Київський Університет імені Тараса Шевченка
Механіко-математичний факультет

Юрій Дрозд

Основи математичної логіки

Київ 2003

Передмова

Даний підручник створено за матеріалами курсу математичної логіки, який викладається в Київському університеті імені Тараса Шевченка. Цей курс відіграє значну роль у формуванні математичного мислення та розумінні будови математики як науки. Тому до книги увійшли, перш за все, принципові результати, які стосуються співвідношення семантики та синтаксису, або змісту та форми: теорема Ґеделя про адекватність (повноту) числення відношень та теореми Ґеделя і Тарського про неповноту формальної арифметики. Останні ґрунтуються на теорії рекурсивних функцій, яку також викладено достатньо детально й повно. Інші підрозділи стосуються таких класичних і важливих речей, як пренексні та сколемівські нормальні форми в логіці відношень, теорема Левенгайма – Сколема, існування нестандартних моделей тощо. Окремий підрозділ знайомить читача з поняттями інтуїціоністської логіки (в її формальному варіанті) та її співвідношенням із класичною. Це корисно для загального розвитку студентів; крім того, на цьому матеріалі вони можуть добре потренуватися в техніці виводів.

Невеликий обсяг курсу не дозволяє включити до нього ряду інших результатів. Деякі з них, такі як теорема Поста про повні множини булевих функцій чи будова булевих алгебр, природно входять до інших курсів — дискретної математики, загальної алгебри тощо. Оскільки далеко не завжди вони в цих курсах достатньо висвітлюються, у підручник увійшов відповідний матеріал, але переважно у вигляді вправ (додатки A та B до першого розділу книги). Цього цілком достатньо для того, щоб студент міг самостійно опанувати ці результати. Дуже важливими є результати про рівносильність різних означень конструктивності (обчислюваності), але більш-менш детальний їх розгляд вимагає занадто багато часу, тому у підручнику наведено лише відповідні коментарі. Для ширшого ознайомлення з цими питаннями див. [**Мен**, главу 5], [**Ман**] або [**Мал1**].

З іншого боку, формальна теорія множин не є природною частиною загального курсу математичної логіки. Ця теорія, хоч би якою значною вона не видавалася фахівцям, зараз явно відійшла на узбіччя математичної науки. Результати Ґеделя та Коена про незалежність гіпотези континууму є видатним досягненням формальної логіки, але вони є надто спеціальними і складними для початківця, а викладання основ формальної теорії множин не є дуже повчальним і його цілком можна віднести до факультативів, розрахованих лише на студентів, які особливо зацікавлені в цій тематиці. Класичною монографією з цих питань є книга самого Коена [**Ко**]. У книзі також зовсім не йдеться про застосування до математичної логіки методів абстрактної алгебри, хоча цей напрям

є дуже плідним. Причиною й тут є брак місця. Для ознайомлення з цією тематикою див. [**РС**], а відносно застосування логіки в інших математичних науках — [**Мал2, Роб, Дев**].

Жодну математичну науку неможливо вивчити, лише ознайомившись з її основними положеннями. Неодмінним є розв'язання достатньої кількості задач, від найлегших вправ до самостійного опанування досить складними фрагментами теорії. Тому до книги увійшла велика кількість задач. Читачу конче рекомендовано не пропускати їх вже при першому читанні! До складніших з них наведено деякі натяки, що мають допомогти при їх розв'язанні.

Публікація цієї книги є важливою ще й тому, що зараз дуже бракує підручників з математичної логіки. Класичні книги [**Нов, Мен, Кл1, Кл2**] видано давно, і зараз вони є навіть не в усіх університетських бібліотеках, принаймні в достатній кількості. Книга [**ЕП**] взагалі не рекомендується початківцю. А українською мовою аналогічних підручників зовсім немає. Ця книга, з одного боку, є доступною для студента-математика, який має хоч деякий (навіть невеличкий) досвід у вивченні математичних теорій, а з іншого боку, більш досвідченому читачу вона допоможе підготуватися до роботи з більш ґрунтовними підручниками та монографіями, а також сучасною журнальною літературою з математичної логіки.

Зміст

Вступ
Синтаксис і семантика логічних теорій

Математична, або формальна, логіка — це наука, яка вивчає логічні питання математичними методами. Взагалі, логіка — це наука про правила міркувань, у першу чергу — доведень та спростувань. Як окремий розділ науки вона виникла ще у стародавній Греції. Найбільш відомою працею того часу є «Органон» Аристотеля (IV ст. до Р.Х.), де, зокрема, явно сформульовано й досліджено кілька основних формальних законів логіки. Типовим прикладом логічно правильного міркування, згідно з одним з аристотелівських правил, є такий:

Усі студенти знають логіку.

Петро — студент.

Отже, Петро знає логіку.

При цьому з погляду «чистої» логіки зовсім неважливо, чи дійсно всі студенти знають логіку і чи дійсно Петро, про якого йдеться, є студентом. Суть «логічності» цього міркування полягає в тому, що коли всі його *засновки* (у нашому прикладі — перші два речення) істині, то істиним є й його *висновок* (останнє речення). Навпаки, таке міркування:

Усі студенти знають логіку.

Петро — не студент.

Отже, Петро не знає логіки,

не є логічно правильним (навіть якщо Петро дійсно не знає логіки), тому що *можливим* є випадок, коли засновки є істинними, але висновок — хибним. Таким чином, логічність якогось міркування залежить не від того, чи є істиними або хибними його складові частини, а цілковито від *форми* міркування. В ідеалі задача логіки — описати всі правильні форми міркувань. З цього погляду будь- яка логіка є формальною. Тому вживання слів «формальна логіка» як синоніма «математичної логіки» не зовсім правомірне. Його може виправдати те, що саме при математичному підході до логіки її формальна суть виявляється повністю. Від початку існування математичної логіки її метою було знайти спосіб «механічної», або, як частіше кажуть зараз, «алгоритмічної» побудови всіх правильних форм міркувань. Цю програму висунув у XVII ст. Ляйбніц. Його метою було створення «універсального числення», яке б дозволило розсіяти будь-який сумнів у правомірності того чи іншого судження за допомогою деякого обчислення, на зразок того, як правила арифметики та алгебри дозволяють перевірити істиність розв'язання якоїсь математичної задачі. У часи, коли ідеї Декарта про математизацію науки й алгебризацію математики набували все більшого визнання, таку мету не можна було вважати надто амбіційною. Втім, фактично дослідження

в цьому напряму розпочалися лише у XIX ст., і лише у XX ст. їх було сформульовано як реальну математичну проблему.

Спробуємо дати деяке уявлення про цю проблему, яку можна було б назвати «програмою Ляйбніца» або «Ляйбніца–Гільберта», віддаючи належне математику, який зробив чи не найбільший внесок у її формування та перші кроки до її реалізації. Кожна формально-логічна теорія складається з двох частин: *синтаксису* та *семантики*. Синтаксис визначає правила побудови речень, які розглядає ця теорія, а семантика — як ці речення приймають значення (найчастіше — «істиний» та «хибний») залежно від значень своїх «елементарних частин». Значення елементарних речень визначаються «зовнішніми факторами»; останні найчастіше звуться «інтерпретаціями» теорії, або її «моделями». Зазвичай синтаксис є порівняно простою частиною теорії; важливою вимогою до нього вважається *ефективність*. Саме, вимагається, щоб:

(1) правила синтаксису дозволяли породжувати всі допустимі речення за допомогою деякого алгоритму (тобто чисто механічної процедури);
(2) ці правила також надавали алгоритм перевірки, чи є та або інша послідовність літер допустимим реченням.

З іншого боку, семантика може бути досить складною (якою вона і є в більшості «реальних» людських мов). Вона часто (можна навіть сказати, майже завжди) буває пов'язана з розглядом нескінченних множин та їх відображень. Ясно, що в останньому випадку самі семантичні правила аж ніяк не можуть бути алгоритмічними. Тому, починаючи з Ляйбніца, «мрією логіка» є *зведення семантики до синтаксису*. Інакше кажучи, висувається завдання створити таку *синтаксичну* систему, яка б породжувала всі *семантично* істині речення (і тільки їх). Оскільки множина істиних речень у будь-якій змістовній теорії є нескінченною, то ми маємо фактично дві задачі (назвемо їх «задачами Ляйбніца»):

[L1] Побудувати алгоритм, який би породжував усі істині речення. Цей алгоритм повинен видавати в процесі своєї роботи істині речення, причому кожне істине речення має з'явитися на якомусь кроці роботи цього алгоритму. Такий алгоритм здебільшого зветься *логічним численням*.

[L2] Побудувати алгоритм, який би за кожним даним реченням визначав, чи є воно істиним.

Зауважимо, що розв'язання другої задачі дає також розв'язання першої. Дійсно, якщо ми вміємо продукувати *всі* речення (це забезпечується вимогою (2) до синтаксису логічної теорії) і для кожного речення вміємо вирішувати, чи є воно істиним, то ми можемо просто продукувати всі речення, визначати для кожного нового речення, чи воно істине, і якщо так, то уводити його до реєстру істиних речень. Навпаки, розв'язання першої задачі Ляйбніца ще не дає розв'язання другої. Дійсно, навіть

якщо ми маємо алгоритм, який продукує всі істині речення, ми, взагалі кажучи, не знаємо, на якому кроці слід чекати появи того речення, істиність якого ми хочемо перевірити. Тому в кожний момент часу може залишатися невідомим, чи дане речення взагалі не є істиним, чи ми просто його ще не дочекалися. Отже, ми дійсно маємо дві задачі різних рівнів складності.

У цьому підручнику ми розглянемо деякі основні формально-логічні теорії, вивчимо їх властивості і, зокрема, дослідимо для них задачі Ляйбніца. Для першої з цих теорій — *логіки висловлювань* — обидві задачі є зовсім простими. Оскільки тут семантика має справу лише зі скінченними процедурами, то вона сама дає розв'язання задачі [L2]. Втім, на прикладі цієї теорії можна порівняно легко засвоїти деякі загальні методи, тому ми її розглядаємо аж занадто ретельно. Другий розділ — *логіка відношень* (або *логіка предикатів*) — вже є набагато складнішим, оскільки його семантика потребує розгляду нескінченних сукупностей. Тому тут обидві задачі Ляйбніца стають нетривіальними. Насправді, ми побудуємо *числення відношень*, яке розв'язує першу задачу Ляйбніца (у цьому полягає так звана теорема Ґеделя про повноту). А ось розв'язання другої задачі Ляйбніца для логіки відношень виявляється вже неможливим (у цьому полягає теорема Черча про нерозв'язність). Отже, навіть для цієї порівняно простої логічної теорії (яка, до речі, входить як складова частина практично до всіх інших логічних теорій) програма Ляйбніца–Гільберта виявилась невиконливою. Крім того, сама теорема Ґеделя про повноту, а також тісно пов'язані з нею теорема компактності та теорема Левенгайма–Сколема мають дещо несподівані наслідки (наприклад, існування *нестандартних моделей* більшості математичних теорій), які показують, що «чиста логіка» не може дати повністю адекватного опису конкретних математичних структур.

Нарешті, ми розглянемо одну з найпростіших *логіко-математичних* теорій, в якій робиться спроба звести змістовну математичну теорію до формально-логічної. Це — *формальна арифметика*. Ми побачимо, що тут уже обидві задачі Ляйбніца стають нерозв'язними. Ми не лише не можемо суто формальним, алгоритмічним способом вирішити, чи є задане речення істиним, чи ні. Більше: яке б числення, що продукує істині речення (і лише їх), ми не сконструювали, завжди залишаться істині арифметичні твердження, які цим алгоритмом ніколи не будуть видані. У цьому полягає зміст теореми Ґеделя про неповноту та теореми Тарського про неалгоритмічність поняття істини в арифметиці.

З цього випливає важливий висновок. Уже така найпростіша наука, як математика (або навіть арифметика), не може бути зведена до чисто формальних процедур, які можна було б довірити, скажімо, сучасному комп'ютеру. Її розвиток завжди буде *динамічним* або *творчим* у тому розумінні, що кожна нова задача може вимагати принципово нових методів доведення, які неможливо передбачити наперед. Звичайно, цей

висновок є істотним для філософії науки. Однак він має й суто «практичне» значення для фахівців-математиків. Вони можуть бути спокійними за своє майбутнє. Доки існує математика як наука, потрібним є й існування математиків — людей, які могли б її творчо розвивати.

Мимоволі згадується цікавий випадок з перекладом російською мовою статті Н. Бурбакі «Архітектура математики» (див. [**Бу**]), де французьке речення «substituer les idées au calcul» («замінити обчислення ідеями», або, дослівно, «підставити ідеї на місце обчислень») було необачно перекладено «заменить идеи вычислениями» (йшлося про те, чого прагнуть математики). Насправді математики у своїй творчій діяльності вирішують обидві ці задачі. Вони, звичайно, намагаються знайти справжнє підґрунтя найважливішим результатам з тим, щоб їхні доведення залежали не від майстерної еквілібристики формулами, а від правильного розуміння основних засад відповідного розділу науки. Проте одночасно вони створюють математичну техніку, яка дозволяє перетворити багато фактів, відкриття яких колись вимагало геніальних прозирань, у рутинні вправи, які зараз під силу пересічному студенту (і навіть пересічному комп'ютеру). Теореми про неповноту гарантують, що скільки б не відбувався другий процес, він ніколи не зведе нанівець усю математику. З кожним новим досягненням виникатимуть нові задачі, які потребуватимуть нових ідей.

Розділ 1

Логіка висловлювань

1.1. Висловлювання та дії над ними

Поняття «висловлювання» в логіці зазвичай означає деяке твердження, яке може бути *істиним* або *хибним*. Кажуть, що 'істине' або 'хибне' — це *значення* висловлювання. При цьому формальна логіка висловлювань не бере до уваги зміст цих тверджень і не ставить питань, яким чином висловлювання набуває значення, тобто чому дане висловлювання є істиним чи хибним. Останнє питання мають вирішувати «конкретні» науки, які лежать поза межами логіки висловлювань. Ось приклади висловлювань:

1. $2 \times 2 = 4$.
2. Київ — столиця України.
3. Одеса — столиця Туреччини.
4. Добуток матриць комутативний.

З арифметики відомо, що висловлювання 1 є істиним. З елементарної лінійної алгебри відомо, що висловлювання 4 — хибне. З географії відомо, що твердження 2 є істиним, а твердження 3 — хибним. Втім, останні відомості, взагалі кажучи, не є сталими. Скажімо, у 20-і роки XX ст. твердження 2 було хибним (столицею України був Харків). Але повторимо, що логіку висловлювань ці питання не цікавлять.

Натомість, логіка висловлювань вивчає способи, за якими з одних висовлювань можна утворювати інші, причому так, щоб істиність або хибність нових висловлювань залежала лише від істиності або хибності старих. Для цього використовуються так звані (логічні) *сполучники*.

Означення 1.1.1. *n-місним (логічним) сполучником* зветься операція C, яка за довільними n висловлюваннями $A_1, A_2, \ldots, A_n$ утворює нове висловлювання $\mathsf{C}A_1A_2\ldots A_n$ у такий спосіб, що коли про кожне висловлювання $A_1, A_2, \ldots, A_n$ відомо, яким воно є (істиним чи хибним), то й про висловлювання $\mathsf{C}A_1A_2\ldots A_n$ також відомо, чи воно є істиним, чи хибним.

Оскільки ми абстрагуємося від того, як саме висловлювання набуває значення, то можна вважати, що сполучник — це просто функція, аргументи й значення якої належать двоелементній множині $\mathbf{B} = \{\,\text{істине}, \text{хибне}\,\}$. Множину $\mathbf{B}$ часто звуть множиною *булевих* (або *логічних*) значень. Тому сполучники звуть також *булевими функціями*.

Для скорочення записів звичайно замість 'істине' та 'хибне' пишуть, відповідно, $\mathbf{0}$ та $\mathbf{1}$, тобто вважають, що $\mathbf{B} = \{\,\mathbf{0}, \mathbf{1}\,\}$. Втім, часто логічні сполучники виражають словами деякої мови (тієї, якою пишуть або викладають, тобто в нашому випадку — української), і ми будемо так

робити. Важливо при цьому не забувати, що відповідні слова відіграють не зовсім ту роль, яка відводиться їм у звичайній мові. Саме, вони зберігають лише деякі формальні якості й втрачають те, що відповідає за *зміст* речення. Ми скоро побачимо це на досить цікавому прикладі.

Легко бачити, що всього існує 2^n різних n-місних логічних сполучників. Звичайно, не всі вони відіграють у логіці рівнозначну роль. Найбільш вживаними є такі бінарні (двомісні) сполучники:

1. *Кон'юнкція* двох висловлювань A та B. Її позначають $A \wedge B$ або $A\&B$ і виражають сполучником 'і'. Наведена нижче таблиця показує, яких значень набуває висловлювання $A \wedge B$ при заданих значеннях висловлювань A та B:

A	B	$A \wedge B$
0	**0**	**0**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**

   Отже, висловлювання «A і B» вважається істиним тоді й лише тоді, коли такими є й A й B; інакше воно вважається хибним. Це більш-менш відповідає навіть змісту, який зазвичай вкладається у сполучник 'і'.
2. *Диз'юнкція* двох висловлювань A та B. Її позначають $A \vee B$ і виражають сполучником 'або'. Наведена нижче таблиця показує, яких значень набуває висловлювання $A \vee B$ при заданих значеннях висловлювань A та B:

A	B	$A \vee B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**1**

   Отже, висловлювання «A або B» вважається істиним тоді й лише тоді, коли таким є принаймні одне з висловлювань A чи B; інакше воно вважається хибним. Це також більш-менш відповідає змісту, який зазвичай вкладається у сполучник 'або'.
3. *Імплікація* двох висловлювань A та B. Її позначають $A \Rightarrow B$ або $A \supset B$ і виражають сполучником 'якщо ..., то ...' Наведена нижче таблиця показує, яких значень набуває висловлювання $A \Rightarrow B$

при заданих значеннях висловлювань A та B:

A	B	$A \Rightarrow B$
0	**0**	**1**
0	**1**	**1**
1	**0**	**0**
1	**1**	**1**

Отже, висловлювання «якщо A, то B» є хибним лише у випадку, коли A істине, а B хибне; інакше воно вважається істиним. Тобто з хибного висловлювання випливає будь-що, а з істиного — будь-яке істине, але з істиного не може випливати хибне. Наприклад, висловлювання «Якщо $2 \times 2 = 4$, то Київ — столиця України» та «Якщо Харків — столиця України, то $2 \times 2 = 4$» є істинними, а висловлювання «Якщо Київ — столиця України, то множення матриць комутативне» — хибне. Навряд чи це цілком відповідає звичайному тлумаченню речень типу «Якщо A, то B» у повсякденній мові. Однак, коли мати на увазі, що в логіці висловлювань ми не маємо права розбирати, чи пов'язані *за змістом* речення A та B, а мусимо брати до уваги лише їхні логічні значення, то легко зрозуміти, що іншого варіанта означення цього сполучника немає. Дійсно, те, що з хибного твердження випливає все, що завгодно, ми постійно використовуємо в математиці (і не тільки) при доведеннях «від супротивного». З іншого боку, те, що з істиного твердження виводиться істине, мабуть теж важко заперечити, так само як і те, що з істиного твердження не може випливати хибне. Надалі ми користуватимемося імплікацією саме в цьому розумінні.

4. *Еквіваленція* двох висловлювань A та B. Її позначають $A \Leftrightarrow B$ і виражають словами 'якщо ..., то ... і навпаки'. Наведена нижче таблиця показує, яких значень набуває висловлювання $A \Leftrightarrow B$ при заданих значеннях A та B:

A	B	$A \Leftrightarrow B$
0	**0**	**1**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**

Отже, висловлювання «Якщо A, то B і навпаки» є істиним, якщо A та B мають однакові логічні значення, і хибним у протилежному випадку. Так само, як і для імплікації, це не зовсім відповідає звичайному застосуванню таких виразів, але й у даному випадку це — єдина можливість, яка залишається, якщо не зважати на зміст висловлювань.

Крім них, важливу роль відіграє унарний (одномісний) сполучник, який зветься *запереченням* і позначається ¬ або словом ‘не’. Він задається таблицею значень:

A	$\neg A$
0	**1**
1	**0**

За допомогою цих сполучників можна будувати складні речення на зразок

$$((A \vee B) \Rightarrow ((\neg B) \wedge (C \Leftrightarrow A))) \Rightarrow ((\neg C) \vee B).$$

Дужки, як завжди, вказують порядок дій. Часто, як і в арифметиці, приймають деякі правила, які зменшують кількість дужок. Надалі ми вважатимемо, що перш за все застосовується заперечення, потім кон'юнкція та диз'юнкція (у порядку, визначеному дужками), в останню чергу — імплікація та еквіваленція. Беручи до уваги цю угоду, останнє висловлювання можна скорочено записати в такий спосіб:

$$(A \vee B \Rightarrow \neg B \wedge (C \Leftrightarrow A)) \Rightarrow \neg C \vee B.$$

1.2. Синтаксис та семантика логіки висловлювань

У попередньому розділі поняття логічного висловлювання не було достатньо формалізовано. Тому до нього неможливо застосувати математичні методи. Зараз ми дамо його точне означення, а також визначимо правила, за якими такі висловлювання приймають (логічні) значення.

Означення 1.2.1. 1. *Алфавіт* $\mathfrak{A}_0$ логіки висловлювань складається з таких 8 символів:

$$A,\ |,\ (,\ ),\ \neg,\ \vee,\ \wedge,\ \Rightarrow .$$

2. *Атомом* або *елементарним висловлюванням* зветься слово в даному алфавіті, побудоване за такими правилами:
   (a) слово, яке складається з однієї літери A, є атомом;
   (b) якщо слово W є атомом, то й слово $W|$ також є атомом;
   (c) інших атомів, крім таких, які можуть бути побудовані за правилами (a) і (b), не існує.

3. *Реченням* зветься слово в даному алфавіті, побудоване за такими правилами:
   (a) кожен атом є реченням;
   (b) якщо слово W є реченням, то й слово $\neg W$ є реченням;
   (c) якщо слова W та V є реченнями, то й слова $(W \Rightarrow V)$, $(W \vee V)$, $(W \wedge V)$ також є реченнями;
   (d) інших речень, крім таких, які можуть бути побудовані за правилами (a), (b) і (c), не існує.

Зауваження 1.2.2. Неважко переконатися, що наведене означення є *ефективним*, тобто дозволяє побудувати алгоритм перевірки того, чи є дане слово в алфавіті $\mathfrak{A}_0$ атомом або реченням. Для атомів це зовсім очевидно: довільний атом має вигляд $A||\ldots|$ (довільна кількість $|$). Для речень це трохи складніше. Ось варіант рекурсивного алгоритму для перевірки того, чи є задане слово W реченням.

1. Перевірити, чи містить W підслово вигляду $\neg x$, де x — літера, відмінна від A та $($. Якщо так, W не є реченням. Якщо ні, відкинути всі літери $\neg$. Слово, яке залишилось, позначимо через W'.
2. Перевірити, чи є W' атомом. Якщо так, W є реченням. Якщо ні, йти далі.

3. Перевірити, чи є (першою, а) останньою літерами W'. Якщо ні, W не є реченням. Якщо так, відкинути ці дужки, одержавши слово $W^* = a_1 a_2 \dots a_m$, і йти далі.
4. Якщо $W^* = A|| \dots |aW_1$, де $a \in \{\vee, \wedge, \Rightarrow\}$, то W є реченням тоді й лише тоді, коли W_1 є реченням. Якщо ні, йти далі.
5. Якщо $a_1 \neq (\,$, W не є реченням. Якщо $a_1 = (\,$, йти далі.
6. Обчислити функцію $s(k)$ $(1 \leqslant k < m-1)$ за правилом:

$$s(1) = 1,$$
$$s(k+1) = \begin{cases} s(k)+1, & \text{якщо } a_{k+1} = (, \\ s(k)-1, & \text{якщо } a_{k+1} =), \\ s(k) & \text{інакше.} \end{cases}$$

   Якщо $s(k) \neq 0$ при $1 < k < m-1$, слово W не є реченням. Інакше знайти найменше значення k, для якого $s(k) = 0$ і йти далі.
7. Перевірити, чи виконані всі такі умови:
   (a) слово $W_1 = a_1 a_2 \dots a_k$ є реченням;
   (b) $a_{k+1} \in \{\vee, \wedge, \Rightarrow\}$;
   (c) слово $W_2 = a_{k+2} \dots a_m$ є реченням.

   Якщо так, W є реченням, якщо ні, воно не є реченням.

Читачу залишається обґрунтування цього алгоритму, а також широкі можливості вдосконалити його або запропонувати свій.

Зауваження 1.2.3. Ми обрали варіант формалізації, який користується *скінченним* алфавітом. Інколи це зручно, але на практиці звичайно користуються спрощеними позначеннями. Перш за все, ми будемо дотримуватись тієї ж домовленості про «порядок дій», що й у попередньому підрозділі. Крім того, ми завжди опускатимемо зовнішні дужки, тобто ті, які виникли при останньому застосуванні правила 2(c) з означення 1.2.1. Нарешті, атом $A|| \dots |$ (з n символами $|$) ми часто позначатимемо A_n (зокрема, A_0 позначає A). Наприклад, скорочений запис

$$(A_2 \Rightarrow A_3 \vee (A_0 \Rightarrow \neg A_2)) \wedge \neg(A_1 \vee \neg A_0 \Rightarrow \neg A_2)$$

насправді позначає «справжнє» речення

$$((A|| \Rightarrow (A||| \vee (A \Rightarrow \neg A|))) \wedge \neg((A| \vee \neg A) \Rightarrow \neg A||)).$$

Досі ми розглядали *синтаксис* логіки висловлювань. Переходимо до *семантики*, тобто визначимо, в який спосіб речення набувають *логічних значень* залежно від логічних значень атомів, які до них входять. Наведене нижче означення є просто формалізацією означення логічних сполучників з попереднього підрозділу. Надалі множину атомів позначатимемо $\mathfrak{E}$. Речення, як правило, ми позначатимемо жирними літерами $\mathbf{A}, \mathbf{B}$ тощо.

Означення 1.2.4.

1. *Інтерпретацією* (в логіці висловлювань) зветься функція $\mathcal{I} : \mathfrak{E} \to \mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$.
2. Для кожної інтерпретації $\mathcal{I}$ та довільного речення $\mathbf{A}$ визначимо *значення речення* $\mathbf{A}$ *в інтерпретації* $\mathcal{I}$, яке позначається $\mathrm{val}(\mathcal{I}, \mathbf{A})$ у такий спосіб:

(a) Якщо $\mathbf{A}$ — атом, то $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathcal{I}(\mathbf{A})$.
(b) Якщо $\mathbf{A} = \neg\mathbf{B}$, то

$$\mathrm{val}(\mathcal{I}, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}, \\ \mathbf{1}, & \text{якщо } \mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{0}. \end{cases}$$

(c) Якщо $\mathbf{A} = (\mathbf{B} \vee \mathbf{C})$, то

$$\mathrm{val}(\mathcal{I}, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathrm{val}(\mathcal{I}, \mathbf{C}) = \mathbf{0}, \\ \mathbf{1}, & \text{інакше.} \end{cases}$$

(d) Якщо $\mathbf{A} = (\mathbf{B} \wedge \mathbf{C})$, то

$$\mathrm{val}(\mathcal{I}, \mathbf{A}) = \begin{cases} \mathbf{1}, & \text{якщо } \mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathrm{val}(\mathcal{I}, \mathbf{C}) = \mathbf{1}, \\ \mathbf{0}, & \text{інакше.} \end{cases}$$

(e) Якщо $\mathbf{A} = (\mathbf{B} \Rightarrow \mathbf{C})$, то

$$\mathrm{val}(\mathcal{I}, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}, \text{ а } \mathrm{val}(\mathcal{I}, \mathbf{C}) = \mathbf{0}, \\ \mathbf{1}, & \text{інакше.} \end{cases}$$

Очевидно, цими правилами однозначно визначається значення $\mathrm{val}(\mathcal{I}, \mathbf{A})$ для довільної інтерпретації $\mathcal{I}$ і довільного речення $\mathbf{A}$.

Найбільш важливим у логіці є питання, які речення є *логічними наслідками* одне одного, зокрема, які речення завжди є істинними, незалежно від значень їхніх складових частин. У логіці висловлювань відповідне означення виглядає так.

Означення 1.2.5.

1. Нехай $\mathfrak{M}$ — якась множина речень. Кажуть, що речення $\mathbf{A}$ є *логічним наслідком* множини речень $\mathfrak{M}$, і пишуть $\mathfrak{M} \models \mathfrak{A}$, якщо $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ у довільній інтерпретації $\mathcal{I}$, такій що $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$ для кожного речення $\mathbf{B} \in \mathfrak{M}$.
2. Якщо множина $\mathfrak{M}$ порожня, логічні наслідки з $\mathfrak{M}$, тобто речення $\mathbf{A}$, такі що $\models \mathfrak{A}$, звуться *тавтологіями*. Отже, тавтологія — це речення, яке приймає значення $\mathbf{1}$ у всіх інтерпретаціях.
3. Множина речень $\mathfrak{M}$ зветься *логічно несумісною*, якщо не існує такої інтерпретації $\mathcal{I}$, в якій $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ для всіх речень $\mathbf{A} \in \mathfrak{M}$. (Тоді, згідно з означенням, $\mathfrak{M} \models \mathbf{B}$ для будь-якого речення $\mathbf{B}$.)

Вправа 1.2.6 дає кілька прикладів тавтологій. Ці приклади відіграватимуть важливу роль у наступних підрозділах.

Вправа 1.2.6. Доведіть, що для довільних речень $\mathbf{A}, \mathbf{B}, \mathbf{C}$ такі речення є тавтологіями:

(A1) $\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A})$,

(A2) $(\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}))$,

(A3) $\mathbf{A} \Rightarrow (\mathbf{A} \vee \mathbf{B})$,

(A4) $\mathbf{B} \Rightarrow (\mathbf{A} \vee \mathbf{B})$,

(A5) $(\mathbf{A} \Rightarrow \mathbf{C}) \Rightarrow ((\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \vee \mathbf{B} \Rightarrow \mathbf{C}))$,

(A6) $\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{A}$,

(A7) $\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B}$,

(A8) $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B} \wedge \mathbf{C}))$,

(A9) $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{A} \Rightarrow \neg\mathbf{B}) \Rightarrow \neg\mathbf{A})$,

(A10) $\neg\neg\mathbf{A} \Rightarrow \mathbf{A}$.

Поняття логічного наслідку в логіці висловлювань має кілька простих, але важливих властивостей.

Твердження 1.2.7.

1. *Якщо* $\mathfrak{M} \models \mathbf{A} \Rightarrow \mathbf{B}$ *і* $\mathfrak{M} \models \mathbf{A}$, *то* $\mathfrak{M} \models \mathbf{B}$.
2. *Якщо* $\mathfrak{M} \models \mathbf{A}$ *і* $\mathfrak{N} \models \mathbf{B}$ *для кожного речення* $\mathbf{B} \in \mathfrak{M}$, *то* $\mathfrak{N} \models \mathbf{A}$.
3. *Для довільного речення* $\mathbf{A}$, $\models \mathbf{A} \vee \neg\mathbf{A}$. (Закон виключення третього.)
4. *Множина речень* $\mathfrak{M}$ *несумісна тоді й лише тоді, коли існує таке речення* $\mathbf{A}$, *що одночасно* $\mathfrak{M} \models \mathbf{A}$ *і* $\mathfrak{M} \models \neg\mathbf{A}$.

Доведення. 1. Нехай $\mathcal{I}$ — довільний розподіл, в якому $\mathrm{val}(\mathcal{I}, \mathbf{C}) = \mathbf{1}$ для всіх речень $\mathbf{C} \in \mathfrak{N}$. Тоді $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ і $\mathrm{val}(\mathcal{I}, \mathbf{A} \Rightarrow \mathbf{B}) = \mathbf{1}$. З означення 1.2.4 (2e) випливає, що тоді й $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$.

2. Очевидно.

3. Безпосередньо випливає з означення 1.2.4 (2b,c).

4. Очевидно. □

Надалі в цьому розділі ми розглядатимемо лише скінченні множини речень $\mathfrak{M}$. У цьому випадку досить легко перевірити, чи $\mathfrak{M} \models \mathbf{A}$ для заданого речення $\mathbf{A}$. Для цього достатньо виписати всі можливі значення довільної інтерпретації $\mathcal{I}$ на тих атомах, які входять до речень з множини $\mathfrak{M} \cup \{\, \mathbf{A} \,\}$ (їх лише скінченна кількість), вибрати з них ті, для яких $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$ для всіх $\mathbf{B} \in \mathfrak{M}$, і подивитись, чи буде $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ у всіх цих інтерпретаціях. Зокрема, легко перевірити, чи є задане речення тавтологією. Отже, семантика логіки висловлювань дуже проста. Тим не менш, ми збираємося виконати для логіки висловлювань програму «заміни семантики синтаксисом», проголошену у вступі. Це корисно як полегшений варіант того, що ми розглядатимемо в наступних розділах, на якому можна прослідкувати основні риси такої «вторинної формалізації».

1.3. Аксіоматика логіки висловлювань

Нагадаємо, що, згідно із загальним підходом, *логічне числення* базується на *аксіомах* та *правилах виводу*. Для *числення висловлювань* вони мають такий вигляд.

Означення 1.3.1.

1. *Аксіомами* числення висловлювань звуться всі речення вигляду (A1–A10) із вправи 1.2.6, де $\mathbf{A}, \mathbf{B}, \mathbf{C}$ — довільні речення.
2. Єдиним *правилом виводу* числення висловлювань є правило modus ponens, яке виражається схемою
$$\frac{\mathbf{A} \Rightarrow \mathbf{B},\ \mathbf{A}}{\mathbf{B}},$$
де $\mathbf{A}$, $\mathbf{B}$ — довільні речення.

На цьому означенні базується поняття *виводу* в численні висловлювань.

Означення 1.3.2. Послідовність речень $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ зветься *виводом* речення $\mathbf{A}$ з множини речень $\mathfrak{M}$, якщо $\mathbf{A} = \mathbf{A}_n$ і для кожного номера $i = 1, 2, \ldots, n$ виконується одна з наведених нижче можливостей:

1. $\mathbf{A}_i$ є аксіомою.
2. $\mathbf{A}_i \in \mathfrak{M}$.
3. Існують номери $j < i$ та $k < i$ такі, що $\mathbf{A}_j = \mathbf{A}_k \Rightarrow \mathbf{A}_i$. (У цьому випадку кажуть, що $\mathbf{A}_i$ *одержане за правилом* modus ponens з $\mathbf{A}_j$ та $\mathbf{A}_k$.)

Якщо такий вивід існує, кажуть, що $\mathbf{A}$ є *формальним наслідком* із множини $\mathfrak{M}$, і пишуть $\mathfrak{M} \vdash \mathbf{A}$. Зокрема, якщо $\vdash \mathbf{A}$ (тобто існує вивід $\mathbf{A}$ з порожньої множини), кажуть, що $\mathbf{A}$ є *теоремою* числення висловлювань.

Зауваження 1.3.3. Можна переконатися, що дане означення виводу також є *ефективним*. Ми залишаємо читачу побудову відповідного алгоритму. З іншого боку, зовсім не ясно, чи є ефективним, скажімо, поняття теореми. Дійсно, у виводі коротші речення можуть з'являтися після довших (завдяки правилу modus ponens). Тому безпосереднього рекурсивного алгоритму не існує. Насправді, деякий алгоритм випливає з тверджень про коректність та адекватність, які ми розглянемо нижче, але це пов'язано з простотою логіки висловлювань.

Наступне твердження показує, що наша формалізація логіки висловлювань є *коректною*.

Твердження 1.3.4 (Коректність числення висловлювань). *Якщо* $\mathfrak{M} \vdash \mathbf{A}$, *то* $\mathfrak{M} \models \mathbf{A}$. *Зокрема, кожна теорема є тавтологією.*

Доведення. Це безпосередньо випливає із вправи 1.2.6 та твердження 1.2.7 (1). □

Наша головна мета — довести обернене твердження, яке показує, що наша формалізація є *адекватною*.

Теорема 1.3.5 (Адекватність числення висловлювань). *Якщо* $\mathfrak{M} \models \mathbf{A}$, *то* $\mathfrak{M} \vdash \mathbf{A}$. *Зокрема, кожна тавтологія є теоремою.*

Проте доведення цієї теореми значно складніше, і ми виконаємо його лише в підрозділі 1.5. Зараз ми наведемо два приклади виводів, перший з яких буде використано надалі.

Приклад 1.3.6.

1. Покажемо, що $\vdash \mathbf{A} \Rightarrow \mathbf{A}$ для довільного речення $\mathbf{A}$. Дійсно, наступна послідовність речень є виводом $\mathbf{A} \Rightarrow \mathbf{A}$ з порожньої множини:

(i) $\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A})$,

(ii) $\mathbf{A} \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \mathbf{A})$,

(iii) $(\mathbf{A} \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \mathbf{A})) \Rightarrow ((\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A}))$,

(iv) $(\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A})) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{A})$,

(v) $\mathbf{A} \Rightarrow \mathbf{A}$.

(Номери не входять до складу цієї послідовності; вони приписані для посилань у подальших поясненнях.) А саме: речення (i) є аксіомою вигляду (A1) (при $\mathbf{A} = \mathbf{B}$). Речення (ii) — також аксіома вигляду (A1) (при $\mathbf{B} = \mathbf{A} \Rightarrow \mathbf{A}$). Речення (iii) — це аксіома вигляду (A2) (при $\mathbf{B} = \mathbf{A} \Rightarrow \mathbf{A}$ і $\mathbf{C} = \mathbf{A}$). Речення (iv) одержане з речень (iii) і (ii) за правилом modus ponens, а речення (v) одержане за тим самим правилом з речень (v) і (i).

2. $\vdash \mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B} \wedge \mathbf{A}$ для довільного речення $\mathbf{A}$. Наведемо відповідний вивід:

$$\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{A},\ \mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B},$$
$$(\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow (\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B} \wedge \mathbf{A})),$$
$$(\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow (\mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B} \wedge \mathbf{A}),\ \mathbf{A} \wedge \mathbf{B} \Rightarrow \mathbf{B} \wedge \mathbf{A}.$$

Тут ми не даємо пояснень, залишаючи їх читачу.

3. Множина речень $\mathfrak{M}$ зветься *суперечливою*, якщо існує таке речення $\mathbf{A}$, що одночасно $\mathfrak{M} \vdash \mathbf{A}$ й $\mathfrak{M} \vdash \neg\mathbf{A}$. Покажемо, що тоді $\mathfrak{M} \vdash \mathbf{B}$ для будь-якого речення $\mathbf{B}$. Дійсно, випишемо вивід $\mathbf{A}$ з $\mathfrak{M}$, припишемо до нього вивід $\neg\mathbf{A}$ з $\mathfrak{M}$, а потім такі речення:

$$\mathbf{A} \Rightarrow (\neg\mathbf{B} \Rightarrow \mathbf{A}),\ \neg\mathbf{B} \Rightarrow \mathbf{A},\ \neg\mathbf{A} \Rightarrow (\neg\mathbf{B} \Rightarrow \neg\mathbf{A}),\ \neg\mathbf{B} \Rightarrow \neg\mathbf{A},$$
$$(\neg\mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow ((\neg\mathbf{B} \Rightarrow \neg\mathbf{A}) \Rightarrow \neg\neg\mathbf{B}),\ (\neg\mathbf{B} \Rightarrow \neg\mathbf{A}) \Rightarrow \neg\neg\mathbf{B},$$
$$\neg\neg\mathbf{B},\ \neg\neg\mathbf{B} \Rightarrow \mathbf{B},\ \mathbf{B}.$$

Результатом є вивід $\mathbf{B}$ з $\mathfrak{M}$ (поясніть, чому).

4. Покажемо, що коли $\mathfrak{M} \vdash \mathbf{A} \Rightarrow \mathbf{B}$ і $\mathfrak{M} \vdash \mathbf{B} \Rightarrow \mathbf{C}$, то $\mathfrak{M} \vdash \mathbf{A} \Rightarrow \mathbf{C}$. Дійсно, випишемо вивід $\mathbf{A} \Rightarrow \mathbf{B}$, припишемо до нього вивід $\mathbf{B} \Rightarrow \mathbf{C}$ та речення

$$(\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})),\ \mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C}),$$
$$(\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})),$$
$$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C}),\ \mathbf{A} \Rightarrow \mathbf{C}.$$

Результатом є вивід $\mathbf{A} \Rightarrow \mathbf{C}$ з $\mathfrak{M}$ (чому?).

Вправа 1.3.7.

1. Доведіть, що для довільних речень $\mathbf{A}, \mathbf{B}$
$$\vdash \mathbf{A} \vee \mathbf{B} \Rightarrow \mathbf{B} \vee \mathbf{A}.$$
2. Доведіть, що для довільних речень $\mathbf{A}, \mathbf{B}, \mathbf{C}$
$$\vdash (\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})) \Rightarrow (\mathbf{B} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})).$$
3. Доведіть, що для довільного речення $\mathbf{A}$
$$\vdash (\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \mathbf{A}.$$
Вказівка: Скористайтеся вже відомим $\vdash \neg\mathbf{A} \Rightarrow \neg\mathbf{A}$.
4. Доведіть, що коли $\mathfrak{M} \vdash \mathbf{A}$ і $\mathfrak{N} \vdash \mathbf{B}$ для кожного речення $\mathbf{B} \in \mathfrak{M}$, то й $\mathfrak{N} \vdash \mathbf{A}$.

Зауважимо одну очевидну властивість числення висловлювань.

Твердження 1.3.8. *Якщо множина речень $\mathfrak{M}$ суперечлива, то такою ж є деяка її скінченна підмножина.*

Доведення. Дійсно, з множини $\mathfrak{M}$ виводиться якесь речення $\mathbf{A}$ разом з реченням $\neg\mathbf{A}$. Але кожен вивід містить лише скінченну кількість речень. Якщо $\mathfrak{N}$ — множина тих речень з $\mathfrak{M}$, які зустрічаються у виводі $\mathbf{A}$ або у виводі $\neg\mathbf{A}$, то, очевидно, $\mathfrak{N}$ — скінченна підмножина $\mathfrak{M}$, причому $\mathfrak{N} \vdash \mathbf{A}$ і $\mathfrak{N} \vdash \neg\mathfrak{A}$, тобто $\mathfrak{N}$ суперечлива. □

1.4. Теорема дедукції та її застосування

Побудова виводів є досить складною задачею. Зараз ми доведемо один результат, який значно спрощує пошук виводів.

Теорема 1.4.1 (Теорема дедукції). *Якщо* $\mathfrak{M} \cup \{\mathbf{A}\} \vdash \mathbf{B}$, *то* $\mathfrak{M} \vdash \mathbf{A} \Rightarrow \mathbf{B}$.

Доведення. Доведення, яке ми наведемо, буде також *ефективним*, тобто ми дамо алгоритм, який перероблює вивід речення $\mathbf{B}$ із $\mathfrak{M} \cup \{\mathbf{A}\}$ у вивід $\mathbf{A} \Rightarrow \mathbf{B}$ із $\mathfrak{M}$. Нехай $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n$ — вивід $\mathbf{B}$ з $\mathfrak{M}\{\mathbf{A}\}$, зокрема, $\mathbf{B}_n = \mathbf{B}$. Наш алгоритм послідовно замінює кожне речення $\mathbf{B}_i$ на кілька речень, останнім з яких є $\mathbf{A} \Rightarrow \mathbf{B}_i$. Ця заміна залежить від підстави, на якій речення $\mathbf{B}_i$ увійшло до даного виводу. Саме:

1. Якщо $\mathbf{B}_i$ — аксіома або належить $\mathfrak{M}$, воно замінюється на
$$\mathbf{B}_i,\ \mathbf{B}_i \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_i),\ \mathbf{A} \Rightarrow \mathbf{B}_i.$$
2. Якщо $\mathbf{B}_i = \mathbf{A}$, воно замінюється на вивід речення $\mathbf{A} \Rightarrow \mathbf{A}$ (приклад 1.3.6.1).
3. Якщо $\mathbf{B}_i$ одержане за правилом modus ponens з речень $\mathbf{B}_j$ та $\mathbf{B}_k$ ($j < i$, $k < i$, $\mathbf{B}_j = \mathbf{B}_k \Rightarrow \mathbf{B}_i$), воно замінюється на
$$(\mathbf{A} \Rightarrow \mathbf{B}_j) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}_k) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_i)),$$
$$(\mathbf{A} \Rightarrow \mathbf{B}_k) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_i),\ \mathbf{A} \Rightarrow \mathbf{B}_i.$$

Оскільки $\mathbf{B}_j = \mathbf{B}_k \Rightarrow \mathbf{B}_i$, то тут перше речення є аксіомою вигляду (A2). Друге речення одержане за modus ponens із першого та речення $\mathbf{A} \Rightarrow \mathbf{B}_j$, яке було одержане раніше (при заміні речення $\mathbf{B}_j$), а третє так само одержане з другого та речення $\mathbf{A} \Rightarrow \mathbf{B}_k$, яке теж було одержане раніше (при заміні речення $\mathbf{B}_k$).

Очевидно, в результаті одержимо вивід речення $\mathbf{A} \Rightarrow \mathbf{B}$ (воно є останнім при заміні речення $\mathbf{B}_n$) із множини $\mathfrak{M}$. $\square$

Очевидною індукцією з теореми дедукції одержуємо наступне її узагальнення.

Наслідок 1.4.2. *Якщо* $\mathfrak{M} \cup \{ \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_m \} \vdash \mathbf{B}$, *то*

$$\mathfrak{M} \vdash \mathbf{A}_1 \Rightarrow (\mathbf{A}_2 \Rightarrow (\ldots \Rightarrow (\mathbf{A}_m \Rightarrow \mathbf{B}) \ldots)).$$

Розглянемо кілька прикладів застосування теореми дедукції.

Приклад 1.4.3.

1. Доведемо, що $\vdash \mathbf{A} \Rightarrow \neg\neg\mathbf{A}$. Згідно з теоремою дедукції, для цього достатньо довести, що $\mathbf{A} \vdash \neg\neg\mathbf{A}$. Наведемо відповідний вивід:

   $$\mathbf{A},\ \mathbf{A} \Rightarrow (\neg\mathbf{A} \Rightarrow \mathbf{A}),\ \neg\mathbf{A} \Rightarrow \mathbf{A},\ «\neg\mathbf{A} \Rightarrow \neg\mathbf{A}»,$$
   $$(\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow ((\neg\mathbf{A} \Rightarrow \neg\mathbf{A}) \Rightarrow \neg\neg\mathbf{A}),$$
   $$(\neg\mathbf{A} \Rightarrow \neg\mathbf{A}) \Rightarrow \neg\neg\mathbf{A},\ \neg\neg\mathbf{A}.$$

   Тут ми написали «$\neg\mathbf{A} \Rightarrow \neg\mathbf{A}$» замість того, щоб виписати вивід речення $\neg\mathbf{A} \Rightarrow \neg\mathbf{A}$, наведений у прикладі 1.3.6.1. Надалі будемо постійно користуватися подібними скороченнями (з часом навіть опускаючи лапки).
2. Доведемо, що $\vdash (\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\neg\mathbf{B} \Rightarrow \neg\mathbf{A})$. Для цього достатньо показати, що $\mathbf{A} \Rightarrow \mathbf{B}$, $\neg\mathbf{B} \vdash \neg\mathbf{A}$. Наведемо відповідний вивід:

   $$\neg\mathbf{B} \Rightarrow (\mathbf{A} \Rightarrow \neg\mathbf{B}),\ \neg\mathbf{B},\ \mathbf{A} \Rightarrow \neg\mathbf{B},$$
   $$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{A} \Rightarrow \neg\mathbf{B}) \Rightarrow \neg\mathbf{A}),\ \mathbf{A} \Rightarrow \mathbf{B},$$
   $$(\mathbf{A} \Rightarrow \neg\mathbf{B}) \Rightarrow \neg\mathbf{A},\ \neg\mathbf{A}.$$

3. Множина речень $\mathbf{A}, \neg\mathbf{A}$, очевидно, суперечлива. Тому $\mathbf{A}, \neg\mathbf{A} \vdash \mathbf{B}$ для довільного речення $\mathbf{B}$ (приклад 1.3.6.3). За наслідком 1.4.2, $\vdash \neg\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$.
4. Очевидно, $\mathbf{A}, \mathbf{A} \Rightarrow \mathbf{B} \vdash \mathbf{B}$. Тому $\mathbf{A} \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \mathbf{B})$.

