x \Phi$. Нехай F_σ - множина всіх формул мови L, а $F_{\sigma,0}$ - її підмножина усіх пропозиційно нерозкладних формул. Істиностною оцінкою мови L назвемо довільне відображення $\tau : F_{\sigma,0} \to Bool$. Продовжимо індуктивно τ на всю множину F_σ:

$\tau(\neg\Phi) = \neg\tau(\Phi), \tau(\Phi \vee \Psi) = \tau(\Phi) \vee \tau(\Psi)$. Формула Φ є *тавтологією*, якщо для кожної істиностної оцінки τ: $\tau(\Phi) = 1$. Зрозуміло, що всяка тавтологія є всюди істинною формулою, але зворотне не вірно. Наприклад, всюди істинна формула $x = x$ не є тавтологією.

виразний Означення логічного наслідку у мові L те ж, що і в ПЛ: $\Phi \models \Psi \Leftrightarrow \models \Phi \to \Psi$, тобто між формулами Φ і Ψ є *логічний наслідок*, якщо формула $\Phi \to \Psi$ - всюди істинна.

У деяких випадках логічний наслідок між формулами прямо випливає з їхньої пропозиційної структури. Введемо поняття тавтологічного наслідку $\vDash$. Між формулами Φ і Ψ має місце *тавтологічний наслідок* $\Phi \vDash \Psi$, якщо формула $\Phi \to \Psi$ - тавтологія. Очевидно, має місце наступна

Лема 2.3. $\Phi \vDash \Psi \Rightarrow \Phi \models \Psi$.

►Див. Вправи. ◄

Таким чином, наявність тавтологічного наслідку між формулами гарантує наявність між ними і логічного наслідку, але не навпаки. Дійсно, $\exists x \exists y (x = y) \models \exists y \exists x (x = y)$, але не вірно $\exists y \exists x (x = y) \vDash \exists x \exists y (x = y)$.

Формули Φ і Ψ *тавтологічно еквівалентні* $\Phi \sim_T \Psi$, якщо $\Phi \vDash \Psi$ і $\Psi \vDash \Phi$.

Формули Φ і Ψ *логічно еквівалентні* $\Phi \sim \Psi$, якщо $\Phi \models \Psi$ і $\Psi \models \Phi$, тобто якщо $\models \Phi \leftrightarrow \Psi$.

Формула Ψ є *слабким логічним наслідком* формули Φ ($\Phi \Vert\!= \Psi$), якщо для кожної АС A_σ: $A_\sigma \models \Phi \Rightarrow A_\sigma \models \Psi$.

Всі три останні відношення формулюються і для множини гіпотез $\Gamma = \{\Phi_1, ..., \Phi_n\}$. При цьому множина гіпотез трактується як їхня кон'юнкція. Тобто, формула Ψ є логічним наслідком множини формул $\Gamma \models \Psi$, якщо $\Phi_1 \& ... \& \Phi_n \models \Psi$. Аналогічно, для відношень $\vDash$ та $\Vert\!=$.

Лема 2.4. Основні властивості відношень $\vDash$, $\models$, $\Vert\!=$ та $\sim$:

1) $\models \Phi \Rightarrow \Vert\!= \Psi$, але не вірно навпаки; 2) всі відношення рефлексивні та транзитивні; 3) відношення $\sim$ симетричне.

► Для 1) ($\Leftarrow$) є контрприклад: $x = 0 \Vert\!= \forall x (x = 0)$, але не вірно, що $x = 0 \models \forall x (x = 0)$. В арифметиці N_{ar} візьмемо інтерпретацію $I(x) = 0$. Тоді $(0 = 0)_N \to \forall x (x = 0)_N^I =$ $1 \to 0 = 0$ і логічного наслідку $x = 0 \models \forall x (x = 0)$ немає. Щодо інших доведення див. Вправи. ◄

Приклад 2.6. Покажемо, якщо змінна x не входить вільно у формулу Ψ, то $\Phi \to \Psi \Vert\!= \exists x\, \Phi \to \Psi$. Нехай X – сукупність вільних змінних формули $\Phi \to \Psi$. Припустимо супротивне: існує A_σ така, що $A_\sigma \models \Phi \to \Psi$ і не $A_\sigma \models \exists x\, \Phi \to \Psi$, тобто існує така I, що $\exists x\, \Phi_A^I = 1$ і $\Psi_A^I = 0$. За означенням, для деякого x-аналогу інтерпретації I I' такого, що $I'(x) = b$, маємо $\Phi_A^{I'}(b) = 1$. Але x не вільне в Ψ, тому $\Psi_A^{I'} = \Psi_A^I = 0$. Звідси $(\Phi \to \Psi)_A^{I'} = 0$, що суперечить $A_\sigma \models \Phi \to \Psi$. ■

Виразність в АС. Нехай L – мова сигнатури σ, а A_σ – довільна АС. Предикат $P(x_1,...,x_m)$ – *виразний в* A_σ *формулою* $\Phi(x_1,...,x_m)$ мови L, якщо $P(x_1,...,x_m) \sim \Phi_A(x_1,...,x_m)$. Предикат $P(x_1,...,x_m)$ – *виразний* в A_σ, якщо він виразний в A_σ деякою формулою $\Phi(x_1,...,x_m)$ мови L.

Множина, що є областю істинності предиката, виразного в A_σ, називається виразною в A_σ. Графіком функції $f(x_1,...,x_n)$ називається відношення Γ_f на множині A таке, що $(x_1,...,x_n,b) \in \Gamma_f \Leftrightarrow b = f(a_1,...,a_n)$. Функція, графік якої – виразний в A_σ, називається *виразною* в A_σ.

Приклад 2.7. Предикати "$x=0$" та "$x=1$" в АС $(N,\times)$ виражаються формулами $\forall y(x \times y = x)$ та $\forall y(x \times y = y)$ відповідно. ■

Приклад 2.8. Предикати "$x=0$", "$x \le y$" та "$x=1$" в АС $(Z,+)$ виражаються формулами $x+x=x$, $\exists z(x+z=y)$ та $\exists u(u=0 \& x \ne u \& \forall y(y \ne u \to x \le y))$ відповідно. В останній формулі ми використали метасимволи – константу 0 та предикат "$\le$", які виразні в системі $(Z,+)$.■

Приклад 2.9. Предикат "$|x-y=3|$" в АС $(Q, y=x+3,=)$ виражається формулою $y=x+3 \vee x=y+3$.■

Приклад 2.10. Функція $s(x)=x+1$ виражається в АС $(Z,<)$ формулою $\Gamma_s(x,y) \equiv x<y \& \forall z(x<z \to y \le z))$.■

Умова невиразності певного предикату в деякій АС наводиться в наслідку 4 теореми 2.7 про ізоморфізм.

Системи A_σ і B_σ називаються *елементарно еквівалентними* ($A_\sigma \cong B_\sigma$), якщо для будь-якої формули Φ сигнатури σ $A_\sigma \models \Phi \Leftrightarrow B_\sigma \models \Phi$.

Відношення $\cong$ є еквівалентністю на сукупності однотипних АС, тому виразність предиката в одній АС означає його виразність у всьому класі елементарно еквівалентних АС.

Щоб довести не елементарну еквівалентність двох систем, достатньо навести одну формулу, яка істинна тільки в одній з систем.

Приклад 2.11. Чи будуть елементарно еквівалентні системи: а) $(N,+)$ і $(Z,+)$, б) $(N,<)$ і $(N_+,<)$. Для а) відповідь – ні, тому що формула $\Phi \equiv \exists x(x=x+x \& \forall y \forall z(y+z=x \to y=x \& z=x))$ істинна для натуральних чисел і хибна для – цілих. Для б) відповідь – так. Випливає з того, що $\Phi^{I}{}_{(N,+)}$ = $\Phi^{I'}{}_{(N,+)}$, де $I'(x) = I(x)+1$. ■

Предикати, множини та функції виразні в арифметиці натуральних чисел АС N_{ar} називаються *арифметичними.* Істинні арифметичні формули будемо скорочено називати ІАФ. Парне число назвемо числом Гольдбаха, якщо воно є сумою двох простих.

Приклад 2.12. Предикати "x-просте число" та "x - число Гольдбаха" є арифметичними. Вони виражаються формулами: $P_{пр}(x) \equiv \forall y \forall z (z \times y = x \to z = 1 \vee y = 1) \,\&\, x \neq 1$ та $P_{Гольдбах}(x) \equiv \exists y \exists z (P_{пр}(z) \,\&\, P_{пр}(y) \,\&\, x = y + z)$. Перший предикат не є ІАФ, щодо другого, то його істинність в N_{ar} є відомою відкритою проблемою Гольдбаха (бінарний варіант).■

Далі ми побачимо, що арифметичними є широкий клас функцій, який включає, зокрема, усі АОФ.

2.3. Властивості формул

Як і для ПЛ, для логіки першого порядку має місце

Теорема 2.1 (про семантичну еквівалентність)

Нехай формула Φ' отримана із формули Φ заміною деяких входжень формул $\Phi_1, ..., \Phi_n$ на $\Psi_1, ..., \Psi_n$ відповідно. Якщо при цьому $\Phi_i \sim \Psi_i, i = \overline{1,n}$, то $\Phi \sim \Phi'$.

►Індукція по структурі формули Φ. (Б) Для базових формул твердження очевидне, тому що вони не містять власних підформул.(I) Нехай $\Phi \equiv \neg A$ і для підформули A твердження теореми вірне. Враховуючи, що усі підформули Φ – це формула A і її власні підформули, то $\Phi' \equiv \neg(A')$. Тоді за припущенням, $A \sim A'$

Нехай $\Phi \equiv A \vee B$. Підформулами Φ є формули A, B та їхні власні підформули. Нехай для підформул A і B твердження теореми вірне. Тоді $\Phi' \equiv A' \vee B'$ і з припущень $A \sim A', B \sim B'$ випливає еквівалентність $A \vee B \sim A' \vee B'$.

Нехай $\Phi \equiv \exists x A$. Тоді $\Phi' \equiv \exists x A'$. За припущенням, $A \sim A'$, а значить і $\exists x A \sim \exists x A'$. ◄

Теорема 2.2 (про рівність термів)

Нехай терм t' отримано із терма t заміною деяких входжень його підтермів $t_1, ..., t_n$ на терми $s_1, ..., s_n$ відповідно. Якщо $\models t_i = s_i$, $i = \overline{1,n}$, то $\models t = t'$.

► Індукція за структурою терму t. Див. Вправи. ◄

Теорема 2.3 (про рівність для формул)

Нехай формула Φ' отримана із формули Φ заміною деяких входжень її підтермів $t_1, ..., t_n$ на терми $s_1, ..., s_n$ відповідно. Якщо $\models t_i = s_i$, $i = \overline{1,n}$, то $\Phi \sim \Phi'$.

► Індукція за структурою формули Φ. Див. Вправи. ◄

Покажемо тепер, що кожна формула може бути приведена до певного канонічного вигляду. Скажемо, що формула Φ є у *пренексній формі*, якщо $\Phi \equiv Q_1x_1...Q_nx_n\Psi$, де $Q_1,\ldots,Q_n$ - квантори $\exists,\forall$, а Ψ - певна безкванторна формула. Остання називається матрицею пренексної форми, а $Q_1x_1...Q_nx_n$ - її кванторним префіксом.

Має місце наступна

Лема 2.5. Нехай Q - один з кванторів $\exists$ чи $\forall$, $\overline{Q}$ – протилежний квантор - $\forall$ чи $\exists$, B і C – довільні формули і в C немає вільних входжень змінної x. Тоді

$\exists xB \sim \exists yB_x[y]$, $\forall xB \sim \forall yB_x[y]$

$\neg\forall xB \sim \exists x\neg B$, $\neg\exists xB \sim \forall x\neg B$

$QxB \vee C \sim Qx(B \vee C)$,

$QxB \& C \sim Qx(B \& C)$

(a) $QxB \to C \sim \overline{Q}x(B \to C)$, (b) $B \to QxC \sim Qx(B \to C)$.

► 1)-2) очевидно з означень. В 3) – 5) значення формули C в правій і лівій частинах еквівалентностей при інтерпретації змінних I не залежить від конкретного значення змінної x в ній. При обчисленні цього значення буде досліджуватися множина усіх її значення для усіх x - аналогів I. Тому ліва і права частини цих еквівалентностей мають однакові значення для усіх інтерпретацій. ◄

Зазначимо, що завдяки комутативності формули QxB і C в 2) та 3) можна поміняти місцями.

Теорема 2.3 (про пренексну форму)

Для кожної формули Φ існує еквівалентна пренексна форма Φ'.

► Структурна індукція по формулам. (Б) База індукції виконується, тому що базові формули вже в пренексній формі. (І) Нехай B і C - в пренексній формі. Нехай $\Phi \equiv \neg B$. Тоді за допомогою серії еквівалентних перетворень з п.2 Леми 2.5 і на підставі теореми про семантичну еквівалентність отримає пренексну форму для формули $\neg B$. Нехай $\Phi \equiv B \vee C$. За допомогою перейменувань зв'язаних змінних (п.1 Леми 2.5) у формулі $B \vee C$ зробимо так, щоб сукупності зв'язаних і вільних змінних в ній не перетиналися. Тоді знімаються усі обмеження у п.2 Леми 2.5 і за допомогою еквівалентних перетворень з п. 2) (з урахуванням його комутативного варіанту) всі квантори формули $B \vee C$, розпочинаючи з крайніх і самих глибоких справа в C та B, один за одним будуть винесені у кванторний префікс пренексної форми. Теорема про семантичну еквівалентність гарантує еквівалентність фінальної та початкової формул у цьому процесі. Нехай $\Phi \equiv \exists x B$. Тоді за індуктивним припущенням формула Φ вже в пренексній формі.

◀

Наслідок 1. Черговість винесення кванторів в процесі побудови пренексної форми та вибір змінних, що приймають участь у перейменувані, приводять до різних пренексних форм формули, але за теоремою про семантичну еквівалентність всі вони будуть еквівалентними між собою.

Наслідок 2. Для побудови пренексних форм метаформул можна використовувати еквівалентності з пп. 4-5 Леми 2.5.

Приклад 2.13. Побудуємо пренексну форму для формули $\Phi \equiv \forall x \mathrm{A}(x) \to \neg \forall x \exists y B(x,y,z) \,\&\, C(x,y)$.

1. Спочатку звільнимося від обмежень леми 2.4. Для цього проіндексуємо зв'язані входження змінних x та y: $\forall x_1 \mathrm{A}(x_1) \to \neg \forall x_2 \exists y_1 B(x_2,y_1,z) \,\&\, C(x,y)$.

2. Пересуваємо заперечення в глибину формули: $\forall x_1 \mathrm{A}(x_1) \to (\exists x_2 \forall y_1 \neg B(x_2,y_1,z) \,\&\, C(x,y))$.

3. За правилом п.4: $\forall x_1 \mathrm{A}(x_1) \to \exists x_2 \forall y_1 (\neg B(x_2,y_1,z) \,\&\, C(x,y))$.

4) За правилами п. 5b (двічі) та п.5a отримаємо пренексну форму: $\Phi' \equiv \exists x_2 \forall y_1 \exists x_1 (\mathrm{A}(x_1) \to \neg B(x_2,y_1,z) \,\&\, C(x,y))$. Якщо поміняти порядок останніх дій, то отримаємо іншу пренексну форму $\Phi'' \equiv \exists x_1 \exists x_2 \forall y_1 (\mathrm{A}(x_1) \to \neg B(x_2,y_1,z) \,\&\, C(x,y))$. Але форми Φ' та Φ'' будуть еквівалентні.■

Логічний наслідок між множинами формул. Розглянемо тепер поняття логічного наслідку між множинами формул. Нехай Γ, Δ – деякі множини формул, A_σ – довільна АС сигнатури σ. Множина формул Δ є *логічним наслідком множини формул* Γ *в АС* A_σ ($\Gamma \models_A \Delta$), якщо для всіх інтерпретацій змінних I із того, що Φ_A^I =1 для всіх $\Phi\in\Gamma$, випливає що Ψ_A^I =1 для деякої $\Psi\in\Delta$.

Δ є *логічним наслідком* Γ ($\Gamma|=\Delta$), якщо $\Gamma|=_A\Delta$ для всіх АС A_σ.

Теорема 2.4 (про еквівалентність для множин формул)

Нехай $\Phi\sim\Psi$. Тоді маємо $\Phi,\Gamma|=\Delta\Leftrightarrow\Psi,\Gamma|=\Delta$ та $\Gamma|=\Delta,\Phi\Leftrightarrow\Gamma|=\Delta,\Psi$.

►Див.Вправи. ◄

Всі співідношення Леми 1.3 за Лемою 2.3 мають місце і для формул мови 1-го порядку. Доповнимо їх властивостями відношення **|=,** пов'язаними з перетвореннями та елімінацією кванторів.

Лема 2.6. Нехай $y_1,...,y_n$ - довільні змінні, а $y\notin\Gamma\cup\Delta\cup\exists x\Phi$.

R11) $\exists x\neg\Phi,\Gamma|=\Delta\Leftrightarrow\Gamma|=\Delta,\forall x\Phi$

R12) $\Gamma|=\Delta,\exists x\neg\Phi\Leftrightarrow\forall x\Phi,\Gamma|=\Delta$

R13) $\forall x\neg\Phi,\Gamma|=\Delta\Leftrightarrow,\Gamma|=\Delta,\exists x\Phi$

R14) $\Gamma|=\Delta,\forall x\neg\Phi\Leftrightarrow\exists x\Phi,\Gamma|=\Delta$

R15) $\exists x\Phi,\Gamma|=\Delta\Leftrightarrow\Phi_x[y],\Gamma|=\Delta$

R16) $\Gamma|=\Delta,\exists x\Phi\Leftrightarrow\Gamma|=\Delta,\exists x\Phi,\Phi_x[y_1],\dots,\Phi_x[y_n]$

R17) $\forall x\Phi,\Gamma|=\Delta\Leftrightarrow\Phi_x[y_1],\dots,\Phi_x[y_n],\forall x\Phi,\Gamma|=\Delta$

R18) $\Gamma|=\Delta,\forall x\Phi\Leftrightarrow\Gamma|=\Delta,\Phi_x[y]$

► пп. R11 – R15 – очевидні, п. R16 випливає з п. G2 Леми 2.3, п. R17 випливає з лем 2.1, 2.5 (п.1) та теореми 2.4, п. R18 випливає з 2.5 (п.1) та теореми 2.4. ◄

Гомоморфізми та ізоморфізми систем. Нехай L – мова сигнатури σ. Серед усіх її інтерпретацій є подібні. Ми хочемо уточнити це поняття і дослідити поведінку формул мови в таких "споріднених" інтерпретаціях. Про "спорідненість" систем говорять, наприклад, у ситуаціях, коли одна з алгебричних система моделює іншу.

Коли кажуть, що певна система є *моделлю* іншої (первісної) системи, то мають на увазі. що її елементи копіюють (можливо, з деяким наближенням) первісні об'єкти, а основні операції та предикати імітують поведінку основних операцій і предикатів первісної системи. Моделі систем буває легше описати чи реалізувати. Останнє особливо актуальне для прикладної математики та інформатики. Уточнимо це поняття.

Нехай A_σ та B_σ – довільні АС. Відображення $\varphi: A\to B$ називається відображенням системи A_σ в(на) систему B_σ і позначається $\varphi: A_\sigma\to B_\sigma$.

Ізоморфізмом системи A_σ в (на) однотипну систему B_σ називається взаємооднозначне відображення "в" ("на") $\varphi: \mathrm{A}\to B$, яке зберігає головні операції та предикати системи A_σ, тобто для всіх $a_1, a_2, ... \in A$ та всіх $f^n, p^m \in \sigma$:

$$f_A{}^n(a_1,...,a_n)\varphi = f_B^n(\varphi a_1,...,\varphi a_n) \quad (1)$$

$$p_A{}^m(a_1,...,a_m) = p_B{}^m(\varphi a_1,...,\varphi a_m) \quad (2)$$

Ізоморфізм системи на себе називається *автоморфізмом*. Системи, між якими існує ізоморфізм “на” називаються ізоморфними.

Гомоморфізмом φ системи A_σ в (на) однотипну систему B_σ називається відображення системи A_σ в (на) однотипну систему B_σ, яке зберігає головні операції та істинність предикатів: для всіх $a_1, a_2, ... \in A$ та всіх $p^m \in \sigma$:

$$p_A{}^m(a_1,...,a_m) = 1 \Rightarrow p_B{}^m(\varphi a_1,...,\varphi a_m) = 1 \quad (3).$$

Кожний ізоморфізм є гомоморфізмом. Гомоморфізм системи A_σ *в* (*на*) систему B_σ називається *сильним,* якщо для всіх $b_1,...,b_m \in B$ і всіх $p^m \in \sigma$ виконується: із $p_B^m(b_1,...,b_m) = 1$ випливає існування таких прообразів $a_1 = \varphi^{-1}b_1,...,a_m = \varphi^{-1}b_m$ елементів $b_1,...,b_m$ в A, що $p_A^m(a_1,...,a_m) = 1$.

Всякий взаємооднозначний гомоморфізм скінченної системи на себе є автоморфізмом. Дійсно, якщо для деякого вектора $(a_1,...,a_m)$ $p_B{}^m(\varphi a_1,...,\varphi a_m) = 1$, то із (3) випливає $p_B{}^m(\varphi^k a_1,...,\varphi^k a_m) = 1$ для $k = 2,3,...$. Оскільки ϕ є взаємооднозначним відображенням A на себе, то для деякого k степінь ϕ^k буде тотожним відображенням і $p_B{}^m(a_1,...,a_m) = 1$.

Система B_σ є *наближеною моделлю* системи A_σ відносно функцій кодування φ й декодування φ^{-1}, якщо φ є гомоморфізмом системи A_σ в систему B_σ. Зазначимо, що функція декодування – не однозначна і терм $\varphi^{-1}(b)$ подає довільний прообраз b.

