Зміст

Вступ

Протягом останніх двадцяти років автору доводилось читати різні комбінаторні спецкурси на факультеті кібернетики та механіко-математичному факультеті Київського університету, а останні п'ять років ще й курс комбінаторики для магістрів. Цей курс нетрадиційний своєю калейдоскопічністю: кожна лекція-дві висвітлює деякий напрямок або істотний його фрагмент сучасної комбінаторики і різні лекції досить незалежні, причому в кожній лекції доводяться з нуля кілька нетривіальних, часто центральних результатів відповідного напрямку. Текст, що ви тримаєте в руках,- це майже стенографічний відбиток цього курсу. Вимоги до математичної підготовки читача досить скромні і читати нариси можна в будь-якому з 17! можливих порядків. Досить поширене (навіть серед викладачів, що читають курси дискретної математики) переконання, що комбінаторика — це наука про підрахунки деяких варіантів, кофігурацій тощо. Це й не дивно, адже через брак вітчизняної (і важкодоступність зарубіжної) літератури з комбінаторики обізнаність багатьох читачів з її предметом обмежується біномними коефіцієнтами та принципом Діріхле. Марна й непотрібна справа намагатися визначити, що таке комбінаторика. Проте навіть поверховий аналіз вашого математичного багажу може підтвердити таку тезу: в багатьох нетривіальних твердженнях з різних математичних дисциплін вирішальним є деякий "комбінаторний"аргумент. Звичайно цю тезу не слід радикалізувати до “математика=комбінаторика”, хоча щось у цьому є. В цих нарисах перевага віддається комбінаториці понять (чи ідей) перед комбінаторикою обчислень-оцінок. Деякі з них списано з відповідних джерел, вказаних в кінці нарисів (як от "Комбінаторика в соціальному виборі"), деякі є творчістю автора (як от "Циклічні вимірювання і решітки"), переважна більшість є сплавом цих двох підходів, а всі відображають власні уподобання автора в комбінаториці. Сподіваюся, що не тільки студенти, але й маститі фахівці знайдуть для себе дещо цікаве і нове в цих нарисах. Автор висловлює щиру вдячніс Ігорю Зарічному за комп'ютерний набір тексту, а також Євгену Луценку і Олександру Петренку за його корекцію.

0.1. Комбінаторика гіперграфів

Нехай X — множина, $\mathcal{F}$ — деяка сім'я різних підмножин множини X. Пара $(X, \mathcal{F})$ називається *гіперграфом* з множиною *вершин* X і множиною *гіперребер* $\mathcal{F}$. Гіперграф називається k-*однорідним* (k-деякий кардинал), якщо $|F| = k$ для всіх $F \in \mathcal{F}$.

Гіперграф $(X, \mathcal{F})$ називається *шпернеровим,* якщо жодне з його гіперребер не міститься в іншому. Наприклад, якщо $X = \{1, \ldots, n\}, k \in \{0, \ldots, n\}$, а $\mathcal{F}_k$ —сім'я усіх k-підмножин X, то гіперграф $(X, \mathcal{F}_k)$ шпернерів, а потужність $|\mathcal{F}_k|$ дорівнює біномному кеофіцієнту $\left(\begin{array}{c} n \\ k \end{array}\right)$. Зауважимо, що найбільший з біномних коефіцієнтів $\left(\begin{array}{c} n \\ k \end{array}\right)$ при фіксованому n є числа $\left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array}\right), \left(\begin{array}{c} n \\ \lceil \frac{n}{2} \rceil \end{array}\right)$. Для дійсного числа x через $\lfloor x \rfloor$ та $\lceil x \rceil$ позначається відповідно найближче зліва та найближче справа до x ціле число.

Теорема 0.1.1 (Шпернера). *Якщо* $X = \{1, \ldots, n\}$ *і* $(X, \mathcal{F})$ *— шпернерів гіперграф, то*

$$|\mathcal{F}| \leq \left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array}\right).$$

Доведення. Спочатку ми доведемо таку нерівність Ямамото

$$\sum_{A \in \mathcal{F}} \left(\begin{array}{c} n \\ |A| \end{array}\right)^{-1} \leq 1.$$

Для кожної підмножини $A \subseteq \{1, \ldots, n\}$ позначимо через $P(A)$ сукупність усіх перестановок чисел $\{1, \ldots, n\}$, початковий відрізок яких утворюють елементи підмножини A. Число цих перестановок $|A|!(n - |A|)!$. Умова Шпернера рівносильна тому, що множини $P(A)$, $A \in \mathcal{F}$ попарно не перетинаються. Отже,

$$\sum_{A \in \mathcal{F}} |A|!(n - |A|)! \leq n!$$

Скористаємося нерівністю Ямамото. Оскільки

$$\left(\begin{array}{c} n \\ |A| \end{array} \right) \leq \left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array} \right),$$

то число доданків не первищує $\left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array} \right)$. □

Зауважимо, що границя в теоремі Шпернера досягається лише не гіперграфах $(X, \mathcal{F}_k)$ при $k = \lfloor \frac{n}{2} \rfloor$ і $k = \lceil \frac{n}{2} \rceil$.

Як застосування тереми Шпернера ми розглянемо таку задачу Спенсера: n студентів вирішили провідати один одного. За один вечір студент може зробити кілька візитів, але в той вечір, коли до нього мають прийти гості, він нікого не відвідує. Позначимо через $f(n)$ мінімальну кількість вечорів, необхідних для того, щоб кожен студент відвідав іншого. Стверджується, що

$$f(n) = \min\{m : \left(\begin{array}{c} m \\ \lfloor \frac{m}{2} \rfloor \end{array} \right) \geq n\}.$$

Припустімо, що складено програму відвідувань на m вечорів, що задовольняє умову задачі. Співставимо i-му студенту підмножину $X_i \subseteq \{1, \ldots, m\}$ за таким правилом: $k \in X_i$ тоді і тільки тоді, коли k-того вечора i-ий студент залишається вдома. Одержимо шпернерову сім'ю підмножин $X_1, \ldots, X_n$. Дійсно, якщо припустити, що $X_i \subset X_j$, то j-ий студент не відвідає i-го студента. За теоремою Шпернера, $n \leq \left(\begin{array}{c} m \\ \lfloor \frac{m}{2} \rfloor \end{array} \right)$. З іншого боку, якщо $\left(\begin{array}{c} m \\ \lfloor \frac{m}{2} \rfloor \end{array} \right) \geq n$, ми виберемо $\lfloor \frac{m}{2} \rfloor$-підмножин

$X_1, \ldots, X_n$ множини $\{1\ldots, m\}$. Програму візитів i-го визначимо так: якщо $k \in X_i$, то k-го вечора студент залишається вдома, а якщо $k \notin X_i$ — він відвідує усіх студентів, що того вечора залишились вдома.

Лінійно впорядкована підмножина частково впорядкованої множини $(P, \geq)$ називається *ланцюгом*, а підмножина, в якій жодні два різні елементи x, y не знаходяться у відношеннях $x \leq y$ або $y \leq x$, називається *антиланцюгом.* Кожен гіперграф $(X, \mathcal{F})$ визначає частково впорядковану множину $(\mathcal{F}, \supseteq)$. Очевидно, що підмножина $\mathcal{F}' \subseteq \mathcal{F}$ є антиланцюгом тоді і тільки тоді, коли гіперграф $(X, \mathcal{F}')$ шпернерів.

ТЕОРЕМА 0.1.2 (Дилвортса). *Для довільної скінченної частково упорядкованої множини $(P, \geq)$ мінімальне число ланцюгів, що загалом покривають P дорівнює максимальній з потужностей антиланцюгів в P.*

ДОВЕДЕННЯ. Якщо A — антиланцюг в P, то кожен ланцюг в P може містити щонайбільше один елемент з A. Отже, якщо деяка сукупність $\mathcal{L}$ ланцюгів покриває P, то $|\mathcal{L}| \geq |A|$.

Нехай A — максимальний за потужністю антиланцюг в P, $|A| = m$. Ми покажемо, що P можна покрити m ланцюгами. Застосуємо індукцію по числу $|P|$. Для $|P| = 1$ теорема очевидна. Нехай $|P| > 1$, L — максимальний за включенням ланцюг в P. Після видалення L з P одержуємо частково впорядковану множину $(P \setminus L, \geq)$. Нехай m' — максимальна з потужностей антиланцюгів в $P \setminus L$. Очевидно, що $m' = m - 1$ або $m' = m$. Якщо $m' = m - 1$, то за припущенням індукції $P \setminus L$ можна покрити ланцюгами $L_1, \ldots, L_{m-1}$, значить, $P = L_1 \cup \cdots \cup L_{m-1} \cup L$. Залишилось розглянути випадок $m' = m$. Нехай $A = \{a_1, \ldots, a_m\}$ — антиланцюг в $P \setminus L$. Позначимо

$$U = \{x \in P : x \geq a_i \text{ для деякого } a_i \in A\}$$

$$D = \{x \in P : x \leq a_i \text{ для деякого } a_i \in A\}$$

Нехай ланцюг L має вигляд $l_1 < \cdots < l_k$. Тоді $l_1 \in U$, бо інакше ланцюг L можна продовжити деяким елементом $a_i < l_i$. Аналогічно, $l_k \notin D$. Отже $|U| < |P|$, $|D| < |P|$. Застосуємо припущення індукції до множин $(U, \geq)$, $(D, \geq)$ і покриємо U та D ланцюгами

$$U = U_1 \cup \cdots \cup U_m, \quad D = D_1 \cup \cdots \cup D_m.$$

Оскільки кожен елемент a_i належить деякому ланцюгу U_s і деякому ланцюгу D_t, змінюючи нумерацію ланцюгів, ми можемо вважати, що $a_i \in U_i \cap D_i$ для всіх $i \in \{1, \ldots, m\}$. Очевидно, що $U \cup D = P$, бо існування елементу $b \in P \setminus (U \cup D)$ суперечить максимальності A в P. Позначимо $L_i = U_i \cup D_i$. Очевидно, що L_i — ланцюг і $P = L_1 \cup \cdots \cup L_m$. □

З теорем Шпернера та Дилвортса випливає такий наслідок: якщо $(X, \mathcal{F})$ — скінченний гіперграф, $|X| = n$, то X можна покрити $\leq \left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array} \right)$ ланцюгами, що містяться в $\mathcal{F}$.

Два гіперграфи $(X_1, \mathcal{F}_1)$, $(X_2, \mathcal{F}_2)$ назвемо $\cup$-*ізоморфними,* якщо існує бієкція $f : \mathcal{F}_1 \to \mathcal{F}_2$, така що

$$\cup \mathcal{F}' = X_1 \Leftrightarrow \cup f(\mathcal{F}') = X_2$$

для будь-якої підмножини $\mathcal{F}' \subseteq \mathcal{F}$.

ТЕОРЕМА 0.1.3 (про $\cup$-ізоморфізм). *Для кожного гіпрерграфу $(X, \mathcal{F})$ зі скінченним числом гіперребер $|\mathcal{F}| = n$ знайдеться $\cup$-ізомофний гіперграф з числом вершин $\leq \left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array} \right)$.*

ДОВЕДЕННЯ. Нехай $\mathcal{F} = \{F_1, \ldots F_n\}$. Кожній вершині $x \in X$ співставимо вектор $a_x = (\alpha_1, \ldots, \alpha_n)$, де $\alpha_i = 1$, якщо $x \in F_i$ і $\alpha_1 = 0$ якщо $x \notin F_i$. Множину усіх таких векторів позначимо через P. Кожен вектор з P можна розглядати як підмножину множини $\{1,\ldots,n\}$. Як зазначалось вище, гіперграф $(\{1,\ldots,n\},P)$ можна покрити $k \leq \left(\begin{array}{c} n \\ \lfloor \frac{n}{2} \rfloor \end{array} \right)$ ланцюгами $L_1,\ldots,L_k$. Нехай $a_{x_1},\ldots,a_{x_k}$ — мінімальні елементи цих ланцюгів. Позначимо $Y=\{x_1,\ldots,x_k\}$, $\mathcal{T}=\{F_1\cap Y,\ldots,F_n\cap Y\}$ і переконаймося в тому, що відображення $F_i \mapsto F_i\cap Y$ є $\cup$-ізоморфізмом між $(X,\mathcal{F})$ та $(Y,\mathcal{T})$.

Нехай $\mathcal{F}'\subseteq\mathcal{F}$ і $\mathcal{F}'$ покриває вершини $x_1,\ldots,x_k$, тобто $\{x_1,\ldots,x_k\}\subseteq \cup\mathcal{F}'$. Досить показати, що $\cup\mathcal{F}'=X$. Для довільної вершини $x\in X$ знайдеться вершина x_i, така, що $a_x \geq a_{x_i}$. Оскільки $x_i\in\mathcal{F}$ для деякої підмножини $F\in\mathcal{F}'$, то $x\in F$. Отже $\cup\mathcal{F}'=X$. □

Теорема 0.1.4. *Нехай $A_1,\ldots,A_m$ — різні підмножини множини $\{1,\ldots,n\}$. Якщо $A_i\cap A_j\neq\emptyset$ при $i\neq j$, то $m\leq 2^{n-1}$.*

Доведення. Розглянемо сім'ю підмножин

$$A_1,\ldots,A_m,X\setminus A_1,\ldots X\setminus A_m,$$

де $X=\{1,\ldots,n\}$. За умовою теореми в цій сім'ї немає двох однакових множин, а тому $2^n\geq 2m$. Зауважимо, що границя 2^{n-1} є точною. Дійсно зафіксуємо деякий елемент множини X і розглянемо родину всіх підмножин множини X, що містять цей елемент. □

Нехай $X=\{1,\ldots,n\}$, $(X,\mathcal{F})$ — k-однорідний гіперграф. Яка найбільша потужність множини $\mathcal{F}$ за умови, що будь-які два гіперребра з $\mathcal{F}$ перетинаються? Зрозуміло, що при $k > (\ \lfloor \frac{n}{2} \rfloor \ )$ відповідь очевидна: $\left(\begin{array}{c} n \\ k \end{array} \right)$.

Теорема 0.1.5 (Ердьоша – Ко – Радо). *Якщо $(X,\mathcal{F})$ — k-однорідний гіперграф з множиною вершин $X=\{1,\ldots,n\}$, $0<$*

$k < \lfloor \frac{n}{2} \rfloor$ і будь-які два гіперребра з $\mathcal{F}$ перетинаються, то

$$|\mathcal{F}| \leq \left(\begin{array}{c} n-1 \\ k-1 \end{array} \right).$$

Доведення. Нехай $\mathcal{F}_k$ — сім'я всіх k-підмножин множини X. Кожну підмножину $F \in \mathcal{F}_k$ вважаймо k-членним клубом. Тоді $\mathcal{F}$ — це деяка частина цих клубів. Уявімо собі, що ми вирішили провести круглий стіл з учасниками $\{1, 2, \ldots, n\}$. Навколо столу розташовано n крісел. Кожне розміщення учасників за столом однозначно задається деякою підстановкою $s \in S_n$ на множині $\{1, 2, \ldots, n\}$. Отже, можливі $n!$ варіантів, Але кожен клуб наполягає на тому, щоб його члени сиділи поряд. Зрозуміло, що задовольнити вимоги усіх клубів ми не зможемо. Адже при фіксованому розміщенні гостей таких клубів буде рівно n.

Нехай $F \in \mathcal{F}_k$, $s \in S_n$. Назвімо пару (F, s) допустимою, якщо при підстановці s усі члени клубу F сидять поряд. Позначимо через Σ загальну кількість допустимих пар, а через $\Sigma(\mathcal{F})$ — кількість допустимих пар (F, s), де $F \in \mathcal{F}$. Числа Σ і $\Sigma(\mathcal{F})$ можна порахувати двома способами.

