Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Київський національний університет імені Тараса Шевченка
Міністерство освіти і науки України

Кваліфікаційна наукова
праця на правах рукопису

ПРОХОРЧУК ВЕРОНІКА АНАТОЛІЇВНА

УДК 512.54

ДИСЕРТАЦІЯ

АВТОМАТНІ ЗОБРАЖЕННЯ ГРУП

111 — Математика

Подається на здобуття наукового ступеня *доктора філософії*

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

___________________________ *В. А. Прохорчук*

Науковий керівник: *Олійник Андрій Степанович*
доктор фізико-математичних наук, доцент

Київ – 2022

АНОТАЦІЯ

Прохорчук В. А. Автоматні зображення груп. — Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 111 "Математика" — Київський національний університет імені Тараса Шевченка, Київ, 2022.

Дисертаційна робота присвячена побудові точних скінченно автоматних зображень ряду скінченно породжених груп. Природною необхідною умовою для груп, які допускають такі зображення, є резидуальна скінченність.

Розглядаються точні скінченно автоматні зображення для таких скінченно породжених резидуально скінченних груп, які за своєю комбінаторною структурою є близькими до вільних груп. А саме, груп, що розкладаються у вільні добутки своїх підгруп, амальгамовані вільні добутки, або є HNN-розширеннями.

Дисертація складається з анотацій українською та англійською мовами, переліку умовних позначень, вступу, чотирьох розділів основної частини, висновків, списку використаних джерел та додатку.

У вступі обґрунтовано актуальність теми дослідження, сформульовано мету, об'єкт, предмет, завдання і методи дослідження, зазначено наукову новизну отриманих результатів, їх практичне значення, зв'язок роботи з науковими темами й особистий внесок здобувача, вказано також де було апробовано та опубліковано результати дисертації.

В Розділі 1 наводяться основні означення і твердження, які будуть необхідні в наступних розділах.

Розділ 2 присвячений побудові точних зображень амальгамованих вільних добутків циклічних груп по циклічній підгрупі за допомогою скінченних автоматів над деяким скінченним алфавітом. А саме, використовуючи узагальнення леми про пінг-понг показано, що вказаний амальгамований вільний добуток породжується автоматними підстановками, визначеними ініціальними автоматами з 4 станами. Окремо розглянуто випадок тривіальної амальгамації, тобто побудовано точне зображення амальгамованого вільного добутку вказаних груп по одиничній підгрупі. В цьому випадку автомати, в яких визначаються необхідні автоматні підстановки, мають по 2 внутрішні стани.

В Розділі 3 побудовано точне зображення амальгамованих вільних добутків циклічних груп по циклічній підгрупі скінченно автоматними підстановками над мінімально можливим алфавітом. Наводиться допоміжна конструкція автоматних підстановок довільного скінченного порядку і оцінено кількість станів в автоматі, який задає вказану автоматну підстановку. Для явної побудови автоматів, в станах яких визначатимуться необхідні для доведення автоматні підстановки, використовуються операції з'єднання і послідовного з'єднання двох ініціальних автоматів, а також конструкція l-повного автомата. У випадку точного зображення амальгамованих вільних добутків скінченного числа p-груп ініціальними автоматами додатково показано, що такий амальгамований вільний добуток ізоморфно занурюється в p-$FGA(\mathsf{X})$ для алфавіту X потужності p, тобто перетин p-силовської підгрупи $Syl_p(GA(\mathsf{X}))$ групи всіх автоматних підстановок над X і групи $FGA(\mathsf{X})$ всіх скінченно автоматних підстановок. Доведення останнього твердження базується на загальній конструкції, запропонованій вище, та додатковому аналізі побудованих в ній автоматів.

В Розділі 4 розглянуто питання знаходження HNN-розширень вільних абелевих груп рангу n, $n \geq 1$, які допускають ізоморфні занурення в групу p-$FGA(\mathsf{X})$. Розглядаються такі HNN-розширення, визначені невиродженими цілочисельними матрицями M розміру $n \times n$ з певними, накладеними на них, умовами. Показано, що ці HNN-розширення вільних абелевих груп допускають ізоморфні занурення в групу p-$FGA(\mathsf{X})$. Як наслідок, отримуємо, що відповідні HNN-розширення є резидуально p-скінченними. Також наведено приклад такої матриці розміру 2×2, яка не задовольняє раніше визначеним умовам, але при цьому відповідне їй HNN-розширення занурюється в 2-$FGA(\mathsf{X})$.

У дисертаційній роботі отримано такі нові результати.

1. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою побудовано точні скінченно автоматні зображення. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, кожен з яких має 4 внутрішні стани.

2. Побудовано точні скінченно автоматні зображення вільних добутків скінченних циклічних груп. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, які мають по 2 внутрішні стани.

3. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою, побудовано точні скінченно автоматні зображення над мінімально можливим алфавітом.

4. Для довільного простого числа p доведено, що амальгамовані вільні добутки скінченного числа циклічних p-груп, амальгамованих за циклічною підгрупою, зображаються скінченними автоматами спеціального вигляду. Показано, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

5. Введено клас HNN-розширень вільних абелевих груп скінченного рангу, всі групи з якого зображаються скінченно автоматними підстановками. Доведено, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

Дисертаційне дослідження носить теоретичний характер. Отримані результати можуть бути використані в алгебрі, теорії автоматів, дискретній математиці, теорії алгоритмів та в інших галузях знань, методи яких базуються на автоматних зображення алгебраїчних структур.

Ключові слова: автоматна підстановка, автоморфізм кореневого дерева, амальгамований вільний добуток, вільний добуток, група автомата, ініціальний автомат, кореневе дерево, резидуально скінченна група, скінченний автомат, HNN-розширення, p-силовська підгрупа.

ABSTRACT

Prokhorchuk V. A. Automaton representations of groups. – Qualifying scientific work on the rights of the manuscript.

The thesis presented for the academic degree Doctor of Philosophy in specialty 111 "Mathematics". — Taras Shevchenko National University of Kyiv, Kyiv, 2022.

The thesis is devoted to the study of faithful finite automaton representations of finitely generated groups. Residual finiteness is a natural necessary condition for groups that allow such representations.

Faithful finite automaton representations of finitely generated residually finite groups, which are close to free groups in their combinatorial structure, are considered. More precisely, it is considered groups that decompose into free products or amalgamated free products of their subgroups, and HNN extensions of groups.

The thesis consists of an abstract in Ukrainian and English, a list of symbols, an introduction, four chapters of the main part, conclusions, a references list and an appendix.

The introduction contains motivation of the research topic, formulates the purpose, object, subject, tasks and methods of research, indicates the scientific novelty of the obtained results, their practical significance, the connection of the work with scientific programs and personal contribution of the applicant. Also it is indicated where the results have been discussed and published.

Chapter 1 provides the main definitions and statements which are used in the next chapters of the thesis.

Chapter 2 is devoted to the construction of faithful representations of amalgamated free products of finite cyclic groups with cyclic subgroup amalgamated by finite automata over some finite alphabet. Namely, using a generalization of the ping-pong lemma, it is shown that the specified amalgamated free product is

generated by automaton permutations defined by initial automata with 4 states. The case of trivial amalgamation is considered separately, i.e. a faithful representation of the free product of finite cyclic groups is constructed. In this case, the automata in which the necessary automaton permutations are defined have 2 internal states.

In Chapter 3 a faithful representation of amalgamated free products of cyclic groups with cyclic subgroup amalgamated by finite automaton permutations over the minimal possible alphabet is constructed. The auxiliary construction of automaton permutations with arbitrary finite order is given and the number of states in the automaton that define the specified automaton permutation is estimated. For the explicit construction of automata, in the states of which the automaton permutations required for the proof will be determined, the operations of linking and serial linking of two initial automata are used, as well as the construction of an l-complete automaton. In the case of faithful representations of amalgamated free products of finite number of cyclic p-groups by initial automata, it is additionally shown that such an amalgamated free product is isomorphically embedded in the group $p\text{-}FGA(\mathsf{X})$ over an alphabet X of cardinality p, i.e. the intersection of the p-Sylow subgroup $Syl_p(GA(\mathsf{X}))$ of the group of all automaton permutations over X and the group $FGA(\mathsf{X})$ of all finite automaton permutations over X. The proof of the last statement is based on the general construction proposed above, and on additional analysis of the automaton constructed in it.

Chapter 4 considers the question of finding HNN extensions of free abelian groups of rank n, $n \geq 1$, which allow isomorphic embedding into the group $p\text{-}FGA(\mathsf{X})$. It is introduced HNN extensions defined by invertible integer matrices M of size $n \times n$ with some additional conditions. It is shown that these HNN extensions of free abelian groups allow isomorphic embedding in the group $p\text{-}FGA(\mathsf{X})$. As a result, it is obtained that the corresponding HNN extensions are residually p-finite. It is presented an example of a matrix of size 2×2, such that it does not satisfy the previously defined conditions, but corresponding HNN extension allow an embedding into $2\text{-}FGA(\mathsf{X})$.

The main results that determine the scientific novelty of the thesis are as follows.

1. Faithful finite automaton representations are constructed for amalgamated free products of finite number of finite cyclic groups with amalgamated cyclic subgroup. The automaton permutations that generate corresponding products are defined by initial automata, each of which has 4 internal states.

2. Faithful finite automaton representations of free products of finite cyclic groups are constructed. The automaton permutations that generate corresponding products are defined by initial automata, each of which has 2 internal states.

3. For amalgamated free products of finite number of finite cyclic groups with amalgamated cyclic subgroup, faithful finite automaton representation are constructed over a minimal possible alphabet.

4. For arbitrary prime number p it is proved that amalgamated free products of finite number of cyclic p-groups with amalgamated cyclic subgroup are represented by finite automata of special form. It is shown that corresponding automaton permutations belong to the p-Sylow subgroup of the group of all automaton permutations over the alphabet with p elements.

5. A class of HNN extensions of free abelian groups of finite rank is introduced. All groups from this class are represented by finite automaton permutations. It is proved that corresponding automaton permutations belong to the p-Sylow

subgroup of the group of all automaton permutations over the alphabet with p elements.

The thesis is a theoretical research. The obtained results can be used in algebra, automata theory, discrete mathematics, algorithm theory and other fields of knowledge, the methods of which are based on automaton representations of algebraic structures.

Keywords: automaton permutation, automorphism of rooted tree, amalgamated free product, free product, automaton group, initial automaton, rooted tree, residually finite group, finite automaton, HNN extension, p-Sylow subgroup.

Список публікацій за темою дисертації

1. В. А. Прохорчук. Зображення проективних спеціальних лінійних груп скінченно автоматними підстановками // Четверта всеукраїнська наукова конференція молодих вчених з математики та фізики, 23–25 квітня 2015 р., м. Київ, Україна: Матеріали конференції – 2015. – С. 65.

2. В. А. Прохорчук. Скінченно автоматне зображення групи $GL(2, \mathbb{Z})$ // International mathematical conference "Groups and Actions: Geometry and Dynamics" dedicated to the memory of professor Vitaly Sushchanskyy, December 19–22, 2016. // Taras Shevchenko National University of Kyiv – 2016. – С. 69.

3. В. А. Прохорчук. Скінченно автоматне зображення групи $GL(3, \mathbb{Z})$ // Матеріали XV Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених "Шевченківська весна – 2017". – 2017. – С. 73–75.

4. В. А. Прохорчук. Декомпозиція автоматів і елементарні матриці // Шоста всеукраїнська наукова конференція молодих вчених з математики та фізики, 21–22 квітня 2017 р., м. Київ, Україна: Матеріали конференції // Національний університет "Києво-Могилянська академія" – 2017. – С. 67.

5. В. А. Прохорчук. Моделювання дії автоматів на базі представлення матриць // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених "Теоретичні та прикладні проблеми фізики, математики та інформатики", 25–27 травня 2017 р., м. Київ, Україна: Матеріали конференції // Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Фізико-

технічний інститут – КПІ ім. Ігоря Сікорського Видавництво "Політехніка" – 2017. – Том II – С. 62–64.

6. Prokhorchuk V. A. Automata that generate metabelian groups // 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V.V. Kirichenko, July 3–7, 2017, Kyiv, Ukraine: Book of Abstracts // Institute of Mathematics of NAS of Ukraine, 2017 – P. 106.

7. В. А. Прохорчук. Скінченно-автоматні розширення групи Баумслага-Солітера // Міжнародна наукова конференція "Сучасні проблеми механіки та математики" присвячена 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р., м. Львів, Україна: Матеріали конференції – Львів – 2018. – Том III – С. 229.
Режим доступу до ресурсу: www.http://www.iapmm.lviv.ua/mpmm2018.

8. Prokhorchuk V. A. Amalgamated free products of finite cyclic groups and finite automata // The conference dedicated to the 60th anniversary of the algebra department of Kyiv University, July 14–17, 2020, Kyiv, Ukraine: Book of Abstracts // Taras Shevchenko National University of Kyiv – 2020. – P. 67. https://sites.google.com/view/kyiv-algebra60

9. Prokhorchuk V. Finite state automaton actions of HNN extensions of free abelian groups // The 13th International Algebraic Conference in Ukraine, July 6–9, 2021, Kyiv, Ukraine: Book of Abstracts // Taras Shevchenko National University of Kyiv – 2021. – P. 67. https://sites.google.com/view/iacu

10. A. Oliynyk, V. Prokhorchuk. Amalgamated free product in terms of automata constructions // Communications in Algebra, Vol 50. No. 2, P. 740–750, 2022.

doi: 10.1080/00927872.2021.1967965.

11. V. Prokhorchuk. On finite state automaton actions of HNN extensions of free abelian groups // Carpathian Mathematical Publications, Vol. 13, No. 1, P. 180–188, 2021. doi: 10.15330/cmp.13.1.180-188

12. V. Prokhorchuk. Generation of amalgamated free products of cyclic groups by finite automata over minimal alphabet // Theoretical Computer Science, Vol. 856, 2021, P. 151–164, isn: 0304-3975, doi: 10.1016/j.tcs.2020.12.036.

Зміст

Перелік умовних позначень

Λ — порожнє слово

$\mathcal{A}_{q_1\,R_1}\square_{R_2}\mathcal{A}_{q_2}$ — з'єднання ініціальних автоматів $\mathcal{A}_{q_1}$ та $\mathcal{A}_{q_2}$ відносно множин стрілок R_1, R_2

$\mathsf{Aut}\,\mathcal{T}_d(\mathsf{X})$ — група автоморфізмів дерева $\mathcal{T}_d(\mathsf{X})$

$\overline{0}_n$ — слово $\underbrace{00\ldots0}_{n}$, $n > 0$

l-$\mathcal{A}_q$ — l-повний автомат ініціального автомата $\mathcal{A}_q$

$FGA(\mathsf{X})$ — група всіх скінченно автоматних підстановок над алфавітом X

$G(\mathcal{A})$ — група автомата $\mathcal{A}$

$GA(\mathsf{X})$ — група всіх автоматних підстановок над алфавітом X

$S(\mathsf{X})$ — симетрична група на множині X

$Syl_p(GA(\mathsf{X}))$ — силовська p-підгрупа групи $GA(\mathsf{X})$, де $|\mathsf{X}| = p$, p-просте

$\mathbb{N}$ — множина натуральних чисел

$\mathbb{Z}$ — кільце цілих чисел

$\mathbb{Z}_n$ — кільце лишків за модулем n

$\mathcal{T}_d(\mathsf{X})$ — d-кореневе дерево

$\mathcal{T}_{d,n}(\mathsf{X})$ — d-кореневе дерево глибини n

$\mathcal{A}_{q_1}\square\mathcal{A}_{q_2}$ — послідовне з'єднання автоматів $\mathcal{A}_{q_1}$ та $\mathcal{A}_{q_2}$

X — алфавіт

X^* — множина всіх скінченних слів над алфавітом X

X^ω — множина всіх нескінченних слів над алфавітом X

$\mathsf{X}^{(n)}$ — множина слів довжини не більшої за n над алфавітом X, $n \geq 0$

X^n — множина слів довжини n над алфавітом X; n-й рівень дерева $\mathcal{T}_d(\mathsf{X})$, $n \geq 1$

$\overline{w}$ — вектор довжини $|w|$, координати якого відповідають літерам скінченного слова w

$\varnothing$ — порожня множина

e — тривіальна підстановка; одиничний елемент групи

$id|_G$ — тотожне відображення на множині G

$p - FGA(\mathsf{X})$ — перетин груп $FGA(\mathsf{X})$ та $Syl_p(GA(\mathsf{X}))$

$w[\xi]$ — розбиття нескінченного слова w по нескінченній послідовності $\xi = \{\xi_k\}_{k\geq 0}$

$w[\xi_k]$ — розбиття скінченного слова w по скінченній послідовності $\{\xi_i\}_{i=1}^k$, $k \geq 0$

$w[i,k]$ — i-тий склад довжини k слова w

$w[i]$ — i-та літера слова w

x^σ — образ x під дією підстановки σ

$|w|$ — довжина скінченного слова w

Вступ

Теорія автоматів як окремий напрямок математичних досліджень виникла завдяки появі формальних означень понять алгоритму та алгоритмічно обчислюваних функцій та широкому впровадженню обчислювальної техніки на основі архітектури, розробленої А. Тьюрінгом ([62]) та Дж. фон Нойманом ([63]) в середині двадцятого століття. Найчастіше теорію автоматів відносять до прикладної дискретної математики, як універсальний абстрактний засіб дослідження алгоритмів, проте вона має дуже широкий спектр застосувань і тісно пов'язана з математичною логікою, алгеброю, теорію формальних мов та іншими розділами математики. Окремої уваги заслуговує так звана алгебраїчна теорія автоматів [20, 18], котра включає дослідження алгебраїчних структур, які визначаються автоматами або описуються за допомогою автоматів. В цій теорії одне з найпомітніших місць посідає теорія груп підстановок та напівгруп перетворень, визначених скінченними автоматами трансляторами над скінченними алфавітами ([24, 5]).

Важливу роль таких груп для алгебри та математики в цілому було окреслено в роботі В. М. Глушкова [21], де було спрогнозовано, що за допомогою таких автоматів вдасться знайти приклади груп бернсайдового типу, тобто нескінченних скінченно породжених періодичних груп, чим дати негативну відповідь на загальну проблему Бернсайда. Згодом С. В. Альошин ([2]), В. І. Сущанський ([61]), Р. І. Григорчук ([22]) та Н. Гупта і С. Сідкі ([28]) побудували свої приклади груп бернсайдового типу. Вони використовували різний математичний апарат для їх визначення, проте виявилося, що кожну з побудованих груп можна визначати як групу підстановок, визначених автоматами, тобто розглядати як групу автоматних підстановок. Р. І. Григорчук в фундаментальній роботі [23] показав, що серед груп автоматних підстановок існує континуум попарно неізоморфних періодичних груп проміжного між поліноміальним і експоненційним росту. Тим самим було дано позитивні відповіді на питання Мілнора про існування груп проміжного росту та питання Дея про існування аменабельних, але не елементарно аменабельних груп. Все це стало вирішальним аргументом для окремих досліджень груп автоматних підстановок та автоматних зображень груп. За їх допомогою вдалося знайти ряд інших цікавих властивостей, які природно пов'язують між собою результати з алгебри, геометрії, теорії динамічних систем, фрактального аналізу та теорії чисел. За допомогою автоматних зображень груп було знайдено відповіді на ряд відкритих задач та визначено багато нових цікавих теоретико-групових властивостей. Дослідження груп бернсайдового типу, заданих їхніми автоматними зображеннями, продовжуються ([38]) і дозволяють будувати нові приклади груп з цікавими властивостями, наприклад, прості групи проміжного росту ([49]).

Поряд з цим, спектр груп, котрі допускають точні автоматні зображення, продовжує постійно розширюватися ([12, 4, 39, 15]). Єдиним природним обмеження на такі групи є їхня резидуальна скінченність. Серед них найбільше уваги дослідників приділялося метабелевим групам, зокрема обмеженим вінцевим добуткам абелевих груп і групам блимаючих лампочок ([25, 11, 16, 17]), та вільним групам ([3]) і вільним добуткам груп ([50]). Посилена увага саме до вільних груп пояснюється, зокрема, рядом результатів, які в топологічному ([10]) та ймовірносному ([1]) значеннях доводили, що більшість скінченно породжених груп, визначених автоматами, є вільними. Явні точні автоматні зображення таких груп, зокрема самоподібні ([48]), є предметом дослідженя цілого ряду статей протягом останніх десятиліть ([14, 64, 27, 40, 65, 57, 59, 19]).

Як групи, що багаті вільними підгрупами, вільні добутки скінченних груп є природним класом для досліджень їх скінченно автоматних зображень. Разом з тим, точні скінченно автоматні зображення резидуально скінченних груп, що характеризуються спорідненими конструкціями, а саме амальгамованих добутків груп та HNN-розширень груп, на даний час досліджені мало. Відомі точні скінченно автоматні зображення амальгамованих добутків нескінченних циклічних груп ([52]) та самоподібні скінченно автоматні зображення певних HNN-розширень вільних абелевих груп скінченного рангу ([6]). Разом з тим, відкритим залишається питання про існування точних скінченно автоматних зображень резидуально p-скінченних амальгамованих вільних добутків чи HNN-розширень, які б належали природно визначеним силовським p-підгрупам відповідних груп автоматних підстановок.

Обґрунтування вибору теми дослідження. Таким чином, одним з важливих напрямків досліджень груп, визначених автоматами, є питання про те, які саме резидуально скінченні групи можуть бути породжені автоматними підстановками над скінченним алфавітом. Це питання також можна розглядати, коли зафіксовано алфавіт певної потужності. Зокрема, коли потужність алфавіту є простим числом p, то природно виникає питання про існування точних автоматних зображень для резидуально p-скінченних груп, які належали б силовській p-підгрупі групи всіх автоматних підстановок над цим алфавітом. В даній дисертаційній роботі досліджуються питання про існування точних скінченно автоматних зображень вказаних типів для амальгамованих вільних добутків скінченних циклічних груп та HNN-розширень вільних абелевих груп скінченного рангу. Зокрема досліджується питання мінімізації потужності алафіту, над яким задана резидуально скінченна група допускає точні скінченно автоматні зображення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконане відповідно до індивідуального плану аспірантки кафедри алгебри і комп'ютерної математики Київського національного університету імені Тараса Шевченка, затвердженого вченою радою механіко-математичного факультету, та у межах державної бюджетної науково-дослідної теми "Застосування алгебро-геометричних методів у теоріях груп, напівгруп, кілець, зображень до задач прикладної алгебри та захисту інформації" (номер державної реєстрації 0111U005264) Київського національного університету імені Тараса Шевченка.

Мета і завдання дослідження. Конструктивна побудова нових точних зображень груп автоматними підстановками, визначених в ініціальних станах скінченних автоматів над скінченними алфавітами.

Об'єкт дослідження. Скінченні автомати і скінченно автоматні підстановки, резидуально скінченні скінченно породжені амальгамовані вільні добутки груп та HNN-розширення груп.

Предмет дослідження. Визначення необхідних і достатніх умов, за яких ті чи інші резидуально скінченні групи допускають точні скінченно автоматні зображення. Явні конструкції точних скінченно автоматних зображень резидуально скінченних груп.

Методи дослідження. У роботі застосовуються методи комбінаторної теорії груп, теорії груп підстановок, теорії скінченних автоматів та методи лінійної алгебри.

Наукова новизна отриманих результатів.

В дисертації автором отримано такі нові результати.

1. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою побудовано точні скінченно автоматні зображення. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, кожен з яких має 4 внутрішні стани.

2. Побудовано точні скінченно автоматні зображення вільних добутків скінченних циклічних груп. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, які мають по 2 внутрішні стани.

3. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою, побудовано точні скінченно автоматні зображення над мінімально можливим алфавітом.

4. Для довільного простого числа p доведено, що амальгамовані вільні добутки скінченного числа циклічних p-груп, амальгамованих за циклічною підгрупою, зображаються скінченними автоматами спеціального вигляду. Показано, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

5. Введено клас HNN-розширень вільних абелевих груп скінченного рангу, всі групи з якого зображаються скінченно автоматними підстановками. Доведено, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

Теоретичне та практичне значення отриманих результатів. Дисертаційна робота має теоретичний характер. Викладені в роботі методи та отримані результати можуть бути використані в подальших дослідженнях з теорії груп автоматних підстановок та при побудові нових зображень груп автоматами. Також запропоновані в дисертаційному дослідженні автомати можуть мати практичні застосування при розробці програмного забезпечення для обчислень зі скінченно породженими групами.

Особистий внесок здобувача. Всі основні результати дисертаційної роботи отримані здобувачем самостійно. Вони опубліковані в трьох статтях, дві з яких опубліковано здобувачем без співавторів. В єдиній спільній роботі внески співавторів є рівними.

Апробація матеріалів дисертації. Результати дисертації доповідалися та обговорювалися на наукових конференціях та засіданнях наукових семінарів провідних українських та міжнародних наукових установ.

Конференції:

1. Четверта всеукраїнської наукової конференції молодих вчених з математики та фізики, Київ, 23–25 квітня 2015.

2. International mathematical conference Groups and Actions: Geometry and Dynamics, dedicated to the memory of professor Vitaly Sushchanskyy, Kyiv, December 19–22, 2016.

3. XV міжнародна науково-практична конференція студентів, аспірантів та молодих науковців "Шевченківська весна", Київ, 4–6 квітня 2017.

4. Шоста всеукраїнська наукова конференція молодих вчених з математики та фізики, Київ, 21–22 квітня 2017.

5. XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених "Теоретичні і прикладні проблеми фізики, математики та інформатики", Київ, 25–27 травня 2017.

6. 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V.V. Kirichenko, July 3–7, 2017, Kyiv, Ukraine.

7. Міжнародна наукова конференція "Сучасні проблеми механіки та математики" присвячена 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р., м. Львів, Україна.

8. Міжнародна наукова конференція "Rigidity", 24–28.06.2019, м. Варшава, частина Simon's Semester "Geometric and Analytic Group Theory", м. Варшава, 1 квітня - 15 липня, 2019.

9. The conference dedicated to the 60th anniversary of the algebra department of Kyiv University, July 14-–17, 2020, Kyiv, Ukraine.

10. The 13th International Algebraic Conference in Ukraine, Kyiv, July 6–9, 2021.

11. Семінар з теорії груп та напівгруп Київського національного університету імені Тараса Шевченка (м. Київ, 2016 р., 2020 р. та 2021 р.).

12. Алгебраїчний семінар Київського національного університету імені Тараса Шевченка (м. Київ, 2022 р.).

Публікації. Основні результати дисертаційного дослідження опубліковано в 3 статтях [51, 55, 54], що є науковими виданнями, які входять до переліку фахових видань МОН України і входять до наукометричної бази даних Scopus у журналах, які належать до Q2 Scimago Journal&Country Rank.

Структура та обсяг дисертації.

Дисертація складається з анотацій українською та англійською мовами, переліку умовних позначень, вступу, чотирьох розділів основної частини, висновків, списку використаних джерел та додатку. Загальний зміст дисертації становить 136 сторінок, з них основний текст займає 110 сторінок, а список використаних джерел містить 66 найменувань.

Подяки. Авторка щиро вдячна своєму науковому керівнику, доктору фізико-математичних наук, професору Олійнику Андрію Степановичу за співпрацю, постійну підтримку і допомогу у роботі.

Розділ 1

Попередні відомості

1.1 Автомати та групи визначені автоматами

Нехай X — скінченна множина, яку ми називатимемо алфавітом, $|\mathsf{X}| \geq 2$.

Означення 1.1. Скінченним словом над алфавітом X називається скінченна послідовність w виду

$$x_1 x_2 \dots x_n, \quad x_i \in \mathsf{X}, 1 \leq i \leq n.$$

Довжиною скінченного слова w будемо називати число n і позначати символом $|w|$.

Порожнє слово (слово довжини 0) будемо позначати символом Λ.

Означення 1.2. Нескінченним словом над алфавітом X називається нескінченна послідовність w виду

$$x_1 x_2 \dots, \quad x_i \in \mathsf{X}, i \geq 1.$$

Множину слів над алфавітом X довжини n будемо позначати символом X^n.

Введемо позначення для множини слів довжини не більшої за n:

$$\mathsf{X}^{(n)} = \bigcup_{0 \leq i \leq n} \mathsf{X}^i, n \geq 0.$$

Позначимо множину усіх скінченних слів над X, включно з порожнім словом Λ через X^* і множину всіх нескінченних слів над X через X^ω.

На множині X^* визначимо операцію приписування слів. Для слів

$$u = u_1 u_2 \dots u_n \text{ та } v = v_1 v_2 \dots v_m$$

результатом приписування буде слово

$$uv = u_1 u_2 \dots u_n v_1 v_2 \dots v_m.$$

Має місце рівність

$$|uv| = |u| + |v|, \quad u, v \in \mathsf{X}^*.$$

Твердження 1.1. *Множина* X^* *відносно операції приписування слів є вільним моноїдом з базисом* X.