Ще кілька прикладів залишаємо читачу як вправу. Цими результатами ми також будемо користуватись далі.

Вправа 1.4.4. Доведіть, що:

(1) $$(\neg\mathbf{A} \Rightarrow \neg\mathbf{B}) \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A}),$$

(2) $$\neg\mathbf{A} \Rightarrow (\neg\mathbf{B} \Rightarrow \neg(\mathbf{A} \vee \mathbf{B})),$$

(3) $$(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \mathbf{B})),$$

(4) $$\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A} \wedge \mathbf{B}).$$

1.5. Адекватність числення висловлювань

Зараз ми вже маємо достатньо інформації, щоб довести теорему про адекватність числення висловлювань (теорема 1.3.5). Наше доведення ґрунтується на такій лемі.

Лема 1.5.1 (**Лема Ка́льмара**). *Для кожної інтерпретації* $\mathcal{I} : \mathfrak{E} \to \mathbf{B}$ *і кожного речення* $\mathbf{A}$ *позначимо*

$$\mathbf{A}^{\mathcal{I}} = \begin{cases} \mathbf{A}, & \text{якщо } \operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}, \\ \neg\mathbf{A} & \text{якщо } \operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{0}. \end{cases}$$

Позначимо також $\mathfrak{E}^{\mathcal{I}} = \left\{ \mathbf{E}^{\mathcal{I}} \mid \mathbf{E} \in \mathfrak{E} \right\}$. *Тоді* $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{A}^{\mathcal{I}}$ *для довільного речення* $\mathbf{A}$.

Доведення. Скористаємося індукцією за довжиною речення $\mathbf{A}$. Якщо $\mathbf{A}$ — атом, то $\mathbf{A}^{\mathcal{I}} \in \mathfrak{E}^{\mathcal{I}}$, тому $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{A}^{\mathcal{I}}$. Інакше $\mathbf{A}$ має один з виглядів:

(1) $\mathbf{B} \Rightarrow \mathbf{C}$,

(2) $\mathbf{B} \wedge \mathbf{C}$,

(3) $\mathbf{B} \vee \mathbf{C}$,

(4) $\neg\mathbf{B}$,

де $\mathbf{B}$ і $\mathbf{C}$ — коротші речення, отже, за припущенням індукції можна вважати, що $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{B}^{\mathcal{I}}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{C}^{\mathcal{I}}$. Розглянемо всі випадки залежно від значень $\operatorname{val}(\mathcal{I}, \mathbf{B})$ і $\operatorname{val}(\mathcal{I}, \mathbf{C})$.

1. $\mathbf{A} = \mathbf{B} \Rightarrow \mathbf{C}$. Якщо $\operatorname{val}(\mathcal{I}, \mathbf{B}) = \mathbf{0}$, то $\operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \neg\mathbf{B}$. Однак ми вже знаємо, що $\vdash \neg\mathbf{B} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})$ (приклад 1.4.3.4). Застосувавши modus ponens, одержимо $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{A}$.

Якщо $\operatorname{val}(\mathcal{I}, \mathbf{C}) = \mathbf{1}$, також $\operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{C}$. Оскільки $\vdash \mathbf{C} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{C})$ (аксіома вигляду (A1)), то також $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{A}$.

Нехай, нарешті, $\operatorname{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$, а $\operatorname{val}(\mathcal{I}, \mathbf{C}) = \mathbf{0}$. Тоді $\operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{0}$, $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{B}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \neg\mathbf{C}$. Додамо до відповідних виводів речення

$$\begin{gathered} \mathbf{B} \Rightarrow ((\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow \mathbf{C}),\ (\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow \mathbf{C}, \\ «((\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow \mathbf{C}) \Rightarrow (\neg\mathbf{C} \Rightarrow \neg(\mathbf{B} \Rightarrow \mathbf{C}))», \\ \neg\mathbf{C} \Rightarrow \neg(\mathbf{B} \Rightarrow \mathbf{C}),\ \neg(\mathbf{B} \Rightarrow \mathbf{C}) \end{gathered}$$

(у другому рядку стоїть частковий випадок з прикладу 1.4.3.2). Одержимо вивід $\mathbf{A}^{\mathcal{I}} = \neg\mathbf{A}$ з $\mathfrak{E}^{\mathcal{I}}$.

2. $\mathbf{A} = \mathbf{B} \wedge \mathbf{C}$. Якщо $\operatorname{val}(\mathcal{I}, \mathbf{B}) = \mathbf{0}$, то й $\operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{0}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \neg\mathbf{B}$. Додавши речення

$$\begin{gathered} (\mathbf{B} \wedge \mathbf{C}) \Rightarrow \mathbf{B},\ «((\mathbf{B} \wedge \mathbf{C}) \Rightarrow \mathbf{B}) \Rightarrow (\neg\mathbf{B} \Rightarrow \neg(\mathbf{B} \wedge \mathbf{C}))», \\ \neg\mathbf{B} \Rightarrow \neg(\mathbf{B} \wedge \mathbf{C}),\ \neg(\mathbf{B} \wedge \mathbf{C}), \end{gathered}$$

отримаємо вивід $\mathbf{A}^{\mathcal{I}} = \neg\mathbf{A}$ з $\mathfrak{E}^{\mathcal{I}}$. Те саме міркування працює й тоді, коли $\operatorname{val}(\mathcal{I}, \mathbf{C}) = \mathbf{0}$.

Припустимо, що $\operatorname{val}(\mathcal{I}, \mathbf{B}) = \operatorname{val}(\mathcal{I}, \mathbf{C}) = \mathbf{1}$. Тоді $\operatorname{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$, $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{B}$ і $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{C}$. Залишається додати речення

$$«\mathbf{B} \Rightarrow (\mathbf{C} \Rightarrow \mathbf{B} \wedge \mathbf{C})»,\ \mathbf{C} \Rightarrow \mathbf{B} \wedge \mathbf{C},\ \mathbf{B} \wedge \mathbf{C},$$

щоб одержати вивід $\mathbf{A}$ з $\mathfrak{E}^{\mathcal{I}}$.

Розгляд випадків 3 та 4 ми залишаємо як вправу читачу. □

Нам потрібне також поняття *повноти*, яке відіграє значну роль у всій формальній логіці.

Означення 1.5.2. Множину речень $\mathfrak{M}$ назвемо *повною*, якщо для будь-якого речення $\mathbf{A}$ або $\mathfrak{M} \vdash \mathfrak{A}$, або $\mathfrak{M} \vdash \neg\mathfrak{A}$. Зауважимо, що суперечлива множина є напевне повною, оскільки з неї виводиться довільне речення.

Лема 1.5.3. *Якщо речення $\mathbf{A}$ не виводиться з множини речень $\mathfrak{M}$, то множина $\mathfrak{M} \cup \{\, \neg\mathbf{A} \,\}$ є несуперечливою.*

Доведення. Множина $\mathfrak{M}$ є несуперечливою, оскільки з неї не виводиться $\mathbf{A}$. Припустимо, що множина $\mathfrak{M} \cup \{\, \neg\mathbf{A} \,\}$ суперечлива. Тоді, зокрема, $\mathfrak{M} \cup \{\, \neg\mathbf{A} \,\} \vdash \mathbf{A}$. За теоремою дедукції, $\mathfrak{M} \vdash \neg\mathbf{A} \Rightarrow \mathbf{A}$. Оскільки $\vdash (\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \mathbf{A}$ (вправа 1.3.7.2), то $\mathfrak{M} \vdash \mathbf{A}$ за modus ponens. □

Лема 1.5.4. *Кожна несуперечлива множина речень $\mathfrak{M}$ міститься у повній несуперечливій множині.*

Доведення. Множина всіх речень, очевидно, зліченна. Пронумеруємо всі речення: $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \ldots$ і визначимо множини $\mathfrak{M}_i$ $(i \in \mathbb{N})$ такою рекурсивною процедурою:

$$\mathfrak{M}_1 = \mathfrak{M},$$

$$\mathfrak{M}_{i+1} = \begin{cases} \mathfrak{M}_i, & \text{якщо } \mathfrak{M}_i \vdash \mathbf{A}_i, \\ \mathfrak{M}_i \cup \{\, \neg\mathbf{A}_i \,\}, & \text{інакше.} \end{cases}$$

За лемою 1.5.3 усі множини $\mathfrak{M}_i$ $(i \in \mathbb{N})$ несуперечливі. Тоді й їхнє об'єднання $\mathfrak{M}_\infty = \bigcup_{i=1}^{\infty} \mathfrak{M}_i$ є також несуперечливим за лемою 1.3.8. Проте, за побудовою, для кожного речення $\mathbf{A}_i$ або $\mathfrak{M}_i \vdash \mathbf{A}_i$, а тому й $\mathfrak{M}_\infty \vdash \mathbf{A}_i$, або $\neg\mathbf{A}_i \in \mathfrak{M}_{i+1} \subseteq \mathfrak{M}_\infty$, а тому $\mathfrak{M}_\infty \vdash \neg\mathbf{A}_i$. Отже, множина $\mathfrak{M}_\infty$ повна. □

Доведення теореми про адекватність. Припустимо, що $\mathfrak{M} \nvdash \mathbf{A}$. Тоді $\mathfrak{M} \cup \{\, \neg\mathbf{A} \,\}$ — несуперечлива множина, отже вона міститься у повній несуперечливій множині $\mathfrak{N}$. Розглянемо інтерпретацію $\mathcal{I}$, визначену правилом:

$$\mathcal{I}(\mathbf{E}) = \begin{cases} \mathbf{1}, & \text{якщо } \mathfrak{N} \vdash \mathbf{E}, \\ \mathbf{0}, & \text{якщо } \mathfrak{N} \vdash \neg\mathbf{E}, \end{cases}$$

де $\mathbf{E}$ позначає довільний атом. Покажемо, що $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$ для всіх $\mathbf{B} \in \mathfrak{N}$. Дійсно, згідно з лемою Кальмара, $\mathfrak{E}^{\mathcal{I}} \vdash \mathbf{B}^{\mathcal{I}}$. З іншого боку, $\mathfrak{N} \vdash \mathbf{E}^{\mathcal{I}}$ для кожного атома $\mathbf{E}$ за означенням інтерпретації $\mathcal{I}$. Тому $\mathfrak{N} \vdash \mathbf{B}^{\mathcal{I}}$ (вправа 1.3.7.3). Оскільки $\mathfrak{N}$ несуперечлива, а $\mathbf{B} \in \mathfrak{N}$, обов'язково $\mathbf{B}^{\mathcal{I}} = \mathbf{B}$, тобто $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$. Зокрема, $\mathrm{val}(\mathcal{I}, \mathbf{B}) = \mathbf{1}$ для всіх речень $\mathbf{B} \in \mathfrak{M}$ і $\mathrm{val}(\mathcal{I}, \neg\mathbf{A}) = \mathbf{1}$, тобто $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{0}$. Отже $\mathfrak{M} \not\models \mathbf{A}$. □

Наслідок 1.5.5. *Множина речень $\mathfrak{M}$ є несумісною тоді й лише тоді, коли вона є суперечливою.*

Доведення. Очевидно, суперечлива множина несумісна. Навпаки, якщо множина $\mathfrak{M}$ несумісна, то $\mathfrak{M} \models \mathbf{A}$, а тому й $\mathfrak{M} \vdash \mathbf{A}$ для кожного речення $\mathbf{A}$, зокрема, й для заперечення кожного речення. Тоді ця множина суперечлива. □

Зауважимо, що з теореми про адекватність безпосередньо випливає ще й таке твердження, яке зовсім не є очевидним у межах семантики логіки висловлювань.

Наслідок 1.5.6 (Компактність логіки висловлювань). *Нехай кожна скінченна підмножина множини речень $\mathfrak{M}$ є сумісною. Тоді й уся множина $\mathfrak{M}$ є сумісною.*

Доведення. За лемою 1.5.5 слово «сумісний» можна замінити на «несуперечливий», після чого це твердження стає цілковито очевидним. □

Зауваження 1.5.7. З леми Кальмара можна вивести навіть алгоритм побудови виводу кожної тавтології $\mathbf{A}$. Для цього випишемо множину всіх атомів, які входять до речення $\mathbf{A}$: $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_n$. Позначимо $\mathfrak{E}_m = \{\, \mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_m \,\}$ $(m \leqslant n)$; зокрема, $\mathfrak{E}_0 = \emptyset$. Побудуємо для довільного відображення $\mathcal{I} : \mathfrak{E}_m \to \mathbb{B}$ вивід $\mathbf{A}$ з $\mathfrak{E}_m^{\mathcal{I}}$. Для $m = n$ це лема Кальмара. Далі скористаємося «оберненою рекурсією». Припустимо, що ми вже побудували виводи $\mathbf{A}$ з $\mathfrak{E}_{m+1}^{\mathcal{I}_0}$ і з $\mathfrak{E}_{m+1}^{\mathcal{I}_1}$, де

$$\begin{aligned}
&\mathcal{I}_0(\mathbf{E}_i) = \mathcal{I}_1(\mathbf{E}_i) = \mathcal{I}(\mathbf{E}_i) \quad \text{при} \quad i \leqslant m,\\
&\mathcal{I}_0(\mathbf{E}_{m+1}) = \mathbf{0},\\
&\mathcal{I}_1(\mathbf{E}_{m+1}) = \mathbf{1}.
\end{aligned}$$

За теоремою дедукції одержимо виводи речень $\mathbf{E}_{m+1} \Rightarrow \mathbf{A}$ та $\neg\mathbf{E}_{m+1} \Rightarrow \mathbf{A}$ з множини $\mathfrak{E}_m^{\mathcal{I}}$. Оскільки $\vdash (\mathbf{E}_{m+1} \Rightarrow \mathbf{A}) \Rightarrow ((\neg\mathbf{E}_{m+1} \Rightarrow \mathbf{A}) \Rightarrow \mathbf{A})$ (вправа 1.4.4.3), одержимо вивід $\mathbf{A}$ з $\mathfrak{E}_m^{\mathcal{I}}$. При $m = 0$ одержимо вивід $\mathbf{A}$ з порожньої множини.

1.6. Поняття про інтуїціоністську логіку

У XX ст., у зв'язку з кризою теорії множин, розвинулася течія у математиці, яка отримала назву «інтуїціонізм». Оскільки основи інтуїціонізму лежать скоріше в галузі філософії математики, ми не будемо тут на них зупинятися. Розглянемо лише одну систему формальної логіки, яка виникла під впливом інтуїціонізму. Вона належить одному з активних інтуїціоністів Гейтінгу. Це інтуїціоністське числення висловлювань.

Означення 1.6.1.

1. *Мова* інтуїціоністського числення висловлювань збігається з мовою звичайного («класичного») числення висловлювань (означення 1.2.1).
2. *Аксіомами* інтуїціоністського числення висловлювань звуться всі речення вигляду (A1)–(A9) з вправи 1.2.6, а також усі речення вигляду

$$(\mathrm{A10}^I) \qquad \neg\mathbf{A} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}).$$

3. Єдиним *правилом виводу* інтуїціоністського числення висловлювань є правило modus ponens.
4. Поняття *виводу* в інтуїціоністському численні висловлювань збігається з аналогічним поняттям звичайного числення висловлювань.

Якщо існує вивід речення $\mathbf{A}$ в інтуїціоністському численні висловлювань з множини речень $\mathfrak{M}$, то пишуть $\mathfrak{M} \vdash^I \mathbf{A}$.

Ми не будемо розглядати *семантику* інтуїціоністського числення висловлювань, оскільки вона досить складна. Що стосується виводів у інтуїціоністському численні висловлювань, то ми доведемо теорему, яка встановлює деякий зв'язок із звичайним (класичним) численням висловлювань.

Теорема 1.6.2. *Для кожного речення* $\mathbf{A}$ *позначимо через* $\widetilde{\mathbf{A}}$ *речення* $\neg\neg\mathbf{A}$, *і для кожної множини речень* $\mathfrak{M}$ *позначимо* $\widetilde{\mathfrak{M}} = \left\{ \widetilde{\mathbf{A}} \mid \mathbf{A} \in \mathfrak{M} \right\}$.

1. *Якщо* $\mathfrak{M} \vdash^I \mathbf{A}$, *то й* $\mathfrak{M} \vdash \mathbf{A}$.
2. *Якщо* $\mathfrak{M} \vdash \mathbf{A}$, *то* $\widetilde{\mathfrak{M}} \vdash^I \widetilde{\mathbf{A}}$.
3. *Якщо* $\mathfrak{M} \vdash \neg\mathbf{A}$, *то* $\widetilde{\mathfrak{M}} \vdash^I \neg\mathbf{A}$.

Інакше кажучи, усі «негативні» виводи класичного числення висловлювань можна переробити у виводи інтуїціоністського числення висловлювань. У той же час цього не можна гарантувати для «позитивних» виводів. Зокрема, можна показати, що в інтуїціоністському численні висловлювань не існує виводу речення $\neg\neg\mathbf{A} \Rightarrow \mathbf{A}$ (яке є аксіомою класичного числення висловлювань), хоча це й вимагає апеляції до семантики, а тому не може бути зроблено тут.

Доведення. Ми пропонуємо доведення теореми 1.6.2, що наслідує тому доведенню теореми про адекватність, яке наведене в попередньому розділі. Більшість його кроків буде лише намічено, а деталі доведення залишені читачу для самостійного відтворення. Зауважимо, що твердження 1 цієї теореми тривіальне, оскільки кожен вивід у інтуїціоністському численні висловлювань є таким і в класичному, точніше, може бути перероблений у класичний вивід, якщо кожен раз аксіому (A10^I) замінювати її (класичним) виводом (вправа 1.3.7.2). Твердження 2 випливає з твердження 3, оскільки якщо $\vdash \mathbf{A}$, то й $\vdash \neg\neg\mathbf{A}$ (див. приклад 1.4.3.1). Отже, залишається довести лише твердження 3.

Перш за все зауважимо, що вивід речення $\mathbf{A} \Rightarrow \mathbf{A}$ (приклад 1.3.6.1) і доведення теореми дедукції не використовували аксіому (A10), тому теорема дедукції має місце і в інтуїціоністському численні висловлювань. Далі, аксіома (A10^I) гарантує, що коли $\mathfrak{M} \vdash^I \mathbf{A}$ і $\mathfrak{M} \vdash^I \neg\mathbf{A}$, то $\mathfrak{M} \vdash^I \mathbf{B}$ для довільного речення $\mathbf{B}$. У прикладах 1.4.3.1,2 ми також не користувалися аксіомою (A10), тому $\vdash^I \mathbf{A} \Rightarrow \neg\neg\mathbf{A}$ і $\vdash^I (\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\neg\mathbf{B} \Rightarrow \neg\mathbf{A})$. Звідси випливає, що $\vdash^I \neg\neg\neg\mathbf{A} \Rightarrow \neg\mathbf{A}$ (зокрема, твердження 3 теореми рівносильне твердженню 2).

Ми покажемо, що кожен класичний вивід речення $\mathbf{A}$ з множини $\mathfrak{M}$ можна переробити в інтуїціоністський вивід речення $\widetilde{\mathbf{A}}$ з множини $\widetilde{\mathfrak{M}}$. Спочатку встановимо такі результати.

Лема 1.6.3. *Для довільних речень* $\mathbf{A}$, $\mathbf{B}$
(1) $\neg\neg\mathbf{A},\ \neg\neg(\mathbf{A} \Rightarrow \mathbf{B}) \vdash^I \neg\neg\mathbf{B}$.
(2) $\vdash^I \neg\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A})$.

Доведення. Покажемо спочатку, що $\neg\neg\mathbf{A}, \neg\mathbf{B} \vdash^I \neg(\mathbf{A} \Rightarrow \mathbf{B})$. Ось відповідний вивід:

$$(\mathbf{A} \Rightarrow \neg\mathbf{B}) \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\mathbf{A}),\ \neg\mathbf{B} \Rightarrow (\mathbf{A} \Rightarrow \neg\mathbf{B}),\ \neg\mathbf{B},$$
$$\mathbf{A} \Rightarrow \neg\mathbf{B},\ (\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\mathbf{A},\ \neg\neg\mathbf{A} \Rightarrow ((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\neg\mathbf{A}),$$
$$\neg\neg\mathbf{A},\ (\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\neg\mathbf{A},$$
$$((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\mathbf{A}) \Rightarrow (((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\neg\mathbf{A}) \Rightarrow \neg(\mathbf{A} \Rightarrow \mathbf{B})),$$
$$((\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\neg\mathbf{A}) \Rightarrow \neg(\mathbf{A} \Rightarrow \mathbf{B}),\ \neg(\mathbf{A} \Rightarrow \mathbf{B}).$$

За теоремою дедукції маємо $\neg\neg\mathbf{A} \vdash^I \neg\mathbf{B} \Rightarrow \neg(\mathbf{A} \Rightarrow \mathbf{B})$. Оскільки вже відомо, що $\vdash^I (\neg\mathbf{B} \Rightarrow \neg(\mathbf{A} \Rightarrow \mathbf{B})) \Rightarrow (\neg\neg(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\neg\mathbf{B})$, звідси отримуємо (1).

Далі, з аксіоми $\mathbf{B} \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B})$ одержуємо $\vdash^I \neg(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \neg\mathbf{B}$. Зокрема, $\vdash^I \neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \neg\mathbf{A}$. Тому можна сконструювати такий вивід речення (2) (ми опустили в ньому кілька речень; читачу пропонується заповнити відповідні місця):

$$\neg\mathbf{A} \Rightarrow (\neg\neg\mathbf{A} \Rightarrow \mathbf{A}),\ \neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \neg\neg\mathbf{A},\ \neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \neg\mathbf{A},$$
$$(\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \neg\mathbf{A}) \Rightarrow ((\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A}) \Rightarrow \neg\neg\mathbf{A}) \Rightarrow \neg\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A})),$$
$$\neg\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A})\ \square$$

Ця лема обґрунтовує такий алгоритм переробки класичного виводу $\mathbf{A}$ з $\mathfrak{M}$ в інтуїціоністський вивід $\widetilde{\mathbf{A}}$ з $\widetilde{\mathfrak{M}}$.

1. Аксіоми (A1)–(A9) залишаються.
2. Аксіома (A10) замінюється на інтуїціоністський вивід речення $\neg\neg(\neg\neg\mathbf{A} \Rightarrow \mathbf{A})$.
3. Речення $\mathbf{B} \in \mathfrak{M}$ замінюється на речення $\widetilde{\mathbf{B}} = \neg\neg\mathbf{B} \in \widetilde{\mathfrak{M}}$.
4. Якщо якесь речення $\mathbf{A}_i$ було одержане за правилом modus ponens з речень $\mathbf{A}_j$ та $\mathbf{A}_k = \mathbf{A}_j \Rightarrow \mathbf{A}_i$, де $j, k < i$, то воно замінюється на вивід $\widetilde{\mathbf{A}}_i = \neg\neg\mathbf{A}_i$ з $\widetilde{\mathbf{A}}_j = \neg\neg\mathbf{A}_j$ та $\widetilde{\mathbf{A}}_k = \neg\neg(\mathbf{A}_j \Rightarrow \mathbf{A}_i)$.

У результаті одержимо необхідний вивід (поясніть, чому). $\square$

Вправа 1.6.4 (Варіант інтуїціоністської семантики). Однією з можливостей визначити семантику речень інтуїціоністської логіки є така. Нехай X — деякий метричний (або взагалі топологічний) простір, $\mathcal{U}(X)$ — множина його відкритих підмножин. Через $\complement A$, де $A \subseteq X$, позначимо доповнення $\complement A = X \setminus A$, а через A° — *внутрішність* A, себто об'єднання всіх відкритих підмножин $U \subseteq A$. *Інтуїціоністською інтерпретацією* назвемо відображення $\mathcal{I} : \mathfrak{E} \to \mathcal{U}(X)$. Для речень логіки висловлювань визначимо їхні значення в інтерпретації $\mathcal{I}$ в такий спосіб.

- Якщо $\mathbf{A}$ — атом, то $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathcal{I}(\mathbf{A})$.
- Значення речень, утворених за правилами 3(b,c) з означення 1.2.1, обчислюються за правилами:

$$\mathrm{val}(\mathcal{I}, \neg\mathbf{A}) = \big(\complement\,\mathrm{val}(\mathcal{I}, \mathbf{A})\big)^\circ;$$
$$\mathrm{val}(\mathcal{I}, \mathbf{A} \vee \mathbf{B}) = \mathrm{val}(\mathcal{I}, \mathbf{A}) \cup \mathrm{val}(\mathcal{I}, \mathbf{B});$$
$$\mathrm{val}(\mathcal{I}, \mathbf{A} \wedge \mathbf{B}) = \mathrm{val}(\mathcal{I}, \mathbf{A}) \cap \mathrm{val}(\mathcal{I}, \mathbf{B});$$
$$\mathrm{val}(\mathcal{I}, \mathbf{A} \Rightarrow \mathbf{B}) = \big(\complement\,\mathrm{val}(\mathcal{I}, \mathbf{A}) \cup \mathrm{val}(\mathcal{I}, \mathbf{B})\big)^\circ.$$

Назвемо речення $\mathbf{A}$ *істинним* в інтерпретації $\mathcal{I}$, якщо $\mathrm{val}(\mathcal{I}, \mathbf{A}) = X$. Речення, істинні в кожній інтуїціоністській інтерпретації, назвемо *інтуїціоністськими тавтологіями*. Так само, як у класичній логіці, будемо писати $\mathfrak{M} \models^I \mathbf{A}$, якщо в кожній інтуїціоністській інтерпретації, в якій істинні всі речення з $\mathfrak{M}$, істинне й речення $\mathbf{A}$.

1. Доведіть, що кожна аксіома інтуїціоністського числення висловлювань є інтуїціоністською тавтологією.
2. Доведіть, що з $\mathfrak{M} \vdash^I \mathbf{A}$ випливає $\mathfrak{M} \models^I \mathbf{A}$.
3. Доведіть, що наведені нижче речення, які є тавтологіями класичної логіки, не є інтуїціоністськими тавтологіями:

   $$\neg\neg\mathbf{A} \Rightarrow \mathbf{A}, \quad \mathbf{A} \vee \neg\mathbf{A}, \quad (\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\neg\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow \mathbf{B}),$$

   де $\mathbf{A}, \mathbf{B}$ — деякі атоми. Отже, в інтуїціоністській логіці не можна застосовувати такі класичні засоби, як зведення до абсурду або аналіз випадків.
4. Покажіть, що коли X складається з однієї точки, поняття інтуїціоністської інтерпретації зводиться до звичайного поняття інтерпретації в класичній логіці висловлювань. Це твердження залишається вірним і для довільного скінченного простору X, якщо він є T_1-простором, тобто кожна його точка є замкненою (зауважимо, що скінченний T_1-простір завжди є гаусдорфовим).

Можна довести, що з $\mathfrak{M} \models^I \mathbf{A}$ випливає $\mathfrak{M} \vdash^I \mathbf{A}$. Більш того, останнє твердження залишається вірним, навіть якщо обмежитись інтерпретаціями, в яких X — фіксований нескінченний компактний простір (наприклад, замкнений відрізок $[0, 1]$). Доведення цього факту (та багатьох його узагальнень) можна знайти в [**PC**]. Воно істотно складніше, ніж теорема адекватності для класичного числення висловлювань. Наприклад, лема Кальмара, яка є головним засобом у доведенні теореми адекватності, не має аналога в інтуїціоністському численні висловлювань.

Існують також інші формально-логічні системи, які відображають інтуїціоністські концепції. Серед них відзначимо так звану *мінімальну логіку*. У ній аксіомами вважаються лише речення вигляду (A1)–(A9) з вправи 1.2.6.

Зазначимо, що більшість математиків, які притримуються інтуїціоністських поглядів, вважають, що ніяка *формальна* система не може адекватно відобразити *змістовні* правила міркувань. До деякої міри це буде підтверджено результатами розділу 3, принаймні, якщо йдеться про правила міркувань у математиці.

Додаток А

Булеві функції

Нагадаємо, що *булева функція* — це відображення $f : \mathbb{B}^n \to \mathbb{B}$, де $\mathbb{B} = \{\,\mathbf{0}, \mathbf{1}\,\}$ — множина *булевих значень*. Зокрема, кожен логічний сполучник визначає булеву функцію. Ми будемо позначати цю функцію тим самим символом, що й відповідний сполучник (наприклад, $\vee, \wedge, \neg, \Rightarrow$). Теорія булевих функцій швидше відноситься не до логіки, а до комбінаторики або дискретної математики. Тому ми лише розглянемо кілька фактів із цієї теорії у вигляді серії задач. На наш погляд, розв'язання цих задач цілком доступне кожному читачу.

Основна наша мета — одержати критерій того, що деяка множина $\mathcal{F}$ булевих функцій є *повною* в розумінні наступного означення.

Означення А 1. Множина $\mathcal{F}$ булевих функцій зветься *повною*, якщо довільну булеву функцію можна виразити через функції з $\mathcal{F}$ за допомогою суперпозицій.

Почнемо з того. що встановимо повноту деяких відомих множин. Перш за все — це множина, яка складається з кон'юнкції, диз'юнкції та заперечення.

Вправа А 2.

1. Нехай $f : \mathbb{B}^n \to \mathbb{B}$, — довільна булева функція. Для кожного вектора $\mathbf{a} = (a_1, a_2, \ldots, a_n)$, де $a_i \in \mathbb{B}$, позначимо $T_{\mathbf{a}} = y_1 \wedge y_2 \wedge \ldots y_n$, де
$$y_i = \begin{cases} x_i & \text{якщо } a_i = \mathbf{1}, \\ \neg x_i & \text{якщо } a_i = \mathbf{0}. \end{cases}$$
Перевірте, що
$$f\,(x_1, x_2, \ldots, x_n) = \bigvee_{f(\mathbf{a})=\mathbf{1}} T_{\mathbf{a}}. \tag{A1}$$
Вираз (A1) зветься *диз'юнктивною нормальною формою* функції f.
2. Які зміни треба внести до наведеної конструкції, щоб подати функцію f у *кон'юнктивній нормальній формі*, тобто у вигляді $f\,(x_1, x_2, \ldots, x_n) = \bigwedge T'_{\mathbf{a}}$, де кожне $T'_{\mathbf{a}}$ — кон'юнкція змінних та їх заперечень?

Зокрема, кожна булева функція збігається з деякою функцією, яка виражається через функції $\neg$, $\vee$ та $\wedge$, тобто множина $\{\,\neg, \vee, \wedge\,\}$ є повною. Оскільки $\neg(x \vee y) = \neg x \wedge \neg y$, то звідси одержуємо

Наслідок А 3. *Кожна з множин* $\{\,\neg, \vee\,\}$ *та* $\{\,\neg, \wedge\,\}$ *є повною.*

Ще одна важлива повна множина складається з констант, кон'юнкції та *булевої суми* (або *суми за модулем 2*). Позначимо $x \oplus y = \neg(x \Leftrightarrow y)$. Ця функція називається *булевою сумою* (складіть таблицю її значень, щоб побачити, звідки виникла така назва). Легко перевірити, що мають місце наступні тотожності:

$$x \oplus y = y \oplus x,$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z),$$
$$x \wedge (y \oplus z) = x \wedge y \oplus x \wedge z.$$

Тому ми будемо опускати дужки, коли йдеться про булеву суму кількох доданків, та вільно переставляти ці доданки. *Булевим одночленом* називається кон'юнкція змінних $x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_m}$, де $i_1 < i_2 < \cdots < i_m$; якщо $m = 0$, то вважають, що булів одночлен — це константа $\mathbf{1}$. *Булевим многочленом* називається булева сума різних булевих одночленів. Булеві многочлени можна ототожнити з многочленами над полем лишків за модулем 2, які є лінійними за кожною змінною. Тоді наступний результат може розглядатися як варіант теореми про інтерполяцію.

Вправа А 4. Доведіть, що кожну булеву функцію можна однозначно виразити деяким булевим многочленом.

Вказівка: Ось два можливі варіанти доведення:

1. Індукцією за кількістю змінних: для функції від $n+1$ змінної $f(x_1, x_2, \ldots, x_{n+1})$ виразіть спочатку функції від n змінних $f_0 = f(x_1, x_2, \ldots, x_n, \mathbf{0})$ та $f_1 = f(x_1, x_2, \ldots, x_n, \mathbf{1})$ і скористайтеся тим, що $f = x_{n+1} \wedge f_1 \oplus (\mathbf{1} \oplus x_{n+1}) \wedge f_0$.
2. Перевірити, що кількість різних булевих многочленів від n змінних дорівнює кількості всіх булевих функцій і що різні булеві многочлени задають різні функції.

Отже, набір $\{\mathbf{0}, \mathbf{1}, \oplus, \wedge\}$ є повною множиною булевих функцій. Зауважимо, що, оскільки $\mathbf{1} \oplus \mathbf{1} = \mathbf{0}$, таким є й набір $\{\mathbf{1}, \oplus, \wedge\}$.

Будемо казати, що функція $f : \mathbb{B}^n \to \mathbb{B}$

- *зберігає нуль*, якщо $f(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \mathbf{0}$; множину всіх таких функцій позначимо $\mathcal{F}_0$;
- *зберігає одиницю*, якщо $f(\mathbf{1}, \mathbf{1}, \ldots, \mathbf{1}) = \mathbf{1}$; множину всіх таких функцій позначимо $\mathcal{F}_1$;
- *монотонна*, якщо $f(a_1, a_2, \ldots, a_n) \leqslant f(b_1, b_2, \ldots, b_n)$ кожного разу, коли $a_i \leqslant b_i$ для всіх номерів i (ми вважаємо, що $\mathbf{0} < \mathbf{1}$); множину всіх таких функцій позначимо $\mathcal{F}_2$;
- *самодвоїста*, якщо $f(\neg a_1, \neg a_2, \ldots, \neg a_n) = \neg f(a_1, a_2, \ldots, a_n)$ для всіх значень $a_1, a_2, \ldots, a_n$; множину всіх таких функцій позначимо $\mathcal{F}_3$;
- *лінійна*, якщо вона збігається з деяким лінійним булевим многочленом, тобто $f(x_1, x_2, \ldots, x_n) = c \oplus (\bigoplus_{k=1}^{m} x_{i_k})$ для деяких $i_1 < i_2 < \cdots < i_k$ та $c \in \mathbb{B}$; множину всіх таких функцій позначимо $\mathcal{F}_4$.

Вправа А 5. Доведіть, що всі функції, які можна виразити через функції з $\mathcal{F}_i$ $(i = 0, 1, 2, 3, 4)$, також належать $\mathcal{F}_i$. Отже, якщо $\mathcal{F} \subseteq \mathcal{F}_i$, то множина $\mathcal{F}$ напевне не є повною.

Вправа А 6. Позначимо $\hat{f}(x) = f(x, x, \ldots, x)$. Доведіть, що:

- коли f не зберігає нуль, то або $\hat{f}(x) = \neg x$, або $\hat{f}(x) = \mathbf{1}$;
- коли f не зберігає одиницю, то або $\hat{f}(x) = \neg x$, або $\hat{f}(x) = \mathbf{0}$.

Вправа А 7. Припустимо, що f немонотонна.

1. Доведіть, що знайдуться такі значення $a_1, a_2, \ldots, a_n$ і $b_1, b_2, \ldots, b_n$, що $f(a_1, a_2, \ldots, a_n) = \mathbf{0}$, $f(b_1, b_2, \ldots, b_n) = \mathbf{1}$, причому $a_i = b_i$ для всіх номерів i, крім одного: $i = k$, а в останньому випадку $a_k = \mathbf{1}$, $b_k = \mathbf{0}$.
2. Виведіть звідси, що коли множина $\mathcal{F}$ містить обидві константи й немонотонну функцію, то через функції з $\mathcal{F}$ можна виразити заперечення.

Вправа А 8. Припустимо, що f несамодвоїста, тобто знайдуться такі значення $a_1, a_2, \ldots, a_n$, що $f(a_1, a_2, \ldots, a_n) = f(\neg a_1, \neg a_2, \ldots, \neg a_n)$. Поклавши $y_i = x$, якщо $a_i = \mathbf{1}$, та $y_i = \neg x$, якщо $a_i = \mathbf{0}$, покажіть, що $f(y_1, y_2, \ldots, y_n)$ є константою.

Вправа А 9. З результатів вправ А 6–А 8 виведіть, що коли множина $\mathcal{F} \not\subseteq \mathcal{F}_i$ при всіх $i \in \{0, 1, 2, 3\}$, то через функції з $\mathcal{F}$ можна виразити заперечення та обидві константи.

Вправа А 10. Нехай $f(x_1, x_2, \ldots, x_n)$ — нелінійний булів многочлен, $x_{i_1} \wedge x_{i_2} \wedge \ldots \wedge x_{i_m}$ — деякий нелінійний одночлен, який входить до f, з найменшим значенням $m > 1$.

1. Покладіть $g(x, y) = f(y_1, y_2, \ldots, y_n)$, де $y_{i_1} = x$, $y_{i_2} = \cdots = y_{i_m} = y$, $y_j = \mathbf{0}$, якщо $j \notin \{i_1, i_2, \ldots, i_m\}$; доведіть, що $g(x, y) = c_0 \oplus c_1 \wedge x \oplus c_2 \wedge y \oplus x \wedge y$ для деяких $c_k \in \mathbb{B}$.
2. Доведіть, що або g, або $\neg g$ збігається з однією з функцій $x \wedge y$, $x \vee y$, $x \wedge \neg y$, $\neg x \wedge y$.

Вправа А 11. З результатів вправ А 9 та А 10 виведіть *теорему Поста* (критерій повноти):

Множина булевих функцій $\mathcal{F}$ є повною тоді й лише тоді, коли $\mathcal{F} \not\subseteq \mathcal{F}_i$ при всіх $i \in \{0, 1, 2, 3, 4\}$.

Вправа А 12. 1. Припустимо, що всі булеві функції можна виразити через єдину двомісну функцію $f(x, y)$. Доведіть, що або $f(x, y) = \neg(x \vee y)$ («*штрих Шеффера*» $x|y$), або $f(x, y) = \neg(x \wedge y)$ («*стрілка Пірса*» $x \downarrow y$).

2. Скільки існує булевих функцій f від n змінних таких, що через f виражаються всі булеві функції?

Вправа А 13. 1. Доведіть, що коли $\mathcal{F}$ — повна множина булевих функцій, існує повна підмножина $\mathcal{F}' \subseteq \mathcal{F}$, яка містить щонайбільше 4 функцій.

2. В умовах попереднього пункту припустимо, що всі функції з $\mathcal{F}$ — двомісні. Доведіть, що тоді існує повна підмножина $\mathcal{F}' \subseteq \mathcal{F}$, яка містить щонайбільше 3 функції.
3. Знайдіть повну множину булевих функцій $\mathcal{F}$, яка містить 4 функції, причому жодна її власна підмножина $\mathcal{F}' \subset \mathcal{F}$ вже не є повною.

Додаток В

Булеві алгебри

Другий розділ, який пропонується читачу для самостійної розробки на підставі наведених нижче вправ — це теорія *булевих алгебр*. Знов-таки, це скоріше розділ алгебри, хоча й тісно пов'язаний з логікою.

Означення В 1. *Булевою алгеброю* зветься множина A з двома визначеними на ній бінарними алгебричними операціями $\vee$ та $\wedge$, які задовольняють наступні аксіоми:

(Б1) $x \vee x = x$,

(Б1*) $x \wedge x = x$,

(Б2) $x \vee y = y \vee x$,

(Б2*) $x \wedge y = y \wedge x$,

(Б3) $x \vee (y \vee z) = (x \vee y) \vee z$,

(Б3*) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$,

(Б4) існує елемент $\mathbf{0}$ такий, що $x \vee \mathbf{0} = x$ для всіх x,

(Б4*) існує елемент $\mathbf{1}$ такий, що $x \wedge \mathbf{1} = x$ для всіх x,

(Б5) $x \vee (x \wedge y) = x$,

(Б5*) $x \wedge (x \vee y) = x$,

(Б6) $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$,

(Б6*) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,

(Б7) для кожного x існує елемент $\neg x$ такий, що $x \vee \neg x = \mathbf{1}$ і $x \wedge \neg x = \mathbf{0}$.

Вправа В 2. Доведіть, що

(1) $x \wedge \mathbf{0} = \mathbf{0}$ і $x \vee \mathbf{1} = \mathbf{1}$.

(2) Аксіома Б6* випливає з попередніх аксіом та аксіоми Б6 (і навпаки).

(3) Елементи $\mathbf{0}$, $\mathbf{1}$ та $\neg x$ визначені однозначно.

(4) $\neg(\neg x) = x$.

(5) Доведіть, що $\neg(x \wedge y) = \neg x \vee \neg y$, а $\neg(x \vee y) = \neg x \wedge \neg y$.

Елемент $\neg x$ зветься *доповненням* елемента x. Формули (5) звуться *законами де Моргана*.

Приклад В 3.

1. Множина $\mathbb{B} = \{\, \mathbf{0}, \mathbf{1} \,\}$ з операціями, визначеними звичайними таблицями для кон'юнкції та диз'юнкції (див. стор. 6) є булевою алгеброю, яку ми будемо звати *первинною* булевою алгеброю. Це найменша булева алгебра, в якій $\mathbf{0} \neq \mathbf{1}$. (Зауважимо, що коли

в деякій булевій алгебрі $\mathbf{0} = \mathbf{1}$, то вона містить лише один цей елемент — це одразу випливає з аксіоми Б4 та вправи В 2(1).)

2. Множина $\mathfrak{P}(M)$ усіх підмножин деякої множини M є булевою алгеброю, в якій $A \vee B$ — об'єднання, а $A \wedge B$ переріз підмножин A та B.
3. Булеві функції від n змінних також утворюють булеву алгебру $\mathfrak{B}_n$ зі звичайними операціями $\vee$ та $\wedge$.
4. Будемо писати $\mathbf{A} \equiv \mathbf{B}$, де $\mathbf{A}, \mathbf{B}$ — речення логіки висловлювань, якщо $\mathbf{A} \models \mathbf{B}$ і $\mathbf{B} \models \mathbf{A}$. Нехай $\mathfrak{L}$ — множина класів еквівалентності речень за відношенням $\equiv$, а $[\mathbf{A}]$ — клас, якому належить речення $\mathbf{A}$. Визначимо на $\mathfrak{L}$ операції $\vee$ та $\wedge$, поклавши

$$[\mathbf{A}] \vee [\mathbf{B}] = [\mathbf{A} \vee \mathbf{B}] \quad \text{та} \quad [\mathbf{A}] \wedge [\mathbf{B}] = [\mathbf{A} \wedge \mathbf{B}].$$

   (Доведіть, що ці визначення коректні.) Тоді $\mathfrak{L}$ перетворюється на булеву алгебру. (Перевірте це.) Роль $\mathbf{1}$ відіграє клас тавтологій, а роль $\mathbf{0}$ — клас їх заперечень. Алгебра $\mathfrak{L}$ зветься *алгеброю Ліндербаума* логіки висловлювань.
5. Якщо $\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_n$ — булеві алгебри, їхній декартів добуток $\mathsf{A}_1 \times \mathsf{A}_2 \times \ldots \times \mathsf{A}_n$ перетворюється на булеву алгебру, якщо визначити операції покоординатно:

$$(a_1, a_2, \ldots, a_n) \vee (b_1, b_2, \ldots, b_n) = (a_1 \vee b_1, a_2 \vee b_2, \ldots, a_n \vee b_n),$$
$$(a_1, a_2, \ldots, a_n) \wedge (b_1, b_2, \ldots, b_n) = (a_1 \wedge b_1, a_2 \wedge b_2, \ldots, a_n \wedge b_n).$$

   Ця алгебра зветься *прямим добутком* алгебр $\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_n$. Якщо всі алгебри A_i збігаються з фіксованою алгеброю A, то ми позначатимемо цей добуток через A^n.
6. Для кожної булевої алгебри A визначимо *обернену алгебру* A° як таку, елементи якої ті самі, що й в алгебрі A, але $a \vee b$ у новій алгебрі збігається з $a \wedge b$ в A і навпаки. Доведіть, що A° — теж булева алгебра. Зокрема, для кожного твердження теорії булевих алгебр вірним є й обернене твердження, яке отримується перестановкою в усіх формулах знаків $\vee$ та $\wedge$.

Вправа В 4. Встановіть ізоморфізм булевих алгебр $\mathbb{B}^n \simeq \mathfrak{P}(M)$, де M — множина з n елементів.

Вказівка: Вважаючи, що $M = \{1, 2, \ldots, n\}$, зіставте кожному набору $(a_1, a_2, \ldots, a_n)$, де $a_i \in \mathbb{B}$, підмножину $M(a) = \{k \mid a_k = \mathbf{1}\}$.

Доведемо теорему, яка повністю описує будову всіх скінченних булевих алгебр.

Теорема В 5. *Довільна скінченна булева алгебра ізоморфна $\mathbb{B}^n$ для деякого n.*

Зокрема, така алгебра містить 2^n елементів.

Доведення цієї теореми розіб'ємо на кілька вправ. Почнемо з деяких означень. Далі A позначає деяку булеву алгебру, яка містить принаймні два елементи.

Означення В 6.

1. Уведемо в A (частковий) порядок, вважаючи, що $a \leqslant b$, якщо $a \vee b = b$. Доведіть, що:

(a) $a \leqslant b$ тоді й лише тоді, коли $a \wedge b = a$;
(b) відношення $\leqslant$ дійсно є (частковим) порядком на A;
(c) $\mathbf{0}$ є найменшим, а $\mathbf{1}$ — найбільшим елементом відносно цього порядку;
(d) якщо $a \leqslant b$, то $\neg b \leqslant \neg a$ і навпаки.

2. Елемент $a \in \mathsf{A}$ зветься *атомом*, якщо $a \neq \mathbf{0}$, але з $x < a$ випливає, що $x = \mathbf{0}$.
Не слід плутати це поняття з атомами (елементарними висловлюваннями) логіки висловлювань. У цьому розділі термін «атом» вживається лише в розумінні атомів булевих алгебр.

Вправа B 7. Нехай a — атом. Доведіть, що:

1. $\neg a \neq \mathbf{1}$, але з $\neg a < x$ випливає, що $x = \mathbf{1}$. Навпаки, якщо c — такий елемент, що $c \neq \mathbf{1}$, але з $c < x$ випливає, що $x = \mathbf{1}$, то $\neg c$ — атом.
2. Якщо $a \not\leqslant x$, то $a \wedge x = \mathbf{0}$; якщо $x \not\leqslant \neg a$, то $x \vee \neg a = \mathbf{1}$.
3. Якщо b — інший атоми, то $a \neq b$ тоді й лише тоді, коли $a \wedge \neg b = a$. (Зауважте, що коли $x \leqslant \neg x$, то $x = \mathbf{0}$.)

У скінченній булевій алгебрі завжди є атоми. Більш того, для кожного елемента $x \neq \mathbf{0}$ знайдеться такий атом a, що $a \leqslant x$ (чому?). Далі ми вважаємо алгебру A скінченною і позначаємо через $E = \{ a_1, a_2, \ldots, a_n \}$ множину всіх (попарно різних) атомів цієї алгебри.