Для даного клубу позначимо через d кількість підстановок, що задовольняють його вимогу. В силу симетрії це число не залежить від вибору клубу. Отже,

$$\Sigma = d \left(\begin{array}{c} n \\ k \end{array} \right), \quad \Sigma(\mathcal{F}) = d|\mathcal{F}|.$$

З іншого боку зафіксуємо підстановку $s \in S_n$ і позначимо через $c(s, \mathcal{F}_k)$ — кількість допустимих пар (F, s), $F \in \mathcal{F}_k$, а через $c(s, \mathcal{F})$ — кількіть допустимих пар (F, s), $F \in \mathcal{F}$. Тоді $c(s, \mathcal{F}_k) = n$. Оскільки підмножини з $\mathcal{F}$ попарно перетинаються і $k \leq \lfloor \frac{n}{2} \rfloor$, то $c(s, \mathcal{F}) \leq k$. Значить, $c(s, \mathcal{F}) \leq \frac{k}{n} c(s, \mathcal{F}_k)$

і

$$\Sigma(\mathcal{F}) = \sum_{s \in S_n} c(s, \mathcal{F}) \leq \sum_{s \in S_n} \frac{k}{n} c(s, \mathcal{F}_k) = \frac{k}{n} \Sigma$$

Враховуючи, що $\Sigma = d \begin{pmatrix} n \\ k \end{pmatrix}$, $\Sigma(\mathcal{F}) = d|\mathcal{F}|$, одержуємо $|\mathcal{F}| \leq \frac{k}{n} \begin{pmatrix} n \\ k \end{pmatrix}$. □

Сім'я $\mathcal{F}$ підмножин деякої множини X називається *соняшником,* якщо $F \cap F' = \cap\mathcal{F}$ для будь-яких різних підмножин $F, F' \in \mathcal{F}$. Кожна підмножина $F \in \mathcal{F}$ називається *пелюстком,* а спільний перетин пелюсток соняшника — його серцевиною. Диз'юнктна сім'я підмножин є соняшником з порожньою серцевиною.

Теорема 0.1.6 (Ердьоша – Радо). *Нехай k, s — натуральні числа, $(X, \mathcal{F})$ — гіперграф, $|F| = k$ для кожного $F \in \mathcal{F}$. Якщо $|\mathcal{F}| > k!(s-1)^k$, то $\mathcal{F}$ містить соняшник з s пелюстками.*

Доведення. Ми застосуємо індукцію по числу k. Для $k = 1$ ми маємо сім'ю одноелементних підмножин, що містить $> s-1$ членів. А тому будь-які s підмножин цієї сім'ї утворюють соняшник з s пелюстками і порожньою серцевиною.

Для $k \geq 2$ виділимо з $\mathcal{F}$ максимальну диз'юнктну сім'ю $\mathcal{T}$. Якщо $|\mathcal{T}| \geq s$, то $\mathcal{T}$ — шуканий соняшник. Нехай $\mathcal{T} = \{T_1, \ldots, T_r\}$ і $r < s$. Позначмо $T = \bigcup_{i=1}^{r} T_i$. Тоді $|T| \leq k(s-1)$. Оскільки $\mathcal{T}$ — максимальна диз'юнктна сім'я, кожна підмножина з $\mathcal{F}$ перетинається з T. А тому існує точка $x \in T$, що міститься щонайбільше в

$$\frac{|\mathcal{F}|}{|T|} \geq \frac{k!(s-1)^k}{k(s-1)} = (k-1)!(s-1)^{k-1}$$

множинах із $\mathcal{F}$. За припущенням індукції ці підмножини містять соняшник з s пелюстками. $\square$

Гіперграфи $(X, \mathcal{F})$ та $(X', \mathcal{F}')$ назвемо $\cap$-ізоморфними, якщо існує бієкція $f : \mathcal{F} \to \mathcal{F}'$, така, що для довільних $F, F' \in \mathcal{F}$

$$F \cap F' \neq \emptyset \Leftrightarrow f(F) \cap f(F') \neq \emptyset.$$

З кожним гіперграфом $(X, \mathcal{F})$ можна пов'язати його граф перетинів з множиною вершин $\mathcal{F}$ і множиною ребер $\{(F, F') : F \neq F', \quad F \cap F' \neq \emptyset\}$. Очевидно, що два графи $\cap$-ізоморфні тоді і тільки тоді, коли їх графи перетинів ізоморфні.

Теорема 0.1.7 (про $\cap$-ізоморфізм). *Для кожного гіпергріфу $(X, \mathcal{F})$ зі скінченним числом гіперребер, $|\mathcal{F}| = k$ існує $\cap$-ізоморфний гіперграф $(X', \mathcal{F}')$ з числом вершин $\leq \left\lfloor \frac{k^2}{4} \right\rfloor$.*

Доведення. Для $k = 1, 2$ теорема очевидна. Ми припустимо, що теорему доведено для гіперграфіва з числом ребер k і доведемо її для гіперграфів з числом гіперребер $k+2$. Отже нехай $\mathcal{F} = \{X_1, \dots, X_{k+2}\}$. Якщо підмножини $X_1, \dots, X_{k+2}$ попарно не перетинаються, то $(X, \mathcal{F})$ $\cap$-ізоморфноий гіперграфу з $k+2$ вершинами і оноелементними ребрами. Отже змінюючи нумерацію ребер, можна вважати, що $X_{k+1} \cap X_{k+2} \neq \emptyset$. За припущенням індукції гіперграф $(X, \{X_1, \dots, X_k\})$ має $\cap$-ізоморфний гіперграф $(Y, \{Y_1, \dots, Y_k\})$, такий що $|Y| \leq \left\lfloor \frac{k^2}{4} \right\rfloor$. Нехай $A = \{a_1, \dots, a_{k+1}\}$ — довільна множина, що не перетинається з Y, $Z = Y \cup A$. Позначмо $Z_1 = Y \cup \{a_1\}, \dots, Z_k = Y \cup \{a_k\}$. Підмножини Z_{k+1}, Z_{k+2} множини Z ми визначимо так: $a_{k+1} \in Z_{k+1}, \quad a_{k+1} \in Z_{k+2}$ і для кожного $a_i \in \{1, \dots, k\}$ $a_i \in Z_{k+1} \Leftrightarrow X_{k+1} \cap X_i \neq \emptyset$, $a_i \in Z_{k+2} \Leftrightarrow X_{k+2} \cap X_i \neq \emptyset$, За побудовою гіперграф $(Z, \{Z_1, \ldots, Z_{k+2}\}$ $\cap$-ізоморфний гіперграфу $(X, \mathcal{F})$. Залишилося помітити, що

$$|Z| = |Y \cup A| \leq \left\lfloor \frac{k^2}{4} \right\rfloor + k + 1 = \left\lfloor \frac{(k+2)^2}{4} \right\rfloor .$$

$\square$

Вказана в теоремі границя $|\mathcal{F}'| \leq \left\lfloor \frac{k^2}{4} \right\rfloor$ є точною. Для кожного $n = 2k$ і $n = 2k + 1$ ми вкажемо гіперграф з n гіперребрами, для якого не існує $\cap$-ізоморфного гіперграфу з k^2 і $k(k+1)$ вершинами. Нехай $\Gamma(k, k)$ і $\Gamma(k, k+1)$ — повні дводольні графи. За множину вершин гіперграфу $(X_n, \{X_1, \ldots, X_n\})$ ми візьмемо множини ребер графів $\Gamma(k, k)$ і $\Gamma(k, k+1)$, а гіперребро X_i визначимо як множину усіх ребер відповідного дводольного графу, що інцидентні до його вершини i, $i \in \{1, \ldots, n\}$. Нехай гіперграф $(Y, \{Y_1, \ldots, Y_n\}$ $\cap$-ізоморфний гіперграфу $(X_n, \{X_1, \ldots, X_n\})$. Нехай долями графів $\Gamma(k, k)$ і $\Gamma(k, k+1)$ є підмножини $\{1, \ldots, k\}$, $\{k+1, \ldots, 2k\}$ і $\{1, \ldots, k\}$, $\{k + 1, \ldots, 2k + 1\}$. Для кожної пари (i, j), $i \in \{1, \ldots, k\}$, $j \in \{k + 1, \ldots, n\}$ має існувати вершина $y_{ij} \in Y_i \cap Y_j$, причому різним парам мають відповідати різні вершини. Отже, $|Y| \leq k^2$ і $|Y| \leq k(k + 1)$ відповідно до $n = k^2$ і $n = k(k + 1)$.

Досить просто показати, що для кожного графу $\mathrm{Gr}(V, E)$ існує гіперграф $(X, \mathcal{F})$, граф перетинів якого ізоморфний $\mathrm{Gr}(V, E)$. Ми можемо вважати, що граф $\mathrm{Gr}(V, E)$ зв'язний. Візьмемо за X множину E ребер графу $\mathrm{Gr}(V, E)$, а за множину $\mathcal{F}$ гіперребер множину

$$\{\{e \in E : x \in e\} : x \in V\}.$$

Якщо X — інтервал прямої $\mathbb{R}$, а $\mathcal{F}$ — деяка скінченна сукупність його підінтервалів, гіперграф $(X, \mathcal{F})$ називають *гіперграфом інтервалів*. Такі гіперграфи докладно вивачають в математичній генетиці [?]. Граф $\mathrm{Gr}(V, E)$ називають *інтервальним,* якщо він ізоморфний графу перетинів деякого гіперграфу інтервалів. Харатеризацію інтервальних графів дає теорема Гілмора-Хоффмана [?].

ТЕОРЕМА 0.1.8. *Скінченний граф $\mathrm{Gr}(V, E)$ є інтервальним тоді і тільки тоді, коли кожен його чотирикутник має діагональ, а граф $\overline{\mathrm{Gr}}$ транзитивно орієнтовний.*

Пояснімо формулювання цієї теореми. Чотирикутник в графі — це цикл v_1, v_2, v_3, v_4, а його діагоналі — це ребра v_1, v_3, та (v_2, v_4).

Граф називається транзитивно орієнтовним, якщо множину його ребер можна орієнтувати так, що для кожної пари ребер $v_1 \to v_2$, $v_2 \to v_3$ в графі існує ребро (v_1, v_3). Через $\overline{\mathrm{Gr}}$ позначимо граф з множиною вершин V і множиною ребер $(V \times V) \setminus E$.

Підмножина $Y \subseteq X$ називається *трансверсаллю* гіперграфу $(X, \mathcal{F})$, якщо $Y \cap F \neq \emptyset$ для всіх $F \in \mathcal{F}$.

ТЕОРЕМА 0.1.9. *Нехай $(X, \mathcal{F})$ — гіперграф зі скінченною множиною вершин, n — натуральне число, $n > 1$. Якщо $|\mathcal{F}| \leq 2^n - 2$ і кожне гіперребро $F \in \mathcal{F}$ містить більше половини вершин з X, то знайдеться трансверсаль $Y \subseteq X$, така що $|Y| \leq n - 1$.*

ДОВЕДЕННЯ. Ми застосуємо індукцію по числу n. Для $n = 2$ маємо $|\mathcal{F}| \leq 2$. Якщо $|\mathcal{F}| = 1$, теорема очевидна. Нехай $\mathcal{F} = \{F_1, F_2\}$. За умовою теореми $F_1 \cap F_2 \neq \emptyset$. Виберемо довільний елемент $y \in F_1 \cap F_2$ і покладемо $Y = \{y\}$.

Припустімо, що для n теорему доведено. Нехай $X = \{x_1, \dots, x_k\}$, $\mathcal{F} = \{F_1, \dots, F_m\}$, $m \leq 2^{n+1} - 2$. Визначимо матрицю $A =$

$(a_{ij})_{k\times n}$ за таки правилом

$$a_{ij} = \begin{cases} 1, & \text{якщо } x_i \in F_j, \\ -1, & \text{якщо } x_i \notin F_j. \end{cases}$$

Оскільки кожна підмножина F_j містить більше половини вершин з X, то сума елементів кожного стовпчика додатна. Отже, додатною є і сума усіх елементів матриці, а тому ми можемо вибрати рядок з деяким номером i, такий що сума усіх елементів цього рядка додатна. Це означає, що вершина x_i належить більше ніж половині гіперребер $\{F_1, \dots, F_m\}$. Гіперребер, що не містять x_i залишається $< \frac{1}{2}(2^{n+1}-2) = 2^n-1$. Оскільки число цих гіперребер $\leq 2^n-2$, за припущенням індукції існує підмножина $Z \subseteq X$, така, що $|Z| \leq n-1$ і $Z \cap F_j \neq \emptyset$ за умови $x_i \notin F_j$. Тоді $Z \cup \{x_i\}$ — шукана трансверсаль гіперграфу $(X, \mathcal{F})$. □

Нехай $(X, \mathcal{F})$ — гіперграф, $Y \subseteq X$, $f : \mathcal{F} \to Y$ — бієкція. Пару (Y, f) назвемо системою представників гіперграфу $(X, \mathcal{F})$, якщо $f(F) \in F$ для всіх $F \in \mathcal{F}$.

ТЕОРЕМА 0.1.10 (Ф. Холла). *Для скінченного гіперегрaфу $(X, \mathcal{F})$ існує система представників тоді і тільки тоді, коли $| \cup \mathcal{F}'| \geq |\mathcal{F}'|$ для всіх підмножин $\mathcal{F}' \subseteq \mathcal{F}$.*

ДОВЕДЕННЯ. Якщо (Y, f) — система представників гіперграфу $(X, \mathcal{F})$, то $f(\mathcal{F}') \subseteq \cup\mathcal{F}'$ і $|\mathcal{F}'| = |f(\mathcal{F}')| \leq | \cup \mathcal{F}'|$ для довільної підмножини $\mathcal{F}' \subseteq \mathcal{F}$.

Для доведення достатньості застосуємо індукцію по числу гіперребер $|\mathcal{F}|$. Нехай $\mathcal{F} = \{F_1, \dots, F_m\}$. Для $m = 1$ твердження очевидне. Розглянемо два випадки.

Випадок 1. Для кожної власної підмножини $\mathcal{F}' \subset \mathcal{F}$ справджується нерівність $| \cup \mathcal{F}'| > |\mathcal{F}'|$. Зафіксуємо довільний елемент $x \in F_m$. Тоді гіперграф $(X \setminus \{x\}, \{F_1 \setminus \{x\}, \dots, F_{m-1} \setminus \{x\})$

також задовольняє умову теореми і за припущенням індукції має систему представників (Y', f'). Означимо бієкцію $f : \mathcal{F} \to Y' \cup \{x\}$ за правилом $f(F_1) = f'(F_1), \dots, f(F_{m-1}) = f'(F_{m-1}), f'(F_m) = x$. Тоді $(Y' \cup \{x\}, f)$ — система представників гіперграфу $(X, \mathcal{F})$.

Випадок 2. Існує власна підмножина $\mathcal{F}' \subset \mathcal{F}$, для якої $| \cup \mathcal{F}'| = |\mathcal{F}'|$. Нехай для визначеності $\mathcal{F}' = \{F_1, \dots, F_k\}$. До гіперграфу $(X, \mathcal{F}')$ ми застосуємо припущення індукції і виберемо систему представників (Y', f'). Гіперграф $(X \setminus Y', \{F_{k+1} \setminus Y', \dots, F_m \setminus Y'\})$ теж задовольняє умову теореми, бо інакше знайдеться підмножина $\mathcal{F}'' \subseteq \{F_{k+1} \setminus Y, \dots, F_m \setminus Y\}$, для якої $| \cup \mathcal{F}''| < |\mathcal{F}''|$. Але тоді умова теореми для гіперграфу $(X, \mathcal{F})$ порушується на множині гіперребер $\mathcal{F}' \cup \{F \cup Y' : F \in \mathcal{F}''\}$. З'єднаймо систему представників (Y', f') з системою (Y'', f'') представників гіперграфу $(X \setminus Y', \{F_{k+1} \setminus Y', \dots, F_m \setminus Y'\})$ і одержимо систему представників $(Y' \cup Y'', f' \cup f'')$ гіперграфу $(X, \mathcal{F})$. □

Нехай $(X, \mathcal{F})$, $(X, \mathcal{T})$ — скінченні гіперграфи зі спільною множиною вершин і однаковим числом гіперребер
$\mathcal{F} = \{F_1, \dots, F_m\}$, $\mathcal{T} = \{T_1, \dots, T_m\}$. Якщо (Y, f) та (Y, g) — система представників гіперграфів $(X, \mathcal{F})$ та $(Y, \mathcal{F})$, то назвемо трійку (Y, f, g) — спільною ситемою представників гіперграфів $(X, \mathcal{F})$ та $(X, \mathcal{T})$. Ми доведемо, що $(X, \mathcal{F})$, $(X, \mathcal{T})$ мають спільну ситему представників тоді і тільки тоді, коли

$$|(\cup \mathcal{F}) \cap (\cup \mathcal{T}')| \leq |\mathcal{F}'| + |\mathcal{T}'| - m$$

для довільних підмножин $\mathcal{F}' \subseteq \mathcal{F}, \mathcal{T}' \subseteq \mathcal{T}$.