Зауважимо, що коректно визначеними є операції приписування справа нескінченного слова до скінченного, а також приписування зліченної послідовності скінченних слів, результатом кожної з яких є нескінченне слово.

Для непорожнього слова $w \in \mathsf{X}^l$ символом $w[i]$ позначатимемо i-ту літеру слова w. Тоді w можна записати у вигляді

$$w = w[1]w[2] \dots w[l].$$

Для непорожнього слова $w \in \mathsf{X}^l$ введемо позначення

$$\overline{w} = (w[1], w[2], \dots, w[l])$$

для відповідного йому вектора довжини l.

Означення 1.3. Автоматом над алфавітом X називається трійка

$$\mathcal{A} = \langle Q, \lambda, \mu \rangle$$

така, що

- Q — це непорожня множина, яку називатимемо множиною внутрішніх станів автомата $\mathcal{A}$;
- $\lambda : Q \times \mathsf{X} \to Q$ — функція переходів;
- $\mu : Q \times \mathsf{X} \to \mathsf{X}$ — функція виходів.

Означення 1.4. Автомат $\mathcal{A}$ з виділеним внутрішнім станом q_0 називається ініціальним і позначається $\mathcal{A}_{q_0}$.

Означення 1.5. Автомат називається скінченним, якщо множина його станів скінченна.

Для кожного стану $q \in Q$ автомата $\mathcal{A} = \langle Q, \lambda, \mu \rangle$ визначимо перетворення

$$\mu_q : \mathsf{X} \to \mathsf{X}$$

за допомогою рівності

$$\mu_q(x) = \mu(q, x), x \in \mathsf{X}.$$

Зауважимо, що функція виходів автомата буде однозначно визначеною, якщо в кожному стані q цього автомата визначено перетворення μ_q.

Означення 1.6. Автомат $\mathcal{A}$ називається підстановочним, якщо для кожного його стану q перетворення μ_q є підстановкою на множині X.

Діаграма Мура. Автомат $\mathcal{A} = \langle Q, \lambda, \mu \rangle$ над алфавітом X може бути графічно зображений за допомогою діаграми Мура. А саме, діаграма Мура автомата $\mathcal{A}$ — це орієнтований граф, множиною вершин якого є множина станів Q. Множина стрілок в діаграмі Мура визначена функцією переходів λ. А саме, стани q_1 та q_2 з Q з'єднані стрілкою з поміткою x тоді і лише тоді, коли

$$\lambda(q_1, x) = q_2, x \in \mathsf{X}.$$

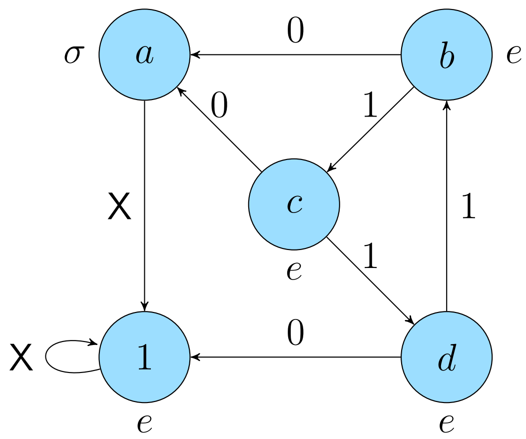


Рис. 1.1 Автомат над алфавітом $\{0, 1\}$, $\sigma = (0, 1)$.

Для спрощення позначень зображатимемо лише одну стрілку з q_1 в q_2 з поміткою $A \subset X$, якщо для $x \in \mathsf{X}$ рівність

$$\lambda(q_1, x) = q_2$$

виконується тоді й лише тоді, коли $x \in A$. Також, в діаграмі Мура кожна вершина $q \in Q$ має помітку μ_q.

Пара $(q, x) \in Q \times \mathsf{X}$ однозначно визначає орієнтоване ребро з початком в стані q і кінцем в стані $\lambda(q, x)$ з поміткою x. Тому цю пару будемо природно отожнювати з цим орієнтованим ребром і називати стрілкою. Для ініціальних автоматів ми додатково виділятимемо їхні ініціальні стани.

Для тотожного перетворення будемо використовувати позначення e. Приклад діаграми Мура автомата з множиною внутрішніх станів $\{a, d, c, d, 1\}$ над алфавітом $\mathsf{X} = \{0, 1\}$ зображено на Рис. 1.1.

Розглянемо автомат $\mathcal{A} = \langle Q, \lambda, \mu \rangle$ над алфавітом X. Функції переходів і виходів λ та μ автомата $\mathcal{A}$ можуть бути природно продовжені на множину $Q \times \mathsf{X}^*$. А саме, для довільних $x \in \mathsf{X}$, $q \in Q$, $w \in \mathsf{X}^*$ покладаємо:

$$\lambda(q, \Lambda) = q, \quad \lambda(q, xw) = \lambda(\lambda(q, x), w),$$

$$\mu(q, \Lambda) = \Lambda, \quad \mu(q, xw) = \mu(q, x)\mu(\lambda(q, x), w).$$

Таким чином, в кожному стані $q \in Q$ автомата $\mathcal{A}$ визначене перетворення на множині усіх скінченних слів X^*. Це перетворення називається перетворенням визначеним автоматом $\mathcal{A}$ в його стані q і позначається тим самим символом q.

Означення 1.7. Автоматним перетворенням над X називається таке перетворення $f : \mathsf{X}^* \to \mathsf{X}^*$, що знайдеться автомат $\mathcal{A}$ над X і стан q цього автомата, для яких перетворення f є перетворенням визначеним в цьому стані. Якщо знайдеться скінченний автомат з такою властивістю, то перетворення f називається скінченно автоматним перетворенням.

Означення 1.8. Якщо автоматне (скінченно автоматне) перетворення є бієктивним, то воно називається автоматною (скінченно автоматною) підстановкою.

Твердження 1.2. *Перетворення $f : \mathsf{X}^* \to \mathsf{X}^*$ буде автоматним тоді і лише тоді коли виконуються такі дві умови*

1. *для довільного слова $w \in \mathsf{X}^*$ виконується $|f(w)| = |w|$;*
2. *для довільних слів $w, u, v \in \mathsf{X}^*$ знайдуться слова $u_1, v_1 \in \mathsf{X}^*$ такі що*

$$f(wu) = f(w)u_1, \quad f(wv) = f(w)v_1.$$

Оскільки кожне автоматне перетворення зберігає довжини спільних префіксів слів, то воно може бути однозначно продовжено на множину X^ω. Для автомата $\mathcal{A} = \langle Q, \lambda, \mu \rangle$ над X дія автоматного перетворення $q \in Q$ на нескінченних словах може бути визначена наступним рекурсивним правилом:

$$q(xw) = x^{\mu_q} \lambda(q, x)(w),$$

де $x \in \mathsf{X}$, $w \in \mathsf{X}^\omega$ і x^{μ_q} позначає образ x під дією перетворення μ_q.

Нехай автомат $\mathcal{A}$ є підстановочним автоматом. Тоді для кожного стану q автомата $\mathcal{A}$ автоматне перетворення, визначене в q, є підстановкою як на множині X^*, так і на множині X^ω.

Позначимо символом $GA(\mathsf{X})$ множину усіх автоматних підстановок на X, а символом $FGA(\mathsf{X})$ множину всіх скінченно автоматних підстановок над цим алфавітом.

Твердження 1.3. *1. Множина $GA(\mathsf{X})$ відносно суперпозиції є групою.*

2. Множина $FGA(\mathsf{X})$ є зліченною підгрупою групи $GA(\mathsf{X})$.

Означення 1.9. Група G називається групою автоматних підстановок над алфавітом X, якщо G ізоморфна деякій підгрупі групи $GA(\mathsf{X})$.

Означення 1.10. Група називається групою автоматних підстановок, якщо вона є групою автоматних підстановок над деяким алфавітом.

Означення 1.11. Група G називається групою скінченно автоматних підстановок над алфавітом X, якщо G ізоморфна деякій підгрупі групи $FGA(\mathsf{X})$.

Означення 1.12. Група називається групою скінченно автоматних підстановок, якщо вона є групою скінченно автоматних підстановок над деяким алфавітом.

Означення 1.13. Групою підстановочного автомата $\mathcal{A}$ називається група, породжена автоматними підстановками, визначеними автоматом $\mathcal{A}$ у всіх його внутрішніх станах. Групу автомата $\mathcal{A}$ позначатимемо $G(\mathcal{A})$.

Приклад 1.1. *Група автомата зображеного на Рис. 1.1 є скінченно породженою нескінченною 2-групою, відомою як група Григорчука ([22]).*

Означення 1.14. Група G називається самоподібною, якщо вона ізоморфна групі деякого підстановочного автомата.

Кожна самоподібна група є групою автоматних підстановок. Для кожної групи G автоматних підстановок природно визначена самоподібна група, яка її містить. А саме, в якості такої групи досить розглянути групу, породжену усіма станами усіх ініціальних автоматів, які визначають деяку систему твірних групи G.

1.2 Проскінченні групи

Означення 1.15. Бінарне відношення $\leq$ на множині I називається нестрогим частковим порядком, якщо воно є

- рефлексивним (для довільного $a \in I$ $a \leq a$);
- антисиметричним (для довільних $a, b \in I$ з $a \leq b, b \leq a$ випливає $a = b$);
- транзитивним (для довільних $a, b, c \in I$ з $a \leq b, b \leq c$ випливає $a \leq c$).

Означення 1.16. Множина з нестрогим частковим порядком $(I, \leq)$ називається частково впорядкованою множиною.

Означення 1.17. Частково впорядкована множина $(I, \leq)$ називається направленою множиною, якщо для довільних $i_1, i_2 \in I$ існує $j \in I$ такий, що $i_1 \leq j$ та $i_2 \leq j$.

Приклад 1.2.

1. *Множина натуральних чисел $\mathbb{N}$ з природним нестрогим частковим порядком $\leq$ є направленою;*
2. *Множина цілих чисел $\mathbb{Z}$ з природним нестрогим частковим порядком $\leq$ є направленою;*
3. *Нехай Ω — деяка множина. Тоді відносно включення множина усіх підмножин Ω є направленою;*

4. *Визначимо нестрогий частковий порядок* $\leq$ *на множині усіх скінченних слів* X^* *над алфавітом* X*: для слів* $u, v \in X^*$ *виконується* $u \leq v$ *тоді і лише тоді, коли* v *— це префікс* u*, тобто* $u = vu_1$ *для деякого* $u_1 \in X^*$*. Тоді* $(X^*, \leq)$ *є направленою.*

Зафіксуємо деяку направлену множину індексів $(I, \leq)$. Нехай $G_i, i \in I$ — родина груп.

Означення 1.18. Проективною системою називається множина

$$\{G_i, \varphi_{ij} : i, j \in I, i \leq j\},$$

в якій $\varphi_{ij} : G_j \to G_i$ — епіморфізм груп, $i, j \in I, i \leq j$, причому виконані наступні умови:

1. для довільного $i \in I$ відображення $\varphi_{ii} = id|_{G_i}$ — тотожне;

2. для довільних $i, j, k \in I$, $i \leq j \leq k$ маємо рівність
$$\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}.$$

Означення 1.19. Граничною групою проективної системи

$$\{G_i, \varphi_{ij} : i, j \in I, i \leq j\}$$

називається підгрупа декартового добутку

$$\prod_{i \in I}^{D} G_i,$$

яка складається з усіх елементів виду $(g_i)_{i \in I}$ таких, що виконується рівність

$$g_j = \varphi_{ij}(g_i), i, j \in I, i \leq j.$$

Твердження 1.4. *Гранична група проективної системи існує і єдина з точністю до ізоморфізму.*

Граничні групи проективних систем родини груп $G_i, i \in I$ називатимемо проективними границями цієї родини груп і позначатимемо $\varprojlim G_i$.

Окремий випадок проективних систем виникає, коли маємо послідовність груп

$$G_0, G_1, G_2, \ldots$$

і сюр'єктивні гомоморфізми

$$\varphi_i : G_i \to G_{i-1}, i \geq 1.$$

Отримуємо проективну систему, коли визначимо рівності

$$\varphi_{ij} = \varphi_{i+1} \circ \ldots \circ \varphi_j, 1 \leq i < j$$

Нехай $\mathcal{F}$ — деякий клас скінченних груп.

Означення 1.20. Група G називається $\mathcal{F}$-групою, якщо $G \in \mathcal{F}$.

Означення 1.21. Група G називається про-$\mathcal{F}$ групою, якщо G є проективною границею $\mathcal{F}$-груп.

Відмітимо, що кожна $\mathcal{F}$-група є про-$\mathcal{F}$ групою. Досить взяти проективну систему з направленою множиною, що містить єдиний елемент.

Нехай p — просте число.

Означення 1.22. Група G називається p-групою, якщо порядок кожного її елемента рівний степеню числа p.

Якщо $\mathcal{F}$ — клас усіх скінченних груп, то проективні границі груп з цього класу називаються проскінченними групами. Якщо $\mathcal{F}$ — клас усіх скінченних p-груп, то проективні границі груп з цього класу називаються про-p групами.

Наведемо критерій проскінченності для топологічних груп.

Твердження 1.5. *Нехай G — топологічна група. Наступні твердження еквівалентні*

(i) G — проскінченна;

(ii) G ізоморфна (як топологічна група) замкненій підгрупі декартового добутку скінченних груп;

(iii) G — компактна і цілком незв'язна.

Означення 1.23. Клас груп $\mathcal{F}$ називається замкненим:

- відносно взяття підгруп, якщо кожна підгрупа $\mathcal{F}$-групи є $\mathcal{F}$-групою;
- відносно взяття факторгруп, якщо кожна фактор-група $\mathcal{F}$-групи є $\mathcal{F}$-групою;
- відносно взяття прямих добутків груп, якщо для груп $G_1, G_2 \in \mathcal{F}$ їх прямий добуток $G_1 \times G_2$ також належить $\mathcal{F}$.

Твердження 1.6. *Нехай $\mathcal{F}$ — клас скінченних груп, замкнений відносно взяття підгруп і прямих добутків груп і топологічна група G є про-$\mathcal{F}$ групою. Тоді для кожної відкритої нормальної підгрупи L групи G існує відкрита нормальна підгрупа N групи G, така що $N \leq L$ і $G/N \in \mathcal{F}$.*

Класи усіх скінченних груп та усіх скінченних p-груп замкнені відносно взяття підгруп, факторгруп та відносно взяття прямих добутків груп. Звідси випливає, що в проскінченних групах індекси відкритих нормальних підгруп є скінченними.

Означення 1.24. Нехай G — проскінченна група.

- Проскінченним індексом $[G : H]$ замкненої підгрупи H групи G називається найменше спільне кратне індексів відкритих підгруп групи G, що містять H.

- Проскінченним порядком $|G|$ групи G називається проскінченний індекс її одиничної підгрупи.

- Проскінченним порядком елемента $x \in G$ називається проскінченний порядок підгрупи, топологічно породженої елементом x, тобто топологічне замикання абстрактної групи, породженої елементом x.

Зауважимо, що проскінченні індекси і проскінченні порядки є супернатуральним числами ([66]).

Твердження 1.7. *Проскінченний індекс замкненої підгрупи H проскінченної групи G дорівнює найменшому спільному кратному індексів вигляду $[G : NH]$, де N — відкрита нормальна підгрупа G.*

Твердження 1.8. *Проскінченна група є про-p групою тоді і лише тоді, коли її проскінченний порядок є степенем (можливо нескінченним) числа p.*

Нехай G — скінченна група і p — просте число.

Означення 1.25. Силовською p-підгрупою групи G називається така підгрупа $Syl_p(G)$ що

1. $Syl_p(G)$ є p-групою;

2. індекс $[G : Syl_p(G)]$ взаємно простий з p.

Нехай G — проскінченна група і p — просте число.

Означення 1.26. Підгрупа P називається p-силовською підгрупою групи G, якщо порядок P є степенем (можливо нескінченним) числа p і індекс $[G : P]$ взаємно простий з p.

Твердження 1.9. *Нехай G — проскінченна група і p — просте число. Тоді мають місце наступні твердження:*

(i) в G існує p-силовська підгрупа;

(ii) якщо P — p-силовська підгрупа групи G і T — про-p підгрупа групи G, то $g^{-1}Tg \leq P$ для деякого $g \in G$;

(iii) кожна про-p підгрупа групи G міститься в її p-силовській підгрупі;

(iv) якщо P_1, P_2 — дві p-силовські підгрупи групи G, то $g^{-1}P_1g = P_2$ для деякого $g \in G$.

Таким чином, p-силовські підгрупи є максимальними про-p підгрупами проскінченної групи G, а силовська теорія для проскінченних груп узагальнює силовську теорію для скінченних груп.

1.3 Кореневі дерева та їх автоморфізми

Нехай $\mathsf{X} = \{x_0, x_1, \ldots, x_{d-1}\}$ — алфавіт потужності d, $d \geq 2$.

Множину X^* усіх скінченних слів над X можна природно ототожнити з множиною вершин d-регулярного кореневого дерева $\mathcal{T}_d(\mathsf{X})$ (див. Рис. 1.2), в якому два слова з'єднані ребром тоді і лише тоді, коли вони мають вигляд v і vx, де $v \in \mathsf{X}^*$, $x \in \mathsf{X}$. Порожнє слово Λ буде коренем цього дерева.

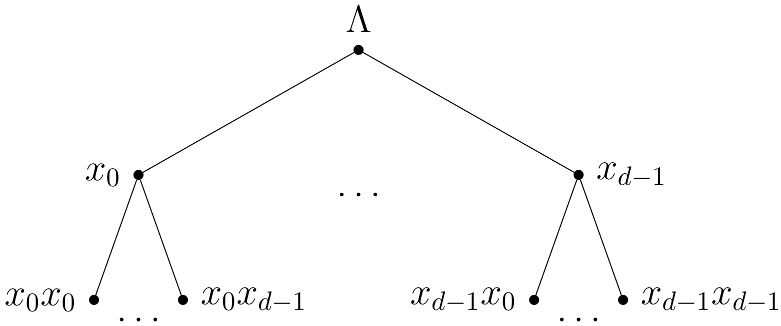


Рис. 1.2 d-регулярне кореневе дерево $\mathcal{T}_d(\mathsf{X})$

Означення 1.27. Автоморфізмом d-регулярного кореневого дерева $\mathcal{T}_d(\mathsf{X})$ називається таке бієктивне відображення $f : \mathsf{X}^* \to \mathsf{X}^*$, що довільні вершини v і vx з'єднані ребром тоді й лише тоді, коли вершини $f(v)$ і $f(vx)$ також з'єднані ребром, $v \in \mathsf{X}^*$, $x \in \mathsf{X}$.

Зауважимо, що образом кореня дерева $\mathcal{T}_d(\mathsf{X})$ під дією автоморфізму f буде він сам. Для автоморфізму f і довільної вершини $v \in \mathsf{X}^*$ розглянемо множину

$$\{vx : x \in \mathsf{X}\}.$$

Тоді образами вершин з цієї множини є вершини з множини

$$\{f(v)x : x \in \mathsf{X}\}.$$

Таким чином, однозначно визначена підстановка σ_v на множині X така, що

$$f(vx) = f(v)\sigma_v(x), \quad x \in \mathsf{X}.$$

Означення 1.28. Портретом автоморфізму f називається помічене дерево $\mathcal{T}_d(\mathsf{X})$, в якому кожна вершина $v \in \mathsf{X}^*$ має помітку σ_v.

Твердження 1.10. *Кожен автоморфізм однозначно визначається своїм портретом.*

Групу всіх автоморфізмів дерева $\mathcal{T}_d(\mathsf{X})$ будемо позначати $\mathsf{Aut}\,\mathcal{T}_d(\mathsf{X})$.

Твердження 1.11. *Група $\mathsf{Aut}\,\mathcal{T}_d(\mathsf{X})$ як група підстановок множини $\mathsf{X}^\star$ збігається з групою автоматних підстановок $GA(\mathsf{X})$.*

Множину $\mathsf{X}^n \subset \mathsf{X}^*$ будемо називати n-им рівнем дерева $\mathcal{T}_d(\mathsf{X})$, $n \geq 0$. Для кожного $n \geq 0$ розглянемо кореневе піддерево дерева $\mathcal{T}_d(\mathsf{X})$, множиною вершин якого є перші $n+1$ рівнів дерева $\mathcal{T}_d(\mathsf{X})$. Будемо його називати d-регулярним кореневим деревом глибини n і позначати $\mathcal{T}_{d,n}(\mathsf{X})$.

Для кожного $n \geq 0$ позначимо через $\mathsf{Aut}\,\mathcal{T}_{d,n}(\mathsf{X})$ групу автоморфізмів d-регулярного кореневого дерева $\mathcal{T}_{d,n}(\mathsf{X})$ глибини n. Визначимо сюр'єктивні гомоморфізми

$$\psi_n : \mathsf{Aut}\,\mathcal{T}_{d,n}(\mathsf{X}) \to \mathsf{Aut}\,\mathcal{T}_{d,n-1}(\mathsf{X}), n \geq 1.$$

А саме, під дією гомоморфізму ψ_n кожен автоморфізм $f \in \mathsf{Aut}\,\mathcal{T}_{d,n}(\mathsf{X})$ переходить у автоморфізм дерева $\mathcal{T}_{d,n-1}(\mathsf{X})$, що є звуженням автоморфізму f на це дерево. Таким чином, отримаємо проективну систему скінченних груп $\mathsf{Aut}\,\mathcal{T}_{d,n}(\mathsf{X})$ та їх гомоморфізмів ψ_n, $n \geq 1$.

Твердження 1.12. $\varprojlim \mathsf{Aut}\,\mathcal{T}_{d,n}(\mathsf{X}) \simeq GA(\mathsf{X})$.

Звідси випливає

Твердження 1.13. *Група $GA(\mathsf{X})$ є проскінченною.*

Зафіксуємо просте число p і алфавіт X потужності p.

Група $GA(\mathsf{X})$ містить силовську p-підгрупу, яку будемо позначати через $Syl_p(GA(\mathsf{X}))$. Опишемо її будову в термінах автоматних підстановок заданими автоматами спеціального вигляду.

А саме, зафіксуємо деякий цикл σ довжини p над X.

Означення 1.29. Автомат $A = \langle Q, \lambda, \mu \rangle$ над алфавітом X називається p-автоматом, якщо для довільного стану $q \in Q$ функція виходів μ для деякого $k \geq 0$ визначається рівністю

$$\mu_q = \sigma^k.$$

Твердження 1.14. *Група $Syl_p(GA(\mathsf{X}))$ складається з тих автоматних підстановок, які задаються p-автоматами над алфавітом X.*

Позначимо символом p-$FGA(\mathsf{X})$ перетин груп $Syl_p(GA(\mathsf{X}))$ і $FGA(\mathsf{X})$. Тоді маємо

Твердження 1.15. *Група p-$FGA(\mathsf{X})$ складається з тих автоматних підстановок, які задаються скінченними p-автоматами над алфавітом X.*

1.4 Резидуально скінченні групи

Означення 1.30. Група G називається резидуально скінченною, якщо для довільного неодиничного елемента $g \in G$ існує гомоморфізм φ з G в деяку скінченну групу такий, що $\varphi(g) \neq 1$.

Теорема 1.16. *Нехай G — деяка група. Тоді наступні умови еквівалентні:*

1. *G — резидуально скінченна;*
2. *для кожного неодиничного елемента $g \in G$ в групі G існує нормальна підгрупа скінченного індекса, що не містить g;*
3. *перетин усіх підгруп скінченного індекса групи G тривільний;*
4. *перетин усіх нормальних підгруп скінченного індекса групи G тривільний;*
5. *група G може бути занурена в декартів добуток сім'ї скінченних груп.*

Наведемо деякі властивості резидуально скінченних груп.

Твердження 1.17.

1. *Підгрупа резидуально скінченної групи є резидуально скінченною.*
2. *Прямий добуток резидуально скінченних груп є резидуально скінченним.*

Проте фактор група резидуально скінченної групи не обов'язково є резидуально скінченною.

Приклад 1.3.

1. *Кожна скінченна група є резидуально скінченною.*

2. Кожна скінченно породжена абелева група є резидуально скінченною.

Означення 1.31. Група називається хопфою, якщо вона не має власних факторгруп ізоморфних самій собі.

Твердження 1.18 ([42]). *Довільна скінченно породжена резидуальна скінченна група є хопфою.*

Твердження 1.19 ([8]). *Група автоморфізмів скінченно породженої резидуально скінченної групи є резидуально скінченною.*

Твердження 1.20. *Кожна проективна границя резидуально скінченних груп є резидуально скінченною групою.*

Твердження 1.21. *Кожна проскінченна група є резидуально скінченною.*

Звідси, як наслідок, маємо

Твердження 1.22. *Група $GA(\mathsf{X})$ всіх автоматних підстановок над скінченним алфавітом X є резидуально скінченною.*

Це означає, що всі групи автоматних підстановок є резидуально скінченними. Таким чином, досліджувати питання про існування точного зображення автоматними підстановками (відповідно, скінченно автоматними підстановками) має сенс лише для резидуально скінченних груп (відповідно, для зліченних резидуально скінченних груп).

Зафіксуємо просте число p.

Означення 1.32. Група G називається резидуально p-скінченною, якщо для кожного неодиничного елемента $g \in G$ існує гомоморфізм φ з G в деяку скінченну p-групу такий, що $\varphi(g) \neq 1$.

Кожна резидуально p-скінченна група є резидуально скінченною.

Теорема 1.23. *Нехай G — деяка група. Тоді наступні умови еквівалентні:*

1. *G — резидуально p-скінченна;*

2. *для кожного неодиничного елемента $g \in G$ в групі G існує нормальна підгрупа, індекс якої є степенем числа p і яка не містить g;*

3. *перетин усіх нормальних підгруп групи G, індекси яких є степенями числа p, тривільний;*

4. *група G може бути занурена в декартів добуток сім'ї скінченних p-груп.*

Наведемо деякі властивості резидуально p-скінченних груп.

Твердження 1.24. 1. *Підгрупа резидуально p-скінченної групи є резидуально p-скінченною.*

2. *Прямий добуток резидуально p-скінченних груп є резидуально p-скінченним.*

Проте, фактор група резидуально p-скінченної групи не обов'язково є резидуально p-скінченною.

Приклад 1.4. *Кожна скінченна p-група є резидуально p-скінченною.*

Твердження 1.25. *Скінченно породжена абелева група є резидуально p-скінченною тоді і тільки тоді, коли вона не містить елементів простого порядку, відмінного від p.*

Твердження 1.26. *Кожна про-p група є резидуально p-скінченною.*

Звідси, як наслідок, маємо

Твердження 1.27. *Група $Syl_p(GA(\mathsf{X}))$, де $|\mathsf{X}| = p$, є резидуально p-скінченною.*

Добре відомою є

Теорема 1.28 ([33]). *Група $Syl_p(GA(\mathsf{X}))$, де $|\mathsf{X}| = p$, містить ізоморфну копію довільної зліченної резидуально скінченної p-групи.*

Зауважимо, що знаходження явних скінченно автоматних зображень скінченно породжених резидуально скінченних p-груп є природною і важливою задачею. Зокрема, групи бернсайдового типу, побудовані в роботах [2, 61, 22, 28], природно задаються саме як групи скінченно автоматних підстановок, що належать до $Syl_p(GA(\mathsf{X}))$ ([13]).

1.5 Групи, задані твірними і співвідношеннями

Нагадаємо основні поняття комбінаторної теорії груп, які використовуються при дослідженні груп, заданих множинами твірних та визначальних співвідношень.

Означення 1.33. Група G називається вільною, якщо в ній існує така система твірних X, що для довільної групи H та для довільного відображення $\phi : \mathsf{X} \to H$ існує гомоморфізм $\Phi : G \to H$, який є продовженням ϕ, тобто $\Phi|_{\mathsf{X}} = \phi$.

Підмножина X називається базисом вільної групи.

Означення 1.34. Рангом вільної групи називається потужність її довільного базису.

Якщо ранг вільної групи є числом n, то таку вільну групу позначимо через $F_n, n \geq 1$.

Приклад 1.5. *Тривіальна група є вільною групою рангу 0, оскільки її базисом є порожня множина* $\mathsf{X} = \varnothing$.

Приклад 1.6. *Розглянемо адитивну групу цілих чисел* $G = \mathbb{Z}$.

Група G *породжується множиною* $\mathsf{X} = \{1\}$, *тобто* $\langle 1 \rangle = \mathbb{Z}$.

Зафіксуємо довільну групу H *і відображення* $\phi : \mathsf{X} \to H$ *таке, що* $\phi(1) = h \in H$. *Тоді побудуємо гомоморфізм* Φ, *який є продовженням* ϕ. *Для нього має виконуватись рівність* $\Phi(m) = h^m, m \in \mathbb{Z}$. *Можливі два випадки:*

1. *якщо* h *має* ∞ *порядок, тоді* Φ *— ізоморфізм між* $\mathbb{Z}$ *і* $\langle h \rangle$.