Таким чином, щоб знайти значення певної операції системи, достатньо закодувати її аргументи (перейти до моделі), застосувати до них відповідну модельну операцію й розкодувати результат. У випадку, коли гомоморфізм φ сильний, говорять про *сильну модель*. Коли φ взаємооднозначний, то про моделі говорять як про *точні.* Коли ж φ є ізоморфізмом, то говорять про *ізоморфні* моделі.

Розглянемо кілька прикладів моделей систем. Кодування векторів елементів при моделюванні зводиться до кодування їхніх компонентів, тобто кодом вектора елементів є вектор кодів компонентів.

Приклад 2.14. Десяткова і двійкова арифметики цілих чисел ізоморфні відносно функцій кодування й декодування, що переводять десяткові числа в рівні їм двійкові, і навпаки ■

Приклад 2.15. Розглянемо систему $R_1 \equiv (R_+, \times, =)$ додатних дійсних чисел з операцією множення й систему $R_2 \equiv (R, +, =)$ усіх дійсних чисел з операцією додавання. Вони ізоморфні відносно функцій кодування $\lg x$ і декодування 10^x. Дійсно, досить згадати тотожність $\lg(x \times y) = \lg x + \lg y$. ■

Моделі й конгруенції. У зв'язку з поняттям моделі цілком природно постають питання: якою є сукупність усіх можливих моделей даної системи, чи є серед них моделі з тими чи іншими властивостями тощо? Спробуємо дати певну відповідь на ці й подібні запитання.

Нехай ρ – деяка еквівалентність на системі A_σ, $[a]_\rho$ – фактор–клас еквівалентності ρ, що містить елемент a, $[A]_\rho$ – сукупність усіх фактор-класів відношення ρ. Відображення вигляду $\chi: A \to [A]_\rho$ та $\chi^{-1}: [A]_\rho \to A$ такі, що $\chi a = [a]_\rho, \chi^{-1}[a]_\rho = a$ називаються канонічними. Кажуть, що відношення ρ *стабільне* відносно n-арної операції $f_A \in \sigma_A$, коли для будь-яких $a_1,...,a_n, b_1,...,b_n \in A$ таких, що $a_i \rho b_i$ для всіх $1 \le i \le n$, виконується $f_A(a_1,...,a_n) \rho\ f_A(b_1,...,b_n)$.

Еквівалентність ρ на системі A_σ називається *конгруенцією*, якщо вона стабільна відносно кожної головної операції системи.

Щоб спростити позначення, зафіксуємо певну конгруенцію ρ на системі A_σ і будемо пустимо індекс ρ в позначеннях фактор-класів. Конгруенція ρ дозволяє визначити на фактор-класах $[A]$ *фактор-систему* $[A]_\sigma = ([A], \sigma_{[A]})$, яка є моделлю системи A_σ. А саме, для всіх $a_1, a_2, ... \in A$ та всіх $f^n, p^m \in \sigma$ покладемо:

$f^n_{[A]}([a_1],...,[a_n]) = [\, f^n_A(a_1,...,a_n)]$ та $p^m_{[A]}([a_1],...,[a_m]) = 1 \Leftrightarrow$ існують такі $a_1' \in [a_1],...,a_m' \in [a_m]$, що $p^m_A(a_1',...,a_m') = 1$.

Означення операцій та предикатів системи $[A]_\sigma$ коректне і канонічне відображення вигляду $\chi: A \to [A]$ є сильним гоморфізмом системи A_σ на фактор-систему $[A]_\sigma$.

Кожний гомоморфізм $\varphi: A_\sigma \to B_\sigma$ породжує на елементах системи A_σ відношення *ядерної* еквівалентності $\theta \subseteq A \times A: a\theta b \Leftrightarrow a\varphi = b\varphi$.

Має місце наступна

Лема 2.6 (про ядерну еквівалентність гомоморфізму). Ядерна еквівалентність θ гомоморфізму $\varphi: A_\sigma \to B_\sigma$ системи A_σ в систему B_σ є конгруенцією. Канонічні відображення $\chi: A \to [A]_\theta$ та $\chi^{-1}: [A]_\theta \to A$ є гомоморфізмами. Якщо $\varphi: A_\sigma \to B_\sigma$ – сильний гомоморфізм, то B_σ є точною моделлю системи $[A]_\sigma$.

►Див. Вправи. ◄

Отже, кожній сильній моделі B_σ системи A_σ відповідає певна ізоморфна їй фактор-система системи A_σ. Ураховуючи, що кожна фактор-система $[A]_\sigma$ за конгруенцією є сильною моделлю системи A_σ, можемо зробити важливий висновок

Лема 2.7. Сукупність усіх сильних моделей системи A_σ з точністю до ізоморфізму вичерпується сукупністю всіх її фактор-систем за різними конгруенціями.

►Випливає з леми 2.6 . ◄

Таким чином, задачі: 1) знайти з точністю до ізоморфізму всі сильні моделі системи A_σ та 2) знайти всі конгруенції на A_σ – рівносильні.

Приклад 2.16. На кожній системі A_σ є принаймні дві конгруенції – рівність і тотальна. У першому випадку кожний фактор-клас з $[A]_\sigma$ одноелементний, у другому – сукупність $[A]_\sigma$ одноелементна і її елемент збігається з носієм системи. ■

Приклад 2.17. Розглянемо приклад моделі алгебри $N_+ = (N - \{0\}, +)$. Нехай $B_2 = (\{-1,1\}; \times)$ – двоелементна алгебра, тоді відображення $\varphi n = (-1)^n$ є гомоморфізмом алгебри N_+ на алгебру B_2, тобто остання є наближеною моделлю N_+. Дійсно, $(-1)^{n+m} = (-1)^n \times (-1)^m$. Сукупність $[N_+]$ – для даного гомоморфізму двоелементна і складається з підмножин парних і непарних чисел. Як бачимо, при гомоморфізмі наближена модель може бути дуже грубою. Крім даної ядерної конгруенції, на N_+ існують і інші конгруенції. (Див. Вправи.) ■

Вільні АС. При вивченні й моделюванні однотипних систем сигнатури σ важлива роль належить вільним системам. Носієм вільної системи є сукупність T_σ усіх можливих термів, що відповідають функціональним символам та символам-констант сигнатури σ. З кожним функціональним символом $f^n \in \sigma$ пов’яжемо конструктор термів $\hat{f}^n$, який за термами $t_1,...,t_n$ будує терм $f^n(t_1,...,t_n)$, тобто $\hat{f}^n(t_1,...,t_n) = f^n(t_1,...,t_n)$.

Визначимо сукупність T як замкнення множини предметних констант сигнатури σ відносно всіх операцій-конструкторів $\hat{f}_i$.

Вільною *АС* сигнатури σ $U_\sigma = (T_\sigma, \sigma_T)$ називається довільна *АС* на універсумі термів T_σ, операції та предикати якої є операції-конструктори термів та предикати на термах. Одним із найпростіших прикладів вільних АС є вільна напівгрупа $Fs = (W^*, \circ, \varepsilon, c_w : w \in W)$ слів з операцією конкатенації слів, одиницею та константами – однобуквеними словами алфавіту W.

Покажемо, що будь-яка система A_σ є сильною моделлю вільної АС U_σ сигнатури σ, тобто система A_σ ізоморфна певній фактор-системі вільної системи U_σ.

Теорема 2.5 (про вільні системи). Відображення "на" $\varphi : V \to A$, може бути єдиним чином розширене до гомоморфізму вільної системи U_σ на систему A_σ.

►Для кожного функціонального та предикатного символів $f^n, p^m \in \sigma$ покладемо $\varphi f^n(t_1,...,t_n) = f_A^n(\varphi t_1,...,\varphi t_n)$, $p_T^m(t_1,...,t_m) = p_A^m(\varphi t_1,...,\varphi t_m)$. Тоді відображення $\varphi : T_\sigma \to A$ – гомоморфізм і "на" за побудовою.

Нехай ϕ – інший гомоморфізм і $\phi c = \varphi c, c \in \sigma_0$. Покажемо, що $\phi = \varphi$. Застосуємо структурну індукцію для термів. База (Б) індукції виконується. (І) Нехай $\phi t_1 = \varphi t_1, ..., \phi t_n = \varphi t_n$ і розглянемо терм $f^n(t_1,...,t_n)$. Тоді

$$\varphi f^n(t_1,...,t_n) = f_A^n(\varphi t_1,...,\varphi t_n) = f_A^n(\phi t_1,...,\phi t_n) = \phi f^n(t_1,...,t_n). ◄.$$

Як свідчить теорема 2.5, вибираючи в кожному фактор-класі $[U_\sigma]$ певний терм за канонічний представник усього класу, можна отримати термальну копію будь-якої системи A_σ й перейти від абстрактних елементів носія A до конкретної множини термів. Це відкриває універсальний шлях до словарного моделювання довільних систем.

Тепер повернемося до формул мови L. Має місце наступна

Теорема 2.6 (про гомоморфізм для термів).

Нехай $\varphi : A \to B$ – гомоморфізм АС A_σ в B_σ. Тоді для будь-якого терму t і довільної інтерретації змінних I в A: $\varphi t_A^I = t_B^{I'}$, де $I' = \varphi I$.

► Структурна індукція для термів. (Б) База випливає з означення $I' = \varphi I$. (І) Нехай $t = f(t_1,...,t_n)$, і $\varphi t_{iA}^I = t_{iB}^{I'}$ $\forall 1 \le i \le n$. Нехай $t_{iA}^I = a_i$, $t_{iB}^{I'} = b_i$ для певних $a_i \in A$, $b_i \in B$. Тоді $t_B^{I'} = f_B(t_{1B}^{I'},...,t_{nB}^{I'}) = f_B(b_1,...,b_n)$ і

$\varphi f_A(a_1,...,a_n) = f_B(b_1,...,b_n)$ за властивістю 1) гомоморфізму.

◄

Теорема 2.7 (про ізмоморфізм для формул).

Нехай $\varphi: A \to B$ – ізоморфізм системи A_σ на B_σ. Тоді для будь-якої формули Φ і довільної інтерпретації змінних I в A: $\Phi_A^I = \Phi_B^{I'}$, де $I' = \varphi I$.

►Структурна індукція для формул. (Б) База випливає з теореми про гомоморфізм для термів і властивості 2) з означення ізоморфізму. (І) Якщо твердження теореми вірне для формул A та B, то воно буде вірне і для формул $\neg\mathrm{A}$, $\mathrm{A} \vee \mathrm{B}$ та $\exists x\mathrm{A}$ (див. Вправи).

◄

Наслідок 1. Формула Φ сигнатури σ всюди істинна, тоді і тільки тоді, коли вона істина в кожній вільній АС U_σ . ■

Наслідок 2. Для встановлення неізоморфності двох систем, достатньо знайти формулу сигнатури σ, яка їх розділяє, тобто яка істина в одній системі і хибна в іншій. Наприклад, системи $(N,+)$ і $(Z,+)$ з прикладу 2.11 не ізоморфні, тому що їх розділяє формула $\Phi \equiv \exists x(x = x + x \,\&\, \forall y \forall z(y + z = x \to y = x \,\&\, z = x))$. ■

Наслідок 3. Нехай $\varphi: A \to A$ – автоморфізм АС A_σ. Тоді для будь-якої формули $\Phi\,(x_1,...,x_m)$ мови L і довільної інтерпретації змінних $Ix_i = a_i$, $i = \overline{1,m}$: $\Phi_A^I\,(a_1,...,a_m) = \Phi_A^{I'}\,(\varphi a_1,...,\varphi a_m)$, де $I' = \varphi I$. Тобто, при автоморфізмі усі формули зберігають свої значення.■

Наступний наслідок надає достатню умову невиразності в АС певної властивості.

Наслідок 4. Нехай $P\,(x_1,...,x_m)$- довільний предикат на A, φ – певний автоморфізм АС A_σ і для певних $a_1,...,a_m \in A$ $P\,(a_1,...,a_m) \neq P\,(\varphi a_1,...,\varphi a_m)$. Тоді предикат P – не виразний в системі A_σ. Дійсно, як випливає з Наслідку 3, при автоморфізмі всі формули мови L зберігають своє значення, тому формули еквівалентної P в L не існує. ■

Приклад 2.18. 1) Предикат "$x + y = z$" не виразний в АС $Z_< = (Z;<)$. Тому, що зсув множини Z вправо або вліво на певну константу c є автоморфізмом системи $Z_<$, для якого $0 + 0 = 0$, але $(0 + c) + (0 + c) \neq (0 + c)$.

2) Предикат "$x < y$" не виразний в АС $(Z;+)$. Тому, що дзеркальне відображення $\varphi x = -x$ є автоморфізмом системи $(Z;+)$, для якого $2 < 3$, але $-2 > -3$.

3) Предикат "$y = x + 1$" не виразний в АС $(N; y = x + 2)$. Просто зсув множини в право буде автоморфізмом "в", а не "на". Тому розглянемо

комбінований зсув φ : на +1 вправо для парних чисел і зсув вліво на -1 – для непарних. Такий зсув вже буде автоморфізмом нашої системи, для якого $2=1+1$, але $\varphi(2)\neq\varphi(1)+1$, тому що $\varphi(2)=3,$ а $\varphi(1)=0.$

4) Предикат “$x=2$” не виразний в АС $(N;\times)$. Відображення $\varphi(2^a3^bc)=2^b3^ac$ є автоморфізмом системи $(N;\times)$, для якого $2=2$, але $\varphi 2=3\neq 2$.■

Зауваження. Якщо виникає необхідність у розгляді властивостей алгебричних систем з частковими операціями та предикатами, то в багатьох випадках буває достатньо ввести спеціальний новий елемент # – невизначеність і часткові операції та предикати довизначити цим значенням на елементах поза областю визначення. Щоправда, для предикатів це приводить до необхідності розгляду трьохзначної логіки, тому зв’язки ЛПП також необхідно довизначити аналогічно – щоб вони зберігали невизначеність, якщо, принаймні, один з аргументів є невизначенність. Нова логіка буде мати ті ж основні властивості, що і класична ЛПП.

2.4. Секвенційне числення першого порядку

Сутність секвенційного числення 1-го порядку (СЧ-1) та ж, що і в ПЛ – спроба звести відношення логічного наслідку між формулами до логічного наслідку між їхніми частинами. Не дивно, що і формально СЧ-1 спирається на пропозиційне СЧ. Формулами СЧ-1 є формули ЛПП, *секвенціями* – вирази вигляду $[\Gamma\Rightarrow\Delta]$, де Γ, Δ – сукупності формул, а символи [,] є метасимволами, *аксіомами* – замкнені секвенції вигляду $[\Phi,\Gamma\Rightarrow\Delta,\Phi]$. До *правил виведення* ПВ1-ПВ10 з пропозиційного СЧ долучаються правила для маніпуляції з кванторами (Лема 2.6). Секвенція $[\Gamma\Rightarrow\Delta]$ *виконується*, якщо має місце логічний наслідок $\Gamma\models\Delta$. Секвенція – *вивідна* в СЧ-1 (є теоремою), якщо вона має доведення з аксіом

Нагадаємо, що $x,y_1,...,y_n$ - довільні змінні, а $y\notin\Gamma\cup\Delta\cup\exists x\Phi$. Покладемо

ПВ11) $[\Gamma\Rightarrow\Delta,\forall x\Phi]\ \vdash [\exists x\neg\Phi,\Gamma\Rightarrow\Delta]$

ПВ12) $[\forall x\Phi,\Gamma\Rightarrow\Delta]\ \vdash [\Gamma\Rightarrow\ \Delta,\exists x\neg\Phi]$

ПВ13) $[\Gamma\Rightarrow\Delta,\exists x\Phi\ ]\ \vdash [\ \forall x\neg\Phi,\Gamma\Rightarrow\Delta]$

ПВ14) $[\exists x\Phi,\Gamma\Rightarrow\Delta\ ]\ \vdash [\ \Gamma\Rightarrow\Delta,\forall x\neg\Phi]$

ПВ15) $[\Phi_x[y],\Gamma\Rightarrow\Delta]\ \vdash [\exists x\Phi,\Gamma\Rightarrow\Delta]$

ПВ16) $[\Gamma\Rightarrow\Delta,\exists x\Phi,\ \Phi_x[y_1],\ldots,\Phi_x[y_n]]\vdash [\Gamma\Rightarrow\Delta,\exists x\Phi\ ]$

ПВ17) $[\Phi_x[y_1],\ldots,\Phi_x[y_n],\forall x\Phi,\Gamma\Rightarrow\Delta]\ \ \vdash [\forall x\Phi,\Gamma\Rightarrow\Delta\ ]$

ПВ18) $[\Gamma\Rightarrow\Delta,\ \Phi_x[y]]\vdash [\Gamma\Rightarrow\Delta,\forall x\Phi]$.

Правила виведення з числа ПВ1 – ПВ18 з парними номерами будемо називати *лівими правилами* для даної зв'язки, а з непарними номерами – *правими*. Наприклад, будемо говорити про правила: правого заперечення (праве $\neg$-правило) для ПВ2, лівої диз'юнкіції (ліве $\vee$-правило) ПВ3, лівого підтвердження (ліве $\exists$- правило) ПВ15 тощо.

Лема 2.8. Числення СЧ-1 є коректним, тобто всі його теореми-секвенції є виконуваними.

► Індукція за структурою секвенцій. Аксіоми СЧ-1 є виконуваними секвенціями, а правила виведення П11-П18 зберігають виконуваність за Лемою 2.6.◄

Як і в ПЛ, вводиться спрощена форма секвенцій $\vdash \Gamma \dashv \Delta$. Поняття севенційного дерева в СЧ-1 те ж , що і в пропозиційному випадку з урахуванням додаткових правил для кванторів ПВ11 – ПВ18. Розглянемо приклад побудови секвенційного дерева.

Приклад 2.19. Побудуємо секвенційне дерево з коренем $\dashv (\exists xP(x) \to Q(x)) \to P(x) \to \exists xQ(x)$ (Рис. 2.1).

$$\dashv (\exists xP(x) \to Q(x)) \to P(x) \to \exists xQ(x).$$

$$\vdash \exists xP(x) \to Q(x),\ \dashv P(x) \to \exists xQ(x) \text{ ПВ8}$$

$$\dashv \exists xP(x),\ \dashv P(x) \to \exists xQ(x) \qquad \vdash Q(x),\ \dashv P(x) \to \exists xQ(x) \text{ ПВ7}$$

$$\dashv \exists xP(x),\ \vdash P(x),\ \dashv \exists xQ(x) \text{ ПВ8} \qquad \vdash Q(x),\ \vdash P(x),\ \dashv \exists xQ(x) \text{ ПВ8}$$

$$\dashv \exists xP(x), \dashv P(x), \vdash P(x), \dashv \exists xQ(x)\ \times\text{ПВ16} \quad \vdash Q(x), \dashv Q(x), \vdash P(x), \dashv \exists xQ(x)\ \times \text{ПВ16}$$

Дерево замкнене. ■

Теорема 2.8 (повноти для СЧ-1). Нехай $\Gamma \models \Delta$. Тоді секвенція $\vdash \Gamma \dashv \Delta$ вивідна.

► Для доведення цієї теореми потрібна певна підготовка. Відразу зазначимо, що ми будемо розглядати тільки секвенції з основних формул, тобто формул без метазв'язок . Секвенційне дерево для певної секвенції будемо називати термінальним, якщо воно скінченне і всі його листки або замкнені, або містять тільки секвенції з виключно базових формул або це дерево є нескінченним. Секвенційне дерево – замкнене, якщо воно скінченне і всі його листки є замкненими. Зазначимо, що в СЧ-1, на підміну від пропозиційного СЧ, не всяке замкнене дерево може бути продовжене до термінального дерева (причина – в правому $\exists$-правилі ПВ16).

Розглянемо тепер більш детально процедуру побудови термінального секвенційного дерева для довільної секвенції $\Sigma \equiv \vdash \Gamma \dashv \Delta$. Така побудова розпочинається з кореня дерева Σ, яке "росте" вниз, як у прикладі 2.19. В процесі побудови від складніших формул переходимо до простіших (і до них самих – у випадку правого $\exists$-правила) за допомогою правил ПВ1-ПВ4 та ПВ15-ПВ16, застосовуючи їх справа наліво.

Зафіксуємо деякий потенційно необмежений список TN предметних змінних, що не зустрічаються в секвенції Σ.

Спробуємо унормувати процес побудови секвенційного дерева, розбивши його на етапи. На першому етапі доступна лише пара перших формул списків $\vdash\Gamma$ та $\dashv\Delta$ (або єдина $\dashv$-формула чи $\vdash$-формула, якщо один із списків порожній). Кожне застосування секвенційного правила проводиться до скінченної множини *доступних* на даний момент формул.

На початку кожного етапу виконується *крок доступу*: до списку доступних формул додаємо по одній формулі зі списків $\dashv$-формул чи $\vdash$-формул. Якщо недоступних $\dashv$-формул чи $\vdash$-формул немає (відповідний список вичерпаний), то на подальших кроках доступу додаємо по одній формулі ще невичерпаного списку. Нехай виконано k етапів процедури. На етапі k+1 перевіряємо, чи буде кожен з листів дерева замкненою секвенцією. Якщо всі листи замкнені, то процедура успішно завершена, ми отримали замкнене секвенційне дерево. Якщо ні, то для кожного незамкненого листа ξ робимо наступний крок доступу, після чого добудовуємо піддерево з вершиною ξ наступним чином: а) активізуємо всі доступні складені формули ξ, б) по черзі до кожної активної формули застосовуємо відповідне секвенційне правило, в) після виконання правила формула стає пасивною, до пасивних та утворених на даному етапі формул секвенційні правила не застосовуються. Повтори формул усуваються.

Деталізуємо далі п. б). Спершу виконуємо всі ліві $\exists$-правила. При його застосуванні беремо ім'я y – перше з ще не використаних до цього у списку TN. Після застосування всіх лівих $\exists$-правил, до кожної з решти активних формул застосовуються відповідно правила ліве і праве заперечення, ліва і права диз'юнкція та праве $\exists$-правило. При застосуванні останнього правила $y,...,y_n$ - вільні змінні формул листка і його наступників, якщо ж таких імен немає, то береться перше незадіяне ім'я списку TN.