Вправа B 8. Доведіть, що:

1. $a_1 \vee (\neg a_1 \wedge \neg a_2 \wedge \ldots \wedge \neg a_n) = a_1$.
2. $\neg a_1 \wedge \neg a_2 \wedge \ldots \wedge \neg a_n = \mathbf{0}$.
3. $a_1 \vee a_2 \vee \cdots \vee a_n = \mathbf{1}$.
4. Для довільного елемента $x \in \mathsf{A}$ позначимо
$$E(x) = \{ a \in E \mid a \leqslant x \}.$$
Тоді $x = \bigvee_{a \in E(x)} a$.

Останнє твердження показує, що елемент x повністю визначається підмножиною $E(x)$.

Вправа B 9. Доведіть, що
$$E(x) \vee E(y) = E(x \vee y) \quad \text{і} \quad E(x) \wedge E(y) = E(x \wedge y).$$

Отже, відображення $x \to E(x)$ є ізоморфізмом алгебри A на алгебру $\mathfrak{P}(E)$ підмножин у множині атомів E. Згідно з вправою B 4 остання ізоморфна $\mathbb{B}^n$, що й завершує доведення теореми B 5. Зокрема, алгебра $\mathfrak{B}_n$ булевих функцій від n змінних ізоморфна $\mathbb{B}^n$.

Вправа B 10.

1. Покажіть, що в алгебрі Лінденбаума $\mathfrak{L}$ (приклад B 3.4) немає атомів.
Вказівка: Якщо $\mathbf{E}$ — елементарне висловлювання, яке не входить до речення $\mathbf{A}$, то $\mathbf{A} \wedge \mathbf{E} < \mathbf{A}$.
2. Позначимо через $\mathfrak{L}_n$ підалгебру в $\mathfrak{L}$, утворену класами речень $[\mathbf{A}]$ таких, що $\mathbf{A}$ містить лише елементарні висловлювання $A_k = A||\ldots|$ (k разів '|') з $k < n$. Доведіть, що $\mathfrak{L}_n \simeq \mathfrak{B}_n$. Очевидно, $\mathfrak{L} = \bigcup_{n=1}^{\infty} \mathfrak{L}_n$.

3. Виведіть звідси, що алгебра Лінденбаума ізоморфна *прямій сумі* зліченної кількості алгебр $\mathbb{B}$, тобто підалгебрі прямого добутку $\mathbb{B} \times \mathbb{B} \times \ldots$, яка складається з тих (нескінченних) векторів $(a_1, a_2, \ldots, a_n, \ldots)$, в яких лише скінченна кількість координат a_i відмінна від $\mathbf{0}$.
4. Доведіть, що атомами булевої алгебри $\mathfrak{L}_n$ є класи кон'юнкцій $[B_0 \wedge B_1 \wedge \ldots B_{n-1}]$, де кожне B_k збігається або з елементарним висловлюванням A_k, або з $\neg A_k$.

Наступна вправа встановлює зв'язок булевих алгебр з теорією кілець.

Вправа В 11.

1. Нехай A — булева алгебра. Визначимо на множині A операцію «додавання» $\oplus$, поклавши $x \oplus y = (x \vee y) \wedge (\neg x \vee \neg y)$. Доведіть, що:
   (a) Операція $\oplus$ задовольняє аксіоми комутативної групи, нейтральним елементом якої є $\mathbf{0}$, а оберненим до x — $\neg x$.
   (b) $x \wedge (y \oplus z) = x \wedge y \oplus x \wedge z$. Отже, відносно операцій $\oplus$ («сума») та $\wedge$ («добуток») A є комутативним кільцем. Зауважимо, що всі елементи цього кільця — ідемпотенти (тобто $x \wedge x = x$).
2. Навпаки, нехай A — таке кільце, в якому $x^2 = x$ для всіх x. Доведіть, що:
   (a) $xy + yx = 0$ для всіх x; зокрема, коли $y = 1$, одержимо $x + x = 0$, тобто $x = -x$, звідки одержуємо також, що $xy = yx$.
   (b) Покладіть $x \wedge y = xy$, $x \vee y = x + y + xy$ і доведіть, що в такий спосіб A перетворюється на булеву алгебру. При цьому $\neg x = 1 + x$.

   Отже, з погляду теорії кілець, булеві алгебри — те саме, що кільця, які складаються з самих ідемпотентів (як ми бачили, кожне таке кільце комутативне, а його адитивна група — періоду 2.)
3. Перекладіть теорему В 5 мовою теорії кілець.

Розділ 2

Логіка відношень

2.1. Предикати та квантори

Логіка відношень, на відміну від логіки висловлювань, уже аналізує внутрішню будову речень, точніше, ту її частину, яка пов'язана зі вживанням слів «усі» («будь-які») та «існує» («для якогось»). Наприклад, у логіці висловлювань неможливо визначити, чи є правильним таке міркування:

- Усі студенти знають логіку.
- Петро — студент.
- Отже, Петро знає логіку.

Дійсно, у логіці висловлювань усі ці речення є елементарними (атомами), тобто не мають внутрішньої будови. Тому питання, чи є дане логічне міркування правильним, має таку формальну структуру: чи вірно, що $\mathbf{A}, \mathbf{B} \models \mathbf{C}$? Звичайно, у логіці висловлювань відповідь — «ні». У той же час зрозуміло, що насправді це міркування логічно правильне (безвідносно до того, чи дійсно всі студенти знають логіку, і чи дійсно Петро — студент). Саме такими міркування й займається логіка відношень, або логіка предикатів.

Коротко кажучи, *предикат* P — це формальне відбиття поняття функції, визначеної на деякій множині «елементів» M, яка набуває булевих значень $\mathbf{0}, \mathbf{1}$. У такому випадку стає змістовним питання про те, чи для всіх значень аргумента функція набуває значення $\mathbf{1}$, або чи знайдеться принаймні одне таке значення. Відповідні речення коротко записують у вигляді виразів на кшалт, відповідно, $\forall x P(\mathrm{x})$ та $\exists x P(\mathrm{x})$. Символи $\forall$ та $\exists$ звуть, відповідно, *квантором загальності* та *квантором існування*. Надалі з подібних виразів можна конструювати складені речення, користуючись логічними сполучниками, до цих речень знову приписувати квантори (можливо, кілька разів) і т.д.

Розглянемо один варіант формалізації логіки відношень, схожий на формалізацію логіки висловлювань з попереднього розділу.

Означення 2.1.1.

1. *Алфавіт* $\mathfrak{A}$ логіки відношень складається зі зліченого набору літер:
$$\mathrm{v}_n, \mathrm{p}_n^m, \mathrm{f}_n^m, \neg, \Rightarrow, \vee, \wedge, \forall, \exists, (,) \,,$$
де $m, n \in \mathbb{N} = \{\, 0, 1, 2, 3, \dots \}$.

   Літери v_n звуться *змінними*, літери p_n^m звуться *предикатами*, літери f_n^m звуться *функціоналами*. Число m у літерах p_n^m та f_n^m зветься *місністю*, або *арністю* відповідного предиката чи функціонала; кажуть, що предикат f_n^m або функціонал f_n^m є *m-арним*. 0-місні функціонали f_n^0 звуться також *константами*, а 0-місні

предикати p_n^0 — *висловлюваннями* (або *сталими висловлюваннями*).

2. *Термом* зветься слово в алфавіті $\mathfrak{A}$, побудоване за такими правилами:
   (a) змінна є термом;
   (b) якщо $\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m$ — терми, а F — m-місний функціонал, то $F\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$ — терм;
   (c) інших термів, крім побудованих за правилами (a),(b), не існує.

   Для виразності замість $F\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$ часто пишуть $F(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)$.
3. *Атомом* або *елементарним реченням* зветься слово в алфавіті $\mathfrak{A}$, яке має вигляд $P\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$, де P — деякий m-місний предикат, а $\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m$ — деякі терми (якщо $m = 0$, це слово має вигляд P, без переліку термів). Знов-таки, для виразності ми часто писатимемо $P(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)$ замість $P\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$.
4. *Реченням* логіки відношень зветься слово в алфавіті $\mathfrak{A}$, побудоване за такими правилами:
   (a) кожен атом є реченням;
   (b) якщо $\mathbf{A}, \mathbf{B}$ — речення, то $\neg\mathbf{A}, (\mathbf{A} \vee \mathbf{B}), (\mathbf{A} \wedge \mathbf{B}), (\mathbf{A} \Rightarrow \mathbf{B})$ — теж речення;
   (c) якщо $\mathbf{A}$ — речення, а x — змінна, то $\forall\mathrm{x}\mathbf{A}$ і $\exists\mathrm{x}\mathbf{A}$ — теж речення;
   (d) інших речень, крім побудованих за правилами (a),(b),(c), не існує.

Ось приклади термів:

$$\mathrm{f}_4^2\mathrm{v}_3\mathrm{v}_0,\ \mathrm{f}_6^3\mathrm{f}_1^1\mathrm{v}_7\mathrm{v}_5\mathrm{f}_1^1\mathrm{v}_5,\ \mathrm{f}_2^1\mathrm{f}_3^2\mathrm{v}_3\mathrm{f}_1^0$$

та атомів (елементарних речень):

$$\mathrm{p}_1^2\mathrm{v}_0\mathrm{v}_5,\ \mathrm{p}_2^3\mathrm{v}_1\mathrm{f}_2^2\mathrm{v}_1\mathrm{f}_3^0\mathrm{f}_2^2\mathrm{v}_5\mathrm{v}_2,\ \mathrm{p}_2^2\mathrm{f}_2^2\mathrm{v}_1\mathrm{v}_1\mathrm{f}_2^2\mathrm{v}_0\mathrm{f}_3^1\mathrm{v}_2$$

(перевірте, що це справді терми та атоми).

Так само, як і в першому розділі, ці означення цілком ефективні, тобто існує алгоритм перевірки, чи є задане слово реченням. Ми залишаємо побудову такого алгоритму читачу (один з варіантів неістотно відрізняється від запропонованого в зауваженні 1.2.2).

Зауваження. Ми запропонували варіант, в якому кількість літер нескінченна. Насправді, його легко перетворити на варіант, який має лише скінченну кількість літер. Для цього достатньо замість v_n, p_n^m та f_n^m писати, відповідно, $\mathrm{v}||\ldots|$, $\mathrm{p}||\ldots|*\ast\cdots\ast$ та $\mathrm{f}||\ldots|*\ast\cdots\ast$ з n символами $|$ та m символами $*$ (аналогічно тому, як ми робили це в логіці висловлювань).

Важливим поняттям логіки відношень, яке постійно зустрічатиметься надалі, є поняття *вільної змінної*. Це така змінна, від якої може залежати (хоча не обов'язково) логічне значення речення. Формальне означення базується на понятті *області квантора*.

Означення 2.1.2. Нехай $\mathrm{Q}\mathrm{x}$ — деяке входження квантора $\forall$ або $\exists$ до речення $\mathbf{A}$. Його *область* визначається такими правилами:

1. Якщо $\mathbf{A} = \mathrm{Qx}\mathbf{B}$ для деякої змінної x та деякого речення $\mathbf{B}$, то областю цього квантора є все речення $\mathbf{A}$; області дії кванторів, які входили до речення $\mathbf{B}$, не змінюються.
2. Якщо $\mathbf{A}$ має вигляд $\neg\mathbf{B}$, $\mathbf{B} \vee \mathbf{C}$, $\mathbf{B} \wedge \mathbf{C}$ або $\mathbf{B} \Rightarrow \mathbf{C}$, а Q входить до речення $\mathbf{B}$ ($\mathbf{C}$), то область квантора Qx в реченні $\mathbf{A}$ збігається з областю цього квантора в реченні $\mathbf{B}$ ($\mathbf{C}$).
3. Входження змінної x до речення $\mathbf{A}$ зветься *вільним*, якщо воно не належить області якогось квантора Qx, і *пов'язаним* (квантором Q), якщо воно належить такій області.
4. Кажуть, що x — *вільна змінна* речення $\mathbf{A}$, якщо в цьому реченні є принаймні одне вільне входження змінної x.
5. Речення $\mathbf{A}$ зветься *замкненим*, якщо в ньому немає жодної вільної змінної.
6. *Замиканням* речення $\mathbf{A}$ зветься замкнене речення $\forall \mathrm{x}_1\, \forall \mathrm{x}_2 \ldots \forall \mathrm{x}_n \mathbf{A}$, де $\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n$ — усі вільні змінні речення $\mathbf{A}$, узяті в порядку своїх номерів (тобто v_k іде перед v_m, якщо $k < m$).

Наприклад, у реченні

$$(\forall \mathrm{v}_3 \neg \mathrm{p}_2^3(\mathrm{v}_4, \mathrm{v}_1, \mathrm{v}_3)) \Rightarrow \exists \mathrm{v}_1(\mathrm{p}_2^2(\mathrm{v}_1, \mathrm{v}_5) \wedge \mathrm{p}_5^1(\mathrm{f}_3^2(\mathrm{v}_4, \mathrm{v}_1)))$$

вільними є змінні $\mathrm{v}_1, \mathrm{v}_4, \mathrm{v}_5$. Змінна v_3 пов'язана квантором $\forall$. Зауважимо, що змінна v_1 є вільною, хоча в частині $\exists \mathrm{v}_1(\mathrm{p}_2^2(\mathrm{v}_1, \mathrm{v}_5) \wedge \mathrm{p}_5^1(\mathrm{v}_4))$ вона пов'язана квантором $\exists$. Замиканням цього речення є речення

$$\forall \mathrm{v}_1 \forall \mathrm{v}_4 \forall \mathrm{v}_5((\forall \mathrm{v}_3 \neg \mathrm{p}_2^3(\mathrm{v}_4, \mathrm{v}_1, \mathrm{v}_3)) \Rightarrow \exists \mathrm{v}_1(\mathrm{p}_2^2(\mathrm{v}_1, \mathrm{v}_5) \wedge \mathrm{p}_5^1(\mathrm{f}_3^2(\mathrm{v}_4, \mathrm{v}_1)))).$$

Ось ще приклад замкненого речення:

$$\exists \mathrm{v}_2 \neg \forall \mathrm{v}_3(\mathrm{p}_1^1(\mathrm{v}_2) \vee \mathrm{p}_3^2(\mathrm{v}_3, \mathrm{f}_2^2(\mathrm{v}_2, \mathrm{v}_2)) \Rightarrow \exists \mathrm{v}_1(\mathrm{p}_3^2(\mathrm{v}_2, \mathrm{v}_1) \wedge \mathrm{p}_3^1(\mathrm{v}_3)))$$

(поясніть).

Наступна наша задача — визначити *семантику* логіки відношень, тобто спосіб, у який речення набувають логічних значень. Відповідне означення істотно складніше ніж у логіці висловлювань, особливо в частині, де фігурують квантори.

Означення 2.1.3.

1. *Інтерпретація* $\mathcal{I}$ логіки відношень складається з таких частин:
   (a) деякої непорожньої множини $M = M(\mathcal{I})$, яка зветься *областю інтерпретації* $\mathcal{I}$;
   (b) відображення, яке кожному m-місному предикату P ставить у відповідність функцію $\mathcal{I}(P) : M^m \to \mathbb{B}$ (зокрема, якщо $m = 0, \mathcal{I}(P) \in \mathbb{B}$ — булева стала);
   (c) відображення, яке кожному m-місному функціоналу F ставить у відповідність функцію $\mathcal{I}(F) : M^n \to M$ (зокрема, якщо $m = 0, \mathcal{I}(F) \in M$ — фіксований елемент).
2. *Розподілом* (в інтерпретації $\mathcal{I}$) зветься відображення $\phi : \mathfrak{X} \to M$, де $\mathfrak{X}$ — множина змінних.
3. Якщо ϕ — розподіл, а x — змінна, то через ϕ^{x} позначається множина всіх таких розподілів ψ, що $\psi(\mathrm{y}) = \phi(\mathrm{y})$ для всіх змінних $\mathrm{y} \neq \mathrm{x}$.
4. *Значення* $\phi(\mathrm{t})$ *терма* t на розподілі ϕ визначається такими правилами:

(a) якщо $\mathrm{t} = \mathrm{v}_n$, то $\phi(\mathrm{t}) = \phi(\mathrm{v}_n)$;
(b) якщо $\mathrm{t} = F\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$, де F — m-місний функціонал, то $\phi(\mathrm{t}) = \mathcal{I}(F)(\phi(\mathrm{t}_1), \phi(\mathrm{t}_2), \ldots, \phi(\mathrm{t}_m))$.

5. *Значення* $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A})$ *речення* $\mathbf{A}$ на розподілі ϕ в інтерпретації $\mathcal{I}$ визначається такими правилами:
(a) якщо $\mathbf{A} = P\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$ — елементарне речення, то
$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathcal{I}(P)(\phi(\mathrm{t}_1), \phi(\mathrm{t}_2), \ldots, \phi(\mathrm{t}_m));$$
(b) Якщо $\mathbf{A} = \neg\mathbf{B}$, то
$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathbf{1}, \\ \mathbf{1}, & \text{якщо } \mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathbf{0}. \end{cases}$$
(c) Якщо $\mathbf{A} = (\mathbf{B} \vee \mathbf{C})$, то
$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathrm{val}(\mathcal{I}, \phi, \mathbf{C}) = \mathbf{0}, \\ \mathbf{1}, & \text{інакше.} \end{cases}$$
(d) Якщо $\mathbf{A} = (\mathbf{B} \wedge \mathbf{C})$, то
$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \begin{cases} \mathbf{1}, & \text{якщо } \mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathrm{val}(\mathcal{I}, \phi, \mathbf{C}) = \mathbf{1}, \\ \mathbf{0}, & \text{інакше.} \end{cases}$$
(e) Якщо $\mathbf{A} = (\mathbf{B} \Rightarrow \mathbf{C})$, то
$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \begin{cases} \mathbf{0}, & \text{якщо } \mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathbf{1}, \text{ а } \mathrm{val}(\mathcal{I}, \phi, \mathbf{C}) = \mathbf{0}, \\ \mathbf{1}, & \text{інакше.} \end{cases}$$
(f) $\mathrm{val}(\mathcal{I}, \phi, \forall\mathrm{x}\mathbf{A}) = \min\{\, \mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) \mid \psi \in \phi^{\mathrm{x}} \,\}$;
(g) $\mathrm{val}(\mathcal{I}, \phi, \exists\mathrm{x}\mathbf{A}) = \max\{\, \mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) \mid \psi \in \phi^{\mathrm{x}} \,\}$.

В останніх двох рядках покладаємо, як і раніше, що $\mathbf{0} < \mathbf{1}$. Тому фактично $\mathrm{val}(\mathcal{I}, \phi, \forall\mathrm{x}\mathbf{A}) = \mathbf{1}$ тоді й лише тоді, коли $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathbf{1}$ для кожного розподілу ψ, який відрізняється від ϕ щонайбільше значенням на змінній x, а $\mathrm{val}(\mathcal{I}, \phi, \exists\mathrm{x}\mathbf{A}) = \mathbf{1}$ тоді й лише тоді, коли $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$ принаймні для одного з таких розподілів.

Зауважимо, що на відміну від свого аналога в логіці висловлювань, останнє означення *не є ефективним*, якщо область інтерпретації нескінченна (а саме такі інтерпретації найбільш цікаві, наприклад, коли йдеться про математичні теорії). Це одразу робить логіку відношень незрівнянно складнішою за логіку висловлювань. Це не випадково: надалі ми побачимо, що багато змістовних математичних теорій можуть бути формально описані мовою логіки відношень.

Назва «*логіка відношень*» пов'язана з тим, що функції $f : M^n \to \mathbb{B}$ звуться *n-місними* (або *n-арними*) *відношеннями* на множині M. Отже, значення $\mathcal{I}(P)$, де $\mathcal{I}$ — інтерпретація, а P — n-місний предикат, є n-місним відношенням на множині M (області цієї інтерпретації). У багатьох підручниках з логіки для таких відношень також застосовується термін «предикат», а логіка відношень зветься «логікою предикатів». Ми віддаємо перевагу назві «логіка відношень», оскільки термін «відношення» набагато більш уживаний у математиці. Назву «предикат» ми залишаємо для формальних символів, які набувають значення відношень у

конкретних інтерпретаціях. Досить часто відношення f ототожнюється з підмножиною $M = \{\, \mathbf{a} \in \mathbb{N}^n \mid f(\mathbf{a}) = \mathbf{1} \,\}$. Ми будемо інколи так робити в наступному розділі.

Відзначимо один простий, але дуже важливий результат.

Твердження 2.1.4. *Припустимо, що змінна* x *не є вільною в реченні* $\mathbf{A}$*, а* ψ *та* ϕ *— такі розподіли, що* $\psi \in \phi^{\mathrm{x}}$*. Тоді* $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathrm{val}(\mathcal{I}, \psi, \mathbf{A})$*. Отже, значення речення* $\mathbf{A}$ *на деякому розподілі* ϕ *залежить лише від значень цього розподілу на тих змінних, які є вільними в* $\mathbf{A}$*. Зокрема, якщо речення* $\mathbf{A}$ *замкнене, значення* $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A})$ *взагалі не залежить від розподілу* ϕ*. Надалі ми позначатимемо його* $\mathrm{val}(\mathcal{I}, \mathbf{A})$.

Доведення. Скористаємося індукцією за довжиною речення $\mathbf{A}$. Якщо $\mathbf{A}$ елементарне, то x узагалі не зустрічається в ньому, і твердження очевидне. Якщо $\mathbf{A} = \mathrm{Q}\mathrm{x}\mathbf{B}$ для деякого квантора Q, це випливає з означення, оскільки $\psi^{\mathrm{x}} = \phi^{\mathrm{x}}$. Якщо ж $\mathbf{A}$ має вигляд $\neg\mathbf{B}$, $\mathbf{B} \Rightarrow \mathbf{C}$, $\mathbf{B} \vee \mathbf{C}$, $\mathbf{B} \wedge \mathbf{C}$ або $\mathrm{Q}\mathrm{y}\mathbf{B}$ для деякого квантора Q та деякої змінної $\mathrm{y} \neq \mathrm{x}$, то, згідно з означенням 2.1.2, x не є вільною змінною ані у $\mathbf{B}$, ані в $\mathbf{C}$. За припущенням індукції, їхні значення на розподілах ψ та ϕ збігаються, а тоді те саме вірне й для значення речення $\mathbf{A}$ □

Означення 2.1.5. Кажуть, що речення $\mathbf{A}$

(1) *тотожно-істинне в інтерпретації* $\mathcal{I}$, якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$ на кожному розподілі ϕ в цій інтерпретації;
(2) *тотожно-істинне на множині* M, якщо воно тотожно-істинне в кожній інтепретації з областю M;
(3) *тотожно-істинне*, якщо воно тотожно-істинне на кожній множині.

Це позначається, відповідно, $\models_{\mathcal{I}} \mathbf{A}$, $\models_M \mathbf{A}$ та $\models \mathbf{A}$.

Розглянемо деякі приклади. Перш за все виділимо один важливий клас тотожно-істинних речень.

Твердження 2.1.6. *Нехай* $\mathbf{R}$ *— деяке речення логіки висловлювань,* $\mathbf{E}_1, \mathbf{E}_2, \ldots, \mathbf{E}_n$ *— усі атоми логіки висловлювань, які до нього входять, і* $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ *— деякі речення логіки відношень. Позначимо через* $\mathbf{R}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$ *речення, одержане з* $\mathbf{R}$ *підстановкою замість кожного атома* $\mathbf{E}_i$ *речення* $\mathbf{A}_i$ *(з тим самим номером). Тоді* $\mathbf{R}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$ *є реченням логіки відношень, причому якщо* $\mathbf{R}$ *— тавтологія, то* $\mathbf{R}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$ *— тотожно-істинне.*

В останньому випадку кажуть, що $\mathbf{R}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$ *— підстановковий випадок тавтології* (ПВТ).

Доведення цього факту (індукцією за довжиною речення $\mathbf{R}$) цілком очевидне, і ми залишаємо його читачу.

Зокрема, для довільних речень $\mathbf{A}, \mathbf{B}, \mathbf{C}$ логіки відношень речення вигляду (A1)–(A10) зі вправи 1.2.6 є тотожно-істинними.

Ось менш елементарні приклади.

Твердження 2.1.7.

1. *Нехай* $\mathbf{A}$ *— деяке речення логіки відношень,* x *— змінна,* t *— терм і* $y_1, y_2, \ldots, y_m$ *— усі змінні, які входять до терма* t*. Кажуть, що терм* t *є* вільним для x в $\mathbf{A}$*, якщо жодне вільне входження* x *у речення* $\mathbf{A}$ *не знаходиться в області жодного квантора вигляду* $\mathrm{Q}y_i$ $(i = 1, 2, \ldots, m)$*. Позначимо через* $\mathbf{A}^{\mathrm{x}}_{\mathrm{t}}$ *речення, яке одержується з* $\mathbf{A}$ *підстановкою* t *замість кожного вільного входження змінної* x*. Якщо терм* t *є вільним для* x *в* $\mathbf{A}$*, то такі речення тотожно-істинні:*

(A11) $$\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{t}},$$

(A12) $$\mathbf{A}^{\mathrm{x}}_{\mathrm{t}} \Rightarrow \exists \mathrm{x}\mathbf{A}.$$

2. *Нехай* $\mathbf{A}$, $\mathbf{B}$ *— речення логіки відношень, а* x *— змінна, яка не є вільною в реченні* $\mathbf{A}$*. Тоді такі речення тотожно-істинні:*

(A13) $$\forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}),$$

(A14) $$\forall \mathrm{x}(\mathbf{B} \Rightarrow \mathbf{A}) \Rightarrow (\exists \mathrm{x}\mathbf{B} \Rightarrow \mathbf{A}).$$

Доведення. Ми доведемо, що тотожно-істинними є речення вигляду (A12) та (A13), залишивши останні два випадки як вправу.

(A12) Згадаємо, що єдиним випадком, коли ця імплікація хибна, є той, коли $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}^{\mathrm{x}}_{\mathrm{t}}) = \mathbf{1}$, а $\mathrm{val}(\mathcal{I}, \phi, \exists \mathrm{x}\mathbf{A}) = \mathbf{0}$. Треба довести, що це неможливо. Дійсно, нехай $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}^{\mathrm{x}}_{\mathrm{t}}) = \mathbf{1}$. Розглянемо розподіл ψ такий, що

$$\psi(\mathrm{y}) = \begin{cases} \phi(\mathrm{y}) & \text{якщо } \mathrm{y} \neq \mathrm{x}, \\ \phi(\mathrm{t}) & \text{якщо } \mathrm{y} = \mathrm{x}. \end{cases}$$

Очевидно, $\psi \in \phi^{\mathrm{x}}$ і $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathrm{val}(\mathcal{I}, \phi, \mathbf{A}^{\mathrm{x}}_{\mathrm{t}}) = \mathbf{1}$, звідки, за правилом (g), також $\mathrm{val}(\mathcal{I}, \phi, \exists \mathrm{x}\mathbf{A}) = \mathbf{1}$.

(A13) Знов-таки треба довести, що коли $\mathrm{val}(\mathcal{I}, \phi, \forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B})) = \mathbf{1}$, тобто $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A} \Rightarrow \mathbf{B}) = \mathbf{1}$ для всіх $\psi \in \phi^{\mathrm{x}}$, то й $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}) = \mathbf{1}$, тобто неможливо, щоб $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$, а $\mathrm{val}(\mathcal{I}, \phi, \forall \mathrm{x}\mathbf{B}) = \mathbf{0}$. Розглянемо довільний розподіл $\psi \in \phi^{\mathrm{x}}$. Тоді, за твердженням 2.1.4, $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$. Оскільки $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A} \Rightarrow \mathbf{B}) = \mathbf{1}$, також $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{1}$. Отже, і $\mathrm{val}(\mathcal{I}, \phi, \forall \mathrm{x}\mathbf{B}) = \mathbf{1}$ □

Зауважимо, що змінна x напевне є вільною для x у кожному реченні й $\mathbf{A}^{\mathrm{x}}_{\mathrm{x}} = \mathbf{A}$. Тому частковими випадками речень вигляду (A11–12) є всі речення вигляду $\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}$ і $\forall \Rightarrow \exists \mathrm{x}\mathbf{A}$.

Вправа 2.1.8.

1. Нехай $\mathrm{Q}\mathrm{x}$ — деяке входження квантора Q до речення $\mathbf{A}$, y — така змінна, яка не зустрічається в області цього входження, а речення $\mathbf{B}$ одержане з $\mathbf{A}$ заміною x всюди в цій області на y. Доведіть, що $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathrm{val}(\mathcal{I}, \phi, \mathbf{B})$ для довільної інтерпретації $\mathcal{I}$ та довільного розподілу ϕ.
2. Доведіть, що речення $\mathbf{A}$ є тотожно-істинним в інтерпретації $\mathcal{I}$ (або на множині M) тоді й лише тоді, коли таким є речення $\forall \mathrm{x}\mathbf{A}$, де x — довільна змінна. Зокрема, $\mathbf{A}$ є тотожно-істинним в інтерпретації $\mathcal{I}$ (або на множині M) тоді й лише тоді, коли таким є його замикання.

3. Наведіть приклад, який показує, що речення вигляду $\mathbf{A} \Rightarrow \forall x\mathbf{A}$ може не бути тотожно-істинним.

2.2. Теорії першого порядку. Моделі

Означення 2.2.1.

1. *Теорією першого порядку* зветься довільна множина $\mathfrak{T}$ речень логіки відношень. Кажуть, що предикат або функціонал (зокрема, висловлювання або константа) *належить теорії* $\mathfrak{T}$, або теорія $\mathfrak{T}$ *містить* цей предикат або функціонал, якщо він зустрічається принаймні в одному з речень, які належать $\mathfrak{T}$. Кажуть, що речення $\mathbf{A}$ є *реченням теорії* $\mathfrak{T}$, якщо воно містить лише ті предикати та функціонали, які належать теорії $\mathfrak{T}$.
2. *Моделлю* теорії $\mathfrak{T}$ зветься така інтерпретація $\mathcal{I}$, що $\models_{\mathcal{I}} \mathbf{A}$ для всіх речень $\mathbf{A} \in \mathfrak{T}$. Якщо M — область цієї інтерпретації, кажуть, що $\mathcal{I}$ — модель теорії $\mathfrak{T}$ на множині M. Потужність множини M звуть також *потужністю моделі* $\mathcal{I}$.

Речення з $\mathfrak{T}$ у математиці часто звуть *постулатами* цієї теорії. Ми не вживатимемо для них назву «*аксіоми*», оскільки в логіці цю назву використовують у зовсім іншому значенні при аксіоматизації того чи іншого розділу формальної логіки. Оскільки термін «теорія» в цій книзі не буде використовуватись в іншому розумінні, ми часто називатимемо теорію першого порядку просто «теорія».

Очевидно, при перевірці того, чи є інтерпретація $\mathcal{I}$ моделлю теорії $\mathfrak{T}$, достатньо знати значення $\mathcal{I}(P)$ та $\mathcal{I}(F)$ лише для предикатів та функціоналів, які належать теорії $\mathfrak{T}$. Тому при розгляді моделей ми задаватимемо лише значення цих предикатів та функціоналів. У багатьох випадках таких предикатів та функціоналів узагалі лише скінченна кількість. Якщо теорія не містить жодного функціонала, кажуть, що це — *чиста* теорія першого порядку. Зокрема, *чиста логіка відношень* має порожні множини функціоналів та постулатів. Зауважимо, що згідно із вправою 2.1.8.2, інтерпретація $\mathcal{I}$ є моделлю теорії $\mathfrak{T}$ тоді й лише тоді, коли вона є моделлю теорії, яка одержується з $\mathfrak{T}$ заміною всіх речень їхніми замиканнями. Тому ми завжди можемо обмежитись розглядом теорій, які складаються із самих замкнених речень. Це буває дуже зручно при доведенні багатьох загальних результатів. Утім, при розгляді конкретних теорій, як правило, перевага надається більш короткому запису без кванторів узагальнення.

Значні фрагменти змістовних математичних теорій можна подати як теорії першого порядку. Одну з них — формальну арифметику — ми детально вивчимо в наступних розділах. А зараз розглянемо ще кілька прикладів. Зауважимо, що в математиці особливу роль відіграє відношення *рівності*. Тому ми одразу виділимо клас теорій та інтерпретацій, які спеціально пристосовані до цієї обставини.

Означення 2.2.2.

1. Теорія першого порядку $\mathfrak{T}$ зветься *теорією першого порядку з рівністю* (або коротше *теорією з рівністю*), якщо вона містить

двомісний предикат E та постулати

(E1) $\qquad E\mathrm{v}_0\mathrm{v}_0,$

(E2$_{F,k,l}$) $\qquad E\mathrm{v}_0\mathrm{v}_1 \Rightarrow E(F\mathbf{u}\mathrm{v}_0\mathbf{v}, F\mathbf{u}\mathrm{v}_1\mathbf{v}),$

(E3$_{P,k,l}$) $\qquad E\mathrm{v}_0\mathrm{v}_1 \Rightarrow (P\mathbf{u}\mathrm{v}_0\mathbf{v} \Rightarrow P\mathbf{u}\mathrm{v}_1\mathbf{v})),$

де в реченнях (E2) та (E3) F і P позначають, відповідно, довільний функціонал або предикат, який належить теорії $\mathfrak{T}$, $\mathbf{u} = \mathrm{v}_2 \dots \mathrm{v}_{k+1}$ і $\mathbf{v} = \mathrm{v}_{k+2} \dots \mathrm{v}_{k+l+1}$, де k, l — довільні невід'ємні числа такі, що $k + l + 1 = n$, якщо функціонал F або предикат P є n-місним.

2. Модель $\mathcal{I}$ теорії з рівністю $\mathfrak{T}$ зветься *нормальною*, якщо $\mathcal{I}(E)$ — відношення рівності, тобто $\mathcal{I}(E)(a, b)) = \mathbf{1}$ тоді й лише тоді, коли $a = b$.

Аксіоми (E2) та (E3) формалізують той факт, що значення функцій (зокрема, відношень) не змінюються, якщо якийсь елемент замінити на рівний йому. Надалі при розгляді теорій з рівністю будемо писати $\mathrm{t} = \mathrm{t}'$ замість $E\mathrm{t}\mathrm{t}'$. Зауважимо, що коли теорія $\mathfrak{T}$ містить лише скінченну кількість функціоналів та предикатів, то й речень вигляду (E2) та (E3) теж є лише скінченна кількість.

Наведемо приклади теорій першого порядку, які формалізують змістовні математичні теорії. У цих прикладах ми будемо позначати літерами $\mathrm{x}, \mathrm{y}, z, \mathrm{t}, \dots$ деякий фіксований набір змінних (наприклад, $\mathrm{v}_0, \mathrm{v}_1, \mathrm{v}_2, \mathrm{v}_3, \dots$).

Приклад 2.2.3.

1. Нехай теорія $\mathfrak{O}$ складається з двох речень:

$$L(\mathrm{x}, \mathrm{y}) \Rightarrow \neg L(\mathrm{y}, \mathrm{x}),$$
$$L(\mathrm{x}, \mathrm{y}) \wedge L(\mathrm{y}, \mathrm{z}) \Rightarrow L(\mathrm{x}, \mathrm{z}),$$

де L — деякий двомісний предикат. Інтерпретація $\mathcal{I}$ є моделлю цієї теорії тоді й лише тоді, коли відношення $\mathcal{I}(L)$ є відношенням (часткового) *строгого порядку*. Тому теорію $\mathfrak{O}$ можна назвати *теорією (часткового) порядку*. Зауважимо, що дана теорія є чистою теорією першого порядку.

2. Нехай теорія з рівністю $\mathfrak{G}$ містить один двомісний функціонал P та одну константу e і складається з речень

(i) $\qquad P(\mathrm{x}, P(\mathrm{y}, z)) = P(P(\mathrm{x}, \mathrm{y}), z),$

(ii) $\qquad P\mathrm{e}\mathrm{x} = \mathrm{x} \wedge P\mathrm{x}\mathrm{e} = \mathrm{x},$

(iii) $\qquad \exists \mathrm{y} P\mathrm{x}\mathrm{y} = \mathrm{e} \wedge P\mathrm{y}\mathrm{x} = \mathrm{e}.$

Нормальні моделі цієї теорії — це групи. Функція $\mathcal{I}(P) : M \times M \to M$ — це добуток елементів; постулат (i) виражає асоціативність цього добутку; постулат (ii) твердить, що $\mathcal{I}(\mathrm{e})$ — нейтральний елемент (одиниця групи), а постулат (iii) — що у кожного елемента є обернений. Тому теорія $\mathfrak{G}$ зветься *теорією груп*.

3. *Теорією полів* зветься теорія першого порядку з рівністю $\mathfrak{F}$, яка містить два двомісних функціонала S, P, дві константи o, e і складається з речень

$$S(\mathrm{x}, S(\mathrm{y}, z)) = S(S(\mathrm{x}, \mathrm{y}), z),$$
$$S\mathrm{xy} = S\mathrm{yx},$$
$$S\mathit{x}\mathrm{o} = \mathrm{x},$$
$$\exists \mathrm{y} S\mathrm{xy} = \mathrm{o},$$

$$P(\mathrm{x}, P(\mathrm{y}, z)) = P(P(\mathrm{x}, \mathrm{y}), z),$$
$$P\mathrm{xy} = P\mathrm{yx},$$
$$P\mathrm{xe} = \mathrm{x},$$
$$\neg \mathrm{x} = \mathrm{o} \Rightarrow \exists \mathrm{y} P\mathrm{xy} = \mathrm{e},$$
$$P(\mathrm{x}, S\mathrm{yz}) = S(P\mathrm{xy}, P\mathrm{xz}).$$

Нормальна модель $\mathcal{I}$ теорії $\mathfrak{F}$ — це поле: функція $\mathcal{I}(S)$ — це сума елементів, $\mathcal{I}(P)$ — їхній добуток; $\mathcal{I}(\mathrm{o})$ — нуль, а $\mathcal{I}(\mathrm{e})$ — одиниця цього поля.

4. Останній з наших прикладів — це *елементарна теорія дійсних чисел* $\mathfrak{R}$. Вона містить дві константи o, e, два функціонали S, P і один предикат L. Постулатами цієї теорії є всі постулати теорій $\mathfrak{O}$ та $\mathfrak{F}$, а також такі:

$$\neg \mathrm{x} = \mathrm{y} \Rightarrow L\mathrm{xy} \vee L\mathrm{yx},$$

(це означає, що порядок є *лінійним*)

$$L\mathrm{xy} \Rightarrow L(S\mathrm{xz}, S\mathrm{yz}),$$
$$L\mathrm{oz} \vee L\mathrm{xy} \Rightarrow L(P\mathrm{xz}, P\mathrm{yz}),$$

(це означає, що порядок *узгоджений з діями в полі*)

$$(\exists \mathrm{x}\mathbf{A} \wedge \exists \mathrm{y} \forall \mathrm{x}(\mathbf{A} \Rightarrow L\mathrm{xy})) \Rightarrow$$
$$\Rightarrow (\exists \mathrm{y}((\forall \mathrm{x}(\mathbf{A} \Rightarrow L\mathrm{xy} \vee \mathrm{x} = \mathrm{y})) \wedge$$
$$\wedge \forall z(L\mathrm{zy} \Rightarrow \exists \mathrm{x}(L\mathrm{zx} \wedge \neg \mathbf{A}))),$$

де $\mathbf{A}$ — довільне речення теорії $\mathfrak{R}$, яке містить єдину вільну змінну x. Постулатів такого вигляду, очевидно, є нескінченно багато. Вони виражають той факт, що коли множина елементів, для яких речення $\mathbf{A}$ істинне, непорожня й обмежена зверху, то ця множина має точну верхню грань. Тому неважко збагнути, що поле дійсних чисел із звичайними діями та відношенням порядку є моделлю теорії $\mathfrak{R}$.

Зауважимо, що далеко не всі підмножини множини дійсних чисел можна задати реченням теорії $\mathfrak{R}$. Це цілком очевидно, бо множина таких речень зліченна, а вже сама множина дійсних чисел незліченна, не кажучи про множину її підмножин. Ми побачимо надалі, що це призводить до того, що існують моделі теорії $\mathfrak{R}$, які дуже відрізняються від поля дійсних чисел. Наприклад, деякі з них є зліченними, інші є *неархімедовими*, тобто містять

пари додатних елементів a, b таких, що $na < b$ для довільного натурального числа n. У сучасній алгебрі моделі теорії $\mathfrak{R}$ звуться *формально дійсними полями* і відіграють істотну роль у багатьох питаннях.

Для теорій з рівністю розгляд нормальних моделей не є істотним обмеженням, як показує такий результат.

Теорема 2.2.4. *Нехай $\mathfrak{T}$ — теорія з рівністю, $\mathcal{I}$ — її модель з областю M.*

1. *Відношення $\sim = \mathcal{I}(E)$ є відношенням еквівалентності на множині M.*
2. *Позначимо $\widetilde{M} = M/\sim$ множину класів еквівалентності за відношенням $\sim$. Правила*

$$\widetilde{\mathcal{I}}(F)(A_1, A_2, \ldots, A_n) = \mathcal{I}(F)(a_1, a_2, \ldots, a_n), \qquad \text{де } a_i \in A_i,$$

$$\widetilde{\mathcal{I}}(P)(A_1, A_2, \ldots, A_n) = \mathcal{I}(P)(a_1, a_2, \ldots, a_n), \qquad \text{де } a_i \in A_i,$$

де F (P) — n-місний функціонал (предикат), коректно визначають інтерпретацію $\widetilde{\mathcal{I}}$ з областю $\widetilde{M}$, тобто значення правих частин не змінюються, якщо замінити a_i на інші елементи $b_i \in A_i$.

3. *$\widetilde{\mathcal{I}}$ є нормальною моделлю теорії $\mathfrak{T}$.*

Доведення. 1. З постулатів (E1), (E3$_{E,0,1}$) та (E3$_{E,1,0}$) випливає, що коли $a \sim b$, то й $b \sim a$, а також коли $a \sim b$ та $a \sim c$, то й $b \sim c$. Отже, дійсно, $\sim$ — відношення еквівалентності.

Твердження 2 є безпосереднім наслідком постулатів (E2) та (E3).

3. Нехай $a \in A$, $b \in B$ для деяких класів A, B. За означенням, $\widetilde{\mathcal{I}}(E)(A, B) = \mathcal{I}(E)(a, b) = \mathbf{1}$ тоді й лише тоді, коли $a \sim b$, тобто $A = B$. Отже, інтерпретація $\mathcal{I}$ нормальна. Якщо $\mathbf{A}$ — довільне речення теорії $\mathfrak{T}$, то його значення в інтерпретації $\widetilde{\mathcal{I}}$ на розподілі ϕ збігається зі значенням $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A})$, де ψ — довільний розподіл, в якому $\psi(\mathrm{x}) \in \phi(\mathrm{x})$ для кожної змінної x. Це випливає з означення інтерпретації $\widetilde{\mathcal{I}}$ для елементарних речень, звідки легко виводиться очевидною індукцією для довільних речень теорії $\mathfrak{T}$. Тому, зокрема, усі речення з $\mathfrak{T}$ є тотожно-істинними в інтерпретації $\widetilde{\mathcal{I}}$, оскільки вони є такими в інтепретації $\mathcal{I}$. Отже, $\widetilde{\mathcal{I}}$ дійсно є нормальною моделлю теорії $\mathfrak{T}$ □

Означення 2.2.5. Нехай $\mathfrak{T}$ — теорія першого порядку.

1. Кажуть, що теорія $\mathfrak{T}$ *сумісна*, якщо існує її модель, і *несумісна*, якщо жодної моделі теорії $\mathfrak{T}$ не існує.
2. Кажуть, що речення $\mathbf{A}$ є *істинним в теорії* $\mathfrak{T}$, і пишуть $\mathfrak{T} \models \mathbf{A}$, якщо $\models_{\mathcal{I}} \mathbf{A}$ для довільної моделі $\mathcal{I}$ теорії $\mathfrak{T}$.

Зокрема, кожне речення є істинним у довільній несумісній теорії.

Твердження 2.2.6. 1. *Теорія $\mathfrak{T}$ сумісна тоді й лише тоді, коли такою є теорія $\bar{\mathfrak{T}}$, яка складається із замикань усіх речень теорії $\mathfrak{T}$.*

2. *Замкнене речення $\mathbf{A}$ є істинним у теорії $\mathfrak{T}$ тоді й лише тоді, коли теорія $\mathfrak{T} \cup \{ \mathbf{A} \}$ несумісна.*

3. *Теорія* $\mathfrak{T}$ *несумісна тоді й лише тоді, коли існує речення* $\mathbf{A}$ *таке, що* $\mathfrak{T} \models \mathbf{A}$ *і* $\mathfrak{T} \models \neg\mathbf{A}$.

Доведення очевидне.

Вправа 2.2.7. Нехай $\mathfrak{T}$ — деяка теорія першого порядку.

1. Доведіть, що коли існує модель $\mathfrak{T}$ на множині M, то існує модель цієї теорії на довільній множині N, потужність якої не менша за потужність M.
2. Наведіть приклад сумісної теорії, яка не має:
   (a) моделей на множині, кількість елементів якої менша за m, де m — задане натуральне число;
   (b) моделей на скінченній множині.
3. Наведіть приклад сумісної теорії з рівністю, яка має нормальні моделі лише на множинах з m елементами, де m — задане натуральне число.

2.3. Аксіоматика логіки відношень

Так само, як для логіки висловлювань, для логіки відношень виникає задача про аксіоматизацію, тобто заміни семантики синтаксисом. Більш того, тут це має принципове значення, бо, як відзначено вище, семантика логіки відношень, на відміну від семантики логіки висловлювань, неефективна. Ми наведемо варіант аксіоматизації логіки відношень, який близький до аксіоматизації логіки висловлювань і має схожі властивості.

Означення 2.3.1.

1. *Аксіомами* числення відношень звуться всі речення вигляду (A1–A10) із вправи 1.2.6, де $\mathbf{A}, \mathbf{B}, \mathbf{C}$ — довільні речення логіки відношень, а також речення вигляду (A11–A14) із твердження 2.1.7, де $\mathbf{A}$ і $\mathbf{B}$ — довільні речення, які задовольняють вказані там вимоги.
2. *Правилами виводу* числення відношень є правило modus ponens
$$\frac{\mathbf{A} \Rightarrow \mathbf{B},\ \mathbf{A}}{\mathbf{B}},$$
де $\mathbf{A}, \mathbf{B}$ — довільні речення, а також *правило узагальнення*, яке виражається схемою
$$\frac{\mathbf{A}}{\forall \mathrm{x}\mathbf{A}},$$
де $\mathbf{A}$ — довільне речення, а x — довільна змінна.

Так само, як у численні висловлювань, визначається поняття виводу.

Означення 2.3.2. Послідовність речень $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ зветься *виводом* речення $\mathbf{A}$ з теорії (тобто множини речень) $\mathfrak{T}$, якщо $\mathbf{A}_n = \mathbf{A}$ і для кожного номера $i = 1, 2, \ldots, n$ виконується одна з таких можливостей:

1. $\mathbf{A}_i$ є аксіомою.
2. $\mathbf{A}_i \in \mathfrak{T}$.
3. Існують такі номери $j < i$ та $k < i$, що $\mathbf{A}_j = \mathbf{A}_k \Rightarrow \mathbf{A}_i$. («$\mathbf{A}_i$ одержане з $\mathbf{A}_j$ та $\mathbf{A}_k$ за modus ponens».)
4. Існує номер $j < i$ такий, що $\mathbf{A}_i = \forall \mathrm{x}\mathbf{A}_j$, де x — деяка змінна. («$\mathbf{A}_i$ одержане з $\mathbf{A}_j$ узагальненням за змінною x».)

Якщо такий вивід існує, кажуть, що $\mathbf{A}$ *виводиться в теорії* $\mathfrak{T}$ або є *теоремою теорії* $\mathfrak{T}$, і пишуть $\mathfrak{T} \vdash \mathbf{A}$. Зокрема, якщо теорія $\mathfrak{T}$ порожня, кажуть, що $\mathbf{A}$ *виводиться в численні відношень* або є *теоремою числення відношень*.