Нехай $X = \{x_1, \dots, x_k\}$. Можна вважати, що $X \cap \{1, \dots, m\} = \emptyset$. Розглянемо гіперграф $(X, \mathcal{H})$ з множиною вершин $H = X \cup \{1, \dots, m\}$ і множиною гіперребер $\mathcal{H} = \{F_1, \dots, F_m, H_{x_1}, \dots, H_{x_k}\}$, де

$$H_{x_i} = \{x_j\} \cup \{j \in \{1, \dots, m\} : x_j \in T_j\}.$$

Ми перевіримо, що гіперграфи $(X, \mathcal{F})$, $(X, \mathcal{T})$ мають спільну систему представників тоді і тільки тоді, коли систему представників має гіперграф $(X, \mathcal{H})$.

Нехай (Y, f, g) — спільна система представників гіперграфів $(X, \mathcal{F})$, $(X, \mathcal{T})$. Ми визначимо бієкцію $h : \mathcal{H} \to Y$ таку, що (H, h) — система представників гіперграфу $(H, \mathcal{H})$. Покладемо $h(F_i) = f(F_i)$ для всіх $i \in \{1, \ldots, m\}$. Для кожної вершини $x_i \in Y$ знайдемо $g^{-1}(x_i) = T_j$ і позначимо $h(H_{x_i}) = j$. Якщо $x_i \notin Y$, покладемо $h(H_{x_i}) = x_i$.

Навпаки, нехай (Z, h) — система представників гіперграфу $(H, \mathcal{H})$. Позначимо $Y = h(\{F_1, \ldots, F_m\})$ і покладемо $f(F_i) = h(F_i)$. Для кожної вершини $x_i \in Y$ знайдемо $h(H_{x_i}) = j$ і покладемо $g(T_j) = x_i$. Тоді (Y, f, g) — спільна система представників $(X, \mathcal{F})$ та $(X, \mathcal{T})$.

А далі до гіперграфу $(H, \mathcal{H})$ можна застосувати теорему Холла.

Доведення багатьох класичних теорем комбінаторики скінченних множин уніфікуються теоремою Форда-Фалкерсона [**5**] про максимальний потік і мінімальний розріз в мережах. Більше того, алгоритми побудови максимального потоку є базовими для багатьох ефективних комбінаторних алгоритмів.

Мережа — це скінченний орієнтований граф $N(V, E)$, в якому виділено дві вершини: *джерело* s та *стік* t, причому в джерело не заходить жодне ребро, а зі стоку не виходить жодне ребро. Кожному ребру $e \in E$ співставлено також невід'ємне дійсне число $\psi(e)$, що називається *пропускною спроможністю* цього ребра. Вважається також, що кожні дві вершини з V пов'язані неорієнтованим шляхом. Для мережі $(N(V, E), \psi)$ *потік* φ через N — це відображення множини його ребер в множину невід'ємних дійсних чисел, для якого $\varphi(e) \leq \psi(e)$ для кожного ребра $e \in E$ і для кожної вершини v відмінної від s і t сума $\sum \varphi(e)$ по всіх ребрах, що закінчуються в v дорівнює сумі $\sum \varphi(e)$ по всіх ребрах, що виходять з вершини v. Зрозуміло, що $\sum \varphi(e)$ по всіх ребрах, що виходять з джерела дорівнює сумі $\sum \varphi(e)$ по всіх ребрах, що заходять у стік. Це число називають величиною потоку φ.

Розрізом мережі (N, ψ) називають множину ребер $E' \subseteq E$, таку що кожен орієнтований шлях від s до t містить принаймні одне ребро з E'. Пропускна спроможність розрізу E' — це сума пропускних спроможностей усіх ребер, що входять до E'. Розріз мінімальної пропускної спроможності називають *мінімальним розрізом мережі.*

ТЕОРЕМА 0.1.11 (Форда-Фалкерсона). *Для кожної мережі величина будь-якого максимального потоку дорівнює пропускній спроможності мінімального розрізу.*

ДОВЕДЕННЯ. Зауважимо, що величина будь-якого потоку не перевищує пропускної спроможності будь-якого розрізу, а тому досить довести існування розрізу, пропускна спроможність якого дорівнює величині максимального потоку. Отже нехай φ — максимальний потік. Ребро e назвемо насиченим, якщо $\varphi(e) = \psi(e)$. Означимо розбиття $S \cup T$ множини вершин V: вершина $v \in V$ належить S тоді і тільки тоді, коли існує послідовність вершин $v_1, \ldots, v_k, v_1 = s, v_k = v$, така що $(v_i, v_{i+1}) \in E$ або $(v_{i+1}, v_i) \in E$ для всіх $i \in \{1, \ldots, k-1\}$, якщо $(v_i, v_{i+1}) \in E$, то це ребро насичене, а якщо $(v_{i+1}, v_i) \in E$, то потік по цьому ребру ненульовий. Зауважимо, що $s \in S$ і переконаймося, що $t \in T$. Припустимо супротивне і нехай $v_1, \ldots, v_k, v_1 = s, v_k = t$, — відповідна послідовність вершин. Виберемо $\epsilon > 0$ так, що $\epsilon \leq \psi(v_i, v_{i+1}) - \varphi(v_i, v_{i+1})$ для кожного ребра $(v_i, v_{i+1}) \in E$ і $\epsilon \leq \varphi(v_{i+1}, v_i)$ для кожного ребра $(v_{i+1}, v_i) \in E$. Якщо потік через кожне ребро першого типу збільшити на ϵ, а потік через кожне ребро другого типу зменшити на ϵ, то ми визначимо потік в N більшої величини і одержимо суперечність з максимальністю потоку φ.

Для завершення доведення позначимо через E' множину усіх ребер $(x,y) \in E$, для яких $x \in S, y \in T$. Зрозуміло, що E' — розріз. Крім того, кожне ребро $(x,y) \in E'$ насичене, бо інакше $y \in S$. Отже, пропускна спроможність розрізу E' дорівнює величині потоку φ. ☐

Спираючись на доведення теореми неважко вказати алгоритм побудови максимального потоку шляхом збільшення потоків по неорієнтовних шляхах від s до t. Про ефективність відомих алгоритмів побудови максимального потоку див. [**1, 6**]. Зауважимо, що існують алгоритми складності $O(mn(m+n))$, де $m = |v|, n = |E|$.

Поняття $\cup$-ізоморфізму та $\cap$-ізоморфізму було введено для аналізу задач про *покриття* та *пакування* скінченних гіперграфів. Нехай $(X, \mathcal{F})$ — скінченний гіперграф, $\cup\mathcal{F} = X$ і кожному гіперребру $F \in \mathcal{F}$ співставлено деяке додатне число $c(F)$ — вартість гіперребра. В задачі про покриття треба з $\mathcal{F}$ виділити підпокриття мінімальної вартості, а в задачі про пакування — виділити з $\mathcal{F}$ диз'юнктну підсистему максимальної вартості. В цій загальній постановці задачі про покриття та пакування є NP повними [**3**].

Припустимо, що гіперграф $(X, \mathcal{F})$ $\cup$-ізоморфний ($\cap$-ізоморфний) гіперграфу $(X', \mathcal{F}')$. Тоді задача про покриття (пакування) гіперграфу $(X, \mathcal{F})$ рівносильна задачі про покриття (пакування) гіперграфу $(X', \mathcal{F}')$. Нехай ми встановили $\cup$ — ізоморфізм між $(X, \mathcal{F})$ і деяким гіперграфом інтервалів $((s,t), J)$, де (s,t) — інтервал числової прямої, а J — скінченна система підінтервалів, для якої $\cup J = (s,t)$. Розглянемо граф з множиною вершин $J \cup \{s, t\}$. Два інтервали $I_1 = (s_1, t_1)$, $I_2 = (s_2, t_2)$ поєднаємо ребром, якщо $s_1 < s_2 \leq t_1 < t_2$. З'єднаємо також вершину s з усіма інтервалами з J, лівими кінцями яких є s. Аналогічно, з'єднаємо t ребрами з усіма інтервалами з J, правими кінцями яких є t. Тоді задача про покриття $((s, t), J)$ зводиться до пошуку найкоротшого шляху в побудованому графі від вершини s до вершини t. При цьому довжину ребра (s, I) треба визначити як $c(I)$, ребра (I_1, I_2) — як $c(I_2)$, а ребра (I_1, t) — як $c(I)$. Цю задачу можна ров'язати за $O(m \log n)$ кроків [**1**], де m -число вершин, а n — число ребер графу.

На завершення нарису — кілька задач і нерозв'язаних проблем.

Задача 0.1.1. Нехай $A_1, \ldots, A_n$ — різні підмножини множини $\{1, \ldots, n\}$. Доведіть, що можна видалити деякий елемент $a \in \{1, \ldots, n\}$ так, що підмножини $A_1 \setminus \{a\}, \ldots, A_m \setminus \{a\}$ також різні.

Задача 0.1.2. Перемикачі $\Pi_1, \ldots, \Pi_n$ деяким чином з'єднано з ліхтарями $\Lambda_1, \ldots, \Lambda_n$, причому кожен перемикач контролює стан ліхтаря з яким він з'єднаний. Відомо, що кожен перемикач Π_i з'єднаний з ліхтарем Λ_i, крім того, якщо Π_i з'єднаний з Λ_j, то Π_j з'єднаний з Λ_i. В початковому стані всі ліхтарі вимкнено. Довести, що деякою маніпуляцією з перемикачами можна запалити усі ліхтарі.

Задача 0.1.3. Нехай $\mathcal{P}_1, \mathcal{P}_2$ — розбиття скінченної множини X, причому всі підмножини цих розбиттів мають однакову кількість елементів. Доведіть, що гіперграфи $(X, \mathcal{P}_1)$, $(X, \mathcal{P}_2)$ мають спільну систему представників.

Задача 0.1.4. Чи існує континуальна сім'я підмножин множини натуральних чисел, лінійно впорядкована за включенням?

Задача 0.1.5. Чи існує континуальна майже диз'юнктна сім'я підмножин множини натуральних чисел? Сім'я називається майже диз'юнктною якщо перетин будь-яких двох різних її елементів скінченний.

Задача 0.1.6. Нехай k — незліченний регулярний кардинал, $(X, \mathcal{F})$ — гіперграф, $|\mathcal{F}| = k$ і всі гіперребра з $\mathcal{F}$ скінченні. Доведіть, що $\mathcal{F}$ містить соняшник з k пелюстками.

Проблема 0.1.1. Скільки різних шпернерових родин можна утворити з множини, що містить n елементів? Вказати оцінки зверху та знизу.

Проблема 0.1.2. Чи існує натуральне число c, таке що кожен k-рівномірний гіперграф $(X, \mathcal{F})$ з $|\mathcal{F}| > c^k$ обов'язково містить соняшник з трьома пелюстками.

Проблема 0.1.3. Охарактеризувати скінченні гіперграфи, $\cup$-ізоморфні гіперграфам інтервалів.

Проблема 0.1.4. Нехай k, n — натуральні числа, $k \leq n$. Два гіперграфи $(X_1, \mathcal{F}_1)$, $(X_2, \mathcal{F}_2)$ називаються $\cup_k$-ізоморфними (відповідно $\cap_k$-ізоморфними), якщо $|\mathcal{F}_1| = |\mathcal{F}_2| = n$ і існує бієкція $f : \mathcal{F}_1 \to \mathcal{F}_2$, така що для будь-якої підмножини $\mathcal{F}' \subseteq \mathcal{F}_1$, $|\mathcal{F}'| = k$, маємо $\cup\mathcal{F}' = \mathcal{F}_1$ (відповідно, $\cap\mathcal{F}' \neq \emptyset$) тоді і тільки тоді, коли $\cup f(\mathcal{F}') = \mathcal{F}_2$ (відповідно, $\cap f(\mathcal{F}') \neq \emptyset$). Позначимо через $f(k, n)$ (відповідно, $f'(k, n)$) найменше натуральне число, таке що кожен гіперграф $(X, \mathcal{F})$, $|\mathcal{F}| = n$ $\cup_k$-ізоморфний (відповідно, $\cap_k$-ізоморфний) деякому гіперграфу з числом вершин $f(k, n)$ (відповідно, $f'(k, n)$)? Неважко перевірити, що $f(k, n) \leq \left(\begin{array}{c} n \\ k \end{array} \right)$. За теоремою 1.7 про $\cap$-ізоморфізм $f'(2, n) = \lfloor \frac{n^2}{4} \rfloor$. Вказати явний вигляд (або знайти нетривіальні оцінки) функцій $f(k, n)$ та $f'(k, n)$.

Проблеми 1, 2 поставлені Ердьошом, а проблеми 3, 4 — автором в [**4**].

Бібліоґрафія

[1] Липський В. Комбинаторика для программистов. М., "Мир 1988.

[2] Микин Б. Г., Родин С. Н. Графи и гены. М. "Наука 1977.

[3] Пападимитриу Х. Стайглиц К. Комбинаторная оптимализация. М. "Мир 1985.

[4] Протасов И. В. Карты подмножеств и задачи о покрытиях и упаковках, Исследование операций и АСУ, 17 (1981), 118-122.

[5] Gilmore P. G., Hoffman A. J. F characterization of comparability graphs and of inverval graphs. Canad. J. Math. 16 (1964), 539-548.

[6] Форд Л. Р. Фалкерсон Д. Р. Потоки в сетях. М., "Мир 1966

0.2. Лінійна алгебра в комбінаториці

Задача 0.2.1. В місті з n жителями створено $n+1$ клубів $A_1, \ldots, A_{n+1}$. Довести, що знайдуться підмножини $\{i_1, \ldots, i_k\}$, $\{j_1, \ldots, j_m\}$ множини індексів, такі що

$$\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_m\} = \emptyset, \quad A_{i_1} \cup \cdots \cup A_{i_k} = A_{j_1} \cup \cdots \cup A_{j_m}.$$

Розв'язок. Якщо серед клубів є хоча б один порожній, скажімо A_i, то відповідь забезпечується підмножиною $\emptyset, \{i\}$. Отже, ми можемо вважати, що всі клуби непорожні. Занумеруємо жителів числами $1, \ldots, n$. За означенням, характеристичний вектор підмножини $A \subseteq \{1, \ldots, n\}$ — це вектор $a = (\alpha_1, \ldots, \alpha_n)$, де $\alpha_i = 1$, якщо, $i \in A$, $\alpha_i = 0$, якщо $i \notin A$ для всіх $i \in \{1, \ldots, n\}$. Ми розглянемо характеристичні вектори $a_1, \ldots, a_{n+1}$ клубів $A_1, \ldots, A_{n+1}$ як елементи векторного простору $\mathbb{R}^n$. Оскільки їх число $n+1$ більше за розмірність n прстору $\mathbb{R}$, то ситема векторів $a_1, \ldots, a_{n+1}$ лінійно залежна, а тому існує нетривіальна лінійна комбінація $\partial_1 a_1 + \cdots + \partial_{n+1} a_{n+1}$, що дорівнює нуль-вектору θ. Оскільки всі вектори $a_1, \ldots, a_{n+1}$ відмінні від θ, серед чисел $\partial_1, \ldots, \partial_{n+1}$ обов'язково мають бути як додатні, так і відємні. Після відповідного упорядкування і перепозначення ми можемо вважати, що

$$\partial_1 > 0, \ldots, \partial_r > 0, \partial_{r+1} < 0, \ldots, \partial_t < 0, \partial_{t+1} = \ldots = \partial_{n+1} = 0.$$

Якщо $i \leq r$ і $x \in A_i$, то x-координата вектора $\partial_1 a_1 + \cdots + \partial_r a_r$ більша 0. Оскільки $\partial_1 a_1 + \cdots + \partial_r a_r = -\partial_{r+1} - \cdots - \partial_t a_t$, то серед векторів $a_{r+1}, \ldots, a_t$ має бути принаймні один, скажімо a_j, x-координата якого дорівнює 1. Звідси випливає, що

$$A_1 \cup \cdots \cup A_r \subseteq A_{r+1} \cup \cdots \cup A_t.$$

Зворотнє включення переверяємо аналогічно.