При побудові дерева можливі такі випадки:

1) Процедура завершена позитивно, маємо замкнене дерево.

2) Процедура завершена негативно, маємо скінченне незамкнене дерево. В дереві існує скінченний шлях $\Sigma \equiv \Sigma_1,\ \Sigma_2,\ \ldots,\ \Sigma_n$, всі вершини якого – незамкнені секвенції, а всі формули останньої Σ_n – базові. Такий шлях ρ назвемо незамкненим. До формул Σ_n жодне з секвенційних правил вже не застосовне.

3) Процедура не завершується, маємо нескінченне незамкнене дерево. За лемою Кеніга нескінченне дерево із скінченними розгалуженнями має хоча б один нескінченний шлях. Вершини цього шляху не можуть бути замкненими секвенціями, бо при появі замкненої секвенції до неї вже не

застосовується секвенційні правила і процес побудови дерева для цього шляху обривається.

Отже, в дереві існує нескінченний шлях $\rho \equiv\ \Sigma = \Sigma_1,\ \Sigma_2,\ \ldots,\ \Sigma_n,\ \ldots$ всі вершини якого – незамкнені секвенції. Такий шлях також назвемо незамкненим.

Кожна з формул секвенції $\mathbf{\Sigma}$ зустрінеться на шляху ρ і стане доступною. Нехай H – множина всіх формул шляху ρ, W – множина всіх вільних змінних формул з H.

Нам знадобиться поняття модельної множини. Множина H відмічених формул *модельна*, якщо виконуються такі умови:

H_0) Для кожної базової формули Φ лише одна з формул $\vdash\Phi$ чи $\dashv\Phi$ може належати до H.

$\mathrm{H}\neg$) Якщо $\dashv\ \neg\Phi \in \mathrm{H}$, то $\vdash \Phi \in \mathrm{H}$; якщо $\dashv \Phi \in \mathrm{H}$, то $\vdash\neg\Phi \in \mathrm{H}$.

$\mathrm{H}\vee$) Якщо $\dashv\ \Phi \vee \Psi \in \mathrm{H}$, то $\dashv\ \Phi \in \mathrm{H}$ або $\dashv\ \Psi \in \mathrm{H}$;

якщо $\vdash \Phi \vee \Psi \in \mathrm{H}$, то $\vdash\ \Phi \in \mathrm{H}$ та $\vdash \Psi \in \mathrm{H}$.

$\mathrm{H}\exists$) Якщо $\dashv\ \exists x\Phi \in \mathrm{H}$, то існує $y \in W$ таке $\dashv\ \Phi_x[y] \in \mathrm{H}$;

якщо $\vdash \exists x\Phi \in \mathrm{H}$, то для всіх $y \in W \vdash \Phi_x[y] \in \mathrm{H}$.

Лема 2.9. Якщо ρ – незамкнений шлях в секвенційному дереві, а H - множина всіх відмічених формул секвенцій цього шляху, то H - модельна множина.

► Для переходу від поточної вершини до наступної використовується одне з секвенційних правил ПВ1-ПВ4 та ПВ15-ПВ16. При цьому секвенція поточної вершини знаходиться в правій частині правила, а секвенції її нащадків – в лівій. Два нащадки буде тільки при застосування правила ПВ3.

Ці переходи точно відповідають пунктам $\mathrm{H}\neg$, $\mathrm{H}\vee$ та $\mathrm{H}\exists$) визначення модельної множини. Кожна складена формула, що зустрічається на шляху ρ, рано чи пізно буде розкладена згідно секвенційних правил. Всі секвенції шляху ρ незамкнені, тому виконується пункт H_0 визначення модельної множини.

◄

Лема 2.10. Нехай H - модельна множина. Тоді існують АС $A_\sigma = (A, \sigma_A)$ з носієм A, потужність якого збігається з потужністю множини W і ін'єктивне відображення $I : W \to A$ такі, що (1) якщо $\vdash \Phi \in \mathrm{H}$, то Φ_A^I=1, (2) якщо $\vdash \Phi \in \mathrm{H}$, то Φ_A^I=0.

► Індукція за структурою формули Φ з врахуванням способу побудови модельної множини.

(Б) З урахуванням п. H_0 означення модельності для базових формул з H покладемо: Φ_A^I=1 для $\vdash\Phi$ та Φ_A^I=0 для $\vdash\Phi$.

(І) Нехай $\vdash\neg\Phi\in\mathrm{H}$. За визначенням H, маємо $\dashv\ \Phi\in\mathrm{H}$. За припущенням індукції Φ_A^I=0, звідти $\neg\Phi_A^I$=1.

Нехай $\dashv\neg\Phi\in\mathrm{H}$. За визначенням H, маємо $\vdash\Phi\in\mathrm{H}$. За припущенням індукції Φ_A^I=1, звідки $\neg\Phi_A^I$ =0.

Нехай $\dashv\ \Phi\vee\Psi\in\mathrm{H}$. За визначенням H, маємо $\dashv\ \Phi\in\mathrm{H}$ або $\dashv\ \Psi\in\mathrm{H}$. За припущенням індукції, Φ_A^I=1 або Ψ_A^I=1, звідки $(\Phi\vee\Psi)_A^I=1$.

Нехай $\vdash\Phi\vee\Psi\in\mathrm{H}$. За визначенням H маємо $\vdash\Phi\in\mathrm{H}$ та $\vdash\Psi\in\mathrm{H}$. За припущенням індукції, $\Phi_A^I=\Psi_A^I$=0, звідки $(\Phi\vee\Psi)_A^I=0$.

Нехай $\dashv\ \exists x\Phi\in\mathrm{H}$. За визначенням H, існує $y\in W$ таке $\dashv\ \Phi_x[y]\in\mathrm{H}$. За припущенням індукції, $\Phi_x[y]_A^I=1$, звідки $(\exists x\Phi)_A^I=1$.

Нехай $\vdash\exists x\Phi\in\mathrm{H}$. За визначенням H, то для всіх $y\in W$ $\vdash\Phi_x[y]\in\mathrm{H}$. За припущенням індукції, для всіх $y\in W$ $\Phi_x[y]_A^I=0$. Звідки, враховуючи, що $I:W\to A$ – ін'єкція, випливає, що $(\exists x\Phi)_A^I=0$.

◄

Повернемося тепер безпосередньо до доведення теореми повноти 2.8.

Нехай $\Gamma\models\Delta$. Припустимо супротивне, тобто що секвенція $\Sigma\equiv\ \vdash\Gamma\dashv\ \Delta$ не вивідна. Тоді в секвенційному дереві для $\mathbf{\Sigma}$ існує незамкнений шлях. Згідно Леми 2.9 множина H всіх відмічених формул секвенцій цього шляху – модельна множина.

Тоді згідно Леми 2.10 , існують АС $A_\sigma=(A,\sigma_A)$ і інтерпретація I такі, що (1) якщо $\vdash\Phi\in\mathrm{H}$, то Φ_A^I=1, (2) якщо $\dashv\ \Phi\in\mathrm{H}$, то Φ_A^I=0.

За побудовою, всі формули $\mathbf{\Sigma}$ входять в H. Значить для всіх $\Phi\in\Gamma$ маємо Φ_A^I=1, для всіх $\Psi\in\Delta$ маємо Ψ_A^I=0. Це заперечує $\Gamma\models\Delta$. Кінець доведення теореми 2.8.

◄

2.5. Резолюційне числення логіки першого порядку

Як ми вже бачили в 1.4, метод резолюцій належить до методів спростування формул, а точніше до методів перевірки формул на суперечність.

Його ідейною основою є теореми 2.5 , 2.7 та 2.10 – про вільні АС, ізоморфізм для формул та друга теорема Ербрана відповідно.

Семантичні дерева. Зафіксуємо певну мову L сигнатури σ. Нехай T_σ та Φ_σ- сукупності всіх термів та формул мови L. Сукупність усіх замкнених термів $\overline{T}_\sigma$ сигнатури σ називають *ербрановим універсумом*, а відповідні вільні інтерпретації називаються *ербрановими*[5]. Терми і базові формули – замкнені, якщо вони не містять предметних змінних. Нагадаємо, що частковий випадок формули $\mathrm{E}(x_1,...,x_n)$ є результатом допустимої підстановки в E термів t_i замість змінних x_i і позначається $\mathrm{E}_{x_1,...,x_n}[t_1,...,t_n]$. Сукупність усіх замкнених часткових випадків базових формул сигнатури, утворених шляхом підстановки в них замість предметних змінних замкнених термів з $\overline{T}_\sigma$ називається *ербранівським базисом* мови L множини S і позначається $\overline{\Phi}_\sigma$.

Літерами називаються базові формули та їхні заперечення. *Диз'юнктами* називаються скінченні диз'юнкції літер. *Контрарними* називаються літери A і $\neg A$. Диз'юнкт, який містить контрарну пару є тавтологією, як і в ПЛ.

Розпочнемо з проблеми спростування сукупностей диз'юнктів, яка є центральною в методі резолюцій. Зафіксуємо певну сукупність диз'юнктів $S=\{D_1,...,D_n\}$. За означенням, сукупність S – суперечність, якщо заперечення кон'юнкції всіх її формул є всюди істинною формулою, тобто виконується $\models\neg(D_1\&...\&D_n)$. Іншими словами, для будь-якої інтерпретації мови L принаймні одна з формул D_i – хибна.

Має місце

Лема 2.11. Сукупність S – суперечність $\Leftrightarrow$ S хибна на всіх ербранових інтерпретаціях мови L.

►Випливає з наслідку 1 теореми 2.7 про ізоморфізм для формул. ◄

Умову суперечності сукупності S можна послабити. Позначимо $\overline{\sigma}\subset\sigma$ підмножину функціональних та предикатних символів і предметних констант, які зустрічаються у формулах сукупності S. Позначимо $\overline{L}$ – звуження мови L на сигнатуру $\overline{\sigma}$ і нехай $\overline{T}\subset T_\sigma$ та $\overline{\Phi}\subset\Phi_\sigma$- ті частини Ербранівських універсуму та базису, які утворені тільки символами з $\overline{\sigma}$. Якщо в сигнатурі $\overline{\sigma}$ немає констант, то долучимо до неї одну – c. Нехай $T_S=(\overline{T},\overline{\sigma}_T)$ – вільна АС, породженою константами з $\overline{\sigma}$. Із леми 2.11 випливає, що суперечність сукупності S пов'язана зі значеннями її формул на всіх ербранових інтепретаціях мови L. Насправді, можна обмежитися тільки ербрановими інтепретаціями (T_S, I) мови $\overline{L}$. З практичної точки зору це важливо, принаймні, тому що, на відміну від сигнатури σ, сигнатура $\overline{\sigma}$ - скінченна. Покладемо $\overline{\sigma}=\{f_i^{n_i}:1\le i\le k\}\cup\{p_j^{m_j}:1\le j\le l\}\cup\{c_i:0\le i\le r\}$ для деяких $k,l,r\ge 0$. Нехай $e_0,e_1,...$ – список усіх термів ербранівського універсуму $\overline{T}$ упорядкованих за квазілексикографічним порядком $\triangleleft$ (при цьому константи передують функціональним символам, а дужки й коми

[5] Такий універс і відповідні інтерпретації уперше ввів до розгляду Ж. Ербран .

ігноруються), а $\omega_0, \omega_1, ...$ -список усіх формул ербранівським базису $\overline{\Phi}$, впорядкованих за квазілексикографічним порядком $\triangleleft$ (при цьому рівність $=$ передує іншим предикатним символам, які в свою чергу передують константам та функціональним символам, а кома й дужки – ігноруються). Наприклад, $f(c_{99}) \triangleleft f(c_{100})$ --[$c_{99} < c_{100}$], $f_1^1(f_5^1(c_{100}) \triangleleft f_1^1(f_2^2(c_0, c_0)$ --[різні довжини],

$p(t') \triangleleft p(t'')$, якщо $t' \triangleleft t''$, $p_1^2(c_{100}, c_{100}) \triangleleft p_2^2(c_0, c_0)$ --[$p_1^2 < p_2^2$].

Формули ербранівського базису називають ще *атомами* сукупності S.

Приклад 2.20. Побудуємо ербранівські універсуми та базиси сукупностей $S_1 = \{p(c), p(z) \to p(f(z))\}$ та $S_2 = \{p(x,x), q(f(x,z))\}$. Покладемо сигнатури $\bar{\sigma}_1 = \{f^1, p^1, c\}$ та $\bar{\sigma}_2 = \{f^2, p^2, q^2, c\}$. Тоді

$\overline{T}_1 = c, f(c), f(f(c)),...$, $\overline{\Phi}_1 = p(c), p(f(c)), p(f(f(c))),...;$

$\overline{T}_2 = c, f(c,c), f(c, f(c,c)), f(f(c,c),c), f(c, f(c, f(c,c))), f(f(c, f(c,c)),c), ...;$

$\overline{\Phi}_2 = p(c,c), q(f(c,c)), p(c, f(c,c)), p(f(c,c),c)), q(f(c, f(c,c))), q(f(f(c,c),c)), p(f(c,c), f(c,c)), ...$ ■

При побудові ербранівських універсуму та базиса більш зручною є префіксна бездужкова форма термів і атомів (див. Вправи).

Усі атоми ербранового базису замкнені і при інтерпретації отримують істиносне значення 0 або 1. Усі можливі інтерпретації базису $\overline{T}$ можна задати, так званим, бінарним нескінченним семантичним деревом D_∞. Воно будується індуктивно за висотою m проміжних дерев. (Б) $m = 0$. З кореня виходить дві дуги, зважені атомами ω_0 та $\neg\omega_0$.

(І) Нехай побудовано дерево D_m висоти m. Воно має 2^m листків. Для побудови наступного дерева D_{m+1} з кожного листка дерева D_m будуємо дві дуги в два нових листка. Дуги зважені атомами ω_m та $\neg\omega_m$. Отримаємо дерево висоти $m+1$ з 2^{m+1} листками.

(П) D_∞ - семантичне дерево для сукупності S .

Шлях дерева називається *термінальним*, коли він нескінченний або скінченний і закінчується листком дерева.

Зауваження. За побудовою, (1) всі термінальні шляхи дерева D_∞ - нескінченні і кожний атом ербранового базису $\overline{T}$ або його заперечення належать кожному з термінальних шляхів дерева D_∞; (2) кожному термінальному шляху ρ дерева D_∞ відповідає певна інтерпретація ербранового базиса $I : \overline{T} \to \{0,1\}$, а саме, якщо $\omega_m \in \rho$, то $\omega_m^I = 1$, і навпаки, якщо ж $\neg\omega_m \in \rho$, то $\omega_m^I = 0$; (3) кожній інтерпретації ербранового базиса $I : \overline{\Phi} \to \{0,1\}$ відповідає певний термінальний шлях дерева D_∞ і сукупність інтерпретованих часткових випадків сукупності S, утворених з літер на ребрах.

Вершину дерева D_∞ назвемо *вершиною-спростуванням*, якщо шлях до неї з кореня містить хибний частковий випадок одного з диз'юнктів з S і цей шлях – найкоротший, тобто без неї вже залишок шляху не містить такого часткового випадку. Піддерево $\hat{D}$ дерева D_∞ назвемо *деревом-спростуванням* для S, якщо а) корені обох дерев збігаються, б) всі листки піддерева $\hat{D}$ є вершинами-спростосування і в) піддереву $\hat{D}$ належать всі вершини-спростування дерева D_∞ і всі вершини всіх нескінченних шляхів, які не містять жодної вершини-спростування для S.

Має місце

Теорема 2.9 (Ербрана 1**).** Сукупність S є суперечністю $\Leftrightarrow$ коли для неї існує скінченне дерево-спростування $\hat{D}$.

►($\Rightarrow$) Нехай S – суперечність. І нехай $I:\overline{\Phi}\to\{0,1\}$ довільна інтерпретація ербранового базиса сукупності S. В S обов'язково існує хибний диз'юнкт $D_i^I=0$. Розглянемо шлях ρ дерева D_∞, який відповідає інтерпретації I. В цьому шляху обов'язково існує вершина-спростування для диз'юнкта D_i^I. За означенням, піддерево $\hat{D}$ містить цю вершину і вона є листком дерева. Таким чином, для кожної інтерпретації I в дереві $\hat{D}$ є вершина–спростування. Кожен термінальний шлях $\hat{D}$ – скінченний і це дерево бінарне, тому за лемою Кьоніга воно є скінченним.

($\Leftarrow$) Нехай дерево спростування $\hat{D}$ є скінченним. Нехай S не є суперечністю. Тоді існує інтерпретація I, що всі $D_1^I=D_2^I=...=D_n^I=1$. Тоді інтерпретації I в дереві D_∞ відповідає нескінченний шлях, який не містить вершини-спростування для S, а значить дерево спростування $\hat{D}$ є нескінченним, що за умовою не так. Отже, S – суперечність.

◄

Теорема 2.10 (Ербрана 2**).** Сукупність S є суперечлива $\Leftrightarrow$ коли існує скінченна суперечлива сукупність часткових випадків її диз'юнктів.

►Випливає з теореми Ербрана 1.◄

Наслідок 1. Проблема суперечності скінченної множини диз'юнктів S мови L частково розв'язна. Можна запропонувати наступну процедуру для часткового розв'язку проблеми суперечності сукупності диз'юнктів мови L.

Маємо списки: а) $e_0, e_1, \ldots$ – всіх термів ербранівського універсуму $\bar{T}$ упорядкованих за квазілексикографічним порядком, б) $\omega_0, \omega_1, \ldots$ – всіх часткових випадків S' даної сукупності S на термах універсуму $\bar{T}$, в) $\theta_0, \theta_1, \ldots$ – всіх скінченних підмножин часткових випадків S' сукупності S

Для кожної з сукупностей $\theta_0, \theta_1, \ldots$ методом резолюцій для ПЛ перевіряємо, чи є θ_i суперечливою. Якщо відповідь – так, то процедура закінчує роботу і повертає 1, якщо ж – ні, то перевіряє на суперечливість наступну сукупність θ_{i+1}.

Якщо робота процедури буде продовжуватися нескінченно, то її результат для S - не визначений. ■

Наведена процедура для спростування сукупностей диз'юнктів, як і аналогічна перебірна процедура для ПЛ (лема 1.1), неприйнятна для практичного застосування. Більш ефективну процедуру забезпечує метод резолюцій.

Сколемівська форма. Метод резолюцій ЛПП потребує попереднього перетворення формул до спеціальної сколемівської форми.

Домовимося про певні позначення. Нехай Φ – довільна формула мови L. Позначимо її замкнену пренексну формулу $\Phi' \equiv Q\bar{v}M(\bar{v})$, де $Q\bar{v}$ – кванторний префікс, $\bar{v}$ – список усіх вільних предметних змінних безкванторної формули M, при цьому $\bar{v}$ складається зі списку $\exists$-кванторних імен $y_1, \ldots, y_n$ та списку $\forall$-кванторних імен $x_1, \ldots, x_m$. Формулу M будемо називати матрицею префіксної форми.

Інтуїтивно комбінація кванторів $\forall x \exists y$ може трактуватися як твердження про існування певної функції, значення y якої залежить від x. Зіставимо кожному кванторному префіксу $\exists y_i$ із $Q\bar{v}$ терм $g_i(\bar{x}_i)$ де $\bar{x}_i$ – список всіх тих $\forall$-кванторних імен з $\bar{v}$, що передують y_i в $Q\bar{v}$**,** а g_i-новий функціональний символ, арність якого збігається з кількістю змінних в списку $\bar{x}_i$. Якщо цей список порожній, то g_i – нова предметна константа. Для кожного $1 \le i \le n$ замінимо всі входження y_i в матриці M на терм $g_i(\bar{x}_i)$. В результаті отримаємо універсальну замкнену формулу $\tilde{\Phi} \equiv \forall x_1 \ldots \forall x_m M(x_1, \ldots, x_m, g_1(\bar{x}_1), \ldots, g_n(x_n))$ (*), яка і називається *сколемівською формою* формули Φ, а сам процес вище – *сколемізацією* формули Φ.

Має місце

Теорема 2.11 $\Phi \leftrightarrow \tilde{\Phi}$.

►Див. Вправи.◄

Приклад 2.21.