З тверджень 2.1.6,2.1.7 та вправи 2.1.8.2 одразу випливає

Теорема 2.3.3 (**Теорема коректності для числення відношень**). *Кожна теорема теорії першого порядку* $\mathfrak{T}$ *є істинною в цій теорії. Зокрема, кожна теорема числення відношень є тотожно-істинною.*

Для числення відношень вірною є й **теорема адекватності**.

Теорема 2.3.4. *Кожне речення, істинне в теорії першого порядку* $\mathfrak{T}$*, є теоремою цієї теорії. Зокрема, кожне тотожно-істинне речення є теоремою числення відношень.*

Доведення цієї теореми ми розглянемо в наступних розділах, коли виробимо відповідну техніку.

Розглянемо деякі приклади виводів і теорем. Перш за все встановимо один результат, яким будемо постійно користуватися.

Твердження 2.3.5 (Див. твердження 2.1.6). *Кожен підстановковий випадок тавтології є теоремою числення відношень. Більш того, для такого речення завжди існує вивід, в якому зустрічаються лише аксіоми вигляду* (A1–A10) *і правило* modus ponens.

Доведення. Дійсно, нехай $\mathbf{A} = \mathbf{R}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$, де $\mathbf{R}$ — тавтологія. За теоремою адекватності для числення висловлювань (теорема 1.3.5) існує вивід $\mathbf{R}_1, \mathbf{R}_2, \ldots, \mathbf{R}_m$ речення $\mathbf{R}$ у численні висловлювань. Тоді послідовність $\mathbf{A}_1, \mathbf{A}_2, \ldots\ \mathbf{A}_m$, де $\mathbf{A}_i = \mathbf{R}_i{}^{\mathbf{E}_1,\mathbf{E}_2,\ldots,\mathbf{E}_n}_{\mathbf{A}_1,\mathbf{A}_2,\ldots,\mathbf{A}_n}$, є виводом речення $\mathbf{A}$ в численні відношень (поясніть, чому). Очевидно, у цьому виводі не зустрічаються ані аксіоми вигляду (A11–A14), ані правило узагальнення $\square$

Надалі будемо вільно вставляти підстановкові випадки тавтологій (скорочено ПВТ) у виводи. Насправді на місці кожного ПВТ треба вставити його вивід, але, як і в численні висловлювань, ми не будемо цього робити явно.

Інші приклади виводів:

Твердження 2.3.6.

1. $\vdash \neg\exists \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\neg\mathbf{A}$.
2. $\vdash \exists \mathrm{x}\neg\mathbf{A} \Rightarrow \neg\forall \mathrm{x}\mathbf{A}$.
3. *Якщо змінна* y *не зустрічається в реченні* $\mathbf{A}$*, то* $\vdash \forall \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{y}\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}$.

Доведення. 1. Ось відповідний вивід:

$$\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{A},\ (\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{A}) \Rightarrow (\neg\exists \mathrm{x}\mathbf{A} \Rightarrow \neg\mathbf{A}),$$

$$\neg\exists \mathrm{x}\mathbf{A} \Rightarrow \neg\mathbf{A},\ \forall \mathrm{x}(\neg\exists \mathrm{x}\mathbf{A} \Rightarrow \neg\mathbf{A}),$$

$$\forall \mathrm{x}(\neg\exists \mathrm{x}\mathbf{A} \Rightarrow \neg\mathbf{A}) \Rightarrow (\neg\exists \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\neg\mathbf{A}),\ \neg\exists \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\neg\mathbf{A}.$$

Друге речення — ПВТ $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\neg\mathbf{B} \Rightarrow \neg\mathbf{A})$; інші речення особливих коментарів не потребують.

Доведення твердження 2 аналогічне і залишається читачу як нескладна вправа.

3. Ось відповідний вивід:

$$\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{y}},\ \forall \mathrm{y}(\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{y}}),$$
$$\forall \mathrm{y}(\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{y}}) \Rightarrow (\forall \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{y}\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}),\ \forall \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{y}\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}.$$

Коментарі залишаємо читачу □

Відзначимо ще кілька важливих властивостей.

Твердження 2.3.7.

1. *Якщо* $\mathfrak{M} \vdash \mathbf{A}$ *і* $\mathfrak{T} \vdash \mathbf{B}$ *для кожного речення* $\mathbf{B} \in \mathfrak{M}$, *то* $\mathfrak{T} \vdash \mathbf{A}$.
2. *Якщо* $\mathfrak{T} \vdash \mathbf{A}$, *то* $\mathfrak{T} \vdash \forall \mathrm{x}\mathbf{A}$ *для довільної змінної* x *і навпаки. Зокрема* $\mathfrak{T} \vdash \bar{\mathbf{A}}$, *де* $\bar{\mathbf{A}}$ *— замикання речення* $\mathbf{A}$.
3. *Нехай* F *— деякий* m*-місний функціонал, який не зустрічається в реченнях теорії* $\mathfrak{T}$, $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ *— деякий вивід з теорії* $\mathfrak{T}$, *а* y *— змінна, яка не зустрічається в цьому виводі. Тоді послідовність* $\mathbf{A}'_1, \mathbf{A}'_2, \ldots, \mathbf{A}'_n$, *де кожне речення* $\mathbf{A}'_i$ *одержане з відповідного речення* $\mathbf{A}_i$ *заміною в останньому всіх підслів* $F\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$, *де* $\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m$ *— довільні терми, на змінну* y, *також є виводом з теорії* $\mathfrak{T}$.
4. *Нехай* P *— деякий* m*-місний предикат, який не зустрічається в реченнях теорії* $\mathfrak{T}$, $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ *— деякий вивід з теорії* $\mathfrak{T}$, Q *— довільний (*r*-місний) предикат теорії* $\mathfrak{T}$, *а* $\mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_r$ *— змінні, які не зустрічаються в цьому виводі. Тоді послідовність* $\mathbf{A}'_1, \mathbf{A}'_2, \ldots, \mathbf{A}'_n$, *де кожне речення* $\mathbf{A}'_i$ *одержане з відповідного речення* $\mathbf{A}_i$ *заміною в останньому всіх підслів* $P\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m$, *де* $\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m$ *— довільні терми, на слово* $Q\mathrm{y}_1\mathrm{y}_2\ldots\mathrm{y}_r$, *також є виводом з теорії* $\mathfrak{T}$.

Доведення очевидне.

Зауважимо, що теорія першого порядку може не мати жодного функціонала (зокрема, жодної константи), але вона обов'язково містить хоча б один предикат: без цього не можна утворити жодного речення.

З останніх двох пунктів твердження 2.3.7 випливає такий корисний наслідок.

Наслідок 2.3.8. *Нехай* $\mathbf{A}$ *— речення теорії* $\mathfrak{T}$. *Якщо* $\mathfrak{T} \vdash \mathbf{A}$, *то існує такий вивід речення* $\mathbf{A}$ *з теорії* $\mathfrak{T}$, *в якому всі речення є реченнями теорії* $\mathfrak{T}$ *(тобто не містять ніяких зайвих функціоналів та предикатів).*

Теорема коректності гарантує, що неможливо одночасно $\vdash \mathbf{A}$ і $\vdash \neg\mathbf{A}$. Вправа 2.3.9 дає, зокрема, доведення цього факту, яке не потребує звернення до семантики логіки відношень.

Вправа 2.3.9. Занумеруємо в якийсь спосіб усі предикати логіки відношень: $P_0, P_1, \ldots, P_n, \ldots$. Кожному реченню $\mathbf{A}$ логіки відношень зіставимо речення $\mathbf{A}^*$ логіки відношень, яке одержується з $\mathbf{A}$, якщо опустити всі знаки змінних, функціоналів та кванторів, а кожний предикат P_k замінити елементарним висловлюванням $A_k = A|| \ldots |$ (k разів $|$). Доведіть, що

1. Якщо $\mathbf{A}$ — аксіома числення відношень, то речення $\mathbf{A}^*$ є тавтологією.
2. Якщо $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ — вивід речення $\mathbf{A}$ з множини речень $\mathfrak{M}$ у численні відношень, то $\mathbf{A}_1^*, \mathbf{A}_2^*, \ldots, \mathbf{A}_n^*$ — вивід речення $\mathbf{A}^*$ з множини речень $\mathfrak{M}^*$ у численні висловлювань. Зокрема, якщо $\vdash \mathbf{A}$, то $\mathbf{A}^*$ — тавтологія.
3. У численні висловлювань для жодного речення $\mathbf{A}$ неможливо одночасно $\vdash \mathbf{A}$ і $\vdash \neg\mathbf{A}$.

2.4. Теорема дедукції в логіці відношень

Так само, як і в логіці висловлювань, у численні відношень зручно користуватися *теоремою дедукції*. Зауважимо, що ми не можемо стверджувати її в точно такій формі, як у численні висловлювань. Дійсно, за правилом узагальнення, ми можемо твердити, що $\mathbf{A} \vdash \forall \mathrm{x}\mathbf{A}$ для довільного речення $\mathbf{A}$ та довільної змінної x. Проте ми вже знаємо, що речення $\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{A}$, узагалі кажучи, не є тотожно-істинним (вправа 2.1.8.3); отже, невірно, що $\vdash \mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{A}$. Насправді ми мусимо накласти деякі обмеження на виводи.

Означення 2.4.1.

1. Нехай $\mathfrak{T} = \mathfrak{T}_1 \cup \mathfrak{T}_2$ і послідовність $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n$ є виводом з теорії $\mathfrak{T}$. Кажуть, що речення $\mathbf{B}_i$ в цьому виводі *не залежить від* $\mathfrak{T}_2$, якщо існує підпослідовність $\mathbf{B}_{i_1}, \mathbf{B}_{i_2}, \ldots, \mathbf{B}_{i_k}$ $(i_1 < i_2 < \cdots < i_k)$, яка є виводом з теорії $\mathfrak{T}_1$ і містить речення $\mathbf{B}_i$.
2. Вивід $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n$ зветься *вільним для* $\mathfrak{T}_2$, якщо в ньому узагальнення за змінними, які є вільними в реченнях з $\mathfrak{T}_2$, не застосовуються до речень, які залежать від $\mathfrak{T}_2$ в цьому виводі.

Вправа 2.4.2. Перевірте, що за умов визначення 2.4.1 речення $\mathbf{B}_i$ не залежить від $\mathfrak{T}_2$ тоді й лише тоді, коли виконується принаймні одна з таких умов:

- $\mathbf{B}_i$ є аксіомою або належить до $\mathfrak{T}_1$;
- $\mathbf{B}_i$ може бути одержане за modus ponens з таких речень $\mathbf{B}_j$ та $\mathbf{B}_k$ $(j, k < i)$, жодне з яких не залежить у цьому виводі від $\mathfrak{T}_2$;
- $\mathbf{B}_i$ може бути одержане узагальненням з речення $\mathbf{B}_j$ $(j < i)$, яке не залежить у цьому виводі від $\mathfrak{T}_2$.

Теорема 2.4.3 (Теорема дедукції). *Припустимо, що існує вивід речення* $\mathbf{B}$ *з теорії* $\mathfrak{T} \cup \{\mathbf{A}\}$, *вільний для* $\mathbf{A}$. *Тоді існує вивід речення* $\mathbf{A} \Rightarrow \mathbf{B}$ *з теорії* $\mathfrak{T}$, *в якому застосовуються узагальнення лише за тими ж змінними, що й у даному виводі* $\mathbf{B}$ *з* $\mathfrak{T} \cup \{\mathbf{A}\}$. *Зокрема, якщо в даному виводі взагалі не застосовується узагальнення за змінними, які є вільними в* $\mathbf{A}$ *(наприклад, речення* $\mathbf{A}$ *замкнене) і* $\mathfrak{T} \cup \{\mathbf{A}\} \vdash \mathbf{B}$, *то* $\mathfrak{T} \vdash \mathbf{A} \Rightarrow \mathbf{B}$.

Доведення. Ми наслідуємо доведення теореми 1.4.1, тобто перероблюємо вивід $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_m$ речення $\mathbf{B}$ з теорії $\mathfrak{T} \cup \{\mathbf{A}\}$ у вивід $\mathbf{A} \Rightarrow \mathbf{B}$ з $\mathfrak{T}$. Якщо речення $\mathbf{B}_i$ не залежить у цьому виводі від $\mathbf{A}$, ми зберігаємо його й додаємо одразу після нього речення $\mathbf{B}_i \Rightarrow (\mathbf{A} \Rightarrow \mathbf{B}_i)$, $\mathbf{A} \Rightarrow \mathbf{B}_i$. Якщо $\mathbf{B}_i = \mathbf{A}$ або залежить від $\mathbf{A}$ й одержане за modus ponens, ми замінюємо його так само, як у доведенні теореми 1.4.1. Залишився випадок,

коли речення $\mathbf{B}_i$, яке залежить від $\mathbf{A}$, одержане з $\mathbf{B}_j$ узагальненням за змінною x, тобто $\mathbf{B}_i = \forall \mathrm{x}\mathbf{B}_j$, причому x не є вільною змінною в реченні $\mathbf{A}$. Тоді ми замінюємо $\mathbf{B}_i$ на три речення:

$$\forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}_j), \quad \forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}_j) \Rightarrow (\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}_j), \quad \mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}_j.$$

Перше з них одержане узагальненням з речення $\mathbf{A} \Rightarrow \mathbf{B}_j$, яке вже ввійшло в перероблений вивід; друге — аксіома вигляду (A13); третє одержане з перших двох за modus ponens. У результаті всіх цих замін ми одержимо необхідний вивід речення $\mathbf{A} \Rightarrow \mathbf{B}$ з $\mathfrak{T}$ □

Наслідок 2.4.4. *Припустимо, що існує вивід речення* $\mathbf{B}$ *з теорії* $\mathfrak{T} \cup \{ \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n \}$, *вільний для* $\{ \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n \}$. *Тоді існує вивід речення* $\mathbf{A}_1 \Rightarrow (\mathbf{A}_2 \Rightarrow (\ldots \Rightarrow (\mathbf{A}_m \Rightarrow \mathbf{B}) \ldots))$ *з теорії* $\mathfrak{T}$, *в якому застосовуються узагальнення лише за тими ж змінними, що й у даному виводі. Зокрема, якщо всі речення* $\mathbf{A}_i$ *замкнені і* $\mathfrak{T} \cup \{ \mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n \} \vdash \mathbf{B}$, *то* $\mathfrak{T} \vdash \mathbf{A}_1 \Rightarrow (\mathbf{A}_2 \Rightarrow (\ldots \Rightarrow (\mathbf{A}_m \Rightarrow \mathbf{B}) \ldots))$.

Застосуємо теорему дедукції до виводу деяких теорем числення відношень. Ми будемо писати $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{B}$, якщо $\mathfrak{T} \vdash \mathbf{A} \Rightarrow \mathbf{B}$ і $\mathbf{A} \equiv_{\mathfrak{T}} \mathbf{B}$, якщо $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{B}$ і $\mathbf{B} \Rightarrow_{\mathfrak{T}} \mathbf{A}$. Якщо $\mathfrak{T} = \emptyset$, ми писатимемо $\mathbf{A} \equiv \mathbf{B}$. Зауважимо, що з тавтології $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\neg\mathbf{B} \Rightarrow \neg\mathbf{A})$ одразу випливає, що коли $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{B}$, то $\neg\mathbf{B} \Rightarrow_{\mathfrak{T}} \neg\mathbf{A}$, зокрема якщо $\mathbf{A} \equiv_{\mathfrak{T}} \mathbf{B}$, то й $\neg\mathbf{A} \equiv_{\mathfrak{T}} \neg\mathbf{B}$. Зауважимо також, що з тавтології $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{B} \Rightarrow \mathbf{C}) \Rightarrow (\mathbf{A} \Rightarrow \mathbf{C})$ випливає, що коли $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{B}$ і $\mathbf{B} \Rightarrow_{\mathfrak{T}} \mathbf{C}$, то й $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{C}$. Зокрема, якщо у виводі зустрілося речення $\mathbf{A} \Rightarrow \mathbf{B}$, то можна вставити речення $\mathbf{A}' \Rightarrow \mathbf{B}'$ для довільних $\mathbf{A}' \equiv_{\mathfrak{T}} \mathbf{A}$ і $\mathbf{B}' \equiv_{\mathfrak{T}} \mathbf{B}$. Надалі ми вільно користуватимемося такими замінами.

Твердження 2.4.5. *Для довільних речень* $\mathbf{A}$ *і* $\mathbf{B}$ *та довільної змінної* x*:*

1. *Якщо* $\mathbf{A} \Rightarrow_{\mathfrak{T}} \mathbf{B}$, *то* $\forall \mathrm{x}\mathbf{A} \Rightarrow_{\mathfrak{T}} \forall \mathrm{x}\mathbf{B}$ *і* $\exists \mathrm{x}\mathbf{A} \Rightarrow_{\mathfrak{T}} \exists \mathrm{x}\mathbf{B}$.
2. *Якщо* $\mathbf{A} \equiv_{\mathfrak{T}} \mathbf{B}$, *то* $\forall \mathrm{x}\mathbf{A} \equiv_{\mathfrak{T}} \forall \mathrm{x}\mathbf{B}$ *і* $\exists \mathrm{x}\mathbf{A} \equiv_{\mathfrak{T}} \exists \mathrm{x}\mathbf{B}$.
3. $\neg\exists \mathrm{x}\mathbf{A} \equiv \forall \mathrm{x}\neg\mathbf{A}$, *а тому* $\exists \mathrm{x}\mathbf{A} \equiv \neg\forall \mathrm{x}\neg\mathbf{A}$.
4. $\neg\forall \mathrm{x}\mathbf{A} \equiv \exists \mathrm{x}\neg\mathbf{A}$, *а тому* $\forall \mathrm{x}\mathbf{A} \equiv \neg\exists \mathrm{x}\neg\mathbf{A}$.
5. *Якщо змінна* y *вільна для* x *у реченні* $\mathbf{A}$ *і не є сама вільною змінною в цьому реченні, то* $\forall \mathrm{x}\mathbf{A} \equiv \forall \mathrm{y}\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}$ *і* $\exists \mathrm{x}\mathbf{A} \equiv \exists \mathrm{y}\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}$.
6. $\exists \mathrm{x}\mathbf{A} \Rightarrow \mathbf{B} \equiv \forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B})$, *якщо* x *не є вільною зиінною в реченні* $\mathbf{B}$.

Доведення. 1. До виводу $\mathbf{A} \Rightarrow \mathbf{B}$ з теорії $\mathfrak{T}$ додамо речення

$$\forall \mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}, \ \mathbf{A}, \ \mathbf{B}, \ \forall \mathrm{x}\mathbf{B}.$$

Одержимо вивід $\forall \mathrm{x}\mathbf{B}$ з $\mathfrak{T} \cup \{ \forall \mathrm{x}\mathbf{A} \}$. За теоремою дедукції $\mathfrak{T} \vdash \forall \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}$. Тепер до виводу $\mathbf{A} \Rightarrow \mathbf{B}$ з $\mathfrak{T}$ додамо ПВТ $(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow ((\mathbf{B} \Rightarrow \exists \mathrm{x}\mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}))$ і речення

$$(\mathbf{B} \Rightarrow \exists \mathrm{x}\mathbf{B}) \Rightarrow (\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}), \ \mathbf{B} \Rightarrow \exists \mathrm{x}\mathbf{B}, \ \mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}, \ \forall \mathrm{x}(\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}),$$

$$\forall \mathrm{x}(\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}) \Rightarrow (\exists \mathrm{x}\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}), \ \exists \mathrm{x}\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}.$$

Одержимо вивід $\exists \mathrm{x}\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B}$.

2 безпосередньо випливає з 1.

3 та 4 доводяться аналогічно. Ми доведемо 4, залишивши 3 як вправу. У твердженні 2.3.6 уже було доведено, що $\vdash \neg\forall x\mathbf{A} \Rightarrow \exists x\neg\mathbf{A}$. Доведемо, що $\vdash \exists x\neg\mathbf{A} \Rightarrow \neg\forall x\mathbf{A}$. Для цього з уже доведеного $\vdash \neg\exists x\neg\mathbf{A} \Rightarrow \forall x\neg\neg\mathbf{A}$ (твердження 2.3.6.1) заміною $\neg\neg\mathbf{A}$ на $\mathbf{A}$ одержимо $\vdash \neg\exists\neg\mathbf{A} \Rightarrow \forall x\mathbf{A}$. Звідси $\vdash \neg\forall x\mathbf{A} \Rightarrow \neg\neg\exists\neg\mathbf{A}$, а тому й $\vdash \neg\forall x\mathbf{A} \Rightarrow \exists x\neg\mathbf{A}$.

5. Ось вивід $\forall y\mathbf{A}^x_y$ з $\forall x\mathbf{A}$:

$$\forall x\mathbf{A},\ \forall x\mathbf{A} \Rightarrow \mathbf{A}^x_y,\ \mathbf{A}^x_y,\ \forall y\mathbf{A}^x_y.$$

Оскільки, очевидно, x вільна для y в реченні $\mathbf{A}^x_y$, не є вільною змінною в цьому реченні і $(\mathbf{A}^x_y)^y_x = \mathbf{A}$, то й $\mathbf{A}$ виводиться з $\mathbf{A}^x_y$, що доводить першу еквівалентність. Друга випливає з першої та тверджень 3,4 (подробиці залишаємо як вправу).

6. З речення $\exists x\mathbf{A} \Rightarrow \mathbf{B}$ та ПВТ $(X \Rightarrow Y) \Rightarrow (\neg Y \Rightarrow \neg X)$ виводимо $\neg\mathbf{B} \Rightarrow \neg\exists x\mathbf{A}$. За твердженням 2.3.6.1 та ПВТ $(X \Rightarrow Y) \Rightarrow ((Y \Rightarrow Z) \Rightarrow (X \Rightarrow Z))$ одержимо $\neg\mathbf{B} \Rightarrow \forall x\neg\mathbf{A}$. Оскільки $\forall x\mathbf{A} \Rightarrow \mathbf{A}$, то за тією ж тавтологією одержимо $\neg\mathbf{B} \Rightarrow \neg\mathbf{A}$, а тому й $\mathbf{A} \Rightarrow \mathbf{B}$. Узагальнення дає $\forall x(\mathbf{A} \Rightarrow \mathbf{B})$. Отже, $\exists x\mathbf{A} \Rightarrow \mathbf{B} \vdash \forall x(\mathbf{A} \Rightarrow \mathbf{B})$. За теоремою дедукції $\vdash \exists x\mathbf{A} \Rightarrow \mathbf{B} \Rightarrow \forall x(\mathbf{A} \Rightarrow \mathbf{B})$. Обернена імплікація — це аксіома вигляду (A14) □

Вправа 2.4.6.

1. Доведіть, що коли $\mathbf{A} \equiv_{\mathfrak{T}} \mathbf{A}'$ і $\mathbf{B} \equiv_{\mathfrak{T}} \mathbf{B}'$, то

$$\neg\mathbf{A} \equiv_{\mathfrak{T}} \neg\mathbf{A}';$$
$$\mathbf{A} \wedge \mathbf{B} \equiv_{\mathfrak{T}} \mathbf{A}' \wedge \mathbf{B}';$$
$$\mathbf{A} \vee \mathbf{B} \equiv_{\mathfrak{T}} \mathbf{A}' \vee \mathbf{B}';$$
$$\mathbf{A} \Rightarrow \mathbf{B} \equiv_{\mathfrak{T}} \mathbf{A}' \Rightarrow \mathbf{B}'.$$

2. Доведіть, що

$$\forall x(\mathbf{A} \wedge \mathbf{B}) \equiv \forall x\mathbf{A} \wedge \forall x\mathbf{B};$$
$$\exists x(\mathbf{A} \vee \mathbf{B}) \equiv \exists x\mathbf{A} \vee \exists x\mathbf{B};$$
$$\exists x(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \forall x\mathbf{A} \Rightarrow \exists x\mathbf{B},$$

зокрема,

$\exists x(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \mathbf{A} \Rightarrow \exists x\mathbf{B}$, якщо x не є вільною змінною в $\mathbf{A}$,

$\exists x(\mathbf{A} \Rightarrow \mathbf{B}) \equiv \forall x\mathbf{A} \Rightarrow \mathbf{B}$, якщо x не є вільною змінною у $\mathbf{B}$;

$\forall x(\mathbf{A} \vee \mathbf{B}) \equiv \forall x\mathbf{A} \vee \mathbf{B}$, якщо x не є вільною змінною у $\mathbf{B}$;

$\exists x(\mathbf{A} \wedge \mathbf{B}) \equiv \exists x\mathbf{A} \wedge \mathbf{B}$, якщо x не є вільною змінною у $\mathbf{B}$.

3. Доведіть, що $\mathbf{A} \Rightarrow \forall x\mathbf{B} \equiv \forall x(\mathbf{A} \Rightarrow \mathbf{B})$, якщо x не є вільною змінною в реченні $\mathbf{A}$.

Вправа 2.4.7.

1. Доведіть, що $\vdash \exists y\forall x\mathbf{A} \Rightarrow \forall x\exists y\mathbf{A}$. Чи можна вивести обернену імплікацію?
2. Доведіть, що $\forall x\forall y\mathbf{A} \equiv \forall y\forall x\mathbf{A}$ і $\exists x\exists y\mathbf{A} \equiv \exists y\exists x\mathbf{A}$.
3. Чи вірно, що

(a) $\forall \mathrm{x}(\mathbf{A} \vee \mathbf{B}) \equiv \forall \mathrm{x}\mathbf{A} \vee \forall \mathrm{x}\mathbf{B}$?
(b) $\exists \mathrm{x}(\mathbf{A} \wedge \mathbf{B}) \equiv \exists \mathrm{x}\mathbf{A} \wedge \exists \mathrm{x}\mathbf{B}$?
(c) $\forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}) \equiv (\exists \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B})$?

Важливу роль у логіці відношень має теорема, яка дозволяє звести розгляд довільних речень до речень спеціального типу.

Теорема 2.4.8. *Для довільного речення* $\mathbf{A}$ *логіки відношень існує еквівалентне йому речення вигляду* $\mathbf{A}' = \mathrm{Q}_1 x_1 \mathrm{Q}_2 x_2 \dots \mathrm{Q}_m x_m \mathbf{A}_0$, *де* $\mathrm{Q}_1, \mathrm{Q}_2, \dots, \mathrm{Q}_m$ *— деякі квантори,* $\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_m$ *— змінні, а* $\mathbf{A}_0$ *— речення, яке не містить кванторів.*

Речення вказаного вигляду звуться *пренексними*, а пренексне речення, еквівалентне реченню $\mathbf{A}$, зветься *пренексною формою речення* $\mathbf{A}$. Слово $\Pi = \mathrm{Q}_1 x_1 \mathrm{Q}_2 x_2 \dots \mathrm{Q}_m x_m$ зветься *префіксом* пренексного речення $\mathbf{A}'$, а речення $\mathbf{A}_0$ — його *ядром*.

Доведення. Користуючись твердженням 2.4.5.5, можна замінити $\mathbf{A}$ еквівалентним реченням, в якому жодна змінна не з'являється одночасно як вільна й як пов'язана. Надалі вважатимемо, що ця умова виконана. Доведення теореми проведемо індукцією за довжиною речення $\mathbf{A}$. Якщо $\mathbf{A}$ не містить кванторів, то воно вже є пренексним. Припустимо, що для коротших ніж $\mathbf{A}$ речень пренексні форми існують. Якщо $\mathbf{A} = \mathrm{Q}\mathrm{x}\mathbf{B}$, де Q — деякий квантор, то $\mathbf{A} \equiv \mathbf{A}' = \mathrm{Q}\mathrm{x}\mathbf{B}'$, де $\mathbf{B}'$ — пренексна форма речення $\mathbf{B}$, і речення $\mathbf{A}'$ — пренексне. Надалі будемо користуватися результатами твердження 2.4.5 і вправи 2.4.6.

Якщо $\mathbf{A} = \neg\mathbf{B}$ і $\mathbf{B}' = \mathrm{Q}_1 x_1 \mathrm{Q}_2 x_2 \dots \mathrm{Q}_m x_m \mathbf{C}$, де речення $\mathbf{C}$ не містить кванторів, — пренексна форма речення $\mathbf{B}$, то

$$\mathbf{A} \equiv \mathbf{A}' = \mathrm{Q}'_1 x_1 \mathrm{Q}'_2 x_2 \dots \mathrm{Q}'_m x_m \neg\mathbf{C},$$

де Q'_i — квантор, відмінний від Q_i, і речення $\mathbf{A}'$ — пренексне.

Якщо $\mathbf{A} = \mathbf{B} \vee \mathbf{C}$, то нехай $\mathbf{B}' = \Pi_{\mathbf{B}}\mathbf{B}_0$ і $\mathbf{C}' = \Pi_{\mathbf{C}}\mathbf{C}_0$ — пренексні форми речень $\mathbf{B}$ і $\mathbf{C}$, де $\Pi_{\mathbf{B}}$ та $\Pi_{\mathbf{C}}$ — префікси, а $\mathbf{B}_0$ та $\mathbf{C}_0$ — безквантормі речення. Знов-таки можна вважати, що префікси $\Pi_{\mathbf{B}}$ та $\Pi_{\mathbf{C}}$ не містять однакових змінних. Тоді $\mathbf{A} \equiv \mathbf{A}' = \Pi_{\mathbf{B}}\Pi_{\mathbf{C}}(\mathbf{B}_0 \vee \mathbf{C}_0)$ і речення $\mathbf{A}'$ пренексне.

Випадки, коли $\mathbf{A} = \mathbf{B} \wedge \mathbf{C}$ чи $\mathbf{A} = \mathbf{B} \Rightarrow \mathbf{C}$, залишаємо читачу як вправу □

Вправа 2.4.9. Побудуйте пренексну форму речень $\forall \mathrm{x}\mathbf{A} \vee \forall \mathrm{x}\mathbf{B}$, $\exists \mathrm{x}\mathbf{A} \wedge \exists \mathrm{x}\mathbf{B}$ та $\exists \mathrm{x}\mathbf{A} \Rightarrow \forall \mathrm{x}\mathbf{B}$.

2.5. Адекватність числення відношень

Перейдемо до доведення теореми про адекватність для числення відношень. Ми наслідуватимемо відповідне доведення для числення висловлювань. Уведемо відповідні поняття.

Означення 2.5.1.

1. Теорія $\mathfrak{T}$ зветься *суперечливою*, якщо існує таке речення $\mathbf{A}$, що $\mathfrak{T} \vdash \mathbf{A}$ і $\mathfrak{T} \vdash \neg\mathbf{A}$. (Тоді, звичайно, $\mathfrak{T} \vdash \mathbf{B}$ для кожного речення $\mathbf{B}$.)

2. Теорія $\mathfrak{T}$ зветься *повною*, якщо для довільного *замкненого* речення $\mathbf{A}$ цієї теорії або $\mathfrak{T} \vdash \mathbf{A}$, або $\mathfrak{T} \vdash \neg\mathbf{A}$. (Зокрема, кожна суперечлива теорія напевне є повною.)

Перш за все покажемо, що теорема про адекватність випливає з такої теореми.

Теорема 2.5.2 (**Теорема про модель**). *Кожна несуперечлива теорія першого порядку має зліченну модель.*

Дійсно, припустимо, що ми вже довели теорему про модель. Скористаємось аналогом леми 1.5.3.

Лема 2.5.3. *Якщо замкнене речення* $\mathbf{A}$ *не виводиться з теорії* $\mathfrak{T}$*, то теорія* $\mathfrak{T} \cup \{\, \neg\mathbf{A} \,\}$ *несуперечлива.*

Доведення дослівно повторює доведення леми 1.5.3 з урахуванням того, що речення $\mathbf{A}$ замкнене, а тому довільний вивід є вільним для $\mathbf{A}$ □

Отже, якщо $\mathfrak{T} \models \mathbf{A}$, то, оскільки теорія $\mathfrak{T} \cup \{\, \neg\mathbf{A} \,\}$ напевне не має моделі, обов'язково $\mathfrak{T} \vdash \mathbf{A}$.

Доведення теореми про модель спирається на дві леми. Перша з них — аналог леми 1.5.4.

Лема 2.5.4. *Кожна несуперечлива теорія* $\mathfrak{T}$ *міститься в повній несуперечливій теорії* $\mathfrak{T}^*$*. При цьому можна вважати, що теорія* $\mathfrak{T}^*$ *містить ті самі функціонали та предикати, які мала й теорія* $\mathfrak{T}$*.*

Доведення знов-таки є повторенням доведення леми 1.5.4. Єдина різниця полягає в тому, що ми розглядаємо й нумеруємо лише замкнені речення □

Лема 2.5.5. *Нехай теорія* $\mathfrak{T}$ *несуперечлива,* c *— константа, яка не належить цій теорії, і* $\mathbf{A}$ *— речення, яке містить одну вільну змінну* x*. Тоді теорія* $\mathfrak{T} \cup \{\, \exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}} \,\}$ *також несуперечлива.*

Доведення. Припустимо, що теорія $\mathfrak{T} \cup \{\, \exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}} \,\}$ суперечлива. Тоді з неї виводиться $\neg(\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}})$. Оскільки речення $\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}}$ замкнене, $\mathfrak{T} \vdash (\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}}) \Rightarrow \neg(\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}})$. З тавтології $(\mathbf{B} \Rightarrow \neg\mathbf{B}) \Rightarrow \neg\mathbf{B}$ одержуємо, що $\mathfrak{T} \vdash \neg(\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{c}})$. Розглянемо відповідний вивід. Нехай y — змінна, яка не зустрічається в цьому виводі. З твердження 2.3.7.3 одержимо, що $\mathfrak{T} \vdash \neg(\exists\mathrm{x}\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{x}}_{\mathrm{y}})$. З логіки висловлювань відомо, що $\neg(\mathbf{B} \Rightarrow \mathbf{C}) \equiv \mathbf{B} \wedge \neg\mathbf{C}$. Тому $\mathfrak{T} \vdash \exists\mathrm{x}\mathbf{A}$ і $\mathfrak{T} \vdash \neg\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}$. Користуючись узагальненням, одержимо, що $\mathfrak{T} \vdash \forall\mathrm{y}\neg\mathbf{A}^{\mathrm{x}}_{\mathrm{y}}$. Оскільки $\forall\mathrm{y}\neg\mathbf{A}^{\mathrm{x}}_{\mathrm{y}} \equiv \forall\mathrm{x}\neg\mathbf{A} \equiv \neg\exists\mathrm{x}\mathbf{A}$, також $\mathfrak{T} \vdash \neg\exists\mathrm{x}\mathbf{A}$, а тоді й теорія $\mathfrak{T}$ суперечлива □

Доведення теореми про модель. Нехай теорія $\mathfrak{T}$ несуперечлива. Згідно з твердженням 2.2.6 можна вважати, що всі постулати (речення, які належать $\mathfrak{T}$) замкнені. Випишемо всі речення цієї теорії, які містять одну вільну змінну (їх, звичайно, зліченна кількість): $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n, \ldots$ і позначимо $\mathfrak{T}'$ теорію, отриману з $\mathfrak{T}$ додаванням зліченної множини нових констант $\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_n, \ldots$, а також усіх речень $\exists\mathrm{x}\mathbf{A}_i \Rightarrow \mathbf{A}_i{}^{\mathrm{x}}_{\mathrm{c}_i}$, де x — єдина вільна змінна речення $\mathbf{A}_i$. За твердженням 2.3.7.3 і лемою 2.5.5,

теорія $\mathfrak{T}'$ також несуперечлива, а тому міститься в повній несуперечливій теорії $\mathfrak{T}^*$ такій, що функціонали та предикати $\mathfrak{T}^*$ — це функціонали та предикати $\mathfrak{T}$, а також константи c_i. Зокрема, речення теорії $\mathfrak{T}^*$ — ті ж самі, що й теорії $\mathfrak{T}'$.

Побудуємо модель $\mathcal{I}$ теорії $\mathfrak{T}$. Областю інтерпретації $\mathcal{I}$ буде множина T замкнених термів теорії $\mathfrak{T}^*$ (або, що те саме, $\mathfrak{T}'$). Очевидно, множина T зліченна. Для кожного m-місного функціонала F покладемо

$$\mathcal{I}(F)\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m) = F\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)\,,$$

а для кожного m-місного предиката P покладемо

$$\mathcal{I}(P)\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m) = \begin{cases} \mathbf{1}, & \text{якщо } \mathfrak{T}^* \vdash P\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)\,, \\ \mathbf{0}, & \text{якщо } \mathfrak{T}^* \vdash \neg P\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)\,. \end{cases} \tag{2.5.1}$$

Зауважимо, що коли всі терми $\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m$ замкнені, то таким є й терм $F\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)$ і речення $P\,(\mathrm{t}_1, \mathrm{t}_2, \ldots, \mathrm{t}_m)$. Тому ці означення мають зміст. Для кожного речення $\mathbf{A}$ теорії $\mathfrak{T}$ і розподілу $\phi : \mathfrak{X} \to T$ покладемо $\mathbf{A}^\phi = \mathbf{A}^{\mathrm{x}_1\mathrm{x}_2\ldots\mathrm{x}_m}_{\mathrm{t}_1\mathrm{t}_2\ldots\mathrm{t}_m}$, де $\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_m$ — усі вільні змінні речення $\mathbf{A}$, а $\mathrm{t}_i = \phi(\mathrm{x}_i)$. Речення $\mathbf{A}^\phi$ завжди замкнене. Покажемо, що для кожного речення $\mathbf{A}$ теорії $\mathfrak{T}$ і кожного розподілу $\phi : \mathfrak{X} \to T$

$$\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \begin{cases} \mathbf{1} & \text{якщо } \mathfrak{T}^* \vdash \mathbf{A}^\phi, \\ \mathbf{0} & \text{якщо } \mathfrak{T}^* \vdash \neg\mathbf{A}^\phi. \end{cases} \tag{2.5.2}$$

Доведення проведемо індукцією за кількістю сполучників і кванторів у реченні $\mathbf{A}$. Якщо це речення елементарне, формула (2.5.2) збігається з означенням (2.5.1). Якщо $\mathbf{A}$ має один з виглядів

$$\neg\mathbf{B},\ \mathbf{B} \vee \mathbf{C},\ \mathbf{B} \wedge \mathbf{C},\ \mathbf{B} \Rightarrow \mathbf{C},$$

доведення фактично збігається з доведенням леми Кальмара (лема 1.5.1). Ми проведемо його лише для випадку $\mathbf{A} = \mathbf{B} \Rightarrow \mathbf{C}$, залишивши інші читачу. Очевидно, $\mathbf{A}^\phi = \mathbf{B}^\phi \Rightarrow \mathbf{C}^\phi$. Якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{C}) = \mathbf{1}$, то й $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$. У цьому випадку $\mathfrak{T}^* \vdash \mathbf{C}^\phi$. Разом з аксіомою $\mathbf{C}^\phi \Rightarrow (\mathbf{B}^\phi \Rightarrow \mathbf{C}^\phi)$ це дає $\mathfrak{T}^* \vdash \mathbf{A}^\phi$. Так само, якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathbf{0}$, то $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$ і $\mathfrak{T}^* \vdash \neg\mathbf{B}^\phi$. Разом з ПВТ $\neg\mathbf{B}^\phi \Rightarrow (\mathbf{B}^\phi \Rightarrow \mathbf{C}^\phi)$ це знов дає $\mathfrak{T}^* \vdash \mathbf{A}^\phi$. Нехай, нарешті, $\mathrm{val}(\mathcal{I}, \phi, \mathbf{B}) = \mathbf{1}$, а $\mathrm{val}(\mathcal{I}, \phi, \mathbf{C}) = \mathbf{0}$; тоді $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}^\phi) = \mathbf{0}$. У цьому випадку $\mathfrak{T} \vdash \mathbf{B}^\phi$ і $\mathfrak{T} \vdash \neg\mathbf{C}^\phi$. Скориставшись ПВТ $\mathbf{B}^\phi \Rightarrow (\neg\mathbf{C}^\phi \Rightarrow \neg(\mathbf{B}^\phi \Rightarrow \mathbf{C}^\phi))$, одержимо $\mathfrak{T} \vdash \neg\mathbf{A}^\phi$.

Нехай тепер $\mathbf{A} = \exists\mathrm{x}\mathbf{B}$, причому всі вільні змінні $\mathbf{B}$ — це $\mathrm{x}, \mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_m$. Позначимо $\mathbf{B}^* = \mathbf{B}^{\mathrm{y}_1,\mathrm{y}_2,\ldots,\mathrm{y}_m}_{\mathrm{t}_1,\mathrm{t}_2,\ldots,\mathrm{t}_m}$, де $\mathrm{t}_i = \phi(\mathrm{y}_i)$. Тоді $\mathbf{B}^*$ містить одну вільну змінну x, тому теорія $\mathfrak{T}^*$ містить речення $\exists\mathrm{x}\mathbf{B}^* \Rightarrow \mathbf{B}^{*\mathrm{x}}_{\mathrm{c}}$ для деякої константи c. Однак $\mathbf{A}^\phi = \exists\mathrm{x}\mathbf{B}^*$. Припустимо, що $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$, тобто існує розподіл $\psi \in \phi^{\mathrm{x}}$, такий що $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{1}$. Тоді $\mathfrak{T}^* \vdash \mathbf{B}^\psi$, причому $\mathbf{B}^\psi = \mathbf{B}^{*\mathrm{x}}_{\mathrm{t}}$, де $\mathrm{t} = \psi(\mathrm{x})$. Разом з аксіомою $\mathbf{B}^{*\mathrm{x}}_{\mathrm{t}} \Rightarrow \exists\mathrm{x}\mathbf{B}^*$ це дає $\mathfrak{T}^* \vdash \mathbf{A}^\phi$. Навпаки, якщо $\mathfrak{T}^* \vdash \mathbf{A}^\phi$, то також $\mathfrak{T}^* \vdash \mathbf{B}^{*\mathrm{x}}_{\mathrm{c}}$, а тоді $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{1}$, де $\psi \in \phi^{\mathrm{x}}$ — такий розподіл, що $\psi(\mathrm{x}) = \mathrm{c}$.

Нарешті, нехай $\mathbf{A} = \forall\mathrm{x}\mathbf{B}$, причому всі вільні змінні $\mathbf{B}$ — це $\mathrm{x}, \mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_m$. Позначимо $\mathbf{B}^* = \mathbf{B}^{\mathrm{y}_1,\mathrm{y}_2,\ldots,\mathrm{y}_m}_{\mathrm{t}_1,\mathrm{t}_2,\ldots,\mathrm{t}_m}$, де $\mathrm{t}_i = \phi(\mathrm{y}_i)$. Це речення знов містить одну вільну змінну x і $\mathbf{A}^\phi = \forall\mathrm{x}\mathbf{B}^*$. Якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{0}$, то існує розподіл $\psi \in \phi^{\mathrm{x}}$, такий що $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{0}$. Тоді $\mathfrak{T}^* \vdash \neg\mathbf{B}^\psi$ і $\mathbf{B}^\psi = \mathbf{B}^{*\mathrm{x}}_{\mathrm{t}}$, де $\mathrm{t} = \psi(\mathrm{x})$.

Разом з аксіомою $\forall \mathrm{x}\mathbf{B}^* \Rightarrow \mathbf{B}^{*\mathrm{x}}_{\mathrm{t}}$ і ПВТ $(\forall \mathrm{x}\mathbf{B}^* \Rightarrow \mathbf{B}^{*\mathrm{x}}_{\mathrm{t}}) \Rightarrow (\neg\mathbf{B}^{*\mathrm{x}}_{\mathrm{t}} \Rightarrow \neg\forall \mathrm{x}\mathbf{B}^*$ це дає $\mathfrak{T}^* \vdash \neg\mathbf{A}^{\phi}$. Навпаки, якщо $\mathfrak{T} \vdash \neg\mathbf{A}^{\phi}$, то з твердження 2.4.5.4 випливає, що $\mathfrak{T}^* \vdash \exists \mathrm{x}\neg\mathbf{B}^*$. Але $\mathfrak{T}^*$ містить речення $\exists \mathrm{x}\neg\mathbf{B}^* \Rightarrow \mathbf{B}^{*\mathrm{x}}_{\mathrm{c}}$ для деякої константи c. Тому $\mathfrak{T}^* \vdash \mathbf{B}^{*\mathrm{x}}_{\mathrm{c}}$, а це речення збігається з $\mathbf{B}^{\psi}$, де $\psi \in \phi^{\mathrm{x}}$ — такий розподіл, що $\psi(\mathrm{x}) = \mathrm{c}$. Звідси $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{0}$ і $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{0}$.

Отже, правило (2.5.2) повністю доведене. Тепер, якщо $\mathbf{A} \in \mathfrak{T}$, то за припущенням $\mathbf{A}$ — замкнене речення і тривіально $\mathfrak{T}^* \vdash \mathbf{A}$, а тому $\mathrm{val}(\mathcal{I}, \mathbf{A}) = \mathbf{1}$, тобто $\mathcal{I}$ є моделлю теорії $\mathfrak{T}$ □

Отже, ми довели теорему про модель і разом з нею теорему про адекватність числення відношень. Якщо нас цікавлять *теорії з рівністю* та *нормальні моделі* (які найчастіше зустрічаються в математиці) то з теорем 2.5.2 і 2.2.4 одразу випливає

Теорема 2.5.6 (**Теорема про нормальну модель**). *Кожна несуперечлива теорія першого порядку з рівністю має скінченну або злічену нормальну модель.*

Важливий наслідок теореми про модель — це *теорема про компактність.*

Теорема 2.5.7 (**Теорема про компактність**). *Якщо кожна скінченна частина $\mathfrak{T}' \subseteq \mathfrak{T}$ має модель, то вся теорія $\mathfrak{T}$ має зліченну модель. Якщо $\mathfrak{T}$ — теорія з рівністю, то вона має скінченну або зліченну нормальну модель.*

Теорема про модель має деякі несподівані наслідки. Наприклад, з неї одразу випливає, що, скажімо, елементарна теорія дійсних чисел має зліченну нормальну модель (легко бачити, що вона не має скінченних моделей). У цій моделі виконуються всі властивості дійсних чисел, які можна виразити мовою логіки відношень. З іншого боку, розглянемо теорію $\mathfrak{R}^{\infty}$, яка одержується з елементарної теорії дійсних чисел додаванням нової константи c і речень $L\overline{\mathrm{n}}\mathrm{c}$, де $\overline{\mathrm{n}}$ позначає терм

$$\underbrace{SS\ldots S}_{n-1 \text{ разів}}\underbrace{\mathrm{e}\mathrm{e}\ldots\mathrm{e}}_{n \text{ разів}}$$

($n > 1$ — довільне натуральне число). У звичайній моделі — полі дійсних чисел — значенням терма $\overline{\mathrm{n}}$ є натуральне число n. Більш того, ця модель є моделлю довільної скінченної частини теорії $\mathfrak{T}'$. Дійсно, така частина містить лише скінченну кількість «нових» речень, а тоді всі вони істинні, бо в полі дійсних чисел напевно є число, яке більше всіх чисел з довільного скінченного набору. Його й можна зіставити константі c. Отже, теорія $\mathfrak{T}'$ має модель $\mathcal{I}$. У цій моделі виконуються всі «елементарні» властивості дійсних чисел, але є «актуальне нескінченно велике число» $\mathcal{I}(\mathrm{c})$, яке більше за всі натуральні числа. Зауважимо, що всі ці властивості не залежать від вибору теорії першого порядку, якою ми хочемо формалізувати теорію дійсних чисел. Вони притаманні кожній такій теорії. Звідси можна зробити висновок, що, коли ми хочемо зберегти всі властивості дійсних чисел, це неможливо зробити в межах теорій першого порядку. У наступному розділі ми побачимо, що це стосується й теорії натуральних чисел, і взагалі практично всіх змістовних теорій нескінченних математичних об'єктів. Більш того, намагання використати

більш складні формальні теорії веде до не менш разючих парадоксів (такий розгляд виходить за межі нашої книги; читач може звернутися, наприклад, до класичної монографії Черча [**Ч**]). Це означає, в деякому розумінні, що всупереч намаганням багатьох поколінь логіків змістовна математика не може бути зведена до логіки.