Задача 0.2.2. В місті з n жителями створено m різних клубів, причому

(i) кожен клуб містить непарну кількість членів;

(ii) будь-які два різні клуби містять парну кількість спільних членів.

Довести, що $m \leq n$.

Розв'язок. Характеристичні вектори клубів $a_1, \ldots, a_m$ ми вважаємо елементами векторного простору $\mathbb{F}_2^n$, де $\mathbb{F}_2 = \{0, 1\}$ — поле з двох елементів. Для довільних векторів $a, b \in \mathbb{F}_2^n$, нехай

$$(a, b) = (\alpha_1 \beta_1 + \ldots + \alpha_n \beta_n) \operatorname{mod} 2.$$

Очевидно, що $(a, b) = 0$ тоді і тільки тоді, коли відповідні векторам a, b підмножин $A, B \subseteq \{1, \ldots, n\}$ мають парну кількість спільних членів. Досить перевірити, що вектори $a_1, \ldots, a_m$ лінійно незалежні. Припустімо, що

$$\lambda_1 a_1 + \cdots + \lambda_i a_i + \cdots + \lambda_m a_m = \theta$$

і домножимо це співвідношення на a_i. Оскільки за умовою (ii) $(a_i, a_j) = 0$ при $i \neq j$, маємо $\lambda_i(a_i, a_i) = 0$, а за умовою (i) $(a_i, a_i) = 1$ і $\lambda_i = 0$.

Зауважимо, що доведена оцінка є точною — досить взяти n одноелементних клубів.

Задача 0.2.3. В місті з n жителями створено m різних клубів, причому

(i) кожен клуб має парну кількість членів;

(ii) кожна пара різних клубів має парну кількість спільних членів

Довести, що $m \leq 2^{\lfloor \frac{n}{2} \rfloor}$ і ця оцінка є точною.

Розв'язок. Нехай $a_1, \ldots, a_m$ — характеристичні вектори клубів, M — підпростір простору $\mathbb{F}_2^n$, натягнутий на ці вектори, r — розмірність простору M. Очевидно, що $m \leq 2^r$. Нехай

A — матриця рядками якої є вектори $a_1, \dots, a_m$. Тоді ортогональне доповнення $M^\perp = \{x \in \mathbb{F}_2^n : (x, a) = 0$ для всіх $a \in M\}$ задається системою лінійних рівнянь $Ax^T = \theta$. Отже, $\dim M^\perp = n - r$. З умов задачі випливає, що $Aa_i^T = \theta$ для всіх $i \in \{1, \dots, m\}$. Значить, $M \subseteq M^\perp$, $r \leq n - r$ і $r < \lfloor \frac{n}{2} \rfloor$.

Щоб довести точність оцінки, ми можемо вважати число n парним. Розіб'ємо жителів міста на пари. Таких пар $\frac{n}{2}$, будь-яка підмножина цих пар оголошується клубом, причому умови (i) та (ii) задовільняються.

Теорема 0.2.1 (Фішера-Бозе.). *Нехай $A_1, \dots, A_m$ — різні підмножини множини $\{1, \dots, n\}$, k — ціле число, $0 < k \leq n$. Якщо $|A_i \cap A_j| = k$ для всіх $i \neq j$, то $m \leq n$.*

Доведення. Припустімо спочатку, що серед підмножин $A_1, \dots, A_m$ є підмножина, скажімо A_1, що містить рівно k елементів. Тоді підмножини $A_2 \setminus A_1, \dots, A_m \setminus A_1$ попарно не перетинаються, а тому $m - 1 \leq n - k$ і $m \leq n$.

Нехай $|A_1| = n_1, \dots, |A_m| = n_m$ і $n_i > k$ для всіх $i \in \{1, \dots, m\}$. Нехай також A — матриця, рядками якої є характеристичні вектори клубів, що розглядаються як елементи векторного простору $\mathbb{R}^n$. Очевидно, що

$$AA^T = \begin{pmatrix} n_1 & k & \dots & k \\ k & n_2 & \dots & k \\ \multicolumn{4}{c}{\dotfill} \\ k & k & \dots & n_m \end{pmatrix}.$$

Визначник матриці AA^T дорівнює визначнику

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & n_1 & k & \dots & k \\ 0 & k & n_2 & \dots & k \\ \multicolumn{5}{c}{\dotfill} \\ 0 & k & k & \dots & n_m \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ -k & n_1 - k & 0 & \dots & 0 \\ -k & 0 & n_2 - k & \dots & 0 \\ \multicolumn{5}{c}{\dotfill} \\ 0 & 0 \ \dots & 0 & & n_m - k \end{vmatrix} =$$

$$= (1 + \frac{k}{n_1 - k} + \dots + \frac{k}{n_m - k})(n_1 - k)(n_2 - k) \dots (n_m - k).$$

Отже, $\det AA^T \neq 0$ і ранг матриці AA^T дорівнює m. Оскільки ранг добутку не перевищує рангу співмножників, $m \leq n$. □

Розглянемо одне елегантне застосування теореми Фішера-Бозе і задачі 0.2.2 до теорії Рамсея. За теоремою Рамсея, для будь-яких натуральних чисел t, r знайдеться натуральне число $m(t, r)$, таке, що для довільного r-розфарбування множини ребер повного графу $K_{m(t,r)}$ з $m(t, r)$ вершинами знайдеться повний підграф з t вершинами, всі ребра якого однокольрові. Найменше з чисел $m(t, r)$ називається числом Рамсея з відповідними параметрими і позначається $R(t, r)$. Ердьош довів, що існує 2-розфарбування ребер повного грфу з $2^{\lfloor \frac{t}{2} \rfloor}$ вершинами, що не має однокольрових повних пігрфів з t вершинами, тобто $R(t, 2) > 2^{\lfloor \frac{t}{2} \rfloor}$. Існування такого розфарбування доведено ймовірнісними методами. Нагі запропонував таке конструктивне 2-розфарбування повного графа з $n = \begin{pmatrix} t \\ 3 \end{pmatrix}$ вершинами без однокольрових підграфів K_{t+1}. Ми ототожнимо множину вершин графу K_n з трьохелементними підмножинами множини $\{1, \dots, t\}$. Ребро між двома вершинами пофарбуємо червоним кольром, якщо відповідні підмножини мають рівно один спільний елемент, а в іншому разі — синім кольром. Нехай K_m повний підграф K_n, всі ребра якого однокольорові. Якщо колір ребер червноий, то за теоремою Фішера-Бозе $m \leq t$. Якщо ж колір синій, то нерівність $m \leq t$ випливає з задачі 0.2.2.

ТЕОРЕМА 0.2.2 (Чоудхурі-Вільсона.). *Нехай* $A_1, \dots, A_m$ — *різні підмножини множини* $\{1, \dots, n\}$, $|A_1| = \dots = |A_m| =$

k, $L = \{l_1, \ldots, l_s\}$ — множина невідємних цілих чисел, $l_1 < k, \ldots, l_s < k$. Якщо $|A_i \cap A_j| \in L$, $i \neq j$, то $m \leq \left(\begin{array}{c} n \\ s \end{array} \right)$.

Доведення. Нехай F — поле, $\Omega = \{0,1\}^n \subseteq F^n$, f — поліном степеня $\leq t$ від n змінних $x_1, \ldots, x_n$ над F. Мультилінійний поліном — це сума мономів, моном — це добуток різних змінних. Для поліному f існує мультилінійний поліном $\widetilde{f}$ степеня $\leq t$ від тих самих змінних, такий, що $f(x) = \widetilde{f}(x)$ для всіх $x \in \Omega$. Дійсно, якщо x_i — одна зі змінних, то $x_i^k = x_i$ при $x_i \in \{0,1\}$. Отже, кожен поліном від n змінних на Ω можна замінити (як функцію) на деякий мультилінійний поліном. Ототожнимо Ω з родиною усіх підмножин множини $\{1, \ldots, n\}$. Для підмножини $I \subseteq \{1, \ldots, n\}$, $f(I)$ означає $f(a)$, де a — харатеристичний вектор підмножини I. Крім того індексуємо мономи

$$x_I = \prod_{i \in I} x_i, \quad x_\emptyset = 1.$$

Якщо $J \subseteq \{1, \ldots, n\}$ і $I \subseteq J$, то $x_I(J) = 1$, в іншому випадку $x_I(J) = 0$.

Нехай $f : \Omega \to \mathbb{R}$ і $f(I) \neq 0$ для всіх I, $|I| \leq k$. Ми покажемо, що набір функцій $\{x_I f : |I| \leq k\}$ простору $\mathbb{R}^\Omega$ лінійно незалежний. Лінійно упорядкуємо підмножини множини $\{1, \ldots, n\}$ так, щоб з $J \prec I$ випливало $|J| \leq |I|$. Тоді для всіх $|I|, |J| \leq k$

$$x_I(J) f(J) = \begin{cases} f(J) \neq 0, & \text{якщо } J = I; \\ 0, & \text{якщо } J \prec I. \end{cases}$$

Матриця $(x_I(J) f(J))$, $|I| \leq k$, $|J| \leq k$ трикутна і її визначник відмінний від нуля. Отже вектори-рядки цієї матриці лінійно незалежні, а тому лінійно незалежні і функції $x_I f$, $|I| \leq k$.

Нехай $a_1, \ldots, a_m$ — характеристичні вектори підмножин $A_1, \ldots, A_m$. Означимо функції $f_i \in \mathbb{R}^{\Omega}$, $i \in \{1, \ldots, m\}$ за правилом

$$f_i(x) = \prod_{r=1}^{s}((a_i, x) - l_r).$$

Очевидно, що $f_i(A_j) \neq 0$, якщо $i = j$, $f_i(A_j) = 0$, якщо $i \neq j$. Отже, набір функцій $f_1, \ldots, f_m$ лінійно незалежний. Ми покажемо більше: система функцій $\{f_i\}$ разом з функціями $\{x_I(\sum\limits_{j=1}^{n} x_j - k) : |I| \leq s-1\}$ залишається лінійно незалежною. Нехай

$$\sum_{i=1}^{n} \lambda_i f_i + \sum_{|I| \leq s-1} \mu_I x_I (\sum_{j=1}^{n} x_j - k) = 0.$$

Підставимо A_i, всі доданки другої суми дорівнюють нулю. Отже $\lambda_i = 0$ для всіх $i \in \{1, \ldots, m\}$. Позначимо $f = \sum\limits_{j=1}^{n} x_j - k$. За доведеним вище $\mu_I = 0$ для всіх $|I| \leq s-1$. Таким чином ми знайшли $m + \sum\limits_{i=0}^{s-1} \left(\begin{array}{c} n \\ i \end{array} \right)$ лінійно незалежних функцій, кожна з яких представлена поліномом степеня $\leq s$. Простір таких мультилінійних поліномів має розмірність $\sum\limits_{i=0}^{s} \left(\begin{array}{c} n \\ i \end{array} \right)$. Отже, $m \leq \left(\begin{array}{c} n \\ i \end{array} \right)$. □

Зауважимо, що вказана оцінка є точною. Як приклад можна взяти родину усіх s-підмножини множини $\{1, \ldots, n\}$, $L = \{0, 1, \ldots, s-1\}$. Ще одна теорема Чоудхурі-Вільсона про обмеження на перетини формулюється так.

Теорема 0.2.3. *Нехай $\mathcal{F}$ сім'я різних підмножин множини $\{1,\dots,n\}$ L — скінченна множина невід'ємних цілих чисел, $|L|=s$. Якщо $|F\cap F'|\in L$ для будь-яких різних підмножин $F,F'\in\mathcal{F}$, то*

$$|\mathcal{F}|\le\begin{pmatrix} n\\ 0\end{pmatrix}+\begin{pmatrix} n\\ 1\end{pmatrix}+\dots+\begin{pmatrix} n\\ s\end{pmatrix}.$$

В 1933 році Борсук поставив таку проблему. Чи можна кожну підмножину діаметра 1 із $\mathbb{R}^d$ розбити на $d+1$ підмножин діаметра <1? Діаметром множини називається супремум відстаней між точками цієї підмножини.

Позначимо через $f(d)$ найменше ціле число, таке що кожну підмножину $\mathbb{R}^d$ діаметра 1 можна розбити на $f(d)$ частин меншого діаметра. Правильний симплекс із $\mathbb{R}^d$ показує, що $f(d)\ge d{+}1$. Гіпотеза Борсука полягала у тому, що $f(d)=d{+}1$. Сам Бореукс підтвердив гіпотезу для $d=2$, а Еглстон — для $n=3$. Крім того, гіпотеза Борсук виявилася справедливою для всіх розмірностей для центрально симетричних опуклих тіл, а ткож для опуклих тіл з гладкою границею.

В 1993 році Кан та Каллаї спростували гіпотезу Бореукса, використовуючи комбінаторні методи лінійної алгебри.

Теорема 0.2.4 (Кана-Калаї.). *Існує безліч натуральних чисел d, для ких $f(d)\ge(1,2)^{\sqrt{d}}$.*

Доведення. Скористаємось такою комбінаторною теоремо Франкля-Вільсона [**4**]

Нехай $m=4k$, k —степінь простого числа, K — деяка родина $\frac{m}{2}$-підмножин множини $\{1,\dots,m\}$. Якщо $|K|>2\begin{pmatrix} m-1\\ \frac{m}{4}-1\end{pmatrix}$, то знайдуться дві підмножини з K, що перетинаються по $\frac{m}{4}$ елементах.

Контрприкладом до гіпотези Борсука буде деяка скінченна підмножина з $\mathbb{R}^d$, елементи якої мають координати $0,1$.

Нехай $V = \{1, \ldots, m\}$, W — сім'я двоелементних підмножин із V. Для кожного розбиття $P = \{A, B\}$ множини V на дві однакові частини позначимо через $S(A, B)$ сім'ю двоелементних підмножин, один з елементів якої лежить в A, а інший в B. Нехай K — сім'я двоелементних підмножин, що відповідають розбиттям V на дві частини

$$K = \{S(A, B) : \quad A = 2k\}.$$

Очевидно, що K — сім'я $\frac{m^2}{4}$-підмножин множини із $\frac{m(m-1)}{2}$ елементів. Найменший перетин між $S(A, B)$ і $S(C, D)$ буде лише коли $|A \cap C| = k$. З теореми Франкля-Вільсона випливає, що будь-яка підсім'я з K, що містить більш ніж $2 \left(\begin{array}{c} m-1 \\ \frac{m}{4}-1 \end{array} \right)$ підмножин містить дві підмножини з найменшим перетином (а, отже, з максимальною відстанню між відповідними точками простору $\mathbb{R}^{\frac{m(m-1)}{2}}$). Таким чином, множину K не можна розбити на менше ніж

$$\frac{1}{2} \left(\begin{array}{c} m \\ \frac{m}{2} \end{array} \right) / \sqrt{2} \left(\begin{array}{c} m-1 \\ \frac{m}{4}-1 \end{array} \right)$$

частин так, що найменший пертин не досягається в жодній з цих частин. Цей вираз, за формулою Стірлінга, $\geq (1,203)^{\sqrt{d}}$ при досить великих $d = \frac{m(m-1)}{2}$. □

Теорема Кана-Калаї дає негативну відповідь на запитання Борсука для $d = 1325$. На разі відомі негативні приклади в розмірності $d = 561$ [**2**].