2. *якщо* h *має скінченний порядок* $n < +\infty$, *тоді* $\langle h \rangle \simeq \mathbb{Z}$.

   Маємо, що відображення Φ *є природним гомоморфізмом з* $\mathbb{Z}$ *на* ${}^{\mathbb{Z}}/_{n\mathbb{Z}}$.

Таким чином, адитивна група цілих чисел $\mathbb{Z}$ *є вільною групою рангу 1.*

Побудова вільної групи з базисом X Зафіксуємо непорожню множину X, який будемо називати алфавіт. Побудуємо групу, в якій X буде базисом.

Розглянемо бієктивну копію алфавіту X, яку позначатимемо X^{-1}, причому $\mathsf{X} \cap \mathsf{X}^{-1} = \varnothing$ і $\mathsf{X}^{-1} = \{x^{-1} \mid x \in \mathsf{X}\}$,

Покладемо $(x^{-1})^{-1} = x, x \in \mathsf{X}$. Тоді функція ${}^{-1} : \mathsf{X} \cap \mathsf{X}^{-1} \to \mathsf{X} \cap \mathsf{X}^{-1}$ є інволюцією.

Розглянемо Y^* — множину усіх скінченних слів над Y відносно бінарної дії приписування справа (конкатенації):

$$(z_1 \dots z_k) \cdot (u_1 \dots u_l) = z_1 \dots z_k u_1 \dots u_l.$$

Тоді одержимо моноїд Y^*.

Розглянемо в цьому моноїді конгруенцію, яка породжена усіма можливими парами виду: $(yy^{-1}, \lambda), y \in \mathsf{Y}$.

Тобто, два слова будуть еквівалентними, якщо від одного слова до другого можна перейти за скінченне число кроків, видаляючи і вставляючи пари вигляду $(yy^{-1}, \Lambda), y \in \mathsf{Y}$.

Тоді ${}^{\mathsf{Y}^*}/_{\sim}$ — вільна група рангу $|\mathsf{X}|$.

В кожному класі еквівалентності існує і єдине редуковане слово, тобто таке слово, в якому немає підслів виду $yy^{-1}, y \in \mathsf{Y}$.

Оберненим до $y_1 \dots y_k$ є $y_k^{-1} \dots y_1^{-1}$.

Тобто, ${}^{\mathsf{Y}^*}/_{\sim} \simeq F(\mathsf{X})$.

Теорема 1.29. *Група G — вільна тоді і лише тоді коли в групі G існує така система твірних X, що $G = F(\mathsf{X})$.*

Теорема 1.30. *Для будь-якої групи G існує така вільна група $F(\mathsf{X})$, що G є гомоморфізмом образу $F(\mathsf{X})$, тобто $G \simeq {}^{F(\mathsf{X})}/_{N}$, де $N \triangleleft F(\mathsf{X})$.*

Кожна група G є гомоморфним образом деякої вільної групи. Точніше, існує вільна група $F(\mathsf{X})$ та нормальна підгрупа $N \triangleleft F(\mathsf{X})$ такі, що $G \simeq {}^{F(\mathsf{X})}/_{N}$.

Припустимо, що N породжується підмножиною R, як нормальна підгрупа, тобто

$$N = \bigcap_{\substack{H \triangleleft F(\mathsf{X}) \\ H \supseteq R}} = \{w_1^{-1} r_1^{\epsilon_1} w_1 \dots w_k^{-1} r_k^{\epsilon_k} w_k \mid \epsilon_i = \pm 1, w_i \in F(\mathsf{X}), 1 \leq i \leq k, k \geq 0\}.$$

Тоді G записується множиною твірних X та співвідношень R:

$$G = \langle \mathsf{X} \mid R \rangle.$$

Означення 1.35. Групу G називають скінченно породженою, якщо існує її задання $G = \langle \mathsf{X} \mid R \rangle$, в якому X — скінченна.

Означення 1.36. Групу G називають скінченно заданою, якщо існує її задання $G = \langle \mathsf{X} \mid R \rangle$, в якому X та R — скінченні.

Приклад 1.7. $\mathbb{Z} = \langle a \mid \varnothing \rangle$, $\mathbb{Z}_n = \langle a \mid a^n \rangle$.

Твердження 1.31. *Нехай групи G_1, G_2 мають наступні задання $G_1 = \langle \mathsf{X}_1 \mid R_1 \rangle$, $G_2 = \langle \mathsf{X}_2 \mid R_2 \rangle$. Тоді*

$$G_1 \times G_2 = \langle \mathsf{X}_1 \cup \mathsf{X}_2 \mid R_1 \cup R_2 \cup \{x_1^{-1} x_2^{-1} x_1 x_2 \mid x_1 \in \mathsf{X}_1, x_2 \in \mathsf{X}_2\} \rangle.$$

Твердження 1.32 ([47], [43])**.** *Резидуально скінченна скінченно задана група має розв'язну проблему слів.*

Теорема 1.33 ([32])**.** *Кожна вільна група скінченного рангу є резидуально p-скінченною для кожного простого p.*

Теорема 1.34 ([50])**.** *Кожна вільна група скінченного рангу допускає точне скінченно автоматне зображення над бінарним алфавітом.*

1.6 Вільні добутки груп

Розглянемо групи G_1 і G_2, задані твірними та визначальними співвідношеннями. Нехай $G_1 = \langle X_1 \mid R_1 \rangle, G_2 = \langle X_2 \mid R_2 \rangle$, причому $X_1 \cap X_2 = \varnothing$.

Означення 1.37. Вільним добутком груп G_1 та G_2 називається група

$$G_1 * G_2 = \langle X_1 \cup X_2 \mid R_1 \cup R_2 \rangle.$$

Вільний добуток заданих груп визначений однозначно, з точністю до ізоморфізму, тобто має місце

Твердження 1.35. *Вільний добуток не залежить від задання початкових груп твірними і співвідношеннями.*

Означення 1.38. Кажуть, що група G розкладається в добуток своїх підгруп G_1 та G_2, якщо $G_1 * G_2 \simeq G$.

Приклад 1.8. *Вільна група пангу 2 є вільним добутком двох нескінченних циклічних груп, тобто $F_2 \simeq \mathbb{Z} * \mathbb{Z}$. Справді, нехай $F_2 = F(\{x_1, x_2\})$. Тоді*

$$F_2 = \langle x_1, x_2 \mid \varnothing \rangle \simeq \langle x_1 \mid \varnothing \rangle * \langle x_2 \mid \varnothing \rangle.$$

Нехай $G = G_1 * G_2$.

Означення 1.39. Послідовність елементів $g_1, g_2, \ldots, g_n \in G$ називається канонічною, якщо:

1. $g_i \in G_1$ або $g_i \in G_2, i \geq 1$;

2. якщо $n > 1$, то $g_i \neq e, i \geq 1$;

3. g_i та g_{i+1} належать різним групам, $i \geq 1$.

Теорема 1.36. *Кожен елемент g вільного добутку $G_1 * G_2$ однозначно подається, як добуток $g = g_1 g_2 \ldots g_n$, де $g_1, \ldots, g_n$ — канонічна послідовність.*

Аналогічно визначаються вільні добутки довільних родин груп.

Приклад 1.9. *Вільна група рангу n розкладається у вільний добуток n нескінченних циклічних груп:*

$$F_n \simeq \underbrace{\mathbb{Z} \star \ldots \star \mathbb{Z}}_{n}, n \geq 2.$$

Для елементів вільного добутку довільної родини груп аналогічно вводиться поняття канонічної послідовності і доводиться аналог Теореми 1.36 про існування та єдиність розкладу елементів як добутку членів канонічної послідовності.

Теорема 1.37 (Теорема 4.1,[26]). *Нехай G, H — резидуально скінченні групи. Тоді вільний добуток $G \star H$ є резидуально скінченною групою.*

Теорема 1.38 ([27]). *Вільний добуток скінченного числа скінченних груп є групою скінченно автоматних підстановок групою над алфавітом, потужність якого дорівнює максимальному з порядків композиційних факторів заданих груп.*

Теорема 1.39 ([19]). *Нехай G, H — групи скінченно автоматних підстановок. Тоді вільний добуток $G \star H$ також є групою скінченно автоматних підстановок.*

1.7 Амальгамовані вільні добутки груп

Нехай G_1 і G_2 — такі групи, в яких вибрано підгрупи H_1 і H_2 відповідно, які ізоморфні деякій групі H. Припустимо, що зафіксовано ізоморфізм $\varphi : H_1 \to H_2$.

Означення 1.40. Амальгамованим вільним добутком груп G_1 і G_2 (амальгамованим за підгрупою H) називається група

$$G_1 \star_H G_2 = \langle G_1, G_2 \mid \varphi(h) = h, h \in H_1 \rangle.$$

Таким чином, маємо

$$G_1 \star_H G_2 \simeq {}^{G_1 \star G_2}/_{\langle \varphi(h)h^{-1}, h \in H_1 \rangle}.$$

Зауважимо, що у випадку, коли група H є одиничною, тобто амальгамація є тривіальною, то амальгамований вільний добуток $G_1 \star_H G_2$ є вільним добутком $G_1 \star G_2$.

Означення 1.41. Зв'язною послідовністю у амальгамованому вільному добутку $G_1 \star_H G_2$, де $H_1 < G_1$, $H_2 < G_2$, $\varphi : H_1 \to H_2$ — ізоморфізм, $H \simeq H_1 \simeq H_2$ називається така послідовність $g_1 g_2 \dots g_n$, що для неї виконуються наступні умови

1. $g_i \in G_1$ або $g_i \in G_2$, $i \geq 1$;

2. якщо $n \geq 1$, то $g_i \notin H_1$ і $g_i \notin H_2$, $i \geq 1$;

3. g_i та g_{i+1} належать різним групам G_1 та G_2, $1 \leq i \leq n$;

4. якщо $n > 1$,то $g_i \neq e$, $i \geq 1$.

Теорема 1.40. *В амальгамованому вільному добутку $G_1 \star_H G_2$ для кожної зведеної послідовності добуток її членів є неодиничним елементом.*

Поняття амальгамованого вільного добутку природно узагальнюється на довільну родину груп. Нехай $G_i, i \in I$ — родина груп, H — така група, що в кожній G_i існує підгрупа H_i ізоморфна H. Для кожної пари $i, j \in I$ зафіксуємо ізоморфізм $\varphi_{ij} : H_i \to H_j$.

Означення 1.42. Амальгамованим вільним добутком груп $G_i, i \in I$ (амальгамованих за підгрупою H) називається група, задана в термінах твірних і визначальних співвідношень

$$(\star G_i)_H = \langle G_i \mid \varphi_{ij}(h) = h, h \in H_i, i.j \in I \rangle.$$

Аналогічно вводиться поняття зведеної послідовності і доводиться аналог Теореми 1.40.

Питання про резидуальну скінченність та резидуальну p-скінченність амальгамованих вільних добутків досліджувалися в ряді робіт різних авторів ([29, 35, 37, 34]).

Теорема 1.41 ([52]). *Амальгамований вільний добуток скінченного числа нескінченних циклічних груп є групою скінченно автоматних підстановок.*

1.8 HNN-розширення

Однією з центральних конструкцій комбінаторної теорії груп, є розширення Хігмана-Ноймана-Нойман, більш відоме, як HNN-розширення груп.

Нехай G — деяка група, H_1, H_2 — ізоморфні підгрупи групи G, для яких зафіксовано ізоморфізм $\varphi : H_1 \to H_2$.

Означення 1.43. HNN-розширенням групи G називається група

$$\langle G, t \mid t^{-1}ht = \varphi(h), h \in H_1 \rangle,$$

тобто

1. до твірних групи G додається єдиний елемент t,
2. до співвідношень групи G додаються такі

$$t^{-1}ht = \varphi(h), h \in H_1.$$

За допомогою цієї конструкції доведено зокрема такий класичний результат про занурення.

Теорема 1.42 ([30]). *Кожна зліченна група ізоморфна підгрупі деякої 2-породженої групи.*

Означення 1.44. Зведеною послідовністю у HNN-розширенні групи G називається послідовність

$$g_0 t^{\epsilon_1} g_1 t^{\epsilon_2} g_2 \ldots t^{\epsilon_n} g_n$$

в якій

1. $g_0, g_1, g_2, \ldots, g_n \in G$;
2. $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n \in \{1, -1\}$;

3. немає входжень виду $t^{-1}ht$, $h \in H_1$ та $t\varphi(h)t^{-1}$, $h \in H_1$;

4. немає входжень виду $t^{\varepsilon_i}et^{\varepsilon_{i+1}}$.

Теорема 1.43. *В HNN-розширенні групи G для кожної зведеної послідовності добуток її членів є неодиничним елементом.*

Нехай G — група, $H_i < G, i \in I$ — родина попарно ізоморфних між собою підгруп, $H_i \simeq H < G, i \in I$. Зафіксуємо ізоморфізми $\varphi_i : H \to H_i$, $i \in I$.

Означення 1.45. HNN-розширенням групи G називається група

$$\langle G, t_i, i \in I \mid t_i^{-1}ht_i = \varphi_i(h), h \in H, i \in I\rangle.$$

Однією з найвідоміших серій груп, кожна з яких є HNN-розширенням нескінченної циклічної групи, є серія груп Баумслага-Солітера ([9]).

Означення 1.46. Для натуральних чисел $n, m \in \mathbb{N}$ група

$$BS(n, m) = \langle a, t \mid t^{-1}a^nt = a^m\rangle,$$

називається групою Баумслага-Солітера.

Приклад 1.10. *Нехай $G = \mathbb{Z} = \langle a\rangle$. Розглянемо її ізоморфні підгрупи $H_1 = \langle a^m\rangle \simeq \mathbb{Z}$ та $H_1 = \langle a^n\rangle \simeq \mathbb{Z}$. Визначимо ізоморфізм $\varphi : H_1 \to H_2$ такий що $\varphi(a^m) = a^n$. Тоді $BS(n, m)$ – HNN-розширення $\mathbb{Z}$.*

Твердження 1.44 ([44, 46]). *Група Баумслага-Солітера $BS(m, n)$ є резидуально скінченною тоді і лише тоді, коли $|m| = 1$, $|n| = 1$ або $|m| = |n|$.*

Питання про резидуальну скінченність та резидуальну p-скінченність HNN-розширень досліджувалися в роботах [7, 45, 36].

1.9 Висновки до розділу

Цей розділ є допоміжним і не містить нових результатів.

У ньому викладено основні поняття і сформульовано твердження, які будуть використовуватися в дисертації. Зокрема, наведено необхідні означення, які стосуються автоматів та груп, ними визначених, проскінченних груп, кореневих дерев та їх автоморфізмів, резидуально скінченних груп, вільних груп і груп, заданих твірними та визначальними співвідношеннями, вільних добутків груп, амальгамованих вільних добутків груп, HNN-розширень груп. Зроблено короткий огляд результатів, котрі стосуються автоматних зображень вільних груп, вільних добутків груп та амальгамованих вільних добутків груп.

Розділ 2

Автоматні зображення амальгамованих вільних добутків

В цьому розділі буде побудоване конструктивне доведення того, що амальгамований вільний добуток циклічних груп порядків $l_1, l_2, \ldots, l_r, r \geq 2$ по циклічний підгрупі порядку k занурюється в групу скінченно автоматних підстановок. Для цього буде використане узагальнення леми про пінг-понг.

Ми будемо використовувати ліву дію для груп підстановок, тобто у добутку fg елемент g діє першим.

2.1 Узагальнення леми про пінг-понг

Нагадаємо лему про пінг-понг [41, Proposition 12.4 на с. 168], яка дає достатню умову розкладеності груп підстановок у амальгамований вільний добуток двох своїх підгруп. Наведемо також її доведення для повноти подальшого викладу результатів.

Лема 2.1 (про пінг-понг [41])**.** *Нехай група G породжується своїми підгрупами G_1 і G_2, при цьому $G_1 \cap G_2 = H$, де H — власна підгрупа кожної з груп G_1 та G_2 і в жодній з них вона не є підгрупою індексу 2. Припустимо, що G діє на множині Ω і існують такі непорожні підмножини $\Omega_1, \Omega_2 \subseteq \Omega$, для яких виконуються наступні умови:*

1. $\Omega_1 \cap \Omega_2 = \varnothing$;

2. $\Omega_1^H \subseteq \Omega_1, \quad \Omega_2^H \subseteq \Omega_2$*;*

3. $\Omega_1^{G_1\setminus H} \subseteq \Omega_2, \quad \Omega_2^{G_2\setminus H} \subseteq \Omega_2$*.*

Тоді група G є амальгамованим вільним добутком своїх підгруп G_1 та G_2 по підгрупі H, тобто $G = G_1 \star_H G_2$.

Доведення. Розглянемо випадок, коли $[G_1 : H] > 2$.

Якщо $g \in G_1 \setminus H$, то існує елемент $f \in G_1$ такий, що класи суміжності H, Hg, Hf попарно різні. Оскільки рівність $Hg = Hf$ виконується тоді і лише тоді, коли $g = hf$ для деякого $h \in H$, тобто

$$gf^{-1} = h \in H,$$

то звідси випливає, що

$$gf^{-1} \in G_1 \setminus H.$$

Оскільки $g, f, gf^{-1} \in G_1 \setminus H$, то з умови 3 леми випливає, що

$$\Omega_1^g, \Omega_1^f, \Omega_1^{gf^{-1}} \subseteq \Omega_2.$$

Подіявши елементом f на обидві частини включення

$$\Omega_1^{gf^{-1}} \subseteq \Omega_2$$

отримуємо нестроге включення

$$\Omega_1^g \subseteq \Omega_2^f.$$

З умови 1 маємо рівність

$$\Omega_1^f \cap \Omega_2^f = \varnothing.$$

Тому з включення

$$\Omega_1^g \subseteq \Omega_2^f$$

випливає рівність

$$\Omega_1^f \cap \Omega_1^g = \varnothing.$$

Так як Ω є непорожньою множиною, то виконується

$$\Omega_1^f \neq \varnothing.$$

Тому маємо рівність

$$\Omega_1^f \cap \Omega_1^g = \varnothing$$

і нестроге включення

$$\Omega_1^g, \Omega_1^f \subseteq \Omega_2.$$

Звідси отримуємо строге включення

$$\Omega_1^g \subsetneq \Omega_2.$$

У випадку $[G_2 : H] > 2$ міркуваннями, аналогічними до попередніх, можна показати, що для $g \in G_2 \setminus H$ має місце строге включення

$$\Omega_2^g \subsetneq \Omega_1.$$

Таким чином, для довільного $g \in G$ виконується принаймні одне з двох тверджень: з умови $g \in G_1 \setminus H$ випливає умова

$$\Omega_1^g \subsetneq \Omega_2$$

або з умови $g \in G_2 \setminus H$ випливає умова

$$\Omega_2^g \subsetneq \Omega_1.$$

Тепер достатньо показати, що добуток

$$w = hg_1g_2 \dots g_n,$$

такий що елемент $h \in H$, а елементи $g_1 g_2 \dots g_n$ по черзі належать $G_1 \setminus H$ і $G_2 \setminus H$, причому h — неодиничний елемент у випадку $n = 0$, є нетривіальним елементов групи G (див. [41, Theorem 2.6 на с. 187]).

У випадку $n < 2$ нерівність $w \neq 1$ випливає з означення підгрупи H. А саме, при $n = 1$ маємо

$$w = hg_1,$$

де $h \in H, g_1 \in G_1 \setminus H$ або $g_1 \in G_2 \setminus H$, звідки $h \neq g_1$, тобто $w \neq 1$.

Нехай $n \geq 2$. Не обмежуючи загальності, припустимо, що

$$w = hg_1 g_2 \dots g_n,$$

де $g_1 \in G_1 \setminus H$, $g_2 \in G_2 \setminus H$, $g_3 \in G_1 \setminus H$, $g_4 \in G_2 \setminus H$, $\dots$.

З умов 3, 2 маємо, що

$$\Omega_2^H \subseteq \Omega_2, \quad \Omega_2^{g_1} \subseteq \Omega_1, \quad \Omega_1^{g_2} \subseteq \Omega_2.$$

Як було показано вище, принаймні одне з останніх двох включень є строгим. Тому має місце строге включення

$$\Omega_2^{hg_1 g_2} \subsetneq \Omega_2.$$

По індукції, з включення

$$\Omega_2^{hg_1 g_2 \cdots g_{2m}} \subsetneq \Omega_2$$

випливає

$$\Omega_2^{hg_1 g_2 \cdots g_{2m} g_{2m+1}} \subsetneq \Omega_1$$

і з включення

$$\Omega_2^{hg_1 g_2 \cdots g_{2m} g_{2m+1}} \subsetneq \Omega_1$$

випливає

$$\Omega_2^{hg_1 g_2 \cdots g_{2m} g_{2m+1} g_{2m+2}} \subsetneq \Omega_2.$$

Отже, маємо

$$\Omega_2 w \subsetneq \Omega_1 \text{ або } \Omega_2 w \subsetneq \Omega_2.$$

В будь-якому випадку $\Omega_2 w \neq \Omega_2$, тобто $w \neq 1$. □

Наведене доведення леми показує, що умову 3 можна послабити. Наведемо природне узагальнення на випадок довільної скінченної кількості підгруп заданої групи підстановок.

Лема 2.2. *Нехай група G породжена своїми нетривіальними підгрупами $G_1, G_2, \ldots, G_r$, $r \geq 2$, при цьому $\langle G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_r \rangle \cap G_i = H$, де H — власна підгрупа груп $G_i, 1 \leq i \leq r$. Припустимо, що група G діє на множині Ω і існують непорожні підмножини $\Omega_1, \ldots, \Omega_r$ множини Ω, що попарно не перетинаються і задовольняють наступним умовам:*

1. $\Omega_i^H \subseteq \Omega_i, \quad 1 \leq i \leq r,$
2. $\Omega_j^{g_i} \subsetneq \Omega_i, \quad g_i \in G_i \setminus H,\ 1 \leq i, j \leq r,\ i \neq j.$

Тоді група G є амальгамованим вільним добутком груп $G_i, 1 \leq i \leq r$ по підгрупі H.

Доведення. Розглянемо довільний добуток $w = hg_{i_1}g_{i_2}\ldots g_{i_n}$, в якому $h \in H$ та

$$g_{i_1} \in G_{i_1} \setminus H,\ g_{i_2} \in G_{i_2} \setminus H,\ \ldots,\ g_{i_n} \in G_{i_n} \setminus H,$$
$$1 \leq i_1, i_2, \ldots, i_n \leq r,\ i_1 \neq i_2, i_2 \neq i_3, \ldots, i_{n-1} \neq i_n,\ n \geq 1.$$

Як і при доведенні Леми 2.1 достатньо показати, що $w \neq 1$.

Розглянемо множину Ω_j таку, що $j \neq i_1$. Тоді з умови 1 маємо включення

$$\Omega_j^h \subseteq \Omega_j.$$

З умови 2 випливає строге включення

$$\Omega_j^{hg_{i_1}} \subsetneq \Omega_{i_1}.$$

Тоді послідовно отримуємо

$$\Omega_j^{hg_{i_1}g_{i_2}} \subsetneq \Omega_{i_2}, \ldots, \Omega_j^{hg_{i_1}g_{i_2}\cdots g_{i_n}} \subsetneq \Omega_{i_n}.$$

Отже, $\Omega_j^w \neq \Omega_j$, тобто $w \neq 1$. Таким чином, лему доведено. $\square$

2.2 Амальгамований вільний добуток скінченних циклічних груп

Зафіксуємо деяке число $r \geq 2$. Розглянемо цілі невід'ємні числа

$$l_1, \ldots, l_r, k$$

такі, що $k \mid l_1, \ldots, k \mid l_r$ і $1 \leq k < l_1 \leq \ldots \leq l_r$. Тоді існують невід'ємні цілі числа $m_1, \ldots, m_r$ такі, що $km_i = l_i, 1 \leq i \leq r$.

Таким чином, коректно визначений амальгамований вільний добуток циклічних груп порядків $l_1, \ldots, l_r$ по циклічній підгрупі порядку k. Позначимо цю групу через $G(l_1, \ldots, l_r, k)$.

Група $G(l_1, \ldots, l_r, k)$ має наступне представлення в термінах твірних і визначальних співвідношень:

$$G(l_1, \ldots, l_r, k) = \langle a_1, a_2, \ldots, a_r \mid a_1^{l_1} = e, a_2^{l_2} = e, \ldots, a_r^{l_r} = e, a_i^{m_i} = a_j^{m_j}, i \neq j \rangle.$$

Тоді має місце наступна теорема

Теорема 2.3. *Група $G(l_1, \ldots, l_r, k)$ діє точно скінченними автоматами над деяким скінченним алфавітом.*

Для доведення теореми необхідно визначити алфавіт і побудувати скінченні ініціальні автомати над цим алфавітом, що породжуватимуть групу $G(l_1, \ldots, l_r, k)$.

Нехай $L = l_1 \ldots l_r$ і $K_i = L/l_i, 1 \leq i \leq r$. Визначимо алфавіт X потужності L, який будемо ототожнювати з кільцем лишків за модулем L, тобто

$$\mathsf{X} = \{0, 1, \ldots, L-1\}.$$

Розіб'ємо алфавіт X на наступні попарно неперетинні підмножини:

$$\begin{aligned}
&\mathsf{Y}_1 = \{1, \ldots, L_1\},\\
&\mathsf{Y}_2 = \{L_1 + 1, \ldots, L_1 + L_2\},\\
&\mathsf{Y}_3 = \{L_1 + L_2 + 1, \ldots, L_1 + L_2 + L_3\},\\
&\ldots\\
&\mathsf{Y}_r = \{L_1 + \ldots + L_{r-1} + 1, \ldots, L_1 + \ldots + L_{r-1} + L_r\},
\end{aligned}$$

де $L_i = m_i - 1$, $1 \leq i \leq r$. Оскільки $L_1 + \ldots + L_r < L$, ці підмножини коректно визначені.

Нехай $\mathsf{X}_i = \mathsf{Y}_i \cup \{0\}, 1 \leq i \leq r$.

Визначимо наступні r циклів на алфавіті X:

$$\begin{aligned}
&\sigma_1 = (0, 1, \ldots, L_1),\\
&\sigma_2 = (0, L_1 + 1, \ldots, L_1 + L_2),\\
&\sigma_3 = (0, L_1 + L_2 + 1, \ldots, L_1 + L_2 + L_3),\\
&\ldots\\
&\sigma_r = (0, L_1 + \ldots + L_{r-1} + 1, \ldots, L_1 + \ldots + L_{r-1} + L_r).
\end{aligned} \tag{2.1}$$

Довжини цих циклів рівні $m_1, m_2, m_3, \ldots, m_r$ відповідно. Позначимо через τ довільний цикл довжини L на множині X. Також через τ будемо позначати

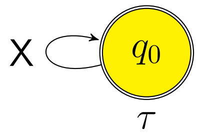


Рис. 2.1 Автомат визначений підстановкою τ

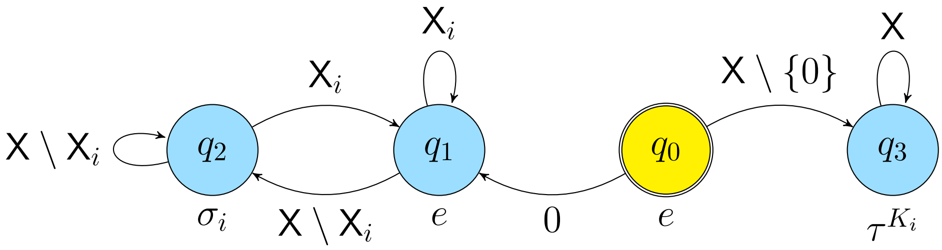


Рис. 2.2 Автомат A_i

жорстке розширення цього циклу на множину X^ω, тобто, автоматну підстановку, що діє на кожній літері кожного нескінченного слова підставкою τ (див. Рис. 2.1).

Для кожного i, $1 \leq i \leq r$, визначимо ініціальний автомат $\mathcal{A}_i$ над алфавітом X за допомогою діаграми Мура (див. Рис. 2.2). Позначатимемо через e і тривіальну підстановку, і одиничний елемент групи.