Нехай $\Phi \equiv \forall x \forall y(A(x,y) \to B(x,y)) \to \forall y(\forall x \neg B(x,y) \to \forall x \neg A(x,y))$. Побудуємо для заперечення $(\neg\Phi)$ сколемівську форму. Спочатку перетворимо формулу $\neg\Phi$ до пренексної форми Φ'. На першому етапі переставимо місцями заперечення $\neg$ і квантори:

$$\neg(\forall x \forall y(A(x,y) \to B(x,y)) \to \forall y(\forall x \neg B(x,y) \to \forall x \neg A(x,y)) \leftrightarrow$$
$$(\neg\neg\forall x \forall y(A(x,y) \to B(x,y)) \& \neg\forall y(\forall x \neg B(x,y) \to \neg\forall x A(x,y)) \leftrightarrow$$
$$\forall x \forall y(A(x,y) \to B(x,y)) \& \exists y \neg(\forall x \neg B(x,y) \to \forall x \neg A(x,y)) \leftrightarrow$$
$$\forall x \forall y(A(x,y) \to B(x,y)) \& \exists y(\forall x \neg B(x,y) \& \exists x A(x,y)).$$

Щоб уникнути колізій (див. Лему 2.5) в процесі подальших перетвореннь, проіндексуємо змінні x та y в другій частині формули. Квантори можна виносити за дужки у будь-якому порядку. Ми ж будемо притримуватися такого правила: винесення кванторів відбувається справа-наліво, при цьому квантори існування мають пріоритет перед універсальними кванторами. Тоді отримаємо шукану пренексну форму Φ':

$$\forall x \forall y(A(x,y) \to B(x,y)) \& \exists y_1(\forall x_1 \neg B(x_1,y_1) \& \exists x_2 A(x_2,y_1)) \leftrightarrow$$
$$\Phi' \equiv \exists y_1 \exists x_2 \forall x_1 \forall x \forall y((A(x,y) \to B(x,y)) \& \neg B(x_1,y_1) \& A(x_2,y_1)).$$

Щоб отримати сколемівську форму з Φ', змінним x_2 та y_1 поставим у відповідність константи a та b і підставимо їх у формулу Φ' замість x_2 та y_1, а також усунемо квантори $\exists y_1, \exists x_2$. Отримана формула $\forall x_1 \forall x \forall y((A(x,y) \to B(x,y)) \& \neg B(x_1,b) \& A(a,b))$ і є сколемівською формою формули $(\neg\Phi)$.■

Прикладом замкненої формули $\forall x_1 \ldots \forall x_m \Phi(x_1, \ldots, x_m)$, де Φ – безкванторна формула, назвемо частковий випадок формули $\Phi_{x_1,\ldots,x_m}[t_1,\ldots,t_m]$, де $t_1, \ldots, t_m$ – замкнені терми. Кон'юнкцію прикладів формули Ψ вигляду $\Psi_{x_1,\ldots,x_m}[t_1^1,\ldots,t_m^1] \& \ldots \& \Psi_{x_1,\ldots,x_m}[t_1^k,\ldots,t_m^k]$, де $k \geq 1$, а $t_1^1,\ldots,t_m^1,\ldots,t_1^k,\ldots,t_m^k$ – довільні терми ербранівського універсуму формули Ψ, за С. Кліні будемо називати *ербранівською розгорткою* формули Ψ.

Теорема 2.12. (Ербрана 3). Нехай $\tilde{\Phi} \equiv \forall x_1 \ldots \forall x_m M(x_1,\ldots,x_m,g_1(x_1),\ldots,g_n(x_n))$ сколемівська форма формули Φ, а $\Psi(x_1,\ldots,x_m) \equiv M(x_1,\ldots,x_m,g_1(x_1),\ldots,g_n(x_n))$. Тоді Φ – суперечлива $\Leftrightarrow$ існує суперечлива ербранівська розгортка матриці M $\Psi_{x_1,\ldots,x_m}[t_1^1,\ldots,t_m^1] \& \ldots \& \Psi_{x_1,\ldots,x_m}[t_1^k,\ldots,t_m^k]$.

►Маємо $\models \Phi \Leftrightarrow \models \tilde{\Phi} \Leftrightarrow \models M(x_1,\ldots,x_m,g_1(x_1),\ldots,g_n(x_n)) \Leftrightarrow$ $\neg M(x_1,\ldots,x_m,g_1(x_1),\ldots,g_n(x_n))$ - суперечність $\Leftrightarrow$ існує суперечлива ербранівська розгортка матриці M $\Psi_{x_1,\ldots,x_m}[t_1^1,\ldots,t_m^1] \& \ldots \& \Psi_{x_1,\ldots,x_m}[t_1^k,\ldots,t_m^k]$ (теорема Ербрана 2). ◄

Уніфікація. Методи резолюцій для ПЛ і ЛПП ідейно близькі, але перехід від диз'юнктів з пропозиційними літерами до диз'юнктів першого порядку породжує проблему пошуку контрарної пари літер-формул, яка в ПЛ розв'язувалася тривіально. Пояснимо на прикладі.

Приклад 2.22. Нехай маємо диз'юнкти $D_1 \equiv A(x) \vee B(x)$ та $D_2 \equiv \neg A(f(y)) \vee C(y)$. В D_1 та D_2 немає контрарної пари. Однак, можна зробити підстановку терму $f(y)$ замість x в D_1. Отримаємо диз'юнкти $D_1' \equiv A(f(y)) \vee B(f(y))$ та D_2, де літери $A(f(y))$ та $\neg A(f(y))$ вже контрарні. Тепер D_1' та D_2 вже мають резольвенту $R \equiv B(f(y)) \vee C(y)$. ■

Зрозуміло, що, підставляючи різні терми замість y в R, отримаємо інші резольвенти, які можна отримати з D_1 та D_2 за правилом резолюцій. У цьому плані R – найзагальніша, інші резольвенти є її частковими випадками.

Таким чином, для отримання резольвент необхідно робити певні підстановки термів.

Нехай L – мова першого порядку з множиною предметних імен (змінних) V і множиною термів T. *Підстановкою* назвемо довільне однозначне відображення $\alpha : V \to T$. Підстановки задають інтерпретації змінних в Ербранових інтерпретаціях. Буде зручно трактувати підстановки як їхні графіки – сукупність пар $(x, \alpha(x))$. В графіках підстановок пари вигляду (x, x) будуть опускатися. Враховуючи, що нас будуть цікавити підстановки тільки скінченної кількості змінних з V, то типова підстановка буде мати вигляд $\alpha = \{(x_1, t)_1, ..., (x_n, t_n)\}$. Такі множини отримали назву іменних. Домовимося їхні елементи позначати скорочено $x \mapsto \alpha(x)$, а сукупності таких елементів брати не в фігурні, а в квадратні дужки. Наприклад, будемо писати $\alpha = [x \mapsto a, y \mapsto f(y)]$. Порожню іменну множину[] позначимо ε, а ніде не визначену підстановку позначимо Λ. Нам знадобиться операція оновлення ∇ для імених множин: для довільних множин $\alpha = [x_1 \mapsto t_1, ..., x_n \mapsto t_n]$ і $\beta = [y_1 \mapsto t_1', ..., y_m \mapsto t_m']$ покладемо: $Z = \{x_1, ..., x_n\} \cap \{y_1, ..., y_m\}$, $\alpha_{-Z} = \{x_i \mapsto t_i, x_i \notin Z\}$ і $\alpha \nabla \beta = \alpha_{-Z} \cup \beta$.

Прикладом терму t за підстановкою $\alpha = \{x_1 \mapsto t_1, ..., x_n \mapsto t_n\}$ або α-прикладом терму t, будемо називати його частковий випадок $\alpha(t) \equiv t_{x_1,...,x_n}[t_1, ..., t_n]$, тобто значення терму t при інтерпретації α.

Добутком (композицією) підстановок α та β називається підстановка $\alpha \circ \beta = \beta \nabla [x_i \mapsto \beta(t_i), x_i \notin Z]$. Надалі добуток підстановок будемо позначати традиційно $\alpha\beta$.

Приклад 2.23 1) Нехай $t = g(x, h(x, y, z))$, $\alpha = [x \mapsto a, y \mapsto f(b), z \mapsto c]$. Тоді $\alpha(t) = g(a, h(a, f(b), c))$.

2) Нехай $\alpha = [x \mapsto f(y), y \mapsto z]$, $\beta = [x \mapsto a, y \mapsto b, z \mapsto y]$. Тоді $Z = \{x, y\}$, $\alpha \circ \beta =$ $[x \mapsto a, y \mapsto b, z \mapsto y] \nabla [x \mapsto \beta(f(y)), y \mapsto \beta(z)]$ $= [x \mapsto f(b), z \mapsto y]$. Зауважимо, що в результаті опущена компонента $y \mapsto y$. ■

Нескладно перевірити, що сукупність усіх скінченних підстановок разом з операцією множення $\circ$ утворюють напівгрупу з одиницею ε і нулем Λ. За означенням, $\alpha\Lambda = \Lambda\alpha = \Lambda$, $\alpha\varepsilon = \varepsilon\alpha = \alpha$ і $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ (див. Вправи)

Підстановка α є *уніфікатором* для множини термів $\{t_1, ..., t_n\}$, якщо $\alpha(t_1) = ... = \alpha(t_n)$. У цьому випадку кажуть, що множина термів $\{t_1, \ldots, t_n\}$ *уніфікується* підстановкою α. Множина термів уніфікується, якщо для неї існує уніфікатор. Поняття уніфікатора можна узагальнити на множини пар термів. Підстановка α є *уніфікатором векторів* $(t_1, ..., t_n)$ та $(t_1', .., t_n')$, якщо $\alpha(t_1) = \alpha(t_1'), ..., \alpha(t_n) = \alpha(t_n')$.

Формули Ербраного універсуму $p(t_1, ..., t_n)$ та $p(t_1', .., t_n')$ *уніфікуються*, якщо вектори термів $(t_1, ..., t_n)$ та $(t_1', .., t_n')$ уніфікуються

Уніфікатор υ – *найзагальніший уніфікатор* (*НЗУ*) множини термів $\{t_1, ..., t_n\}$, якщо для кожного уніфікатора α цієї множини існує підстановка η така, що $\alpha = \upsilon\eta$.

Приклад 2.24. Нехай маємо множину термів $\{x, f(y)\}$. Тоді $\upsilon = [x \mapsto f(y)]$ – найзагальніший уніфікатор цієї множини.

Справді, уніфікатори даної множини мають вигляд $\alpha = [x \mapsto f(t), y \mapsto t]$. Однак тоді для α підходить підстановка $\eta = [y \mapsto t]$: $[x \mapsto f(y)] \circ [y \mapsto t] = [y \mapsto t] \nabla [x \mapsto \eta(f(y))] = [x \mapsto f(t), y \mapsto t] = \alpha$. ■

Опишемо процедуру $Uni(t_1, t_2)$ уніфікації термів t_1 та t_2, яка дозволяє побудувати найзагальніший їхній уніфікатор. Опис індуктивний. За означенням, покладемо $Uni(t_1, t_2) = Uni(t_2, t_1)$. Нехай $z \in V$.

(Б) $Uni(t, z) = \Lambda$, якщо $t \neq z$ і z входить в t;

$Uni(t, z) = \varepsilon$, якщо $t = z$;

$Uni(t, z) = [z \mapsto t]$ у решті випадків;

(І) $Uni((t_1, ..., t_k), (t_1', ..., t_n')) = \Lambda$, якщо $\kappa \neq n$;

$Uni((t_1, ..., t_n), (t_1', .., t_n')) = \upsilon \circ Uni((\upsilon(t_2), ..., \upsilon(t_n)), (\upsilon(t_2'), .., \upsilon(t_n')))$, де $\upsilon = Uni(t_1, t_1')$;

$Uni(f(t_1, ..., t_k), g(t_1', .., t_n')) = \Lambda$, якщо $f \neq g$;

$Uni(f(t_1, ..., t_n), f(t_1', .., t_n')) = Uni((t_1, ..., t_n), (t_1', .., t_n'))$.

Лема 2.12. $Uni(t_1,t_2)$ є НЗУ термів t_1 та t_2.

►Доведення проводиться індукцією по структурі термів та довжині векторів термів.◄

Метод резолюцій. Навчившись уніфікувати формули Ербранового універсуму, можемо тепер дати означення резольвенти для пари диз'юнктів літер D_1 та D_2.

Якщо дві або більше літер в диз'юнкті C мають НЗУ υ, то $\upsilon(C)$ є результатом *склеюванням* диз'юнкту C. Наприклад, візьмемо диз'юнкт $D=r(x)\vee r((f(y))\vee\neg q(x)$. Його літерали $r(x)$ та $r((f(y))$ мають НЗУ $\upsilon=[x\mapsto f(y)]$. Тоді диз'юнкт $\upsilon(D)=r((f(y))\vee\neg q(f(y))$) – результат склеювання диз'юнкту D. Означимо спочатку, що таке бінарна резольвента диз'юнктів D_1 та D_2.

Нехай $nm(D)$ – сукупність всіх змінних диз'юнкту D. Вважається, що дані диз'юнкти не маються спільних змінних, тобто $nm(D_1)\cap$ $nm(D_2)=\varnothing$. Літери $L_1\in D_1$ та $\neg L_2\in D_2$ утворюють контрарну пару, якщо L_1 та L_2 мають НЗУ υ. Нехай L_1 і $\neg L_2$ – контрарна пара в D_1 та D_2. Тоді диз'юнкт $\upsilon(D_1)\setminus\upsilon(L_1)\cup\upsilon(D_2)\setminus\upsilon(L_2)$ називається *бінарною резольвентою* D_1 і D_2, а літери L_1 і $\neg L_2$ - *відрізними*.

Диз'юнкт $D=R(D_1,D_2)$ – *резольвента* диз'юнктів D_1 і D_2, якщо D є однією з бінарних резольвент:

1) D_1 і D_2;

2) D_1 та склеювання чи прикладу D_2;

3) D_2 та склеювання чи прикладу D_1;

4) склеювання чи прикладу D_1 та склеювання чи прикладу D_2.

Диз'юнкти D_1 і D_2 можуть мати і інші резольвенти, отримані за допомогою похідних, по відношенню до НЗУ, уніфікаторів.

Приклад 2.25. Знайдемо резольвенту $R(D_1,D_2)$. 1)Нехай $D_1=$ $r(y)\vee\neg q((x,f(y))$ та $D_2=p(x)\vee q(g(a),x))$. Маємо $nm(D_1)\cap nm(D_2)=\{x\}$, тому візьмемо α-приклад $D_2'=\alpha(D_2)=p(u)\vee q(g(a),u)$, де $\alpha=[x\mapsto u]$. Літери $p(x,f(y))$ та $p(g(a),u)$ мають НЗУ $\upsilon=[x\mapsto g(a),u\mapsto f(y)]$, тому $\upsilon(D_1)=$ $r(y)\vee\neg q((g(a),f(y))$, $\upsilon(D_2')=p(f(y))\vee q(g(a),f(y))$. Тоді $R(D_1,D_2)=r(y)\vee$ $p(f(y))$.

2) Нехай $D_1=p(x)$ $D_1=p(x)\vee p(g(y))\vee q(f(y))$ та $D_2=\neg p(g(f(a)))\vee p(b)$. Склеюванням D_1 за найзагальнішим уніфікатором $[x\mapsto g(y)]$ буде $D'_1=p(g(y))\vee q(f(y))$. Бінарною резольвентою D'_1 та D_2 за найзагальнішим уніфікатором $[y\mapsto f(a)]$ буде $D=q(g(f(a)))\vee p(b)$.

Отже, D – резольвента диз'юнктів-засновків D_1 та D_2. ■
Має місце

Лема 2.13. Нехай D_1' та D_2' – приклади диз'юнктів D_1 і D_2, тоді кожна резольвента $D' = R(D_1', D'_2)$ є прикладом деякої резольвенти $D = R(D_1, D_2)$.

►Нехай L_1' і $\neg L_2'$- відрізні літери при побудові резольвенти D', а υ – їхній НЗУ . Тоді $D' = \upsilon(D_1') \setminus \upsilon(L_1') \cup \upsilon(D_2') \setminus \upsilon(L_2')$. Нехай α_1 і α_2 такі, що $D_1' = \alpha_1(D_1)$ і $D_2' = \alpha_2(D_2)$. Покладемо $\alpha = \alpha_1 \cup \alpha_2$ (це коректно, тому що $nm(D_1) \cap nm(D_2) = \varnothing$). Маємо $D_1' = \alpha(D_1)$ і $D_2' = \alpha(D_2)$. Нехай $L_1' = \alpha(L_1)$ і $\neg L_2' = \neg\alpha(L_2)$ для відповідних літер $L_1 \in D_1$ і $\neg L_2 \in D_2$. Тоді підстановка $\alpha\upsilon$ буде уніфікатором літер L_1 і $\neg L_2$ і диз'юнкт $D = \alpha\upsilon(D_1) \setminus \alpha\upsilon(L_1) \cup \alpha\upsilon(D_2) \setminus \alpha\upsilon(L_2)$ – резольвентою $R(D_1, D_2)$. За побудовою, D' - $\alpha\upsilon$-приклад D .

◄

Лема 2.14. Сукупність $S = \{D_1, D_2\}$ – суперечність$\Leftrightarrow$ резольвента $D = R(D_1, D_2)$- суперечлива.

► $(\Rightarrow)$ Нехай S - суперечлива і нехай L_1 і $\neg L_2$ – контрарна пара в D_1 та D_2, $D_1 = D_1' \vee L_1$, $D_2 = D_2' \vee \neg L_2$, υ – НЗУ L_1 та L_2, а $D = \upsilon(D_1') \cup \upsilon(D_2') = R(D_1, D_2)$. І нехай $I : \overline{\Phi} \to \{0,1\}$ довільна інтерпретація ербранового базиса сукупності S. Візьмемо довільну підстановку (тобто інтерпретацію змінних) α. За умовою, $\upsilon\alpha(D_1)^I \,\&\, \upsilon\alpha(D_2)^I = (\upsilon\alpha(D_1')^I \vee \upsilon\alpha(L_1)^I) \,\&\, (\upsilon\alpha(D_2')^I \vee \upsilon\alpha(\neg L_2)^I) = 0$. Зазначимо, що $\upsilon\alpha$ – уніфікатор L_1 та L_2. Тоді, якщо $\upsilon\alpha(L_1)^I = 1$, то $\upsilon\alpha(\neg L_2)^I = 0$ і $\upsilon\alpha(D_2')^I = 0$. Візьмемо інтерпретацію $J : \overline{\Phi} \to \{0,1\}$, яка відрізняється від I тільки значенням на атомі $\upsilon\alpha(L_1)$ і покладемо $\upsilon\alpha(L_1)^J = 0$. За умовою, $\upsilon\alpha(D_1)^J \,\&\, \upsilon\alpha(D_2)^J = (\upsilon\alpha(D_1')^J \vee \upsilon\alpha(L_1)^J) \,\&\, (\upsilon\alpha(D_2')^J \vee \upsilon\alpha(\neg L_2)^J) = 0$. Зазначимо, що $\upsilon\alpha$ – уніфікатор L_1 та L_2. Тоді, враховуючи, що $\upsilon\alpha(L_1)^J = 0$, то $\upsilon\alpha(\neg L_2)^J = 1$ і $\upsilon\alpha(D_2')^J \vee \upsilon\alpha(\neg L_2)^J = 1$. Значить, $\upsilon\alpha(D_1')^J = 0$. Враховуючи, що після склеювання в D_1' немає входжень літери L_1, то $\upsilon\alpha(D_1')^I = \upsilon\alpha(D_1')^J = 0$. Таким чином, маємо $\alpha(\upsilon(D_1')^I) \vee \alpha(\upsilon(D_2')^I) = 0$ і $\alpha(D)^I = 0$. Отже, резольвента D є суперечність.

$(\Leftarrow)$ Нехай резольвента $D = R(D_1, D_2)$ – суперечність, L_1 та $\neg L_2$ – відрізні літери, υ – НЗУ L_1 та L_2. За теоремою Ербрана 1, для неї існує скінченне дерево- скасування $\widehat{D}$. Долучимо до кожного листка дерева $\widehat{D}$ двох нащадків, дуги до яких зважені атомами $\upsilon(L_1)$ та $\upsilon(\neg L_2)$. Отримане дерево буде деревом- спростування для сукупності $S=\{D_1, D_2\}$ і за теоремою Ербрана 1 – S – суперечлива.

◄

На сукупностях дизьюнктів побудуємо резолюційне числення для суперечностей з двома правилами – правилом резолюцій (R-правилом) $S\cup\{D_1, D_2\}\mid\!- S\cup\{R(D_1,D_2)\}$ та оберненим правилом резолюції (RR-правилом) $S\cup\{R(D_1,D_2)\}\mid\!- S\cup\{D_1, D_2\}$ та аксіомою $S=\{D_\varnothing\}$. Теоремами резолюційного числення є сукупності S, які виводяться з аксіоми $\{D_\varnothing\}$. Цей факт, як і у всіх численнях, записується $\mid\!- S$.

Лема 2.15. Резолюційне числення коректне.

► Нехай $\mid\!- S$. Покажемо, що S- суперечність. Аксіома $D_\varnothing$- суперечність за означенням, а R- та RR-правила зберігають суперечність. Отже, всі теореми – суперечності.

◄

Теорема 2.13 (повноти 1 методу резолюцій). *Множина диз'юнктів S – суперечлива* $\Leftrightarrow$ $S \mid\!- D_\varnothing$.

►$(\Rightarrow)$ Нехай множина S- суперечлива. Нехай D_∞ – закрите семантичне дерево для S. За теоремою Ербрана 1, в D_∞ для S існує скінченне дерево спростування $\widehat{D}$. Покажемо, що існує виведення $D_\varnothing$ з S за допомогою R-правила. Застосуємо індукцію за кількістю вершин n в дереві $\widehat{D}$. Коли $n=1$, то дерево складається тільки з кореня і тоді $S=\{D_\varnothing\}$. Нехай із всіх суперечливих сукупностй диз'юнктів S'з деревом спростування, яке містить менше n вершин, виводиться за допомогою R-правила порожній диз'юнкт $D_\varnothing$. Покажемо, що з S виводиться за допомогою R-правила порожній диз'юнкт. Якщо $n>1$, то в дереві $\widehat{D}$ є, принаймні, одна вершина-виведення N (вершина з двома нащадками-листками N_1, N_2). Нехай $A(N)=a_1,...,a_k$, $A(N_1)=a_1,...,a_k,a_{k+1}$; $A(N_2)=a_1,...,a_k,\neg a_{k+1}$- послідовності атомів щляхів дерева $\widehat{D}$, що ведуть з кореня до вершини N та її нащадків N_1, N_2 . Нагадаємо, що останні є вершинами-спростування. Значить існують два основні приклади D_1' і D_2' диз'юнктів D_1 і D_2 з S, які хибні в $A(N_1)$; $A(N_2)$ і які не спростовуються в $A(N)$. Тоді $\neg a_{k+1}\in D_1'$ і $a_{k+1}\in D_2'$. Відрізаючи їх, отримуємо резольвенту $D'=D_1'\setminus\neg a_{k+1}\cup D_2'\setminus a_{k+1}$. За лемою 2.15, існує така резольвента $D=R(D_1,D_2)$, що D'- приклад D. Візьмемо сукупність $S'=S\cup\{D\}$, яка суперечлива за лемою 2.16 і дерево $\widehat{D}'$, яке отримане з $\widehat{D}$ вилученням піддерева вершини, де спростовується резольвента D'. Дерево $\widehat{D}'$ є деревом-спростування для сукупності S' і воно має вершин менше n. За припущенням, з сукупності S' виводиться за допомогою R-правила порожній диз'юнкт. Тоді він виводиться і з сукупності S, тому що $D = R(D_1, D_2)$ для $D_1, D_2 \in S$.