Задача 0.2.4. Після кожної лекції з комбінаторики деяка частина студентів (але не всі) йде до кав'ярні для обговорення поставлених проблем. Одне правило непорушне: будь-які два студенти можуть опинитися в одній кавовій компанії не більше одного разу. Припустімо, що після m лекці кожна пара з n студентів побувала в кав'ярні разом. Довести, що $m \geq n$.

Розв'язок. Кожному студенту $i \in \{1,\ldots,n\}$ ми співставимо вектор $a_i = (\alpha_1,\ldots,\alpha_m) \in \{0,1\}^m$ відвідувань кав'ярні, де $\alpha_j = 1$ тоді і тільки тоді, коли після j-ої лекції студент відвідує кав'ярню. Переконаймося, що вектори $a_1,\ldots,a_n$ простору $\mathbb{R}^n$ лінійно незалежні. Розглянемо визначник Грама $g(a_1,\ldots,a_n)$ цієї системи векторів

$$g(a_1,\ldots,a_n) = \begin{vmatrix} (a_1,a_1) & \ldots & (a_1,a_n) \\ \ldots & \ldots & \ldots\ldots \\ (a_n,a_1) & \ldots & (a_n,a_n) \end{vmatrix} = \begin{vmatrix} (a_1,a_1) & 1 & \ldots & 1 \\ 1 & (a_2,a_2) & \ldots & 1 \\ & & & \\ \ldots & \ldots & \ldots & \ldots\ldots \\ 1 & 1 & \ldots & (a_n,a_n) \end{vmatrix}.$$

За умовою задачі $(a_i,a_i) > 1$ для всіх $i \in \{1,\ldots,n\}$. Отже, $g(a_1,\ldots,a_n) \neq 0$.

Чи можна скласти програму відвідувань так, щоб після n лекцій усі пари студентів побували в кав'ярні. Відповідо очевидна: після першої лекції один із студентів залишається в авдиторії, а решта йде в кав'ярню, а далі після кожної лекції цей студент ходить до кав'ярні в парі з усіма іншими. Ця програма надто неврівноважена — всі суденти, крім одного, побували в кав'ярні двічі, а цей один — $n-1$ разів. Чи для кожного n можна вказати врівноважену прграму n відвідувань. Іншими словами, чи можна знайти сім'ю підмножин $A_1,\ldots,A_n$ множини $\{1,\ldots,n\}$, таку, що $|A_1| = \cdots = |A_n|$ і кожна пара елементів $i,j \in \{1,\ldots,n\}$ належить тільки одній підмножині A_k. Для деяких n позитивну відповідь дає проективна геометрія.

Проективна площина — це множина точок P і множина L підмножин з P, що називається прямими, причому

(i) через кожні дві точки проходить одна і тільки одна пряма;

(ii) будь-які дві прямі перетинаються в одній точці;

(iii) існують чотири точки, що не лежать на одній прямій.

Кожне скінченне поле F визначає деяку проектину площину: за P візьмемо сім'ю усіх одновимірних підпросторів F^3, а кожен двовимірний підпростір з F^3 визначає пряму як сукупність усіх одновимірних підпросторів, що в ньому міститься.

Нехай $\mathcal{F}$ —сім'я підмножин множини X. Підмножина $Y \subseteq X$ називається трансверсаллю сім'ї $\mathcal{F}$, якщо $F \cap Y \neq \emptyset$ для будь-якої підмножини $F \in \mathcal{F}$. Таким чином, кожна підмножина сім'ї $\mathcal{F}$ має представника серед елементів трасверсалі.

Теорема 0.2.5 (Болобаша). *Нехай X — скінченна множина, $\mathcal{F} = \{A_1, \dots, A_m\}$ — сім'я підмножин X, $|A_1| = \ldots = |A_m| = r$. Якщо кожні $k \leq \begin{pmatrix} r+s \\ s \end{pmatrix}$ підмножин сім'ї $\mathcal{F}$ мають трансверсаль потужності s, то і вся сім'я $\mathcal{F}$ має трансверсаль потужності s.*

Доведення. Кілька необхідних означень. Трансверсальність $\tau(\mathcal{F})$ сім'ї $\mathcal{F}$ — це мінімальна потужність трансверсалей $\mathcal{F}$. Сім'я підмножин називається критичною, якщо її трансверсальність зменшується після видалення будь-якої підмножини цієї сім'ї. Ми покажемо, що теорема випливає з такого твердження.

(*) Якщо сім'я $\mathcal{F}$ критична і $\tau(\mathcal{F}) = s+1$, то $|\mathcal{F}| \leq \begin{pmatrix} r+s \\ s \end{pmatrix}$.

Дійсно, якщо кожні $k \leq \begin{pmatrix} r+s \\ s \end{pmatrix}$ підмножин з $\mathcal{F}$ мають s-трансверсаль, але $\mathcal{F}$ не має s-трансверсалей, то $\tau(\mathcal{F}) \geq s+1$. Видаляємо тепер з $\mathcal{F}$ підмножини доти, поки не отримаємо критичну сім'ю $\mathcal{F}'$ з $\tau(\mathcal{F}') = s + 1$. За твердженням (*) $|\mathcal{F}'| \leq \left(\begin{array}{c} r+s \\ s \end{array}\right)$, що суперчить припущенню теореми.

Отже, нехай сім'я $\mathcal{F}$ критична, $\tau(\mathcal{F}) = s + 1$. Для кожного $i \in \{1, \ldots, m\}$ видалимо підмножину A_i з $\mathcal{F}$ і одержимо сім'ю $\mathcal{F}_i$, що має s-трансверсаль B_i. Ясно, що $A_i \cap B_i = \emptyset$, $A_i \cap B_j \neq \emptyset$ для всіх $i \neq j$. А тому (*) випливає з такого твердження.

(**) Нехай $A_1, \ldots, A_m$ та $B_1, \ldots, B_m$ — підмножини скінченної множини X, $|A_1| = \cdots = |A_m| = r$, $|B_1| = \cdots = |B_m| = s$. Якщо $A_i \cap B_i = \emptyset$ для всіх $i \in \{1, \ldots, m\}$, $A_i \cap B_j \neq \emptyset$ при $i \neq j$, то $m \leq \left(\begin{array}{c} r+s \\ s \end{array}\right)$.

Для доведення (**), кожній точці $v \in X$ співставимо вектор

$$\rho(v) = (\rho_0(v), \rho_1(v), \ldots, \rho_r(v)) \in \mathbb{R}^{r+1}$$

так, щоб кожні $r + 1$ векторів були лінійно незалежними. З кожною підмножиною $W \subseteq X$ асоціюємо поліном

$$f_W(x) = \prod_{v \in W} (\rho_0(v)x_0 + \cdots + \rho_r(v)x_r).$$

Це однорідний поліном степеня $|W|$. Зауважимо, що

$$f_W(x) = \begin{cases} 0, & \text{якщо } x \text{ ортогональний до деякого } \rho(v), v \in W; \\ \neq 0, & \text{в іншому випадку.} \end{cases}$$

Нехай $f_i(x)$ означає $f_{B_i}(x)$. Тоді $f_1(x), \ldots, f_m(x)$ — однорідні поліноми степеня s. Ми доведемо, що ці поліноми лінійно незалежні. Вектори, що відповідають підмножині A_j породжують підпростір розмірності r в $\mathbb{R}^{r+1}$. Виберемо ненульовий вектор a_i із ортогонального доповнення до цього підпростору. Оскільки вектори $\rho(v)$, $v \in X$ вибрано в загальному положенні, то $a_j \perp \rho(v)$ тоді і тільки тоді, коли $v \in A_j$. Отже,

$$f_i(a_j) = 0 \Leftrightarrow A_j \cap B_i \neq \emptyset \Leftrightarrow i \neq j.$$

Значить, $f_i(a_j) = 0$, якщо $i \neq j$, $f_i(a_i) \neq 0$. Звідси випливає лінійна незалежність поліномів $f_1(x), \ldots, f_m(x)$. Отже, m не первищує розмірності простору онорідних поліномів степеня s від $r+1$ змінної. Базис цього простору утворюють оночлени $x_0^{t_0} x_1^{t_1} \cdots x_r^{t_r}$, де $t_0 + t_1 + \cdots + t_r = s$. Кількість таких одночленів дорівнює числу цілочисельних невідємних розв'язків рівняння $t_0 + t_1 + \cdots + t_r = s$, а це число $\left(\begin{array}{c} r+s \\ s \end{array} \right)$. □

Нехай $Gr(V, E)$ — скінченний гріф з множиною вершин V і множиною ребер E. Підмножина $W \subseteq V$ називається трансверсаллю деякої підмножини ребер $R \subseteq E$, якщо для кожного ребра із R в множині W знайдеться вершина, що є кінцем цього ребра. Теорема Болобаша є узагальненням такої теореми Ердьоша-Хайнала-Муна.

Теорема 0.2.6. *Якщо кожні* $k \leq \left(\begin{array}{c} s+2 \\ s \end{array} \right)$. *ребер графу* $Gr(V, E)$ *мають трансверсаль потужності* s, *то множина усіх ребер має трансверсаль потужності* s.

Далі ми розглянемо кілька оптимізаційних задач.

Задача 0.2.5. Дано квадратну матрицю порядку n з дісними додатніми елементами. Необхідно знайти таку підмножину елементів матриці, що

(i) в кожному стовпчику міститься не більше одного вибраного елементу;

(ii) сума всіх вибраних елементів максимальна.

Спробуємо розв'язати цю задачу так: з кожного стовпчика, починаючи з першого будемо вибирати найбільший елемент так, щоб не порушити умову (i). Подібні алгоритми називаються *жадібними.* Наприклад, для матриці A жадібний алгоритм

$$A = \begin{pmatrix} \underline{7} & \underline{5} & 1 \\ 3 & 4 & \underline{3} \\ 2 & 3 & 1 \end{pmatrix}$$

дає суму 15, що виявляється максимальною. Дещо змінимо задачу.

Задача 0.2.6. Необхідно знайти таку підмножину елементів матриці, що

(i) в кожному рядку і кожному стовпчику міститься не більше одного вибраного елементу;

(ii) сума всіх вибраних елементів максимальна.

На цей раз застосування жадібного алгоритму до матриці A дає результат 12

$$A = \begin{pmatrix} \underline{7} & 5 & 1 \\ 3 & \underline{4} & 3 \\ 2 & 3 & \underline{1} \end{pmatrix},$$

що не є правильним, бо підмножина

$$A = \begin{pmatrix} \underline{7} & 5 & 1 \\ 3 & 4 & \underline{3} \\ 2 & \underline{3} & 1 \end{pmatrix}$$

дає суму 13. Природньо виникає запитання: коли вигідно бути жадібним? Для того, щоб сформулювати це запитання математично, ми розглянемо таку загальну оптимізаційну задачу.

Задача 0.2.7. Нехай E — скінченна множина, $\mathcal{F}$ — сім'я підмножин множини E, $\omega : E \to \mathbb{R}^+$. Знайти підмножину $S \in \mathcal{F}$ з найбільшою сумою $\sum\limits_{e \in S} \omega(e)$.

Тепер наше запитання формулюється строго: за яких умов на сім'ю $\mathcal{F}$ жадібний агоритм правильно розв'язує Задачу 0.2.7 для довільної вагової функції ω? Виявляється, відповідь на це запитання коротка: необхідно і достатньо, щоб пара $(E, \mathcal{F})$ утоворювала так званий матроїд. Матроїди ввів в 1935 році Уїтні [**6**] як комбінаторне узагальнення поняття лінійної незалежності.

Матроїдом називають пару $(E, \mathcal{F})$, де E — скінченна множина, $\mathcal{F}$ —сім'я підмножин множини E, така, що

(M1) $\emptyset \in \mathcal{F}$ і якщо $A \in \mathcal{F}$, $B \subseteq A$, то $B \in \mathcal{F}$;

(M2) для довільних $A, B \in \mathcal{F}$, таких що $|B| = |A| + 1$ існує елемент $e \in B \setminus A$, такий, що $A \cup \{e\} \in \mathcal{F}$.

Множини сім'ї $\mathcal{F}$ називаються *незалежними,* а інші — *залежними* множинами матроїду $\mathcal{M} = (E, \mathcal{F})$. Незалежна множина, що не міститься в більшій незалежній множині даного матроїду називається *максимальною незалежною* множиною. Легко перевірити, що будь-які дві максимальні незалежні множини містять однакове число елементів. Це число називають рангом матроїду. Крім того, умови M1, M2 рівносильні умовам M1, M3, де

(M3) для кожної підмножини $C \subseteq E$ будь-які дві максимальні незалежні підмножини C мають однакове число елементів.

Приклад 0.2.1. Нехай E — скінченна підмножина деякого векторного простору, $\mathcal{F}$ — сім'я всіх лінійно незалежних підмножин з E. Очевидно, що пара $(E, \mathcal{F})$ — матроїд.

Приклад 0.2.2. Нехай $Gr(V, E)$ — скінченний зв'язний граф. Підмножину $A \subseteq E$ назвемо незалежною, якщо граф $Gr(V, A)$ не має циклів. Нехай $\mathcal{F}$ — сім'я усіх незалежних множин ребер. Оскільки будь-яка максимальна незалежна множина містить $|V| - 1$ ребер, умови M1, M3 задовольняються, отже, $(E, \mathcal{F})$ — матроїд.

Ми опишемо докладніше жадібний алгоритм для Задачі 0.2.7 Нехай $E = \{e_1, \ldots, e_n\}$, $\omega(e_1) \geq \cdots \geq \omega(e_n)$. На першому кроці вибираємо перший елемент e_{i_1}, для якого $\{e_{i_1}\} \in \mathcal{F}$ і викреслюємо всі попередні елементи $e_1, \ldots, e_{i_1-1}$. Нехай вже вибрано елементи $e_{i_1}, \ldots, e_{i_k}$. На $(k+1)$-му кроці вибираємо перший з невикреслених елментів $e_{i_{k+1}}$, для якого $\{e_{i_1}, \ldots, e_{i_k}, e_{i_{k+1}}\} \in \mathcal{F}$, і викреслюємо всі попердні елементи.