Позначимо через a_i, b_i, c_i, d_i автоматні підстановки множини X^ω визначені автоматом $\mathcal{A}_i$ у його внутрішніх станах q_0, q_1, q_2, q_3 відповідно, $1 \leq i \leq r$. З визначення $\mathcal{A}_i$ прямо випливають рекурсивні правила дії автоматних підстановок $a_i^n, b_i^n, c_i^n, d_i^n$, $1 \leq i \leq r$, $n \geq 1$ на нескінченних словах над X. Тобто, для довільних $x \in \mathsf{X}, w \in \mathsf{X}^\omega$ виконуються наступні рівності:

$$a_i^n(xw) = \begin{cases} x b_i^n(w), & \text{якщо } x = 0 \\ x d_i^n(w), & \text{якщо } x \neq 0, \end{cases} \tag{2.2}$$

$$b_i^n(xw) = \begin{cases} x b_i^n(w), & \text{якщо } x \in \mathsf{X}_i \\ x c_i^n(w), & \text{якщо } x \in \mathsf{X} \setminus \mathsf{X}_i, \end{cases} \tag{2.3}$$

$$c_i^n(xw) = \begin{cases} x^{\sigma_i^n} b_i^n(w), & \text{якщо } x \in \mathsf{X}_i \\ x^{\sigma_i^n} c_i^n(w), & \text{якщо } x \in \mathsf{X} \setminus \mathsf{X}_i, \end{cases} \tag{2.4}$$

$$d_i^n(xw) = x^{\tau^{K_i n}} d_i^n(w). \tag{2.5}$$

Зафіксуємо деяке i, $1 \leq i \leq r$.

Нехай $w = x_1 x_2 x_3 \ldots$ — нескінченне слово над алфавітом X. Доведемо рекурсивні правила (2.2)-(2.5) по індукції за n, $n \geq 1$.

У випадку $n = 1$, рекурсивні правила (2.2)-(2.5) прямо випливають з означення автомату $\mathcal{A}_i$.

Припустимо, що рекурсивні правила (2.2)-(2.5) виконуються для усіх степенів не вищих за n. Перевіримо твердження у випадку $n+1$.

Використовуючи індуктивне припущення і означення автоматної підстановки d_i отримуємо наступні рівності:

$$\begin{aligned} d_i^{n+1}(x_1 x_2 x_3 \ldots) &= d_i(x_1^{\tau^{K_i n}} d_i^n(x_2 x_3 \ldots)) = \\ &= x_1^{\tau^{K_i(n+1)}} d_i(d_i^n(x_2 x_3 \ldots)) = \\ &= x_1^{\tau^{K_i(n+1)}} d_i^{n+1}(x_2 x_3 \ldots). \end{aligned} \tag{2.6}$$

Отже, з рівностей (2.6) випливає рекурсивне правило (2.5).

Використовуючи індуктивне припущення і означення автоматних підстановок b_i, c_i отримуємо наступні рівності:

$$b_i^{n+1}(x_1x_2x_3\ldots) = \begin{cases} b_i(x_1b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}_i \\ b_i(x_1c_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases}$$
$$= \begin{cases} x_1b_i(b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1c_i(c_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases} \tag{2.7}$$
$$= \begin{cases} x_1b_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1c_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases}.$$

$$c_i^{n+1}(x_1x_2x_3\ldots) = \begin{cases} c_i(x_1^{\sigma_i^n}b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}_i \\ c_i(x_1^{\sigma_i^n}c_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases}$$
$$= \begin{cases} x_1^{\sigma_i^{n+1}}b_i(b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1^{\sigma_i^{n+1}}c_i(c_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases} \tag{2.8}$$
$$= \begin{cases} x_1^{\sigma_i^{n+1}}b_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1^{\sigma_i^{n+1}}c_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 \in \mathsf{X}\setminus\mathsf{X}_i \end{cases}.$$

Оскільки множини X_i і $\mathsf{X}\setminus\mathsf{X}_i$ інваріантні під дією підстановки σ_i, друга рівність в (2.8) правильна.

Отже, з рівностей (2.7)-(2.8) випливають рекурсивні правила (2.3)-(2.4).

Використовуючи індуктивне припущення і означення автоматних підстановок a_i, b_i, d_i отримуємо наступні рівності:

$$\begin{aligned} a_i^{n+1}(x_1x_2x_3\ldots) &= \begin{cases} a_i(x_1b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 = 0 \\ a_i(x_1d_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\{0\} \end{cases} \\ &= \begin{cases} x_1b_i(b_i^n(x_2x_3\ldots)), & \text{якщо } x_1 = 0 \\ x_1d_i(d_i^n(x_2x_3\ldots)), & \text{якщо } x_1 \in \mathsf{X}\setminus\{0\} \end{cases} \\ &= \begin{cases} x_1b_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 = 0 \\ x_1d_i^{n+1}(x_2x_3\ldots), & \text{якщо } x_1 \in \mathsf{X}\setminus\{0\} \end{cases}. \end{aligned} \tag{2.9}$$

Отже, з рівності (2.9) випливає рекурсивне правило (2.2).

Позначимо через G_i циклічну групу породжену ініціальним автоматом $\mathcal{A}_i, 1 \leq i \leq r$. Тоді визначимо групу G як групу породжену ініціальними автоматами $\mathcal{A}_i, 1 \leq i \leq r$. Іншими словами,

$$G_i = \langle a_i \rangle, 1 \leq i \leq r, \quad G = \langle a_1, \ldots, a_r \rangle = \langle G_1, \ldots, G_r \rangle.$$

Для доведення Теореми 2.3 покажемо, що група G рокладається у амальгамований вільний добуток циклічних груп порядків $l_1, \ldots, l_r$ амальгамований по циклічній підгрупі порядку k. Для доведення цього твердження, необхідно застосувати Лему 2.2. Розіб'ємо доведення на твердження, в кожному з яких зафіксуємо i таке, що $1 \leq i \leq r$.

Твердження 2.4. *Порядки автоматних підстановок b_i і c_i рівні m_i.*

Доведення. Оскільки σ_i — це цикл довжини m_i, то порядок підстановки σ_i на множині X рівний m_i. Помітимо, що автоматна підстановка $c_i^{m_i}$ діє тривіально на перших літерах слів з множини X^ω. Звідси, з рекурсивних правил (2.3) і (2.4) маємо, що автоматні підстановки $b_i^{m_i}$ і $c_i^{m_i}$ діють тривіально на кожній літері довільного нескінченного слова. З тих самих рівностей випливає,

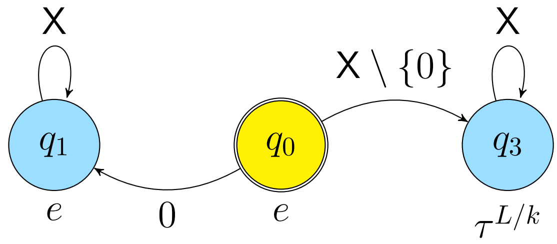


Рис. 2.3 Автомат $\mathcal{T}$

що m_i — це найменше таке число, що має вказану властивість. Отже, m_i — порядок автоматних підстановок b_i і c_i. □

Твердження 2.5. *Циклічна група G_i має порядок рівний l_i.*

Доведення. Для доведення цього твердження, достатньо показати, що автоматна підстановка a_i має порядок l_i.

З рекурсивного правила (2.5) випливає, що порядок автоматної підстановки d_i рівний порядку циклу τ^{K_i}. Оскільки, $K_i = L/l_i$ і τ — цикл довжини L, то порядок циклу τ^{K_i} рівний l_i. Отже, порядок автоматної підстановки d_i рівний l_i.

З рекурсивного правила (2.2) випливає, що автоматна підстановка a_i^n діє тривіально на усіх нескінченних словах над алфавітом X тоді і лише тоді, коли автоматні підстановки b_i^n і d_i^n діють тривіально на усіх нескінченних словах над X. Звідси випливає, що порядок автоматної підстановки a_i рівний найменшому спільному кратному порядків автоматних підстановок b_i та d_i. Оскільки порядки автоматних підстановок b_i, d_i рівні m_i, l_i відповідно і $m_i \mid l_i$, то автоматна підстановка a_i має порядок l_i, що і доводить твердження. □

З Твердження 2.5 випливає, що група G породжена циклічними підгрупами порядків $l_1, \ldots, l_r$.

Визначимо ініціальний автомат $\mathcal{T}$ (див. Рис. 2.3) і позначимо через t автоматну підстановку визначену цим автоматом. Тоді t діє на X^ω за наступним рекурсивним правилом:

$$t = \begin{cases} xw, & \text{якщо } x = 0 \\ x\tau^{L/k}(w), & \text{якщо } x \neq 0 \end{cases}, \quad x \in \mathsf{X}, w \in \mathsf{X}^{\omega}. \tag{2.10}$$

Символом H позначимо підгрупу групи G, породжену автоматною підстановкою t.

Твердження 2.6. *Група H — власна циклічна підгрупа порядку k групи G_i.*

Доведення. В Твердженні 2.4 було доведено, що автоматна підстановка b_i має порядок m_i. Оскільки $K_i m_i = L/k$, з рівностей (2.2) і (2.10) випливає, що

$$a_i^{m_i} = t.$$

З рівності

$$km_i = l_i$$

отримуємо, що автоматна підстановка $a_i^{m_i}$ має порядок k. Звідси H — це підгрупа порядку k циклічної групи G_i.

Оскільки $k < l_i$, підгрупа H — власна. □

Позначимо через B_i підгрупу групи G породжену підгрупами

$$G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_r.$$

Твердження 2.7. *Перетин підгруп B_i і G_i є підгрупою H.*

Доведення. З Твердження 2.6 випливає, що H — це підгрупа обох груп B_i та G_i. Припустимо, що $g \in B_i \cap G_i$. Нехай

$$w = 0x0w_1,$$

де $x \in \mathsf{X} \setminus \mathsf{X}_i$, $w_1 \in \mathsf{X}^\omega$. Оскільки $g \in B_i$, для деякого $x_1 \in \mathsf{X} \setminus \mathsf{Y}_i$ і автоматної підстановки g_1 маємо, що

$$g(w) = 0xx_1g_1(w_1).$$

Оскільки $g \in G_i$, для деякого $s \geq 1$ маємо, що

$$g(w) = a_i^s(w) = 0x0^{\sigma_i^s}g_1(w_1).$$

З іншого боку, $0^{\sigma_i^s} \in \mathsf{X}_i$. Тому, з того, що

$$(\mathsf{X} \setminus \mathsf{Y}_i) \cap \mathsf{X}_i = \{0\},$$

маємо рівність

$$x_1 = 0.$$

Оскільки порядок σ_i рівний m_i, маємо, що m_i ділить s. Отже, $g \in H$. $\square$

Визначимо наступні r непорожніх підмножин множини X^ω:

$$\Omega_i = \{0wy00\ldots : w \in \mathsf{X}^*, y \in \mathsf{Y}_i\}, \quad 1 \leq i \leq r. \tag{2.11}$$

Твердження 2.8. *Підмножини $\Omega_i, 1 \leq i \leq r$ попарно не перетинаються.*

Доведення. Твердження випливає з того, що $\mathsf{Y}_i, 1 \leq i \leq r$ попарно не перетинаються. $\square$

Твердження 2.9. *Виконуються наступні включення:*

$$\Omega_i^H \subseteq \Omega_i, \quad 1 \leq i \leq r.$$

Доведення. Для кожного $i, 1 \leq i \leq r$ перша літера нескінченного слова w з множини Ω_i рівна 0. З визначення автоматної підстановки t маємо

$$t(w) = w.$$

Оскільки t породжує групу H, маємо необхідне твердження. $\square$

Твердження 2.10. *Мають місце наступні строгі включення:*

$$\Omega_j^{G_i \setminus H} \subsetneq \Omega_i, 1 \leq i, j \leq r, i \neq j.$$

Доведення. Зафіксуємо довільні i та j, $1 \leq i, j \leq r, i \neq j$.

Нехай $g \in G_i \setminus H$. З того, що

$$G_i = \langle a_i \rangle \text{ і } H = \langle a_i^{m_i} \rangle$$

маємо рівність

$$g = a_i^s$$

для деякого s такого, що $m_i \nmid s$. Візьмемо довільне нескінченне слово з множини Ω_j. З визначення множини Ω_j (див. (2.11)) це слово має вигляд

$$0wy00\ldots,$$

де $w \in \mathsf{X}^*$, $y \in \mathsf{Y}_j$. Розглянемо дію елемента g на це слово. З рекурсивного зображення (2.2) маємо:

$$g(0wy00\ldots) = a_i^s(0wy00\ldots) = 0w_1y_1y_200\ldots$$

для деякого $w_1 \in \mathsf{X}^*, y_1 \in \mathsf{Y}_i, y_2 = 0^{\sigma_i^s}$. Оскільки $m_i \nmid s$, літера $y_2 \neq 0$. З визначення циклу σ_i (див. (2.1)) маємо, що $y_2 \in \mathsf{Y}_i$. Тому нескінченне слово

$$0w_1y_1y_200\ldots$$

належить множині Ω_i.

Оскільки $w_1 \in \mathsf{X}^*$ та $y_1 \in \mathsf{X}$, маємо що скінченне слово w_1y_1 — непорожнє. З іншого боку, нескінченні слова

$$0y00\ldots, \quad y \in \mathsf{Y}_i$$

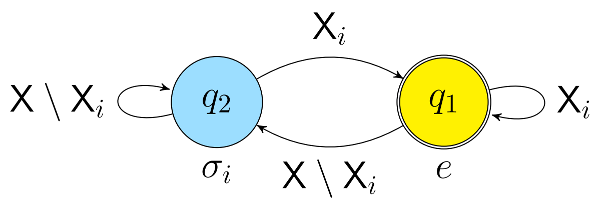


Рис. 2.4 Автомат $\mathcal{A}'_i$, $1 \leq i \leq r$

належать множині Ω_i. Отже, множина Ω_i строго включає множину всіх нескінченних слів виду

$$0w_1y_1y_200\ldots, \quad w_1 \in \mathsf{X}^*,\ y_1 \in \mathsf{X},\ y_2 \in \mathsf{Y}_i,$$

що і доводить твердження. □

Твердження 2.6-2.10 дозволяють застосувати Лему 2.2 до групи G. Таким чином, Теорема 2.3 доведена.

2.3 Випадок тривіальної амальгамації

Доведення Теореми 2.3 представлене в Розділі 2.2 ґрунтується на конструкції ініціального автомата з 4-ма внутрішніми станами. Проте, у випадку $k = 1$ можна використати автомат з двома внутрішніми станами. В цьому випадку група $G(l_1, \ldots, l_r, k)$ має наступне представлення в термінах твірних і визначальних співвідношень:

$$G(l_1, \ldots, l_r, 1) = \langle a_1, a_2, \ldots, a_r \mid a_1^{l_1} = e, a_2^{l_2} = e, \ldots, a_r^{l_r} = e \rangle.$$

Таким чином, група розкладається у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$. Щоб побудувати точну дію скінченними автоматами для цієї групи необхідно визначити ініціальний автомат $\mathcal{A}'_i$, $1 \leq i \leq r$ (див. Рис. 2.4).

Позначення використані для цього визначення такі самі як і в доведенні Теореми 2.3. Автоматні підстановки визначені автоматом $\mathcal{A}'_i$ в станах q_1, q_2 дорівнюють автоматним підстановкам b_i, c_i, визначених автоматом $\mathcal{A}_i$ в станах q_1, q_2 відповідно, $1 \leq i \leq r$.

Теорема 2.11. *Обидві групи породжені автоматними підстановками $b_1, \ldots, b_r$ та $c_1, \ldots, c_r$ розкладаються у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$.*

Будемо доводити твердження теореми для групи, породженої автоматними підстановками $b_1, \ldots, b_r$. Для групи породженої автоматними підстановками $c_1, \ldots, c_r$ доведення аналогічне.

Позначимо через $\widetilde{G}$ групу породжену автоматними підстановками $b_1, \ldots, b_r$ і через $\widetilde{G}_i$ циклічні групи породжені $b_i, 1 \leq i \leq r$. Покажемо, що $\widetilde{G}$ розкладається у вільний добуток груп $\widetilde{G}_1, \ldots, \widetilde{G}_r$.

Зафіксуємо число i таке, що $1 \leq i \leq r$. Оскільки $k = 1$, то виконуються рівності $l_i = m_i$. З Твердження 2.4 випливає, що автоматна підстановка b_i має порядок l_i. Отже, порядок циклічної групи $\widetilde{G}_i$ рівний l_i.

Позначимо через $\widetilde{B}_i$ підгрупу групи $\widetilde{G}$ породжену підгрупами

$$\widetilde{G}_1, \ldots, \widetilde{G}_{i-1}, \widetilde{G}_{i+1}, \ldots, \widetilde{G}_r.$$

Твердження 2.12. *Підгрупи $\widetilde{B}_i$ і $\widetilde{G}_i$ мають тривіальний перетин.*

Доведення. Припустимо, що $g \in \widetilde{B}_i \cap \widetilde{G}_i$. Нехай

$$w = x0w_1,$$

де $x \in \mathsf{X} \setminus \mathsf{X}_i$, $w_1 \in \mathsf{X}^\omega$. Оскільки $g \in \widetilde{B}_i$, для деякого $x_1 \in \mathsf{X} \setminus \mathsf{Y}_i$ і автоматної підстановки g_1 ми маємо

$$g(w) = xx_1g_1(w_1).$$

Оскільки $g \in \widetilde{G}_i$, для деякого $s \geq 1$ ми маємо

$$g(w) = b_i^s(w) = x0^{\sigma_i^s} g_1(w_1).$$

Але $0^{\sigma_i^s} \in \mathsf{X}_i$. Тому з $(\mathsf{X} \setminus \mathsf{Y}_i) \cap \mathsf{X}_i = \{0\}$ ми маємо $x_1 = 0$. Оскільки порядок σ_i рівний l_i ми отримаємо, що l_i ділить s. Отже, $g = e$. □

Визначимо наступні r непорожніх підмножин множини X^ω:

$$\widetilde{\Omega}_i = \{wy00\ldots : w \in \mathsf{X}^*, y \in \mathsf{Y}_i\}, \quad 1 \leq i \leq r. \tag{2.12}$$

Твердження 2.13. *Підмножини $\widetilde{\Omega}_i, 1 \leq i \leq r$ попарно не перетинаються.*

Доведення. Оскільки $\mathsf{Y}_i, 1 \leq i \leq r$ попарно не перетинаються, твердженння виконується. □

Твердження 2.14. *Наступні строгі включення виконуються:*

$$\widetilde{\Omega}_j^{\widetilde{G}_i \setminus \{e\}} \subsetneq \widetilde{\Omega}_i, \quad 1 \leq i, j \leq r,\, i \neq j.$$

Доведення. Зафіксуємо довільні i та j, $1 \leq i, j \leq r$, $i \neq j$.

Нехай $g \in \widetilde{G}_i$, $g \neq e$. Оскільки

$$\widetilde{G}_i = \langle b_i \rangle,$$

маємо рівність

$$g = b_i^s$$

для деякого s такого, що $l_i \nmid s$. Візьмемо довільне нескінченне слово з множини $\widetilde{\Omega}_j$. З визначення множини $\widetilde{\Omega}_j$ (див. (2.12)) це слово має вигляд

$$wy00\ldots,$$

де $w \in \mathsf{X}^*$, $y \in \mathsf{Y}_j$. Розглянемо дію елемента g на це слово. З рекурсивного правила (2.3) маємо наступне:

$$g(wy00\ldots) = b_i^s(wy00\ldots) = w_1 y_1 y_2 00\ldots$$

для деякого $w_1 \in \mathsf{X}^*, y_1 \in \mathsf{Y}_i, y_2 = 0^{\sigma_i^s}$. Оскільки $l_i \nmid s$, літера $y_2 \neq 0$. З визначення циклу σ_i (див. (2.1)) маємо, що $y_2 \in \mathsf{Y}_i$. Звідси випливає, що нескінченне слово

$$w_1 y_1 y_2 00 \ldots$$

належить множині $\widetilde{\Omega}_i$.

Оскільки $w_1 \in \mathsf{X}^*$ і $y_1 \in \mathsf{X}$ ми маємо, що скінченне слово $w_1 y_1$ — непорожнє. З іншого боку, нескінченні слова $y00\ldots$, $y \in \mathsf{Y}_i$ належать множині $\widetilde{\Omega}_i$. Отже, множина $\widetilde{\Omega}_i$ строго включає множину усіх нескінченних слів виду

$$w_1 y_1 y_2 00 \ldots, \quad w_1 \in \mathsf{X}^*,\, y_1 \in \mathsf{X},\, y_2 \in \mathsf{Y}_i$$

що і доводить твердження. □

Доведення Теореми 2.11. Твердження 2.12-2.14 дозволяють застосувати Лему 2.2 до групи $\widetilde{G}$. Отже, група $\widetilde{G}$ розкладається у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$. □

Нагадаємо означення оновлювального автомата над алфавітом X (див. [58]).

Означення 2.1. Літера $x \in \mathsf{X}$ називається оновлювальною, якщо $|\lambda(q, x)| = 1$, $q \in Q$, тобто x скидає автомат до стану $\lambda(q, x)$.

Автомат називається оновлювальним, якщо кожна літера алфавіту, над яким він розглядається, є оновлювальною.

Зафіксуємо $i, 1 \le i \le r$. Легко бачити, що автомат $\mathcal{A}'_i$ є оновлювальним. Група автомата $\mathcal{A}'_i$ описана в наступній теоремі.

Теорема 2.15. *Група автомата $G(\mathcal{A}'_i)$ розкладається в прямий добуток двох циклічних груп порядку m_i.*

Для доведення теореми доведемо наступну лему.

Лема 2.16. *Автоматні підстановки b_i та c_i комутують.*

Доведення. Для доведення твердження леми достатньо показати, що для довільного нескінченного слова w над X виконується рівність

$$b_i c_i(w) = c_i b_i(w).$$

Нехай

$$w = x_1 w_1, \quad x_1 \in \mathsf{X},\, w_1 \in \mathsf{X}^\omega$$

нескінченне слово над X. З рівності (2.1) випливає, що множини X_i і $\mathsf{X} \setminus \mathsf{X}_i$ інваріантні відносно дії σ_i. Тоді з рівностей (2.3), (2.4) маємо

$$\begin{aligned} b_i c_i(w) = b_i c_i(x_1 w_1) &= \\ &= \begin{cases} b_i(x_1^{\sigma_i} b_i(w)), & \text{якщо } x_1 \in \mathsf{X}_i \\ b_i(x_1 c_i(w)), & \text{якщо } x_1 \in \mathsf{X} \setminus \mathsf{X}_i \end{cases} \\ &= \begin{cases} x_1^{\sigma_i} b_i^2(w), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1 c_i^2(w), & \text{якщо } x_1 \in \mathsf{X} \setminus \mathsf{X}_i \end{cases}, \end{aligned} \tag{2.13}$$

$$\begin{aligned} c_i b_i(w) = c_i b_i(x_1 w_1) &= \\ &= \begin{cases} c_i(x_1 b_i(w)), & \text{якщо } x_1 \in \mathsf{X}_i \\ c_i(x_1 c_i(w)), & \text{якщо } x_1 \in \mathsf{X} \setminus \mathsf{X}_i \end{cases} \\ &= \begin{cases} x_1^{\sigma_i} b_i^2(w), & \text{якщо } x_1 \in \mathsf{X}_i \\ x_1 c_i^2(w), & \text{якщо } x_1 \in \mathsf{X} \setminus \mathsf{X}_i \end{cases}. \end{aligned} \tag{2.14}$$

Отже, з рівностей (2.13), (2.14) випливає твердження леми. □

Доведення Теореми 2.15. З Леми 2.16 випливає, що група автомата $G(\mathcal{A}_i')$ абелева. З Твердження 2.4 випливає, що c_i і b_i мають порядок m_i. Припустимо, що для деяких додатних цілих чисел s_1, s_2 рівність

$$b_i^{s_1} = c_i^{s_2}$$

виконується.

Нехай

$$w = xw_1,$$

де $x \in \mathsf{X_i}$, $w_1 \in \mathsf{X}^\omega$. З рівностей (2.3), (2.4) маємо

$$b_i^{s_1}(w) = xb_1^{s_1}(w_1) = x^{\sigma_i^{s_2}} b_i(w_1) = c_i^{s_2}(w).$$

Отже, s_2 ділиться на m_i. Тоді перетин підгруп $G(\mathcal{A}'_i)$ породжених b_i та c_i тривільний. Звідси випливає твердження теореми. □

Разом з тим, питання про структурний опис групи, пороженої усіма автоматними підстановками $b_1, \ldots, b_r$ та $c_1, \ldots, c_r$, залишається відкритим. Зокрема, природно виникає питання про задання цієї групи твірними та співвідношеннями.

2.4 Висновки до розділу

Побудовано точні зображення амальгамованих вільних добутків скінченних циклічних груп по циклічній підгрупі за допомогою скінченних автоматів над деяким скінченним алфавітом. Для цього доведено узагальнення леми про пінг-понг для амальгамованих вільних добутків скінченної кількості груп. Було показано, що вказаний амальгамований вільний добуток породжується автоматними підстановками, визначеними ініціальними автоматами з 4 станами. Окремо розглянуто випадок тривіальної амальгамації, тобто вільного добутку скінченних циклічних груп. Побудовані в цьому випадку ініціальні автомати, в яких визначаються необхідні автоматні підстановки, мають по 2 внутрішні стани і є оновлювальними автоматами. Показано, що групи кожного з цих автоматів розкладаються в прямі добутки двох скінченних циклічних груп.

Розділ 3

Мінімальні автоматні зображення амальгамованих вільних добутків

В цьому розділі розглянемо амальгамовані вільні добутки скінченних груп і побудуємо скінченні ініціальні автомати над мінімально можливими алфавітами, які визначають ці групи. Якщо для простого числа p амальгамований вільний добуток скінченних циклічних груп є резидульно скінченною p-групою, то буде показано, що побудовані автомати визначають елементи з p-силовської підгрупи групи $GA(\mathsf{X})$. Останній результат може бути розглянутий як ізоморфне занурення в скінченно-становий вінцевий добуток регулярних простих циклічних груп (див. [53]).

3.1 Розширення дій на словах

Нехай w — деяке нескінченне слово над алфавітом X і $\xi = \{\xi_k\}_{k\geq 0}$ — послідовність додатних цілих чисел.

Означення 3.1. Розбиттям $w[\xi]$ по послідовності ξ будемо називати таке розбиття нескінченного слова w на склади, довжини яких рівні відповідним членам послідовності ξ, тобто

$$w = w[1, \xi_1]w[2, \xi_2] \dots w[k, \xi_k] \dots .$$

Нехай w — деяке скінченне слово над алфавітом X і $\xi_k = \{\xi_i\}_{i=1}^{k}, k \geq 0$ —

скінченна послідовність додатних цілих чисел така, що $|w| = \xi_1 + \ldots + \xi_k$.

Означення 3.2. Розбиттям $w[\xi_k]$ по послідовності ξ_k будемо називати таке розбиття скінченного слова w на склади, довжини яких рівні відповідним членам послідовності ξ_k, тобто

$$w = w[1, \xi_1]w[2, \xi_2] \ldots w[k, \xi_k].$$

Означення 3.3. Автоматна підстановка a є жорстким розширенням своєї дії на скінченних словах, якщо існує $l > 0$ таке, що для довільного розбиття $w[\xi]$ має місце рівність:

$$a(w[\xi]) = a(w[1, l])a(w[2, l]) \ldots a(w[k, l]) \ldots . \tag{3.1}$$

Лема 3.1. *Нехай автоматна підстановка a є жорстким розширенням своєї дії на скінченних словах довжини l. Тоді вона має скінченний порядок, рівний порядку звуження автоматної підстановки a на скінченні слова довжини l.*

Доведення. Доведення випливає з рівності (3.1). □

Нехай $m > 1$ — додатне ціле число. Розглянемо канонічний розклад m на прості множники

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},$$

де $p_1, p_2, \ldots, p_t$ — попарно різні прості числа, $\alpha_1, \alpha_2, \ldots, \alpha_t \geq 0$, $t \geq 1$. Для числа m символом $d(m)$ позначимо суму

$$\alpha_1 + \alpha_2 + \ldots + \alpha_t.$$

Будемо використовувати ліву дію для груп підстановок, тобто в добутку fg елемент g діє першим.