($\Leftarrow$) Нехай $S = S_0, \ldots, S_m = \{D_\varnothing\}$ – R-виведення $D_\varnothing$ з S. Тоді $\{D_\varnothing\} = S_m, \ldots, S_0 = S$ - є RR-виведенням і $\vdash S$. Тоді з коректності R-числення випливає, що S – суперечність .

◄

Теорема 2.14 (повноти 2 резолюційного числення). *Множина диз'юнктів* S *– суперечлива* $\Leftrightarrow$ $\vdash S$.

► Випливає з теореми 2.13 та коректності R-числення.◄

Практично метод резолюцій зводиться до побудови сколемівської форми для даної формули Φ і спробі виведення порожнього диз'юнкту з відповідної сукупності диз'юнктів.

Приклад 2.26. З'ясуємо, чи буде формула $\Phi \equiv \forall x \forall y (A(x,y) \to B(x,y)) \to \forall y (\forall x \neg B(x,y) \to \neg \forall x A(x,y))$ з прикладу 2.21 всюди істинною. Розглянемо її заперечення ($\neg\Phi$). В прикладі 2.21 для формули $\neg\Phi$ побудована сколемівська форма $\Phi'' \equiv \forall x_1 \forall x \forall y ((A(x,y) \to B(x,y)) \& \neg B(x_1,b) \& A(a,b))$. Перетворимо її матрицю до КНФ:

$\Phi''' \equiv (\neg A(x,y) \vee B(x,y)) \& \neg B(x_1,b) \& A(a,b)$. З сукупності диз'юнктів S КНФ Φ''' маємо виведення порожнього диз'юнкту : $S = S_0 \vdash S_1 \vdash S_2 = D_\varnothing$, де

$S_0 = \{\neg A(x,y) \vee B(x,y), \neg B(x_1,b), A(a,b)\}$--[відрізні л-ри $B(x,y), \neg B(x_1,b)$, $\upsilon = [x \mapsto x_1, y \mapsto b]$];

$S_1 = \{\neg A(x_1,b), A(a,b)\}$ -- [відрізні літери $\neg A(x_1,b), A(a,b)$, $\upsilon = [x_1 \mapsto a]$];

$S_2 = D_\varnothing$.

Значить, $\neg\Phi$ – суперечність і Φ - всюди істина. ■

Існує низка практичних реалізацій різних варіантів методу резолюцій (лінійна резолюція, лок-резолюція, семантична резолюція, стратегія поглинання і т. п.). Цей метод покладено в основу логічного програмування, зокрема реалізації відомої мови Пролог.

ВПРАВИ

1. Довести леми 2.3, 2.4, 2.6, 2.10, 2.12 та теореми 2.2, 2.3, 2.7.
2. Збудувати в секвенційному численні СЧ-1 виведення або довести його відстутність для секвенцій $\dashv \Phi$, де Φ :
   1) $\exists x(A \to B) \to (\exists x A \to \exists x B)$;

2) $\forall x(A\to B)\to(\forall xA\to\forall xB)$;

3) $\forall x(A\to B)\to(\exists xA\to\forall xB)$

4) $\exists x(A\to B)\to(\forall xA\to\exists xB)$;

5) $\exists x(A\to B)\to(\forall xA\to\forall xB)$;

6) $\exists x(A\vee B)\leftrightarrow\exists xA\vee\exists xB$;

7 $\exists x(A\&B)\to\exists xA\&\exists xB$;

8) $\exists x(A\vee\exists xB)\to\exists x\neg A$.

3. При побудові ербранівських універсуму та базиса більш зручними є префіксна бездужкова форма термів і атомів. Наприклад, терм $f^3(x,x,y+z)=z$ в такій формі записується як $=f^3xx+yzz$. Побудувати ербранівські універсуми та базиси з прикладу 2.20, використовуючи бездужкову форму.

1) $\forall xA(x)\to\forall y(\exists zB(x,y,z)\to\neg\forall xA(x)\&\exists xC(x,y))$;

2) $\forall x\neg\exists yA(x,y)\to\forall xB(x)\to\neg\exists yA(x,y)$;

3) $\neg\forall xA(x)\&\exists xB(x)\vee\forall x(\forall yC(x,y)\to A(y))$;

4) $\forall xA(x)\to\forall y(\forall zB(x,y,z)\to\neg\forall xA(x))$;

5) $\forall x\forall yA(x,y)\&\exists xB(x)\to\neg\exists xA(x,y)$.

6) $\exists x\neg\forall yA(x,y)\to\neg\exists xB(x,y)\to\exists yA(x,y)$.

7) $\neg\forall xA(x)\vee\neg\exists xB(x)\vee\forall x(\forall yC(x,y,z)\to A(y))$.

8) $\exists xA(x,y)\to\forall y(\forall zB(x,y,z)\to\neg\forall x\forall yA(x,y))$.

9) $\forall x\exists yA(x,y,z)\&\neg\exists xB(x,y)\to\forall xC(x,y)$.

10) $\exists xA(x)\to\exists y(\forall xB(x,y)\vee\neg\forall zC(x,z)\to\neg\exists xC(x,y))$.

11) $\exists z(x=y+z)\to(x=y)\vee\exists z((x=y+z)\&\neg(z=0))$.

5. Зведіть до сколемівської форми з матрицею в кон'юнктивній нормальній формі такі формули:

а) $\forall x\neg p(x,x)\ \&\ \forall x\exists y\, p(x,y)\ \&\ \forall x\forall z\forall y(p(x,z)\&\, p(z,y)\to p(x,y))$;

б) $\forall x\neg q(x,x)\ \&\ \forall x\forall z\exists y(q(x,y)\to q(x,z)\&\, q(z,y))\ \&\ \forall x\forall y\forall z(q(x,y)\&\, q(y,z)\to q(x,z))$;

в) $\exists x(p(x)\&\forall y(q(y)\to h(x,y)))\ \&\ \forall x(p(x)\to\forall y(r(y)\to\neg h(x,y)))\to\forall x(q(x)\to\neg r(x))$.

6. Доведіть, що $(\alpha*\beta)*\gamma=\alpha*(\beta*\gamma)$, де $*$ – множення підстановок.

7. Які з наведених множин мають найзагальніший уніфікатор? Знайдіть такі найзагальніші уніфікатори, якщо вони є:

а) $\{p(x), p(y)\}$;

б) $\{q(x,y), q(x,x)\}$;

в) $\{q(x,y,f(y)), q(x,z,z)\}$;

г) $\{p(x,y,z), p(u,f(u,v),v)\}$;

д) $\{q(x,y,f(y),z,g(y,z),v), q(a,h(a),b,s(a,b),u,h(a,b,u))\}$.

8. Побудуйте всі можливі резольвенти (якщо вони є) для таких пар:

а) $D_1=p(x,y)\vee\neg q(x)$ та $D_2=p(z,y)\vee q(z)$;

б) $D_1=\neg p(x)\vee q(x,x)$ та $D_2=\neg q(y,f(y))$;

в) $D_1 = \neg p(x, y, a) \vee \neg p(y, z, b) \vee \neg p(x, b, v) \vee \neg p(a, z, v)$ та $D_2 = p(f(x, y), x, y)$.

9. Доведіть чи спростуйте методом резолюцій:
   а) $\forall x(G(x) \to L(x)) \& \neg \exists x(K(x) \& L(x)) \& \forall x(\neg G(x) \to \neg E(x)) \models \neg \exists x(K(x) \& E(x))$;
   б) $\forall x \forall y \forall z(R(x, y) \& R(y, z) \to R(x, z)) \models \forall x \forall y \forall z \forall u(R(x, y) \& R(y, z) \& R(z, u) \to R(x, u))$;
   в) $\forall x \forall y(B(x, y) \to P(x, y)) \models \forall y(\forall x \neg P(x, y) \to \forall x \neg B(x, y))$;
   г) $\forall x(L(x) \to T(x)) \models \forall x \forall y(L(x) \& S(x, y) \to \exists z(T(z) \& S(z, y)))$;
   д) $\forall x \forall y(B(x, y) \leftrightarrow A(x) \& A(y)) \models \forall x \forall y(B(x, y) \to B(y, x))$.

Розділ III.
АКСІОМАТИЧНІ ТЕОРІЇ ЛОГІКИ ПЕРШОГО ПОРЯДКУ

3.1 Теорії логіки першого порядку

Аксіоматичною теорією логіки першого порядку (далі просто теорією) називається трійка $T=(L,Ax,P)$, де Ax - система аксіом, яка складається з логічних та власних аксіом, P - сукупність правил виведення. Логічні аксіоми та правила виведення – одні і ті ж у всіх аксіоматичних теоріях логіки першого порядку. Таким чином, аксіоматичні теорії з мовою L відрізняються тільки власними аксіомами. Нагадаємо, що нас цікавлять лише коректні правила виведення, тобто які зберігають в ЛПП відношення логічного наслідку $\models$.

Нехай, як і раніше, f^n та p^m - довільні функціональний та предикатний символи сигнатури σ. Логічними аксіомами є:

Ax1) $\neg\Phi\vee\Phi$ (пропозиційна аксіома),

Ax2) $\Phi_x[t]\rightarrow\exists x\Phi$ (аксіома підстановки),

Ax3) $x=x$ (аксіома тотожності),

Ax4) $x_1=y_1\rightarrow\ldots\rightarrow x_n=y_n\rightarrow f(x_1,\ldots,x_n)=f(y_1,\ldots,y_m)$,

$x_1=y_1\rightarrow\ldots\rightarrow x_m=y_m\rightarrow p(x_1,\ldots,x_n)=p(y_1,\ldots,y_n)$ - (аксіоми рівності).

Правилами виведення (ПВ) є правила виведення П1-П4 пропозиційного числення та правило П5: $\Phi\rightarrow\Psi\ \vdash\exists x\Phi\rightarrow\Psi$, якщо x - не вільна в Ψ (правило $\exists-$введення).

Теоремами теорії T називаються формули, які виводяться з аксіом за допомогою скінченної кількості застосувань ПВ. Те, що формула A - теорема теорії T, позначатимемо, як і в ПЧ, $T\vdash\mathrm{A}$ або просто $\vdash\mathrm{A}$, а множину теорем теорії T - $Th(T)$.

Лема 3.0 1) Логічні аксіоми є всюди істинними формулами.

2) Висновки правил П1–П4 – тавтологічні наслідки засновків.

3) Висновок правила П5 – слабкий логічний наслідок засновку.

► 1)-2) Очевидно. Для аксіоми підстановки див. Приклад 2.5 d). Для п. 3) див. Приклад 2.6. ◄

Теорія з порожньою сукупністю власних аксіом називається *чистою*.

Наслідок. Кожна теорема чистої теорії T є всюди істинною формулою. Доводиться структурною індукцією за індуктивним означенням сукупності теорем теорії T. ■

Теорія T' називається *розширенням* теорії T, якщо кожна формула теорії T є формулою теорії T' і $Th(T) \subseteq Th(T')$. В цьому випадку теорію T називають *звуженням* теорії T'. Розширення (звуження) T' теорії T називають *простим,* якщо T та T' мають однакові мови. Теорії T_1 та T_2 називаються *еквівалентними*, якщо в них однакові мови та множини теорем.

Потужністю теорії T називають потужність множини $\mathrm{Th}(T)$. Зокрема, теорія T із зліченною сигнатурою злічення, теорія T з сигнатурою потужності α має потужність α.

Розглянемо кілька прикладів теорій 1-го порядку.

Приклад 3.1. Чиста теорія 1-го порядку називається *численням предикатів першого порядку.* Якщо при цьому в сигнатурі відсутні функціональні символи, то отримуємо *чисте числення предикатів першого порядку.* Такі числення називатимемо також відповідно *численням предикатів* і *чистим численням предикатів*. ■

Приклад 3.2. Особливе місце серед формальних теорій займає *формальна арифметика*. Позначимо її *Ar*. Мовою *Ar* є мова L_{ar}.

Власні аксіоми *Ar* такі:

Ar1) $\neg(x + 1 = 0)$;

Ar2) $x + 1 = y + 1 \to x = y$;

Ar3) $x + 0 = x$;

Ar4) $x + (y + 1) = (x + y) + 1$;

Ar5) $x \times 0 = 0$;

Ar6) $x \times (y + 1) = x \times y + x$;

Ar7) $\mathrm{A}_x[0]\ \&\ \forall x(\mathrm{A} \to \mathrm{A}_x[x + 1]) \to \forall x\mathrm{A}$ – аксіоми індукції.

Кожна власна аксіома формальної арифметики є ІАФ. ■

Приклад 3.3. *Елементарною теорією груп* називається теорія першого порядку *Gr* сигнатури $\{\bullet, e, =\}$, де e – константний символ, $\bullet$ – бінарний функціональний символ.

Власні аксіоми *Gr* такі:

G1) $x\bullet (y\bullet z) = (x\bullet y)\bullet z$;

G2) $\forall x(e\bullet x = x)$;

G3) $\forall x\exists y(y\bullet x = e)$. ■

Моделлю теорії T називається інтерпретація мови теорії, на якій істинні всі власні аксіоми теорії T[6].

---

[6] Не плутати з поняттям моделі АС, пов'язаним з поняттям гомоморфізму та ізоморфізму останніх.

Приклад 3.4. 1) Моделлю елементарної теорії груп Gr є кожна група. 2) Моделлю формальної арифметики Ar є $\boldsymbol{N}$ – стандартна інтерпретація мови L_{ar}. Цю модель називають *стандартною моделлю* формальної арифметики. ■

Мають місце наступні очевидні теореми (див.Вправи).

Теорема 3.2 (теорема істинності). Кожна теорема теорії T істинна в T. ■

Теорема 3.3 (теорема тавтології). Кожна тавтологія є теоремою. ■

Наслідок. Якщо $\Phi_1,...,\Phi_n \models \Psi$ і $\vdash \Phi_1, ..., \vdash \Phi_n$, то $\vdash \Psi$.■

Як випливає з Наслідку теореми 3.3, всі доведення з леми 1.5а мають місце і в теоріях 1-го порядку. Доповнимо цей список рядом важливих доведень формул з кванторами.

Лема 1.5а (продовження) Для довільних формул A, B, змінної y не вільної в A, $\overline{A}$ – замикання A, термів a, b, c мови L:

11) $\vdash \forall x A \to A$; (внутрішнє узагальнення)

12) $A \to B \vdash A \to \forall y B$ (правило $\forall$-введення);

13) $A \to B \vdash$ а) $\exists x A \to \exists x B$, б) $\forall x A \to \forall x B$ (правила дистрибутивності) ;

14) $A \vdash \forall x A$ (правило узагальнення) ;

15) $\forall x A \vdash A$ (правило усоблення) ;

16) $A \vdash \Leftrightarrow \vdash \overline{A}$ (правило замикання);

17) $A \vdash A_{x_1,...,x_n}[t_1,\ldots, t_n]$ (частковий випадок).

18) а) $\vdash A_{x_1,...,x_n}[t_1,\ldots, t_n] \to \exists x_1...\exists x_n A$ та б) $\vdash \forall x_1...\forall x_n A \to A_{x_1,...,x_n}[t_1,\ldots, t_n]$ (підстановки).

19) $\vdash a = b \leftrightarrow b = a$ (симетрія рівності).

20) $\vdash a = b \to b = c \to a = c$ (транзитивність рівності).

► 11) $\neg A \to \exists x \neg A$ (аксіома Ax3), $\neg\exists x \neg A \to A$ (контр.+ $\neg\neg$– усун.), $\forall x A \to A$.

12) $A \to B$, $\neg B \to \neg A$ (контр.), $\exists x \neg B \to \neg A$ (П5), $\neg\neg A \to \neg\exists x \neg B$ (контр.), $\vdash A \to \forall x B$ ($\neg\neg$– усун.).

13) а) $A \to B$, $B \to \exists x B$ (аксіома Ax3), $A \to \exists x B$ (транзит.), $\exists x A \to \exists x B$ (П5);

б) $A \to B$, $\neg B \to \neg A$ (контр.) , $\neg A \to \exists x \neg A$ (аксіома Ax3), $\neg B \to \exists x \neg A$ (транзит.), $\exists x \neg B \to \exists x \neg A$ (П5), $\neg\exists x \neg A \to \neg\exists x \neg B$ (контр.), $\vdash \forall x A \to \forall x B$.

14) A, $\forall x A \vee A$ (П1), $\neg A \to \forall x A$ (ПК+ $\neg\neg$– введен.) , $\exists x \neg A \to \forall x A$ (П5), $\forall x A \vee \forall x A$, $\forall x A$ (П2).

15) $\forall x A$, $\forall x A \to A$ (внутр. узагал.), A (відокр.)

16) Випливає з правил узагальнення та уособлення.

17) Спочатку доведемо для $n=1$: A(гіпот.), $\neg A_x[t]\to\exists x\neg A$ (аксіома Ax2), $\forall xA\to A_x[t]$ (конт.+ $\neg\neg-$усун.), $\forall xA$ (узагал.), $A_x[t]$ (відокр.). Нехай предметні змінні $y_1,...,y_n\notin A\cup A_{x_1,...x_n}[t_1,...,t_n]$. Покладемо $B\equiv A_{x_1,...x_n}[y_1,...,y_n]$. Тоді маємо ланцюг $|\!-A_{x_1}[y_1]$, $|\!-A_{x_1,x_2}[y_1,y_2]$, … , $|\!-A_{x_1,...x_n}[y_1,...,y_n]$, $|\!-B_{y_1}[t_1]$, $|\!-B_{y_1,y_2}[t_1,t_2]$, …, $|\!-B_{y_1,...y_n}[t_1,...,t_n]$. Але формула $B_{y_1,...y_n}[t_1,...,t_n]$ збігається з $A_{y_1,...y_n}[t_1,...,t_n]$.

18) а) За аксіомою *Ax3)* маємо $A\to\exists x_1...\exists x_nA$, $\exists x_nA\to\exists x_{n-1}\exists x_nA$, …, $\exists x_2...\exists x_nA\to\exists x_1...\exists x_nA$, $A\to\exists x_1...\exists x_nA$(транзит.), $A_{x_1,...x_n}[t_1,...,t_n]\to\exists x_1...\exists x_nA$ (частковий випадок). б) За внутрішнім узагальненням маємо

$\forall x_nA\to A$, … , $\forall x_1..\forall x_nA\to\forall x_2..\forall x_nA$, $\forall x_1..\forall x_nA\to A$(транзит.),

$\forall x_1...\forall x_n A\to A_{x_1,...,x_n}[t_1,\dots,t_n]$ (частковий випадок).

19) $|\!-x=y\to x=x\to x=x\to y=x$ (аксіома рівності для ПС =), звідки $|\!-x=x\to x=x\to y=x\to y=x$ за ТТ. Однак $|\!-x=x$ (аксіома тотожності), тому послідовно $|\!-x=x\to y=x\to y=x$ та $|\!-x=y\to y=x$ за МР. Аналогічно $|\!-y=x\to x=y$, тому $|\!-x=y\leftrightarrow y=x$ за ТТ. Звідси $|\!-a=b\leftrightarrow b=a$ за правилом підстановки.

20) Маємо $|\!-y=x\to y=z\to y=y\to x=z$ (аксіома рівності для ПС =), тому $|\!-y=y\to y=x\to y=z\to x=z$ за ТТ. Однак $|\!-y=y$ (аксіома тотожності), тому за МР $|\!-y=x\to y=z\to x=z$. За правилом симетрії $|\!-x=y\to y=x$, тому $|\!-x=y\to y=z\to x=z$ за ТТ. За правилом підстановки $|\!-a=b\to b=c\to a=c$. ◄

Нехай Γ- деяка множина формул. Теорію, отриману з теорії T долученням до її власних аксіом сукупності формул Γ, будемо позначати $T[\Gamma]$.

Теорема 3.4 (дедукції). Нехай A – замкнена формула. Тоді для довільної формули B: $T[A]\,|\!-B\Leftrightarrow T\,|\!-A\to B$.

►Індукція за довжиною виведення в $T[A]$ формули B. Нехай B-аксіома. Тоді $T\,|\!-B$ і $T\,|\!-A\to B$ за П1. Нехай $B\equiv A$. Тоді $|\!-A\to A$ і $T\,|\!-A\to A$.

Нехай B на останньому кроці виведення в $T[A]$ отримана з формули C за допомогою правил П1-П4. Тоді твердження теореми випливає з ТТ і індуктивного припущення (Див. Доведення теореми дедукції 1.7 для ПЧ).

Нехай $B\equiv C\to D$ на останньому кроці отримана з формули $C\to D$ за допомогою правила П5 і значить x- не вільна в D . За індуктивним припущенням, $T\,|\!-A\to(C\to D)$. Тоді за внутрішньою комутативністю $T\,|\!-C\to(A\to D)$, $T\,|\!-\exists xC\to(A\to D)$ за правилом П5 (A- замкнена) і знову за внутрішньою комутативністю – $T\,|\!-A\to(\exists xC\to D)$.◄

Наслідок . Нехай A_1, ..., A_n – замкнені формули. Тоді $T \vdash A_1 \to ... \to A_n \to B \Leftrightarrow T\,[A_1, ..., A_n] \vdash B$ для довільної формули B. ■

Якщо не вимагати замкненості формули A, то теорема дедукції невірна. Справді, $Ar\,[x = 0] \vdash x = 0$, тому $Ar\,[x = 0] \vdash y = 0$ за правилом підстановки. Однак формула $x = 0 \to y = 0$ не є ІАФ, тому невірно, що $Ar \vdash x = 0 \to y = 0$.