Теорема 0.2.7 (Радо-Едмондса.). *Нехай E — скінченна множина, $\mathcal{F}$ — сім'я підмножин E, $\omega : E \to \mathbb{R}^+$. Якщо $(E, \mathcal{F})$ — матроїд , то підмножина $S \in \mathcal{F}$, знайдена за допомогою жадібного алгоритму є незалежною підмножиною максимальної ваги. Якщо ж $(E, \mathcal{F})$ не є матроїдом, то існує функція $\omega : E \to \mathbb{R}^+$ така, що підмножина $S \in \mathcal{F}$, знайдена жадібним алгоритмом, не є підмножиною з $\mathcal{F}$ максимальної ваги.*

Доведення. Нехай $(E, \mathcal{F})$ — матроїд, S — підмножина, побудована жадібним алгоримом, $S = \{s_1, \ldots, s_k\}$, $\omega(s_1) \geq \cdots \geq \omega(s_k)$. Нехай $T = \{t_1, \ldots, t_m\}$ — незалежна множина, $\omega(t_1) \geq \cdots \geq \omega(t_m)$. Зрозуміло, що S має бути максимально незалежною множиною, а тому $m \leq k$. Ми покажемо, що $\omega(t_i) \leq \omega(s_i)$ для всіх $i \in \{1, \ldots, m\}$, а тому $\omega(S) \geq \omega(T)$. Припустимо супротивне $\omega(t_i) > \omega(s_i)$ для деякого $i \in \{1, \ldots, m\}$. Розглянемо незалежні множини

$$A = \{s_1, \ldots, s_{i-1}\}, \quad B = \{t_1, \ldots, t_{i-1}, t_i\}.$$

За умовою M2 існує елемент t_j, $j \in \{1, \ldots, i\}$, такий що множина $\{s_1, \ldots, s_{i-1}, t_j\}$ незалежна. Оскільки $\omega(t_j) \geq \omega(t_i) > \omega(s_i)$, знайдеться $p \in \{1, \ldots, i\}$, такий, що

$$\omega(s_1) \geq \cdots \geq \omega(s_{p-1}) \geq \omega(t_j) > \omega(s_p).$$

Але тоді на p-му кроці жадібного алгоритму ми мали б вибрати елемент t_j, а не s_p.

Нехай тепер $(E, \mathcal{F})$ не є матроїдом. Якщо порушено умову M1, то існують підмножини A, B з E, такі що $A \subset B$, $B \in \mathcal{F}$, $A \notin \mathcal{F}$. Означимо функцію $\omega : E \to \mathbb{R}^+$

$$\omega(e) = \begin{cases} 1, & \text{якщо } e \in A; \\ 0, & \text{якщо } e \in E \setminus A. \end{cases}$$

Зауважимо, що підмножина A не міститься в жодній підмножині, побудованій жадібним алгоритмом, а тому $\omega(S) < \omega(B) = \omega(A)$. Нехай умова M1 виконується, але умова M2 порушується. Тоді існують підмножини $A, B \in \mathcal{F}$, такі що $|A| = k$, $|B| = k + 1$ і $A \cup \{e\} \notin \mathcal{F}$ для кожного $e \in B \setminus A$. Позначимо $p = |A \cap B|$. Очевидно, $p < k$. Зафіксуємо $\epsilon > 0$, $\epsilon < \frac{1}{k-p}$ і задамо відображення $\omega : E \to \mathbb{R}^+$

$$\omega(e) = \begin{cases} 1 + \epsilon, & \text{якщо } e \in A; \\ 1, & \text{якщо } e \in B \setminus A. \\ 0, & \text{в іншому разі.} \end{cases}$$

Жадібний алгоритм спочатку вибере всі елементи множини A, а потім відхилить усі елементи $e \in B \setminus A$. В результаті одержимо множину S з $\omega(S) < \omega(B)$:

$$\omega(S) = \omega(A) = k(1 + \epsilon) = (k - p)(1 + \epsilon) + p(1 + \epsilon) <$$

$$< (k - p)\frac{k + 1 - p}{k - p} + p(1 + \epsilon) = k + 1 - p + p(1 + \epsilon) = \omega(B).$$

Більше про матроїди можна прочитати в [**1, 3, 5**]. □

Бібліоґрафія

[1] Липський В. Комбинаторика для программистов, М., "Мир 1988.
[2] Райгородский А. М. О размерности в проблеме Борсука, УМН, 52 (1997), №6, 181-182.
[3] Уилсон Р. Введение в теорию графов, М., "Мир 1977.
[4] Frankl P. Wilson R. Intersection theorems with geometric consequences, Combinatorica 1 (1981), 357-368.
[5] Welsh D. Matroid Theory, Acad. Press, London, 1976.
[6] Whitney H. On the abstract properties of linear dependence, Amer. J. Math., 57 (1935), 509-533.

0.3. Комбінаторика опуклих множин

Підмножина V із $\mathbb{R}^n$ називається *опуклою,* якщо для будь-яких двох точок $a, b \in V$ відрізок $[a, b] = \{\lambda a + (1 - \lambda)b : 0 \leq \lambda \leq 1\}$ міститься в V. Найменша опукла множина $\operatorname{conv} S$, що містить задану підмножину $S \subseteq \mathbb{R}^n$, називається *опуклою оболнкою* підмножини S. Опукла оболонка $\operatorname{conv} S$ складається з наймождивіших опуклих комбінацій точок із S. Лінійна комбінація $\lambda_1 a_1 + \cdots + \lambda_m a_m$ називається опуклою, якщо $\lambda_1 \geq 0, \ldots, \lambda_m \geq 0, \lambda_1 + \cdots + \lambda_m = 1$.

Теорема 0.3.1 (Радона). *В просторі $\mathbb{R}^n$ задано скінченну множину точок $\{x_1, \ldots, x_m\}$, причому $m \geq n+2$. Цю множину точок завжди можна розбити на дві підмножини так, що їх опуклі оболонки мають спільну точку.*

Доведення. Нехай $x_1 = (a_{11}, \ldots, a_{n1})^T, \ldots, x_m = (a_{1m}, \ldots, a_{nm})^T$. Складемо систему лінійних рівнянь

$$\begin{cases} a_{11}y_1 + a_{12}y_2 + \cdots + a_{1m}y_m = 0, \\ \dotfill \\ a_{n1}y_1 + a_{n2}y_2 + \cdots + a_{nm}y_m = 0, \\ y_1 + y_2 + \cdots + y_m = 0. \end{cases}$$

Оскільки кількість рівнянь менша за кількість невідомих, система має ненульовий роз'язок $\alpha_1, \ldots, \alpha_m$. Змінюючи нумерацію невідомих, можна вважати, що

$$\alpha_1 \geq 0, \ldots, \alpha_r \geq 0, \alpha_{r+1} < 0, \ldots, \alpha_m < 0,$$

причому $0 < r < m$. Позначимо $\alpha = \alpha_1 + \cdots + \alpha_r$. В перші n рівнянь підставимо $\alpha_1, \ldots, \alpha_m$ і запишемо одержану систему співвідношень у векторній формі

$$\alpha_1 x_1 + \cdots + \alpha_r x_r = -\alpha_{r+1} x_{r+1} - \cdots - \alpha_m x_m,$$

позначимо

$$x = \frac{\alpha_1}{\alpha} x_1 + \cdots + \frac{\alpha_r}{\alpha} x_r = \left(-\frac{\alpha_{r+1}}{\alpha}\right) x_{r+1} + \cdots + \left(-\frac{\alpha_m}{\alpha}\right) x_m$$

і помітимо, що $x \in \mathrm{conv}\{x_1, \ldots, x_r\} \cap \mathrm{conv}\{x_{r+1}, \ldots, x_m\}$. $\square$

ТЕОРЕМА 0.3.2 (Каратеодорі). *Кожну точку опуклої оболонки підмножини $S \subseteq \mathbb{R}^n$ можна подати у вигляді опуклої комбінації не більше ніж $(n+1)$-ої точки із S.*

ДОВЕДЕННЯ. Нехай $x \in \mathrm{conv}\, S$, $x = \lambda_1 x_1 + \cdots + \lambda_m x_m$, де $x_1, \ldots, x_m \in S$, $\lambda_i > 0$, $\sum\limits_{i=1}^{m} \lambda_i = 1$. Якщо $m \leq n+1$, теорему доведено. Нехай $m \geq n+2$. За теоремо Радона множину $\{x_1, \ldots, x_m\}$ можна розбити на дві частини так, що їх опуклі оболонки перетинаються. Змінюючи нумерацію, можна вважати, що

$$\mathrm{conv}\{x_1, \ldots, x_r\} \cap \mathrm{conv}\{x_{r+1}, \ldots, x_m\} \neq \emptyset.$$

Візьмемо довільну точку з цього перетину

$$z = \alpha_1 x_1 + \cdots + \alpha_r x_r = \alpha_{r+1} x_{r+1} + \cdots + \alpha_m x_m.$$

Нехай γ — деяка змінна. Тоді

$$x = x - \gamma z + \gamma z = (\lambda_1 + \gamma\alpha_1)x_1 + \cdots + (\lambda_r + \gamma\alpha_r)x_r + (\lambda_{r+1} + \gamma\alpha_{r+1})x_{r+1} + \cdots + (\lambda_m + \gamma\alpha_m)x_m.$$

Позначимо

$$\gamma' = \min\{\frac{\lambda_i}{\alpha_i} : r+1 \leq i \leq m, \alpha_i \neq 0\}.$$

Можна вважати, що цей мінімум досягається, коли $\gamma' = \frac{\lambda_m}{\alpha_m}$. Значить,

$$x = (\lambda_1 + \gamma'\alpha_1)x_1 + \cdots + (\lambda_r + \gamma'\alpha_r)x_r + (\lambda_{r+1} - \gamma'\alpha_{r+1})x_{r+1} + (\lambda_{m-1} - \gamma'\alpha_{m-1})x_{m-1}.$$

Очевидно, що всі коефіцієнти невід'ємні, а їх сума дорівнює 1. Таким чином, ми скортили довжину опуклої комбінації. $\square$

ЗАДАЧА 0.3.1. Доведіть, що опукла оболонка компакта із $\mathbb{R}^n$ є компактом.

ТЕОРЕМА 0.3.3 (Хелі). *Нехай $\mathcal{F} = \{F_1, \dots, F_m\}$ — скінченна сім'я опуклих підмножин із $\mathbb{R}^n$, $m \geq n+1$. Якщо будь-які $n+1$ підмножин із $\mathcal{F}$ мають спільну точку, то перетин усіх підмножин із $\mathcal{F}$ непорожній.*

ДОВЕДЕННЯ. Застосуємо індукцію по числу m. Для $m = n+1$ твердження тривіальне. Позначимо

$$\mathcal{F}_i = \{F_1, \dots, F_{i-1}, F_{i+1}, \dots, F_m\}, \quad i \in \{1, \dots, m\}.$$

До кожної сім'ї $\mathcal{F}_i$ можна застосувати припущення індукції і вибрати точку

$$p_i \in F_1 \cap \dots \cap F_{i-1} \cap F_{i+1} \cap \dots \cap F_m.$$

Розглянемо множину точок $\{p_1, \dots, p_m\}$. Оскільки $m \geq n+2$, за теоремою Радона, після відповідної зміни нумерації точок, знайдеться k, $0 < k < m$, таке що

$$\operatorname{conv}\{p_1, \dots, p_k\} \cap \operatorname{conv}\{p_{k+1}, \dots, p_m\} \neq \emptyset.$$

Візьмемо довільну точку p з цього перетину. Зауважимо, що

$$p_1 \in F_2 \cap \dots \cap F_m, \quad p_2 \in F_1 \cap F_3 \cap \dots \cap F_m, \dots, p_k \in F_1 \cap \dots \cap F_{k-1} \cap F_{k+1} \cap \dots \cap F_m.$$

Оскільки підмножини $F_{k+1}, \dots, F_m$ опуклі,

$$\operatorname{conv}\{p_1, \dots, p_k\} \subseteq F_{k+1} \cap \dots \cap F_m.$$

Отже, $p \in F_{k+1} \cap \dots \cap F_m$. Аналогічно,

$$p_{k+1} \in F_1 \cap \dots \cap F_k \cap F_{k+2} \cap \dots \cap F_m, \dots, p_m \in F_1 \cap \dots \cap F_k \cap \dots \cap F_{m-1},$$

$$\operatorname{conv}\{p_{k+1}, \dots, p_m\} \subseteq F_1 \cap \dots \cap F_k.$$

Отже, $p \in F_1 \cap \dots \cap F_k$ і p — спільна точка усіх підмножин сім'ї $\mathcal{F}$. □

Задача 0.3.2. Доведіть компактний варіант теореми Хелі. Нехай $\mathcal{F}$ — нескінченна сім'я опуклих компактів із $\mathbb{R}^n$. Якщо будь-які $n+1$ підмножин сім'ї $\mathcal{F}$ перетинаються, то перетин усіх підмножин сім'ї $\mathcal{F}$ непорожній

Задача 0.3.3. Опуклу підмножину V із $\mathbb{R}^n$ покрито скінченним числом напівпросторів (відкритих або замкнених). Доведіть, що серед цих напівпросторів можна вибрати $\leq n+1$ так, що вони покривають підмножину V. Відкритий (замкнений) напівпростір задається нерівністю $(a,x) < \alpha$ $((a,x) \leq \alpha))$, де α — ненульовий вектор із $\mathbb{R}^n$, $\alpha \in \mathbb{R}$.

Задача 0.3.4. На колі заданий деякий набір дуг, кожна з яких менша півкола. Перетин будь-яких трьох з цих дуг непорожній. Доведіть, що існує спільна точка для всіх дуг.

Задача 0.3.5. На колі заданий деякий набір дуг, кожна з яких менша третини кола. Перетин будь-яких двох з цих дуг непорожній. Доведіть, що існує спільна точка для всіх дуг.

Задача 0.3.6. На площині заданий спільний набір паралельних відрізків. Відомо, що для будь-яких трьох з цих відрізків знайдеться пряма, що їх перетинає. Доведіть, що існує пряма, що перетнає всі відрізки даного набору.

Задача 0.3.7. Нехай S — обмежена підмножина із $\mathbb{R}^n$, $r > 0$. Відомо, що для довільних $(n+1)$-ої точки із S існує куля радіусу r, що містить усі ці точки. Доведіть, що вся підмножина S міститься в деякій кулі радіуса r.

Теорема 0.3.4 (Юнга). *Якщо $X \subseteq \mathbb{R}^n$ і відстань між будь-якими двома точками з X не перевищує 2, то X міститься в деякій кулі радіуса $\sqrt{\frac{2n}{n+1}}$.*

Доведення. Вважаймо, що ми роз'язали Задачу 0.3.7. Тоді можна вважати, що $X = \{x_0, \ldots, x_n\}$. Позначимо через r

радіус найменшої кулі B, що містить X. Можна вважати, що центр кулі співпадає з початком системи координат. Нехай $\{z_0, \dots, z_m\}$ — всі точки із X, що лежать на поверхні кулі. Зауважимо, що $\theta \in \operatorname{conv}\{z_0, \dots, z_m\}$, а тому $\sum\limits_{i=0}^{m} \alpha_i z_i = \theta$ для деяких $\alpha_i \geq 0$, $\sum\limits_{i=0}^{m} \alpha_i = 1$.

Нехай $d_{ij} = ||z_i - z_j||$. Оскільки $d_{ij} \leq 2$, то $\frac{d_{ij}^2}{4} \leq 1$. Далі,

$$d_{ij}^2 = ||z_i||^2 + ||z_j||^2 - 2(z_i, z_j) = 2r^2 - 2(z_i, z_j),$$

$$1 - \alpha_j = \sum_{i \neq j} \alpha_i \geq \sum_{i=0}^{m} \alpha_i \frac{d_{ij}^2}{4} = \frac{r^2}{2} - \frac{1}{2} \sum_{i=0}^{m} \alpha_i (z_i, z_j) = \frac{r^2}{2}.$$

Оскільки $\sum\limits_{i=0}^{m} \alpha_i z_i = \theta$, то $1 - \alpha_j \geq \frac{r^2}{2}$. Просумуємо по $j \in \{0, \dots, m\}$ і отримаємо $m \geq (m+1)\frac{r^2}{2}$. Отже,

$$r^2 \leq \frac{2m}{m+1} \leq \frac{2n}{n+1}.$$

□

Задача 0.3.8. Нехай X — підмножина із $\mathbb{R}^n$. За означенням, точку y видно з точки x, якщо $[x, y] \subseteq X$. Підмножина Y називається зірчатою, якщо існує точка із X, з якої видно всі інші точки цієї множини.

Нехай X — компакт із $\mathbb{R}^n$, причому для будь-яких $(n+1)$-ої точки із X знайдеться точка $y \in X$, з якої видно всі ці точки. Доведіть, що підмножина X зірчата.