3.2 Дії над автоматами

З'єднання автоматів

Нехай $\mathcal{A}_{q_1} = \langle Q_1, \lambda_1, \mu_1 \rangle$ та $\mathcal{A}_{q_2} = \langle Q_2, \lambda_2, \mu_2 \rangle$ — два ініціальні автомати над алфавітом X, причому $Q_1 \cap Q_2 = \varnothing$. Зафіксуємо непорожні підмножини стрілок R_1, R_2 такі, що

$$R_1 \subset \{(q,x) \mid \lambda_1(q,x) = q_1, q \in Q_1, x \in \mathsf{X}\}, \tag{3.2}$$

$$R_2 \subset \{(q,x) \mid \lambda_2(q,x) = q_2, q \in Q_2, x \in \mathsf{X}\}. \tag{3.3}$$

Введемо операцію

Означення 3.4. З'єднання автоматів $\mathcal{A}_{q_1}$ та $\mathcal{A}_{q_2}$ відносно множин R_1, R_2 називається ініціальний автомат $\mathcal{A}_{q_1\, R_1}\square_{R_2}\mathcal{A}_{q_2} = \langle Q, \lambda, \mu \rangle$, отриманий наступним чином:

- множина внутрішніх станів Q є об'єднанням внутрішніх станів автоматів $\mathcal{A}_{q_1}$ та $\mathcal{A}_{q_2}$, тобто $Q = Q_1 \cup Q_2$;
- для довільного $(q,x) \in Q \times \mathsf{X}$ функція переходів λ визначається за наступним правилом:

$$\lambda(q,x) = \begin{cases} q_2 & \text{якщо } (q,x) \in R_1 \\ q_1 & \text{якщо } (q,x) \in R_2 \\ \lambda_1(q,x) & \text{якщо } (q,x) \notin R_1, q \in Q_1 \\ \lambda_2(q,x) & \text{якщо } (q,x) \notin R_2, q \in Q_2 \end{cases}; \tag{3.4}$$

- для довільного $(q,x) \in Q \times \mathsf{X}$ функція виходів μ визначається за насту-

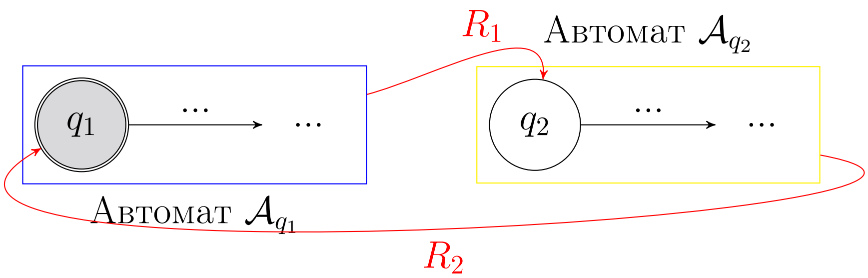


Рис. 3.1 Автомат $\mathcal{A}_{q_1\,R_1}\Box_{R_2}\mathcal{A}_{q_2}$

пним правилом:

$$\mu(q,x) = \begin{cases} \mu_1(q,x) & \text{якщо } q \in Q_1 \\ \mu_2(q,x) & \text{якщо } q \in Q_2 \end{cases}; \tag{3.5}$$

- ініціальним станом автомата $\mathcal{A}_{q_1\,R_1}\Box_{R_2}\mathcal{A}_{q_2}$ є q_1.

Графічне зображення автомата $\mathcal{A}_{q_1\,R_1}\Box_{R_2}\mathcal{A}_{q_2}$ представлене на Рис. 3.1. На цьому рисунку червоними стрілками позначено стрілки, що після приєднання були перевизначені в з'єднанні автоматів.

Для ініціальних автоматів $\mathcal{A}_{q_1}, \mathcal{A}_{q_2}, \mathcal{A}_{q_3}$ і відповідних їм множин стрілок R_1, R_2, R_3 має місце рівність:

$$(\mathcal{A}_{q_1\,R_1}\Box_{R_2}\mathcal{A}_{q_2})_{R_2}\Box_{R_3}\mathcal{A}_{q_3} = \mathcal{A}_{q_1\,R_1}\Box_{R_3}(\mathcal{A}_{q_2\,R_2}\Box_{R_3}\mathcal{A}_{q_3}).$$

Послідовне з'єднання автоматів

Нехай $\mathcal{A}_{q_1} = \langle Q_1, \lambda_1, \mu_1 \rangle$ та $\mathcal{A}_{q_2} = \langle Q_2, \lambda_2, \mu_2 \rangle$ — два ініціальні автомати над алфавітом X, причому $Q_1 \cap Q_2 = \varnothing$. Припустимо, що наступні підмножини стрілок R_1 та R_2 є непорожніми:

$$R_1 = \{(q,x) \mid \lambda_1(q,x) = q_1, q \in Q_1, x \in \mathsf{X}\},$$
$$R_2 = \{(q,x) \mid \lambda_2(q,x) = q_2, q \in Q_2, x \in \mathsf{X}\}.$$

Введемо операцію $\square$ послідовного з'єднання заданих автоматів.

Означення 3.5. Послідовним з'єднання автоматів $\mathcal{A}_{q_1}$ та $\mathcal{A}_{q_2}$ називається ініціальний автомат

$$\mathcal{A}_{q_1} \square \mathcal{A}_{q_2} = \mathcal{A}_{q_1\,R_1} \square_{R_2} \mathcal{A}_{q_2}.$$

Іншими словами, послідовне з'єднання є окремим випадком з'єднання, коли підмножини R_1, R_2 є максимальними за включенням, тобто містять усі стрілки, які ведуть в ініціальний стан.

Безпосередньо з означення випливає, що операція послідовного з'єднання автоматів є асоціативною. Тому ця операція коректно визначається і для довільного скінченнного числа ініціальних автоматів.

Нехай k – деяке натуральне число, $k \geq 2$. Визначимо автоматні підстановки a_1, a_2, $\ldots$, a_k в ініціальних станах автоматів $\mathcal{A}_{q_1}$, $\mathcal{A}_{q_2}$, $\ldots$, $\mathcal{A}_{q_k}$ відповідно і автоматну підстановку a, визначену в ініціальному стані послідовного з'єднання $\mathcal{A}_{q_1} \square \mathcal{A}_{q_2} \square \ldots \square \mathcal{A}_{q_k}$ цих автоматів. Тоді має місце наступна лема.

Лема 3.2. *Нехай автоматні підстановки a_1, a_2, $\ldots$, a_k є жорсткими розширеннями своїх дій на скінченних словах довжини $l_1, l_2, \ldots, l_k$ і мають порядки n_1, n_2, $\ldots$, n_k відповідно. Тоді автоматна підстановка a також є жорстким розиренням своєї дії на скінченних словах довжини $l_1+l_2+\ldots+l_k$ та має скінченний порядок, рівний НСК$\{n_1, n_2, \ldots, n_k\}$.*

Доведення. З визначення автомата $\mathcal{A}_{q_1} \square \mathcal{A}_{q_2} \square \ldots \square \mathcal{A}_{q_k}$ прямо випливає, що автоматна підстановка a є жорсткими розширеннями своєї дії на словах довжини $l = l_1 + l_2 + \ldots + l_k$.

Дія автоматної підстановки a на довільному слові w довжини l над алфавітом X визначається рівністю:

$$a(w[\xi_k]) = a_1(w[1, l_1])a_2(w[2, l_2]) \ldots a_k(w[k, l_k]), \tag{3.6}$$

де $w[\xi_k]$ — розбиття слова w по послідовності $\xi_k = \{l_1, \ldots, l_k\}$.

З Леми 3.1 і рівності (3.6) тепер відразу випливає необхідне твердження.

$\square$

$l-$повний автомат

Нехай $\mathcal{A}_{q_0} = \langle Q, \lambda, \mu \rangle$ — ініціальний автомат над алфавітом X. Припустимо, що автоматна підстановка визначена в стані q_0 автомата $\mathcal{A}_{q_0}$ є жорстким розширенням своєї дії на словах довжини l для деякого $l \geq 1$.

Означення 3.6. Автомат l-$\mathcal{A}_{q_0} = \langle \overline{Q}, \overline{\lambda}, \overline{\mu} \rangle$ над алфавітом X, який називається l-повним автоматом, отримується з $\mathcal{A}_{q_0}$ наступним чином:

- множина внутрішніх станів $\overline{Q} = \bigcup\limits_{k=0}^{l-1} \mathsf{X}^k$;
- для стану w, $0 \leq |w| < l-1$ і літери $x \in \mathsf{X}$ функція переходів $\overline{\lambda}$ визначена рівністю:
$$\overline{\lambda}(w, x) = wx;$$
- для стану w, $|w| = l - 1$ і літери $x \in \mathsf{X}$ функція переходів $\overline{\lambda}$ визначена рівністю:
$$\overline{\lambda}(w, x) = \Lambda; \tag{3.7}$$
- для стану w, $0 \leq |w| \leq l - 1$ і літери $x \in \mathsf{X}$ функція виходів $\overline{\mu}$ визначена рівністю:
$$\overline{\mu}(w, x) = \mu(\lambda(q_0, w), x); \tag{3.8}$$
- ініціальним станом автомата l-$\mathcal{A}_{q_0}$ є Λ.

З Означення 3.6 прямо випливає наступна лема:

Лема 3.3. *Автоматні підстановки визначені в ініціальних станах автомата $\mathcal{A}_{q_0}$ і l-повного автомата l-$\mathcal{A}_{q_0}$ рівні.*

Доведення. Нехай a, a_l — автоматні підстановки визначені в ініціальних станах автоматів $\mathcal{A}_{q_0}$ і l-$\mathcal{A}_{q_0}$. З рівності (3.7) випливає, що автоматна підстановка a_l також є жорстким розширенням своєї дії на словах довжини l. Тому достатньо показати, що автоматні підстановки a_l, a діють однаково на словах довжини не більше l. Доведемо індукцією за довжиною слова.

База індукції виконується, оскільки мають місце рівності:

$$a_l(\Lambda) = \overline{\mu}(\Lambda, \Lambda) = \Lambda = a(\Lambda)$$

Нехай w — слово довжини не більшої за l і $a_l(w) = a(w)$. Тоді для довільного $x \in \mathsf{X}$ має місце:

$$\begin{aligned} a_l(wx) &= \overline{\mu}(\Lambda, w)\overline{\mu}(\overline{\lambda}(\Lambda, w), x) = a(w)\overline{\mu}(w, x) = \\ &= a(w)\mu(\lambda(q_0, w), x) = a(wx). \end{aligned} \tag{3.9}$$

Отже, припущення індукції виконується і автоматні підстановки a і a_l рівні.

□

Приклад 3.1. *Нехай визначений алфавіт* $\mathsf{X} = \{0, 1\}$ *і підстановка* $\sigma = (0, 1)$. *На Рис. 3.2 зліва зображений ініціальний автомат* $\mathcal{A}_{q_1}$. *Автоматна підстановка, визначена автоматом* $\mathcal{A}_{q_1}$, *є жорстким рошиpенням своєї дії на словах довжини* 3. *Справа зображений відповідний йому* 3*-повний автомат* 3-$\mathcal{A}_{q_1}$.

3.3 Автоматні підстановки скінченного порядку

Зафіксуємо натуральне число m. Нехай

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t},$$

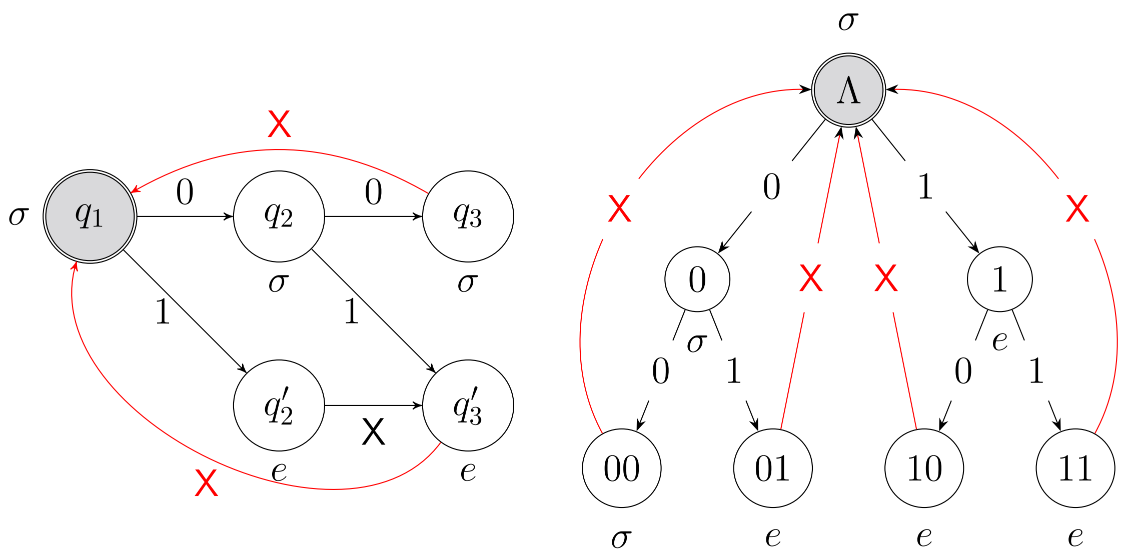


Рис. 3.2 Автомати $\mathcal{A}_{q_1}$ і 3-$\mathcal{A}_{q_1}$

де $p_1, p_2, \ldots, p_t$ — попарно різні прості числа, $\alpha_1, \alpha_2, \ldots, \alpha_t$ — додатні цілі числа. Позначимо через p максимальне з простих чисел $p_1, p_2, \ldots, p_t$, $t \geq 1$. Розглянемо алфавіт $\mathsf{X} = \{0, 1, \ldots, p-1\}$, який будемо ототожнювати з кільцем лишків за модулем p.

Нехай q — деяке просте число, $q \leq p$. Визначимо підстановку

$$\sigma_q = (0, 1, \ldots, q-1)$$

над X. Підмножину перших q літер $\{0, 1, \ldots, q-1\}$ алфавіту X будемо ототожнювати із $\mathbb{Z}_q$.

Нехай $w = x_1 x_2 \ldots x_\alpha$ — слово довжини α, $\alpha \geq 1$ над $\mathbb{Z}_q$. Для слова w визначимо ініціальний автомат $\mathcal{A}_q^w$ над алфавітом X (див. Рис. 3.3). Розглянемо автоматну підстановку a визначену в ініціальному стані q_1 автомата $\mathcal{A}_q^w$.

З означення автомата $\mathcal{A}_q^w$ прямо випливає наступна лема:

Лема 3.4. *Автоматна підстановка a є жорстким розширення своєї дії на словах довжини α.*

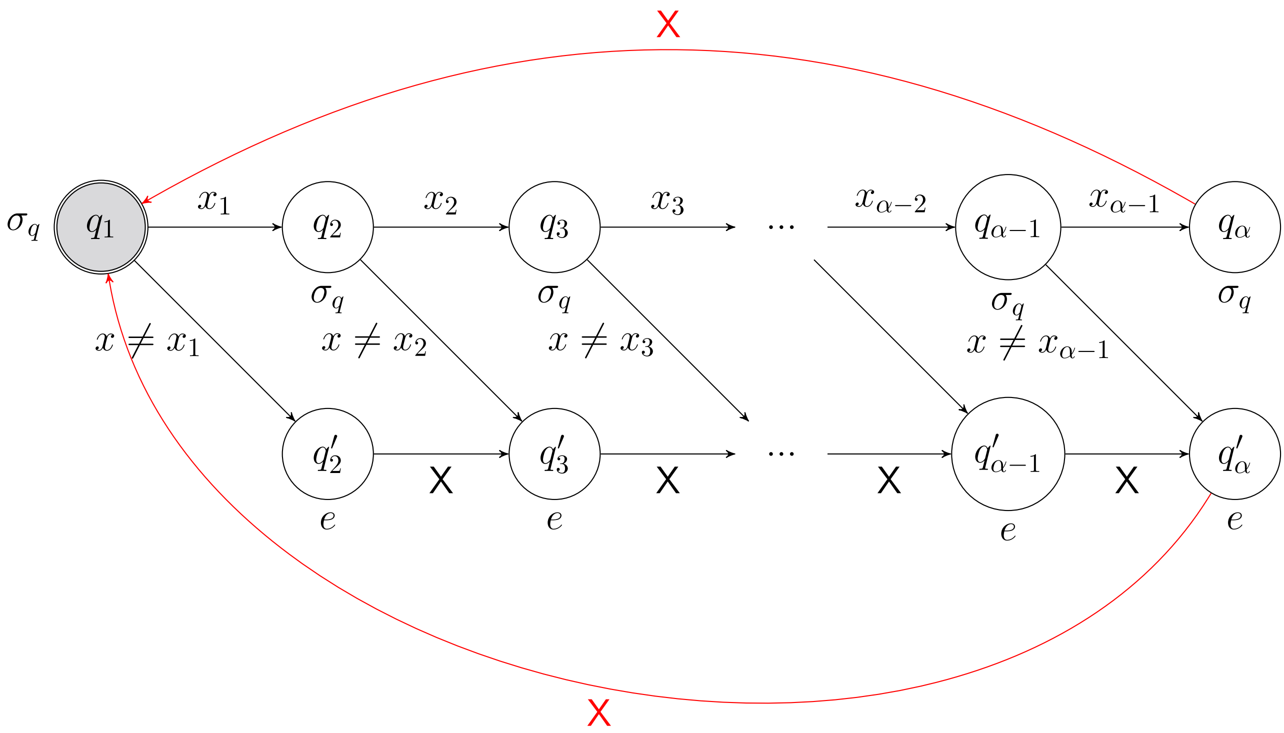


Рис. 3.3 Автомат $\mathcal{A}_q^w$

Автоматна підстановка a діє на слові $u = y_1 y_2 \dots y_\beta, \beta \leq \alpha$ над $\mathbb{Z}_q$ наступним чином:

$$a(u) = a(y_1 y_2 \dots y_\beta) = (y_1 + 1)(y_2 + 1) \dots (y_{k+1} + 1) y_{k+2} \dots y_\beta,$$

де додавання виконується за модулем q та виконані умови $y_i = x_i$ для усіх $1 \leq i \leq k$, $y_{k+1} \neq x_{k+1}$.

Якщо u — це слово довжини α над X, яке містить хоча б одне входження деякої літери x з $\mathsf{X} \setminus \mathbb{Z}_q$, то слово u має вигляд

$$u = u_1 x u_2,$$

де u_1 — слово довжини $\beta, \beta < \alpha$ над $\mathbb{Z}_q$, u_2 — деяке слово над X. Тоді a діє

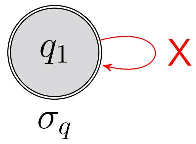


Рис. 3.4 Автомат $\mathcal{A}_x^q$

на u згідно рівності:

$$a(u) = a(u_1)xu_2. \tag{3.10}$$

Для автоматної підстановки a і слова u над X розглянемо орбіту дії групи породженої a:

$$O(u) = \{a^k(u) \mid k \in \mathbb{Z}\}.$$

Твердження 3.5. *Має місце рівність:*

$$O(w) = \mathbb{Z}_q^\alpha.$$

Доведення. Доведемо індукцією за довжиною α слова w.

Нехай $\alpha = 1$. Тоді автомат $\mathcal{A}_q^w$ (див. Рис. 3.4) має єдиний стан з поміткою σ_q і для автоматної підстановки a, визначеної в цьому стані, дія на слові $x \in \mathbb{Z}_q$ довжини α визначена рівністю:

$$a(x) = (x+1) \pmod q.$$

Звідси випливає, що $O(x) = \mathbb{Z}_q$ і база індукції виконується.

Припустимо, що для усіх слів w довжини $\alpha - 1, \alpha \geq 2$ виконується рівність

$$O(w) = \mathbb{Z}_q^{\alpha-1}.$$

Покажемо, що для довільного слова w довжини α виконується рівність

$$O(w) = \mathbb{Z}_q^\alpha.$$

Нехай $w = w_1x$, де w_1 — слово довжини $\alpha - 1$, $x \in \mathbb{Z}_q$. Дія автоматної підстановки a, визначеної в ініціальномі стані автомата $\mathcal{A}_q^w$ (див. Рис. 3.3), на слово w описується рівністю:

$$a(w) = b_1(w_1)\,(x+1)\,(\mathrm{mod}\,q),$$

де b_1 — автоматна підстановка визначена в ініціальномі стані автомата $\mathcal{A}_q^{w_1}$. З припущення індукції випливає, що найменший степінь β, для якого

$$b_1^{\beta}(w_1) = w_1,$$

дорівнює $q^{\alpha-1}$. Тому має місце наступна рівність:

$$a^{\beta}(w) = b_1^{\beta}(w_1)(x+1)\,(\mathrm{mod}\,q), \quad 1 \leq \beta \leq q^{\alpha-1}.$$

Звідси маємо рівності:

$$a^{\beta}(w) = b_1^{\beta\,(\mathrm{mod}\,q^{\alpha-1})}(w_1)(x+k)\,(\mathrm{mod}\,q),$$
$$(k-1)q^{\alpha-1} + 1 \leq \beta \leq kq^{\alpha-1},\ 1 \leq k \leq q.$$

Застосувавши припущення індукції отримуємо необхідне твердження. □

Нехай $u = u_1xu_2$ — слово довжини α над X, таке що u_1 — слово довжини $\beta, \beta < \alpha$ над $\mathbb{Z}_q$, x з $\mathsf{X} \setminus \mathbb{Z}_q$, u_2 — деяке слово над X. Тоді має місце

Твердження 3.6. *Для слова u виконується рівність:*

$$O(u) = \{vxu_2 \mid v \in \mathbb{Z}_q^{\beta}\}.$$

Доведення. З рівності (3.10) маємо

$$O(u) = \{vxu_2 \mid v \in O(u_1)\}. \tag{3.11}$$

З Твердження 3.5 випливає, що

$$O(u_1) = Z_q^{\beta}. \tag{3.12}$$

Рівності (3.11) та (3.12) доводять необхідне твердження. □

Твердження 3.7. *Автоматна підстановка a має порядок q^{α}.*

Доведення. За Лемою 3.4 порядок a дорівнює порядку звуження цієї підстановки на слова довжини α над X. Цей порядок дорівнює найменшому спільному кратному потужностей орбіт дії групи породженої a на словах довжини α. За Твердженнями 3.6 та 3.5 ці потужності набувають всіх можливих значень з множини

$$\{q^{\beta} \mid 0 \leq \beta \leq \alpha\}.$$

Отже, їх найменше спільне кратне дорівнює q^{α}, що і доводить необхідне твердження. $\square$

Таким чином, порядок автоматної підстановки, визначеної в ініціальному стані автомата $\mathcal{A}_q^w$, дорівнює $q^{|w|}$.

Побудуємо для числа m і набору слів

$$W = (w_1, \ldots, w_t),$$

де $w_i \in \mathbb{Z}_{p_i}^{\alpha_i}, 1 \leq i \leq t$ автомат $\mathcal{A}_m^W$ як послідовне з'єднання

$$\mathcal{A}_m^W = \mathcal{A}_{p_1}^{w_1} \square \mathcal{A}_{p_2}^{w_2} \square \ldots \square \mathcal{A}_{p_t}^{w_t}. \tag{3.13}$$

Графічне зображення автомата $\mathcal{A}_m^W$ для числа $m = p_1^{\alpha_1} p_2^{\alpha_2}$ представлене на Рис. 3.5. Червоними стрілками схематично зображені усі стрілки, які після з'єднання перевизначаються у автоматах $\mathcal{A}_{p_1}^{w_1}, \mathcal{A}_{p_2}^{w_2}$.

З Означення 3.4 прямо випливає наступне твердження.

Твердження 3.8. *Кількість станів автомата $\mathcal{A}_m^W$ дорівнює*

$$2\sum_{i=1}^{t} \alpha_i - t.$$

Твердження 3.9. *Автоматна підстановка, визначена в ініціальному стані автомата $\mathcal{A}_m^W$, є жорстким розширенням своєї дії на словах довжини $d(m)$ та має порядок m.*

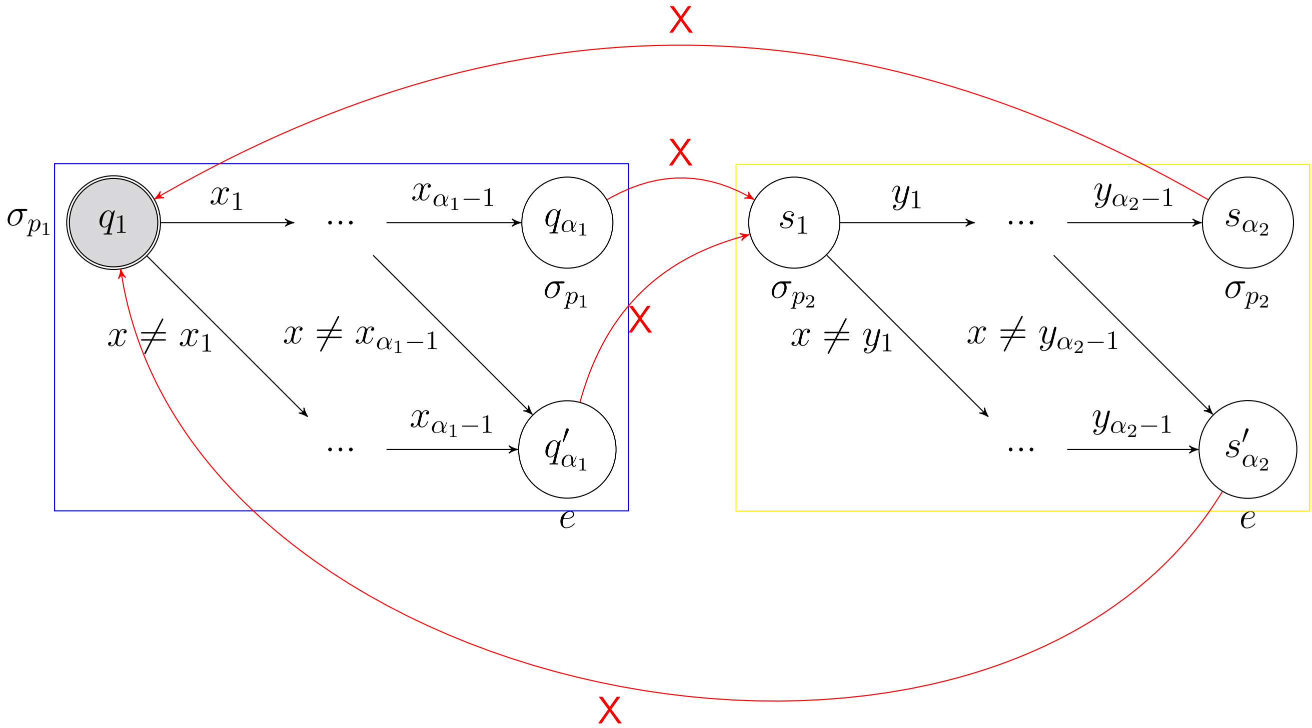


Рис. 3.5 Автомат $\mathcal{A}_{p_1}^{w_1} \square \mathcal{A}_{p_2}^{w_2}$

Доведення. Перша частина твердження випливає з визначення автомата $\mathcal{A}_m^W$ і Леми 3.2.

З Твердження 3.7 і Леми 3.2 отримуємо, що порядок автоматної підстановки, визначеної в ініціальному стані автомата $\mathcal{A}_m^W$, дорівнює найменшому спільному кратному попарно взаємно простих чисел $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_t}$. Звідси відразу випливає друга частина твердження. $\square$

Визначимо ініціальні автомати $\mathcal{I}_n$, $n \geq 1$ (див. Рис. 3.6), кожен з яких визначає тотожну автоматну підстановку.

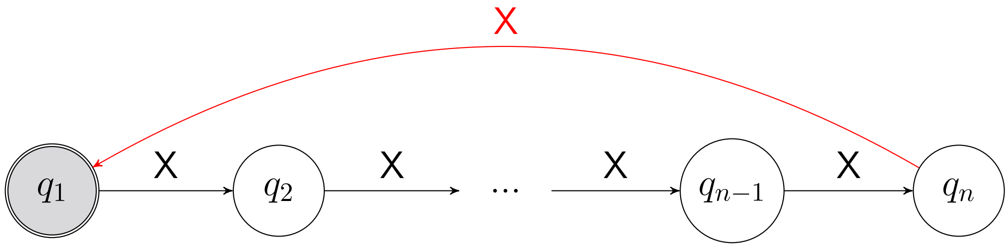


Рис. 3.6 Автомат $\mathcal{I}_n$

3.4 Основна конструкція

Зафіксуємо деяке число $r \geq 2$. Розглянемо цілі додатні числа $l_1, \ldots, l_r, k$ такі, що $k \mid l_1, \ldots, k \mid l_r$ і $1 \leq k < l_1 \leq \ldots \leq l_r$. Тоді існують додатні цілі числа $m_1, \ldots, m_r$ такі, що $km_i = l_i, 1 \leq i \leq r$.

Таким чином, коректно визначений амальгамований вільний добуток циклічних груп порядків $l_1, \ldots, l_r$ по циклічній підгрупі порядку k. Позначимо цю групу через

$$G(l_1, \ldots, l_r, k).$$

Група $G(l_1, \ldots, l_r, k)$ має наступне представлення в термінах твірних і визначальних співвідношень:

$$G(l_1, \ldots, l_r, k) = \langle y_1, y_2, \ldots, y_r \mid y_1^{l_1} = e, y_2^{l_2} = e, \ldots, y_r^{l_r} = e, y_i^{m_i} = y_j^{m_j}, i \neq j \rangle.$$

Нехай $L = l_1 l_2 \ldots l_r$. Позначимо через p найбільший з простих дільників числа L. Зафіксуємо алфавіт $\mathsf{X} = \mathbb{Z}_p$. Тоді має місце наступна теорема

Теорема 3.10. *Група $G(l_1, \ldots, l_r, k)$ ізоморфно занурюється в $FGA(\mathsf{X})$, причому потужність алфавіту X є мінімально можливою.*

Ми наведемо явну конструкцію автоматів над X, які породжують групу ізоморфну $G(l_1, \ldots, l_r, k)$. Для цього побудуємо ряд допоміжних автоматів, а потім доведемо необхідні для доведення теореми твердження.