Утім, доведені теореми мають значні застосування в математиці. Розглянемо одне з них.

Теорема 2.5.8. *Нехай $\mathfrak{T}$ — теорія першого порядку з рівністю. Тоді або потужності всіх скінченних нормальних моделей цієї теорії обмежені, або $\mathfrak{T}$ має зліченну модель.*
(Згідно із вправою 2.2.7, тоді $\mathfrak{T}$ має моделі довільної нескінченної потужності.)

Доведення. Припустимо, що потужності скінченних нормальних моделей теорії $\mathfrak{T}$ необмежені. Додамо до $\mathfrak{T}$ зліченну кількість нових констант $\mathrm{c}_1, \mathrm{c}_2, \ldots, \mathrm{c}_n, \ldots$, усі речення вигляду $\neg E\mathrm{c}_i\mathrm{c}_j$, де $i < j$, а також речення

$$\mathbf{C}_n = \exists z(\neg E z\mathrm{c}_1 \wedge \neg E z\mathrm{c}_2 \wedge \ldots \wedge \neg E z\mathrm{c}_n)$$

для віск натуральних n. Нову теорію позначимо $\mathfrak{T}^*$. Легко бачити, що ця теорія не має скінченних нормальних моделей. Розглянемо довільну скінченну частину $\mathfrak{T}'$ теорії $\mathfrak{T}^*$. Вона містить лише скінченну кількість речень вигляду $\neg E\mathrm{c}_i\mathrm{c}_j$, а також скінченну кількість речень $\mathbf{C}_n$. Нехай n_0 є найбільшим з чисел $\max\{\, n \mid \mathbf{C}_n \in \mathfrak{T}' \,\}$ та $\max\{\, j \mid \neg E\mathrm{c}_i\mathrm{c}_j \in \mathfrak{T}' \text{ для деякого } i \,\}$. За припущенням, теорія $\mathfrak{T}$ має модель $\mathcal{I}$, потужність якої більша за n_0. Виберемо в області M цієї моделі n_0 різних елементів $a_1, a_2, \ldots, a_{n_0}$ і елемент b, відмінний від усіх a_i $(i = 1, 2, \ldots, n_0)$. Продовжимо інтерпретацію $\mathcal{I}$ на константи c_n, поклавши $\mathcal{I}(\mathrm{c}_n) = a_n$ при $n \leqslant n_0$ та $\mathcal{I}(\mathrm{c}_n) = b$ при $n > n_0$. Усі речення $\neg E\mathrm{c}_i\mathrm{c}_j$ $(i < j \leqslant n_0)$ істинні в цій інтерпретації. Якщо ϕ — довільний розподіл, то прийнявши за ψ розподіл, який належить ϕ^z і для якого $\psi(z) = b$, бачимо, що речення $\neg E z\mathrm{c}_1 \wedge \neg E z\mathrm{c}_2 \wedge \ldots \wedge \neg E z\mathrm{c}_n$, де $n \leqslant n_0$, має значення $\mathbf{1}$ на цьому розподілі, звідки й $\mathrm{val}(\mathcal{I}, \mathbf{C}_n) = \mathbf{1}$. Отже, $\mathcal{I}$ — модель теорії $\mathfrak{T}'$, а тому остання несуперечлива. За теоремою компактності теорія $\mathfrak{T}^*$, а тому й теорія $\mathfrak{T}$, має зліченну модель $\square$

Одна із схем застосування цього результату така. Розглядається деяке твердження $\mathbf{A}$ теорії груп (полів, кілець тощо), яке можна записати мовою логіки відношень. Припустимо, що це твердження вірне в усіх зліченних групах (полях, кільцях...). Тоді воно вірне в усіх групах (полях, кільцях...), які мають потужність більшу за деяке натуральне число. Дійсно, якщо це не так, теорія $\mathfrak{T}$, яка складається з усіх речень теорії груп (полів, кілець...) та речення $\neg\mathbf{A}$, має скінченні моделі необмеженої потужності, а тому й зліченну модель, що протирічить припущенню. Конкретні приклади застосування цієї (а також інших) схем можна знайти в книгах Мальцева [**Мал2**] та Робертсона [**Роб**].

2.6. Теорема Левенгайма – Сколема.

Нестандартні моделі

У цьому розділі ми розглянемо питання, пов'язані з *підмоделями*, і побачимо нові аргументи на користь тези «математику не можна звести до логіки».

Означення 2.6.1.

1. Нехай $\mathcal{I}$ — модель теорії першого порядку $\mathfrak{T}$ з областю M, а N — підмножина в M. Припустимо, що для кожного функціонала F теорії $\mathfrak{T}$ і кожних елементів $a_1, a_2, \ldots, a_m \in N$, де m — місність F, обов'язково $\mathcal{I}(F)(a_1, a_2, \ldots, a_m) \in N$; зокрема, $\mathcal{I}(\mathrm{c}) \in N$ для кожної константи теорії $\mathfrak{T}$. Тоді можна розглянути *обмеження* $\mathcal{I}_N$ інтерпретації $\mathcal{I}$ на підмножину N, вважаючи, що

$$\mathcal{I}_N(F)(a_1, a_2, \ldots, a_m) = \mathcal{I}(F)(a_1, a_2, \ldots, a_n),$$
$$\mathcal{I}_N(P)(a_1, a_2, \ldots, a_m) = \mathcal{I}(P)(a_1, a_2, \ldots, a_m)$$

   для довільних функціонала F та предиката P. Якщо $\mathcal{I}_N$ також є моделлю теорії $\mathfrak{T}$, її звуть *підмоделлю* моделі $\mathcal{I}$. Кажуть також, що N є підмоделлю в $\mathcal{I}$, або навіть у M, хоча останнє не зовсім коректно, бо модель складається не лише зі своєї області, а ще й з інтерпретацій функціоналів та предикатів.
2. Підмодель N моделі $\mathcal{I}$ зветься *елементарною*, якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathrm{val}(\mathcal{I}_N, \phi, \mathbf{A})$ для кожного речення $\mathbf{A}$ теорії $\mathfrak{T}$ і кожного розподілу $\phi : \mathfrak{X} \to N$. Зокрема, множини замкнених речень, істинних у моделях $\mathcal{I}$ та $\mathcal{I}_N$, збігаються.
3. Якщо N — підмодель (елементарна підмодель) моделі $\mathcal{I}$, то модель $\mathcal{I}$ зветься *розширенням* (відповідно, *елементарним розширенням*) моделі $\mathcal{I}_N$.

Зауважимо, що коли $\mathfrak{T}$ — теорія з рівністю, а $\mathcal{I}$ — нормальна модель, кожна її підмодель також нормальна.

Наприклад, якщо $\mathfrak{T}$ — теорія груп, розглянута у прикладі 2.2.3.2, а $\mathcal{I}$ — модель цієї теорії, тобто структура групи на деякій множині M (області моделі $\mathcal{I}$), то підмодель $\mathcal{I}$ — це підгрупа в групі M. Зауважимо, що коли теорія $\mathfrak{T}$ не містить функціоналів (зокрема, констант), ми можемо розглядати її обмеження на довільну підмножину $N \subseteq M$, хоча, звичайно, не кожна така підмножина буде підмоделлю. Важливий випадок, коли довільна підмножина $N \subseteq M$ така, що існує обмеження $\mathcal{I}_N$, буде підмоделлю — це так звані *універсальні теорії*, тобто такі, що жодне речення $\mathbf{A} \in \mathfrak{T}$ не містить кванторів існування. Читачу пропонується самому переконатися в цьому.

Ми бачили, що коли теорія першого порядку має моделі, вона має й зліченну модель (якщо йдеться про теорії з рівністю та нормальні моделі, скінченну або зліченну). Зокрема, існує зліченна модель елементарної теорії дійсних чисел та інших елементарних теорій, «стандартні» моделі яких напевне незліченні. Можна було б подумати, що це пов'язано з тим, що в цих моделях інтерпретація функціоналів та предикатів істотно відрізняється від звичайної. Наступна теорема показує, що справа полягає не в цьому.

Теорема 2.6.2 (**Теорема Левенгайма – Сколема**). *Нехай $\mathcal{I}$ — модель теорії $\mathfrak{T}$ з областю M, M_0 — деяка скінченна або зліченна підмножина M. Існує скінченна або зліченна елементарна підмодель N у $\mathcal{I}$ така, що $N \supseteq M_0$. Зокрема, кожна нескінченна модель теорії першого порядку містить елементарну зліченну підмодель.*

Доведення. Побудуємо підмножини $M_k \subseteq M$ $(k \in \mathbb{N})$, $M_0 \subseteq M_1 \subseteq M_2 \subseteq \ldots$ рекурентним способом, починаючи з уже даної підмножини M_0. Вважаючи, що M_k уже побудована, віднесемо до M_{k+1}, крім елементів з M_k, усі елементи вигляду $\mathcal{I}(F)(a_1, a_2, \ldots, a_m)$, де F — (m-місний) функціонал, який належить теорії $\mathfrak{T}$, а $a_1, a_2, \ldots, a_m$ — елементи з M_k (зокрема, до M_{k+1} напевне належатимуть усі значення $\mathcal{I}(\mathrm{c})$, де c — константа теорії $\mathfrak{T}$), а також елементи $e(\mathrm{x}, \mathbf{A}, \phi)$, де $\mathbf{A}$ — речення теорії $\mathfrak{T}$, x — невідома, вільна в цьому реченні, а $\phi : \mathfrak{X} \to M_k$ — деякий розподіл, які визначаються в такий спосіб:

- Якщо існує такий розподіл $\psi \in \phi^{\mathrm{x}}$, що $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathbf{1}$, покладемо $e(\mathrm{x}, \mathbf{A}, \phi) = \psi(\mathrm{x})$. Якщо таких розподілів кілька, обираємо один з них, причому такий, що значення $\psi(\mathrm{x})$ спільне для всіх розподілів, які приймають однакові значення на всіх вільних невідомих речення $\mathbf{A}$, крім x (ясно, що тоді значення $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A})$ для всіх таких розподілів також спільне).
- Якщо $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathbf{0}$ для всіх розподілів $\psi \in \phi^{\mathrm{x}}$, покладемо $e(\mathrm{x}, \mathbf{A}, \phi) = a_0$, де a_0 — деякий (фіксований) елемент з M_0 (ясно, що насправді при цьому нічого до M_k не додається взагалі).

Ми стверджуємо, що $N = \bigcup_{k=0}^{\infty} M_k$ є шуканою підмоделлю. Оскільки, очевидно, кожна множина M_k — скінченна або зліченна, такою ж буде й N.

Дійсно, якщо F — m-місний функціонал теорії $\mathfrak{T}$, а $a_1, a_2, \ldots, a_m \in N$, то існує такий номер k, що $a_1, a_2, \ldots, a_m \in M_k$; але тоді $\mathcal{I}(F)(a_1, a_2, \ldots, a_m) \in M_{k+1} \subseteq N$ за побудовою. Перевірку рівності $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathrm{val}(\mathcal{I}_N, \phi, \mathbf{A})$ для всіх розподілів $\phi : \mathfrak{X} \to N$ проведемо індукцією за довжиною речення $\mathbf{A}$. Для елементарних речень вона очевидна, оскільки $\mathcal{I}_N(P)$ є обмеженням на N відношення $\mathcal{I}(P)$. Якщо $\mathbf{A} = \neg\mathbf{B}$, $\mathbf{A} = \mathbf{B} \Rightarrow \mathbf{C}$, $\mathbf{A} = \mathbf{B} \vee \mathbf{C}$ або $\mathbf{A} = \mathbf{B} \wedge \mathbf{C}$, то ця рівність безпосередньо випливає з відповідних рівностей для $\mathbf{B}$ та $\mathbf{C}$. Нехай $\mathbf{A} = \exists \mathrm{x}\mathbf{B}$, причому всі вільні змінні речення $\mathbf{B}$ — це $\mathrm{x}, \mathrm{y}_1, \mathrm{y}_2, \ldots, \mathrm{y}_m$. Знов-таки, знайдеться такий номер k, що всі елементи $\phi(\mathrm{x})$ та $\phi(\mathrm{y}_i)$ $(i = 1, 2, \ldots, m)$ належать до M_k. Якщо $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{0}$, тобто $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{0}$ для кожного $\psi \in \phi^{\mathrm{x}}$, то тим більш $\mathrm{val}(\mathcal{I}_N, \psi, \mathbf{B}) = \mathbf{0}$ для кожного розподілу $\psi : \mathfrak{T} \to N$, $\psi \in \phi^{\mathrm{x}}$, тобто $\mathrm{val}(\mathcal{I}_N, \phi, \mathbf{A}) = \mathbf{0}$. Якщо ж $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$, тобто $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{1}$ для якогось розподілу $\psi \in \phi^{\mathrm{x}}$, то $\mathrm{val}(\mathcal{I}, \psi, \mathbf{B}) = \mathbf{1}$ для розподілу $\psi \in \phi^{\mathrm{x}}$ такого, що $\psi(\mathrm{x}) = e(\mathrm{x}, \mathbf{B}, \phi) \in M_{k+1} \subseteq N$, отже й $\mathrm{val}(\mathcal{I}_N, \phi, \mathbf{A}) = \mathbf{1}$. Випадок $\mathbf{A} = \forall \mathrm{x}\mathbf{B}$ зводиться до попередніх, бо $\forall \mathrm{x}\mathbf{B} \equiv \neg\exists \mathrm{x}\neg\mathbf{B}$.

Нарешті, останнє твердження одержимо, якщо за M_0 взяти якусь зліченну підмножину нескінченної множини M $\square$

Зауваження 2.6.3. Теорему Левенгайма – Сколема можна узагальнити (з тим самим доведенням) на випадок, коли потужність підмножини M_0 незліченна. Тоді елементарна підмодель $N \subseteq M_0$ матиме таку ж потужність, що й M_0. Ми не робимо цього, оскільки не передбачаємо знання теорії множин поза найпростішими властивостями скінченних та зліченних множин.

Теорема Левенгайма – Сколема показує, наприклад, що існує *зліченна* підмножина $\mathbb{R}_0$ поля дійсних чисел $\mathbb{R}$, в якій виконуються всі властивості дійсних чисел, які можна записати мовою логіки відношень, і не

виконується ніяких «зайвих» властивостей. Як ми вже підкреслювали, існування такої підмножини *не залежить* від вибору конкретної множини постулатів — це притаманно довільній теорії першого порядку. Те саме відноситься й до інших математичних теорій. Один з найразючіших парадоксів, так званий «*парадокс Сколема*», виникає, якщо розглядати *теорію множин*. Добре відомо, що для кожної множини M існує множина більшої потужності (наприклад, множина всіх підмножин M). Однак з теореми Левенгайма – Сколема одразу випливає, що при довільній аксіоматизації теорії множин (засобами логіки відношень) існує *зліченна* множина множин, в якій виконуються всі теореми даної формалізації і не виконується жодна «зайва» теорема. Отже, чисто логічні методи не можуть бути адекватними змістовній математичній теорії.

Ще одне підтвердження цієї тези дає така теорема.

Теорема 2.6.4 (Теорема про нестандартні моделі). *Нехай $\mathfrak{T}$ — теорія першого порядку, $\mathcal{I}$ — її зліченна модель. Тоді існує її* власне *елементарне розширення $\mathcal{I}^*$, тобто таке, що область M моделі $\mathcal{I}$ є власною підмножиною області M^* моделі $\mathcal{I}^*$, причому множину M^* також можна вважати зліченною.*

Доведення. Очевидно, можна вважати, що $\mathfrak{T}$ — теорія з рівністю, а модель $\mathcal{I}$ нормальна. Фіксуємо деяку нумерацію елементів множини M: $M = \{\, a_1, a_2, \dots, a_n, \dots \}$. Додамо до теорії $\mathfrak{T}$ зліченну множину нових констант $\mathrm{c}_1, \mathrm{c}_2, \dots, \mathrm{c}_n, \dots$ і продовжимо модель $\mathcal{I}$ на ці константи поклавши $\mathcal{I}(\mathrm{c}_n) = a_n$ для всіх номерів n. Позначимо $\mathfrak{T}^*$ множину всіх замкнених речень розширеної таким чином теорії, які вірні в інтерпретації $\mathcal{I}$. Зокрема, серед них будуть усі речення $\neg E\mathrm{c}_i\mathrm{c}_j$ при $i \neq j$, які виражають той факт, що всі елементи a_n — різні. Додамо до теорії $\mathfrak{T}^*$ нову константу c і всі речення $\neg\mathrm{c}\mathrm{c}_n$ ($n \in \mathbb{N}$). Цю теорію позначимо $\mathfrak{T}^*_{\mathrm{c}}$. Кожна скінченна підмножина $\mathfrak{M} \subseteq \mathfrak{T}^*_{\mathrm{c}}$ несуперечлива. Дійсно, речення з $\mathfrak{M}$ містять лише скінченну кількість констант c_n; нехай m — максимальний номер таких констант. Тоді модель $\mathcal{J}$ теорії $\mathfrak{M}$ на множині M можна визначити, інтерпретуючи всі функціонали та предикати з $\mathfrak{T}$ так, як у моделі $\mathcal{I}$, і поклавши $\mathcal{J}(\mathrm{c}_n) = a_n$ при $n \leqslant m$, $\mathcal{J}(\mathrm{c}) = a_{m+1}$. За теоремою про компактність, теорія $\mathfrak{T}^*_{\mathrm{c}}$ також має модель $\mathcal{I}^*$, область M^* якої можна вважати зліченною (очевидно, $\mathfrak{T}^*_{\mathrm{c}}$ скінченних моделей не має). Позначимо $b_n = \mathcal{I}^*(\mathrm{c}_n)$, $b = \mathcal{I}^*(\mathrm{c})$, $N = \{\, b_1, b_2, \dots, b_n, \dots \}$. Зауважимо, що $b \notin N$. Нехай $\mathbf{A}$ — речення теорії $\mathfrak{T}$, $\phi : \mathfrak{X} \to N$ — деякий розподіл. Очевидно, що $\mathrm{val}(\mathcal{I}^*, \phi, \mathbf{A}) = \mathrm{val}(\mathcal{I}^*, \mathbf{A}^{\mathrm{x}_1,\mathrm{x}_2,\dots,\mathrm{x}_k}_{\mathrm{c}_{i1},\mathrm{c}_{i2},\dots,\mathrm{c}_{ik}})$, де $\mathrm{x}_1, \mathrm{x}_2, \dots, \mathrm{x}_k$ — усі вільні змінні речення $\mathbf{A}$, причому $\phi(\mathrm{x}_j) = b_{j_i}$. Так само для кожного розподілу $\psi : \mathfrak{X} \to M$ $\mathrm{val}(\mathcal{I}, \psi, \mathbf{A}) = \mathrm{val}(\mathcal{I}, \mathbf{A}^{x_1,x_2,\dots,x_k}_{\mathrm{c}_{i1},\mathrm{c}_{i2},\dots,\mathrm{c}_{ik}})$, де $\psi(\mathrm{x}_j) = a_{ij}$. Тому ми можемо замінити елементи $b_n \in N$ на елементи $a_n \in M$, внесши відповідні зміни до визначення $\mathcal{I}^*(F)$ та $\mathcal{I}^*(P)$; зокрема, вважаючи що $\mathcal{I}^*(\mathrm{c}_n) = a_n$. Тоді $\mathcal{I}^*$ стає власним елементарним розширенням моделі $\mathcal{I}$ теорії $\mathfrak{T}$ $\square$

Зауваження 2.6.5. Так само, як і в зауваженні 2.6.3, обмеження на потужність M можна вилучити. Тоді множину M^* можна вибрати тієї ж потужності, яку має M. Знов-таки, це потребує дещо складнішої

теоретико-множинної техніки ніж та, знайомство з якою ми передбачаємо в читача.

Назва «теорема про нестандартні моделі» пояснюється таким її застосуванням. Припустимо, що ми вивчаємо якусь конкретну математичну систему M (наприклад, натуральні числа) і намагаємось формалізувати її вивчення мовою логіки відношень. Нехай $\mathfrak{T}$ — відповідна теорія першого порядку. Якщо лише ця теорія коректна, тобто всі речення $\mathbf{A} \in \mathfrak{T}$ вірні в системі M, то цю систему можна розглядати як модель теорії $\mathfrak{T}$, яка зветься «стандартною моделлю». Тоді теорема 2.6.4 стверджує, що теорія $\mathfrak{T}$ має й інші моделі, які є власними елементарними розширеннями моделі M. Саме такі моделі звуться «*нестандартними*». Отже, існування нестандартних моделей — обов'язкова риса будь-якої формалізації конкретної математичної теорії засобами логіки відношень.

Слід зазначити, що існування нестандартних моделей, яке здається істотним недоліком таких формалізацій, іноді виявляється досить сильним інструментом дослідження даної математичної теорії і доведення змістовних теорем. Найразючіші приклади виникають у так званому «нестандартному аналізі», який користується нестандартними моделями теорії дійсних чисел та функцій дійсної змінної. Із застосуваннями нестандартного аналізу можна познайомитись за книгою [**Дев**] або за більш елементарною, але й більш доступною для початківця брошурою [**Усп**].

Нестандартні моделі мають, як правило, несподівані риси. Одну з них ми пропонуємо читачу як вправу.

Вправа 2.6.6.

1. Нехай $\mathbb{N}^* \supset \mathbb{N}$ — нестандартна модель арифметики натуральних чисел. Довести, що в $\mathbb{N}^*$ є «нескінченно велике число», тобто такий елемент A, що $A > n$ для кожного «справжнього» натурального числа $n \in \mathbb{N}$.

   Вказівка: Скористайтеся тим, що у звичайній арифметиці натуральних чисел вірним є таке твердження:

   Якщо $a \leqslant n$, *то* $a \in \{1, 2, \ldots, n\}$.

2. Нехай $\mathbb{R}^* \supset \mathbb{R}$ — нестандартна модель арифметики дійсних чисел. Доведіть, що в $\mathbb{R}^*$ є як «нескінченно велике число», тобто такий елемент A, що $A > c$ для всіх «звичайних» чисел $c \in \mathbb{R}$, так і «нескінченно мале число», тобто такий елемент α, що $0 < \alpha < c$ для кожного додатного $c \in \mathbb{R}$.

   Вказівка: Скористайтеся таким твердженням, вірним у звичайній арифметиці дійсних чисел:

   Якщо $0 < a < n$, *де* n — *натуральне число, то для кожного натурального* m *існує таке* $k \in \{1, 2, \ldots, mn\}$, *що* $k/m \leqslant a < (k+1)/m$.

   Розглянувши (звичайну) границю $b = \lim_{m\to\infty} k/m$ (доведіть, що вона існує), покажіть, що коли $a \neq b$, то $|a - b|$ — нескінченно мале число.

2.7. Виводи з вибором. Сколемівські форми

Розглянемо ще один спосіб виводу теорем у численні відношень, так званий «*вивід з вибором*». Він є формалізацією прийому, часто вживаного в математиці, коли, довівши існування об'єкта з деякими властивостями, кажуть: «нехай тепер C — такий об'єкт» (навіть якщо доведення було неефективним, тобто не давало явної конструкції об'єкта з потрібними властивостями).

Означення 2.7.1.

1. *Вивід з вибором* речення $\mathbf{A}$ з теорії $\mathfrak{T}$ — це така послідовність речень $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n = \mathbf{A}$, що для кожного номера i виконується одна з можливостей:
   (a) $\mathbf{A}_i$ є аксіомою.
   (b) $\mathbf{A}_i \in \mathfrak{T}$.
   (c) Існує номер $j < i$ такий, що $\mathbf{A}_j = \exists \mathrm{x}\mathbf{B}$, а $\mathbf{A}_i = \mathbf{B}^{\mathrm{x}}_{\mathrm{c}}$, де x — довільна змінна, а c — константа, яка не зустрічається в реченнях з теорії $\mathfrak{T}$, реченні $\mathbf{A}$ та реченнях $\mathbf{A}_k$ при $k < i$. У цьому випадку назвемо речення $\mathbf{A}_i$ *B-реченням* («реченням з вибором»).
   (d) $\mathbf{A}_i$ одержане з попередніх речень за правилом modus ponens або за правилом узагальнення за деякою змінною, яка не є вільною в жодному з попередніх B-речень.
2. Якщо $\mathfrak{T} = \mathfrak{T}_1 \cup \mathfrak{T}_2$, то кажуть, що речення $\mathbf{A}_i$ в цьому виводі *не залежить від* $\mathfrak{T}_2$, якщо існує підпослідовність $\mathbf{A}_{i1}, \mathbf{A}_{i2}, \ldots, \mathbf{A}_{ik}$ цього виводу, яка містить $\mathbf{A}_i$ та є виводом з вибором з теорії $\mathfrak{T}_1$.
3. Вивід з вибором $\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_n$ зветься *вільним для* $\mathfrak{T}_2$, якщо в ньому узагальнення за змінними, які є вільними в реченнях з $\mathfrak{T}_2$, не застосовуються до речень, які залежать від $\mathfrak{T}_2$ у цьому виводі.

Приклад 2.7.2.

1. Наступна послідовність речень є виводом з вибором речення $\exists \mathrm{x}\mathbf{B}$ із речень $\forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B})$ та $\exists \mathrm{x}\mathbf{A}$:

   $$\exists \mathrm{x}\mathbf{A},\ \text{(B)}\ \mathbf{A}^{\mathrm{x}}_{\mathrm{c}},\ \forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}),\ \mathbf{A}^{\mathrm{x}}_{\mathrm{c}} \Rightarrow \mathbf{B}^{\mathrm{x}}_{\mathrm{c}},$$
   $$\mathbf{B}^{\mathrm{x}}_{\mathrm{c}},\ \mathbf{B}^{\mathrm{x}}_{\mathrm{c}} \Rightarrow \exists \mathrm{x}\mathbf{B},\ \exists \mathrm{x}\mathbf{B}.$$

   Тут B-реченням є друге, позначене знаком (B). Після того, як B-виводи будуть обґрунтовані, звідси одержимо, що $\vdash \forall \mathrm{x}(\mathbf{A} \Rightarrow \mathbf{B}) \Rightarrow (\exists \mathrm{x}\mathbf{A} \Rightarrow \exists \mathrm{x}\mathbf{B})$ — схема доведення, яка досить широко застосовується як у математиці, так і в повсякденному житті.
2. Наведемо приклад, який показує, що обмеження, накладене на застосування узагальнення в пункті 1d, є істотним. Дійсно, розглянемо послідовність речень

   $$\forall \mathrm{x}\exists \mathrm{y}\mathbf{A},\ \exists \mathrm{y}\mathbf{A},\ \text{(B)}\ \mathbf{A}^{\mathrm{y}}_{\mathrm{c}},\ \text{(*)}\ \forall \mathrm{x}\mathbf{A}^{\mathrm{y}}_{\mathrm{c}},$$
   $$\forall \mathrm{x}\mathbf{A}^{\mathrm{y}}_{\mathrm{c}} \Rightarrow \exists \mathrm{y}\forall \mathrm{x}\mathbf{A},\ \exists \mathrm{y}\forall \mathrm{x}\mathbf{A}.$$

   Єдине місце, де умови означення 2.7.1 порушені — це четверте речення (позначене зірочкою). Воно одержане з попереднього узагальненням за змінною x, яка є вільною у B-реченні, позначеному

(в). Якби цей вивід був допустимим, ми б одержали вивід речення $\forall \mathrm{x}\exists \mathrm{y}\mathbf{A} \Rightarrow \exists \mathrm{y}\forall \mathrm{x}\mathbf{A}$. Однак добре відомо, що останнє речення не є тотожно-істинним; воно не є таким навіть на довільній множині, яка містить принаймні два елементи. Достатньо покласти $\mathbf{A} = P\mathrm{xy}$, де P — двомісний предикат, і розглянути інтерпретацію $\mathcal{I}$, в якій $\mathcal{I}(F)$ — відношення рівності.

Наступна теорема виправдовує застосування виводів з вибором у численні відношень.

Теорема 2.7.3. *Нехай $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ — вивід з вибором речення $\mathbf{A}$ з теорії $\mathfrak{T}$. Існує звичайний вивід речення $\mathbf{A}$ з теорії $\mathfrak{T}$. Якщо $\mathfrak{T} = \mathfrak{T}_1 \cup \mathfrak{T}_2$ і даний вибір з виводом є вільним для $\mathfrak{T}_2$, те саме залишається вірним і в результуючому звичайному виводі.*

Доведення. Ми знов укажемо, як переробити вивід з вибором $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ у звичайний вивід $\mathbf{A}$ з $\mathfrak{T}$. Нехай $\mathfrak{B} = \{\, \mathbf{A}_{i_1}, \mathbf{A}_{i_2}, \ \ldots, \mathbf{A}_{i_m} \,\}$ — усі B-речення даного виводу з вибором, причому останнє з них має вигляд $\mathbf{B}^{\mathrm{x}}_{\mathrm{c}}$. Тоді ту саму послідовність $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_n$ можна розглядати як вивід $\mathbf{A}$ з теорії $\mathfrak{T} \cup \mathfrak{B}$, вільний для $\mathfrak{B}$. За теоремою дедукції, його можна переробити у вивід речення $\mathbf{B}^{\mathrm{x}}_{\mathrm{c}} \Rightarrow \mathbf{A}$ з теорії $\mathfrak{T} \cup \mathfrak{B}'$, де $\mathfrak{B}' = \{\, \mathbf{A}_{i1}, \mathbf{A}_{i2}, \ldots, \mathbf{A}_{im-1} \,\}$, вільний для $\mathfrak{B}'$. Виберемо змінну y, яка не зустрічається в останньому виводі, і замінимо в усіх його реченнях константу c на змінну y. Одержимо вивід речення $\mathbf{B}^{\mathrm{x}}_{\mathrm{y}} \Rightarrow \mathbf{A}$. Додамо до нього речення

$$\forall \mathrm{y}(\mathbf{B}^{\mathrm{x}}_{\mathrm{y}} \Rightarrow \mathbf{A}),\ \forall \mathrm{x}(\mathbf{B} \Rightarrow \mathbf{A}),\ \exists \mathrm{x}\mathbf{B} \Rightarrow \mathbf{A},\ \exists \mathrm{x}\mathbf{B},\ \mathbf{A}.$$

Одержимо вивід речення $\mathbf{A}$ з теорії $\mathfrak{T} \cup \mathfrak{B}'$, вільний для $\mathfrak{B}'$. Перші три речення тут еквівалентні, а речення $\exists \mathrm{x}\mathbf{B}$ виводиться з $\mathfrak{T} \cup \mathfrak{B}'$, причому цей вивід — просто частина початкового B-виводу — вільний для $\mathfrak{B}'$. Оскільки єдине нове узагальнення — це узагальнення за змінною y, то одержаний вивід є вільним для $\mathfrak{T}_2$, якщо таким був початковий B-вивід. У той самий спосіб ми можемо вилучити останнє речення з $\mathfrak{B}'$ і т.д., врешті-решт одержавши необхідний вивід $\mathbf{A}$ з $\mathfrak{T}$ □

Вправа 2.7.4. За допомогою виводів з вибором доведіть, що

$$\vdash \exists \mathrm{x}(\mathbf{A} \wedge \mathbf{B}) \Rightarrow \exists \mathrm{x}\mathbf{A} \wedge \exists \mathrm{x}\mathbf{B},$$
$$\vdash (\forall \mathrm{x}\mathbf{A} \vee \forall \mathrm{x}\mathbf{B}) \Rightarrow \forall \mathrm{x}(\mathbf{A} \vee \mathbf{B}).$$

Застосуємо теорему 2.7.3 для того, щоб вивести ще одну важливу властивість теорій першого порядку.

Означення 2.7.5.

1. Пренексне речення $\mathbf{A}$ зветься *сколемівським*, якщо його префікс має вигляд $\exists \mathrm{x}_1 \ldots \exists \mathrm{x}_m \forall \mathrm{y}_1 \ldots \forall \mathrm{y}_k$ (можливо, $m = 0$ або $k = 0$).
2. Нехай $\mathfrak{P}$ — деяка множина предикатів. Будемо казати, що теорія $\mathfrak{T}$ є $\mathfrak{P}$-*теорією*, якщо всі предикати цієї теорії належать множині $\mathfrak{P}$.
3. Нехай $\mathfrak{P}$ — деяка множина предикатів. Сколемівське речення $\mathbf{A}'$ зветься *сколемівською формою* речення $\mathbf{A}$ відносно множини $\mathfrak{P}$, якщо для кожної *чистої* $\mathfrak{P}$-теорії $\mathfrak{T}$ $\mathfrak{T} \vdash \mathbf{A}$ тоді й лише тоді, коли $\mathfrak{T} \vdash \mathbf{A}'$.

Згідно з теоремою про адекватність, останню умову можна також подати у вигляді: $\mathfrak{T} \models \mathbf{A}$ тоді й лише тоді, коли $\mathfrak{T} \models \mathbf{A}'$. У цій формі її часто легше перевіряти, але ми завжди будемо доводити саме синтаксичну умову, оскільки для неї всі наступні твердження насправді є *ефективними*, тобто дозволяють за виводом $\mathbf{A}$ явно побудувати вивід $\mathbf{A}'$ і навпаки.

Теорема 2.7.6. *Нехай $\mathfrak{P}$ — така множина предикатів, що існує нескінченно багато предикатів, які не належать $\mathfrak{P}$. Для кожного речення чистої логіки відношень $\mathbf{A}$ існує сколемівська форма речення $\mathbf{A}$ відносно множини $\mathfrak{P}$.*

Доведення. Скористаємося такою лемою.

Лема 2.7.7. *Нехай $\mathbf{A} = \exists \mathrm{x}_1 \exists \mathrm{x}_2 \dots \exists \mathrm{x}_m \forall \mathrm{y} \mathbf{B}$ — речення чистої логіки відношень, P — $(m+1)$-місний предикат, який не міститься в $\mathfrak{P}$ і не зустрічається в реченні $\mathbf{A}$, $\mathbf{A}' = \exists \mathrm{x}_1 \exists \mathrm{x}_2 \dots \exists \mathrm{x}_m \big(\forall \mathrm{y}(\mathbf{B} \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \dots \mathrm{x}_m\mathrm{y}) \Rightarrow \forall \mathrm{y} P\mathrm{x}_1\mathrm{x}_2 \dots \mathrm{x}_m\mathrm{y}\big)$. Якщо $\mathfrak{T} \vdash \mathbf{A}$ для деякої $\mathfrak{P}$-теорії $\mathfrak{T}$, то й $\mathfrak{T} \vdash \mathbf{A}'$ і навпаки.*

Доведення. Нехай $\mathfrak{T} \vdash \mathbf{A}$. Тоді вивід з вибором речення $\mathbf{A}'$ будується так. Перш за все, вводимо нові константи $\mathrm{c}_1, \mathrm{c}_2, \dots, \mathrm{c}_m$ і речення $\forall \mathrm{y} \mathbf{B}^{\mathrm{x}_1\mathrm{x}_2\dots\mathrm{x}_m}_{\mathrm{c}_1\mathrm{c}_2\dots\mathrm{c}_m}$. З тавтології $X \Rightarrow ((X \Rightarrow Y) \Rightarrow Y))$ та твердження 2.4.5.1 одержимо

$$\vdash \forall \mathrm{y} \mathbf{B}^{\mathrm{x}_1\mathrm{x}_2\dots\mathrm{x}_m}_{\mathrm{c}_1\mathrm{c}_2\dots\mathrm{c}_m} \Rightarrow \big(\forall \mathrm{y}\big(\mathbf{B}^{\mathrm{x}_1\mathrm{x}_2\dots\mathrm{x}_m}_{\mathrm{c}_1\mathrm{c}_2\dots\mathrm{c}_m} \Rightarrow P\mathrm{c}_1\mathrm{c}_2\dots\mathrm{c}_m\mathrm{y}\big) \Rightarrow \forall y P\mathrm{c}_1\mathrm{c}_2\dots\mathrm{c}_m\mathrm{y}\big).$$

Скориставшись аксіомою (A12), одержимо вивід речення $\mathbf{A}'$.

Навпаки, нехай існує вивід речення $\mathbf{A}'$ з $\mathfrak{T}$. Можна вважати, що в цьому виводі всі терми — це змінні й жодна вільна змінна жодного речення не є пов'язаною змінною речення $\mathbf{B}$. Замінимо в кожному реченні цього виводу кожне входження слова $P\mathrm{u}_1\mathrm{u}_2\dots\mathrm{u}_m\mathrm{v}$, де $\mathrm{u}_1, \mathrm{u}_2, \dots, \mathrm{u}_m, \mathrm{v}$ — довільні змінні, словом $\mathbf{B}^{\mathrm{x}_1\mathrm{x}_2\dots\mathrm{x}_m\mathrm{y}}_{\mathrm{u}_1\mathrm{u}_2\dots\mathrm{u}_m\mathrm{v}}$ (саме в цьому місці важливо, що кожен *терм* є насправді деякою *змінною*). Легко бачити (переконайтеся в цьому), що в результаті одержимо вивід речення

$$\widetilde{\mathbf{A}} = \exists \mathrm{x}_1 \exists \mathrm{x}_2 \dots \exists \mathrm{x}_m \big(\forall \mathrm{y}(\mathbf{B} \Rightarrow \mathbf{B}) \Rightarrow \forall \mathrm{y} \mathbf{B}\big).$$

Оскільки $\vdash \mathbf{B} \Rightarrow \mathbf{B}$ (ПВТ), також $\vdash \forall \mathrm{y}(\mathbf{B} \Rightarrow \mathbf{B})$, звідки, очевидно, $\forall \mathrm{y} \mathbf{B} \equiv \forall \mathrm{y}(\mathbf{B} \Rightarrow \mathbf{B}) \Rightarrow \forall \mathrm{y} \mathbf{B}$. За твердженням 2.4.5.2, $\widetilde{\mathbf{A}} \equiv \mathbf{A}$, отже, існує вивід $\mathbf{A}$ з $\mathfrak{T}$. □

Нехай тепер $\mathbf{A}$ — довільне речення чистої логіки відношень. За теоремою 2.4.8 можна вважати, що це речення пренексне. Нехай його префікс має вигляд $\forall = \exists \mathrm{x}_1 \exists \mathrm{x}_2 \dots \exists \mathrm{x}_m \forall \mathrm{y} \Pi \mathbf{B}$, де $\Pi = \mathrm{Q}_1\mathrm{u}_1 \dots \mathrm{Q}_r\mathrm{u}_r$ — деякий префікс, а $\mathbf{B}$ — безквантorне речення. Позначимо

$$\mathbf{A}' = \exists \mathrm{x}_1 \exists \mathrm{x}_2 \dots \exists \mathrm{x}_m \big(\forall \mathrm{y}(\Pi \mathbf{B} \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \dots \mathrm{x}_m\mathrm{y}) \Rightarrow \forall \mathrm{y} P\mathrm{x}_1\mathrm{x}_2 \dots \mathrm{x}_m\mathrm{y}\big),$$

де P — $(m+1)$-місний предикат, який не належить $\mathfrak{P}$ і не зустрічається в реченні $\mathbf{B}$. За лемою 2.7.7 для кожної чистої $\mathfrak{P}$-теорії $\mathfrak{T}$ $\mathfrak{T} \vdash \mathbf{A}$ тоді й лише тоді, коли $\mathfrak{T} \vdash \mathbf{A}'$. З іншого боку, згідно з твердженням 2.4.5.6 та

вправою 2.4.6.2,3,

$$\begin{aligned}\mathbf{A}' &\equiv \exists \mathrm{x}_1 \exists \mathrm{x}_2 \ldots \exists \mathrm{x}_m \forall \mathrm{y} \big(\Pi'(\mathbf{B} \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{y}) \Rightarrow \forall \mathrm{v} P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{v})\big) \\ &\equiv \exists \mathrm{x}_1 \exists \mathrm{x}_2 \ldots \exists \mathrm{x}_m \exists \mathrm{y} \Pi \big((\mathbf{B} \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{y}) \Rightarrow \forall \mathrm{v} P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{v}\big) \\ &\equiv \exists \mathrm{x}_1 \exists \mathrm{x}_2 \ldots \exists \mathrm{x}_m \exists \mathrm{y} \Pi \forall \mathrm{v} \big((\mathbf{B} \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{y}) \Rightarrow P\mathrm{x}_1\mathrm{x}_2 \ldots \mathrm{x}_m\mathrm{v}\big),\end{aligned}$$

де v — змінна, яка не зустрічається в реченні $\mathbf{A}$, $\Pi' = \mathrm{Q}'_1\mathrm{u}_1 \ldots \mathrm{Q}'_r\mathrm{u}_r$, а Q'_j, як і раніше — квантор, відмінний від Q_j. Останнє речення, яке ми позначимо $\mathbf{A}''$, знов пренексне, $\mathfrak{T} \vdash \mathbf{A}$ тоді й лише тоді, коли $\mathfrak{T} \vdash \mathbf{A}''$, але в $\mathbf{A}''$ вже менша кількість кванторів загальності передують кванторам існування. Повторюючи цю процедуру, ми побудуємо сколемівську форму речення $\mathbf{A}$ $\square$

Вправа 2.7.8.

1. Побудуйте сколемівську форму речення $\forall \mathrm{x} \exists \mathrm{y} \mathbf{A}$.
2. Речення $\mathbf{A}$ зветься *виконуваним* у теорії $\mathfrak{T}$, якщо знайдуться модель $\mathcal{I}$ цієї теорії та розподіл ϕ в інтерпретації $\mathcal{I}$ такі, що $\mathrm{val}(\mathcal{I}, \phi, \mathbf{A}) = \mathbf{1}$. Нехай знову $\mathfrak{P}$ — така множина предикатів, що існує нескінченно багато предикатів, які не належать $\mathfrak{P}$. Доведіть, що для кожного речення $\mathbf{A}$ чистої логіки відношень існує таке речення $\mathbf{A}'$ вигляду $\forall \mathrm{x}_1 \ldots \forall \mathrm{x}_m \exists \mathrm{y}_1 \ldots \exists \mathrm{y}_m \mathbf{B}$, де $\mathbf{B}$ не містить кванторів, що для кожної $\mathfrak{P}$-теорії $\mathfrak{T}$ речення $\mathbf{A}$ виконуване в $\mathfrak{T}$ тоді й лише тоді, коли $\mathbf{A}'$ виконуване в цій теорії.
3. Побудуйте речення $\mathbf{A}'$, про яке йдеться в попередній вправі, для речення $\exists \mathrm{x} \forall \mathrm{y} \mathbf{A}$.
4. Поясніть, чому обмеження на множину предикатів $\mathfrak{P}$, накладене в теоремі 2.7.7 та у вправі 2.7.8, насправді не є істотним.

Розділ 3

Формальна арифметика

3.1. Аксіоматика

Означення 3.1.1.

1. Будемо називати *формальною арифметикою* (натуральних чисел) теорію першого порядку з рівністю $\mathfrak{A}$, яка має (крім предиката E) дві константи c_0 та c_1 і два двомісні функціонали S і P, і містить (крім постулатів рівності) такі постулати:
   (N1) $\mathrm{v}+1\neq 0$;
   (N2) $\mathrm{v}+1=\mathrm{v}_1+1\Rightarrow \mathrm{v}=\mathrm{v}_1$;
   (N3) $\mathrm{v}+0=\mathrm{v}$;
   (N4) $\mathrm{v}+(\mathrm{v}_1+1)=(\mathrm{v}+\mathrm{v}_1)+1$;
   (N5) $\mathrm{v}\cdot 0=0$;
   (N6) $\mathrm{v}\cdot(\mathrm{v}_1+1)=\mathrm{v}\cdot\mathrm{v}_1+\mathrm{v}$;
   (N7) $\mathbf{A}_0^{\mathrm{v}}\wedge\forall\mathrm{v}(\mathbf{A}\Rightarrow\mathbf{A}_{\mathrm{v}+1}^{\mathrm{v}})\Rightarrow\forall\mathrm{v}\mathbf{A}$,
   де $\mathbf{A}$ — довільне речення, в якому v є вільною змінною.

   Тут і надалі, дотримуючись звичайних арифметичних позначень, пишемо 0 замість c_0; 1 замість c_1; $a+b$ замість Sab; $a\cdot b$, чи навіть ab, якщо це не викликає непорозумінь, замість Pab; $a=b$ замість Eab; $a\neq b$ замість $\neg a=b$ і вживаємо звичного порядку дій: $\cdot$ виконується раніше ніж $+$, якщо інше не передбачено розстановкою дужок. Надалі будемо також вживати скорочення:
   $a\leqslant b$ позначає $\exists\mathrm{v}\ a+\mathrm{v}=b$;
   $a<b$ позначає $a\leqslant b\wedge a\neq b$;
   $\overline{\mathrm{n}}=\underbrace{(\ldots((1+1)+1)+\cdots+1)}_{n\text{ разів}}$.
2. *Стандартною моделлю* теорії $\mathfrak{A}$ називається інтерпретація $\mathcal{N}$ з областю $\mathbb{N}$ (звичайна множина натуральних чисел з нулем), в якій $\mathcal{N}(E)$ — відношення рівності, $\mathcal{N}(S)(a,b)=a+b$ і $\mathcal{N}(P)(a,b)=ab$.

Очевидно, (N7) — це насправді зліченна множина постулатів, відповідно до зліченної множини речень $\mathbf{A}$. Ці постулати називаються «*постулатами індукції*»[1]. Застосовуючи «перейменування змінних», легко бачити, що з постулатів (N7) виводяться довільні речення вигляду $\mathbf{A}_0^{\mathrm{x}}\wedge\forall\mathrm{x}(\mathbf{A}\Rightarrow\mathbf{A}_{\mathrm{x}+1}^{\mathrm{x}})\Rightarrow\forall\mathrm{x}\mathbf{A}$, де x — довільна змінна, яка є вільною

[1] Їх частіше називають «аксіомами індукції», але ми віддаємо перевагу терміну «постулат», як це звичайно робиться для тих речень теорії, які не збігаються з аксіомами числення відношень.

в реченні $\mathbf{A}$. Такі речення також будемо називати «постулатами індукції», хоча, строго кажучи, вони є не постулатами, а теоремами теорії $\mathfrak{A}$. Надалі ми часто писатимемо $\mathbf{A}(\mathrm{x})$ на знак того, що x є (або принаймні може бути) вільною змінною в реченні $\mathbf{A}$, і позначатимемо $\mathbf{A}(\mathrm{t})$ результат підстановки $\mathbf{A}^{\mathrm{x}}_{\mathrm{t}}$. Якщо одночасно розглядаються дві, три та більше вільних невідомих, пишуть $\mathbf{A}(\mathrm{x},\mathrm{y})$, $\mathbf{A}(\mathrm{x}_1,\mathrm{x}_2,\mathrm{x}_3)$; відповідно $\mathbf{A}(a,b)$, $\mathbf{A}(c_1,\ c_2,c_3)$ і т.п. Ми також уживатимемо скорочення $\mathbf{A}\Leftrightarrow\mathbf{B}$ замість $(\mathbf{A}\Rightarrow\mathbf{B})\wedge(\mathbf{B}\Rightarrow\mathbf{A})$ (це відповідає змісту сполучника $\Leftrightarrow$, який ми не включили до алфавіту логіки відношень) і писатимемо $\exists!\mathrm{x}\mathbf{A}(\mathrm{x})$ замість $\exists\mathrm{x}\big(\mathbf{A}(\mathrm{x})\wedge(\mathbf{A}(\mathrm{y})\Rightarrow\mathrm{y}=\mathrm{x})\big)$.