Задача 0.3.9. В деякій точці простору $\mathbb{R}^3$ розташовано 4 прожектори. Кожен з прожекторів освітлює частину простору деяким нескінченним опуклим світловим конусом при цьому жоден конус не містить двох протилежни променів, будь-які три конуси мають спільний промінь, а чотири — ні. Доведіть, що кожна точка простору освітлена.

Наступна тема — рівноскладеність опуклих многогранників.

Задача 0.3.10. Дано два опуклі многокутники на площині однакової площі. Довести, що один з них можна розрізати прямими на скінченне число частин, з яких можна скласти інший.

Два многогранники в $\mathbb{R}^3$ називаються *рівноскладеними,* якщо їх можна розрізати площинами на скінченне число попарно конгруентних многогранників. Іншими словами, многогранник M рівноскладений з многогоранником N, якщо M можна розрізати на скінченне число многогранників, з яких можна скласти многогранник N.

Третя проблема Гільберта, поставлена 1900 року і того ж року розв'язана Деном, стосувалась рівноскладеності правильного тетраедра та куба однакових об'ємів.

Теорема 0.3.5 (Дена). *Правильний тетраедр та куб не є рівноскладеними.*

Кілька допоміжних тверджень. Нехай V — лінійний простір над деяким полем F. Відображення $f : V \to E$ називають лінійною функцією, якщо $f(\alpha a+\beta b) = \alpha f(a)+\beta f(b)$ для будь-яких $a, b \in V$, $\alpha, \beta \in F$.

Лемма 0.3.1. Розглянемо множину $\mathbb{R}$ дійсних чисел як лінійний простір над полем $\mathbb{Q}$ раціональних чисел. Якщо дійсні числа u, v лінійно незалежні над полем $\mathbb{Q}$, то існує лінійна функція $f : \mathbb{R} \to \mathbb{Q}$, така, що $f(u) = 0$, $f(v) = 1$.

Доведення. Доповнимо u, v до базису простору $\mathbb{R}$ і покладемо $f(u) = 0$, $f(v) = 1$ і $f(w) = 0$ для всіх інших векторів базису. По лінійності це відображення однозначно продовжується на $\mathbb{R}$. □

ЛЕММА 0.3.2. Якщо $\cos\alpha = \frac{1}{3}$, то число $\frac{\alpha}{\pi}$ ірраціональне.

ДОВЕДЕННЯ. Припустиму супротивне: $k\alpha = 2n\pi$ для деяких натуральних чисел k, n. Розкладемо $\cos k\alpha$ за степенями $\cos\alpha, \sin\alpha$

$$1 = \cos k\alpha = \cos^k\alpha - \left(\begin{array}{c} k \\ 2 \end{array}\right)\cos^{k-2}\alpha\sin^2\alpha + \left(\begin{array}{c} k \\ 4 \end{array}\right)\cos^{k-4}\alpha\sin^4\alpha - \ldots,$$

$$1 = \frac{1}{3^k} - \left(\begin{array}{c} k \\ 2 \end{array}\right)\frac{1}{3^{k-2}}(1-\frac{1}{3^2}) + \left(\begin{array}{c} k \\ 4 \end{array}\right)\frac{1}{3^{k-4}}(1-\frac{1}{3^2})^2 - \ldots,$$

$$3^k = 1 - \left(\begin{array}{c} k \\ 2 \end{array}\right)(3^2-1) + \left(\begin{array}{c} k \\ 4 \end{array}\right)(3^2-1)^2 - \ldots,$$

$$3^k = 1 + \left(\begin{array}{c} k \\ 2 \end{array}\right) + \left(\begin{array}{c} k \\ 4 \end{array}\right) + \cdots + 3S = 2^{k-1} + 3S.$$

Залишилось помітити, що $2^{k-1} + 3S$ не ділиться на 3. □

Нехай M — многогранник в $\mathbb{R}^3$ з ребрами $e_1, \ldots, e_m$, $f : \mathbb{R} \to \mathbb{Q}$ лінійна функція, така, що $f(\pi) = 0$. *Інваріантом Дена* $\Phi(M)$ многогранника M називають число

$$\Phi(M) = \sum_{i=1}^{m} |e_i| f(\gamma_i),$$

де $|e_i|$ — довжина ребра e_i, γ_i — двогранний кут при ребрі e_i. Розріжемо многогранник M площиною на два многогранники M_1, M_2. Ребра многогранників M_1, M_2 можуть бути двох типів

(і) частина ребра (або все ребро) многогранника M;

(ii) ребра, що утворюються перетином полощиною якоїсь грані многогранника M;

Звідси випливає, що інваріант Дена аддитивний

$$\Phi(M) = \Phi(M_1) + \Phi(M_2),$$

а отже, інваріанти Дена рівноскладених многогранників співпадають.

Доведення теореми Дена. Нехай α — двогранний кут правильного тетраедра. Оскільки $\cos\alpha = \frac{1}{3}$, за лемою 0.3.1, існує лінійна функція $f : \mathbb{R} \to \mathbb{Q}$, така, що $f(\alpha) = 1$, $f(\pi) = 0$. За допомогою функції f побудуємо інваріанти Дена куба K і правильного тетраедра. Оскільки $\Phi(K) = 0$, $\Phi(T) \neq 0$, то K, T не є рівноскладеними за лемою 0.3.2. $\square$

Нехай S — множина із n точок в $\mathbb{R}^d$, $M = \operatorname{conv} S$ — опукла оболонка множини S. Скільки граней розмірності k може мати многогранник M? Очевидно, що грань розмірності k однозначно визначається вершинами цієї грані. Ми можемо вважати, що кожна точка із S є вершиною, а тому число таких граней не перевищує $\left(\begin{array}{c} n \\ k+1 \end{array}\right)$. Як далека ця границя від точної? Вона точна, якщо $n \leq d + 1$, досить взяти симплекс з n вершинами. Але навіть для малих розмірностей границя не точна, якщо n порівняно велике відносно d. Наприклад, якщо M — многокутник на площині, то число одновимірних граней n, а не $\left(\begin{array}{c} n \\ 2 \end{array}\right)$. Можна показати, що число одновимірних граней многогранника з n вершинами в $\mathbb{R}^3$ не перевищує $3n - 6$. Природно було б сподіватися, що існує лінійна по n оцінка числа одновимірних граней в $\mathbb{R}^4$ і т. д. Але це не так, вже в $\mathbb{R}^4$

границя $\begin{pmatrix} n \\ 2 \end{pmatrix}$ досягається. Більше того, якщо $d > 2k+1$, то границя $\begin{pmatrix} n \\ k+1 \end{pmatrix}$ досягається для будь-якого n.

Многогранник з n вершинами в $\mathbb{R}^d$ називають $(k+1)$-екстремальним, якщо число k-вимірних граней дорівнює $\begin{pmatrix} n \\ k+1 \end{pmatrix}$, тобто довільні $k+1$ вершин визначають k-вимірну грань. Очевидно, що $(k+1)$-екстремальний многогранник є l-екстремальним для всіх $l \leq k+1$.

Ми покажемо, що для кожної пари d, n натуральних чисел існує $\lfloor \frac{d}{2} \rfloor$-екстремальний многогранник M в $\mathbb{R}^d$ з n вершинами. Для побудови такого многогранника скористаймося кривою Вандермонда в $\mathbb{R}^{d+1}$, що задається параметричним рівнянням

$$m_{d+1}(\alpha) = (1, \alpha, \alpha^2, \ldots, \alpha^d), \alpha \in \mathbb{R}.$$

Якщо опустити першу координату, одержимо криву в $\mathbb{R}^d$

$$m'_d(\alpha) = (\alpha, \alpha^2, \ldots \alpha^d), \alpha \in \mathbb{R}.$$

Нехай $n \geq d+1$, $\alpha_1, \ldots, \alpha_n$ — різні дійсні числа. За означенням, *циклічний многогранник* $M(d, n)$ в $\mathbb{R}^d$ — це опукла оболонка точок $m'_d(\alpha_1), \ldots, m'_d(\alpha_n)$.

ТЕОРЕМА 0.3.6 (про циклічний многогранник). *Циклічний многогранник $M(d, n)$ має n вершин і є $\lfloor \frac{d}{2} \rfloor$-екстремальним.*

ДОВЕДЕННЯ. Давайте згодимось на таку термінологію: лінійна гіперплщина — це підпростір корозмірності 1, гіперплощина — це афінний підпростір корозмірності 1.

Для кожного натурального числа $k, k \leq \frac{d}{2}$ ми побудуємо лінійну гіперплощину P в $\mathbb{R}^{d+1}$, таку що крива Вандермонда лежить по один бік від цієї гіперплощини і лише точки

$m_d(\alpha_1), \ldots, m_d(\alpha_k)$ лежать на цій гіперплощині. Лінійну гіперплощину P визначимо рівнянням $(c, x) = 0$, де $c = (\gamma_0, \ldots, \gamma_d)$ — ненульовий вектор, визначений так, що

(i) $(c, m_{d+1}(\xi)) > 0$ для всіх $\xi \in \mathbb{R} \setminus \{\alpha_1, \ldots, \alpha_k\}$;

(ii) $(c, m_{d+1}(\alpha_i)) = 0$ для всіх $i \in \{1, \ldots, k\}$.

Для знаходження c ми розглянемо поліном f степеня k з коренями $\alpha_1, \ldots, \alpha_k$

$$f(\xi) = \prod_{i=1}^{k} (\xi - \alpha_i),$$

а за координати вектора c візьмемо коефіцієнти поліному

$$(f(\xi))^2 = \gamma_0 + \gamma_1 \xi + \cdots + \gamma_d \xi^d.$$

Це можна зробити, оскільки $2k \leq d$.

Візьмемо побудовану лінійну гіперплощину $P \subset \mathbb{R}^{d+1}$, перетнемо її з гіперплощиною $x_0 = 1$, а потім опустимо першу координату кожного вектора. Одержимо гіперплощину P' в $\mathbb{R}^d$, таку, що $M(d, n)$ лежить по один бік від P' і

$$M(d, n) \cap P' = \operatorname{conv}\{m'_d(\alpha_1), \ldots, m'_d(\alpha_k)\}.$$

Для $k = 1$ це доводить, що $m'_d(\alpha_i)$ — дійсно вершина многогранника $M(d, n)$, а для $k \leq \frac{d}{2}$ означає k-екстремальність. □

Таким чином, циклічний многогранник в $\mathbb{R}^d$ має стільки граней, скільки взагалі можливо для кожної розмірності $k \leq \lfloor \frac{d}{2} \rfloor - 1$. Для $k > \frac{d}{2}$ циклічний многогранник $M(d, n)$ вже не є k-екстремальним, але чи існує інший многогранник в $\mathbb{R}^d$ з n-вершинами, кращий за циклічний з точки зору кількості граней. Гіпотеза Моцкіна, доведемна Макмулленом 1970 року, полягала у тому, що таких многогранників немає. Отже не існує многогранника з n вершинами в $\mathbb{R}^d$, що має більше k-вимірних граней ніж $M(d, n)$ для всіх d, n, k.

На завершення ми доведемо теорему Міньковського про опукле тіло, яку можна розглядати як "опуклий“ аналог принципу Діріхле, а також вкажемо на деякі її застосування.

Нехай $a_1, \ldots, a_n$ — система лінійно незалежних векторів з $\mathbb{R}^n$. *Решіткою з базисом* $a_1, \ldots, a_n$ називають множину

$$L(a_1, \ldots, a_n) = \{z_1 a_1 + \cdots + z_n a_n : z_1, \ldots, z_n \in \mathbb{Z}\}.$$

Зрозуміло, що базис решітки визначений неоднозначно. Як перевірити, чи буде лінійно незалежна система векторів $b_1, \ldots, b_n \in L(a_1, \ldots, a_n)$ базисом цієї решітки. З алгебраїчної точки зору необхідно і достатньо, щоб матриця F переходу від $a_1, \ldots, a_n$ до $b_1, \ldots, b_n$ була цілочисельною і унімодальною $|\det F| = 1$, а з геометричної — паралелепіпед

$$P(b_1, \ldots, b_n) = \{x_1 b_1 + \cdots + x_n b_n : 0 \leq x_1, \ldots, x_n \leq 1\}$$

має бути порожнім, тобто не містити елементів решітки, відмінних від вершин $i_1 b_1 + \cdots + i_n b_n, i_1, \ldots, i_n \in \{0, 1\}$. Паралелепіпед, що визначається базисом решітки L називають основним. Як відомо з курсу лінійної алгебри і геометрії, об'єм паралелепіпеду натягнутого на вектори $a_1, \ldots, a_n$, дорівнює модулю визначника, рядками якого є вектори $a_1, \ldots, a_n$. Будь-які два основні паралелепіпеди даної решітки L мають однаковий об'єм, що називають *визначником решітки* L і позначають $\det L$.

Лема 0.3.7 (Бліхфельдта). *Нехай S — вимірна за Лебегом підмножина із $\mathbb{R}^n$, $L = L(a_1, \ldots, a_n)$ — решітка в $\mathbb{R}^n$. Якщо $\mu(S) > \det L$, то існують дві різні точки $s_1, s_2 \in S$, такі, що $s_1 - s_2 \in L$.*

Доведення. Позначимо $P' = P'(a_1, \ldots, a_n) = \{x_1 a_1 + \cdots + x_n a_n : 0 \leq x_i < 1,\ i \in \{1, \ldots, n\}\}$. Легко перевірити, що

(i) $\mathbb{R}^n = \bigcup\limits_{g \in L} (g + P')$;

(ii) $g_1 + P' \cap g_2 + P' = \emptyset$, якщо $g_1, g_2 \in L, g_1 \neq g_2$;

(iii) $\mu(P') = \det L$.

Нехай $P'_g = g + P'$. З (i) випливає, що $S = \bigcup\limits_{g \in L} (S \cap P'_g)$. З (ii) та σ-адитивності міри Лебега випливає, що

$$\mu(S) = \sum_{g \in L} \mu(S \cap P'_g).$$

Позначимо $K_g = (S \cap P'_g) - g$. Очевидно, що $K_g \subseteq P'$ і $\bigcup\limits_{g \in L} K_g \subseteq P'$. Отже, $\mu(\bigcup\limits_{g \in L} K_g) \leq \mu(P') = \det L$. Припустімо, що $K_{g_1} \cap K_{g_2} = \emptyset$ для всіх $g_1, g_2 \in L$, $g_1 \neq g_2$. Тоді

$$\det L = \mu(P') \geq \mu(\bigcup_{g \in L} K_g) = \sum_{g \in L} \mu(S \cap P'_g) = \mu(S),$$

що суперечить припущенню $\mu(S) > \det L$. Отже, знайдуться різні точки g_1, g_2 решітки L, такі, що $K_{g_1} \cap K_{g_2} \neq \emptyset$. Нехай $t \in K_{g_1} \cap K_{g_2}$. Тоді $t = s_1 - g_1 = s_2 - g_2$ для деяких $s_1, s_2 \in S$. Отже, $s_1 - s_2 = g_1 - g_2 \in L$ і лему доведено. ☐

Підмножина $S \subseteq \mathbb{R}^n$ називається *центрально-симетричною*, якщо для будь-якої точки $s \in S$ точка $-s$ належить S.

Теорема 0.3.8 (Міньковського). *Нехай S — опукла центально-симетрична множина із $\mathbb{R}^n$, L — решітка в $\mathbb{R}^n$. Якщо $\mu(S) > 2^n \det L$, то S містить відмінну від нуля θ точку решітки L. Якщо до того ж, підмножина S обмежена і замкнена, теорема справджується і за умови $\mu(S) = 2^n \det L$.*

Доведення. Нехай $S_1 = \frac{1}{2}S$. Тоді $\mu(S_1) = \frac{1}{2^n}\mu(S) > \det L$. За лемою Бліхфельдта знайдуться різні елементи $s_1, s_2 \in S_1$, такі, що $s_1 - s_2 \in L$. За означенням підмножини S_1, $s_1 = \frac{1}{2}t_1$, $s_2 = \frac{1}{2}t_2$ для деяких $t_1, t_2 \in S$. З центальної-симетричності

S випливає, що $-t_2 \in S$, а з опуклості — $\frac{1}{2}t_1 + \frac{1}{2}(-t_2) \in S$. Отже, $s_1 - s_2 \in S \cap L, s_1 - s_2 \neq \theta$.