Для кожного $n > 0$ позначатимемо символом $\overline{0}_n$ слово $\underbrace{00\ldots0}_{n}$.

Нехай

$$d = d(m_1) + d(m_2) + \ldots + d(m_r). \tag{3.14}$$

Тоді $d > 0$.

Зафіксуємо i, $1 \leq i \leq r$. Для числа m_i розглянемо його канонічний розклад на прості множники:

$$m_i = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},$$

де $p_1, p_2, \ldots, p_t$ — попарно різні прості числа, $\alpha_1, \alpha_2, \ldots, \alpha_t$ — додатні цілі числа.

Розглянемо для числа m_i та множини слів

$$W_i = \{\overline{0}_{\alpha_1}, \overline{0}_{\alpha_2}, \ldots, \overline{0}_{\alpha_t}\} \tag{3.15}$$

ініціальний автомат $\mathcal{A}_{m_i}^{W_i}$, визначений рівністю (3.13), над алфавітом X.

Зауваження 3.11. *Множину W_i можна замінити на множину, яка складається із довільних слів довжин $\alpha_1, \alpha_2, \ldots, \alpha_t$ над X без суттєвих змін в подальших міркуваннях.*

Позначимо автомат $\mathcal{A}_{m_i}^{W_i}$ символом $\mathcal{H}_i$. Нехай h_i — автоматна підстановка, визначена в ініціальному стані автомата $\mathcal{H}_i$.

Лема 3.12. *Автоматна підстановка h_i є жорсткими розширеннями своєї дії на словах довжини $d(m_i)$ і має порядок m_i.*

Доведення. Доведення випливає з Твердження 3.9. $\square$

Тепер розглянемо ініціальний автомат $\mathcal{V}_i$ як послідовне з'єднання r автоматів:

$$\mathcal{V}_i = \mathcal{I}_{d(m_1)} \square \ldots \square \mathcal{I}_{d(m_{i-1})} \square \mathcal{H}_i \square \mathcal{I}_{d(m_{i+1})} \square \ldots \square \mathcal{I}_{d(m_r)}, \tag{3.16}$$

де $\mathcal{H}_i$ стоїть на i-тій позиції.

Нехай v_i — автоматна підстановка визначена в ініціальному стані автомата $\mathcal{V}_i$.

Лема 3.13. *Автоматна підстановка v_i є жорстким розширенням своєї дії на словах довжини d і має порядок m_i.*

Доведення. Автомат $\mathcal{I}_n, n \geq 1$ в своєму ініціальному стані визначає автоматну підстановку, яка є жорстким розширенням своєї дії на скінченних словах довжини n.

Тепер доведення випливає з Леми 3.2 і Леми 3.12. □

Розглянемо для слова $\overline{0}_{d(m_i)}$ орбіту дії групи, породженої автоматною підстановкою h_i:

$$O(\overline{0}_{d(m_i)}) = \{h_i^k(\overline{0}_d) \mid k \in \mathbb{Z}\}.$$

Для слова $\overline{0}_d$ позначимо орбіту дії групи, породженої автоматною підстановкою v_i, символом X_i.

Лема 3.14. *Має місце рівність*

$$\mathsf{X}_i = \{\overline{0}_{d(m_1)} \ldots \overline{0}_{d(m_{i-1})} u \overline{0}_{d(m_{i+1})} \ldots \overline{0}_{d(m_r)} \mid u \in O(\overline{0}_{d(m_i)})\}, \tag{3.17}$$

Доведення. Нехай u — довільне слово довжини d над X. Розглянемо його розбиття на склади, визначене послідовністю $d(m_1), \ldots, d(m_r)$:

$$u = u[1, d(m_1)] \ldots u[i-1, d(m_{i-1})] u[i, d(m_i)] u[i+1, d(m_{i+1})] \ldots u[r, d(m_r)].$$

Тоді

$$\begin{aligned} v_i(u) = &u[1, d(m_1)] \ldots u[i-1, d(m_{i-1})] h_i(u[i, d(m_i)]) \\ &u[i+1, d(m_{i+1})] \ldots u[r, d(m_r)]. \end{aligned} \tag{3.18}$$

Поклавши $u = \overline{0}_d$ з рівності (3.18) отримуємо потрібне твердження. □

Розглянемо d-повні автомати d-$\mathcal{I}_d$ та d-$\mathcal{V}_i$. Нехай q_1 і q_2 — ініціальні стани цих автоматів. Розглянемо підмножини стрілок

$$\{(q, u[d]) \mid \lambda_1(q, u) = q_1, q \in Q_1, u \in \mathsf{X}^d \setminus \mathsf{X}_i\},$$
$$\{(q, u[d]) \mid \lambda_2(q, u) = q_2, q \in Q_2, u \in \mathsf{X}_i\},$$

де $u[d]$ — d-та літера слова u. Для простоти, будемо їх позначати символами $\mathsf{X}^d \setminus \mathsf{X}_i$ та X_i відповідно.

Визначимо з'єднання двох автоматів

$$\mathcal{B}_i = d\text{-}\mathcal{I}_d\, {}_{\mathsf{X}^d \setminus \mathsf{X}_i}\square_{\mathsf{X}_i} d\text{-}\mathcal{V}_i \tag{3.19}$$

Нехай $\mathcal{B}_i = \langle Q_1, \lambda_1, \mu_1 \rangle$. Ініціальним станом цього автомата буде q_1.

Розглянемо канонічний розклад L на прості множники:

$$L = \widetilde{p_1}^{\beta_1} \widetilde{p_2}^{\beta_2} \dots \widetilde{p_s}^{\beta_s}, \tag{3.20}$$

де $\widetilde{p_1}, \widetilde{p_2}, \dots, \widetilde{p_s}$ — попарно різні прості числа, $\beta_1, \beta_2, \dots, \beta_s$ — додатні цілі числа. Розглянемо для числа L та множини слів

$$W = \{\overline{0}_{\beta_1}, \overline{0}_{\beta_2}, \dots, \overline{0}_{\beta_s}\}$$

ініціальний автомат $\mathcal{A}_L^W$, визначений рівністю (3.13), над алфавітом X.

Позначимо автоматну підстановку визначену в ініціальному стані цього автомата через f. Нехай $f_i = f^{L/l_i}$.

Тоді з Твердження 3.9 прямо випливає наступна лема.

Лема 3.15. *Автоматні підстановки f та f_i мають порядки L та l_i відповідно.*

Нехай $\mathcal{F}_i = \langle Q_2, \lambda_2, \mu_2 \rangle$ — ініціальний автомат, що визначає автоматну підстановку f_i. Позначимо його ініціальний стан символом q_3.

Будемо вважати, що $Q_1 \cap Q_2 = \varnothing$. Побудуємо ініціальний автомат $\mathcal{A}_i = \langle Q, \lambda, \mu \rangle$ над алфавітом X за наступним правилом:

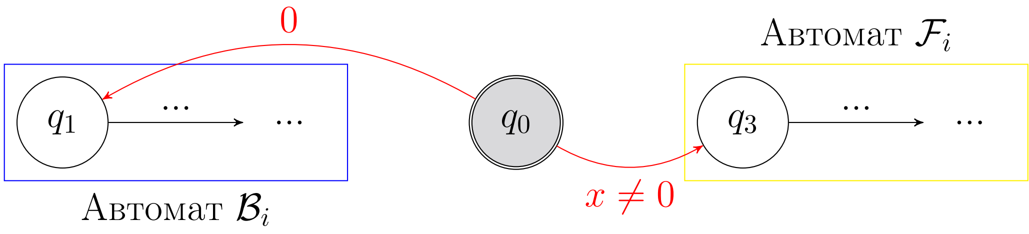


Рис. 3.7 Автомат $\mathcal{A}_i$, $1 \leq i \leq r$

- $Q = Q_1 \cup \{q_0\} \cup Q_2$, де q_0 не належить жодній з множин Q_1, Q_2;
- ініціальним станом автомата $\mathcal{A}_i$ є q_0;
- для $(q, x) \in Q \times \mathsf{X}$ функція переходів λ визначена за правилом:

$$\lambda(q,x) = \begin{cases} q_1 & \text{якщо } q = q_0, x = 0 \\ q_3 & \text{якщо } q = q_0, x \neq 0 \\ \lambda_1(q,x) & \text{якщо } q \in Q_1 \\ \lambda_2(q,x) & \text{якщо } q \in Q_2 \end{cases}; \tag{3.21}$$

- для $(q, x) \in Q \times \mathsf{X}$ функція виходів μ визначена за правилом:

$$\mu(q,x) = \begin{cases} x & \text{якщо } q = q_0 \\ \mu_1(q,x) & \text{якщо } q \in Q_1 \\ \mu_2(q,x) & \text{якщо } q \in Q_2 \end{cases}. \tag{3.22}$$

Автомат $\mathcal{A}_i$ схематично зображено на Рис. 3.7.

Твердження 3.16. *Кількість станів автомата $\mathcal{A}_i$, $1 \leq i \leq r$ дорівнює*

$$2\frac{p^d - 1}{p - 1} + \left(2\sum_{i=1}^{s} \beta_i - s\right)^{L/l_i} + 1,$$

де d, L, β_i, $1 \leq i \leq s$ визначаються з рівностей (3.14), (3.20), (3.19).

Доведення. Множина внутрішніх станів автомата $\mathcal{A}_i$ є диз'юнктним об'єднанням множин внутрішніх станів автоматів $\mathcal{F}_i$ та $\mathcal{B}_i$ і одноелементної множини. Знайдемо окремо потужності цих множин.

Автомат $\mathcal{B}_i$ є послідовним з'єднанням двох d-повних автоматів d-$\mathcal{I}_d$ та d-$\mathcal{V}_i$.

Нехай l-$\mathcal{A}$ — l-повний автомат над алфавітом X для деякого $l, l \geq 1$. Позначимо через n потужність алфавіта X. З Означення 3.6 випливає, що множина внутрішніх станів l-$\mathcal{A}$ дорівнює множині вершин n-кореневого дерева глибини $l-1$. Тому кількість станів автомата l-$\mathcal{A}$ рівна

$$\sum_{i=0}^{l-1} n^i.$$

Отже, число станів обох автоматів d-$\mathcal{I}_d$ та d-$\mathcal{V}_i$ дорівнює

$$\sum_{i=0}^{d-1} p^i.$$

З Означення 3.4 тепер прямо випливає, що множина внутрішніх станів автомата $\mathcal{B}_i$ має потужність

$$2\sum_{i=0}^{d-1} p^i.$$

З Твердження 3.8 і визначення автомата $\mathcal{F}_i$ як автомата, що задає степінь автоматної підстановки випливає, що множина внутрішніх станів автомата $\mathcal{F}_i$ має потужність

$$\left(2\sum_{i=1}^{s} \beta_i - s\right)^{L/l_i}.$$

Таким чином, кількість станів автомата $\mathcal{A}_i$ дорівнює

$$2\sum_{i=0}^{d-1} p^i + \left(2\sum_{i=1}^{s} \beta_i - s\right)^{L/l_i} + 1 = 2\frac{p^d-1}{p-1} + \left(2\sum_{i=1}^{s} \beta_i - s\right)^{L/l_i} + 1.$$

Твердження доведено. □

Зауважимо, що автомат $\mathcal{A}_i$, $1 \leq i \leq r$ не є мінімізованим, тобто не є автоматом з мінімальною кількістю станів, автоматні підстановки визначені в яких будуть ті самі. Зокрема стани w_1 та w_2 автомата d-$\mathcal{V}_i$ можна ототожнити, якщо виконуються наступні умови:

- одночасно $w_1, w_2 \in \mathsf{X}_i$ або $w_1, w_2 \in \mathsf{X} \setminus \mathsf{X}_i$;
- функція виходів $\overline{\mu}$ автомата d-$\mathcal{V}_i$ в станах w_1 та w_2 визначається рівністю

$$\overline{\mu}_{w_1} = \overline{\mu}_{w_2}.$$

Також кількість станів автомата $\mathcal{F}_i$ можна зменшити.

Автоматні підстановки, визначені в станах q_0, q_1, q_2, q_3 автомата $\mathcal{A}_i$, будемо позначати символами a_i, b_i, c_i, f_i відповідно.

Лема 3.17. *Для довільних $x \in \mathsf{X}, u \in \mathsf{X}^d, w \in \mathsf{X}^\omega, n \in \mathbb{N}$ мають місце рівності:*

$$a_i^n(xw) = \begin{cases} xb_i^n(w), & \text{якщо } x = 0 \\ xf_i^n(w), & \text{якщо } x \neq 0, \end{cases} \tag{3.23}$$

$$b_i^n(uw) = \begin{cases} ub_i^n(w), & \text{якщо } u \in \mathsf{X}_i \\ uc_i^n(w), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases} \tag{3.24}$$

$$c_i^n(uw) = \begin{cases} v_i^n(u)b_i^n(w), & \text{якщо } u \in \mathsf{X}_i \\ v_i^n(u)c_i^n(w), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases} \tag{3.25}$$

Доведення. Доведемо індукцією за n.

Нехай $n = 1$. Тоді рівність (3.23) випливає з визначення автоматної підстановки a_i. З Леми 3.3, означення з'єднання автоматів і рівності (3.19) випливають рівності (3.24)-(3.25). Нехай рівності (3.23)-(3.25) виконуються для деякого $n, n \geq 1$. Перевіримо їх для $n+1$. Для довільних $x \in \mathsf{X}, u \in \mathsf{X}^d, w \in \mathsf{X}^\omega, n \in \mathbb{N}$ мають місце рівності:

$$a_i^{n+1}(xw) = \begin{cases} a_i(xb_i^n(w)), & \text{якщо } x = 0 \\ a_i(xf_i^n(w)), & \text{якщо } x \neq 0 \end{cases}$$

$$= \begin{cases} xb_i^{n+1}(w), & \text{якщо } x = 0 \\ xf_i^{n+1}(w), & \text{якщо } x \neq 0 \end{cases}$$

$$b_i^{n+1}(uw) = \begin{cases} b_i(ub_i^n(w)), & \text{якщо } u \in \mathsf{X}_i \\ b_i(uc_i^n(w)), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases}$$

$$= \begin{cases} ub_i^{n+1}(w), & \text{якщо } u \in \mathsf{X}_i \\ uc_i^{n+1}(w), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases}$$

$$c_i^{n+1}(uw) = \begin{cases} c_i(v_i^n(u)b_i^n(w)), & \text{якщо } u \in \mathsf{X}_i \\ c_i(v_i^n(u)c_i^n(w)), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases}$$

$$= \begin{cases} v_i^{n+1}(u)b_i^{n+1}(w), & \text{якщо } u \in \mathsf{X}_i \\ v_i^{n+1}(u)c_i^{n+1}(w), & \text{якщо } u \in \mathsf{X}^d \setminus \mathsf{X}_i, \end{cases}$$

Остання рівність має місце, оскільки X_i є орбітою дії групи, породженою автоматною підстановкою v_i. □

Лема 3.18. *Порядки автоматних підстановок b_i і c_i рівні m_i.*

Доведення. Доведення випливає з Леми 3.13 і рівностей (3.24)-(3.25). □

Позначимо через G_i циклічну групу, породжену автоматною підстановкою a_i:

$$G_i = \langle a_i \rangle, 1 \leq i \leq r.$$

Лема 3.19. *Циклічна група G_i має порядок рівний l_i.*

Доведення. Для доведення цього твердження, достатньо показати, що автоматна підстановка a_i має порядок l_i.

За Лемою 3.15 порядок автоматної підстановки f_i рівний l_i.

З рекурсивного зображення (3.23) випливає, що автоматна підстановка a_i^n діє тривіально на усіх нескінченних словах над алфавітом X тоді і лише тоді, коли автоматні підстановки b_i^n і f_i^n діють тривіально на усіх нескінченних словах над X. Звідси випливає, що порядок автоматної підстановки a_i рівний найменшому спільному кратному порядків автоматних підстановок b_i та f_i, тобто НСК(m_i, l_i). Оскільки $m_i \mid l_i$, то порядок a_i рівний l_i, що і доводить твердження. □

Позначимо через t скінченно автоматну підстановку, яка діє на X^ω за наступним рекурсивним правилом:

$$t(xw) = \begin{cases} xw, & \text{якщо } x = 0 \\ xf^{L/k}(w), & \text{якщо } x \neq 0, \end{cases} \tag{3.26}$$

де $x \in \mathsf{X}, w \in \mathsf{X}^\omega$.

Позначимо через H підгрупу групи $FGA(\mathsf{X})$, породжену автоматною підстановкою t.

Лема 3.20. *Підгрупа H — власна підгрупа порядку k групи G_i.*

Доведення. В Лемі 3.18 було доведено, що автоматна підстановка b_i має порядок m_i. Оскільки $l/l_i\, m_i = L/k$, з рівностей (3.23) і (3.26) і

$$f^{L/k} = (f^{L/l_i})^{m_i} = f_i^{m_i}$$

випливає, що

$$a_i^{m_i} = t.$$

З рівності

$$km_i = l_i$$

отримуємо, що автоматна підстановка $a_i^{m_i}$ має порядок k. Звідси H — це підгрупа порядку k циклічної групи G_i. Оскільки, $k < l_i$, то підгрупа H — власна. $\square$

Позначимо через B_i групу, породжену підгрупами

$$G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_r.$$

Лема 3.21. *Перетин підгруп B_i і G_i є підгрупою H.*

Доведення. З Леми 3.20 випливає, що H — це підгрупа обох груп B_i та G_i. Припустимо, що $g \in B_i \cap G_i$. Нехай

$$w = 0u\overline{0}_d w_1,$$

де $u \in \mathsf{X}^d \setminus \mathsf{X}_i$, $w_1 \in \mathsf{X}^\omega$.

При дії автоматної підстановкм v_j на слово $\overline{0}_d$ змінюється лише j-ий склад довжини $d(m_j)$. У випадку, коли

$$g \in \langle v_1, \ldots, v_{i-1}, v_i, \ldots, v_r \rangle$$

діє на $\overline{0}_d$, i-ий склад довжини $d(m_j)$ змінитися не може. Тому для $g \in B_i$ має місце

$$g(w) = 0uu_1 g_1(w_1)$$

для деякого $u_1 \in (\mathsf{X}^d \setminus \mathsf{X}_i) \cup \{\overline{0}_d\}$ і автоматної підстановки g_1.

Оскільки $g \in G_i$, для деякого $s \geq 1$, маємо

$$g(w) = a_i^s(w) = 0uv_i^s(\overline{0}_d)g_1(w_1),$$

причому $u_i = v_i^s(\overline{0}_d) \in \mathsf{X}_i$. Тому, з того, що

$$((\mathsf{X}^d \setminus \mathsf{X}_i) \cup \{\overline{0}_d\}) \cap \mathsf{X}_i = \{\overline{0}_d\}$$

маємо рівність $u_1 = \overline{0}_d$. Оскільки, порядок v_i рівний m_i, маємо, що m_i ділить s. Отже, $g \in H$. □

Доведення Теореми 3.23. Визначимо групу G як групу породжену автоматними підстановками $a_i, 1 \leq i \leq r$. Іншими словами

$$G = \langle a_1, \ldots, a_r \rangle = \langle G_1, \ldots, G_r \rangle.$$

Для доведення досить показати, що G розкладається у амальгамований вільний добуток циклічних груп порядків $l_1, \ldots, l_r$, амальгамований по циклічній підгрупі порядку k.

З Леми 3.19 і Леми 3.21, а також твердження про канонічний вигляд елементів амальгамованого вільного добутку (див. [56, с.179]) випливає, що досить довести нетривіальність добутку

$$g_n = a_{i_n}^{s_n} \ldots a_{i_1}^{s_1} h,$$

де $h \in H, h \neq e$ і $1 \leq i_1, \ldots, i_n \leq r$, $s_1, \ldots, s_n \in \mathbb{N}$, $n \geq 1$, причому $i_j \neq i_{j+1}, 1 \leq j \leq n-1$ та $m_{i_j} \not| s_j$, $1 \leq j \leq n$.

Зафіксуємо нескінченне слово $u \in \mathsf{X}^\omega$ таке, що його розбиття на склади по послідовності $\xi = \{1, d, d, \ldots\}$ має вигляд:

$$u[\xi] = 0u[2,d]u[3,d] \ldots u[n,d] \ldots,$$

де $u[2,d] \in \mathsf{X}^d \setminus \mathsf{X}_{i_1}, u[i,d] = \overline{0}_d, i \geq 3$.

Покажемо індукцією за довжиною n добутку g_n, що слово $w = g_n(u)$ має вигляд

$$w = 0u[2,d]w[3,d] \ldots w[n,d] \ldots,$$

де $w[n+2,d] \in \mathsf{X}_{i_n} \setminus \{\overline{0}_d\}$ і $w[k,d] = \overline{0}_d, k > n+2$.

Звідси випливатиме, що g_n діє на слово u нетривіально.

Нехай $n = 1$. З рівності (3.26) випливає, що $h(u) = u$. З рівностей (3.23)-(3.25) послідовно отримуємо наступні рівності

$$\begin{aligned} g_1(u) &= a_{i_1}^{s_1} h(u[\xi]) = a_{i_1}^{s_1}(0u[2,d]u[3,d]\ldots u[n,d]\ldots) = \\ &= 0u[2,d]v_{i_1}^{s_1}(u[3,d])b_{i_1}^{s_1}(\overline{0}_d\ldots) = \\ &= 0u[2,d]v_{i_1}^{s_1}(\overline{0}_d)\overline{0}_d\ldots. \end{aligned}$$

Оскільки $m_{i_1} \not| s_1$, маємо що $v_{i_1}^{s_1}(\overline{0}_d) \in \mathsf{X}_{i_1} \setminus \{\overline{0}_d\}$ і $g_1 h(u) \neq u$.

Нехай потрібне твердження доведено для деякого n, $n \geq 1$ і $g_n(u) = w$. Перевіримо його для g_{n+1}. Оскільки $w[n+2,d] \in \mathsf{X}_{i_n} \setminus \{\overline{0}_d\}$, то $w[n+2,d] \in \mathsf{X}^d \setminus \mathsf{X}_{i_{n+1}}$. Тому для g_{n+1} має місце рівність:

$$\begin{aligned} g_{n+1}(u) &= a_{i_{n+1}}^{s_{n+1}} a_{i_n}^{s_n} \ldots a_{i_1}^{s_1} h(u[\xi]) = a_{i_{n+1}}^{s_{n+1}}(w) = \\ &= a_{i_{n+1}}^{s_{n+1}}(0u[2,d]w[3,d]\ldots w[n+2,d]\overline{0}_d\overline{0}_d\ldots) = \\ &= 0u[2,d]\overline{w}[3,d]\ldots\overline{w}[n+2,d]c_{i_{n+1}}^{s_{n+1}}(\overline{0}_d\overline{0}_d\ldots) = \\ &= 0u[2,d]\overline{w}[3,d]\ldots\overline{w}[n+2,d]v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d)b_{i_{n+1}}^{s_{n+1}}(\overline{0}_d\ldots) = \\ &= 0u[2,d]\overline{w}[3,d]\ldots\overline{w}[n+2,d]v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d)\overline{0}_d\ldots, \end{aligned}$$

для деяких слів $\overline{w}[3,d]\ldots\overline{w}[n+2,d]$ довжини d над X.

Оскільки $m_{i_{n+1}} \not| s_{n+1}$, маємо що

$$v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d) \in \mathsf{X}_{i_{n+1}} \setminus \{\overline{0}_d\} \text{ і } g_n(u) \neq u.$$

Потужність алфавіту X є мінімально можливою, оскільки циклічна група простого порядку p не може бути ізоморфно занурена в групу автоматних підстановок над алфавітом потужності меншої за p.

Теорему доведено. $\square$

3.5 Автоматне занурення амальгамованого вільного добутку $p-$груп

Зафіксуємо деяке число $r \geq 2$ і просте число p.

Нехай $l_i = p^{s_i}, 1 \leq i \leq r$ і $k = p^s$ для деяких додатних цілих $s_1, \dots, s_r, s$ таких, що $1 \leq s < s_1 \leq \dots \leq s_r$.

Амальгамований вільний добуток циклічних груп порядків $l_1, \dots, l_r$ по циклічній підгрупі порядку k позначимо символом $G_p(s_1, \dots, s_r, s)$. Іншими словами, в позначеннях Розділу 3.4 маємо

$$G_p(s_1, \dots, s_r, s) = G(l_1, \dots, l_r, k).$$

Група $G_p(s_1, \dots, s_r, s)$ є зліченною резидуально скінченною p-групою ([29]). Тому вона ізоморфно занурюється в $Syl_p(GA(\mathsf{X}))$.

Покажемо, що має місце більш сильне твердження

Теорема 3.22. *Група $G_p(s_1, \dots, s_r, s)$ ізоморфно занурюється в p-$FGA(\mathsf{X})$.*

Доведення. Скористаємося конструкцією описаною в доведенні Теореми 3.10. А саме, покажемо, що автомати $\mathcal{A}_i, 1 \leq i \leq r$, котрі визначають автоматні підстановки $a_i, 1 \leq i \leq r$ є p-автоматами.

Зафіксуємо i, $1 \leq i \leq r$. Нехай $m_i = p^{s_i - s}$.

Розглянемо для числа m_i та слова $w_i = \overline{0}_{s_i - s}$ ініціальний автомат $\mathcal{A}_p^{w_i}$ над алфавітом X (див. Рис. 3.3). Автомат $\mathcal{A}_p^{w_i}$ є p-автоматом, оскільки в кожному стані його функція виходів визначається підстановкою σ_p або тотожною підстановкою. Автомати $\mathcal{I}_n, n \geq 1$ (див. Рис. 3.6), які визначають тотожну автоматну підстановку над X, є p-автоматими. З рівності (3.5) випливає, що з'єднання двох ініціальних p-автоматів є p-автоматом. Тому з'єднання автоматів V_i визначене рівністю (3.16) є p-автоматом.

З рівності (3.8) випливає, що l-повний автомат, який відповідає p-автомату для деякого $l \geq 1$, також є p-автоматом. Оскільки послідовне з'єднання автоматів є частковим випадком з'єднання автоматів, автомат $\mathcal{B}_i$, визначений рівністю (3.19), також є p-автоматом.

Розглянемо для числа $L = p^{s_1+\ldots+s_r}$ та слова $w = \overline{0}_{s_1+\ldots+s_r}$ ініціальний автомат $\mathcal{A}_p^w$ над алфавітом X (див. Рис. 3.3). Визначимо автоматну підстановку $f_i = f^{L/l_i}$, де f — автоматна підстановка визначена автоматом $\mathcal{A}_p^w$. Оскільки автомат $\mathcal{A}_p^w$ є p-автоматом, то автомат $\mathcal{F}_i$, що визначає f_i, також є p-автоматом.

Автомат $\mathcal{A}_i$ є p-автоматом, оскільки його функція виходів визначається рівністю (3.22), де μ_1 і μ_2 — функції виходів p-автоматів $\mathcal{B}_i$ та $\mathcal{F}_i$ відповідно. З Теореми 3.10 тепер відразу випливає необхідне твердження. $\square$

3.6 Випадок тривіальної амальгамації

Розглянемо групу $G(l_1, \ldots, l_r, k)$ у випадку, коли $k = 1$. В цьому випадку група $G(l_1, \ldots, l_r, k)$ має наступне представлення в термінах твірних і визначальних співвідношень:

$$G(l_1, \ldots, l_r, 1) = \langle a_1, a_2, \ldots, a_r \mid a_1^{l_1} = e, a_2^{l_2} = e, \ldots, a_r^{l_r} = e \rangle.$$

Тоді ця група розкладається у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$. Доведення Теореми 3.10 представлене в Розділі 3.4 грунтується на конструкції ініціального автомата $\mathcal{A}_i$, $1 \leq i \leq r$. Проте, у випадку $k = 1$ можна використати автомат $\mathcal{B}_i$, $1 \leq i \leq r$ (див. 3.19) з меншою кількістю внутрішніх станів. Позначення використані в подальших міркуваннях такі самі як і в доведенні Теореми 3.10. Більше того, автоматні підстановки визначені автоматом $\mathcal{B}_i$ в станах q_1, q_2 дорівнюють автоматним підстановкам b_i, c_i, визначені автоматом $\mathcal{A}_i$ в станах q_1, q_2 відповідно, $1 \leq i \leq r$.

Теорема 3.23. *Група породжена автоматними підстановками $b_1, \ldots, b_r$ розкладаєтьса у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$. Причому потужність алфавіту X, над яким визначені автоматні підстановки $b_1, \ldots, b_r$, є мінімально можливою.*

Позначимо через $\widetilde{G}$ групу породжену автоматними підстановками $b_1, \ldots, b_r$ і через $\widetilde{G}_i$ циклічні групи породжені $b_i, 1 \leq i \leq r$. Покажемо, що $\widetilde{G}$ розкладається у вільний добуток груп $\widetilde{G}_1, \ldots, \widetilde{G}_r$.