Зауважимо, що, узагалі кажучи, ні звідки не випливає, що $\mathcal{N}$ дійсно є *моделлю* формальної арифметики. Більш того, надалі побачимо, що це твердження не може бути *формально* доведено. Утім його фактично приймають усі математики.[2] Назвемо це припущення «*принципом коректності*» формальної арифметики або «*гіпотезою про стандартну модель*». З нього випливає *несуперечливість* теорії $\mathfrak{A}$ (суперечлива теорія не має моделей). Інколи ми вживатимемо більш сильний наслідок із принципу коректності — так звану «*ω-несуперечливість*», яка полягає в твердженні:

($\boldsymbol{\Omega}$) *Не існує такого речення* $\mathbf{A}(\mathrm{v})$ *теорії* $\mathfrak{A}$, *що* $\mathfrak{A}\vdash\neg\mathbf{A}(\overline{\mathrm{n}})$ *для кожного натурального* n *і одночасно* $\mathfrak{A}\vdash\exists\mathrm{v}\mathbf{A}$.

Традиційна трактовка натуральних чисел як таких, що утворюються послідовним додаванням одиниць, свідчить на користь твердження про ω-несуперечливість.

З іншого боку, надалі ми доведемо, що формальна арифметика, на відміну від числення відношень, *не є адекватною* (до «неформальної» арифметики натуральних чисел): у ній існують такі замкнені речення $\mathbf{A}$, які істинні у стандартній моделі, але не є теоремами теорії $\mathfrak{A}$. Очевидно, тоді ані $\mathfrak{A}\vdash\mathbf{A}$, ані $\mathfrak{A}\vdash\neg\mathbf{A}$, тобто формальна арифметика також *не є повною*. Більш того, цьому не можна зарадити ніяким *ефективним* розширенням множини постулатів. Під ефективністю розуміється існування алгоритма, який за кожним реченням перевіряє, чи є воно постулатом, чи ні.

Зауваження. У підручниках з математичної логіки здебільшого прийнятий трохи відмінний варіант формальної арифметики, в якому немає константи 1, але крім функціоналів S та P є ще додатковий одномісний функціонал N (пишуть t' замість $N\mathrm{t}$) — формалізація поняття «наступне число». Відповідно змінюються всі аксіоми, в яких "+1" всюди замінюється на "$'$", а терм $\overline{\mathrm{n}}$ визначається як $\underbrace{NN\ldots N}_{n\text{ разів}}0$. Така формалізація ближча до початкових ідей Пеано. Легко бачити, що ці дві формалізації рівносильні. Ми обрали ту з них, яка має «кількісний» характер, на відміну від «порядкового» характеру аксіом Пеано. Це, звичайно, є лише питанням смаку, але нам ближче піфагорейський погляд на натуральні числа (порівняйте евклідове «*число є сукупність одиниць*»).

[2] Або *майже всі*, тобто, за прийнятою в математичному жаргоні традицією, *усі, крім скінченного числа.*

Розглянемо приклади виводів у формальній арифметиці. Сподіваємося, що читач уже має достатньо досвіду, щоб відтворювати очевидні деталі наступних доведень, тому ми надалі будемо все більше їх скорочувати.

Твердження 3.1.2. *Наведені речення є теоремами формальної арифметики:*

1. $x \neq 0 \Rightarrow \exists y\, x = y + 1$.
2. $x + y = y + x$.
3. $(x + y) + z = x + (y + z)$.
4. $x(y + z) = xy + xz$ і $(x + y)z = xz + yz$.
5. $xy = yx$.
6. $x(yz) = (xy)z$.
7. $x + z = y + z \Rightarrow x = y$.
8. $x \leqslant y \vee y \leqslant x$ (або, що те саме, $x < y \vee y < x \vee x = y$).

9. $x < y + 1 \Leftrightarrow x \leqslant y$ і $x < y \Rightarrow x + 1 \leqslant y$, зокрема, $\neg x < 0$.
10. $x + y = 0 \Rightarrow x = 0 \wedge y = 0$.
11. $xy = 0 \Rightarrow x = 0 \vee y = 0$
12. $xz = yz \wedge z \neq 0 \Rightarrow x = y$.
13. $x < y \Rightarrow x + z < y + z$.
14. $x < y \wedge z \neq 0 \Rightarrow xz < yz$.

Доведення. 1. Позначимо це речення $\mathbf{A}(x)$. Очевидно, $\mathfrak{A} \vdash \mathbf{A}(0)$ (це ПВТ $\neg X \Rightarrow (X \Rightarrow Y)$). З іншого боку, $x+1 = x+1 \Rightarrow \exists y\, x+1 = y+1$ — аксіома (A11), отже $\mathfrak{A} \vdash \exists y\, x + 1 = y + 1$ і $\mathfrak{A} \vdash \mathbf{A}(x) \Rightarrow \mathbf{A}(x + 1)$. За постулатом індукції, $\mathfrak{A} \vdash \forall x \mathbf{A}$.

2. Доведемо спочатку, що $\mathfrak{A} \vdash 0 + x = x$. За (N3), $0 + 0 = 0$. Далі, за (N4), $0 + (x + 1) = (0 + x) + 1$, отже, з припущення $0 + x = x$ і аксіоми рівності (E2) виводиться $0+(x+1) = x+1$. Отже, $0+x = 0 \Rightarrow 0+(x+1) = 0$. З постулату індукції $0 + 0 = 0 \wedge \forall x(0 + x = 0 \Rightarrow 0 + (x + 1) = x + 1) \Rightarrow \forall x\, 0 + x = x$ одержуємо $\mathfrak{A} \vdash 0 + x = x$.

Тепер виведемо $(x+1)+y = (x+y)+1$. При $y = 0$ з (N3) та (E2) маємо $(x + 1) + 0 = x + 1 = (x + 0) + 1$. Припустимо, що $(x + 1) + y = (x + y) + 1$. Тоді, за (N4) та (E2), $(x+1)+(y+1) = ((x+1)+y)+1 = ((x+y)+1)+1 = (x + (y + 1)) + 1$. За постулатом індукції, $\mathfrak{A} \vdash (x + 1) + y = (x + y) + 1$.

Припустимо тепер, що $x + y = y + x$. Тоді $(x + 1) + y = (x + y) + 1 = (y + x) + 1 = y + (x + 1)$. За постулатом індукції, $\mathfrak{A} \vdash x + y = y + x$.

3. $(x + y) + 0 = x + y = x + (y + 0)$. Якщо $(x + y) + z = x + (y + z)$, то $(x + y) + (z + 1) = ((x + y) + z) + 1 = (x + (y + z)) + 1 = x + ((y + z) + 1) = x + (y + (z + 1))$. За постулатом індукції, $\mathfrak{A} \vdash (x + y) + z = x + (y + z)$.

4. $x(y + 0) = xy = xy + 0 = xy + x0$. Якщо $x(y + z) = xy + xz$, то $x(y + (z + 1)) = x((y + z) + 1) = x(y + z) + x = (xy + xz) + x = xy + (xz + x) = xy + x(z + 1)$. Отже, $\mathfrak{A} \vdash x(y+z) = xy+xz$. Другу рівність ми одержимо з першої та твердження 5, при доведенні якого не будемо нею користуватися.

5. $0 \cdot 0 = 0$, і якщо $0x = 0$, то $0(x + 1) = 0x + 0 = 0 + 0 = 0$, отже, $\mathfrak{A} \vdash 0x = 0 = x0$. Покажемо, що $\mathfrak{A} \vdash (x + 1)y = yx + y = y(x + 1)$. Якщо $y = 0$, то $(x+1) \cdot 0 = 0 = x \cdot 0+0$. Припустимо, що $(x+1)y = xy+y$. Тоді $(x+1)(y+1) = (x+1)y+(x+1) = (xy+y)+(x+1) = (xy+x)+(y+1) = x(y + 1) + (y + 1)$; отже, за постулатом індукції, $\mathfrak{A} \vdash (x + 1)y = xy + y$. (Ми скористалися вже виведеними формулами 2 і 3; поясніть, де і як.) Тепер $\mathfrak{A} \vdash xy = yx$ знов за постулатом індукції.

6 залишається як вправа читачу. Надалі, користуючись твердженнями 1–5, ми часто будемо опускати дужки у виразах типу $(xy)(zt)$ або $x + ((y + z) + t)$ і писати, відповідно, $xyzt$ та $x + y + z + t$, а також вільно переставляти доданки чи співмножники.

7. При $z = 0$ це випливає з (N3). Припустимо, що $x+z = y+z \Rightarrow x = y$ і $x+(z+1) = y+(z+1)$. Тоді $(x+z)+1 = (y+z)+1$ і, за (N2), $x+z = y+z$, звідки $x = y$. За постулатом індукції, $\mathfrak{A} \vdash x + z = y + z \Rightarrow x = y$.

8. $0 \leqslant y$, оскільки $y = y + 0 = 0 + y$. Якщо $y \leqslant x$, тобто $x = y + z$, то $x + 1 = y + z + 1$, отже $y \leqslant x + 1$. Припустимо, що $x \leqslant y$, тобто $y = x + z$. Якщо $z \neq 0$, то $\mathfrak{A} \vdash \exists z\, z = z + 1$. Виберемо c таке, що $z = c + 1$. Тоді $y = x + (c + 1) = (x + 1) + c$ і $y \leqslant x + 1$. Якщо ж $z = 0$, то $y = x \leqslant x + 1$.

Отже, за аксіомою (A5), $x+1 \leqslant y$ або $y \leqslant x+1$. За постулатом індукції, $\mathfrak{A} \vdash x \leqslant y \vee y \leqslant x$.

9 залишається як легка вправа.

10 — очевидний наслідок з 9.

11. Припустимо, що $y \neq 0$; унаслідок 1 можна вибрати c так, щоб $y = c+1$. Тоді $xy = xc + x$ і з 10 випливає, що коли $xy = 0$, то $x = 0$.

12. Позначимо $\mathbf{A}(x) = (xz = yz \wedge z \neq 0 \Rightarrow x = y)$. Якщо $x = 0$, то $xz = 0$; тоді з $xz = yz$ та 11 випливає $y = 0$. Отже, $\mathfrak{A} \vdash \mathbf{A}(0)$. Припустимо, що виконується $\mathbf{A}(x)$. Оскільки $x+1 \neq 0$ (N1), то, за 11, $z \neq 0 \Rightarrow (x+1)z \neq 0$. Тому, якщо $(x+1)z = yz \wedge z \neq 0$, то $y \neq 0$ (знов за 11). За 1 можна вибрати c таке, що $y = c+1$, тобто $xz + z = cz + z$. За 7 $xz = cz$, отже, згідно з припущенням, $x = c$ і $x+1 = c+1 = y$, тобто виконується $\mathbf{A}(x+1)$. За постулатом індукції $\mathfrak{A} \vdash \mathbf{A}(x)$.

Нарешті, 13 очевидно випливає з означення та 7, а 14 — з означення та 11 $\square$

Вправа 3.1.3. Доведіть, що наведені речення є теоремами формальної арифметики:

1. $x + y = 1 \Rightarrow (x = 1 \wedge y = 0) \vee (x = 0 \wedge y = 1)$.
2. $xy = 1 \Rightarrow x = 1 \wedge y = 1$.
3. $x < y \Rightarrow \neg y < x$.
4. $x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$.
5. $x \leqslant y \wedge y < z \Rightarrow x < z$ і $x < y \wedge y \leqslant z \Rightarrow x < z$.
6. $x < y \Leftrightarrow x + z < y + z$.
7. $x < y \wedge z \neq 0 \Leftrightarrow xz < yz$.

Позначимо $\mathrm{x}|\mathrm{y}$ речення $\exists \mathrm{z}\, \mathrm{y} = \mathrm{xz}$.

8. $\mathrm{x}|\mathrm{y} \wedge \mathrm{y} \neq 0 \Rightarrow \mathrm{x} \leqslant \mathrm{y}$.
9. $\mathrm{x}|\mathrm{y} \wedge \mathrm{y}|\mathrm{z} \Rightarrow \mathrm{x}|\mathrm{z}$.

Доведемо ще кілька важливих властивостей теорії $\mathfrak{A}$.

Твердження 3.1.4. *Наступні речення є теоремами теорії* $\mathfrak{A}$.

1. («Друга форма постулатів індукції»)

$$\forall \mathrm{x}\Big(\forall \mathrm{y}\big(\mathrm{y} < \mathrm{x} \Rightarrow \mathbf{A}(\mathrm{y})\big) \Rightarrow \mathbf{A}(\mathrm{x})\Big) \Rightarrow \forall \mathrm{x}\mathbf{A}(\mathrm{x}) \tag{N7a}$$

для кожного речення $\mathbf{A}(\mathrm{x})$ *теорії* $\mathfrak{A}$.

2. («Принцип найменшого елемента»)

$$\exists \mathrm{x}\mathbf{A}(\mathrm{x}) \Rightarrow \exists \mathrm{x}\Big(\mathbf{A}(\mathrm{x}) \wedge \forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big)\Big) \tag{N7b}$$

для кожного речення $\mathbf{A}(\mathrm{x})$ *теорії* $\mathfrak{A}$.

3. $\mathrm{x} \leqslant \overline{\mathrm{n}} \Rightarrow (\mathrm{x} = 0 \vee \mathrm{x} = 1 \vee \mathrm{x} = 2 \vee \dots \vee \mathrm{x} = \overline{\mathrm{n}})$ *для кожного натурального числа* n.
4. («Ділення із залишком»)

$$\mathrm{x} \neq 0 \Rightarrow \exists!\, \mathrm{z}\, \exists!\, \mathrm{t}\, (\mathrm{y} = \mathrm{xz} + \mathrm{t} \wedge \mathrm{t} < \mathrm{x}).$$

Доведення. 1. Позначимо $\mathbf{B}(\mathrm{x}) = \forall \mathrm{y}\big(\mathrm{y} \leqslant \mathrm{x} \Rightarrow \mathbf{A}(\mathrm{y})\big)$ і покажемо, що з $\forall \mathrm{x}\Big(\forall \mathrm{y}\big(\mathrm{y} < \mathrm{x} \Rightarrow \mathbf{A}(\mathrm{y})\big) \Rightarrow \mathbf{A}(\mathrm{x})\Big)$ виводиться $\forall \mathrm{x}\mathbf{B}(\mathrm{x})$. Цього достатньо, оскільки очевидно $\mathbf{B}(\mathrm{x}) \Rightarrow \mathbf{A}(\mathrm{x})$. Згідно з 7, $\mathbf{B}(\mathrm{x}) \equiv \forall \mathrm{y}\big(\mathrm{y} < \mathrm{x}+1 \Rightarrow \forall(\mathrm{y})\big)$, тому, за припущенням, $\mathbf{B}(\mathrm{x}) \Rightarrow \mathbf{A}(\mathrm{x}+1)$. Речення $\mathbf{B}(0)$ — це $\forall \mathrm{y}\big(\mathrm{y} \leqslant 0 \Rightarrow \mathbf{A}(0)\big)$; оскільки $\mathrm{y} \leqslant 0 \Leftrightarrow \mathrm{y} = 0$, то $\mathbf{B}(0) \equiv \mathbf{A}(0)$. Оскільки $\neg \mathrm{y} < 0$, то $\forall \mathrm{y}\big(\mathrm{y} < 0 \Rightarrow \mathbf{A}(\mathrm{y})\big)$, отже, має місце $\mathbf{A}(0)$, тобто $\mathbf{B}(0)$. Припустимо, що має місце $\mathbf{B}(\mathrm{x})$. Тоді також має місце $\mathbf{A}(\mathrm{x}+1)$. Однак $\mathrm{y} \leqslant \mathrm{x}+1 \equiv \mathrm{y} = \mathrm{x}+1 \vee \mathrm{y} \leqslant \mathrm{x}$; в обох випадках має місце $\mathbf{A}(\mathrm{y})$. Отже, ми вивели й $\mathbf{B}(\mathrm{x}+1)$ і, за постулатом індукції, $\forall \mathrm{x}\mathbf{B}(\mathrm{x})$.

Надалі, при посиланні на теорему вигляду (N7a), ми часто називатимемо її також «постулатом індукції», опускаючи слова «друга форма».

2. Припустимо, що $\neg\exists \mathrm{x}\Big(\mathbf{A}(\mathrm{x}) \wedge \forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big)\Big)$. Застосовуючи теореми логіки відношень, перепишемо його у вигляді $\forall \mathrm{x}\Big(\neg\mathbf{A}(\mathrm{x}) \vee \neg\forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big)\Big)$ або $\forall \mathrm{x}\Big(\forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big) \Rightarrow \neg\mathbf{A}(\mathrm{x})\Big)$ (ми скористалися тим, що $X \vee Y \equiv (\neg Y \Rightarrow X)$) або $\forall \mathrm{x}\Big(\forall \mathrm{y}\big(\mathrm{y} < \mathrm{x} \Rightarrow \neg\mathbf{A}(\mathrm{y})\big) \Rightarrow \neg\mathbf{A}(\mathrm{x})\Big)$ (ми скористалися тим, що $(X \Rightarrow Y) \equiv (\neg Y \Rightarrow \neg X)$). Тепер, згідно з (N7a), виводиться $\forall \mathrm{x}\neg\mathbf{A}(\mathrm{x})$ або $\neg\exists \mathrm{x}\mathbf{A}(\mathrm{x})$. Отже, ми вивели $\neg\exists \mathrm{x}\Big(\mathbf{A}(\mathrm{x}) \wedge \forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big)\Big) \Rightarrow \neg\exists \mathrm{x}\mathbf{A}(\mathrm{x})$, або, що еквівалентно, $\exists \mathrm{x}\mathbf{A}(\mathrm{x}) \Rightarrow \exists \mathrm{x}\Big(\mathbf{A}(\mathrm{x}) \wedge \forall \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \Rightarrow \mathrm{x} \leqslant \mathrm{y}\big)\Big)$.

3. Позначимо $\mathbf{A}_n$ речення $\mathrm{x} \leqslant \overline{\mathrm{n}} \Rightarrow (\mathrm{x} = 0 \vee \mathrm{x} = 1 \vee \mathrm{x} = 2 \vee \dots \vee \mathrm{x} = \overline{\mathrm{n}})$. Зауважимо, що $\overline{\mathrm{n}+1} = \overline{\mathrm{n}} + 1$ і $\mathbf{A}_{n+1} \equiv \mathbf{A} \vee \mathrm{x} = \overline{\mathrm{n}} + 1$. Користуючись цим, укажемо рекурентний спосіб побудови виводу речення $\mathbf{A}_n$ для довільного натурального числа n. Якщо $n = 0$, то $\overline{\mathrm{n}} = 0$, а $\mathrm{x} \leqslant 0 \Rightarrow \mathrm{x} = 0$ (доведіть це). Припустимо, ми вже маємо вивід $\mathbf{A}_n$. Додамо до нього

вже виведене $\mathrm{x} \leqslant \overline{\mathrm{n}}+1 \Rightarrow \mathrm{x}=\overline{\mathrm{n}}+1 \vee \mathrm{x} \leqslant \overline{\mathrm{n}}$. Скориставшись ПВТ $(X \vee Y) \wedge (Y \Rightarrow Z) \Rightarrow (Z \vee X)$, одержимо вивід $\mathbf{A}_{n+1}$.

4. Покажемо, перш за все, що $\mathrm{y}=\mathrm{xz}+\mathrm{t}=\mathrm{xz}'+\mathrm{t}' \wedge \mathrm{t}<\mathrm{x} \wedge \mathrm{t}'<\mathrm{x} \Rightarrow \mathrm{z}=\mathrm{z}' \wedge \mathrm{t}=\mathrm{t}'$. Згідно з твердженням 3.1.2.8, або $\mathrm{t} \leqslant \mathrm{t}'$, або $\mathrm{t}' \leqslant \mathrm{t}$. Нехай $\mathrm{t} \leqslant \mathrm{t}'$, тобто $\mathrm{t}'=\mathrm{u}+\mathrm{t}$. Тоді $\mathrm{xz}+\mathrm{t}=\mathrm{xz}'+\mathrm{u}+\mathrm{t}$, звідки $\mathrm{xz}=\mathrm{xz}'+\mathrm{u}$; зокрема, $\mathrm{xz}' \leqslant \mathrm{xz}$. Згідно з твердженням 3.1.2.12 і вправою 3.1.3.7, $\mathrm{z}' \leqslant \mathrm{z}$, тобто $\mathrm{z}=\mathrm{z}'+\mathrm{v}$, звідки $\mathrm{xz}'+\mathrm{xv}=\mathrm{xz}'+\mathrm{u}$ і $\mathrm{xv}=\mathrm{u}$. Оскільки $\mathrm{t}'=\mathrm{u}+\mathrm{t}$, то $\mathrm{u} \leqslant \mathrm{t}'$; разом із $\mathrm{t}'<\mathrm{x}$ і вправою 3.1.3.5 це спричиняє $\mathrm{u}<\mathrm{x}$. Тому за вправою 3.1.3.8 $\mathrm{u}=0$, звідки $\mathrm{t}=\mathrm{t}'$ і $\mathrm{z}=\mathrm{z}'$. Так само розбирається випадок $\mathrm{t}' \leqslant \mathrm{t}$. Залишається послатися на аксіому (A5) логіки відношень.

Треба ще вивести речення $\mathbf{A}(\mathrm{y})=\exists \mathrm{z}\, \exists \mathrm{t}\, (\mathrm{y}=\mathrm{xz}+\mathrm{t} \wedge \mathrm{t}<\mathrm{x})$. Оскільки $0=\mathrm{x} \cdot 0+0$ і $\mathrm{x} \neq 0 \Rightarrow 0<\mathrm{x}$, то $\mathfrak{A} \vdash \mathbf{A}(0)$. Припустимо, що $\mathbf{A}(\mathrm{y})$, і виберемо c, d такі, що $\mathrm{y}=\mathrm{cx}+\mathrm{d} \wedge \mathrm{d}<\mathrm{x}$. Тоді $\mathrm{y}+1=\mathrm{cx}+(\mathrm{d}+1)$. За твердженням 3.1.2.9, $\mathrm{d}+1 \leqslant \mathrm{x}$, тобто $\mathrm{d}+1<\mathrm{x} \vee \mathrm{d}+1=\mathrm{x}$. Якщо $\mathrm{d}+1=\mathrm{x}$, то $\mathrm{y}+1=\mathrm{cx}+(\mathrm{d}+1)=\mathrm{cx}+\mathrm{x}=(\mathrm{c}+1)\mathrm{x}+0$. Отже, завжди виводиться $\mathbf{A}(\mathrm{y}+1)$. За постулатом індукції, $\forall \mathrm{y} \mathbf{A}(\mathrm{y})$ $\square$

«Ділення із залишком» (твердження 3.1.4.4) дозволяє вивести з теорії $\mathfrak{A}$ усі звичайні властивості подільності натуральних чисел, такі як існування найбільшого спільного дільника, однозначність розкладу на первинні множники (але не його існування — збагніть, що цьому заважає!) і т. ін. Ми будемо надалі вільно користуватися цими властивостями. Виведення їх у формальній арифметиці залишаємо на розсуд читачу (залежно від того, коли ця діяльність йому набридне і він зволіє за краще повірити, що й інші доведення можна також переказати формально).

Уведемо функції $[x/y]$ та $\mathrm{res}(x, y)$, визначені на $\mathbb{N}^2$ зі значеннями в $\mathbb{N}$, такими правилами:

- якщо $b \neq 0$, то $\mathrm{res}(a, b)<b$ і $a=b[a/b]+\mathrm{res}(a, b)$;
- $[a/0]=0$ і $\mathrm{res}(a, 0)=a$.

Згідно з твердженням 3.1.4.4, вони коректно визначені. Кажуть, що $[a/b]$ — *неповна частка*, а $\mathrm{res}(a, b)$ — *залишок* при діленні числа a на число b.

Вправа 3.1.5. Довести наведені далі твердження, де $a, b, \ldots$ — натуральні числа, $\overline{\mathrm{a}}, \overline{\mathrm{b}}, \ldots$ — відповідні терми формальної арифметики, а $\mathbf{A}$ — довільне речення формальної арифметики.

1. Якщо $a<b$, то $\mathfrak{A} \vdash \overline{\mathrm{a}}<\overline{\mathrm{b}}$ і навпаки (очевидно, якщо $a=b$, то терми $\overline{\mathrm{a}}$ і $\overline{\mathrm{b}}$ просто збігаються).
2. $\mathfrak{A} \vdash \overline{\mathrm{a}+\mathrm{b}}=\overline{\mathrm{a}}+\overline{\mathrm{b}}$ і $\mathfrak{A} \vdash \overline{\mathrm{ab}}=\overline{\mathrm{a}}\overline{\mathrm{b}}$.
3. Нехай $F(x_1, x_2, \ldots, x_m)$ — многочлен з натуральними коефіцієнтами, $a_1, a_2, \ldots, a_m$ — натуральні числа, $b=F(a_1, a_2, \ldots, a_m)$. Позначимо $\overline{\mathrm{F}}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n)$ терм формальної арифметики, який одержується з F, якщо кожний коефіцієнт c замінити термом $\overline{\mathrm{c}}$. Тоді $\mathfrak{A} \vdash \overline{\mathrm{F}}(\overline{\mathrm{a}}_1, \overline{\mathrm{a}}_2, \ldots, \overline{\mathrm{a}}_m)=\overline{\mathrm{b}}$.
4. $\mathbf{A}(0) \wedge \mathbf{A}(1) \wedge \ldots \wedge \mathbf{A}(\overline{\mathrm{n}}) \equiv_{\mathfrak{A}} \forall \mathrm{x}\big(\mathrm{x} \leqslant \overline{\mathrm{n}} \Rightarrow \mathbf{A}(\mathrm{x})\big)$, а $\mathbf{A}(0) \vee \mathbf{A}(1) \vee \cdots \vee \mathbf{A}(\overline{\mathrm{n}}) \equiv_{\mathfrak{A}} \exists \mathrm{x}\big(\mathrm{x} \leqslant \overline{\mathrm{n}} \wedge \mathbf{A}(\mathrm{x})\big)$.
5. («Принцип нескінченного спуску»)

$$\mathfrak{A} \vdash \forall \mathrm{x}\big(\mathbf{A}(\mathrm{x}) \Rightarrow \exists \mathrm{y}\big(\mathbf{A}(\mathrm{y}) \wedge \mathrm{y}<\mathrm{x}\big)\big) \Rightarrow \forall \mathrm{x} \neg \mathbf{A}(\mathrm{x}).$$

Виведіть звідси, що кожна модель формальної арифметики містить підмодель, ізоморфну стандартній.

3.2. Арифметичні множини й функції

Ми переходимо до вивчення важливих класів функцій. Маючи на увазі вправу 3.1.5, надалі, як правило, не будемо розрізняти в позначеннях натуральне число n та відповідний терм $\overline{\mathrm{n}}$ формальної арифметики і писатимемо, наприклад, $\mathbf{A}(n)$ замість $\mathbf{A}(\overline{\mathrm{n}})$. Сподіваємось, що це не викличе ускладнень, оскільки з контексту завжди має бути ясно, про що саме йдеться. Якщо можливі двозначності, то будемо повертатися до позначень типу $\overline{\mathrm{n}}$.

Означення 3.2.1.

1. Підмножина $M \subseteq \mathbb{N}^n$ називається *напіварифметичною*, якщо існує таке речення $\mathbf{A}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n)$ формальної арифметики, що $(a_1, a_2, \ldots, a_n) \in M$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{A}(a_1, a_2, \ldots, a_n)$. У такому випадку кажуть, що речення $\mathbf{A}$ *визначає підмножину* M.
2. Підмножина $M \subseteq \mathbb{N}^n$ називається *арифметичною*, якщо вона та її доповнення — арифметичні. Інакше кажучи, існують такі речення $\mathbf{A}$ та $\mathbf{A}'$, що $(a_1, a_2, \ldots, a_n) \in M$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{A}(a_1, a_2, \ldots, a_n)$, і $(a_1, a_2, \ldots, a_n) \notin M$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{A}'(a_1, a_2, \ldots, a_n)$.
3. Функція $f : \mathbb{N}^n \to \mathbb{N}$ називається *напіварифметичною* (*арифметичною*), якщо її *графік*, тобто множина

$$\Gamma(f) = \left\{ \left(a_1, a_2, \ldots, a_n, f(a_1, a_2, \ldots, a_n)\right) \right\},$$

є напіварифметичною (відповідно, арифметичною) підмножиною в $\mathbb{N}^{n+1}$. Про речення, яке визначає графік, кажуть також, що воно *визначає функцію* f.

Зауважимо, що для арифметичної підмножини завжди є *алгоритм перевірки*, чи належить заданий елемент цій множині. Дійсно, нехай речення $\mathbf{A}$ визначає підмножину $M \subseteq \mathbb{N}^n$, а речення $\mathbf{A}'$ — її доповнення M'. Для кожної n-ки $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ або $\mathbf{a} \in M$, тобто $\mathfrak{A} \vdash \mathbf{A}(a_1, a_2, \ldots, a_n)$, або $\mathbf{a} \in M'$, тобто $\mathfrak{A} \vdash \mathbf{A}'(a_1, a_2, \ldots, a_n)$. Ми бачили, що існує процедура, яка виписує *всі* теореми формальної арифметики: $\mathbf{T}_1, \mathbf{T}_2, \ldots, \mathbf{T}_m, \ldots$. Залишається «запустити» цю процедуру та чекати, яка теорема з'явиться: $\mathbf{A}(a_1, a_2, \ldots, a_n)$ чи $\mathbf{A}'(a_1, a_2, \ldots, a_n)$. Звичайно, ми не можемо передбачити час чекання — у цьому розумінні цей алгоритм неефективний, але те, що врешті-решт одна з цих теорем з'явиться, нам гарантовано. Те саме стосується напіварифметичної функції: якщо речення $\mathbf{A}(\mathbf{x}, \mathrm{y}) = \mathbf{A}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{y})$ визначає графік функції f, то, щоб обчислити значення $f(a_1, a_2, \ldots, a_n)$, достатньо «запустити» процедуру побудови всіх теорем формальної арифметики й дочекатися, коли з'явиться теорема вигляду $\mathbf{A}(a_1, a_2, \ldots, a_n, b)$ для деякого b. Тоді одержимо $f(a_1, a_2, \ldots, a_n) = b$. Така теорема обов'язково з'явиться, оскільки функція f визначена на кожному елементі множини $\mathbb{N}^n$. З іншого боку, для напіварифметичної множини аналогічний алгоритм дає відповідь, якщо $\mathbf{a} \in M$ (на якомусь кроці з'явиться теорема $\mathbf{A}(\mathbf{a})$). Проте якщо $\mathbf{a} \notin M$, цей алгоритм працюватиме нескінченно. Оскільки ніякої оцінки для числа кроків, за яке теорема $\mathbf{A}(\mathbf{a})$ має з'явитися, немає, то в цьому випадку ми ніколи не дізнаємось, чи $\mathbf{a} \in M$, чи ні. Така асиметрія в поведінці напіварифметичних функцій і множин насправді є уявною: нижче ми доведемо, що кожна напіварифметична функція є насправді арифметичною. Легко збагнути також, що справа полягає в тому, що ми розглядаємо функції, які *всюди визначені*. Якщо ввести аналогічні поняття для функцій $M \to \mathbb{N}$, де M — довільна підмножина в $\mathbb{N}^n$, напіварифметичні функції вже можуть не бути арифметичними й алгоритму обчислення для них, узагалі кажучи, не існує.

Зауважимо також, що всі ці означення мають зміст лише в припущенні того, що формальна арифметика несуперечлива: інакше з неї виводиться довільне речення. Утім, якщо ми збираємося застосовувати формальну арифметику до вивчення функцій натурального аргументу, природно припустити, що виконується гіпотеза про стандартну модель. Надалі ми будемо вільно користуватися цим припущенням, спеціально про нього не згадуючи.

Нагадаємо, що *характеристична функція* χ_M підмножини $M \subseteq \mathbb{N}^n$ визначається правилом:

$$\chi_M(a_1, a_2, \ldots, a_n) = \begin{cases} 0 & \text{якщо } (a_1, a_2, \ldots, a_n) \in M, \\ 1 & \text{якщо } (a_1, a_2, \ldots, a_n) \notin M. \end{cases}$$

Зауважимо, що частіше значення характеристичної функції задають навпаки: 1, якщо елемент належить підмножині, 0, якщо не належить, але ми змінили означення, оскільки це спрощує деякі наступні обчислення.

Твердження 3.2.2.

1. *Якщо підмножина $M \subseteq \mathbb{N}^n$ арифметична, такою є й її характеристична функція.*
2. *Якщо характеристична функція χ_M напіварифметична, підмножина M арифметична (отже, такою є й χ_M).*

Доведення. 1. Нехай речення $\mathbf{A}$ визначає підмножину M, а $\mathbf{A}'$ — її доповнення. Тоді легко бачити, що

- $\chi_M(\mathbf{a}) = b$ тоді й лише тоді, коли
$$\mathfrak{A} \vdash (\mathbf{A}(\mathbf{a}) \wedge b = 1) \vee (\mathbf{A}'(\mathbf{a}) \wedge b = 0);$$
- $\chi_M(\mathbf{a}) \neq b$ тоді й лише тоді, коли
$$\mathfrak{A} \vdash (\mathbf{A}'(\mathbf{a}) \wedge b = 1) \vee (\mathbf{A}(\mathbf{a}) \wedge b = 0) \vee b > 1.$$

2. Нехай графік функції χ_M визначається реченням $\mathbf{B}$. Тоді

$$\mathbf{a} \in M \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \mathbf{B}(\mathbf{a}, 0),$$
$$\mathbf{a} \notin M \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \mathbf{B}(\mathbf{a}, 1) \quad \square$$

Вправа 3.2.3. Доведіть, що коли напіварифметична функція приймає лише скінченну кількість значень, вона арифметична.

З технічною метою ми введемо ще такі поняття.

Означення 3.2.4.

1. Будемо казати, що речення $\mathbf{A}(\mathbf{x})$ *правильно визначає* підмножину $M \subseteq \mathbb{N}^n$, якщо це речення визначає M, а його заперечення $\neg\mathbf{A}$ визначає доповнення до M. Інакше кажучи,
$$\mathbf{a} \in M \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \mathbf{A}(\mathbf{a}),$$
$$\mathbf{a} \notin M \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \neg\mathbf{A}(\mathbf{a}).$$
Очевидно, тоді підмножина M арифметична.
2. Будемо казати, що речення $\mathbf{A}(\mathbf{x}, \mathbf{y})$ *правильно визначає* функцію $f : \mathbb{N}^m \to \mathbb{N}$, якщо кожного разу, коли $f(\mathbf{a}) = b$, $\mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, b) \wedge \big(\mathbf{A}(\mathbf{a}, \mathrm{y}) \Rightarrow \mathrm{y} = b\big)$.

3. Підмножину (функцію) будемо називати *правильно арифметичною*, якщо вона правильно визначається деяким реченням.

У наступних розділах ми доведемо таку основну теорему.

Теорема 3.2.5.
1. *Кожна арифметична підмножина в* $\mathbb{N}^n$ *є правильно арифметичною.*
2. *Кожна напіварифметична функція є правильно арифметичною (а тому арифметичною).*

Отже, поняття напіварифметичної, арифметичної та правильно арифметичної функції (відображення) збігаються, так само як поняття арифметичної та правильно арифметичної підмножини.

Поки що ми розглянемо деякі властивості цих понять.

Твердження 3.2.6. *Якщо речення* $\mathbf{A}(\mathbf{x})$ *правильно визначає функцію* $f(\mathbf{x})$*, то*

$$b = f(\mathbf{a}) \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, b);$$
$$b \neq f(\mathbf{a}) \text{ тоді й лише тоді, коли } \mathfrak{A} \vdash \neg\mathbf{A}(\mathbf{a}, b).$$

Зокрема, те саме речення правильно визначає графік $\Gamma(f)$*.*

Доведення. Якщо $b = f(\mathbf{a})$, то, згідно з означенням, $\mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, b)$. Припустимо, що $b \neq f(\mathbf{a})$ і $f(\mathbf{a}) = c$. Тоді $\mathfrak{A} \vdash b \neq c$, тому й $\mathbf{A}(\mathbf{a}, b) \Rightarrow b \neq c$. Проте нам дано, що $\mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, \mathrm{y}) \Rightarrow \mathrm{y} = c$, зокрема, $\mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, b) \Rightarrow b = c$. За ПВТ $(X \Rightarrow Y) \Rightarrow ((X \Rightarrow \neg Y) \Rightarrow \neg X$, одержимо $\mathfrak{A} \vdash \neg\mathbf{A}(\mathbf{a}, b)$.

Навпаки, нехай $\mathfrak{A} \vdash \mathbf{A}(\mathbf{a}, b)$. Тоді напевне з $\mathfrak{A}$ не виводиться $\neg\mathbf{A}(\mathbf{a}, b)$, отже неможливо, щоб $f(\mathbf{a}) \neq b$. Тому $b = f(\mathbf{a})$. Так само, якщо $\mathfrak{A} \vdash \neg\mathbf{A}(\mathbf{a}, b)$, то $b \neq f(\mathbf{a})$ □

Вправа 3.2.7. Доведіть, що коли речення $\mathbf{A}$ правильно визначає підмножину $M \subseteq \mathbb{N}^n$, а речення $\mathbf{B}$ визначає ту ж підмножину, то $\mathbf{A}(\mathbf{a}) \Rightarrow_{\mathfrak{A}} \mathbf{B}(\mathbf{a})$ для кожного набору натуральних чисел $\mathbf{a} = (a_1, a_2, \ldots, a_n)$. Зокрема, якщо речення $\mathbf{B}$ також правильно визначає підмножину M, то $\mathbf{A}(\mathbf{a}) \equiv_{\mathfrak{A}} \mathbf{B}(\mathbf{a})$ для кожного набору натуральних чисел $\mathbf{a}$.

Зауважимо, що звідси в загальному випадку не випливає, що $\mathfrak{A} \vdash \forall\mathbf{x}(\mathbf{A} \Rightarrow \mathbf{B})$, хоча, звичайно, заперечення останнього речення не можна вивести у формальній арифметиці — це випливає з її ω-несуперечливості (поясніть, чому).

Розглянемо деякі приклади; частина з них буде використовуватись при наступних доведеннях.

Приклад 3.2.8.
1. Стала функція $f(x_1, x_2, \ldots, x_m) = c$ правильно визначається реченням $\mathrm{y} = c$.

2. Підмножина $M = \{\, \mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \,\}$, яка складається зі скінченної кількості елементів $\mathbf{a}_i = (a_{i1}, a_{i2}, \ldots, a_{im})$, правильно визначається реченням

$$\big(\mathrm{x}_1 = a_{11} \wedge \mathrm{x}_2 = a_{12} \wedge \ldots \wedge \mathrm{x}_m = a_{1m}\big) \vee \\ \vee \big(\mathrm{x}_1 = a_{21} \wedge \mathrm{x}_2 = a_{22} \wedge \ldots \wedge \mathrm{x}_m = a_{2m}\big) \vee \\ \vee \cdots \vee \big(\mathrm{x}_1 = a_{k1} \wedge \mathrm{x}_2 = a_{k2} \wedge \ldots \wedge \mathrm{x}_m = a_{km}\big).$$

3. Будь-яка функція, яка задається многочленом $F(x_1, x_2, \ldots, x_m)$ з натуральними коефіцієнтами, правильно визначається реченням $\overline{\mathrm{F}}\,(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_m) = \mathrm{y}$ (див. вправу 3.1.5.3 щодо визначення $\overline{\mathrm{F}}$; надалі часто писатимемо F замість $\overline{\mathrm{F}}$).
4. *Проектор* $p_k^m : \mathbb{N}^m \to \mathbb{N}$, $p_k^m\,(x_1, x_2, \ldots, x_m) = x_k$, правильно визначається реченням $\mathrm{y} = \mathrm{x}_k$.
5. Функції $\mathrm{res}(x, y)$ та $[x/y]$ є правильно арифметичними. (Напишіть речення, які їх правильно визначають.)
6. Якщо функція $f : \mathbb{N}^m \to \mathbb{N}$ правильно визначається реченням $\mathbf{F}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_m, \mathrm{y})$, а кожна з функцій $g_i : \mathbb{N}^n \to \mathbb{N}$ правильно визначається реченням $\mathbf{G}_i(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{y})$ $(i = 1, 2, \ldots, m)$, то композиція $h = f\,(g_1, g_2, \ldots, g_m) : \mathbb{N}^n \to \mathbb{N}$, задана формулою

$$h\,(x_1, x_2, \ldots, x_n) = \\ = f\big(g_1\,(x_1, x_2, \ldots, x_n)\,, g_2\,(x_1, x_2, \ldots, x_n)\,, \ldots, g_m\,(x_1, x_2, \ldots, x_n)\,\big),$$

правильно визначається реченням

$$\mathbf{H}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{y}) = \exists \mathrm{z}_1 \exists \mathrm{z}_2 \ldots \exists \mathrm{z}_m \mathbf{G}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{z}_1) \wedge \\ \mathbf{G}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{z}_2) \wedge \ldots \wedge \mathbf{G}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{z}_m) \wedge \mathbf{F}(\mathrm{z}_1, \mathrm{z}_2, \ldots, \mathrm{z}_m, \mathrm{y}).$$

Доведення. Приклади 1,2.4 очевидні; 3 випливає із вправи 3.1.5.3, а 5 — із твердження 3.1.4.4.

6. Нехай $b = h\,(x_1, x_2, \ldots, x_n)$; позначимо $c_i = g_i\,(x_1, x_2, \ldots, x_n)$, тоді $b = f\,(c_1, c_2, \ldots, c_m)$. Згідно з означенням,

$$\mathfrak{A} \vdash \mathbf{F}(c_1, c_2, \ldots, c_m, b) \wedge \big(\mathbf{F}(c_1, c_2, \ldots, c_m, \mathrm{y}) \Rightarrow \mathrm{y} = b\big); \\ \mathfrak{A} \vdash \mathbf{G}_i(a_1, a_2, \ldots, a_n, c_i) \wedge \big(\mathbf{F}(a_1, a_2, \ldots, a_n, \mathrm{z}_i) \Rightarrow \mathrm{z}_i = c_i\big)$$

для кожного $i = 1, 2, \ldots, m$. Звідси, очевидно, виводиться й речення $\mathbf{H}(a_1, a_2, \ldots, a_n, b)$. Припустимо, що $\mathbf{H}(a_1, a_2, \ldots, a_n, \mathrm{y})$, і виберемо константи $c_1', c_2', \ldots, c_m'$ такі, що виконується $\mathbf{G}_i(a_1, a_2, \ldots, a_n, c_i')$ для кожного i й $\mathbf{F}(c_1', c_2', \ldots, c_m', \mathrm{y})$. Оскільки

$$\mathfrak{A} \vdash \mathbf{G}_i(a_1, a_2, \ldots, a_n, \mathrm{z}) \Rightarrow \mathrm{z} = c_i,$$

звідси виводиться $c_i' = c_i$. Оскільки також

$$\mathfrak{A} \vdash \mathbf{F}(c_1, c_2, \ldots, c_m, \mathrm{y}) \Rightarrow \mathrm{y} = b,$$

виводиться й $\mathrm{y} = b$. Отже, $\mathfrak{A} \vdash \mathbf{H}(a_1, a_2, \ldots, a_n, \mathrm{y}) \Rightarrow \mathrm{y} = b$, тобто речення $\mathbf{H}$ правильно визначає функцію h $\square$

Вправа 3.2.9. Доведіть, що:

1. Кожна *скінченна* підмножина $M \subseteq \mathbb{N}^n$ є правильно арифметичною.

2. Якщо речення $\mathbf{A}$ визначає (правильно визначає) підмножину $M \subseteq \mathbb{N}^n$, а речення $\mathbf{B}$ визначає (відповідно, правильно визначає) підмножину $N \subseteq \mathbb{N}^n$, то речення $\mathbf{A} \vee \mathbf{B}$ визначає (відповідно, правильно визначає) підмножину $M \cup N$, а речення $\mathbf{A} \wedge \mathbf{B}$ визначає (відповідно, правильно визначає) підмножину $M \cap N$.
3. Об'єднання й перетин довільних напіварифметичних (арифметичних, правильно арифметичних) підмножин знов є такими ж підмножинами. Зауважимо, що *доповнення арифметичної* (правильно арифметичної) підмножини знов є такою ж множиною згідно з означенням, але *доповнення напіварифметичної* підмножини може не бути напіварифметичним (так, очевидно, буде, якщо ця множина не арифметична). (Скористайтеся твердженням 3.1.4.4.)

У наступних розділах важливу роль відіграватиме так звана *функція Ґеделя*

$$\boldsymbol{\beta}(x, y, z) = \mathrm{res}(x, y(z+1)+1).$$

З твердження 3.2.8 випливає, що ця функція правильно арифметична. Ми позначимо B(x, y, z, t) речення, яке правильно визначає цю функцію (довільне; побудову прикладу такого речення ми залишаємо читачу як вправу). Роль функції Ґеделя визначається таким результатом.

Лема 3.2.10. *Для довільних натуральних чисел $c_0, c_1, \ldots, c_n$ існують такі a, b, що $\boldsymbol{\beta}(a, b, k) = c_k$ для всіх $k = 0, 1, \ldots, n$.*

Доведення. Виберемо число b, яке ділиться на $n!$ та є більшим за всі числа c_k (наприклад, $n!(m+1)$, де $m = \max[c_k/n!]$). Тоді всі числа $d_k = b(k+1)+1$ попарно співпервинні (не мають спільних дільників, крім 1). Дійсно, спільний дільник d_k та d_l ($k \neq l$) ділить також $d_k - d_l = b(k-l)$, але не має спільних дільників з b (крім 1), бо b і d_k співпервинні. Отже, він ділить $k-l$ і, оскільки $0 < |k-l| \leqslant n$, ділить також $n!$, а тому й b, що неможливо. Скористаємося тепер так званою «китайською теоремою про лишки» (див. нижче вправу 3.2.11). Згідно з нею, існує таке натуральне число a, що $a \equiv c_k \pmod{d_k}$ для всіх $k = 0, 1, \ldots, n$. Оскільки $c_k < d_k$, то звідси одержимо, що $c_k = \mathrm{res}(a, d_k) = \boldsymbol{\beta}(a, b, k)$ □

Вправа 3.2.11. Доведіть «китайську теорему про лишки»:

Якщо натуральні числа $d_1, d_2, \ldots, d_n$ попарно співпервинні, то для довільних натуральних $c_1, c_2, \ldots, c_n$ існує таке натуральне a, що $a \equiv c_k \pmod{d_k}$ для всіх $k = 1, 2, \ldots, n$.

Вказівка: Якщо $n = 2$, скористайтеся тим, що існують такі цілі числа b_1, b_2, що $b_1 c_1 + b_2 c_2 = 1$. Далі використайте індукцію за n.

3.3. Рекурсивні функції

У цьому розділі ми введемо деякий клас арифметичних функцій, які задаються досить простими правилами. У наступному розділі ми побачимо, що насправді *всі* (напів)арифметичні функції належать цьому класу. Це буде основним кроком у доведенні теореми 3.2.5. Визначимо спочатку дві процедури, якими ми будемо користуватися при побудові цих функцій.

Означення 3.3.1.

1. Нехай задано функції $g : \mathbb{N}^n \to \mathbb{N}$ і $h : \mathbb{N}^{n+2} \to \mathbb{N}$. Кажуть, що функцію $f : \mathbb{N}^n \to \mathbb{N}$ *одержано рекурсією* (або *примітивною рекурсією*) з функцій g та h, якщо для довільних $a_1, a_2, \ldots, a_n$

$$f(a_1, a_2, \ldots, a_n, 0) = g(a_1, a_2, \ldots, a_n)$$

і для кожного b

$$f(a_1, a_2, \ldots, a_n, b+1) = h(a_1, a_2, \ldots, a_n, b, g(a_1, a_2, \ldots, a_n, b)).$$

Ми писатимемо $f = \mathrm{Rec}(g, h)$ і називатимемо g *початковою умовою*, а h — *рекурсивним кроком* для f.