Обійти проблему незамкненості формули A дозволяє

Теорема 3.5 (про константи). Нехай T' – константне розширення теорії T. Тоді для кожної формули A теорії T та кожної послідовності c_1, ..., c_n нових константних символів : $T \vdash A \Leftrightarrow T' \vdash A[c_1, ..., c_n]$.

►Якщо $T \vdash A$, то $T' \vdash A$, звідки $T' \vdash A[c_1, ..., c_n]$ за правилом підстановки.

Нехай $T' \vdash A[c_1,..., c_n]$. Розглянемо виведення $A[c_1,..., c_n]$ у T' і виберемо n предметних імен $y_1,..., y_n$, які не зустрічаються у формулах цього виведення та в A. Замінимо в усіх формулах цього виведення всі входження $c_1,..., c_n$ на $y_1,..., y_n$ відповідно. Власні аксіоми, які можуть зустрітися в цьому виведенні, не зміняться, тому що не містять нових констант, кожна логічна аксіома стане логічною аксіомою тієї самої схеми, кожне застосування правила виведення стане застосуванням того самого правила виведення. Дістали виведення $A[y_1,..., y_n]$ у T, тобто $T \vdash A[y_1,..., y_n]$, звідки $T \vdash A$ за правилом підстановки.

◄

Нехай x_1, ..., x_n – усі вільні імена формули A. Нехай T' – константне розширення теорії T за допомогою нових констант c_1, ..., c_n.

За теоремою про константи й теоремою дедукції тоді $T \vdash A \to B \Leftrightarrow T' \vdash A[c_1,..., c_n] \to B[c_1,..., c_n] \Leftrightarrow T'\,[A[c_1,..., c_n]] \vdash B[c_1,..., c_n]$.

Теорема 3. 6 (редукції). Нехай **Г** – деяка множина формул. Тоді $T\,[\mathbf{\Gamma}] \vdash A \Leftrightarrow T \vdash B_1 \to ... \to B_n \to A$ для деяких B_1, …, B_n, де кожна формула B_k є замиканням деякої формули з **Г**.

► Нехай у виведенні $T\,[\mathbf{\Gamma}] \vdash A$ використано A_1, …, A_n, нехай B_1, …, B_n – замикання формул A_1, …, A_n. Маємо $T\,[\mathbf{\Gamma}] \vdash A \Leftrightarrow T\,[A_1, …, A_n] \vdash A$. За теоремою замикання тоді $T\,[B_1, …, B_n] \vdash A_1$, …, $T\,[B_1, …, B_n] \vdash A_n$. Отже, $T\,[B_1, …, B_n] \vdash A$, звідки $T \vdash B_1 \to ... \to B_n \to A$ за наслідком теореми дедукції.

Нехай $T \vdash B_1 \to ... \to B_n \to A$, де B_1, …, B_n – замикання певних формул з **Г**. Тоді $T\,[\mathbf{\Gamma}] \vdash B_1 \to ... \to B_n \to A$. За теоремою замикання $T\,[\mathbf{\Gamma}] \vdash B_k$ для всіх $k \in \{1, …, n\}$. Застосовуючи MP, маємо $T\,[\mathbf{\Gamma}] \vdash A$.

◄

3.2. Синтаксичні варіанти семантичних властивостей формул

Для теорій 1-го порядку вірні синтаксичні варіанти теорем рівності, еквівалентності та про пренексну форму.

Теорема 3.7 (еквівалентності). Нехай A' отримана з формули A заміною деяких входжень формул $B_1, ..., B_n$ на $P_1, ..., P_n$ відповідно. Якщо $|\!-B_1\leftrightarrow P_1, ..., |\!-B_n \leftrightarrow P_n$, то $|\!-A\leftrightarrow A'$.

►Індукція за структурою формули A. (Б) Нехай A – базова формула, тоді довільним входженням формули в A є сама A. Тому або замінюється вся A, або ніякої заміни немає. У першому випадку A є B_k та A' є P_k для деякого k, тому $|\!-A\leftrightarrow A'$ за умовою. У другому випадку A збігається з A', тому $|\!-A\leftrightarrow A'$ за ТТ. (І) Нехай A має вигляд $\neg C$. Довільним входженням формули в A або є вся A, або таке входження цілком міститься в C. У першому випадку доводимо аналогічно 1). У другому випадку A' є $\neg C'$, де C' отримана замінами із C так, як описано в теоремі. За припущенням індукції $|\!-C\leftrightarrow C'$, тому $|\!-A\leftrightarrow A'$ за ТТ. Аналогічно доводимо для випадку, коли A має вигляд $\vee BC$. Нехай A має вигляд $\exists xC$. Довільним входженням формули в A або є вся A, або таке входження цілком міститься в C. У першому випадку доводимо аналогічно 1). У другому випадку A' є $\exists xC'$, де C' отримана замінами із C так, як описано в теоремі. За припущенням індукції $|\!-C\leftrightarrow C'$, тому $|\!-C\to C'$ та $|\!-C'\to C$ за ТТ. За правилом дистрибутивності $|\!-\exists xC\to\exists xC'$ та $|\!-\exists xC'\to\exists xC$, тобто $|\!-A\to A'$ та $|\!-A'\to A$. Звідси $|\!-A\leftrightarrow A'$ за ТТ.

◄

Теорема 3.7 (рівності для термів). Нехай терм τ' отримано з терму τ заміною деяких входжень термів $t_1,..., t_n$ на терми $s_1,..., s_n$ відповідно. Якщо $|\!-t_1 = s_1, ..., |\!-t_n = s_n$, то $|\!-\tau = \tau'$.

►Структурна індукція за будовою термів.◄

Теорема 3.8 (рівності для формул). Нехай формулу Ф' отримано з формули Ф заміною деяких входжень термів $t_1,..., t_n$ на терми $s_1, ..., s_n$ відповідно. Якщо $|\!-t_1 = s_1, ..., |\!-t_n = s_n$, то $|\!-\Phi \leftrightarrow \Phi'$.

► Структурна індукція за будовою формул. ◄

Теорема 3.9 (про варіанту). Якщо A' – варіанта формули A, то $|\!- A \leftrightarrow A'$.

► Покажемо $|\!-\exists xB\leftrightarrow\exists yB_x[y]$, якщо y не вільна у B. Тоді твердження теореми про варіанту випливатиме з теореми еквівалентності та ТТ. Маємо $|\!-B_x[y] \to\exists xB$ (аксіома Ax3), звідки $|\!-\exists yB_x[y]\to\exists xB$ за П5. Однак $(B_x[y])_y[x]$

збігається з B, тому що y не вільне у B. Тому $\vdash B\to\exists yB_x[y]$ як Ах3, звідки за П5 $\vdash\exists xB\to\exists yB_x[y]$. Звідси та з $\vdash\exists yB_x[y]\to\exists xB$ за ТТ $\vdash\exists xB\leftrightarrow\exists yB_x[y]$.

◄

Теорема 3.10. 1) $\vdash\neg\forall xB\leftrightarrow\exists x\neg B$ та $\vdash\neg\exists xB\leftrightarrow\forall x\neg B$;

2) $\vdash\exists xB\vee C\leftrightarrow\exists x(B\vee C)$ та $\vdash\forall xB\vee C\leftrightarrow\forall x(B\vee C)$, якщо x не вільна в C;

3) $\vdash B\vee\exists xC\leftrightarrow\exists x(B\vee C)$ та $\vdash B\vee\forall xC\leftrightarrow\forall x(B\vee C)$, якщо x не вільна в B.

► 1) За ТТ $\vdash\neg\neg\neg\exists x\neg B\leftrightarrow\exists x\neg B$, тобто $\vdash\neg\exists xB\leftrightarrow\forall x\neg B$. За ТТ маємо $\vdash B\leftrightarrow\neg\neg B$, звідки $\vdash\neg\exists xB\leftrightarrow\neg\exists x\neg\neg B$ за теоремою еквівалентності, тобто $\vdash\neg\exists xB\leftrightarrow\forall x\neg B$.

2). За ТТ $\vdash B\to B\vee C$, тому $\vdash\exists xB\to\exists x(B\vee C)$ за правилом дистрибутивності. Маємо $\vdash B\vee C\to\exists x(B\vee C)$ (аксіома Ах3), звідки за ТТ $\vdash C\to\exists x(B\vee C)$. Звідси та з $\vdash\exists xB\to\exists x(B\vee C)$ за ТТ $\vdash\exists xB\vee C\to\exists x(B\vee C)$. За ТТ $\vdash B\to B\vee C$, тому $\vdash\forall xB\to\forall x(B\vee C)$ за правилом дистрибутивності. За ТТ $\vdash C\to B\vee C$, тому $\vdash C\to\forall x(B\vee C)$ за правилом $\forall$-введення. Звідси та з $\vdash\forall xB\to\forall x(B\vee C)$ за ТТ випливає $\vdash\forall xB\vee C\to\forall x(B\vee C)$. Маємо $\vdash B\to\exists xB$ (аксіома Ах3), звідки $\vdash B\vee C\to\exists xB\vee C$ за ТТ, тому $\vdash\exists x(B\vee C)\to\exists xB\vee C$ за П5.

Маємо $\vdash\forall x(B\vee C)\to B\vee C$ за теоремою підстановки, звідки за ТТ $\vdash\forall x(B\vee C)\&\neg C\to B$. Тоді $\vdash\forall x(B\vee C)\&\neg C\to\forall xB$ за правилом $\forall$-введення, звідки за ТТ $\vdash\forall x(B\vee C)\to\forall xB\vee C$. За ТТ із $\vdash\exists xB\vee C\to\exists x(B\vee C)$ та $\vdash\exists x(B\vee C)\to\exists xB\vee C$ маємо $\vdash\exists xB\vee C\leftrightarrow\exists x(B\vee C)$, із $\vdash\forall xB\vee C\to\forall x(B\vee C)$ та $\vdash\forall x(B\vee C)\to\forall xB\vee C$ випливає $\vdash\forall xB\vee C\leftrightarrow\forall x(B\vee C)$.

3). Якщо x не вільне у B, то $\vdash\exists xC\vee B\leftrightarrow\exists x(C\vee B)$ та $\vdash\forall xC\vee B\leftrightarrow\forall x(C\vee B)$ згідно з 2), звідки за теоремою еквівалентності $\vdash\exists xC\vee B\leftrightarrow\exists x(B\vee C)$ та $\vdash\forall xC\vee B\leftrightarrow\forall x(B\vee C)$. Тепер 3) дістаємо за ТТ.

◄

Теорема 3.11 (про пренексну форму**).** Нехай – Φ' – пренексна форма формули Φ. Тоді $\vdash\Phi\leftrightarrow\Phi'$.

►Індукція по структурі формули з використанням теореми 3.10.◄

3.3. Несуперечливість теорій першого порядку.

Теорія першого порядку T *несуперечлива*, якщо не існує формули Φ такої, що $T\vdash\Phi$ і $T\vdash\neg\Phi$. Несуперечлива теорія першого порядку T називається *повною*, якщо для кожної замкненої формули Φ маємо $T\vdash\Phi$ або $T\vdash\neg\Phi$.

Як і для ПЛ, теорія першого порядку T *суперечлива* $\Leftrightarrow$ $T\vdash\Phi$ для кожної формули Φ мови T.

Лема 3.1. Числення предикатів першого порядку неповне.

►Нехай $S \equiv \forall x \forall y(x = y)$. Формула S істинну тільки на 1-елементних інтерпретаціях. Тоді $\neg S$ істинна на всіх n-елементних інтерпретаціях, де $n > 1$. Якщо $\vdash S$, то $\models S$, що неможливо; якщо ж $\vdash \neg S$, то $\models \neg S$, що теж неможливо.
◄

Теорема 3.12 (несуперечливості). Нехай T – теорія першого порядку, A – замкнена формула така, що $A \notin Th(T)$. Тоді теорія $T\ [\neg A]$ несуперечлива.

►Припустимо супротивне: $T\ [\neg A]$ суперечлива. Тоді за теоремою 7.2.1 $T\ [\neg A] \vdash A$, звідки за теоремою дедукції $T\ \vdash \neg A \to A$. Тому за ТТ $T\ \vdash A$, що суперечить $A \notin Th(T)$.
◄

Наслідок. Нехай T – теорія першого порядку, A – замкнена формула. Тоді $T\ \vdash$A $\Leftrightarrow$ $T\ [\neg$A] суперечлива.

►Нехай $T\ \vdash A$. Тоді $T\ [\neg A] \vdash A$. Однак $T\ [\neg A] \vdash \neg A$, тому що $\neg A$ є аксіомою $T\,[\neg A]$, тому $T\ [\neg A]$ суперечлива. Нехай тепер $T\,[\neg A]$ суперечлива. Тоді $T\ [\neg A] \vdash A$, звідки $T\ \vdash \neg A \to A$ за теоремою дедукції. Звідси $T\ \vdash A$ за ТТ.
◄

Теорема 3.13 (Ліnденбаума). Кожна несуперечлива теорія першого порядку має несуперечливе просте повне розширення.

►Доведемо для випадку зліченних теорій. Нехай T – несуперечлива теорія першого порядку. Множина всіх формул T зліченна, тому множина всіх замкнених формул T теж зліченна. Нехай B_0, B_1, ,..., B_n, ... – перелік усіх замкнених формул T. Задамо наступну послідовність теорій $\Sigma_0 = T$, $\Sigma_1, \Sigma_2 ...$: для $n > 1$

$$\Sigma_{n+1} = \begin{cases} \Sigma_n, \neg B_n \in Th(\Sigma_n) \\ \Sigma_n[B_n], \neg B_n \notin Th(\Sigma_n) \end{cases}.$$

Індукцією за n доведемо, що кожна з теорій Σ_n несуперечлива.

(Б) Теорія $\Sigma_0 = T$ несуперечлива за умовою. (І) Нехай Σ_n несуперечлива. Тоді Σ_{n+1} теж несуперечлива. Справді, якщо $\Sigma_{n+1} = \Sigma_n$, то Σ_{n+1} несуперечлива за припущенням. Якщо $\Sigma_{n+1} = \Sigma_n[B_n]$, то Σ_{n+1} несуперечлива за теоремою 3.12. Отже, за (П) всі Σ_n несуперечливі.

Нехай Σ – теорія першого порядку, множина аксіом якої є об'єднанням множин аксіом усіх теорій Σ_n. Тоді Σ - несуперечлива. Справді, якщо Σ суперечлива, то в Σ існує виведення суперечності – формули вигляду $A\&\neg A$. Таке виведення використовує скінченну кількість аксіом, тому всі вони є аксіомами теорії Σ_n для деякого n. Тому $\Sigma_n \vdash A\&\neg A$, що неможливо, так як Σ_n несуперечлива.

Теорія Σ повна. Справді, кожна замкнена формула є формулою для деякого m. Якщо $\neg B_m \in Th(T)$, то $\neg B_m \in Th(\Sigma)$, тобто маємо $\Sigma \vdash \neg B_m$. Якщо $\neg B_m \notin Th(\Sigma_m)$, то $\Sigma_{m+1} = \Sigma_m[B_m]$, звідки $\Sigma_{m+1} \vdash B_m$, тому маємо $\Sigma \vdash B_m$. Отже, теорія Σ повна.

◄

3.4. Розв'язність та перелічність аксиоматичних теорій

Розглянемо важливі поняття розв'язності та перелічності аксіоматичних теорій. Розв'язність теорії означає алгоритмічну розв'язність множини її теорем відносно множини всіх формул мови теорії. Перелічність означає, що множина теорем теорії алгоритмічно перелічна.

Зафіксуємо певну ефективну нумерацію $\kappa : N \to \Phi_\sigma$ множини формул мови теорії. Маємо такі визначення. Теорія *T розв'язна* або *рекурсивна*, якщо множина κ(Th(*T*)) номерів теорем теорії *T* розв'язна. Теорія *T перелічна* або *рекурсивно-перелічна*, якщо множина κ(Th(*T*)) алгоритмічно перелічна.

Найпростішим прикладом розв'язної теорії є розглянуте в 1.5 ПЧ.

Теорема 3.14. Нехай Т – теорія першого порядку з алгоритмічно перелічною множиною аксіом. Тоді Т- перелічна.

►Нехай $\aleph$ – алгоритм для переліку аксіом теорії *T*.

Тоді алгоритм, який перелічує всі теореми теорії *T*, по черзі виконує дії:

1) видати алгоритмом $\aleph$ чергову аксіому А;

2) до множини вже отриманих теорем однократно застосувати всіма можливими способами правила П1–П5;

3) отримані нові теореми та нову аксіому А по черзі подати на вихід і поповнити ними множину теорем.

◄

Теорія *T рекурсивно-аксіоматизована*, якщо множина κ(Ax) номерів її власних аксіом рекурсивна. Це означає, що множина її власних аксіом Ax алгоритмічно розв'язна відносно множини всіх формул мови теорії.

Теорія *T рекурсивно-аксіоматизовна*, якщо *T* еквівалентна деякій рекурсивно-аксіоматизованій теорії.

Теорема 3.15 (про розв'язність). Нехай Т – повна теорія першого порядку з алгоритмічно перелічною множиною аксіом. Тоді Т розв'язна.

►Нехай $\aleph$ – алгоритм для переліку аксіом теорії T. Укажемо алгоритм $\Re$, який за кожною формулою S установлює $T \vdash S$ чи $T \vdash \neg S$, тобто $S \in Th(T)$ чи $S \notin Th(T)$. Спочатку алгоритм $\Re$ за формулою S будує її замикання $\bar{s}$, потім по черзі виконує такі дії:

1) видати алгоритмом $\aleph$ чергову аксіому А;

2) до множини вже отриманих теорем однократно застосувати всіма можливими способами правила П1–П5; множину отриманих нових формул позначимо **Fr**;

3) a) якщо $\bar{s} \in \mathbf{Fr} \cup \{A\}$, то видати результат "так" і зупинитись;

b) якщо $\neg\bar{s} \in \mathbf{Fr} \cup \{A\}$, то видати результат "ні" і зупинитись;

c) якщо $\bar{s} \notin \mathbf{Fr} \cup \{A\}$ та $\neg\bar{s} \notin \mathbf{Fr} \cup \{A\}$, то поповнити множину теорем формулами із $\mathbf{Fr} \cup \{A\}$ і перейти до 1).

За теоремою замикання $T \vdash S \Leftrightarrow T \vdash \bar{s}$ та $T \vdash \neg S \Leftrightarrow T \vdash \neg\bar{s}$.

При $T \vdash \bar{s}$ маємо $T \vdash S$.

При $T \vdash \neg\bar{s}$ за несуперечливістю T неможливо $T \vdash \bar{s}$, тому неможливо $T \vdash S$.

Однак $T \vdash \bar{s}$ або $T \vdash \neg\bar{s}$ за повнотою T, тому $\Re$ завжди зупиниться і поверне результат.

◄

Наслідок. Нехай T – повна перелічна теорія першого порядку. Тоді теорія T розв'язна. ■

Повертаючись до доведення теореми Лінденбаума, зауважимо, що множина аксіом теорії Σ_n далеко не в усіх випадках алгоритмічно перелічна, тому що проблема $\neg B_n \in Th(\Sigma_n)$, узагалі кажучи, алгоритмічно нерозв'язна. Тому в загальному випадку теорія Σ – несуперечливе просте повне розширення теорії T – неперелічна.

3.5. Теорема Геделя про повноту та її наслідки

Відомо багато різноманітних доведень теореми Геделя про повноту. Розглянемо одне з таких доведень, яке базується на використанні вільної інтерпретації мови L і побудові на її основі моделі для несуперечливої теорії.

Спочатку розглянемо наступну лему.

Лема 3.2. Нехай теорія першого порядку T_1 сигнатури σ_1 є розширенням теорії T сигнатури σ. Нехай $\mathbf{A_1} = (A, \sigma_1)$ є моделлю для T_1. Тоді $\mathbf{A} = (A, \sigma)$ є моделлю для теорії T.

►Індукцією за побудовою формули доводимо $\boldsymbol{A} \models \Phi \Leftrightarrow \boldsymbol{A_1} \models \Phi$ для кожної формули Φ сигнатури σ. Звідси отримуємо твердження Леми ◄.

Нехай T – теорія першого порядку потужності α, сигнатура σ якої містить константні символи.

Носієм моделі несуперечливої теорії T будуть фактор-класи замкнених термів, рівних між собою в теорії T.

Визначимо тепер канонічну інтерпретацію $\boldsymbol{M} = (U_{\approx}, \sigma_U)$ для теорії T.

Нехай a та b – замкнені терми мови L. Визначимо відношення

$a \approx b \Leftrightarrow T \vdash a = b$.

Покажемо, що відношення $\approx$ є еквівалентністю. Маємо $a \approx a$, тому що $\vdash a = a$ за правилом підстановки та аксіомою тотожності. Згідно з теоремами симетрії та транзитивності, $\vdash a = b \leftrightarrow b = a$ та $\vdash a = b \rightarrow b = c \rightarrow a = c$.

Отже, якщо $a \approx b$, то $b \approx a$; якщо $a \approx b$ та $b \approx c$, то $a \approx c$.

Нехай $U_{\approx}$ – множина всіх класів еквівалентності відносно $\approx$. Клас еквівалентності, який містить терм a, позначимо a'. Для $f^n, p^m \in \sigma$ Покладемо

$$f^n_M((a_1)', ..., ((a_n)') = (fa_1...a_n)' \quad (1)$$

$$p^m_M((a_1)', ..., ((a_m)') = 1 \Leftrightarrow T \vdash p^m a_1...a_m \quad (2)$$

і покажемо, що дана еквіваленція є конгруенцією відносно так визначених операцій і предикатів. Зрозуміло, що якщо c – константний символ, то $c_U = c'$.

Нехай $(a_1)' = (b_1)'$, ..., $(a_n)' = (b_n)'$, тобто $T \vdash a_1 = b_1$, ..., $T \vdash a_n = b_n$. (3)

Маємо $T \vdash a_1 = b_1 \rightarrow ... \rightarrow a_n = b_n \rightarrow fa_1...a_n = fb_1...b_n$ за аксіомою Ax4 і правилом підстановки.