Зафіксуємо число i таке, що $1 \leq i \leq r$. Оскільки $k = 1$ виконуються рівності $l_i = m_i$. З Твердження 3.18 випливає, що автоматна підстановка b_i має порядок l_i. Отже, порядок циклічної груп $\widetilde{G}_i$ рівний l_i.

Позначимо через $\widetilde{B}_i$ підгрупу групи $\widetilde{G}$ породжену підгрупами

$$\widetilde{G}_1, \ldots, \widetilde{G}_{i-1}, \widetilde{G}_{i+1}, \ldots, \widetilde{G}_r.$$

Твердження 3.24. *Підгрупи $\widetilde{B}_i$ і $\widetilde{G}_i$ мають тривіальний перетин.*

Доведення. Припустимо, що $g \in \widetilde{B}_i \cap \widetilde{G}_i$. Нехай

$$w = u\overline{0}_d w_1,$$

де $u \in \mathsf{X}^d \setminus \mathsf{X}_i$, $w_1 \in \mathsf{X}^\omega$. Оскільки $g \in \widetilde{B}_i$, для деякого $u_1 \in \mathsf{X}^d \setminus \mathsf{Y}_i$ і автоматної підстановки g_1 ми маємо

$$g(w) = uu_1 g_1(w_1).$$

Оскільки $g \in \widetilde{G}_i$, для деякого $s \geq 1$ ми маємо

$$g(w) = b_i^s(w) = u\overline{0}_d^{\sigma_i^s} g_1(w_1).$$

Але $0^{\sigma_i^s} \in \mathsf{X}_i$. Тому з $(\mathsf{X} \setminus \mathsf{Y}_i) \cap \mathsf{X}_i = \{0\}$ ми маємо $u_1 = \overline{0}_d$. Оскільки порядок σ_i рівний l_i ми отримаємо, що l_i ділить s. Отже, $g = e$. $\square$

Доведення Теореми 3.23. Для доведення досить показати, що $\widetilde{G}$ розкладається у вільний добуток циклічних груп порядків $l_1, \ldots, l_r$.

З того, що порядок циклічної груп $\widetilde{G}_i$ рівний l_i, і Леми 3.24, а також твердження про канонічний вигляд елементів вільного добутку (див. [56, с.163]) випливає, що досить довести нетривіальність добутку

$$g_n = b_{i_n}^{s_n} \ldots b_{i_1}^{s_1},$$

де $1 \leq i_1, \ldots, i_n \leq r$, $s_1, \ldots, s_n \in \mathbb{N}$, $n \geq 1$, причому $i_j \neq i_{j+1}, 1 \leq j \leq n-1$ та $m_{i_j} \not| s_j$, $1 \leq j \leq n$.

Зафіксуємо нескінченне слово $u \in \mathsf{X}^\omega$ таке, що його розбиття на склади по послідовності $\xi = \{d, d, \ldots\}$ має вигляд:

$$u[\xi] = u[1,d]u[2,d]\ldots u[n,d]\ldots,$$

де $u[1,d] \in \mathsf{X}^d \setminus \mathsf{X}_{i_1}, u[i,d] = \overline{0}_d, i \geq 2$.

Покажемо індукцією за довжиною n добутку g_n, що слово $w = g_n(u)$ має вигляд

$$w = u[1,d]w[2,d]\ldots w[n,d]\ldots,$$

де $w[n+2,d] \in \mathsf{X}_{i_n} \setminus \{\overline{0}_d\}$ і $w[k,d] = \overline{0}_d, k > n+2$.

Звідси випливатиме, що g_n діє на слово u нетривіально.

Нехай $n = 1$. З рівностей (3.23)-(3.25) послідовно отримуємо наступні рівності

$$\begin{aligned} g_1(u) = b_{i_1}^{s_1}(u[\xi]) = b_{i_1}^{s_1}(u[1,d]u[2,d]\ldots u[n,d]\ldots) = \\ = u[1,d]v_{i_1}^{s_1}(u[2,d])b_{i_1}^{s_1}(\overline{0}_d\ldots) = \\ = u[1,d]v_{i_1}^{s_1}(\overline{0}_d)\overline{0}_d\ldots. \end{aligned}$$

Оскільки $m_{i_1} \not| s_1$, маємо що

$$v_{i_1}^{s_1}(\overline{0}_d) \in \mathsf{X}_{i_1} \setminus \{\overline{0}_d\}$$

і виконується

$$g_1(u) \neq u.$$

Нехай потрібне твердження доведено для деякого n, $n \geq 1$ і виконується рівність

$$g_n(u) = w.$$

Перевіримо її для g_{n+1}. Оскільки виконується

$$w[n+2, d] \in \mathsf{X}_{i_n} \setminus \{\overline{0}_d\},$$

то має місце

$$w[n+2, d] \in \mathsf{X}^d \setminus \mathsf{X}_{i_{n+1}}.$$

Тому для g_{n+1} має місце рівність:

$$\begin{aligned}
g_{n+1}(u) = b_{i_{n+1}}^{s_{n+1}} b_{i_n}^{s_n} \ldots b_{i_1}^{s_1}(u[\xi]) = b_{i_{n+1}}^{s_{n+1}}(w) = \\
= b_{i_{n+1}}^{s_{n+1}}(u[1, d]w[2, d] \ldots w[n+2, d]\overline{0}_d\overline{0}_d \ldots) = \\
= u[1, d]\overline{w}[2, d] \ldots \overline{w}[n+2, d]c_{i_{n+1}}^{s_{n+1}}(\overline{0}_d\overline{0}_d \ldots) = \\
= u[1, d]\overline{w}[2, d] \ldots \overline{w}[n+2, d]v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d)b_{i_{n+1}}^{s_{n+1}}(\overline{0}_d \ldots) = \\
= u[1, d]\overline{w}[2, d] \ldots \overline{w}[n+2, d]v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d)\overline{0}_d \ldots,
\end{aligned}$$

для деяких слів $\overline{w}[2, d] \ldots \overline{w}[n+2, d]$ довжини d над X.

Оскільки $m_{i_{n+1}} \not| s_{n+1}$, маємо що

$$v_{i_{n+1}}^{s_{n+1}}(\overline{0}_d) \in \mathsf{X}_{i_{n+1}} \setminus \{\overline{0}_d\}$$

і виконується

$$g_n(u) \neq u.$$

Потужність алфавіту X є мінімально можливою, оскільки циклічна група простого порядку p не може бути ізоморфно занурена в групу автоматних підстановок над алфавітом потужності меншої за p.

Теорему доведено. $\square$

3.7 Висновки до розділу

Для амальгамованих вільних добутків скінченних циклічних груп побудовано скінченні автомати над мінімально можливими алфавітами, які визначають точні скінченно автоматні зображення таких груп. Для кожного простого p розглянуто випадок амальгамованого вільного добутку циклічних p-груп. В цьому випадку показано, що відповідні амальгамовані вільні добутки допускають точні скінченно автоматні зображення скінченними автоматами, що належать до силовської p-підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

Розділ 4

Автоматні зображення HNN-розширень

В цьому розділі для довільного простого p буде визначено природний клас HNN-розширень вільних абелевих груп скінченного рангу, які діють скінченно автоматними підстановками над алфавітом X потужності p і належать до p-силовської підгрупи групи автоматних підстановок над X. Як наслідок, звідси випливатиме, що всі такі HNN-розширення є резидуально p-скінченними групами.

4.1 Групи Баумслага-Солітера і їх узагальнення

Одним з найпростіших прикладів HNN-розширень є HNN-розширення нескінченних циклічних груп. Такі групи природно виникли в контексті дослідження класу хопфових груп. Нагадаємо, що група G називається хопфовою, якщо кожен епіморфізм $G \to G$ є ізоморфізмом. В 1930-х роках була сформульована проблема існування скінченно заданих нехопфових груп ([31]). Перші приклади скінченно породжених груп з одним співвідношенням, що не є хопфовими, були знайдені в родині груп Баумслага-Солітера $BS(k, l)$. Таким чином, припущення про хопфовість кожної скінченно породженої групи з одним співвідношенням було спростовано. Ця родина груп була визначена в

1962 році в роботі [9]. Нагадаємо її означення і наведемо деякі її властивості.

Зафіксуємо ненульові цілі числа k і l, $|l| \geq k > 0$. Група

$$BS(k,l) = \langle a, t \mid ta^k t^{-1} = a^l \rangle$$

називається групою Баумслага-Солітера.

Характеризацію резидуально скінченних та p-резидуально скіченних груп Баумслага-Солітера для простого p наведено в наступних теоремах

Теорема 4.1 ([44]). *Група $BS(k,l)$ є резидуально скінченною тоді і лише тоді, коли $l = 1$ або $|l| = k$.*

Теорема 4.2 ([45]). *Група $BS(1,l)$ є резидуально p-скінченною, p — просте, тоді і лише тоді, коли $l \equiv 1$ ($mod\ p$).*

Як легко бачити з означення, групи Баумслага-Солітера є HNN-розширеннями нескінченної циклічної групи, тобто вільної абелевої групи рангу 1. Розглянемо природні узагальнення цих груп, які є HNN-розширеннями вільних абелевих груп довільного скінченного рангу.

Зафіксуємо $n \geq 1$. Нехай $M = (m_{ij})_{i,j=1}^n$ — невироджена цілочисельна матриця розміру $n \times n$. Розглянемо групу G_M

$$\langle a_1, a_2, \ldots, a_n, t \mid a_i \text{ попарно комутують, } a_i^t = a_1^{m_{1i}} a_2^{m_{2i}} \ldots a_n^{m_{ni}}, 1 \leq i \leq n \rangle.$$

З цього означення відразу випливає, що група G_M є HNN-розширенням своєї підгрупи

$$\langle a_1, a_2, \ldots, a_n \rangle,$$

яка є вільною абелевою групою рангу n.

Нехай матриця M задовольняє умовам

(A1) визначник матриці M взаємно простий з деяким натуральним числом $l > 1$;

(A2) M має нескінченний мультиплікативний порядок.

Нагадаємо, що ∞-нормою матриці M називається число

$$\|M\| = \max_{1 \le i \le n} \sum_{j=1}^{n} |m_{ij}|.$$

Нехай $\mathsf{X} = \{0, 1, \ldots, l-1\}$. Розглянемо алфавіт X^n.

Визначимо автомат $\mathcal{A}_M = \langle Q, \lambda, \mu \rangle$ над алфавітом X^n такий, що

- Q — множина цілочисельних векторів-стовпчиків розмірності n, кожна координата яких лежить у проміжку між $-\|M\|$ і $\|M\| - 1$ включно;
- $\lambda(v, x) = \mathrm{Div}(v + Mx)$, $v \in Q$, $x \in \mathsf{X}^n$, де Div позначає операцію покоординатного взяття частки від ділення на l;
- $\mu(v, x) = \mathrm{Mod}(v + Mx)$, $v \in Q$, $x \in \mathsf{X}^n$, де Mod позначає операцію покоординатного взяття остачі від ділення на l.

Теорема 4.3 ([6], [60]). *Група автомата $\mathcal{A}_M$ ізоморфна групі G_M.*

Відмітимо, що у випадку $n = 1$ матриця M — одновимірна, тобто $M = (m)$, де $m \in \mathbb{Z}$ і m не ділиться на l. Тоді група G_M — це насправді група Баумслага-Солітера $BS(1, m)$.

Наслідок 4.4 ([6]). *Група Баумслага-Солітера $BS(1, m)$ є групою деякого скінченного автомата над алфавітом з l елементів, де m та l взаємно прості.*

4.2 Достатні умови резидуальної $p-$скінченності HNN-розширень

Нехай p — просте число, $n \ge 1$.

Зафіксуємо цілочисельну матрицю $M = (m_{ij})$ розміру $n \times n$ таку, що

(B1) $m_{ii} \equiv 1 \pmod p$, $1 \le i \le n$;

(B2) m_{ij} ділиться на p при $i \neq j$, $1 \le i, j \le n$;

(B3) M має нескінченний мультиплікативний порядок.

Прикладом такої матриці є матриця з натуральними елементами, всі діагональні елементи якої рівні одиниці, а всі інші кратні p.

Лема 4.5. *Визначник матриці M взаємно простий з p.*

Доведення. Визначник матриці M можна записати у вигляді

$$\det(M) = m_{11}m_{22}\dots m_{nn} + a,$$

де a є сумою таких добутків цілих чисел, що кожен з них містить хоча б один позадіагональний елемент матриці M. З умови **(B1)** випливає, що

$$m_{11}m_{22}\dots m_{nn} \equiv 1 \pmod p.$$

З умови **(B2)** випливає, що a ділиться на p.

Отже,

$$\det(M) \equiv 1 \pmod p,$$

що і потрібно було довести. □

Лема 4.6. *Для матриці M виконується нерівність*

$$\|M\| \ge p - 1.$$

Доведення. Розглянемо два випадки.

Нехай M — не діагональна матриця. З умови **(B2)** випливає, що ненульовий елемент m_{ij} цієї матриці, який стоїть поза діагоналлю, задовольняє нерівність

$$|m_{ij}| \ge p.$$

Тому

$$\|M\| \geq p > p - 1.$$

$$|m_{ij}| \geq p - 1.$$

Тому

$$\|M\| \geq p - 1.$$

Отже, твердження леми виконується. $\square$

Адитивну групу векторного простору V позначимо символом G. Група G ізоморфна прямому добутку n циклічних груп порядку p, тобто $\mathbb{Z}_p^n$.

Лема 4.7. *1. Для довільних $v \in Q$, $x \in \mathsf{X}^n$ має місце рівність*

$$\mu_v(x) = \mathrm{Mod}(v + x). \tag{4.1}$$

2. В кожному стані $v \in Q$ автомата $\mathcal{A}_M$ функція μ_v задає природну дію деякого елемента групи G на $\mathbb{Z}_p^n$.

3. Кожен елемент групи G реалізується в деякому стані автомата $\mathcal{A}_M$.

Доведення. Зафіксуємо стан $v \in Q$.

З умов **(B1)** і **(B2)** випливає, що для $x \in \mathsf{X}^n$ мають місце наступні рівності

$$\mu_v(x) = \mathrm{Mod}(v + Mx) = \mathrm{Mod}\begin{pmatrix} v_1 + m_{11}x_1 + \sum_{j=2}^{n} m_{ij}x_j \\ \dots \\ v_n + \sum_{j=1}^{n-1} m_{ij}x_j + m_{nn}x_n \end{pmatrix} =$$

$$= \mathrm{Mod}\begin{pmatrix} v_1 + x_1 \\ \dots \\ v_n + x_n \end{pmatrix} = \mathrm{Mod}(v + x).$$

Тобто, має місце рівність (4.1).

Для $v_1, v_2 \in Q$, $x \in \mathsf{X}^n$ виконується

$$\mu_{v_2}(\mu_{v_1}(x)) = \mathrm{Mod}(v_2 + \mathrm{Mod}(v_1 + x)) =$$
$$= \mathrm{Mod}(v_2 + v_1 + x) = \mu_{v_1+v_2}(x).$$

Таким чином, в кожному стані $v \in Q$ функція виходів μ_v реалізує природну дію елемента групи G на $\mathbb{Z}_p^n$.

Для доведення третього твердження леми досить показати, що норма матриці M задовольняє нерівність

$$\|M\| \geq p - 1.$$

З Леми 4.6 і рівності (4.1) маємо, що для множини внутрішніх станів автомата $\mathcal{A}_M$ виконується вкладення $G \subset Q$ і третє твердження леми виконується. $\square$

Для довільної підстановки $\sigma \in S(\mathsf{X})$ і цілочисельного вектора $g = (g_0, \ldots, g_{n-1})$ довжини n, $n \geq 1$ визначимо автомат $\mathcal{A}(\sigma, g) = \langle Q, \lambda, \mu \rangle$ над алфавітом X наступним чином:

- $Q = \{v \mid v \in \mathsf{X}^*, |v| \leq n-1\}$, тобто Q є множиною вершин дерева $\mathcal{T}_{d,n-1}(\mathsf{X})$;
- $\lambda(v, x) = \begin{cases} vx, & \text{якщо } |v| < n-1 \\ v, & \text{якщо } |v| = n-1 \end{cases}, v \in Q, x \in \mathsf{X};$
- $\mu_v = \sigma^{g_{|v|}}$, $v \in Q$.

З визначення автомата $\mathcal{A}(\sigma, g)$ прямо випливає наступна лема

Лема 4.8. *Автомат $\mathcal{A}(\sigma, g)$ в стані Λ визначає автоматну підстановку, під дією якої слово*

$$x_1 x_2 \ldots x_n$$

над X *довжини* n *переходить у слово*

$$\sigma^{g_0}(x_1)\sigma^{g_1}(x_2)\dots\sigma^{g_{n-1}}(x_n).$$

Зафіксуємо підстановку $\sigma = (0, 1, \dots, p-1)$.

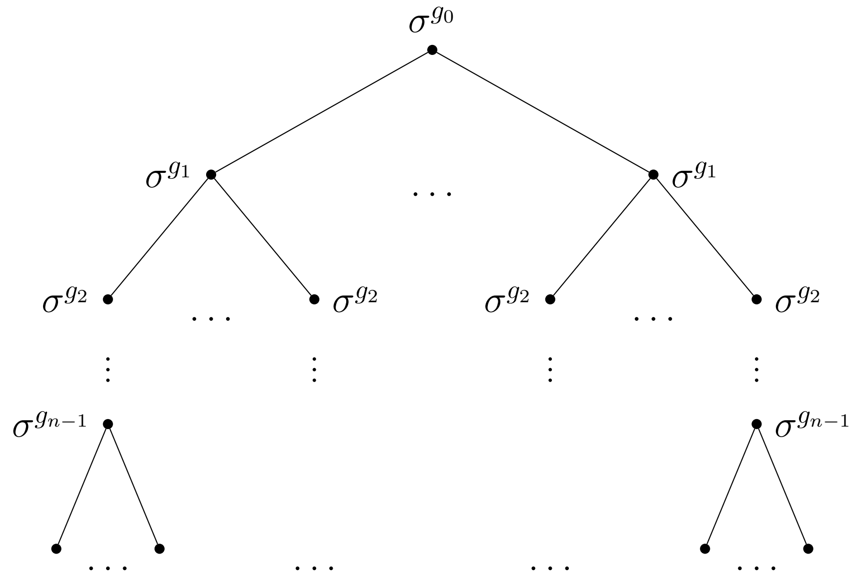


Рис. 4.1 Портрет автоматної підстановки, визначеної автоматом $\mathcal{A}(\sigma, g)$ в стані Λ

Побудуємо автомат $\mathcal{B}_M = \langle Q_\star, \lambda_\star, \mu_\star \rangle$ над алфавітом X певним чином перетворивши автомат $\mathcal{A}_M = \langle Q, \lambda, \mu \rangle$.

Для кожного стану $v \in Q$ автомата $\mathcal{A}_M$ розглянемо автомат

$$\mathcal{A}(\sigma, v) = \langle Q_v, \lambda_v, \mu_v \rangle$$

над алфавітом X (див. Рис. 4.1). Оскільки v є цілочисельним вектором довжини n, множиною станів Q_v автомата $\mathcal{A}(\sigma, v)$ є множина вершин p-кореневого дерева $\mathcal{T}_{p,n-1}(\mathsf{X})$ глибини $n-1$, тобто $\mathbb{Z}_p^{(n-1)}$.

Тепер автомат $\mathcal{B}_M$ визначається наступними рівностями

- $Q_\star = Q \times \mathbb{Z}_p^{(n-1)}$;

- $\lambda_\star((v,w),x) = \begin{cases} (v, \lambda_v(\Lambda, wx)), & \text{якщо } |w| < n-1 \\ (\lambda(v, \overline{wx}), \Lambda), & \text{якщо } |w| = n-1 \end{cases}$, $(v,w) \in Q_\star$, $x \in \mathsf{X}$;
- $\mu_\star((v,w),x) = \mu_v(w,x)$, $(v,w) \in Q_\star$, $x \in \mathsf{X}$.

Нехай H_B — це підгрупа групи автомата B_M породжена усіма автоматними підстановками, визначеними в станах вигляду (v,Λ), $v \in Q$.

Лема 4.9. *Група H_B ізоморфна G_M.*

Доведення. Розглянемо нескінченне слово $w = x_1x_2\dots x_n\dots$ над X. Слово w можна природним чином розбити на блоки довжини n:

$$\begin{aligned} w &= (x_1x_2\dots x_n)(x_{n+1}x_{n+2}\dots x_{2n})\dots(x_{kn+1}x_{kn+2}\dots x_{(k+1)n})\dots = \\ &= w[1,n]w[2,n]\dots w[k,n]\dots. \end{aligned} \tag{4.2}$$

Слово

$$\varphi(w) = y_1y_2\dots y_k\dots,$$

де $y_i = \overline{w[i,n]}, i \in \mathbb{N}$, є нескінченним словом над X^n. Легко бачити, що φ є бієкцію між множинами нескінченних слів над X та X^n.

Для кожного $v \in Q$ розглянемо стани $v, (v,\Lambda)$ автоматів $\mathcal{A}_M$ та $\mathcal{B}_M$ відповідно. Тоді в станах v та (v,Λ) визначено автоматні підстановки f_v та F_v над алфавітами X^n та X відповідно. Для доведення леми достатньо показати, що для довільного нескінченного слова w над X і довільного стану $v \in Q$ має місце рівність

$$f_v(\varphi(w)) = \varphi(F_v(w)). \tag{4.3}$$

Розпишемо кожну з частин рівності (4.3). Нескінченне слово w розіб'ємо на блоки довжини n (див. рівність (4.2)). Тоді

$$w = w[1,n]w_1$$

для деякого нескінченного слова w_1 над X.

Маємо

$$\begin{aligned} F_v(w) = F_v(w[1,n]w_1) &= \mu_\star((v,\Lambda), w[1,n])F_{\lambda(v,\overline{w[1,n]})}(w_1) \\ &= \mu_v(\Lambda, w[1,n])F_{\lambda(v,\overline{w[1,n]})}(w_1). \end{aligned}$$

За означенням автомата $\mathcal{A}_M$ стан $v \in Q$ є цілочисельним вектором

$$v = (v_0, v_1, \ldots, v_{n-1}).$$

Тому за Лемою 4.8 маємо рівність

$$\mu_v(\Lambda, w[1,n]) = \sigma^{v_0}(x_1)\sigma^{v_1}(x_2)\ldots\sigma^{v_{n-1}}(x_n).$$

Отже,

$$F_v(w) = \sigma^{v_0}(x_1)\sigma^{v_1}(x_2)\ldots\sigma^{v_{n-1}}(x_n)F_{\lambda(v,\overline{w[1,n]})}(w_1). \tag{4.4}$$

З іншого боку,

$$f_v(\varphi(w)) = f_v(\overline{w[1,n]}\varphi(w_1)) = \mu_v(\overline{w[1,n]})f_{\lambda(v,\overline{w[1,n]})}(\varphi(w_1)). \tag{4.5}$$

З Леми 4.7 випливає, що

$$\mu_v(\overline{w[1,n]}) = \mathsf{Mod}(v + \overline{w[1,n]}) = (\sigma^{v_0}(x_1), \sigma^{v_1}(x_2), \ldots, \sigma^{v_{n-1}}(x_n)). \tag{4.6}$$

Тоді з рівностей (4.4)-(4.6) випливає потрібна рівність (4.3). □

Сформулюємо основну теорему

Теорема 4.10. *Група G_M ізоморфно занурюється в p-$FGA(\mathsf{X})$.*

Доведення. За побудовою автомата $\mathcal{B}_M$ в кожному його стані реалізується підстановка на алфавіті X, що є степенем підстановки

$$\sigma = (0, 1, \ldots, p-1).$$

Тому $\mathcal{B}_M$ є p-автоматом.

Тоді за Лемою 4.9 група G_M породжується автоматними підстановками, визначеними в станах скінченного p-автомата. Звідси отримуємо твердження теореми. $\square$

4.3 Приклад резидуального $2-$скінченного HNN-розширення

Наведемо приклад матриці, для якої виконуються умови **(A1)**-**(A2)** і відповідна їй група G_M ізоморфно занурюється в p-$FGA(\mathsf{X})$. З іншого боку, покажемо, що така матриця не задовольняє набору умов **(B1)**-**(B3)**, а, отже, умови, накладені на матрицю в Теоремі 4.10, не є необхідними.

Зафіксуємо $p = 2$ і матрицю

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}.$$

Тоді

$$G_M = \langle a_1, a_2, t \mid a_1 a_2 = a_2 a_1, a_1^t = a_2, a_2^t = a_1 a_2^2 \rangle.$$

Діагональні елементи матриці M є парними числами, а тому матриця M не задовольняє умові **(B1)**.

Визначник матриці M рівний -1. Тому він взаємно простий з p і виконується умова **(A1)**.

Покажемо, що виконується умова **(A2)**, тобто матриця M має нескінченний мультиплікативний порядок. Розглянемо послідовність матриць

$$M^{n+1} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}, n \geq 0.$$

Тоді

$$\begin{aligned}
a_0 &= 0, & a_n &= c_{n-1}, \\
b_0 &= 1, & b_n &= d_{n-1}, \\
c_0 &= 1, c_1 = 2, & c_n &= c_{n-2} + 2c_{n-1}, \\
d_0 &= 2, d_1 = 5, & d_n &= d_{n-2} + 2d_{n-1}
\end{aligned}$$

Для послідовностей $c_n, d_n, n > 0$ маємо нерівності

$$c_n = c_{n-2} + 2c_{n-1} > c_{n-1}, \text{оскільки } c_0, c_1 > 0,$$
$$d_n = d_{n-2} + 2d_{n-1} > d_{n-1}, \text{оскільки } d_0, d_1 > 0.$$

Тоді $c_n, d_n, n > 0$ є зростаючими послідовностями. І звідси отримуємо необхідну властивість.

Розглянемо автомат $\mathcal{A}_M$ над алфавітом $\mathbb{Z}_2^2$, визначений для матриці M. Для $\mathcal{A}_M$ множина внутрішніх станів

$$Q = \{(v_1, v_2) \mid -3 \leq v_1, v_2 \leq 2\},$$

оскільки $\|M\| = 3$.

Для стану $v \in Q$ позначимо вектор $\mathrm{Mod}(v)$ через $\psi(v)$. Тоді функція ψ діє з множини станів Q в $\mathbb{Z}_2^2$. Для $v \in Q$, $x = (x_1, x_2) \in \mathbb{Z}_2^2$ маємо

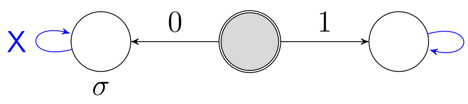
$$\mu_v(x) = \mathrm{Mod}(v + Mx) = \mathrm{Mod}\begin{pmatrix} v_1 + x_2 \\ v_2 + x_1 \end{pmatrix} = \mathrm{Mod}\left(\begin{pmatrix} x_2 \\ x_1 \end{pmatrix} + \psi(v)\right).$$

Побудуємо автомат $\mathcal{B}_M = \langle Q_\star, \lambda_\star, \mu_\star \rangle$ над алфавітом $\mathbb{Z}_2$ певним чином перетворивши автомат $\mathcal{A}_M$.

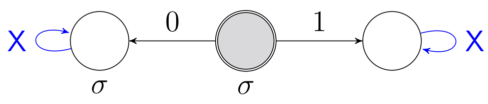
Для кожного стану $v \in Q$ розглянемо множину $Q_v = \{v\} \times \{\Lambda, 0, 1\}$. Нехай $\sigma = (0, 1)$. Визначимо автомат $\mathcal{A}(\sigma, \psi(v)) = \langle Q_v, \lambda_v, \mu_v \rangle$ над алфавітом $\mathbb{Z}_2$ діаграма Мура якого зображена на Рис. 4.2.

Тепер автомат $\mathcal{B}_M$ визначається наступними рівностями

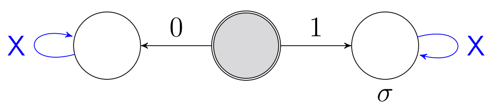
- $Q_\star = Q \times \{\Lambda, 0, 1\} = \bigcup\limits_{v \in Q} Q_v$;
- $\lambda_\star((v,w),x) = \begin{cases} (v, \lambda_v(\Lambda, x)), & \text{якщо } w = \Lambda \\ (\lambda(v, \overline{wx}), \Lambda), & \text{якщо } w \in \{0,1\} \end{cases}, \ (v,w) \in Q_\star, \ x \in \mathbb{Z}_2$;
- $\mu_\star((v,w),x) = \mu_v(w,x)$, $(v,w) \in Q_\star$, $x \in \mathbb{Z}_2$.