2. Нехай функція $g : \mathbb{N}^{n+1} \to \mathbb{N}$ має властивість, що для довільних $a_1, a_2, \ldots, a_n$ існує таке b, що $g(a_1, a_2, \ldots, a_n, b) = 0$. Кажуть, що функцію $f : \mathbb{N}^n \to \mathbb{N}$ одержано *мініобертанням*, або *μ-операцією* з функції g, якщо для довільних чисел $a_1, a_2, \ldots, a_n$

$$f(a_1, a_2, \ldots, a_n) = \min\{\, b \mid g(a_1, a_2, \ldots, a_n, b) = 0 \,\}.$$

У цьому випадку пишуть

$$f(x_1, x_2, \ldots, x_n) = \mu_y g(x_1, x_2, \ldots, x_n, y).$$

(Зауважимо, що функція f не залежить від y; остання змінна є пов'язаною в цьому виразі.)

Доведемо важливу властивість цих процедур.

Теорема 3.3.2. *Якщо функцію f одержано рекурсією або мініобертанням з правильно арифметичних функцій, вона також є правильно арифметичною.*

Доведення. 1. Нехай $f = \mu_y g$, де $g : \mathbb{N}^{n+1} \to \mathbb{N}$ правильно виражається реченням $\mathbf{G}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{y}, \mathrm{z})$; зокрема, $f(\mathbf{a}, b) = 0$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{G}(\mathbf{a}, b, 0) \wedge (\mathbf{G}(\mathbf{a}, b, \mathrm{z}) \Rightarrow \mathrm{z} = 0)$. Покажемо, що f правильно виражається реченням

$$\mathbf{F}(\mathrm{x}, \mathrm{y}) = \mathbf{G}(\mathrm{x}, \mathrm{y}, 0) \wedge \forall \mathrm{z}\big(\mathrm{z} < \mathrm{y} \Rightarrow \neg \mathbf{G}(\mathrm{x}, \mathrm{z}, 0)\big).$$

Дійсно, якщо $f(\mathbf{a}) = b$, то $\mathfrak{A} \vdash \mathbf{G}(\mathbf{a}, b, 0) \wedge (\mathbf{G}(\mathbf{a}, b, \mathrm{z}) \Rightarrow \mathrm{z} = 0)$. Якщо $b = 0$, то з $\mathfrak{A} \vdash \neg \mathrm{z} < 0$ одержимо $\mathfrak{A} \vdash \mathbf{F}(\mathrm{x}, 0)$. Крім того, $\mathfrak{A} \vdash \mathrm{y} \neq 0 \Rightarrow 0 < \mathrm{y}$, що разом з $\mathfrak{A} \vdash \mathbf{G}(\mathrm{x}, 0, 0)$ дає $\mathfrak{A} \vdash \mathrm{y} \neq 0 \Rightarrow \neg \mathbf{F}(\mathbf{a}, \mathrm{y})$. Тому $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a}, 0) \wedge (\mathbf{F}(\mathbf{a}, \mathrm{y}) \Rightarrow \mathrm{y} = 0)$.

Нехай $b > 0$. Якщо $k < b$, то $f(\mathbf{a}, k) \neq 0$, звідки, за твердженням 3.2.6, $\mathfrak{A} \vdash \neg \mathbf{G}(\mathbf{a}, k, 0)$. Оскільки $\mathrm{y} < b \equiv_{\mathfrak{A}} \mathrm{y} = 0 \vee \mathrm{y} = 1 \vee \mathrm{y} = b - 1$, то маємо $\mathfrak{A} \vdash \mathrm{y} < b \Rightarrow \neg \mathbf{G}(\mathrm{x}, \mathrm{y}, 0)$, тобто $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a}, b)$. Але $\mathfrak{A} \vdash \mathrm{y} \neq b \Rightarrow \mathrm{y} < b \vee \mathrm{y} < b$, а з $\mathbf{G}(\mathbf{a}, b, 0)$ випливає, що $\mathfrak{A} \vdash b < \mathrm{y} \Rightarrow \neg \mathbf{F}(\mathbf{a}, \mathrm{y})$. Тому $\mathfrak{A} \vdash \mathrm{y} \neq b \Rightarrow \neg \mathbf{F}(\mathbf{a}, \mathrm{y})$ і $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a}, \mathrm{y}) \Rightarrow \mathrm{y} = b$, що й треба було довести.

2. Нехай тепер $f = \mathrm{Rec}(g, h)$, де g і h правильно виражаються, відповідно, реченнями $\mathbf{G}(\mathrm{x}, \mathrm{y})$ та $\mathbf{H}(\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{t})$. Покажемо, що f правильно виражається реченням

$$\begin{aligned}\mathbf{F}(\mathrm{x}, \mathrm{y}, \mathrm{z}) = \big(\mathrm{y} = 0 \Rightarrow \mathbf{G}(\mathrm{x}, \mathrm{z})\big) \wedge \\ \wedge \exists \mathrm{u} \exists \mathrm{v} \forall \mathrm{t} \exists \mathrm{w} \big((\mathrm{t} = 0 \Rightarrow \mathbf{G}(\mathrm{x}, \mathrm{w})) \wedge \big(\mathrm{t} < \mathrm{y} \Rightarrow \exists \mathrm{w}' \big(\mathrm{B}(\mathrm{u}, \mathrm{v}, \mathrm{t}, \mathrm{w}) \wedge \\ \wedge \mathrm{B}(\mathrm{u}, \mathrm{v}, \mathrm{t}+1, \mathrm{w}') \wedge \mathbf{H}(\mathrm{x}, \mathrm{t}, \mathrm{w}, \mathrm{w}')\big)\big) \wedge \mathrm{B}(\mathrm{u}, \mathrm{v}, \mathrm{y}, \mathrm{z})\big),\end{aligned}$$

де $\mathrm{B}(\mathrm{x},\mathrm{y},\mathrm{z},\mathrm{t})$ — речення, яке правильно виражає функцію Ґеделя $\boldsymbol{\beta}(x,y,z)$. Дійсно, нехай $c = f(\mathbf{a},b)$. Якщо $b = 0$, то $c = g(\mathbf{a})$, тому $\mathfrak{A} \vdash \mathbf{G}(\mathbf{a},c) \wedge (\mathbf{G}(\mathbf{a},\mathrm{z}) \Rightarrow \mathrm{z} = 0)$. Зокрема, $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a},0,c)$. Крім того, з $\mathbf{F}(\mathbf{a},0,\mathrm{z})$ виводиться, що $\mathbf{G}(\mathbf{a},\mathrm{z})$, а тому й $\mathrm{z} = c$. Отже, також $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a},0,\mathrm{z}) \Rightarrow \mathrm{z} = c$.

Нехай $b \neq 0$. Позначимо $c_m = f(\mathbf{a},m)$ для $m = 1,2,\ldots,b$; зокрема, $c_b = c$. За лемою 3.2.10 існують числа k,l такі, що $\boldsymbol{\beta}(k,l,m) = f(\mathbf{a},m)$ для всіх $m \leqslant b$. Тоді $\mathfrak{A} \vdash \mathrm{B}(k,l,m,c_m) \wedge (\mathrm{B}(k,l,m,\mathrm{w}) \Rightarrow \mathrm{w} = c_m)$. Крім того, $\mathfrak{A} \vdash \mathbf{G}(\mathbf{a},c_0) \wedge (\mathbf{G}(\mathbf{a},\mathrm{w}) \Rightarrow \mathrm{w} = 0)$. Для кожного $m < b$ також $c_{m+1} = h(\mathbf{a},m,c_m)$, тому $\mathfrak{A} \vdash \mathbf{H}(\mathbf{a},m,c_m,c_{m+1}) \wedge (\mathbf{H}(\mathbf{a},m,c_m,\mathrm{w}) \Rightarrow \mathrm{w} = c_{m+1})$. Звідси, зокрема,

$$\mathfrak{A} \vdash \forall\mathrm{t}\exists\mathrm{w}\big((\mathrm{t}=0 \Rightarrow \mathbf{G}(\mathbf{a},\mathrm{w})) \wedge \big(\mathrm{t} < b \Rightarrow \exists\mathrm{w}'\big(\mathrm{B}(k,l,\mathrm{t},\mathrm{w}) \wedge \\ \wedge \mathrm{B}(k,l,\mathrm{t}+1,\mathrm{w}') \wedge \mathbf{H}(\mathbf{a},\mathrm{t},\mathrm{w},\mathrm{w}')\big)\big) \wedge \mathrm{B}(k,l,b,c)\big),$$

отже, $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a},b,c)$.

Припустимо тепер, що $\mathbf{F}(\mathbf{a},b,\mathrm{z})$. Оскільки $b \neq 0$, це рівносильно

$$\exists\mathrm{u}\exists\mathrm{v}\forall\mathrm{t}\exists\mathrm{w}\big((\mathrm{t}=0 \Rightarrow \mathbf{G}(\mathbf{a},\mathrm{w})) \wedge \big(\mathrm{t} < b \Rightarrow \exists\mathrm{w}'\big(\mathrm{B}(\mathrm{u},\mathrm{v},\mathrm{t},\mathrm{w}) \wedge \\ \wedge \mathrm{B}(\mathrm{u},\mathrm{v},\mathrm{t}+1,\mathrm{w}') \wedge \mathbf{H}(\mathbf{a},\mathrm{t},\mathrm{w},\mathrm{w}')\big)\big) \wedge \mathrm{B}(\mathrm{u},\mathrm{v},b,\mathrm{z})\big).$$

Введемо константи d,d' такі, що

$$\forall\mathrm{t}\exists\mathrm{w}\big((\mathrm{t}=0 \Rightarrow \mathbf{G}(\mathbf{a},\mathrm{w})) \wedge \big(\mathrm{t} < b \Rightarrow \exists\mathrm{w}'\big(\mathrm{B}(d,d',\mathrm{t},\mathrm{w}) \wedge \\ \wedge \mathrm{B}(d,d',\mathrm{t}+1,\mathrm{w}') \wedge \mathbf{H}(\mathbf{a},\mathrm{t},\mathrm{w},\mathrm{w}')\big)\big) \wedge \mathrm{B}(d,d',b,\mathrm{z})\big).$$

Тоді для кожного числа $b' < b$

$$\exists\mathrm{w}\exists\mathrm{w}'\big((b'=0 \Rightarrow \mathbf{G}(\mathbf{a},\mathrm{w})) \wedge \mathrm{B}(d,d',b',\mathrm{w}) \wedge \mathrm{B}(d,d',b'+1,\mathrm{w}') \wedge \\ \wedge \mathbf{H}(\mathbf{a},b',\mathrm{w},\mathrm{w}')\big).$$

Знов-таки, можна вибрати константи e,e' такі, що

$$(b'=0 \Rightarrow \mathbf{G}(\mathbf{a},e)) \wedge \mathrm{B}(d,d',b',e) \wedge \mathrm{B}(d,d',b'+1,e') \wedge \mathbf{H}(\mathbf{a},b',e,e').$$

Оскільки ці константи залежать від b', ми писатимемо $e(b')$ та $e'(b')$. Оскільки речення $\mathbf{G}$ правильно визначає функцію f, то з $\mathbf{G}(\mathbf{a},e(0))$ одержуємо $e(0) = c_0$. Далі, аналогічно, з $\mathrm{B}(d,d',b'+1,e'(b'))$ та $\mathrm{B}(d,d',b'+1,e(b'+1))$ виводимо $e'(b') = e(b'+1) = \boldsymbol{\beta}(d,d',b'+1)$. Нарешті, з $\mathbf{H}(\mathbf{a},b',e(b),e'(b'))$ одержуємо $e'(b') = h(\mathbf{a},b',e(b'))$. Тепер, починаючи з $b' = 0$, виводимо $e'(0) = e(1) = h(\mathbf{a},0,c_0) = c_1$, $e'(1) = e(2) = h(\mathbf{a},1,c_1) = c_2,\ldots,e'(b-1) = h(\mathbf{a},b-1,c_{b-1}) = c_b = c$. Оскільки, крім того, $\mathrm{B}(d,d',b,z)$, то з рівності $\beta(d,d',b) = c$ одержуємо $\mathrm{z} = c$. Отже, $\mathfrak{A} \vdash \mathbf{F}(\mathbf{a},b,\mathrm{z}) \Rightarrow \mathrm{z} = c$, тобто речення $\mathbf{F}$ правильно визначає функцію f $\square$

Введемо тепер головних персонажей нашого розгляду. Позначимо $\mathrm{O}(x)$ функцію, тотожно рівну 0, $\mathrm{S}(x) = x+1$.

Означення 3.3.3.

1. Функція $f : \mathbb{N}^n \to \mathbb{N}$ називається *примітивно-рекурсивною*, якщо її можна одержати з функцій O, S та проекторів p_k^n ($k \leqslant n,\ n, k \in \mathbb{N}$) операціями підстановки та примітивної рекурсії.
2. Функція $f : \mathbb{N}^n \to \mathbb{N}$ називається *рекурсивною*, якщо її можна одержати з функцій O, S та проекторів p_k^n ($k \leqslant n,\ n, k \in \mathbb{N}$) операціями підстановки, примітивної рекурсії та мініобертання.
3. Підмножина $M \subseteq \mathbb{N}^n$ називається *рекурсивною* (відповідно, *примітивно-рекурсивною*), якщо такою є її характеристична функція.

Надалі не будемо розрізняти підмножину $M \subseteq \mathbb{N}^n$ та її характеристичну функцію χ_M і писатимемо $M(x_1, x_2, \ldots, x_n)$ замість $\chi_M(x_1, x_2, \ldots, x_n)$. Отже, $(a_1, a_2, \ldots, a_n) \in M$ тоді й лише тоді, коли $M(a_1, a_2, \ldots, a_n) = 0$, а $(a_1, a_2, \ldots, a_n) \notin M$ тоді й лише тоді, коли $M(a_1, a_2, \ldots, a_n) = 1$.

З прикладів 3.2.8 та теореми 3.3.2 одразу випливає

Наслідок 3.3.4. *Кожна рекурсивна функція (підмножина) є правильно арифметичною.*

Отже, теорема 3.2.5 випливає з такого результату, який буде доведено в наступному розділі.

Теорема 3.3.5.

1. *Кожна напіварифметична функція рекурсивна.*
2. *Кожна арифметична підмножина рекурсивна.*

Спочатку встановимо рекурсивність деяких класів функцій. Покажемо перш за все, що перестановки та ототожнення аргументів не порушують рекурсивність.

Твердження 3.3.6. *Нехай $f(x_1, x_2, \ldots, x_n)$ — рекурсивна (примітивно-рекурсивна) функція. Тоді такою ж є і функція $f(x_{k_1}, x_{k_2}, \ldots, x_{k_n})$ для довільного вибору індексів $k_i \in \{1, 2, \ldots, n\}$* (не обов'язково різних).

Доведення. Цю функцію можна записати як результат підстановки $f(p_{k_1}^n, \ldots, p_{k_n}^n)$ □

Твердження 3.3.7. *Кожен многочлен з натуральними коефіцієнтами є примітивно-рекурсивною функцією.*

Доведення. Очевидно, достатньо довести примітивну рекурсивність функцій $x + y$ та xy. Однак вони визначаються за допомогою рекурсій:

$$\begin{aligned} x + 0 &= x = p_1^1(x), \\ x + (y + 1) &= (x + y) + 1 = \mathrm{S}(x + y); \\ x \cdot 0 &= 0 = \mathrm{O}(x), \\ x(y + 1) &= xy + x. \end{aligned}$$

(При розгляді добутку ми скористалися тим, що попередні рядки доводять примітивну рекурсивність суми) □

Твердження 3.3.8. *Наведені далі функції є примітивно-рекурсивними:*

(i) $$\mathrm{S}^*(x) = \begin{cases} 0 & \text{якщо } x = 0, \\ x - 1 & \text{якщо } x \neq 0; \end{cases}$$

(ii) $$x \dot{-} y = \begin{cases} 0 & \text{якщо } x \leqslant y, \\ x - y & \text{якщо } x > y; \end{cases}$$

(iii) $$|x - y|;$$

(iv) $$\mathrm{sg}(x) = \begin{cases} 0 & \text{якщо } x = 0, \\ 1 & \text{якщо } x \neq 0; \end{cases}$$

(v) $$\mathrm{res}(x, y);$$

(vi) $$[x/y].$$

Доведення. (i) $\mathrm{S}^*(0) = 0,\ \mathrm{S}^*(x+1) = x.$
(ii) $x \dot{-} 0 = x,\ x \dot{-} (y+1) = \mathrm{S}^*(x \dot{-} y).$
(iii) $|x - y| = (x \dot{-} y) + (y \dot{-} x).$
(iv) $\mathrm{sg}(0) = 0,\ \mathrm{sg}(x+1) = 1.$
(v) $\mathrm{res}(0, y) = 0,\ \mathrm{res}(x+1, y) = \mathrm{S}(\mathrm{res}(x, y)) \cdot \mathrm{sg}(|y - \mathrm{S}(\mathrm{res}(x, y))|)$. Тут виражено той факт, що коли $y \neq 0$ і $\mathrm{res}(x, y) + 1 < y$, то $\mathrm{res}(x+1, y) = \mathrm{res}(x, y) + 1$, якщо ж $\mathrm{res}(x, y) + 1 = y$, то $\mathrm{res}(x+1, y) = 0$. Перевірте самі, що формула для $\mathrm{res}(x+1, y)$ залишається вірною й при $y = 0$.
(vi) $[0/y] = 0,\ [(x+1)/y] = [x/y] + (1 \dot{-} \mathrm{sg}(|y - \mathrm{S}(\mathrm{res}(x, y)|)$ (поясніть, чому) $\square$

Позначимо також

$$\overline{\mathrm{sg}}(x) = 1 \dot{-} \mathrm{sg}(x) = \begin{cases} 1 & \text{якщо } x = 0, \\ 0 & \text{якщо } x \neq 0. \end{cases}$$

Вправа 3.3.9. Доведіть примітивну рекурсивність функцій:

$$x!,\ x^y,\ [\sqrt[x]{y}],\ \min(x, y),\ \max(x, y),$$
$$\min(x_1, x_2, \ldots, x_n),\ \max(x_1, x_2, \ldots, x_n).$$

Тут $[\sqrt[x]{y}]$ — це ціла частина кореня, тобто якщо $x \neq 0$, найбільше натуральне z таке, що $z^x \leqslant y$. Вважаємо також, що $[\sqrt[0]{y}] = 0$ для всіх y.

Твердження 3.3.10. *Нехай функція $f(x_1, x_2, \ldots, x_n, y)$ — рекурсивна (примітивно-рекурсивна). Тоді такими ж є функції:*

(i) $$\textstyle\prod_{z \leqslant y} f(x_1, x_2, \ldots, x_n, z) = \prod_{k=0}^{y} f(x_1, x_2, \ldots, x_n, k);$$

(i) $$\textstyle\sum_{z \leqslant y} f(x_1, x_2, \ldots, x_n, z) = \sum_{k=0}^{y} f(x_1, x_2, \ldots, x_n, k);$$

(iii) $$\mu_{z<y} f(x_1, x_2, \ldots, x_n, z) =$$
$$= \begin{cases} y, \text{ якщо } f(\mathbf{x}, k) \neq 0 \text{ для всіх } k < y, \\ \min\{\, k \mid f(\mathbf{x}, k) = 0 \,\} \text{ інакше.} \end{cases}$$

Те саме має місце, якщо в цих означеннях знак $\leqslant$ всюди замінити на знак $<$.

Доведення. (i) $\prod_{z\leqslant 0} f(\mathbf{x}, z) = 1$ і

$$\prod_{z\leqslant y+1} f(\mathbf{x}, z) = f(\mathbf{x}, y+1)\prod_{z\leqslant y} f(\mathbf{x}, z).$$

Так само доводиться (ii).

(iii) $\mu_{z<0} f(\mathbf{x}, z) = 0$ і

$$\mu_{z<y+1} f(\mathbf{x}, z) = \overline{\mathrm{sg}}(f(\mathbf{x}, \mu_{z<y} f(\mathbf{x}, z)))\cdot \\ \cdot \mu_{z<y} f(\mathbf{x}, z)(y+1)\,\mathrm{sg}(f(\mathbf{x}, \mu_{z<y} f(\mathbf{x}, z))) \;\square$$

Якщо задано n-місне відношення на множині $\mathbb{N}$, тобто функція $P : \mathbb{N}^n \to \mathbb{B}$, його можна ототожнити з характеристичною функцією відповідної підмножини. Зауважимо, що згідно з нашим означенням характеристичної функції ми фактично замінюємо булеве значення «вірний», або **1**, на числове значення 0, а булеве значення «хибний», або **0**, — на числове значення 1. Зокрема, можна говорити про рекурсивні (примітивно-рекурсивні) відношення. До таких відношень ми будемо вільно застосовувати логічні сполучники. Оскільки всі логічні сполучники виражаються через $\wedge$, $\vee$ та $\neg$, причому $\neg P = 1 \dot{-} P$, $P \wedge Q = \min(P, Q)$ і $P \vee Q = \max(P, Q)$, то застосування логічних сполучників до рекурсивних (примітивно-рекурсивних) відношень знов дає такі самі відношення.

Приклад 3.3.11.

1. Наведені відношення є примітивно-рекурсивними:
   (a) $x = y$ — відповідна функція є $\mathrm{sg}(|x - y|)$.
   (b) $x < y$ — відповідна функція є $\overline{\mathrm{sg}}(y \dot{-} x)$.
   (c) $x|y$ — відповідна функція є $\mathrm{sg}(\mathrm{res}(y, x))$.
   (d) $\mathrm{Pr}(x)$ =«x — первинне число» — відповідна функція є $\overline{\mathrm{sg}}(x \dot{-} 1)\,\mathrm{sg}(|D(x) - 2|)$, де $D(x) = \sum_{y\leqslant x} \overline{\mathrm{sg}}(\mathrm{res}(x, y))$ — кількість дільників числа x.
2. Наведені функції є примітивно-рекурсивними:
   (a) $\mathrm{p}(x)$ =«первинне число з номером x» (тобто, $\mathrm{p}(0) = 2$, $\mathrm{p}(1) = 3$, $\mathrm{p}(2) = 5, \ldots$). Дійсно, $\mathrm{p}(0) = 2$ і $\mathrm{p}(x+1) = \mu_{z<\mathrm{p}(x)!+1} g(x, z)$, де $g(x, y) = (\mathrm{p}(x) < y \wedge \mathrm{Pr}(y))$.
   (b) $v(x, y)$ =«показник, з яким первинне число $\mathrm{p}(y)$ входить у розклад числа x на первинні множники» (вважаємо, що $v(0, y) = 0$). Дійсно,

   $$v(x, y) = \mu_{z<x} g(x, \mathrm{p}(y), z), \quad \text{де} \quad g(x, y, z) = \neg y^{z+1} | x.$$

   (c) Так само примітивно-рекурсивною є функція $\mathrm{len}(x) = \max\{\, y \mid v(x, y) \neq 0 \,\}$ (перевірте це).
   (d) Визначимо функцію $x{*}y$ («*зчеплення*», або «*конкатенація*») у такий спосіб:

   $$x * y = \mathrm{p}(0)^{k_0}\,\mathrm{p}(1)^{k_1} \ldots \mathrm{p}(r)^{k_r}\,\mathrm{p}(r+1)^{l_0}\,\mathrm{p}(r+2)^{l_1} \ldots \mathrm{p}(r+s+1)^{l_s},$$

   якщо $x = \mathrm{p}(0)^{k_0}\,\mathrm{p}(1)^{k_1} \ldots \mathrm{p}(r)^{k_r}$, де $r = \mathrm{len}(x)$, а $y = \mathrm{p}(0)^{l_0}\,\mathrm{p}(1)^{l_1} \ldots \mathrm{p}(s)^{l_s}$, де $s = \mathrm{len}(y)$. Ця функція також примітивно-рекурсивна:

   $$x * y = x \prod_{z\leqslant \mathrm{len}(y)} \mathrm{p}(\mathrm{len}(x) + z + 1)^{v(y,z)}.$$

(e) Якщо функція $f(\mathbf{x}, y)$ рекурсивна (примітивно-рекурсивна), то такою ж є функція

$$f^\sharp(\mathbf{x}, y) = \prod_{z<y} \mathrm{p}(z)^{f(\mathbf{x},z)}$$

(поясніть, чому). Навпаки, якщо функція $f^\sharp$ рекурсивна (примітивно-рекурсивна), то такою ж є і $f(\mathbf{x}, y) = v(f^\sharp(\mathbf{x}, y+1), y)$. Це дає можливість використовувати «рекурсію за всіма попередніми значеннями», а саме, задавати функцію f правилом $f(\mathbf{x}, y) = h(\mathbf{x}, y, f^\sharp(\mathbf{x}, y))$. Якщо h рекурсивна (примітивно-рекурсивна), такою ж є й $f^\sharp$, оскільки $f^\sharp(\mathbf{x}, 0) = 1$ і

$$f^\sharp(\mathbf{x}, y+1) = f^\sharp(\mathbf{x}, y)\,\mathrm{p}(y)^{f(\mathbf{x},y)} = f^\sharp(\mathbf{x}, y)\,\mathrm{p}(y)^{h(\mathbf{x},y,f^\sharp(\mathbf{x},y))},$$

а тому й f. Зауважимо, що $f^\sharp(\mathbf{x}, y)$ містить повну інформацію про всі значення $f(\mathbf{x}, z)$ при $z < y$. Саме, $f(\mathbf{x}, z) = v(f^\sharp(\mathbf{x}, y), z)$.

(f) Зокрема, рекурсивною (примітивно-рекурсивною) є функція, визначена «довгою рекурсією»:

$$f(\mathbf{x}, 0) = g_0(\mathbf{x}),\ \ f(\mathbf{x}, 1) = g_1(x), \ldots, f(\mathbf{x}, m) = g_m(\mathbf{x}),$$
$$f(\mathbf{x}, y+m+1) = h(\mathbf{x}, y, f(\mathbf{x}, y), \mathbf{x}(y+1), \ldots, \mathbf{x}(y+m)),$$

де функції g_k та h рекурсивні (примітивно-рекурсивні), а m — фіксоване натуральне число. Доведення залишаємо читачу як корисну вправу.

(g) Нагадаємо, що при фіксованому $m > 1$ кожне натуральне число x однозначно записується у *m-їчній системі числення*, тобто у вигляді $a_0 + a_1 m + a_2 m^2 + \cdots + a_r m^r$, де $0 \leqslant a_k < m$ для всіх k. Очевидно, тут $r = [\log_m x]$, тобто $\max\{\, l \mid m^l \leqslant x \,\}$. Неважко переконатися, що ця функція примітивно-рекурсивна (доведіть це). Назвемо число a_k *k-им m-їчним знаком* числа x і позначатимемо його $Z(x, k, m)$. Легко бачити, що $Z(x,\ k, m) = \mathrm{res}([x/m^k], m)$, отже, це теж примітивно-рекурсивна функція.

(h) Якщо функції $g_1, g_2, \ldots, g_n$ та відношення $\mathrm{R}_1, \mathrm{R}_2, \ldots, \mathrm{R}_m$ рекурсивні (примітивно-рекурсивні), причому для кожного $\mathbf{a}$ істинним є точно одне з цих відношень, то такою ж є функція

$$f(\mathbf{x}) = \begin{cases} g_1(\mathbf{x}) & \text{якщо істинне } \mathrm{R}_1(\mathbf{x}), \\ g_2(\mathbf{x}) & \text{якщо істинне } \mathrm{R}_2(\mathbf{x}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ g_m(\mathbf{x}) & \text{якщо істинне } \mathrm{R}_m(\mathbf{x}). \end{cases}$$

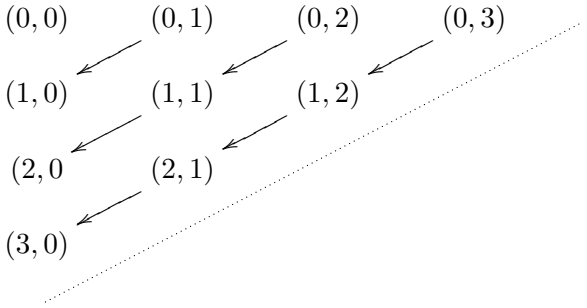
Дійсно, $f(\mathbf{x}) = \sum_{k=1}^{m} g_k(\mathbf{x})(1 \dot{-} \mathrm{R}(\mathbf{x}))$.

Розглянемо ще один важливий клас рекурсивних функцій, які встановлюють взаємно однозначну відповідність між $\mathbb{N}^n$ та $\mathbb{N}$ для довільного n.

Теорема 3.3.12. *Для кожного $n \geqslant 2$ існують такі примітивно-рекурсивні функції $\sigma_k^n(x)$ $(k = 1, 2, \ldots, n)$ та $\tau^n(x_1, x_2, \ldots, x_n)$, що*

$$\tau^n(\sigma_1^n(x), \sigma_2^n(x), \ldots, \sigma_n^n(x)) = x;$$
$$\sigma_k^n(\tau(x_1, x_2, \ldots, x_n)) = x_k \quad \text{для кожного } k.$$

Доведення. Нехай спочатку $n = 2$. Оскільки цей випадок буде для нас особливо важливим, ми писатимемо τ замість τ_2 і σ_k $(k = 1, 2)$ замість σ_k^2. Пари (a, b) натуральних чисел можна перенумерувати «по діагоналях»:



Інакше кажучи, пара (a, b) передує в цій нумерації парі (a', b'), якщо $a + b < a' + b'$ або $a + b = a' + b'$ і $a < a'$. Оскільки всього є $m + 1$ пара з $a + b = m$, отже, $m(m + 1)/2$ пар з $a + b < m$, номер $\tau(a, b)$ пари (a, b) у цій нумерації визначається формулою $\tau(a, b) = a + (a + b)(a + b + 1)/2$ (нагадаємо, що нумерація починається з нуля: $\tau(0, 0) = 0$). Навпаки, якщо задано номер c, то щоб визначити координати пари $(\sigma_1(c), \sigma_2(c))$ з номером c, треба спочатку знайти кількість d повних діагоналей, які передують цій парі: d — найбільше натуральне число таке, що $d(d + 1)/2 \leqslant c$, тобто $d = \left[(\sqrt{8c + 7} - 1)/2\right]$. Після цього одержуємо: $\sigma_1(c) = c - d$, $\sigma_2(c) = d - \sigma_1(c)$. Легко бачити, що функція, якою визначається d, примітивно-рекурсивна (залишаємо доведення цього читачу); отже, всі функції τ, σ_1, σ_2 примітивно-рекурсивні.

Загальний випадок доводиться індукцією за n: якщо σ_k^n та τ^n уже побудовані, можна покласти

$$\tau^{n+1}(x_1, x_2, \ldots, x_{n+1}) = \tau^n(x_1, x_2, \ldots, x_{n-1}, \tau^2(x_n, x_{n+1}));$$
$$\sigma_k^{n+1}(x) = \begin{cases} \sigma_k^n(x), & \text{якщо } k < n, \\ \sigma_1^2(\sigma_n^n(x)), & \text{якщо } k = n, \\ \sigma_2^2(\sigma_n^n(x)), & \text{якщо } k = n + 1 \end{cases}$$

(перевірте правильність цих формул) □

Завдяки функціям τ^n та σ_k^n ми можемо (і будемо, за деякими виключеннями) надалі розглядати замість підмножин у $\mathbb{N}^n$ та функцій $\mathbb{N}^n \to \mathbb{N}$ підмножини в $\mathbb{N}$ та функції $\mathbb{N} \to \mathbb{N}$. Зокрема, будемо називати відображення $f : \mathbb{N}^n \to \mathbb{N}^m$ *рекурсивним*, якщо такою є композиція $\sigma^n \circ f \circ \tau^m$, де $\sigma^n(x) = (\sigma_1^n(x), \ldots, \sigma_n^n(x))$. Рівносильна властивість: $f(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}))$, де всі функції f_i рекурсивні (поясніть, чому.)

3.4. Рекурсивність арифметичних функцій та множин

Переходимо до доведення теореми 3.3.5. Воно базується на теорії рекурсивних функцій та так званій *ґеделівській нумерації* речень формальної арифметики. Визначимо її у варіанті, дещо відмінному від оригінального ґеделівського. Оскільки нам потрібно розглядати не лише окремі речення, але й їхні послідовності (наприклад, виводи), додамо до алфавіту формальної арифметики ще розділовий знак _. Таким чином, послідовність речень виглядає як $R_1\_R_2\_\ldots\ \_R_n$, де R_i — окремі речення. Отже, загалом наш алфавіт $\mathcal{A}$ складається з 16 символів:

$$0 \quad 1 \quad \mathrm{v} \quad | \quad E \quad S \quad P \quad \vee \quad \wedge \quad \Rightarrow \quad \neg \quad \forall \quad \exists \quad (\quad) \quad \_$$

Перш за все ми пронумеруємо всі слова в цьому алфавіті.

Означення 3.4.1.

1. *Ґеделівські номери* літер алфавіту $\mathcal{A}$ визначаються таблицею:

0	1	v	|	E	S	P	$\vee$	$\wedge$	$\Rightarrow$	$\neg$	$\forall$	$\exists$	(	)	_
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

   Ґеделівський номер літери a позначається $\gamma(a)$.
2. *Ґеделівський номер* слова $w = a_n a_{n-1} \ldots a_1 a_0$ в алфавіті $\mathcal{A}$ визначається як $\gamma(w) = 16^n\gamma(a_n) + 16^{n-1}\gamma(a_{n-1}) + \cdots + 16\gamma(a_1) + \gamma(a_0)$. Іншими словами, геделівський номер слова — це число, 16-річний запис якого складається з ґеделівських номерів його літер (у тому самому порядку). Зауважимо, що згідно зі звичаєм ми нумеруємо цифри (а тому й літери) справа наліво.

З цього означення випливає, що функція γ встановлює взаємно однозначну відповідність між словами в алфавіті $\mathcal{A}$ та натуральними числами. Надалі ми часто казатимемо «номер слова» замість «ґеделівський номер», оскільки ніяких інших номерів словам в алфавіті $\mathcal{A}$ ми не приписуємо.

При обчисленні ґеделівських номерів постійно використовуються функції $\mathrm{l}(n) = [\log_{16} n] + 1$ (довжина 16-річного запису числа n) та $Z_k(n) = Z(n, k, 16)$ (k-й 16-річний знак числа n); див. приклад 3.3.11.2g.

Приклад 3.4.2.

1. Ґеделівський номер постулату $E\mathrm{vv}$ дорівнює $4 \cdot 16^2 + 2 \cdot 16 + 2 = 1072$.
2. Ґеделівський номер терма $\overline{\mathrm{n}} = \underbrace{SS\ldots S}_{n-1}\underbrace{11\ldots1}_{n}$ дорівнює
$$5 \cdot 16^{2n-2} + 5 \cdot 16^{2n-3} \cdots + 5 \cdot 16^n + 16^{n-1} + 16^{n-2} + \cdots + 1.$$
3. Ґеделівський номер приписування слів $w_0 w_1 w_2 \ldots w_n$ дорівнює

$$\gamma(w_n) + \gamma(w_{n-1}) \cdot 16^{\mathrm{l}(w_n)} + \gamma(w_{n-2}) \cdot 16^{\mathrm{l}(w_n)+\mathrm{l}(w_{n-1})} + \\ + \cdots + \gamma(w_0) \cdot 16^{\sum_{k=1}^{n} \mathrm{l}(w_k)} \tag{3.4.1}$$

(поясність, чому).

4. Наприклад, якщо $\gamma(w) = n$, $\gamma(w') = m$, то ґеделівський номер послідовності $w\_(w \Rightarrow w')\_w'$ дорівнює

$$m + 15 \cdot 16^{\mathrm{l}(m)} + 14 \cdot 16^{\mathrm{l}(m)+1} + m \cdot 16^{\mathrm{l}(m)+2} + \\ + 9 \cdot 16^{2\mathrm{l}(m)+2} + n \cdot 16^{2\mathrm{l}(m)+3} + 13 \cdot 16^{2\mathrm{l}(m)+\mathrm{l}(n)+3} + \\ + 15 \cdot 16^{2\mathrm{l}(m)+\mathrm{l}(n)+4} + n \cdot 16^{2\mathrm{l}(m)+\mathrm{l}(n)+5}.$$

Твердження 3.4.3. *Наведені відношення та функції на множині натуральних чисел є примітивно-рекурсивними:*

1. $\mathrm{Var}(x)$ — «x — ґеделівський номер змінної».
2. $\mathrm{Term}(x)$ — «x — ґеделівський номер терма».
3. $\mathrm{Atom}(x)$ — «x — ґеделівський номер атома (елементарного речення)».
4. $\mathrm{Sent}(x)$ — «x — ґеделівський номер речення».
5. $\mathrm{MP}(x, y, z)$ — «речення з номером x одержане за правилом modus ponens з речень з номерами y та z».
6. $\mathrm{Occ}(x, y, z)$ — «змінна з номером y входить у речення з номером x, причому перша зліва цифра цього входження знаходиться на z-му місці у 16-річному запису числа x».
7. $\mathrm{Oct}(x, y)$ — «змінна з номером y входить у терм з ґеделівським номером x».
8. $\mathrm{Dom}(x, y, z)$ — «у реченні з номером x входження змінної, 16-річний запис якого починається з z-го місця, знаходиться в області квантора $\mathrm{Q}v$, де v — змінна з номером y».
9. $\mathrm{Free}(x, y, z)$ — «входження змінної з номером y у речення з номером x, 16-річний запис якого починається з z-го місця, є вільним».
10. $\mathrm{Sub}(x, y, z)$ — номер речення, одержаного з речення з номером x підстановкою терма з номером y замість змінної з номером z.
11. $\mathrm{Gen}(x, y)$ — «речення з номером x одержане з речення з номером y узагальненням».
12. $\mathrm{Tfr}(x, y, z)$ — «терм з номером y є вільним для змінної з номером y у реченні з номером z».
13. $\mathrm{Ded}(x, y)$ — «x — номер виводу (у формальній арифметиці) речення з номером y».

Доведення. Оскільки доведення всіх пунктів цього твердження дуже подібні одне до одного, то викладемо лише частину з них, лишаючи інші як корисну й не дуже складну вправу для читача.

1. З означення 2.1.1.2 випливає, що ґеделівські номери змінних — це $2 \cdot 16^n + 3 \cdot 16^{n-1} + \cdots + 3 \cdot 16 + 3$ (2 при $n = 0$), де x — довжина 16-річного запису. Тому характеристична функція множини цих номерів має вигляд

$$\mathrm{Var}(x) = \mathrm{sg}\left(\left|Z_{\mathrm{l}(x)}(x) - 2\right| + \textstyle\sum_{y<\mathrm{l}(x)} \left|Z_y(x) - 3\right|\right).$$

2. Рекурсивна побудова термів в означенні 2.1.1.3 і те, що формальна арифметика містить дві константи, 0 та 1, і два двомісні функціонали,

S та P, показує, що

$$\begin{aligned}
&\text{(i)} \qquad \mathrm{Term}(x) = \mathrm{sg}\Big((x \dot{-} 1)\cdot\\
&\text{(ii)} \qquad \cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - \big(5\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)} + y\cdot 16^{\mathrm{l}(z)} + z\big)\big| +\\
&\qquad\qquad + \mathrm{Term}(y) + \mathrm{Term}(z)\big)\cdot\\
&\text{(iii)} \qquad \cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - \big(6\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)} + y\cdot 16^{\mathrm{l}(z)} + z\big)\big| +\\
&\qquad\qquad + \mathrm{Term}(y) + \mathrm{Term}(z)\big)\Big).
\end{aligned}$$

Дійсно, співмножник у рядку (i) дорівнює 0 тоді й лише тоді, коли $x = 0 = \gamma(0)$ або $x = 1 = \gamma(1)$; співмножник у рядку (ii) дорівнює 0 тоді й лише тоді, коли 16-річний запис числа x має вигляд $5ab$, де a та b — 16-річні записи номерів $y = \gamma(v)$ та $z = \gamma(w)$, причому v і w — терми, отже $x = \gamma(Svw)$; те саме (із заміною 5 на 6, а S на P) стосується співмножника в рядку (iii). Зауважимо, що тут ми скористалися «рекурсією за всіма попередніми значеннями» (приклад 3.3.11.2e).

3. Елементарні речення в арифметиці мають вигляд $E\mathrm{t}_1\mathrm{t}_2$, де $\mathrm{t}_1, \mathrm{t}_2$ — терми. Тому

$$\begin{aligned}
\mathrm{Atom}(x) = \mathrm{sg}\Big(&\textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (4\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)} + y\cdot 16^{\mathrm{l}(z)} + z)\big| +\\
&+ \mathrm{Term}(y) + \mathrm{Term}(z)\big)\Big).
\end{aligned}$$

4. Знов-таки, з рекурсивного означення 2.1.1.7 випливає, що

$$\begin{aligned}
&\mathrm{Sent}(x) = \mathrm{sg}\Big(\,\mathrm{Atom}(x)\cdot\\
&\cdot \textstyle\prod_{y<x}\big(\big|x - (10\cdot 16^{\mathrm{l}(y)} + y)\big| + \mathrm{Sent}(y)\big)\cdot\\
&\cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (13\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+2} + y\cdot 16^{\mathrm{l}(z)+2} + 7\cdot 16^{\mathrm{l}(z)+1} +\\
&\qquad + z\cdot 16 + 14)\big| + \mathrm{Sent}(y) + \mathrm{Sent}(z)\big)\cdot\\
&\cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (13\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+2} + y\cdot 16^{\mathrm{l}(z)+2} + 8\cdot 16^{\mathrm{l}(z)+1} +\\
&\qquad + z\cdot 16 + 14)\big| + \mathrm{Sent}(y) + \mathrm{Sent}(z)\big)\cdot\\
&\cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (13\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+2} + y\cdot 16^{\mathrm{l}(z)+2} + 9\cdot 16^{\mathrm{l}(z)+1} +\\
&\qquad + z\cdot 16 + 14)\big| + \mathrm{Sent}(y) + \mathrm{Sent}(z)\big)\cdot\\
&\\
&\cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (11\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)} + y\cdot 16^{\mathrm{l}(z)} + z)\big| +\\
&\qquad + \mathrm{Var}(y) + \mathrm{Sent}(z)\big)\cdot\\
&\cdot \textstyle\prod_{y<x}\prod_{z<x}\big(\big|x - (12\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)} + y\cdot 16^{\mathrm{l}(z)} + z)\big| +\\
&\qquad + \mathrm{Var}(y) + \mathrm{Sent}(z)\big)\Big).
\end{aligned}$$

5 — вправа.

6. Зауважимо, що цифри 2 і 3 (номери літер v і |) у 16-річному записі ґеделівського номера речення завжди є складовими частинами ґеделівського номера змінної, яка входить у це речення, причому першою зліва обов'язково є цифра 2, а наступний за цим входженням знак

відмінний від $|$. Тому

$$\mathrm{Occ}(x,y,z) = \mathrm{sg}\Big(\mathrm{Sent}(x) + \mathrm{Var}(y) + \big|Z_l(x) - 2\big| + \\ + \big|y - \big[\mathrm{res}(x, 16^{z+1})/16^{(z+1)\dot{-}\mathrm{l}(y)}\big]\big| + \overline{\mathrm{sg}}\,\big|Z_{z\dot{-}\mathrm{l}(y)}(x) - 3\big|\Big).$$

7 та 8 — вправи.

9. $\mathrm{Free}(x,y,z) = \mathrm{sg}\big(\mathrm{Occ}(x,y,z) + (1 \dot{-} \mathrm{Dom}(x,y,z))\big)$.

10. Введемо спочатку функцію $\mathrm{Sub}_1(x,y,z)$ — ґеделівський номер речення, одержаного з речення з номером x підстановкою терма з номером y замість першого (справа) вільного входження змінної з номером z:

$$\begin{aligned}\mathrm{Sub}_1(x,y,z) = {} & \mathrm{sg}\big((\mathrm{l}(x) \dot{-} u) + \mathrm{Term}(y)\big)\big(\mathrm{res}(x, 16^{(u+1)\dot{-}\mathrm{l}(z)}) + \\ & + 16^{(u+1)\dot{-}\mathrm{l}(z)} y + 16^{((u+1)\dot{-}\mathrm{l}(z))+\mathrm{l}(y)}[x/16^{u+1}]\big) + \\ & + \overline{\mathrm{sg}}\,\big((\mathrm{l}(x) \dot{-} u) + \mathrm{Term}(y)\big)x,\end{aligned}$$

де $u = \mu_{t<\mathrm{l}(x)}\,\mathrm{Free}(x,z,t)$. Дійсно, якщо дана змінна зовсім не входить вільно у дане речення (або x — не номер речення, або y — не номер терма), то $u = \mathrm{l}(x)$ і $\mathrm{Sub}_1(x,y,z) = x$. Інакше речення має вигляд $w_1 w_2 w_3$, де слово w_2 — перше входження даної змінної, тому його довжина дорівнює $\mathrm{l}(z)$, а його перша зліва літера займає місце з номером u. Тоді $\mathrm{res}(x, 16^{(u+1)\dot{-}\mathrm{l}(z)})$ — номер слова w_3, а $[x/16^{u+1}]$ — номер слова w_1. Тому результат обчислення за наведеною формулою дає номер слова $w_1 w_4 w_2$, де w_4 — даний терм, що й є результатом бажаної підстановки.

Тепер означимо функцію $\mathrm{Sub}(x,y,z,t)$ рекурсією

$$\begin{aligned}\mathrm{Sub}(x,y,z,0) &= x,\\ \mathrm{Sub}(x,y,z,t+1) &= \mathrm{Sub}_1(\mathrm{Sub}(x,y,z,t),y,z).\end{aligned}$$

Очевидно, $\mathrm{Sub}(x,y,z) = \mathrm{Sub}(x,y,z,\mathrm{l}(x))$.

11 та 12 — вправи.

13. Числення відношень має 14 схем аксіом (A1–A14); крім них, формальна арифметика має 7 аксіом рівності (аксіома (E1), 4 аксіоми типу (E2) для функціоналів S і T та 2 аксіоми типу (E3) для предиката E), 6 постулатів (N1–N6) та схему постулатів індукції (N7); усього 28 схем та конкретних аксіом і постулатів. Позначимо $\mathrm{Ax}_k(x)$ відношення «x — номер аксіоми (постулату), яка є k-ою в цьому переліку» і перевіримо, що це відношення примітивно-рекурсивне. Оскільки $\mathrm{Ax}(x) = \prod_{k=1}^{28}\mathrm{Ax}_k(x)$, то й відношення $\mathrm{Ax}(x)$ теж примітивно-рекурсивне. Ми виконаємо лише три перевірки, залишивши інші (цілком аналогічні) читачу.

$\mathrm{Ax}_1(x)$ — «x — ґеделівський номер аксіоми вигляду (A1)», тобто $(\mathbf{A} \Rightarrow (\mathbf{B} \Rightarrow \mathbf{A}))$:

$$\begin{aligned}\mathrm{Ax}_1(x) = {} & \mathrm{sg}\Big(\textstyle\prod_{y<x}\prod_{z<x}\big(\mathrm{Sent}(y) + \mathrm{Sent}(z) + \\ & + \big|x - (14 + 14\cdot 16 + y\cdot 16^2 + 9\cdot 16^{\mathrm{l}(y)+2} + \\ & + z\cdot 16^{\mathrm{l}(y)+3} + 13\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+3} + 9\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+4} + \\ & + y\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+5} + 13\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(z)+5})\big|\big)\Big).\end{aligned}$$

$\mathrm{Ax}_{12}(x)$ — «x — ґеделівський номер аксіоми вигляду (A12)», тобто $(\mathbf{A}^{\mathrm{z}}_{\mathrm{t}} \Rightarrow \exists \mathrm{z}\mathbf{A})$, де терм t вільний для змінної z у реченні $\mathbf{A}$:

$$\begin{aligned}\mathrm{Ax}_{12}(x) = \mathrm{sg}\Big(\prod_{y<x}\prod_{z<y}\prod_{t<x}\big(\mathrm{Sent}(y) + \mathrm{Var}(z) + \mathrm{Term}(t) + \\ + \mathrm{Tfr}(y,z,t) + \big|x - (14 + 16y + z\cdot 16^{\mathrm{l}(y)+1} + \\ + 12\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+1} + 9\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+2} + \\ + u\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+3} + 13\cdot 16^{\mathrm{l}(y)+\mathrm{l}(z)+\mathrm{l}(u)+3})\big|\big)\Big),\end{aligned}$$

де $u = \mathrm{Sub}(y,t,z)$.