Використовуючи (3), за МР маємо $T \vdash fa_1...a_n = fb_1...b_n$, тобто $(fa_1...a_n)' = (fb_1...b_n)'$.

Маємо $T \vdash a_1 = b_1 \rightarrow ... \rightarrow a_n = b_n \rightarrow pa_1...a_n \rightarrow pb_1...b_n$ за Ax4 і правилом підстановки. Використовуючи (3), маємо $T \vdash pa_1...a_n \rightarrow pb_1...b_n$ за МР.

Аналогічно $T \vdash pb_1...b_n \rightarrow pa_1...a_n$, звідки за ТТ $T \vdash pa_1...a_n \leftrightarrow pb_1...b_n$.

Отже, $p_M((a_1)', ..., (a_n)') = p_M((b_1)', ..., (b_n)')$ і відношення $\approx$ є конгруенцією відносно операцій і предикатів (1),(2). Значення цих операцій і предикатів не залежить від представників класів еквівалентності. Позначимо $\boldsymbol{M}$ – фактор- систему вільної АС $\boldsymbol{U}$ сигнатури σ по конгруенції $\approx$, яку і будемо називати канонічною для теорії T.

Лема 3.3. Нехай $\boldsymbol{M} = (U_{\approx}, \sigma_U)$ – канонічна інтерпретація теорії Т. Тоді для кожного замкненого терму t та кожної замкненої атомарної формули Ф теорії Т маємо:

1) $t_U = [t]$;

2) $\boldsymbol{M} \models \Phi \Leftrightarrow T \vdash \Phi$.

► Для доведення 1) використаємо індукцію за довжиною a.

Якщо a – константний символ, то $a_M = a'$.

Нехай $a = fa_1...a_n$. За припущенням індукції $(a_i)_M = (a_i)'$ для всіх $i \in \{1,\ldots,n\}$. Тому $(a_i)_M = f_M(fa_1...a_n) = = (fa_1...a_n)' = a'$.

Нехай замкнена атомарна формула Ф – це формула $pa_1...a_n$. Тоді $\boldsymbol{M} \models \Phi \Leftrightarrow p_M((a_1)', ..., ((a_n)') = T \Leftrightarrow \Leftrightarrow T \vdash pa_1...a_n \Leftrightarrow T \vdash \Phi$.

◄

Отже, для атомарних замкнених формул маємо $\boldsymbol{M} \models \Phi \Leftrightarrow T \vdash \Phi$. Для того, щоб умова $\boldsymbol{M} \models \Phi \Leftrightarrow T \vdash \Phi$ виконувалась для всіх формул теорії T, треба накласти на T деякі умови.

Теорія першого порядку T називається *теорією Генкіна*, якщо для кожної замкненої формули вигляду $\exists x$A існує константний символ e такий, що $T \vdash \exists x\mathrm{A} \to \mathrm{A}_x[e]$.

Теорема 3.17. Нехай Т – повна теорія Генкіна. Тоді канонічна інтерпретація **M** = (M, σ) для T є моделлю для T.

►Покажемо, що для кожної замкненої формули Ф теорії T маємо $\boldsymbol{M} \models \Phi \Leftrightarrow T \vdash \Phi$. Використаємо індукцію за кількістю символів логічних операцій формули Ф.

Для атомарних замкнених формул це уже доведено (теорема 7.3.2).

Нехай Ф має вигляд ¬B. Тоді $\boldsymbol{M} \models \Phi \Leftrightarrow \boldsymbol{M} \not\models \mathrm{B} \Leftrightarrow$ невірно $T \vdash \mathrm{B}$ (припущення індукції) $\Leftrightarrow T \vdash \neg\mathrm{B}$ (повнота T), тобто $T \vdash \Phi$.

Нехай Ф має вигляд ∨BC. Якщо $\boldsymbol{M} \models \vee\mathrm{BC}$, то маємо $\boldsymbol{M} \models \mathrm{B}$ або $\boldsymbol{M} \models \mathrm{C}$, тому за припущенням індукції $T \vdash \mathrm{B}$ або $T \vdash \mathrm{C}$. Звідси $T \vdash \vee\mathrm{BC}$ за ТТ, тобто $T \vdash \Phi$. Якщо $\boldsymbol{M} \not\models \vee\mathrm{BC}$, то $\boldsymbol{M} \not\models \mathrm{B}$ та $\boldsymbol{M} \not\models \mathrm{C}$, звідки невірно $T \vdash \mathrm{B}$ та невірно $T \vdash \mathrm{C}$ за припущенням індукції.

За повнотою T маємо $T \vdash \neg\mathrm{B}$ та $T \vdash \neg\mathrm{C}$, звідки за ТТ $T \vdash \neg\mathrm{B} \& \neg\mathrm{C}$, тому $T \vdash \neg\vee\mathrm{BC}$ за ТТ, тобто $T \vdash \neg\Phi$. Звідси невірно $T \vdash \Phi$ за несуперечливістю T. Отже, $\boldsymbol{M} \models \vee\mathrm{BC} \Leftrightarrow T \vdash \vee\mathrm{BC}$.

Нехай Ф має вигляд ∃xB. Маємо $\boldsymbol{M} \models \exists x\mathrm{B} \Leftrightarrow \mathrm{B}_M(a') = T$ для деякого $a' \in M$ $\Leftrightarrow \boldsymbol{M} \models \mathrm{B}_x[a]$ (формула $\mathrm{B}_x[a]$ замкнена, $a_M = a'$) $\Leftrightarrow T \vdash \mathrm{B}_x[a]$ (припущення індукції).

Покажемо $T \vdash \mathrm{B}_x[a] \Leftrightarrow T \vdash \exists x\mathrm{B}$.

Якщо $T \vdash \mathrm{B}_x[a]$, то, ураховуючи $T \vdash \mathrm{B}_x[a] \to \exists x\mathrm{B}$ (аксіома Ax3), маємо $T \vdash \exists x\mathrm{B}$ за MP.

Якщо $T \vdash \exists x\mathrm{B}$, то, ураховуючи $T \vdash \exists x\mathrm{B} \to \mathrm{B}_x[e]$ (тому що T – теорія Генкіна), для деякого константного символу e за MP $T \vdash \mathrm{B}_x[e]$. Тому $\boldsymbol{M} \models \mathrm{B}_x[e]$ за припущенням індукції. Однак e – ім'я деякого $a' \in M$, тому $\boldsymbol{M} \models \mathrm{B}_x[a]$, звідки $T \vdash \mathrm{B}_x[a]$ за припущенням індукції.

Ми показали $\boldsymbol{M} \models \Phi \Leftrightarrow T \vdash \Phi$ для кожної замкненої формули Ф теорії T. Ураховуючи теорему замикання, маємо $\boldsymbol{M} \models \Psi \Leftrightarrow T \vdash \Psi$ для кожної формули Ψ теорії T. Отже, $\boldsymbol{M}$ – модель для T.

◄

Укажемо тепер спосіб розширення довільної теорії першого порядку до теорії Генкіна. Нехай L – мова першого порядку. Індукцією за n визначимо спеціальні константні символи – константи-свідки рівня n.

Для кожної замкненої формули вигляду $\exists x$B мови L символ c з нижнім індексом $\exists x$B є константою-свідком рівня 0. Нехай константи-свідки всіх рівнів $<n$ уже визначені. Нехай замкнена формула вигляду $\exists x$B утворена із символів мови L та цих констант, причому $\exists x$B містить хоч одну константу-свідка рівня n–1. Символ c з нижнім індексом $\exists x$B є константою-свідком рівня n.

Додавши до мови L константи-свідки всіх рівнів, дістанемо мову L_C.

Константу-свідка з нижнім індексом A називають константою-свідком для A.

Якщо $\exists x$A – замкнена формула мови L_C, то в L_C існує єдина константа-свідок для $\exists x$A, причому її рівень на 1 більше максимального рівня всіх констант-свідків, які входять до $\exists x$A, або рівний 0, якщо $\exists x$A не містить констант-свідків. Нехай c – константа-свідок для $\exists x$A. Формулу $\exists x\mathrm{A}\to\mathrm{A}_x[c]$ назвемо аксіомою для свідка c.

Нехай T – теорія першого порядку з мовою L. Тоді теорія першого порядку T_C з мовою L_C, власними аксіомами якої є власні аксіоми теорії T та всі аксіоми для свідків із L_C, є теорією Генкіна.

Лема 3.4. Якщо T несуперечлива, то $\mathrm{T_C}$ несуперечлива.

►Нехай T_1 – константне розширення теорії T за допомогою всіх констант-свідків із L_C. Якщо T_1 суперечлива, то $T_1 \vdash c \neq c$ для деякої константи c. Тоді $T \vdash x \neq x$ за теоремою про константи, звідки T суперечлива. Отже, T_1 несуперечлива.

Нехай **S** – множина всіх аксіом для свідків із L_C. Тоді $T_C = T_1[\mathbf{S}]$.

Покажемо, що тоді $T_C \vdash$ A $\Leftrightarrow$ $T_1 \vdash$ A для кожної формули A теорії T.

Нехай A – довільна формула теорії T, нехай $T_C \vdash$ A, тобто $T_1[\mathbf{S}] \vdash$A. За теоремою редукції існують формули $\mathrm{B}_1, ..., \mathrm{B}_n$ із **S** такі, що $T_1 \vdash \mathrm{B}_1\to...\to\mathrm{B}_n\to\mathrm{A}$. Для доведення $T_1 \vdash$ A застосуємо індукцію за n.

Якщо $n = 0$, то вже маємо $T_1 \vdash$ A.

Нехай $n > 0$, нехай B_1 – це формула $\exists x\mathrm{D}\to\mathrm{D}_x[c]$. Без обмеження загальності вважаємо, що рівень константи-свідка c, для якої B_1 є аксіомою, не нижче рівнів констант-свідків, для яких $\mathrm{B}_2, ..., \mathrm{B}_n$ є аксіомами. Тоді константа-свідок c не входить до складу $\mathrm{B}_2, ..., \mathrm{B}_n$, A. Формулу $\mathrm{B}_2\to...\to\mathrm{B}_n\to\mathrm{A}$ позначимо R.

Нехай y – нове ім'я, яке не входить до складу A, $\mathrm{B}_1, ..., \mathrm{B}_n$. Нехай Ф – формула $(\exists x\mathrm{D}\to\mathrm{D}_x[c])\to\mathrm{R}$. Тоді $\mathrm{B}_1\to\mathrm{R}$ – це формула $\Phi_y[c]$.

Маємо $T_1 \vdash \Phi_y [c]$. Звідси за теоремою 7.2.15 $T_1 \vdash \Phi$, тобто $T_1 \vdash (\exists x\mathrm{D}\to\mathrm{D}_x[c])\to\mathrm{R}$.

За П5 тоді $T_1 \vdash \exists y(\exists x\mathrm{D}\to \mathrm{D}_x[y])\to\mathrm{R}$. Однак за теоремою про варіанту маємо $T_1 \vdash \exists x\mathrm{D}\to\exists y\mathrm{D}_x[y]$, тобто $T_1 \vdash \neg\exists x\mathrm{D}\vee\exists y\mathrm{D}_x[y]$. Звідси $T_1 \vdash \exists y(\neg\exists x\mathrm{D}\vee\mathrm{D}_x[y])$ за теоремою 7.1.21, тобто $T_1 \vdash \exists y(\exists x\mathrm{D}\to\mathrm{D}_x[y])$.

За МР звідси та з $T_1 \vdash \exists y(\exists x\mathrm{D}\to\mathrm{D}_x[y]) \to\mathrm{R}$ маємо $T_1 \vdash\mathrm{R}$, тобто $T_1 \vdash \mathrm{B}_2\to\ldots\to\mathrm{B}_n\to\mathrm{A}$. За припущенням індукції тоді $T_1 \vdash\mathrm{A}$.

Нехай T_C суперечлива. Тоді $T_C \vdash x \neq x$, звідки $T_1 \vdash x \neq x$, тобто T_1 суперечлива. Однак T_1 несуперечлива, тому T_C несуперечлива.

◄.

Теорема 3.18 (Геделя – Генкіна). Нехай T – несуперечлива теорія першого порядку потужності α. Тоді T має модель потужності $\leq\alpha$.

►Побудуємо для T теорію Генкіна T_C. Згідно з теоремою 7.3.4, T_C несуперечлива. Нехай σ та σ_C – сигнатури теорій T та T_C відповідно. Згідно з теоремою Ліндербаума, T_C має несуперечливе просте повне розширення K, яке теж є теорією Генкіна, тому що є простим розширенням теорії T_C. За теоремою 7.3.2 канонічна інтерпретація $\boldsymbol{M} = (M, \sigma_C)$ є моделлю для K, тому за теоремою 7.3.1 (M, σ) є моделлю для T. Зрозуміло, що потужність M не перевищує α.

◄

Наслідок. Кожна несуперечлива зліченна теорія першого порядку має зліченну або скінченну модель. ■

Теорема 3.19 (Геделя про повноту, модельне формулювання). Теорія першого порядку T несуперечлива $\Leftrightarrow$ T має модель.

►Якщо T несуперечлива, то T має модель згідно з теоремою 3.18.

Якщо T має модель $\boldsymbol{M}$, то кожна формула вигляду $\neg\mathrm{A}\&\mathrm{A}$ на $\boldsymbol{M}$ хибна, тому $T \vdash \neg\mathrm{A}\&\mathrm{A}$ неможливо, звідки T несуперечлива.

◄.

Теорема 3.20 (Геделя про повноту, теорема адекватності). Нехай T – теорія першого порядку. Тоді формула Φ істинна в T $\Leftrightarrow$ $\mathrm{T}\vdash\Phi$.

►Випливає з теореми 3.18.. Справді, нехай $\bar{\Phi}$ – замикання формули Φ. Тоді маємо: $T \vdash \Phi \Leftrightarrow T \vdash \bar{\Phi}$ (за правилом замикання) $\Leftrightarrow T[\neg\bar{\Phi}]$ суперечлива $\Leftrightarrow$ теорія $T[\neg\bar{\Phi}]$ не має моделі (за теоремою 3.19) $\Leftrightarrow$ $\bar{\Phi}$ істинна в T (тому що кожна модель для $T[\neg\bar{\Phi}]$ – це така модель $\boldsymbol{M}$ теорії T, для якої $\boldsymbol{M} \not\models \bar{\Phi}$, тому, якщо теорія $T[\neg\bar{\Phi}]$ не має моделі, то $\boldsymbol{M} \models \bar{\Phi}$ для кожної моделі $\boldsymbol{M}$ теорії T, тобто $\bar{\Phi}$ істинна в T) $\Leftrightarrow$ Φ істинна в теорії T (за правилом замикання).

◄

Теорема Геделя про повноту засвідчує повноту логічних засобів логік першого порядку. Вона стверджує, що логічних засобів теорії першого порядку, тобто її аксіом і правил виведення, достатньо для виведення кожної істинної в теорії формули. Інакше кажучи, теорема про повноту свідчить, що семантична та синтаксична істинності адекватні.

Із теореми Геделя про повноту безпосередньо випливає

Теорема 3.21 (Левенгейма – Сколема про спуск). Нехай теорія першого порядку потужності α має модель, тоді вона має модель потужності $\leq\alpha$.

►Якщо теорія *T* має модель, то *T* несуперечлива. За теоремою 3.18 *T* має модель потужності $\leq\alpha$.◄

Наслідок. Якщо зліченна теорія першого порядку має нескінченну модель, то вона має зліченну модель. ■

З теореми Геделя про повноту випливає низка важливих наслідків. Розглянемо їх детальніше.

Як встановив А.Чорч, проблема всюди істинності формул першого порядку в загальному випадку алгоритмічно нерозв'язна. У той же час

Теорема 3.22. Проблема всюди істинності формул першого порядку зліченної сигнатури частково розв'язна.

►За теоремою Геделя про повноту для кожної формули А маємо $\vdash A \Leftrightarrow\ \models A$. Числення предикатів першого порядку зліченної сигнатури має перелічну множину аксіом, тому за теоремою 3.14 множина його теорем перелічна, звідки проблема "$\vdash A$" частково розв'язна.

◄

Теорема компактності. Важливим наслідком теореми Геделя про повноту є теорема компактності.

Теорія *T скінченно-аксіоматизована,* якщо множина її власних аксіом скінченна.

Теорія *T скінченно-аксіоматизовна,* якщо *T* еквівалентна деякій скінченно-аксіоматизованій теорії.

Скінченно-аксіоматизованою частиною (САЧ) теорії *T* називають просте скінченно-аксіоматизоване звуження теорії *T*.

Теорема 3.23 (компактності, перше формулювання). Формула Ф істинна в T $\Leftrightarrow$ Ф істинна в деякій САЧ $K\subseteq T$.

►Нехай Ф істинна в *T*. За теоремою 3.20 тоді $T \vdash \Phi$. Таке виведення використовує тільки скінченну кількість аксіом, тому може бути проведено в межах деякої *САЧ* $K\subseteq T$. Отже, $K \vdash \Phi$, тому Ф істинна в *K*.

Кожна модель теорії *T* є моделлю кожного її звуження, тому, якщо Ф істинна в деякій САЧ $K\subseteq T$, то Ф істинна в *T*.

◄

Теорема 3.24 (компактності, друге формулювання). Теорія першого порядку Т має модель ⇔ кожна САЧ теорії Т має модель.

►Якщо T має модель $\boldsymbol{M}$, то всі аксіоми T істинні на $\boldsymbol{M}$. Отже, кожна аксіома з довільної скінченної підмножини аксіом T істинна на $\boldsymbol{M}$. Тому $\boldsymbol{M}$ є моделлю кожної САЧ теорії T.

Якщо кожна САЧ теорії T має модель, то T несуперечлива, тому що виведення кожної суперечності (формули вигляду ¬A&A) використовує скінченну кількість аксіом. Тому за теоремою 3.19 теорія T має модель.

◄

Теорема 3.25 (Левенгейма – Сколема про підйом). Нехай теорія першого порядку Т потужності α має нескінченну модель. Тоді Т має модель довільної потужності $\beta \geq \alpha$.

►Нехай $\boldsymbol{M} = (M, \sigma)$ – нескінченна модель для T, нехай $\{c_i\}_{i\in\beta}$ – множина нових констант потужністю β. Розглянемо $T_1 = T\,[\,\wp\,]$ сигнатури $\sigma' = \sigma\cup\{c_i\}_{i\in\beta}$, де $\wp$ складається з усіх можливих формул вигляду $c_i \neq c_j$ для $i\neq j,\ i, j\in\beta$. Кожна САЧ K теорії T_1 містить скінченну кількість нових аксіом вигляду $c_i \neq c_j$, тому всі нові константи з їх складу можна так інтерпретувати на $\boldsymbol{M}$, щоб ці аксіоми були істинними на (M, σ'), звідки (M, σ') – модель для K.

Отже, кожна САЧ теорії T_1 має модель, тому і T_1 має модель, отже, T_1 несуперечлива. За теоремо 3.21 теорія T_1 має модель $\boldsymbol{M}_1 = (M_1, \sigma')$ потужності $\leq\beta$. Однак усі формули вигляду $c_i \neq c_j$ для $i \neq j$ істинні на $\boldsymbol{M}_1$, тому потужність $\boldsymbol{M}_1$ не менша за β, звідки потужність $\boldsymbol{M}_1$ дорівнює β і вона є) є моделлю для теорії T.

◄

Наслідок 1. Нехай зліченна теорія першого порядку Т має нескінченну модель. Тоді Т має модель довільної потужності $\beta \geq \alpha$.■

Наслідок 2. Ar має нескінченні моделі як завгодно великої потужності.

Моделі формальної арифметики *Ar*, які неізоморфні її стандартній моделі, названі *нестандартними* або сколемівськими. ■

Наслідок 2 засвідчує існування незліченних нестандартних моделей арифметики *Ar*. Але існують і злічені нестандартні моделі арифметики.

Існування нестандартних моделей формальної арифметики засвідчує неадекватність, неповноту опису множини натуральних чисел за допомогою аксіом *Ar*. У той же час, використовуючи принцип математичної індукції, можна неформально показати єдиність з точністю до ізоморфізму моделі для *Ar*.

Справа тут у тому, що принцип математичної індукції виконується для всіх властивостей натуральних чисел, а таких властивостей – континуум. У той же час, схема аксіом індукції Ar7 забезпечує виконання принципу математичної індукції тільки для зліченної множини властивостей натуральних чисел, які можуть бути виражені мовою арифметики.

Таким чином, принцип математичної індукції формалізується в *Ar* не повністю, що засвідчує принципову відмінність між інтуїтивним і формальним його розумінням.

На щастя, ситуація з формальною арифметикою не настільки погана. Якщо вимагати *обчислюваності* операцій додавання та множення, то існує *єдина* з точністю до ізоморфізму модель *Ar*.

3.6. Теореми Геделя про неповноту

До найвидатніших досягнень сучасної математики належать знамениті теореми Геделя про неповноту. Вони вказують на принципову обмеженість формально-аксіоматичного методу побудови складних математичних теорій.

Перша теорема Геделя про неповноту встановлює для широкого класу формальних систем (які включають, або в яких можна виразити формальну арифметику) існування формул, нерозв'язних у тому смислі, що ні формула, ні її заперечення невивідні в системі.

Друга теорема про неповноту стверджує, що несуперечливість таких систем не можна встановити внутрішніми засобами самих систем.

Теорема 3.26 (перша Геделя про неповноту). Якщо формальна арифметика Ar несуперечлива, то Ar неповна.

►Множина аксіом *Ar* алгоритмічно перелічна, тому за теоремою 3.14 множина Th(*Ar*) алгоритмічно перелічна. Якщо *Ar* несуперечлива, то вона має модель. За теоремою істинності кожна теорема *Ar* істинна на кожній моделі *Ar*, зокрема на її стандартній моделі ***N***. Отже, якщо *Ar* $\vdash$S, то S є ІАФ.