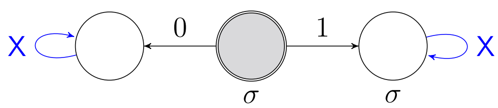
(а) Автомат $\mathcal{A}(\sigma,(0,0))$



(б) Автомат $\mathcal{A}(\sigma,(1,0))$



(в) Автомат $\mathcal{A}(\sigma,(1,1))$



(г) Автомат $\mathcal{A}(\sigma,(0,1))$

Рис. 4.2 Автомати в залежностів від значення $\psi(v)$

Нехай H_B — це підгрупа групи автомата B_M породжена усіма автоматними підстановками, визначеними в станах вигляду (v, Λ), $v \in Q$.

Покажемо, що група H_B ізоморфна G_M.

Розглянемо нескінченне слово w над $\mathbb{Z}_2$. Розіб'ємо w на блоки довжини 2:

$$\begin{aligned} w &= (x_1x_2)(x_3x_4)\ldots(x_{kn+1}x_{kn+2})\ldots = \\ &= w[1,2]w[2,2]\ldots w[k,2]\ldots. \end{aligned} \tag{4.7}$$

Визначимо функцію ν яка діє з $\mathbb{Z}_2^2$ в $\mathbb{Z}_2^2$ за правилами

$$\nu(10) = 00, \quad \nu(01) = 01, \quad \nu(00) = 10, \quad \nu(11) = 11.$$

Слово

$$\varphi(w) = y_1y_2\ldots y_k\ldots,$$

де $y_i = \overline{\nu(w[i,2])}, i \in \mathbb{N}$, є нескінченним словом над $\mathbb{Z}_2^2$. Легко бачити, що φ є бієкцію між множинами нескінченних слів над $\mathbb{Z}_2$ та $\mathbb{Z}_2^2$.

Для кожного $v \in Q$ розглянемо стани v та (v, Λ) автоматів $\mathcal{A}_M$ та $\mathcal{B}_M$ відповідно. Тоді в станах v та (v, Λ) визначено автоматні підстановки f_v та F_v над алфавітами $\mathbb{Z}_2^2$ та $\mathbb{Z}_2$ відповідно. Покажемо, що для довільного нескінченного слова w над $\mathbb{Z}_2$ і довільного стану $v \in Q$ має місце рівність

$$f_v(\varphi(w)) = \varphi(F_v(w)). \tag{4.8}$$

Розпишемо кожну з частин рівності (4.8). Нескінченне слово w розіб'ємо на блоки довжини 2 (див. рівність (4.7)). Тоді

$$w = w[1,2]w_1$$

для деякого нескінченного слова w_1 над $\mathbb{Z}_2$.

Маємо

$$\begin{aligned} F_v(w) = F_v(w[1,2]w_1) = \mu_\star((v,\Lambda), w[1,2])F_{\lambda(v,\overline{w[1,2]})}(w_1) = \\ = \mu_v(\Lambda, w[1,2])F_{\lambda(v,\overline{w[1,2]})}(w_1). \end{aligned}$$

Тоді

$$\begin{aligned} \varphi(F_v(w)) = \varphi(\mu_v(\Lambda, w[1,2])F_{\lambda(v,\overline{w[1,2]})}(w_1)) = \\ = \overline{\nu(\mu_v(\Lambda, w[1,2]))}\varphi(F_{\lambda(v,\overline{w[1,2]})}(w_1)). \end{aligned}$$

З іншого боку,

$$f_v(\varphi(w)) = f_v(\overline{\nu(w[1,2])}\varphi(w_1)) = \mu_v(\overline{\nu(w[1,2])})f_{\lambda(v,\overline{w[1,2]})}(\varphi(w_1)).$$

Оскільки $w[1,2] = x_1x_2$, лишилось показати, що

$$\overline{\nu(\mu_v(\Lambda, x_1x_2))} = \mu_v(\overline{\nu(x_1x_2)}). \tag{4.9}$$

З визначення автомату $\mathcal{A}(\sigma, u)$, $u \in \mathbb{Z}_2^2$ маємо рівність

$$\mu_v(\Lambda, x_1x_2) = \begin{cases} x_1x_2^{\sigma^{1+x_1}}, & \text{якщо } \psi(v) = (0,0) \\ x_1^{\sigma}x_2^{\sigma^{x_1}}, & \text{якщо } \psi(v) = (0,1) \\ x_1^{\sigma}x_2^{\sigma^{1+x_1}}, & \text{якщо } \psi(v) = (1,0) \\ x_1x_2^{\sigma^{x_1}}, & \text{якщо } \psi(v) = (1,1) \end{cases}.$$

Нехай $\psi(v) = (0,0)$.

Розпишемо ліву частину рівності

$$\overline{\nu(\mu_v(\Lambda, w[1,2]))} = \overline{\nu(x_1x_2^{\sigma^{1-x_1}})} =$$
$$= \begin{cases} \overline{\nu(01)}, & \text{якщо } x_1x_2 = 00 \\ \overline{\nu(00)}, & \text{якщо } x_1x_2 = 01 \\ \overline{\nu(10)}, & \text{якщо } x_1x_2 = 10 \\ \overline{\nu(11)}, & \text{якщо } x_1x_2 = 11 \end{cases}$$
$$= \begin{cases} (0,1), & \text{якщо } x_1x_2 = 00 \\ (1,0), & \text{якщо } x_1x_2 = 01 \\ (0,0), & \text{якщо } x_1x_2 = 10 \\ (1,1), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Розпишемо праву частину рівності

$$\mu_v(\overline{\nu(w[1,2])}) = \begin{cases} \mu_v((1,0)), & \text{якщо } x_1x_2 = 00 \\ \mu_v((0,1)), & \text{якщо } x_1x_2 = 01 \\ \mu_v((0,0)), & \text{якщо } x_1x_2 = 10 \\ \mu_v((1,1)), & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (0,1), & \text{якщо } x_1x_2 = 00 \\ (1,0), & \text{якщо } x_1x_2 = 01 \\ (0,0), & \text{якщо } x_1x_2 = 10 \\ (1,1), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Отже, маємо рівність (4.9) для випадку $\psi(v) = (0,0)$.

Нехай $\psi(v) = (0,1)$.

Розпишемо ліву частину рівності

$$\overline{\nu(\mu_v(\Lambda, w[1,2]))} = \overline{\nu(x_1^{\sigma} x_2^{\sigma^{x_1}})} = \begin{cases} \overline{\nu(10)}, & \text{якщо } x_1x_2 = 00 \\ \overline{\nu(11)}, & \text{якщо } x_1x_2 = 01 \\ \overline{\nu(01)}, & \text{якщо } x_1x_2 = 10 \\ \overline{\nu(00)}, & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (0,0), & \text{якщо } x_1x_2 = 00 \\ (1,1), & \text{якщо } x_1x_2 = 01 \\ (0,1), & \text{якщо } x_1x_2 = 10 \\ (1,0), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Розпишемо праву частину рівності

$$\mu_v(\overline{\nu(w[1,2])}) = \begin{cases} \mu_v((1,0)), & \text{якщо } x_1x_2 = 00 \\ \mu_v((0,1)), & \text{якщо } x_1x_2 = 01 \\ \mu_v((0,0)), & \text{якщо } x_1x_2 = 10 \\ \mu_v((1,1)), & \text{якщо } x_1x_2 = 11 \end{cases}$$
$$= \begin{cases} (0,1) + (0,1), & \text{якщо } x_1x_2 = 00 \\ (1,0) + (0,1), & \text{якщо } x_1x_2 = 01 \\ (0,0) + (0,1), & \text{якщо } x_1x_2 = 10 \\ (1,1) + (0,1), & \text{якщо } x_1x_2 = 11 \end{cases}$$
$$= \begin{cases} (0,0), & \text{якщо } x_1x_2 = 00 \\ (1,1), & \text{якщо } x_1x_2 = 01 \\ (0,1), & \text{якщо } x_1x_2 = 10 \\ (1,0), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Отже, маємо рівність (4.9) для $\psi(v) = (0,1)$.

Нехай $\psi(v) = (1,0)$.

Розпишемо ліву частину рівності

$$\overline{\nu(\mu_v(\Lambda, w[1,2]))} = \overline{\nu(x_1^{\sigma} x_2^{\sigma^{1-x_1}})} = \begin{cases} \overline{\nu(11)}, & \text{якщо } x_1x_2 = 00 \\ \overline{\nu(10)}, & \text{якщо } x_1x_2 = 01 \\ \overline{\nu(00)}, & \text{якщо } x_1x_2 = 10 \\ \overline{\nu(01)}, & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (1,1), & \text{якщо } x_1x_2 = 00 \\ (0,0), & \text{якщо } x_1x_2 = 01 \\ (1,0), & \text{якщо } x_1x_2 = 10 \\ (0,1), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Розпишемо праву частину рівності

$$\mu_v(\overline{\nu(w[1,2])}) = \begin{cases} \mu_v((1,0)), & \text{якщо } x_1x_2 = 00 \\ \mu_v((0,1)), & \text{якщо } x_1x_2 = 01 \\ \mu_v((0,0)), & \text{якщо } x_1x_2 = 10 \\ \mu_v((1,1)), & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (0,1) + (1,0), & \text{якщо } x_1x_2 = 00 \\ (1,0) + (1,0), & \text{якщо } x_1x_2 = 01 \\ (0,0) + (1,0), & \text{якщо } x_1x_2 = 10 \\ (1,1) + (1,0), & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (1,1), & \text{якщо } x_1x_2 = 00 \\ (0,0), & \text{якщо } x_1x_2 = 01 \\ (1,0), & \text{якщо } x_1x_2 = 10 \\ (0,1), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Отже, маємо рівність (4.9) для $\psi(v) = (1, 0)$.

Нехай $\psi(v) = (1, 1)$.

Розпишемо ліву частину рівності

$$\overline{\nu(\mu_v(\Lambda, w[1, 2]))} = \overline{\nu(x_1 x_2^{\sigma^{x_1}})} =$$
$$= \begin{cases} \overline{\nu(00)}, & \text{якщо } x_1x_2 = 00 \\ \overline{\nu(01)}, & \text{якщо } x_1x_2 = 01 \\ \overline{\nu(11)}, & \text{якщо } x_1x_2 = 10 \\ \overline{\nu(10)}, & \text{якщо } x_1x_2 = 11 \end{cases}$$
$$= \begin{cases} (1, 0), & \text{якщо } x_1x_2 = 00 \\ (0, 1), & \text{якщо } x_1x_2 = 01 \\ (1, 1), & \text{якщо } x_1x_2 = 10 \\ (0, 0), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Розпишемо праву частину рівності

$$\mu_v(\overline{\nu(w[1,2])}) = \begin{cases} \mu_v((1,0)), & \text{якщо } x_1x_2 = 00 \\ \mu_v((0,1)), & \text{якщо } x_1x_2 = 01 \\ \mu_v((0,0)), & \text{якщо } x_1x_2 = 10 \\ \mu_v((1,1)), & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (0,1)+(1,1), & \text{якщо } x_1x_2 = 00 \\ (1,0)+(1,1), & \text{якщо } x_1x_2 = 01 \\ (0,0)+(1,1), & \text{якщо } x_1x_2 = 10 \\ (1,1)+(1,1), & \text{якщо } x_1x_2 = 11 \end{cases}$$

$$= \begin{cases} (1,0), & \text{якщо } x_1x_2 = 00 \\ (0,1), & \text{якщо } x_1x_2 = 01 \\ (1,1), & \text{якщо } x_1x_2 = 10 \\ (0,0), & \text{якщо } x_1x_2 = 11 \end{cases}.$$

Отже, маємо рівність (4.9) для $\psi(v) = (1,1)$.

Таким чином маємо рівність (4.8).

За побудовою автомата $\mathcal{B}_M$ в кожному його стані реалізується підстановка на алфавіті $\mathbb{Z}_2$, що є степенем підстановки $\sigma = (0,1)$. Тому $\mathcal{B}_M$ є 2-автоматом.

Група G_M породжується автоматними підстановками, визначеними в станах скінченного 2-автомата, а тому вона ізоморфно занурюється в 2-$FGA(\mathsf{X})$.

4.4 Висновки до розділу

В даному розділі розглядаються HNN-розширення вільних абелевих груп скінченного рангу, які допускають точні скінченно автоматні зображення, що належать до силовської p-підгрупи групи всіх автоматних підстановок над p-елементним алфавітом. Кожне таке розширення визначається деякою невиродженою цілочисельною матрицею M розміру $n \times n$. Наведено достатні умови на матрицю M, за яких відповідне HNN-розширення допускає шукане автоматне зображення. Як наслідок, отримано, що всі HNN-розширення вказаного вигляду є резидуально p-скінченними групами. Показано, що накладені на матрицю M не є необхідними для існування зазначених скінченно автоматних зображень.

Висновки

В дисертаційній роботі будуються точні скінченно автоматні зображення ряду скінченно породжених груп. Природною необхідною умовою для груп, які допускають такі зображення, є резидуальна скінченність. Розглядаються точні скінченно автоматні зображення для таких скінченно породжених резидуально скінченних груп, які за своєю комбінаторною структурою є близькими до вільних груп. А саме, груп, що розкладаються у вільні добутки своїх підгруп, амальгамовані вільні добутки, або є HNN-розширеннями.

У дисертаційній роботі отримано такі результати.

1. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою побудовано точні скінченно автоматні зображення. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, кожен з яких має 4 внутрішні стани.

2. Побудовано точні скінченно автоматні зображення вільних добутків скінченних циклічних груп. Автоматні підстановки, які породжують відповідні добутки, визначаються ініціальними автоматами, які мають по 2 внутрішні стани.

3. Для амальгамованих добутків скінченного числа скінченних циклічних груп, амальгамованих за циклічною підгрупою, побудовано точні скінченно автоматні зображення над мінімально можливим алфавітом.

4. Для довільного простого числа p доведено, що амальгамовані вільні добутки скінченного числа циклічних p-груп, амальгамованих за циклічною

підгрупою, зображаються скінченними автоматами спеціального вигляду. Показано, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

5. Введено клас HNN-розширень вільних абелевих груп скінченного рангу, всі групи з якого зображаються скінченно автоматними підстановками. Доведено, що відповідні автоматні підстановки належать до p-силовської підгрупи групи всіх автоматних підстановок над p-елементним алфавітом.

Список використаних джерел

[1] Abért, M., and Glasner, Y. Generic groups acting on regular trees. *Trans. Am. Math. Soc. 361*, 7 (2009), 3597–3610.

[2] Aleshin, S. V. Finite automata and Burnside's problem for periodic groups. *Math. Notes 11* (1972), 199–203.

[3] Aleshin, S. V. A free group of finite automata. *Vestn. Mosk. Univ., Ser. I 1983*, 4 (1983), 12–14.

[4] Bartholdi, L., and Sidki, S. N. Self-similar products of groups. *Groups Geom. Dyn. 14*, 1 (2020), 107–115.

[5] Bartholdi, L., and Silva, P. Groups defined by automata. In *Handbook of automata theory. Volume II. Automata in mathematics and selected applications.* Berlin: European Mathematical Society (EMS), 2021, pp. 871–911.

[6] Bartholdi, L., and Šunić, Z. Some solvable automaton groups. In *Topological and asymptotic aspects of group theory.* Providence, RI: American Mathematical Society (AMS), 2006, pp. 11–29.

[7] Baumslag, B., and Tretkoff, M. Residually finite HNN extensions. *Commun. Algebra 6* (1978), 179–194.

[8] Baumslag, G. Automorphism groups of residually finite groups. *J. Lond. Math. Soc. 38* (1963), 117–118.

[9] Baumslag, G., and Solitar, D. Some two-generator one-relator non-Hopfian groups. *Bull. Am. Math. Soc. 68* (1962), 199–201.

[10] Bhattacharjee, M. The ubiquity of free subgroups in certain inverse limits of groups. *J. Algebra 172*, 1 (1995), 134–146.

[11] Bondarenko, I., D'Angeli, D., and Rodaro, E. The lamplighter group $\mathbb{Z}_3 \wr \mathbb{Z}$ generated by a bireversible automaton. *Comm. Algebra 44*, 12 (2016), 5257–5268.

[12] Bondarenko, I., Grigorchuk, R., Kravchenko, R., Muntyan, Y., Nekrashevych, V., Savchuk, D., and Šunić, Z. On classification of groups generated by 3-state automata over a 2-letter alphabet. *Algebra Discrete Math. 2008*, 1 (2008), 1–163.

[13] Bondarenko, I. V., and Savchuk, D. M. On Sushchansky p-groups. *Algebra Discrete Math. 2007*, 2 (2007), 22–42.

[14] Brunner, A. M., and Sidki, S. The generation of $\mathrm{GL}(n, \mathbb{Z})$ by finite state automata. *Int. J. Algebra Comput. 8*, 1 (1998), 127–139.

[15] Dantas, A. C., Santos, T. M. G., and Sidki, S. N. Intransitive self-similar groups. *J. Algebra 567* (2021), 564–581.

[16] Dantas, A. C., and Sidki, S. N. On self-similarity of wreath products of abelian groups. *Groups Geom. Dyn. 12*, 3 (2018), 1061–1068.

[17] Dantas, A. C., and Sidki, S. N. On state-closed representations of restricted wreath product of groups $g_{p,d} = c_p wr c^d$. *J. Algebra 500* (2018), 335–361.

[18] Dömösi, P., and Nehaniv, C. L. *Algebraic theory of automata networks. An introduction*, vol. 11. Philadelphia, PA: Society for Industrial and Applied Mathematics (SIAM), 2005.

[19] Fedorova, M., and Oliynyk, A. Finite automaton actions of free products of groups. *Algebra Discrete Math. 23*, 2 (2017), 230–236.

[20] Gécseg, F., and Peák, I. The algebraic theory of automata. *Mat. Lapok 17* (1966), 77–134.

[21] Glushkov, V. M. The abstract theory of automata. *Russ. Math. Surv. 16*, 5 (1962), 1–53.

[22] Grigorchuk, R. I. On Burnside's problem on periodic groups. *Funct. Anal. Appl. 14* (1980), 41–43.

[23] Grigorchuk, R. I. Degrees of growth of finitely generated groups, and the theory of invariant means. *Math. USSR, Izv. 25* (1985), 259–300.

[24] Grigorchuk, R. I., Nekrashevich, V. V., and Sushchanskii, V. I. Automata, dynamical systems, and groups. In *Dynamical systems, automata, and infinite groups. Transl. from the Russian.* Moscow: MAIK Nauka/Interperiodica Publishing, 2000, pp. 128–203.

[25] Grigorchuk, R. I., and Żuk, A. The lamplighter group as a group generated by a 2-state automaton, and its spectrum. *Geom. Dedicata 87*, 1-3 (2001), 209–244.

[26] Gruenberg, K. W. Residual properties of infinite soluble groups. *Proc. Lond. Math. Soc. (3) 7* (1957), 29–62.

[27] Gupta, C. K., Gupta, N. D., and Oliynyk, A. S. Free products of finite groups acting on regular rooted trees. *Algebra Discrete Math. 2007*, 2 (2007), 91–103.

[28] GUPTA, N., AND SIDKI, S. Some infinite p-groups. *Algebra Logic 22* (1983), 421–424.

[29] HIGMAN, G. Amalgams of p-groups. *J. Algebra 1* (1964), 301–305.

[30] HIGMAN, G., NEUMANN, B. H., AND NEUMANN, H. Embedding theorems for groups. *J. Lond. Math. Soc. 24* (1950), 247–254.

[31] HOPF, H. Beiträge zur Klassifizerung der Flächenabbildungen. *J. Reine Angew. Math. 165* (1931), 225–236.

[32] IWASAWA, K. Einige Sätze über freie Gruppen. *Proc. Imp. Acad. Tokyo 19* (1943), 272–274.

[33] KALOUJNINE, L. Sur le groupe P_∞ des tableaux infinis. *C. R. Acad. Sci., Paris 224* (1947), 1097–1099.

[34] KIM, G., LEE, Y., AND MCCARRON, J. Residual p-finiteness of certain generalized free products of nilpotent groups. *Kyungpook Mathematical Journal 48*, 3 (2008), 495–502.

[35] KIM, G., AND MCCARRON, J. On amalgamated free products of residually p-finite groups. *J. Algebra 162*, 1 (1993), 1–11.

[36] KIM, G., AND MCCARRON, J. Some residually p-finite one relator groups. *J. Algebra 169*, 3 (1994), 817–826.

[37] KIM, G., AND TANG, C. Y. On generalized free products of residually finite p-groups. *J. Algebra 201*, 1 (1998), 317–327.

[38] KLIMANN, I., PICANTIN, M., AND SAVCHUK, D. A connected 3-state reversible Mealy automaton cannot generate an infinite Burnside group. In *Developments in language theory. 19th international conference, DLT*

2015, Liverpool, UK, July 27–30, 2015. Proceedings. Cham: Springer, 2015, pp. 313–325.

[39] Kochloukova, D. H., and Sidki, S. N. Self-similar groups of type FP_n. *Geom. Dedicata 204* (2020), 241–264.

[40] Lavrenyuk, Y., Mazorchuk, V., Oliynyk, A., and Sushchansky, V. Faithful group actions on rooted trees induced by actions of quotients. *Commun. Algebra 35*, 11 (2007), 3759–3775.

[41] Lyndon, R. C., and Schupp, P. E. *Combinatorial group theory*, vol. 89. Springer-Verlag, Berlin, 1977.

[42] Mal'tsev, A. I. On isomorphic matrix representations of infinite groups. *Rec. Math. Moscou, n. Ser. 8* (1940), 405–422.

[43] McKinsey, J. C. C. The decision problem for some classes of sentences without quantifiers. *J. Symb. Log. 8* (1943), 61–76.

[44] Meskin, S. Nonresidually finite one-relator groups. *Trans. Am. Math. Soc. 164* (1972), 105–114.

[45] Moldavanskii, D. Residuality by a finite p-groups of hnn-extensions. *Vestnik Ivanovo State Univ. 3* (2000), 129–140.

[46] Moldavanskii, D. On the residual properties of Baumslag-Solitar groups. *Commun. Algebra 46*, 9 (2018), 3766–3778.

[47] Mostowski, A. W. On the decidability of some problems in special classes of groups. *Fundam. Math. 59* (1966), 123–135.

[48] Nekrashevych, V. *Self-similar groups.*, vol. 117. Providence, RI: American Mathematical Society (AMS), 2005.

[49] NEKRASHEVYCH, V. Palindromic subshifts and simple periodic groups of intermediate growth. *Ann. Math. (2) 187*, 3 (2018), 667–719.

[50] OLIINYK, A. S. Free products of finite groups and groups of finitely automatic permutations. *Tr. Mat. Inst. Steklova 231*, 1 (2000), 323–331. (in Russian).

[51] OLIYNYK, A., AND PROKHORCHUK, V. Amalgamated free product in terms of automata constructions. *Commun Algebra 50*, 2 (2022), 740–750.

[52] OLIYNYK, A. S. Amalgamated products of infinite cyclic groups generated by finite automata. *NaUKMA Academic Records, Physics and Mathematics Series 100* (2010), 3–6. (in Ukrainian).

[53] OLIYNYK, A. S. Finite state wreath powers of transformation semigroups. *Semigroup Forum 82*, 3 (2011), 423–436.

[54] PROKHORCHUK, V. Generation of amalgamated free products of cyclic groups by finite automata over minimal alphabet. *Theor Comput Sci 856* (2021), 151–164.

[55] PROKHORCHUK, V. On finite state automaton actions of hnn extensions of free abelian groups. *Carpathian Mathematical Publications 13*, 1 (2021), 180–188.

[56] ROBINSON, D. J. S. *A course in the theory of groups.*, vol. 80. New York, NY: Springer-Verlag, 1995.

[57] SAVCHUK, D., AND VOROBETS, Y. Automata generating free products of groups of order 2. *J. Algebra 336*, 1 (2011), 53–66.

[58] Silva, P. V., and Steinberg, B. On a class of automata groups generalizing lamplighter groups. *Int. J. Algebra Comput. 15*, 5-6 (2005), 1213–1234.

[59] Steinberg, B., Vorobets, M., and Vorobets, Y. Automata over a binary alphabet generating free groups of even rank. *Int. J. Algebra Comput. 21*, 1-2 (2011), 329–354.

[60] Šunić, Z., and Ventura, E. The conjugacy problem in automaton groups is not solvable. *J. Algebra 364* (2012), 148–154.

[61] Sushchanskij, V. I. Periodic p-groups of permutations and the unrestricted Burnside problem. *Sov. Math., Dokl. 20* (1979), 766–770.

[62] Turing, A. M. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London Mathematical Society s2-42*, 1 (1937), 230–265.

[63] von Neumann, J. First draft of a report on the EDVAC. Tech. rep., 1945.

[64] Vorobets, M., and Vorobets, Y. On a free group of transformations defined by an automaton. *Geom. Dedicata 124* (2007), 237–249.

[65] Vorobets, M., and Vorobets, Y. On a series of finite automata defining free transformation groups. *Groups Geom. Dyn. 4*, 2 (2010), 377–405.

[66] Wilson, J. S. *Profinite groups*, vol. 19. Oxford: Clarendon Press, 1998.

Додатки

Список публікацій за темою дисертації

1. В. А. Прохорчук. Зображення проективних спеціальних лінійних груп скінченно автоматними підстановками // Четверта всеукраїнська наукова конференція молодих вчених з математики та фізики, 23–25 квітня 2015 р., м. Київ, Україна: Матеріали конференції – 2015. – С. 65.

2. В. А. Прохорчук. Скінченно автоматне зображення групи $GL(2, \mathbb{Z})$ // International mathematical conference "Groups and Actions: Geometry and Dynamics" dedicated to the memory of professor Vitaly Sushchanskyy, December 19–22, 2016. // Taras Shevchenko National University of Kyiv – 2016. – С. 69.

3. В. А. Прохорчук. Скінченно автоматне зображення групи $GL(3, \mathbb{Z})$ // Матеріали XV Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених "Шевченківська весна – 2017". – 2017. – С. 73-–75.

4. В. А. Прохорчук. Декомпозиція автоматів і елементарні матриці // Шоста всеукраїнська наукова конференція молодих вчених з математики та фізики, 21–22 квітня 2017 р., м. Київ, Україна: Матеріали конференції // Національний університет "Києво-Могилянська академія" – 2017. – С. 67.

5. В. А. Прохорчук. Моделювання дії автоматів на базі представлення матриць // XV Всеукраїнська науково-практична конференція студентів,

аспірантів та молодих вчених "Теоретичні та прикладні проблеми фізики, математики та інформатики", 25–27 травня 2017 р., м. Київ, Україна: Матеріали конференції // Національний технічний університет України "Київський політехнічний інститут імені Ігоря Сікорського", Фізико-технічний інститут – КПІ ім. Ігоря Сікорського Видавництво "Політехніка" – 2017. – Том II – С. 62–64.

6. Prokhorchuk V. A. Automata that generate metabelian groups // 11th International Algebraic Conference in Ukraine dedicated to the 75th anniversary of V.V. Kirichenko, July 3–7, 2017, Kyiv, Ukraine: Book of Abstracts // Institute of Mathematics of NAS of Ukraine, 2017 – P. 106.

7. В. А. Прохорчук. Скінченно-автоматні розширення групи Баумслага-Солітера // Міжнародна наукова конференція "Сучасні проблеми механіки та математики" присвячена 90-річчю від дня народження академіка НАН України Ярослава Степановича Підстригача та 40-річчю створеного ним Інституту прикладних проблем механіки і математики НАН України, 22–25 травня 2018 р., м. Львів, Україна: Матеріали конференції – Львів – 2018. – Том III – С. 229. – Режим доступу до ресурсу: www.http://www.iapmm.lviv.ua/mpmm2018.

8. Prokhorchuk V. A. Amalgamated free products of finite cyclic groups and finite automata // The conference dedicated to the 60th anniversary of the algebra department of Kyiv University, July 14—17, 2020, Kyiv, Ukraine: Book of Abstracts // Taras Shevchenko National University of Kyiv – 2020. – P. 67. https://sites.google.com/view/kyiv-algebra60

9. Prokhorchuk V. Finite state automaton actions of HNN extensions of free abelian groups // The 13th International Algebraic Conference in Ukraine,

July 6–9, 2021, Kyiv, Ukraine: Book of Abstracts // Taras Shevchenko National University of Kyiv – 2021. – P. 67. https://sites.google.com/view/iacu

10. A. Oliynyk, V. Prokhorchuk. Amalgamated free product in terms of automata constructions // Communications in Algebra, Vol 50. No. 2, P. 740–750, 2022. doi: 10.1080/00927872.2021.1967965.

11. V. Prokhorchuk. On finite state automaton actions of HNN extensions of free abelian groups // Carpathian Mathematical Publications, Vol. 13, No. 1, P. 180–188, 2021. doi: 10.15330/cmp.13.1.180-188

12. V. Prokhorchuk. Generation of amalgamated free products of cyclic groups by finite automata over minimal alphabet // Theoretical Computer Science, Vol. 856, 2021, P. 151–164, isn: 0304-3975, doi: 10.1016/j.tcs.2020.12.036.