$\mathrm{Ax}_{28}(x)$ — «x — ґеделівський номер постулату індукції», тобто $((\mathbf{A}^{\mathrm{v}}_0 \wedge \forall \mathrm{v}(\mathbf{A} \Rightarrow \mathbf{A}^{\mathrm{v}}_{S\mathrm{v}1})) \Rightarrow \forall \mathrm{v}\mathbf{A})$:

$$\begin{aligned}\mathrm{Ax}_{28}(x) = \mathrm{sg}\Big(\prod_{y<x}\big(\mathrm{Sent}(y) + \big|x - (14 + 16y + 2\cdot 16^{\mathrm{l}(y)+1} + \\ + 11\cdot 16^{\mathrm{l}(y)+2} + 9\cdot 16^{\mathrm{l}(y)+3} + 14\cdot 17\cdot 16^{\mathrm{l}(y)+4} + \\ + u\cdot 16^{\mathrm{l}(y)+6} + 9\cdot 16^{\mathrm{l}(y)+\mathrm{l}(u)+6} + y\cdot 16^{\mathrm{l}(y)+\mathrm{l}(u)+7} + \\ + 13\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+7} + 2\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+8} + 11\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+9} + \\ + 8\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+10} + t\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+11} + \\ + 13\cdot 17\cdot 16^{2\mathrm{l}(y)+\mathrm{l}(u)+\mathrm{l}(t)+11})\big|\big)\Big),\end{aligned}$$

де $t = \mathrm{Sub}(y,2,0)$, $u = \mathrm{Sub}(y,2,1313)$ (зауважимо, що $1313 = 5\cdot 16^2 + 2\cdot 16 + 1 = \gamma(S\mathrm{v}1)$).

14. Розглянемо спочатку відношення $\mathrm{Seq}(x,y)$ — «x — номер послідовності речень, яка містить речення з номером y»:

$$\begin{aligned}\mathrm{Seq}(x,y) = \mathrm{sg}\Big(\mathrm{Sent}(y) + |x-y|\cdot\prod_{z<x}\prod_{t<x}\big(\mathrm{Seq}(z,y) + \mathrm{Sent}(t) + \\ + \big|x - (z + 15\cdot 16^{\mathrm{l}(z)} + t\cdot 16^{\mathrm{l}(z)+1})\big|\cdot \\ \cdot\big|x - (t + 15\cdot 16^{\mathrm{l}(t)} + z\cdot 16^{\mathrm{l}(t)+1})\big|\big)\Big).\end{aligned}$$

Тепер відношення $\mathrm{Ded}(x,y)$ можна обчислити так:

$$\begin{aligned}\mathrm{Ded}(x,y) = \mathrm{sg}\Big(\big(\mathrm{Ax}(y) + |x-y|\big)\cdot\prod_{z<x}\prod_{t\leqslant z}\big(\mathrm{Ded}(z,t) + \\ + \big|x - (y + 15\cdot 16^{\mathrm{l}(y)} + z\cdot 16^{\mathrm{l}(y)+1})\big| + \\ + \mathrm{Ax}(y)\cdot\prod_{u\leqslant z}\big(\mathrm{Seq}(z,u) + \mathrm{Gen}(y,u)\big)\cdot \\ \cdot\prod_{u<z}\prod_{v<z}\big(\mathrm{Seq}(z,u) + \mathrm{Seq}(z,v) + \mathrm{MP}(y,u,v)\big)\Big)\ \square\end{aligned}$$

Тепер ми готові довести теорему 3.3.5, а разом з нею й теорему 3.2.5. Зауважимо, що завдяки теоремі 3.3.12 достатньо розглядати функції від однієї змінної та підмножини в $\mathbb{N}$. Встановимо такий результат, з якого ця теорема випливає.

Теорема 3.4.4. *Якщо функція $f : \mathbb{N}^n \to \mathbb{N}$ напіварифметична, то існує примітивно-рекурсивна функція $g(\mathbf{x}, y)$ така, що $f(\mathbf{x}) = \sigma_1(\mu_y g(\mathbf{x}, y))$, де $\sigma_1 = \sigma_1^2$ — функція, розглянута в теоремі 3.3.12.*

Доведення. Нехай $n = 1$ і речення $\mathbf{A}(\mathrm{x}, \mathrm{y})$ виражає функцію $f(x)$; інакше кажучи, $f(a) = b$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{A}(a, b)$. Позначимо $n = \gamma(\mathbf{A})$, $m = \gamma(\mathrm{x})$, $l = \gamma(\mathrm{y})$ і покладемо

$$h(x, y, z) = \mathrm{Ded}(z, \mathrm{Sub}(\mathrm{Sub}(n, m, x), l, y)).$$

За означенням, $h(a, b, c) = 0$ тоді й лише тоді, коли c — номер виводу речення $\mathbf{A}(a, b)$. Зауважимо, що для кожного a існує єдине b таке, що $\mathfrak{A} \vdash \mathbf{A}(a, b)$, або, що рівносильно, для кожного a існують такі b, c, що $h(a, b, c) = 0$, причому значення b в усіх таких парах спільне. Нехай $g(x, y) = h(x, \sigma_1(y), \sigma_2(y))$. Тоді для кожного a існує таке c, що $g(a, c) = 0$, і при цьому $f(a) = \sigma_1(c)$. Отже, дійсно, $f(x) = \sigma_1(\mu_y g(x, y))$ □

Перейдемо до розгляду напіварифметичних множин. Для цього введемо таке поняття.

Означення 3.4.5. Підмножина $M \subseteq \mathbb{N}^n$ називається (рекурсивно) *перераховною*, якщо вона є множиною значень деякого рекурсивного відображення.

Теорема 3.4.6. *Непорожня підмножина $M \subseteq \mathbb{N}^n$ напіварифметична тоді й лише тоді, коли вона перераховна. Перераховна підмножина завжди є образом деякого примітивно-рекурсивного відображення.*

Доведення. Знов-таки, можна вважати, що $M \subseteq \mathbb{N}$. Припустимо, що M напіварифметична і речення $\mathbf{A}(\mathrm{x})$ з ґеделівським номером m виражає M, тобто $a \in M$ тоді й лише тоді, коли $\mathfrak{A} \vdash \mathbf{A}(a)$. Розглянемо функції $h(x, y) = \mathrm{Ded}(y, \mathrm{Sub}(m, l, x))$, де $l = \gamma(\mathrm{x})$, і $g(x) = h(\sigma_1(x), \sigma_2(x))$. Згідно з означенням, $a \in M$ тоді й лише тоді, коли знайдеться таке число b, що $h(a, b) = 0$. Зафіксуємо елемент $c \in M$ (нагадаємо, що $M \neq \emptyset$) і задамо функцію $f(x)$ правилом

$$f(x) = \begin{cases} \sigma_1(x), & \text{якщо } g(x) = 0, \\ c, & \text{якщо } g(x) \neq 0. \end{cases}$$

Згідно з прикладом 3.3.11.2h, ця функція примітивно-рекурсивна, і, очевидно, M — множина значень цієї функції.

Обернене твердження безпосередньо випливає з наслідка 3.3.4 та такого результату.

Твердження 3.4.7. *Якщо функція $f(x)$ правильно визначається реченням $\mathbf{A}(\mathrm{x}, \mathrm{y})$, то множина M її значень визначається реченням $\exists \mathrm{x} \mathbf{A}(\mathrm{x}, \mathrm{y})$.*

Доведення. Якщо $b \in M$, то існує a таке, що $f(a) = b$, отже, $\mathfrak{A} \vdash \mathbf{A}(a, b)$ і $\mathfrak{A} \vdash \exists \mathrm{x} \mathbf{A}(\mathrm{x}, b)$. Припустимо, що $b \notin M$. Нехай a — довільне натуральне число і $c = f(a)$. Тоді $\mathfrak{A} \vdash \mathbf{A}(a, \mathrm{y}) \Rightarrow \mathrm{y} = c$ і $\mathfrak{A} \vdash b \neq c$, звідки $\mathfrak{A} \vdash \neg \mathbf{A}(a, b)$. З гіпотези про стандартну модель (точніше, з ω-несуперечливості формальної арифметики) випливає, що тоді речення $\exists \mathrm{x} \mathbf{A}(\mathrm{x}, b)$ не виводиться у формальній арифметиці. Отже, речення $\exists \mathrm{x} \mathbf{A}(\mathrm{x}, \mathrm{y})$ визначає підмножину M □

Наслідок 3.4.8. *Образ напіварифметичної (або, що те саме, перераховної) підмножини при арифметичному (або, що те саме, рекурсивному) відображенні є напіварифметичною (тобто перераховною) підмножиною.*

У наступному розділі ми побачимо, що, навпаки, образ арифметичної підмножини може не бути арифметичним (хоча він завжди є напіварифметичним).

3.5. Неповнота формальної арифметики

У цьому розділі ми встановимо серію результатів, які показують, що формальна арифметика не вичерпує (і принципіально не може вичерпати) усіх засобів арифметики натуральних чисел. Перш за все, це — так звана «*теорема Ґеделя про неповноту*» (її можна також назвати «*теоремою про неадекватність*» формальної арифметики).

Теорема 3.5.1. *Існує замкнене речення* Γ *формальної арифметики, яке істинне в її стандартній моделі* $\mathcal{N}$*, але не виводиться у формальній арифметиці.*

Зауважимо, що, оскільки Γ істинне, то $\neg\Gamma$ також не виводиться у формальній арифметиці, якшо ми приймаємо принцип коректності.

Доведення. Розглянемо відношення $G(x,y)$ — «x — ґеделівський номер якогось речення $\mathbf{A}$, а y — номер виводу речення $\mathbf{A}^{\mathrm{v}}_{x}$». Воно примітивно-рекурсивне: $G(x,y) = \mathrm{Ded}(y, \mathrm{Sub}(x, \gamma(x), 2))$. (Як завжди, ми пишемо $\gamma(x)$ замість $\gamma(\overline{\mathrm{x}})$; легко бачити, що ця функція примітивно-рекурсивна.) Тому існує речення $\mathbf{G}(\mathrm{x},\mathrm{y})$, яке правильно виражає це відношення. Очевидно, можна вважати, що $\mathbf{G}$ не містить вільних змінних, крім x і y. Перейменування змінних дозволяє припустити, що $\mathrm{x} = \mathrm{v}$. Позначимо n ґеделівський номер речення $\neg\exists\mathrm{y}\mathbf{G}(\mathrm{v},\mathrm{y})$ і покладемо $\Gamma = \neg\exists\mathrm{y}\mathbf{G}(n,\mathrm{y})$. Тоді $\gamma(\Gamma) = \mathrm{Sub}(n, \gamma(n), 2)$. Припустимо, що $\mathfrak{A} \vdash \Gamma$ і m — ґеделівський номер якогось виводу цього речення. Тоді, за означенням, $G(n,m)$ істинне, тому $\mathfrak{A} \vdash \mathbf{G}(n,m)$ і $\mathfrak{A} \vdash \exists\mathrm{y}\mathbf{G}(n,\mathrm{y})$, тобто $\mathfrak{A} \vdash \neg\Gamma$. Це неможливо, якщо вважати теорію $\mathfrak{A}$ несуперечливою (що випливає з гіпотези про стандартну модель). Отже, речення Γ не можна вивести у формальній арифметиці.

З іншого боку, якщо речення $\exists\mathrm{y}\mathbf{G}(n,\mathrm{y})$ істинне у стандартній моделі, то знайдеться натуральне число m таке, що істинним у цій моделі буде речення $\mathbf{G}(n,m)$. Тоді $G(n,m)$ — істинне (бо $\mathfrak{A} \vdash \neg\mathbf{G}(n,m)$ неможливо), отже, m — номер виводу речення Γ. Ми вже бачили, що це неможливо. Тому речення $\exists\mathrm{y}\mathbf{G}(n,\mathrm{y})$ хибне, а його заперечення, тобто речення Γ, істинне у стандартній моделі $\square$

Теорема Ґеделя про неповноту є своєрідною переробкою класичного «парадокса брехуна», який полягає в нерозв'язному питанні: говорить людина правду чи бреше, коли вона каже «я брешу»? Фактично цей парадокс показує, що такі поняття як «говорити правду» та «брехати» не піддаються формальному означенню. У теоремі Ґеделя речення Γ каже «мене не можна довести». Ясно, що коли б це речення було хибним, його можна було б довести, а тому воно було б істинним. Отже, воно

є істинним, але тоді його таки не можна довести! Головне відкриття Ґеделя полягає в тому, що він показав, як поняття «можна довести» можна формалізувати всередині формальної арифметики.

Відзначимо ще один дещо несподіваний наслідок з теореми Ґеделя.

Наслідок 3.5.2. *Існують такі моделі формальної арифметики, в яких істинними є деякі замкнені речення, хибні у стандартній моделі.*

Зауважимо, що згідно з вправою 3.1.5 усі ці моделі можна вважати *розширеннями* стандартної моделі (отже, неелементарними розширеннями).

Доведення. Оскільки речення Г, про яке йшлося в теоремі 3.5.1, не виводиться з формальної арифметики, теорія $\mathfrak{A} \cup \{\neg Г\}$ несуперечлива, а тому має модель. У цій моделі істинним є речення ¬Г, хибне у стандартній моделі □

Наступний результат — теорема Черча про нерозв'язність — дає, зокрема, приклад перераховної, але нерекурсивної підмножини.

Теорема 3.5.3. *Множина* Th *ґеделівських номерів теорем формальної арифметики є перераховною (отже, напіварифметичною), але не рекурсивною (отже, не арифметичною).*

Доведення. Перше твердження тепер майже очевидне. Дійсно, розглянемо функцію

$$f(x,y) = y(1 \dot{-} \mathrm{Ded}(x,y)) + 1024\,\mathrm{Ded}(x,y).$$

Оскільки 1024 — ґеделівський номер теореми $E00$ (тобто $0 = 0$), множиною значень цієї функції є Th. Отже, Th — перераховна множина.

З іншого боку, припустимо, що Th рекурсивна, а тому правильно виражається деяким реченням $\mathbf{T}(\mathrm{x})$. Іншими словами, якщо речення з номером a є теоремою, то $\mathfrak{A} \vdash \mathbf{T}(a)$, а якщо ні, то $\mathfrak{A} \vdash \neg\mathbf{T}(a)$. Розглянемо також речення $\mathbf{D}(\mathrm{y},\mathrm{z})$, яке правильно виражає примітивно-рекурсивну функцію $\mathrm{Sub}(y, \gamma(y), 2)$. Знов-таки, можна вважати, що $\mathrm{y} = \mathrm{v}$, $\mathrm{z} = \mathrm{x}$ і x є єдиною вільною змінною в реченні $\mathbf{T}$. Позначимо через n номер речення $\mathbf{A}(\mathrm{x}) = \forall\mathrm{x}(\mathbf{D}(\mathrm{v},\mathrm{x}) \Rightarrow \neg\mathbf{T}(\mathrm{x}))$, а через m — номер речення $\mathbf{A}(n) = \forall\mathrm{x}(\mathbf{D}(n,\mathrm{x}) \Rightarrow \neg\mathbf{T}(\mathrm{x}))$. Зауважимо, що $\mathrm{Sub}(n, \gamma(n), 2) = m$, тому $\mathfrak{A} \vdash \mathbf{D}(n,m) \wedge (\mathbf{D}(n,\mathrm{x}) \Rightarrow \mathrm{x} = m)$. Якщо речення $\mathbf{A}(n)$ не є теоремою, то $\mathfrak{A} \vdash \neg\mathbf{T}(m)$. З іншого боку, якщо $\mathbf{A}(n)$ є теоремою, тобто $\mathfrak{A} \vdash \mathbf{A}(n)$, то $\mathfrak{A} \vdash \mathbf{D}(n,m) \Rightarrow \neg\mathbf{T}(m)$, тому теж $\mathfrak{A} \vdash \neg\mathbf{T}(m)$. Отже, завжди $\mathfrak{A} \vdash \neg\mathbf{T}(m)$, тобто $\mathbf{A}(n)$ не є теоремою. Разом з $\mathfrak{A} \vdash \mathbf{D}(n,\mathrm{x}) \Rightarrow \mathrm{x} = m$ це дає $\mathfrak{A} \vdash \mathbf{D}(n,\mathrm{x}) \Rightarrow \neg\mathbf{T}(\mathrm{x})$ і $\mathfrak{A} \vdash \forall\mathrm{x}(\mathbf{D}(n,\mathrm{x}) \Rightarrow \neg\mathbf{T}(\mathrm{x}))$. Отже, $\mathbf{A}(n)$ є теоремою. Одержане протиріччя показує, що наше припущення невірне: множина Th нерекурсивна □

Ще один принциповий результат — це теорема Тарського про неарифметичність поняття істинності в арифметиці.

Теорема 3.5.4. *Множина* Ver *ґеделівських номерів замкнених речень формальної арифметики, істинних у стандартній моделі, не є напіварифметичною (або, що те саме, перераховною).*

Доведення. Припустимо, що існує речення $\mathbf{A}(\mathrm{x})$ таке, що $\mathfrak{A} \vdash \mathbf{A}(a)$ тоді й лише тоді, коли a — номер замкненого речення, істинного у стандартній моделі. Знов-таки, можна вважати, що x — єдина вільна змінна в цьому реченні. Розглянемо речення $\mathbf{A}'(\mathrm{x}) = \neg\mathrm{Cl}(\mathrm{x}) \vee \mathbf{A}(\mathrm{x} + 10 \cdot 16^{\mathrm{l}(x)}))$, де $\mathrm{Cl}(x)$ виражає відношення «x — номер замкненого речення» (легко бачити, що це відношення примітивно-рекурсивне; перевірте це). Оскільки якщо $x = \gamma(w)$, то $x + 10 \cdot 16^{\mathrm{l}(x)} = \gamma(\neg w)$, $\mathfrak{A} \vdash \mathbf{A}'(a)$ тоді й лише тоді, коли a не є номером замкненого речення, істинного у стандартній моделі. Отже, Ver — арифметична підмножина, а тоді існує речення $\mathbf{V}$, яке правильно виражає цю підмножину. Тепер можна повторити доведення теореми 3.5.2, замінивши всюди $\mathbf{T}$ на $\mathbf{V}$ □

Отже, на відміну від множини теорем, яку можна перерахувати (хоча й не існує «обчислювального» критерію належності речення до цієї множини), множину істинних речень (у стандартній моделі) взагалі не можна навіть перерахувати. З «метаматематичного» погляду це означає, що знаходження істинних речень арифметики натуральних чисел може бути лише творчим процесом, в якому вирішальну роль мусить відігравати відкриття нових засобів доведення.

Нарешті, наведемо ще одну теорему Ґеделя, яка, у деякому розумінні, поклала край гільбертівській програмі, націленій на формальне доведення несуперечливості формальних математичних теорій. А саме, нехай речення $\mathbf{T}(\mathrm{v})$ виражає множину Th номерів теорем (нагадаємо, що вона напіварифметична). Розглянемо речення $\mathbf{T}(1025)$. Оскільки $1025 = \gamma(E01)$, це речення виводиться у формальній арифметиці тоді й лише тоді, коли в ній виводиться речення $0 = 1$, тобто, коли формальна арифметика суперечлива. Отже, несуперечливість формальної арифметики виражається реченням $\neg\mathbf{T}(1025)$.

Теорема 3.5.5. *Несуперечливість формальної арифметики (або речення* $\mathrm{Cor} = \neg\mathbf{T}(1025)$*) не може бути виведена у формальній арифметиці.*

Доведення. Ми дамо лише начерк доведення, лишаючи деталі читачу. Перш за все, треба формалізувати доведення теореми 3.5.1 у тій частині, де з несуперечливості $\mathfrak{A}$ було виведено, що Г не є теоремою формальної арифметики. Зі змісту речення Г тоді випливає, що існує вивід $\mathfrak{A} \vdash \mathrm{Cor} \Rightarrow$ Г. Якби існував вивід Cor, то ми б одержали вивід Г, що неможливо □

Вправа 3.5.6.

1. Перевірте, що доведення теореми Ґеделя 3.5.1 можна пере- робити

так, щоб у ньому використовувалась лише *ω-несуперечливість* формальної арифметики.

2. Нехай $\mathbf{G}(\mathrm{v},\mathrm{y})$ має той самий зміст, що й у доведенні теореми 3.5.1, а речення $\mathbf{H}(\mathrm{v},\mathrm{y})$ правильно виражає відношення «x — номер якогось речення, а y — номер виводу речення $\neg\mathbf{A}_x^{\mathrm{v}}$». Позначимо n ґеделівський номер речення

$$\forall\mathrm{y}\big(\mathbf{G}(\mathrm{v},\mathrm{y})\Rightarrow\exists\mathrm{z}(\mathrm{z}<\mathrm{y}\wedge\mathbf{H}(\mathrm{v},\mathrm{z}))\big).$$

Доведіть, користуючись лише *несуперечливістю* формальної арифметики, що ані *речення Россера*

$$\mathrm{P}=\forall\mathrm{y}\big(\mathbf{G}(n,\mathrm{y})\Rightarrow\exists\mathrm{z}(\mathrm{z}<\mathrm{y}\wedge\mathbf{H}(n,\mathrm{z}))\big),$$

ані його заперечення не виводяться у формальній арифметиці.

Вказівка: Ось можлива схема доведення:

(a) Якщо m — номер якогось виводу P, то знайдеться $m'<m$ таке, що m' — номер виводу $\neg$P.

(b) Якщо m — номер якогось виводу $\neg$P, то $\mathfrak{A}\vdash\mathrm{y}\leqslant m\Rightarrow\neg\mathbf{G}(n,\mathrm{y})$. З іншого боку, $\mathfrak{A}\vdash m<\mathrm{y}\Rightarrow\exists\mathrm{z}(\mathrm{z}<\mathrm{y}\wedge\mathbf{H}(n,\mathrm{z}))$. Звідси $\mathfrak{A}\vdash\neg\mathrm{P}\vee\leqslant\mathrm{y}\Rightarrow\exists\mathrm{z}(\mathrm{z}<\mathrm{y}\wedge\mathbf{H}(n,\mathrm{z}))$, отже, $\mathfrak{A}\vdash\mathrm{P}$.

3. Як наслідок, доведіть, що речення Россера є істинним у стандартній моделі арифметики.

3.6. Доповнення й коментарі

3.6.1. Узагальнення принципів неповноти

Ми довели низку «теорем про неповноту», виходячи з конкретної формалізації арифметики натуральних чисел, запропонованої в розділі 3.1. Проте аналіз доведень дозволяє зробити висновок, що насправді їх можна перенести на будь-яку «достатньо потужну» теорію. Наступні розгляди є спробою точно накреслити, що саме для цього потрібно. При цьому всі доведення ми залишаємо читачу як вправи, оскільки вони цілком аналогічні наведеним у попередніх розділах. Зауважимо, перш за все, що коли задано довільний скінченний алфавіт, то можна визначити ґеделівську нумерацію слів у цьому алфавіті, аналогічно тому, як це зроблено в розділі 3.4 для алфавіту формальної арифметики. Ми будемо, як і раніше, позначати через $\gamma(w)$ номер слова w у цій нумерації. Звичайно, число 16 слід замінити на кількість літер у даному алфавіті. Очевидно, обмеження скінченності не є істотним: будь-який зліченний алфавіт $\{\mathrm{a}_0,\mathrm{a}_1,\ldots,\mathrm{a}_n,\ldots\}$ нескладно замінити скінченним, навіть алфавітом, який складається з двох літер, наприклад, $\{0,1\}$, замінюючи літеру a_k двоїчним записом номера k. Надалі через $\mathfrak{T}$ ми позначатимемо деяку теорію першого порядку з алфавітом $\mathcal{T}$. Ми будемо вважати, що $\mathfrak{T}$ — теорія з рівністю, хоча це обмеження теж не дуже істотне. Перш за все, легко встановити (і ми будемо цим користуватися), що пункти 1–12 твердження 3.4.3 залишаються вірними в будь-якій теорії.

Означення 3.6.1. Будемо казати, що теорія $\mathfrak{T}$

(1) *Виражає арифметику*, якщо в ній існують:

- для кожного натурального числа n речення з однією вільною змінною $\mathbf{N}_n(\mathrm{v})$;

- речення $\mathbf{S}(\mathrm{x},\mathrm{y},\mathrm{z})$ та $\mathbf{P}(\mathrm{x},\mathrm{y},\mathrm{z})$ з трьома вільними змінними такі, що виконуються твердження:

(i) $\mathfrak{T} \vdash \exists!\mathrm{v}\,\mathbf{N}_n(\mathrm{v})$ для кожного $n \in \mathbb{N}$;
(ii) $\mathfrak{T} \vdash \mathbf{N}_n(\mathrm{v}) \Rightarrow \neg\mathbf{N}_m(\mathrm{v})$, якщо $n \neq m$;
(iii) $\mathfrak{T} \vdash \mathbf{N}_n(\mathrm{x}) \wedge \mathbf{N}_m(\mathrm{y}) \wedge \mathbf{N}_{n+m}(\mathrm{z}) \Rightarrow \mathbf{S}(\mathrm{x},\mathrm{y},\mathrm{z})$ для довільних $n, m \in \mathbb{N}$;
(iv) $\mathfrak{T} \vdash \mathbf{N}_n(\mathrm{x}) \wedge \mathbf{N}_m(\mathrm{y}) \wedge \mathbf{N}_{nm}(\mathrm{z}) \Rightarrow \mathbf{P}(\mathrm{x},\mathrm{y},\mathrm{z})$ для довільних $n, m \in \mathbb{N}$.

До такої теорії, згідно з правилом «виводу з вибором» (розділ 2.7), можна додати константи $\overline{\mathrm{n}}$ і речення $\mathbf{N}_n(\overline{\mathrm{n}})$. Ми завжди вважатимемо, що це вже зроблено. Тоді умову (i) можна переписати у вигляді $\mathfrak{T} \vdash \mathbf{N}_n(\mathrm{v}) \Rightarrow \mathrm{v} = \overline{\mathrm{n}}$. Будемо казати, що константа $\overline{\mathrm{n}}$ *зображає натуральне число* n. Речення $\mathbf{S}(\mathrm{x},\mathrm{y},\mathrm{z})$ та $\mathbf{P}(\mathrm{x},\mathrm{y},\mathrm{z})$ треба розглядати як формалізацію виразів, відповідно, $x+y=z$ та $xy=z$. Тоді твердженя (iii-iv) означають, що дії над константами, які зображають натуральні числа, збігаються з діями над самими цими числами. Вправа 3.1.5.2 показує, що формальна арифметика дійсно виражає арифметику.

(2) *Виражає рекурсивні функції*, якщо вона виражає арифметику і для кожної рекурсивної функції $f(x_1, x_2, \ldots, x_n)$ існує речення $\mathbf{F}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_{n+1})$ теорії $\mathfrak{T}$ таке, що $a_{n+1} = f(a_1, a_2, \ldots, a_n)$ тоді й лише тоді, коли

$$\mathfrak{T} \vdash \mathbf{F}(\overline{\mathrm{a}}_1, \overline{\mathrm{a}}_2, \ldots, \overline{\mathrm{a}}_{n+1}) \wedge \big(\mathbf{F}(\overline{\mathrm{a}}_1, \overline{\mathrm{a}}_2, \ldots, \overline{\mathrm{a}}_n, \overline{\mathrm{y}}) \Rightarrow \overline{\mathrm{y}} = \overline{\mathrm{a}}_{n+1}\big).$$

Тут, як і вище, $\overline{\mathrm{a}}$ позначає константу теорії $\mathfrak{T}$, яка зображає натуральне число a. Аналогічно означенню 3.2.4, будемо казати, що речення $\mathbf{F}$ *правильно визначає* функцію f.

(3) *Рекурсивна*, якщо множина ґеделівських номерів її постулатів рекурсивна.

Формальна арифметика, як ми знаємо, виражає рекурсивні функції і є рекурсивною. Інший важливий приклад (який ми тут не розглядаємо) — це так звана *аксіоматична теорія множин*. Про неї теж відомо, що вона рекурсивна і виражає рекурсивні функції. З подробицями можна ознайомитись, наприклад, у [**Мен**, гл. 5].

Вправа 3.6.2. Припустимо, що теорія $\mathfrak{T}$ виражає арифметику. Аналогічно вправі 3.1.5.3 доведіть, що коли $F(x_1, x_2, \ldots, x_n)$ — многочлен з цілими коефіцієнтами, то існує речення $\overline{\mathrm{F}}(\mathrm{x}_1, \mathrm{x}_2, \ldots, \mathrm{x}_n, \mathrm{y})$ теорії $\mathfrak{T}$ таке, що $F(a_1, a_2, \ldots, a_n) = b$, де $a_1, a_2, \ldots, a_n$ — натуральні числа, тоді й лише тоді, коли $\mathfrak{T} \vdash \overline{\mathrm{F}}(\overline{\mathrm{a}}_1, \overline{\mathrm{a}}_2, \ldots, \overline{\mathrm{a}}_n, \overline{\mathrm{b}})$.

Теореми попереднього розділу можна узагальнити в такий спосіб.

Теорема 3.6.3. *Припустимо, що несуперечлива теорія $\mathfrak{T}$ рекурсивна і виражає рекурсивні функції. Тоді:*

1. *Існує замкнене речення Γ теорії $\mathfrak{T}$ таке, що ані Γ, ані $\neg\Gamma$ не є теоремами цієї теорії.*
2. *Множина номерів теорем теорії $\mathfrak{T}$ є перераховною, але не рекурсивною.*
3. *Множина істинних речень теорії $\mathfrak{T}$ не є перераховною.*

4. *Існує речення* $\mathrm{Cor}_{\mathfrak{T}}$ *теорії* $\mathfrak{T}$*, яке виражає її несуперечливість, але воно не може бути виведене в теорії* $\mathfrak{T}$*.*

Доведення відповідних пунктів цієї теореми майже дослівно повторює доведення теорем 3.5.1, 3.5.3, 3.5.4 та 3.5.5. Тому ми не наводимо його. Дуже корисною вправою, яка дозволить перевірити, чи дійсно читач зрозумів згадані результати, є самостійне доведення теореми 3.6.3.

Отже, результати про неповноту та нерозв'язність насправді не залежать від того, в який конкретно спосіб ми формалізували арифметику. Вони застосовні до будь-якої ефективної формалізації. Звичайно, ці результати не виключають, що деяка *нерекурсивна* теорія може виявитись *повною*, тобто такою, з якої виводяться всі теореми (вірні речення) арифметики. Утім якщо теорія нерекурсивна, тобто ми не маємо способу ефективно вирішити, чи є якесь речення її постулатом, то ми фактично не одержуємо ніякої переваги перед тривіальною (і напевне повною) «формалізацією», коли ми оголошуємо якесь речення таким, що належить до теорії, якщо воно істинне у стандартній моделі. В обох випадках питання про вірність кожного конкретного речення (навіть про його належність до постулатів) перетворюється на окрему математичну (не чисто логічну!) проблему, розв'язання якої вимагає спеціального дослідження. Тому надалі ми будемо розглядати лише рекурсивні теорії (хоча й будемо явно формулювати умову рекурсивності).

3.6.2. Система Робінсона

Означення 3.6.4. *Системою Робінсона* $\mathfrak{R}$ назвемо теорію першого порядку з рівністю, яка складається з постулатів рівності, постулатів (N1)–(N6) з означення 3.1.1 та наступних трьох постулатів:[3]

(C) $\quad \mathrm{v} + \mathrm{v}_1 = \mathrm{v}_1 + \mathrm{v},$

(N7*) $\quad \mathrm{v} \neq 0 \Rightarrow \exists \mathrm{v}_1\ \mathrm{v} = \mathrm{v}_1 + 1,$

(R) $\quad \mathrm{v} = \mathrm{v}_1\mathrm{v}_2 + \mathrm{v}_3 \wedge \mathrm{v}_3 < \mathrm{v}_1 \wedge \mathrm{v} = \mathrm{v}_1\mathrm{v}_4 + \mathrm{v}_5 \wedge \mathrm{v}_5 < \mathrm{v}_1 \Rightarrow \mathrm{v}_3 = \mathrm{v}_5$ (єдиність залишка).

Тут, як і раніше, ми пишемо $a \leqslant b$ замість $\exists \mathrm{v}\, a + \mathrm{v} = b$ і $a < b$ замість $a \neq b \wedge a \leqslant b$.

Зауважимо, що система Робінсона має лише скінченну кількість постулатів, на відміну від формальної арифметики, яка містить нескінченну кількість постулатів індукції (вигляду (N7)). Насправді ця теорія набагато слабша за формальну арифметику. Проте вона виражає арифметику в розумінні означення 3.6.1(1) (ми залишаємо перевірку цього читачу). Крім того, оскільки всі речення із системи Робінсона є теоремами формальної арифметики, з припущення про стандартну модель випливає, що вона несуперечлива.

Твердження 3.6.5. *Система Робінсона виражає рекурсивні функції.*

[3]Наш варіант відрізняється як від оригінальної системи самого Робінсона, так і від тієї, яка запропонована в [**Мен**, гл. 3, § 6], в основному за рахунок того, що ми знову притримуємося «кількісного» підходу замість «порядкового».

Доведення. Перш за все, за допомогою постулатів (N2), (N4) та (N7*) нескладно довести, що $\mathfrak{R} \vdash \mathrm{x} \leqslant \mathrm{y}+1 \Rightarrow \mathrm{x} \leqslant \mathrm{y} \vee \mathrm{x} = \mathrm{y}+1$. Звідси для кожного натурального числа n виводиться, що

$$\mathfrak{R} \vdash \mathrm{v} \leqslant \overline{\mathrm{n}} \Rightarrow \mathrm{v} = 0 \vee \mathrm{v} = 1 \vee \ldots \mathrm{v} = \overline{\mathrm{n}}$$

і також $\mathfrak{R} \vdash \mathrm{x} \leqslant \overline{\mathrm{n}} \vee \overline{\mathrm{n}} < \mathrm{x}$ (зробіть це; доведеться використати й постулат (C)). Крім того, функція Ґеделя $\beta(x, y, z)$ правильно визначається в теорії $\mathfrak{R}$ тим самим реченням, що й у формальній арифметиці (перевірте це; саме тут потрібен і постулат (R)).

Тепер так само, як при доведенні теореми 3.3.2, доводиться, що коли функція f отримується рекурсією чи міні-обертанням з функцій, які правильно визначаються в теорії $\mathfrak{R}$, сама функція f також правильно визначається в теорії $\mathfrak{R}$ (перевірте це). Оскільки функції O, S та проектори p_k^n правильно визначаються в теорії $\mathfrak{R}$ (тими самими реченнями, що й у формальній арифметиці), звідси випливає твердження 3.6.5 $\square$

Наслідок 3.6.6.

1. *Множина теорем теорії $\mathfrak{R}$ перераховна, але не рекурсивна.*
2. *Множина істинних речень теорії $\mathfrak{R}$ неперераховна.*
3. *Існує речення $\mathrm{Cor}_{\mathfrak{R}}$ теорії $\mathfrak{R}$, яке виражає її несуперечливість, але воно не може бути виведене в $\mathfrak{R}$.*

Вправа 3.6.7.

1. Покажіть, що теорія, яка відрізняється від системи Робінсона тим, що постулат (C) замінено двома:

(N3*) $$0 + \mathrm{v} = \mathrm{v},$$

(N4*) $$(\mathrm{v}+1) + \mathrm{v}_1 = (\mathrm{v} + \mathrm{v}_1) + 1,$$

   також виражає рекурсивні функції.
   Вказівка: Покажіть, що з цієї теорії виводиться $\mathrm{x} + \overline{\mathrm{n}} = \overline{\mathrm{n}} + \mathrm{x}$ для кожного натурального n.
2. Позначимо $\mathbb{M}$ множину, яка складається з многочленів з цілими коефіцієнтами та додатним старшим коефіцієнтом і нульового многочлена. Перевірте, що $\mathbb{M}$ зі звичайними додаванням та множенням многочленів є моделлю теорії $\mathfrak{R}$, але не є моделлю формальної арифметики. Отже, система Робінсона дійсно слабша за формальну арифметику.

Насправді, як показав Рилль-Нардзієвський, не існує теорії зі скінченним числом постулатів, яка була б рівносильна формальній арифметиці в тому розумінні, що з них виводяться ті самі речення.

3.6.3. Неповнота та нерозв'язність теорій

Основна роль системи Робінсона полягає в тому, що за її допомогою можна розповсюдити теорему 3.6.3 на теорії, які, можливо, не виражають арифметику, але *сумісні* з нею. Спочатку дамо відповідні означення.

Означення 3.6.8. Нехай $\mathfrak{T}$ — деяка теорія першого порядку. Будемо казати, що ця теорія *розв'язна*, якщо множина номерів її теорем рекурсивна.

Зробимо перш за все важливе зауваження.

Лема 3.6.9. *Якщо рекурсивна несуперечлива теорія $\mathfrak{T}$ є повною, вона розв'язна.*

Доведення. Якщо теорія $\mathfrak{T}$ рекурсивна, відношення $\mathrm{Ded}(x,y)$: «y — номер виводу замкненого речення з номером x» рекурсивне (перевірте). Припусимо, що теорія $\mathfrak{T}$ повна. Позначимо $\mathrm{Neg}(x)$ функцію, значення якої — номер заперечення речення з номером x. Очевидно, ця функція рекурсивна. Нехай тепер

$$g(x) = \mu_y\big(\,\mathrm{Ded}(x,y)\,\mathrm{Ded}(\mathrm{Neg}(x),y)\big);$$

$$f(x) = \begin{cases} 0 & \text{якщо } \mathrm{Ded}(x,g(x)) = 1, \\ 1 & \text{якщо } \mathrm{Ded}(x,g(x)) = 0. \end{cases}$$

$f(x) = 0$ тоді й лише тоді, коли x — номер замкненого речення, яке є теоремою теорії $\mathfrak{T}$ (чому?); отже, ця теорія розв'язна □

Означення 3.6.10. Нехай кожен предикат і кожен функціонал теорії $\mathfrak{T}_1$ є також предикатом або функціоналом теорії $\mathfrak{T}_2$. Кажуть, що теорія $\mathfrak{T}_2$ *сумісна з теорією* $\mathfrak{T}_1$, якщо теорія $\mathfrak{T}_1 \cup \mathfrak{T}_2$ сумісна (або, що те саме, несуперечлива).

Лема 3.6.11. *Припустимо, що теорія $\mathfrak{T}_1$ містить лише скінченну кількість речень, а теорія $\mathfrak{T}_2$ сумісна з $\mathfrak{T}_1$. Якщо теорія $\mathfrak{T} = \mathfrak{T}_1 \cup \mathfrak{T}_2$ нерозв'язна, такою є й теорія $\mathfrak{T}_2$.*

Доведення. Нехай $\mathfrak{T}_1 = \{\,\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_m\,\}$. За теоремою дедукції, $\mathfrak{T} \vdash \mathbf{A}$ тоді й лише тоді, коли $\mathfrak{T}_2 \vdash \mathbf{A}_1 \Rightarrow (\mathbf{A}_2 \Rightarrow \ldots \Rightarrow (\mathbf{A}_m \Rightarrow \mathbf{A})\ldots)$. Тому, якби теорія $\mathfrak{T}_2$ була розв'язною, такою була б і теорія $\mathfrak{T}$ (поясніть, чому) □

Наслідок 3.6.12. *Якщо теорія $\mathfrak{T}$ сумісна із системою Робінсона, вона нерозв'язна. Якщо, крім того, ця теорія рекурсивна, вона неповна.*

Доведення. Теорія $\mathfrak{R}$, а тому й теорія $\mathfrak{T} \cup \mathfrak{R}$ виражає рекурсивні функції. Тому вона нерозв'язна. Оскільки теорія $\mathfrak{R}$ містить лише скінченну кількість речень, теорія $\mathfrak{T}$ також нерозв'язна □

3.6.4. Нерозв'язність числення відношень

Тепер ми можемо довести теорему Черча про нерозв'язність логіки відношень.

Теорема 3.6.13. *Логіка відношень (і чиста логіка відношень) є нерозв'язною.*

Доведення. Очевидно, логіка відношень — теорія з порожньою множиною постулатів — сумісна із системою Робінсона (вона сумісна з будь-якою несуперечливою теорією). За наслідками 3.6.6 і 3.6.12 вона нерозв'язна.

Для того, щоб охопити чисту логіку відношень, можна перебудувати систему Робінсона, замінивши в ній функціонали $0, 1, S(\mathrm{x}, \mathrm{y}), P(\mathrm{x}, \mathrm{y})$ предикатами, відповідно, $\mathbf{O}(\mathrm{x}), \mathbf{E}(\mathrm{x}), \mathbf{S}(\mathrm{x}, \mathrm{y}, \mathrm{z}), \mathbf{P}(\mathrm{x}, \mathrm{y}, \mathrm{z})$, додавши постулати

$$\mathbf{O}(\mathrm{x}) \wedge \mathbf{O}(\mathrm{y}) \Rightarrow \mathrm{x} = \mathrm{y},$$
$$\mathbf{E}(\mathrm{x}) \wedge \mathbf{E}(\mathrm{y}) \Rightarrow \mathrm{x} = \mathrm{y},$$
$$\mathbf{S}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \wedge \mathbf{S}(\mathrm{x}, \mathrm{y}, \mathrm{z}_1) \Rightarrow \mathrm{z} = \mathrm{z}_1,$$
$$\mathbf{P}(\mathrm{x}, \mathrm{y}, \mathrm{z}) \wedge \mathbf{P}(\mathrm{x}, \mathrm{y}, \mathrm{z}_1) \Rightarrow \mathrm{z} = \mathrm{z}_1$$

і відповідно модифікувавши постулати теорії $\mathfrak{R}$. Ми залишаємо читачу цю очевидну модифікацію. Одержана теорія $\widetilde{\mathfrak{R}}$, як і теорія Робінсона, виражає рекурсивні функції і має лише скінченну кількість речень. Тому для неї зберігається наслідок 3.6.6, а для сумісних з нею теорій — наслідок 3.6.12. Залишається зауважити, що чиста логіка відношень, очевидно, сумісна з теорією $\widetilde{\mathfrak{R}}$ □

3.6.5. Теза Черча

При означенні розв'язності ми виходили з поняття рекурсивної (або, що те саме, арифметичної) функції. При цьому ми виходили з того, що рекурсивні функції — це ті, які можна «ефективно», або «алгоритмічно» обчислити. Однак поняття ефективної обчислюваності чи алгоритму не є точно визначеним. Тому виникає проблема (мабуть, не суто математична): чи не можна знайти іншого його означення, при якому ефективно обчислюваними стали б деякі нові функції. Протягом XX ст. було кілька спроб дати таке означення; тут можна назвати імена Т'юрінга, Поста, Черча, Маркова, Ербрана та інших. Утім, усі ці означення виявились рівносильними в тому розумінні, що результуючий клас «ефективно обчислюваних» функцій збігався з класом рекурсивних функцій. З деякими прикладами можна ознайомитись за книгами [**Мал2**, гл. V,VI] та [**Мен**, гл. 5]. Виходячи з цих (і деяких інших) міркувань, Черч висунув тезу, що інтуїтивне поняття ефективної обчислюваності насправді збігається з поняттям рекурсивності. Звісно, теза Черча не є математичним твердженням. Тому її неможливо «математично» довести. Звичайно, весь попередній досвід свідчить на її користь, але, як казав Єсенін-Вольпін: «Те, що в результаті всі одержали одне й те саме, може з тим же успіхом свідчити, що всі зазнали тієї самої невдачі». Утім переважна більшість фахівців вважає, що теза Черча має вельми серйозні підстави і її можна прийняти при дослідженнях, пов'язаних з алгоритмами та ефективністю.

Зробимо ще одне істотне зауваження. Означення рекурсивної функції, яке ми дали в розділі 3.3, *не є ефективним*. Дійсно, застосування мініобертання (μ-операції) передбачає, що ми вже знаємо, що рівняння $g(\mathbf{x}, y) = 0$ має розв'язок при довільному (фіксованому) x. Однак можна показати, що не існує алгоритма, який би за кожною рекурсивною (або, що те саме, арифметичною) функцією $f(\mathbf{x})$ визначав, чи

існує розв'язок рівняння $f(\mathbf{x}) = 0$. Тому, взагалі кажучи, неможливо ефективно з'ясувати, чи придатна якась функція до міні\-обертання. Насправді, у світлі тези Черча, нічого несподіваного тут немає: *поняття алгоритмічності не може бути алгоритмічним*. Дійсно, припустимо, що існує ефективне означення алгоритмів, скажімо таких, які обчислюють функції від однієї змінної. Звичайно, усі можливі ефективні конструкції можна перерахувати; зокрема, тоді множину ефективно обчислюваних функцій $\mathcal{A}$ можна було б ефективно занумерувати: $\mathcal{A} = \{ A_1, A_2, \ldots, A_n, \ldots \}$. Можливо, цей перелік містить повторення, але важливо, що він містить усі ефективно обчислювані функції. Розглянемо тоді функцію $B(n) = A_n(n) + 1$. Очевидно, вона ефективно задана: її значення алгоритмічно обчислюється для кожного n. З іншого боку, вона не збігається з жодною з функцій A_n: $B(n) \neq A_n(n)$. Фактично ми тут використали діагональний прийом Кантора, добре відомий з елементарної теорії множин. Отже, використання неефективних конструкцій в означенні всіх «ефективно обчислюваних» функцій є неминучим. Звісно, наші розгляди тут були аж надто неформальними, але, по-перше, така неформальність теж неминуча, оскільки саме поняття ефективної обчислюваності є неформальним. По-друге ж, ми сподіваємося, що читач, який розібрався в теоремах неповноти в тому вигляді, як вони подані в цій книзі, буде в змозі сам перекласти ці розгляди на формальну мову в будь-якій ситуації, коли йому запропонують якусь формалізацію поняття алгоритму.

Бібліоґрафія

Бу. Н. Бурбаки. *Очерки по истории математики.* ИЛ, 1963.
Дев. М. Девис. *Прикладной нестандартный анализ.* Мир, 1980.
ЕП. Ю. Л. Ершов и Е. А. Палютин. *Математическая логика.* Наука, 1987.
Кл1. С. К. Клини. *Математическая логика.* Мир, 1973.
Кл2. С. К. Клини. *Введение в метаматематику.* ИЛ, 1957.
Ко. П. Дж. Коэн. *Теория множеств и континуум-гипотеза.* Мир, 1969.
Мал1. А. И. Мальцев. *Алгоритмы и рекурсивные функции.* Наука, 1965.
Мал2. А. И. Мальцев. *Алгебраические системы.* Наука, 1970.
Ман. Ю. И. Манин. *Вычислимое и невычислимое.* Советское радио, 1980.
Мен. Э. Мендельсон. *Введение в математическую логику.* Наука, 1971.
Нов. П. С. Новиков. *Элементы математической логики.* Физматгиз, 1959.
РС. Е. Расёва и Р. Сикорский. *Математика метаматематики.* Наука, 1972.
Роб. А. Робинсон. *Введение в теорию моделей и метаматематику алгебры.* Наука, 1967.
Усп. Успенский. *Нестандартный, или неархимедов, анализ.* Знание, 1983.
Ч. А. Черч. *Введение в математическую логику.* ИЛ, 1961.