За відомою теоремою Тарського множина ІАФ неперелічна, тому Th(*Ar*)$\subset$ІАФ. Візьмемо довільну замкнену формулу Ф$\in$ІАФ\Th(*Ar*). Тоді $\neg$Ф$\notin$ІАФ, звідки $\neg$Ф$\notin$Th(*Ar*). Таким чином, замкнена формула Ф така, що Ф$\notin$Th(*Ar*) і $\neg$Ф$\notin$Th(*Ar*). Звідси випливає, що *Ar* неповна.

◄

Як наслідок теорем Геделя про повноту й неповноту отримуємо ще одне доведення існування нестандартних моделей формальної арифметики.

Нехай ***N*** – єдина (з точністю до ізоморфізму) модель *Ar*. Тоді множина істинних в *Ar* формул збігається з множиною ІАФ. За теоремою Геделя про повноту ця множина збігається з множиною Th(*Ar*), тому Th(*Ar*) = ІАФ.

Маємо суперечність, тому з необхідністю існують моделі *Ar*, які неізоморфні ***N*** – *нестандартні* моделі арифметики.

Таким чином, навіть ті властивості натуральних чисел, які виражаються мовою арифметики, не можуть адекватно описуватися теорією першого порядку з алгоритмічно перелічною множиною аксіом. Справді, за теоремою 3.14 множина теорем такої теорії алгоритмічно перелічна, у той же час множина ІАФ неперелічна. Тому кожне перелічне розширення формальної арифметики з необхідністю неповне й має неізоморфні моделі.

Перша теорема Геделя про неповноту є синтаксичним варіантом теореми Тарського і може розглядатися як її наслідок, хоча для факту неповноти *Ar* достатньо неперелічності множини ІАФ.

Зауважимо, що початкове доведення Геделя не використовувало ні понять теорії алгоритмів, ні теореми Тарського. Використовуючи розроблений ним метод нумерацій, Гедель побудував конкретну арифметичну формулу S, яка виражає власну невивідність, звідки отримав $S\notin\mathrm{Th}(Ar)$ та $\neg S\notin\mathrm{Th}(Ar)$.

Розглянемо тепер питання про розв'язність *Ar*. Можна встановити нерозв'язність *Ar* та її несуперечливих розширень, звідки випливає узагальнення першої теореми Геделя про неповноту.

Арифметична формула $\Phi(x_1,..., _k)$ *виражає* в *Ar* множину $L\subseteq N^k$, якщо

$(\bar{n}_1,...,\bar{n}_k)\in L \Leftrightarrow Ar|-\Phi_{x_1,...,x_k}[\bar{n}_1,...,\bar{n}_k]$.

Множина *L* *виражається* в *Ar*, якщо існує арифметична формула, яка виражає *L* в *Ar*.

Теорема 3.27. Множина L виражається в Ar $\Leftrightarrow$ L є РПМ.

◄ Див. Вправи. ◄

Установлення А. Чорчем нерозв'язності формальної арифметики *Ar* було одним з перших успіхів теорії алгоритмів. Пізніше було доведено, що така нерозв'язність справджується також для всіх несуперечливих розширень *Ar*.

Зауважимо, що просте несуперечливе розширення *Ar* можна отримати, узявши множину ІАФ як множину власних аксіом. Така теорія $T_{\text{п}}$ несуперечлива, тому що $T_{\text{п}}$ є моделлю ***N***. Згідно з $\text{ІАФ}\subseteq\mathrm{Th}(T_{\text{п}})$, маємо $\mathrm{Th}(T_{\text{п}}) = \text{ІАФ}$. Для кожної замкненої арифметичної формули Ф маємо $\Phi\in\text{ІАФ}$ або $\Phi\notin\text{ІАФ}$, тому, згідно з $\mathrm{Th}(T_{\text{п}}) = \text{ІАФ}$, теорія $T_{\text{п}}$ повна. За наслідком теореми 3.15 теорія $T_{\text{п}}$ з необхідністю неперелічна, що дає ще одне доведення неперелічності множини ІАФ.

Друга теорема Геделя про неповноту, як і його перша теорема, справджується для кожної формальної системи, у якій моделюється *Ar*. Тому для кожної достатньо багатої системи доведення її несуперечливості *з необхідністю* вимагає засобів, які лежать *за межами* самої системи.

Теореми Геделя про неповноту засвідчують *принципову обмеженість* формально-аксіоматичного методу. Таким чином, кожна спроба "втиснути" достатньо багату математичну теорію в рамки певної формальної системи неминуче веде до тверджень, які неможливо ні довести, ні спростувати в межах цієї системи. Для доведення несуперечливості такої системи внутрішніх її засобів недостатньо, ми неминуче мусимо використовувати якісь сильніші, зовнішні відносно системи засоби.

Це, звичайно, не означає, що неможливо надійно довести несуперечливість формальної арифметики чи подібних систем. Просто методи доведення несуперечливості *Ar* уже не можуть бути фінітними, конструктивними. Зараз відомо багато таких доведень різноманітними способами, так що несуперечливість арифметики можна вважати надійно обґрунтованою.

ВПРАВИ

1. Довести в численні предикатів наступні теореми:
   1) $|-\exists x\mathrm{A}\&\mathrm{B}\leftrightarrow\exists x(\mathrm{A}\&\mathrm{B})$, якщо x не вільна в B;
   2) $|-\forall x\mathrm{A}\&\mathrm{B}\leftrightarrow\forall x(\mathrm{A}\&\mathrm{B})$, якщо x не вільна в B;
   3) $|-\forall x\forall y\mathrm{A}\leftrightarrow\forall y\forall x\mathrm{A}$;
   4
   5) $|-\forall x(\mathrm{A}\&\mathrm{B})\to\forall x\mathrm{A}\&\mathrm{B}$;
   6) $|-(\mathrm{A}\to\forall x\mathrm{B})\to(\forall x\mathrm{A}\to\mathrm{B})$;
   7
   8
   9) $|-\exists x(\mathrm{A}\to\mathrm{B})\to(\forall x\mathrm{A}\to\exists x\mathrm{B})$;
   10) $|-\forall x(\mathrm{A}\to\mathrm{B})\to(\forall x\mathrm{A}\to\forall x\mathrm{B})$;
   11) $|-\forall x(\mathrm{A}\to\mathrm{B})\to(\exists x\mathrm{A}\to\exists x\mathrm{B})$;
   12) $|-(\forall x\mathrm{A}\to\forall x\mathrm{B})\to\exists x(\mathrm{A}\to\mathrm{B})$;
   13) $|-(\exists x\mathrm{A}\to\exists x\mathrm{B})\to\exists x(\mathrm{A}\to\mathrm{B})$.
2. Довести лему 3.2 та теореми 3.2, 3.3, 3.7, 3.8, 3.11, 3.27.
3. Довести в *Ar* виразність усіх *РПМ*.

ДОДАТОК

Додаткові вправи до Розділу I

1. Довести умову достатності $(\Leftarrow)$ у лемі 1.2.
2. Довести пп. R2 та R4 леми 1.3.
3. Застосувати метод редукції і довести, що наступні формули є
4. а) виконуваними: 1) $A \to B \to (B \to A)$, 2) $A \to (B \to (B \,\&\, A))$, 3) $\neg A \to (B \to A)$;
5. б) спростовними: 1) $\neg(B \to (B \to A))$, 2) $\neg B \,\&\, \neg(B \to A))$, 3) $\neg(A \to B) \,\&\, \neg(A \to \neg B))$.
6. Розв'язати вправу 2 методом редукції.
7. Довести коректність правил виведення ПЧ П1-П4.
8. Довести, що всяка КНФ є теоремою ПЧ, не посилаючись на ТТ..
9. Довести повноту ПЧ з системою аксіом та правилом MP (див. Лема 1.5а):
   $A \to (B \to A), (A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
   $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$.
10. Позначимо $\Im$ – множину всіх формул ПЧ і покладемо $\mathbf{1} \equiv x \vee \neg x$ та $\mathbf{0} \equiv x \,\&\, \neg x$. Нехай $\lambda = \{\neg^1, \vee^2, \&^2\}$ сигнатура операцій на формулах, представлених зв'язками $\neg, \vee, \&$, а $A = (\Im, \lambda)$ – відповідна алгебра сигнатури λ. Покладемо відношення $\Phi \approx \Psi \Leftrightarrow \Phi \leftrightarrow \Psi$. Показати, що а) відношення $\approx$ є конгруенцією на $\Im$ (див. 2.2); фактор алгебра $\Im_{\approx} = ([\Im], \lambda)$ за цією конгруенцією називається алгеброю Лінденбаума; б) алгебра Лінденбаума $\Im_{\approx}$ є булевою алгеброю, в якій клас $[\mathbf{1}]$ є одиницею, клас $[\mathbf{0}]$ – нулем, для операцій заперечення виконуються рівності $[\mathbf{1}] = [X] \vee \neg[X]$, $[\mathbf{0}] = [X] \,\&\, \neg[X]$, а бінарні операції – асоціативні та комутативні і для них справедливі закони дистрибутивності (див. закони ПЛ 3.1 та 3.2).

Додаткові вправи до Розділу 2

Довести асоціативність операції множення для підстановок термів.

1. Доведіть чи спростуйте такі твердження:

$\forall$

$\exists x$

$\exists \forall y$

$\forall y x$

$A x$

$A \to$

$\exists \forall \to$

$\forall y x$

7) $|= \forall x A \& \forall x B \to \forall x(A \& B)$;
8) $|= \forall x(A \& B) \to \forall x A \& \forall x B$;
9) $|= \exists x A \& \exists x B \to \exists x(A \& B)$;
10) $|= \exists x(A \& B) \to \exists x A \& \exists x B$;
11) $|= \exists x A \vee B \to A \vee \exists x B$;
12) $|= A \& \forall x B \to \forall x A \& B$;
13) $|= \forall x A \vee \exists x B \to \exists x A \vee \forall x B$;
14) $|= \exists x A \vee \forall x B \to \forall x A \vee \exists x B$;
15) $|= (A \to B) \to (\exists x A \to \exists x B)$;
16) $|= (A \to B) \to (\forall x A \to \forall x B)$.

2. Чи вірно:
   a) $|= \exists x(P \& Q) \to \exists x P \& Q$?
   b) $|= \exists x P \& Q \to \exists x(P \& Q)$?
   c) $\forall x P \to \exists x Q || = \forall x P \to Q$?
   2) a) $P \to Q |= \forall x P \to \forall x Q$?
   b) $\forall x P \to \forall x Q |= P \to Q$?
   c) $\forall x P \to \forall x Q || = \exists x P \to \exists x Q$?
   3) a) $\forall x P \to Q |= \forall x(P \to Q)$?
   b) $\exists x(P \to Q) |= \exists x P \to Q$?
   c) $\forall x P \to \exists x Q || = P \to \exists x Q$?
   4) a) $|= \forall x(P \vee Q) \to \forall x P \vee Q$?
   b) $|= \forall x P \vee Q \to \forall x(P \vee Q)$?
   c) $\exists x P \to \exists x Q || = \forall x P \to \forall x Q$?

3. Вкажіть формули відповідної мови, що виражають предикати:
   m
   "*x* – парне" та "*x* – непарне" в АС (*Z*; +);
   d
   x
   "*x*=2" в АС (*N*; +); "*y*=*x*+3" в АС (*N*; +);
   y та "*x*=1" в АС (*N*; <);
   в АС (*R*; ·) "|*x*|=2" в АС (*Z*; +);

4. Вкажіть формули, що виражають предикати:
   1) "існує більше чотирьох парних чисел";
   2) "існує не менше чотирьох непарних чисел";
   3) "існує не більше двох повних кубів";
   4) "існує менше трьох повних квадратів";
   5) "не існує простих чисел, кратних 4";
   6) "існують прості числа, кратні 5";

7) "існує рівно 2 непростих числа, кратних 4";
8) "існує менше чотирьох повних квадратів, кратних 5";
9) "існує принаймні 3 непарних простих чисел";
10) "існує рівно 3 парних числа, що є точними кубами";
11) "існує більше двох простих чисел, не кратних 3";
12) "невірно, що існує рівно 2 числа, що є сумою 4-х квадратів";
13) "існує менше чотирьох парних непростих чисел";
14) "існує більше двох чисел, що є сумою трьох кубів";
15) "множина непарних чисел нескінченна";
16) "існує єдине парне просте число";
17) "кожне парне число, більше за 2, є сумою двох простих чисел".

5. Вкажіть формули Lar, що виражають функції:

$x \dot{-} y$;

$-y|$;

$x, [y/z]$);

$HCD(x, y)$;

$HCK(x, y)$;

$HCD(x, [y/z])$;

$[x / HCK(y, z)]$);

$[\sqrt{HCK(x, y)}]$;

1

0 1

1)

)

x

H

C

12) $HCK(x, [\sqrt{[y/z]}])$;

13) $[HCD(x, y) / [\sqrt{z}]]$;

14) $[\sqrt{HCD([x/y], z)}]$.

6. У якому відношенні щ...

N ... Z ... Q ... та (R; +) ?

... та (R;<) ?

7. У якому відношенні щодо елементарної еквівалентності такі АС:

... та (R; {+, =}) ?

... та (Q; {<, =}) ?

8. Опишіть всі автоморфізми таких АС:

... та (R; {≤, =}) ?

... та (C; {×, =}) ?

N x = y

9. Встановіть, чи виразні в АС предикати:
   1) В АС (Z; {+, =}) предикати
      i. "mod (x, 3)=0"; "mod (x, 2)=1"; "mod (x, 5)=2" ?
      ii. "mod (x, 4)=0"; "mod (x, 3)=2"; "mod (x, 4)=3"; "$z=x\times y$" ?
   2) В АС (Z; {×, =}) предикати
      i. "x=3"; "x= −2"; " $z=x+y$" ?
      ii. "x=1"; "x= −1"; "x=5" ?
      iii. "x=0"; "x=7"; "$x=y+6$"; "$z=x+y+1$" ?
10. Встановіть, чи виразні в АС предикати:
    1) В АС (N; {+, =}) предикати "x=3"; "mod(x, 3)=0", "mod(x, 3)=2"; "z=x×y" ?
    2) В АС (N; {×, =}) предикати "x=10"; "mod(x, 3)=0", "mod(x, 2)=1"; "z=x+y" ?
    3) В АС (N; {<, =}) предикати "x=0"; "x=2"; "x=3"; "z=x+1" ?
    4) В АС (N; {y=x+1, =}) предикати "x=0"; "x=1"; "x=2" ?
    5) В АС (N; {y=x+2, =}) предикати " x=1"; "x=6"; "y=x+6"; "y=x+1" ?
    6) В АС (N; {y=x+3, =}) предикати: "x=3", "y=x+2"; "y=x+6"; "x=2" ?
    7) В АС (Z; {y=x+2}) предикати "x=2"; "|x–y|=2"; "y=x+4" ?
    8) В АС (Z; {x–y = 3, =}) предикати "x=4"; "x–y = 4"; "|x–y| = 6" ?
    9) В АС (N; {y=x+4, =}) предикати "x=3"; "y = x+3"; "|x–y| = 12" ?
    10) В АС (R; {$|x–y|$=1, =}) предикати "x=0"; "$x–y$=1"; "$y=x+2$" ?
    11) В АС (Z; {|x–y|=1, =})
    12) В АС (Z; {$|x–y|$=2, =}) предикати "x=2"; "$|x–y|$=3"; "$z=x+y$" ?
    13) В АС (Q; {$|x–y|$=2, =}) предикати "$x–y$=2"; "$z=x+y$"; "$|x–y|$=4"; "$y=x+2$" ?
    14) В АС (Q; {$|x–y|$=3, =}) предикати "x=1"; "$|x–y|$=6"; "$z=x\times y$" ?
    15) В АС (Z; {$|x–y|$=3, =}) предикати "x=3"; "$x–y$=3"; "$|x–y|$ = 12" ?
    16) В АС (Z; {$|x–y|$ = 4, =}) предикати "x=4"; "$x–y$ = 4"; "$|x–y|$ = 8" ?
    17) В АС (Z; {x/y, =}) предикати "x=0"; "x=1"; "$z=x+y$" ?
    18) В АС (N; {x/y, =}) предикати "x=1"; "x=5"; "x – просте" ?
11. Визначіть, вказавши мову та власні аксіоми, теорії 1-го порядку таких математичних структур:
    1) комутативної групи;
    2) кільця;
    3) кільця з одиницею;
    4) комутативного кільця;
    5) тіла (некомутативного поля);
    6) поля;

7) частково впорядкованої множини;
8) лінійно впорядкованої множини;
9) решітки;
10) булевої решітки;
11) повної групи;
12) групи без кручень;
13) алгебраїчно замкненого поля;
14) впорядкованого поля дійсних чисел.

12. Нехай T_0 - чисте ЧП з порожньою сигнатурою функціональних, предикатних та константних символів. Базові формули теорії T_0 мають вигляд $u = v$, де u, v - змінні. Показати, що в теорії T_0 всі аксіоми та правила виведення є незалежними, тобто вилучення кожного з них приводить до втрати теорем [19].

    Вказівка. Розглянемо відображення f на множині формул теорії T_0 з істинністними значеннями таке, що $f(u = v) = 1$, $f(\neg A) = 0$, $f(A \vee B) = f(B)$, $f(\exists x A) = 1$. Показати, що для будь-якої теореми $\Phi \in Th(T_0)$, доведеної без пропозиційної аксіоми $f(\Phi) = 1$. Аналогічно, потрібно підібрати своє відображення f для решти аксіом ЧП та правил виведення П1-П5 теорії T_0.

13. Довести в ЧП теореми:
    1. |
    2. $\vdash$
    3. $\nvdash \forall x \exists y (x=y)$;

    $\leftrightarrow \exists y(x=y \& B(y))$;
    $\leftrightarrow \forall y(x=y \rightarrow B(y))$;

14. Формалізувати певне висловлювання означає ввести позначення для базових його властивостей і записати його у мові 1-го порядку. Наприклад, формалізуємо висловлювання $\Psi \equiv$ «Петру подобається Оксана, але тій він не цікавий.» Нехай $P(x, y)$ означає, що « x подобається y». Тоді Ψ можна записати як $P(\textit{Петро}, \textit{Оксана}) \& \neg P(\textit{Оксана}, \textit{Петро})$. Слід зазначити, що при формалізації може втрачатися частина смислів висловлювання, але це вже інше питання. Формалізувати наступні висловлювання (частина з них з [11]):
    1. Кішки бувають тільки білі і сірі.
    2. Логіка буває заводить мене в глухий кут.
    3. Жодний нероба не стане знаменитістю.
    4. Ніщо розумне не заводить мене в глухий кут. Логіка буває заводить в глухий кут. Отже, логіка буває нерозумною.
    5. Жоден суддя не є справедливим.

6. Деякі поросята не вміють літати. Всі орли вміють літати. Деякі поросята – не орли.
7. Якщо будеш хорошо вчитися – попадеш в Google, якщо ні – станеш тестувальником.
8. Деякі ледарі не оптимісти, але полюбляють життя.
9. Деякі лекції не можливо зрозуміти.

15. Перевести з формальної мови на природню:
    1. $\neg\forall x(C(x) \to Cn(x) \vee V(x))$, $C(x)$- бути студентом, $Cn(x)$- бути спортсменом, $V(x)$- бути відмінником.
    2. $\forall x \forall y(A(x) \,\&\, A(y) \,\&\, З(x, y) \to П(x, y) \vee П(y, x))$, $A(x)$ – бути акулою, $З(x, y)$ – зустрічатися, $П(x, y)$- поїдати.

ЛІТЕРАТУРА

1. Гильберт Д., Бернайс П. Основания математики. Логические мсчисления и формализация арифметики.-М., 1979.
2. Капітонова Ю.В., Кривий С.Л., Летичевський О.А., Луцький Г.М., Печурін М.К. Основи дискретної математики. – К., 2002.
3. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций. – М., 1983.
4. Клини С. Математическая логика. – М., 1973.
5. Кривий С.Л. Дискретна математика: Вибр.питання: Навч. посібник. – К.: 2007. – 572 с.
6. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математической логике и теории алгоритмов. – М., 1975.
7. Лісовик Л.П., Шкільняк С.С. Теорія алгоритмів. – К., 2003.
8. Мальцев А.И. Алгебраические системы. – М., 1970.
9. Манин Ю.И. Доказуемое и недоказуемое. – М., 1979.
10. Мендельсон Э. Введение в математическую логику. – М., 1976.
11. Непейвода Н.Н. Прикладная логика. – Новосибирск, 2000.
12. Нікітченко М.С., Шкільняк С.С. Математична логіка. – К., 2003.
13. Нікітченко М.С., Шкільняк С.С. Математична логіка. Додаткові розділи. – К., 2004.
14. Нікітченко М.С., Шкільняк С.С. Основи математичної логіки. – К., 2006.
15. Шкільняк С.С. Математична логіка. Приклади і задачі: Навчальний посібник. – К.: Видавничо-поліграфічний центр "Київський університет", 2007. – 145 с.
16. Нікітченко М.С., Шкільняк С.С. Математична логіка та теорія влгоритмів: Підручник. – К., 2008. – 528 с.
17. Шкільняк С.С. Математична логіка; Теорія влгоритмів: Навч. посібник. – К., 2009-280 с.
18. Чень Ч., Ли Р. Математическая логика и автоматическое доказательство теорем. – М., 1983.
19. Шенфилд Дж. Математическая логика. – М., 1975.
20. Чорч А. Введение в математическую логику. Том первый.-М., 1960.

Навчальне видання

Зубенко Віталій Володимирович
Шкільняк Степан Степанович

ОСНОВИ МАТЕМАТИЧНОЇ ЛОГІКИ

Навчальний посібник

Підписано до друку 29.04.2020. Формат 60х84\16
Ум. друк. арк. 5,6. Обл.-вид.арк. 5,6
Наклад 300 прим. Зам. № 200268

Видавець і виготовлювач Національний університет біоресурсів
і природокористування України,
вул. Героїв Оборони, 15, м. Київ, 03041.
Свідоцтво суб'єкта видавничої справи
ДК № 4097 від 17.06.2011