Нехай підмножина S обмежена і замкнена, $\mu(S) \geq 2^n \det L$. Візьмемо $\epsilon, 0 < \epsilon < 1$, і позначмо $S_\epsilon = (1+\epsilon)S$. Тоді $\mu(S_\epsilon) = (1+\epsilon)^n \mu(S) > 2^n \det L$. За доведеним, знайдеться точка $y_\epsilon \in S_\epsilon \cap L, y_\epsilon \neq \theta$. Оскільки $S_\epsilon \subseteq 2S$, а підмножина $2S \cap L$ скінченна, y_ϵ може приймати лише скінченне число значень. Виберемо послідовність (ϵ_n), таку що $\epsilon_n \to 0$ і $y = y_{\epsilon_n}$ для всіх n. Тоді $y \in (1+\epsilon_n)S$ і $\frac{1}{1+\epsilon_n}y \in S$. Перейдемо до границі і одержимо $y \in S$. □

Задача 0.3.11. Обгрунтуйте мтематично прислів'я “За деревами не видно лісу."Нехай в цілочисельних точках площини, відмінних від початку координат ростуть дерева діаметру $r < 1$. В початку координат знаходиться спостерігач. Доведіть, що кожну точку віддалену від початку координат на відстань $\geq \frac{1}{r}$ не видно спостерігачу.

Розглянемо систему лінійних нерівностей

$$\begin{array}{l}
|a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n| \leq c_1, \\
|a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n| \leq c_1, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
|a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n| \leq c_n,
\end{array}$$

де $c_1 > 0, \ldots, c_n > 0$ і визначник матриці $A = (a_{ij})_{n \times n}$ відмінний від нуля. Нехай S — множина усіх розв'язків цієї системи. Ясно, що множина S опукла і центрально симетрична. Нехай $\mathcal{A}$ — лінійний оператор в $\mathbb{R}^n$, що в стандартоному базисі задається матрицею A. Зауважимо, що точка $x = (x_1, \ldots, x_n)$ належить множині S тоді і тільки тоді, коли $\mathcal{A}(x)$ належить цеглині $K = \{(y_1, \ldots, y_n) \in \mathbb{R}^n : |y_i| \leq c_i, i \in \{1, \ldots, n\}\}$, тобто

$S = \mathcal{A}^{-1}(K)$. Звідси випливає, що підмножина S обмежена і

$$\mu(S) = \frac{1}{|\det A|}\mu(K) = \frac{2^n c_1 c_2 \dots c_n}{|\det A|}.$$

За теоремою Міньковського S містить ненульову точку решітки $\mathbb{Z}^n$ за умови, що $\mu(S) > 2^n \det \mathbb{Z}^n = 2^n$. Отже, якщо $c_1 c_2 \dots c_n \geq \det A$, то система нерівностей має нетривіальний цілочисельний розв'язок. Ми застосуємо це твердження до діофантових наближень.

Теорема 0.3.9 (Кронекера). *Нехай* $\alpha_1, \alpha_2, \dots, \alpha_n, Q$ *— дійсні числа,* $Q > 1$. *Тоді існують такі цілі числа* $p_1, \dots, p_n, q$, *що*

$$|\alpha_i - \frac{p_i}{q}| \leq \frac{1}{Qq}, \quad 0 < q < Q^n, \quad i \in \{1, \dots, n\}.$$

Доведення. Розглянемо систему лінійних нерівностей

$$\begin{array}{lllll} |\alpha_1 x_1 & -x_2 & & | & \leq \frac{1}{Q}, \\ |\alpha_2 x_1 & & -x_3 & | & \leq \frac{1}{Q}, \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots\dots & \dots\dots \\ |\alpha_n x_1 & & & -x_{n+1}| & \leq \frac{1}{Q}, \\ |x_1 & & & | & \leq Q^n \end{array}$$

Зрозуміло, що $|\det A| = 1$, де A — матриця коефіцієнтів системи. Оскільки $\frac{1}{Q} \dots \frac{1}{Q} \cdot Q^n \geq |\det A|$, система має нетривіальний цілочисельний розв'язок $q, p_1, p_2, \dots, p_n$, причому $q \neq 0$. Змінюючи знаки чисел $p_1, \dots, p_n$, можна вважати, що $q > 0$. □

Для $n = 1$ теорема Кронекера перетворюється в теорему Діріхле: для довільних дійсних чисел $\alpha, Q, Q > 1$ знайдуться цілі числа p, q, такі що $0 < q \leq Q$ і

$$|\alpha - \frac{p}{q}| \leq \frac{1}{Qq} \leq \frac{1}{q^2}.$$

ТЕОРЕМА 0.3.10 (Лагранжа про чотири квадрати). *Кожне додатне ціле число* m *можна подати у вигляді суми квадратів* $m = u_1^2 + u_2^2 + u_3^2 + u_4^2$ *чотирьох цілих чисел* u_1, u_2, u_3, u_4.

ДОВЕДЕННЯ. Ми можемо вважати, що m не ділиться на квадрат простого числа, тобто $m = p_1 p_2 \dots p_k$, де $p_1, p_2, \dots, p_k$ — різні прості числа. Спочатку ми доведемо допоміжне твердження

(*) для кожного простого числа p знайдуться цілі числа a_p, b_p, такі що $a_p^2 + b_p^2 \equiv 0(\bmod p)$.

Для $p = 2$, покладемо $a_p = 1, b_p = 0$. Нехай $p \neq 2$,

$$A = \{a^2 : a \in \mathbb{Z}, 0 \leq a < \frac{1}{2}p\}, B = \{-1 - b^2 : b \in \mathbb{Z}, 0 \leq b < \frac{1}{2}p\}.$$

Кожна з підмножин A, B містить $\frac{1}{2}(p+1)$ чисел, причому різні числа кожної з підмножин є різними за модулем числа p. Дійсно нехай $a_1^2, a_2^2 \in A, a_2 > a_1$ і $a_1^2 \equiv a_2^2(\bmod p)$. Тоді $p | a_2^2 - a_1^2$. Оскільки p просте, то $p | a_2 - a_1$ або $p | a_2 + a_1$, що суперечить нерівностям $0 \leq a_2 - a_1 < p$, $0 < a_1 + a_2 < p$. Оскільки є рівно p класів чисел , еквівалентних за модулем p і $|A| + |B| = p + 1$, знайдеться ціле число c, таке що

$$c \equiv a_p^2(\bmod p), \quad c \equiv -1 - b^2(\bmod p),$$

де $a_p \in A$, $-1 - b_p^2 \in B$. Отже, $a_p^2 + b_p^2 + 1 \equiv 0(\bmod p)$.

Розглянемо сисетему порвінянь

$$\begin{aligned}
u_1 &\equiv a_{p_1} u_3 + b_{p_1} u_4(\bmod p_1), \\
u_2 &\equiv b_{p_1} u_3 - a_{p_1} u_4(\bmod p_1), \\
u_1 &\equiv a_{p_2} u_3 + b_{p_2} u_4(\bmod p_2), \\
u_2 &\equiv b_{p_2} u_3 - a_{p_2} u_4(\bmod p_2), \\
&\dots\dots\dots\dots\dots\dots\dots\dots \\
u_1 &\equiv a_{p_k} u_3 + b_{p_k} u_4(\bmod p_k), \\
u_2 &\equiv b_{p_k} u_3 - a_{p_k} u_4(\bmod p_k),
\end{aligned}$$

де $a_{p_i}^2+b_{p_i}^2+1\equiv 0(\bmod p)$. Множина L цілочисельних розв'язків цієї системи є решіткою в $\mathbb{R}^4$, причому $\det L \le p_1^2p_2^2\dots p_k^2$. Куля S радуса $\sqrt{2m}$ з центром в початку координат має міру $2\pi^2m^2 = 2\pi^2p_1^2p_2^2\dots p_k^2 > 2^4\det L$. За теоремою Міньковського знайдеться ненульова точка

$$u = (u_1, u_2, u_3, u_4) \in L \cap S,$$

а тому $0 < u_1^2+u_2^2+u_3^2+u_4^2 < 2m$. Оскільки точка u задовольняє систему порівнянь, то

$$u_1^2+u_2^2+u_3^2+u_4^2 \equiv (a_{p_i}u_3+b_{p_i}u_4)^2+(b_{p_i}u_3-a_{p_i}u_4)^2+u_3^2+u_4^2(\bmod p_i)$$

для всіх $i \in \{1, 2, \dots, n\}$. Значить,

$$u_1^2+u_2^2+u_3^2+u_4^2 \equiv (a_{p_i}^2+b_{p_i}^2+1)u_3^2+(a_{p_i}^2+b_{p_i}^2+1)u_4^2(\bmod p_i) \equiv 0(\bmod p_i)$$

Оскільки числа $p_1, p_2, \dots, p_k$ попарно взаємно прості,

$$u_1^2+u_2^2+u_3^2+u_4^2 \equiv 0(\bmod p_1p_2\dots p_k) \equiv 0(\bmod m),$$

і твердження теореми випливає з нерівності $u_1^2+u_2^2+u_3^2+u_4^2 < 2m$. □

Про інші застосування теореми Міньковського в геометрії чисел див. [3]. Метод Дена докладніше описано в [1]. Про історію теореми Хелі і її застосування в функціональному аналізі див [2].

Бібліоґрафія

[1] Болтянський В. Г. Третья проблема Гильберта. М., "Наука 1977.
[2] Данцер Л., Грюнбаум Б., Кли В. Теорема Хелли. М., "Мир 1968
[3] Касселс Дж. Введение в геометрию чисел. М., "Мир 1965.

0.4. Принцип Діріхле і теорема Пуанкаре

Якщо m предметів (зазвичай, кролів або голубів) розкладено в n ящиків і $m > n$, то знайдуться принаймні два предмети, що знаходяться в одному ящику. Трохи математичніше, якщо X, Y — скінченні множини, $|X| > |Y|$ і $f : X \to Y$ довільне відображення, то існують різні елементи $x_1, x_2 \in X$ такі, що $f(x_1) = f(x_2)$. Це абсолютно очевидне твердження називають принципом Діріхле (що, мабуть, безпідставно) або pigeonhole principle (що цілком виправдано). Ми продемонструємо як нетривіальні застосування цього твердження (разом з іншими аргументами) приводять до цікавих і не зовсім очевидних результатів. Для розгону пропонуємо підбірку задач з **[11]** на застосування принципу Діріхле.

Задача 0.4.1. Доведіть, що серед будь-яких n натуральних чисел записаних у довільному порядку, можна вибрати кілька сусідніх, сума яких ділиться на n.

Задача 0.4.2. Доведіть, що серед будь-яких $n+1$ різних натуральних чисел, не більших за $2n$, можна знайти два числа, одне з яких ділиться на друге.

Задача 0.4.3. Доведіть, що серед будь-яких $n+1$ різних натуральних чисел, менших за $2n$, можна знайти два числа, сума яких дорівнює третьому.

Задача 0.4.4. Доведіть, що серед будь-яких 100 натуральних чисел можна знайти 15 чисел, таких що різниця будь-яких двох з них ділиться на 7.

Задача 0.4.5. Доведіть, що з будь-яких десяти двозначних чисел можна вибрати дві групи чисел так, що сума чисел в цих групах однакові.

Задача 0.4.6. Нехай a, b, x_0 — натуральні числа. Доведіть, що серед членів послідовності

$$x_0, x_1 = ax_0 + b, \ldots, x_{n+1} = ax_{n-1} + b, \ldots.$$

нескінченно багато чисел, що не є простими.

Задача 0.4.7. Дано п'ять точок площини з цілочисельними координатами. Доведіть, що серед усіх трикутників з вершинами в цих точках є принаймні три, площі яких виражаються цілими числами.

Задача 0.4.8. У квадрат зі стороною 1 кинуто $2n^2+1$ точок. Доведіть, що деякі три з них містяться у крузі радіуса $\frac{\sqrt{2}}{2n}$.

Задача 0.4.9. Куб розбили на 27 однакових кубиків. Жук у початковий момент знаходиться у центральному кубику і далі може перейти в кубик, що має спільну грань з тим, в якому він знаходиться. Чи може жук обійти всі кубики побувавши в кожному лише раз?

ЗАДАЧА 0.4.10. Кожна грань куба пофарбована одним з двох кольрів. Доведіть, що знайдуться дві однакольорові грані, що мають спільне ребро.

ЗАДАЧА 0.4.11. У лісі на площі квадрата зі стороною 1 км росте 4500 дерев, діаметр яких 50 см. Доведіть, що в лісі можна вибрати прямокутник розмірів 10м×20м, в якому не росте жодне дерево.

Свою власну назву принцип Діріхле отримав завдяки наступній теоремі, хоча застосовувався цей аргумент багато століть раніше.

ТЕОРЕМА 0.4.1 (Діріхле). *Нехай α — ірраціональне число, s — будь-яке натуральне число. Тоді існують цілі числа x, y такі що*

$$|\alpha x - y| < \frac{1}{s}, 0 < x \leq s.$$

ДОВЕДЕННЯ. Нехай $[a], \{a\}$ — ціла та дробова частини числа a. Надаватимемо x в $\{x\alpha\}$ значень $0, 1, \ldots, s$. Тоді дістанемо $s + 1$ різне число з відрізка $[0, 1]$. Усі числа будуть різними, бо якщо при $x_1 \neq x_2$ $x_1\alpha - [x_1\alpha] = x_2\alpha - [x_2\alpha]$, то число $\alpha = \frac{[x_1\alpha]-[x_2\alpha]}{x_1-x_2}$ раціональне. Поділимо відрізок $[0, 1]$ на s рівних проміжків довжиною $\frac{1}{s}$. За принципом Діріхле існує проміжок що містить два числа $\{x_1\alpha\}$, $\{x_2\alpha\}$, $x_2 > x_1$. Тоді $|\{x_2\alpha\} - \{x_1\alpha\}| < \frac{1}{s}$ і покладемо $x = x_2 - x_1$ $y = [x_2\alpha] - [x_1\alpha]$. □

Теорема Діріхле виникла у зв'язку з наближеннями ірраціональних чисел раціональними — діофантовою апроксимізацією. З неї безпосередньо випливає, що для будь-якого ірраціонального числа α існує нескінченно багато натуральних чисел $\frac{m}{n}$, таких що $|\alpha - \frac{m}{n}| < \frac{1}{n^2}$. Таку послідовність $\left(\frac{p_k}{q_k}\right)_{k\in\omega}$

наближень можна побудувати за допомогою розкладень α в ланцюговий дріб.

Дещо делікатнішим є таке застосування принципу Діріхле.

Теорема 0.4.2 (Зігеля). *Дано систему лінійних діофантових рівнянь*

$$\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0, \\ \dotfill \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0. \end{array}$$

Якщо $m < n$ і $|a_{ij}| < C$ для всіх i, j, то існує нетривіальний цілочисельний розв'язок $x^* = (x_1^*, \ldots, x_n^*)$, в якому

$$|x_j|^* \leq 2(nC)^{\frac{m}{n-m}}, j \in \{1, \ldots, n\}.$$

Доведення. Визначимо лінійний оператор $\mathcal{A} : \mathbb{R}^n \to \mathbb{R}^m$

$$\mathcal{A}(x) = (a_{11}x_1 + \cdots + a_{1n}x_n, \ldots, a_{m1}x_1 + \cdots + a_{mn}x_n).$$

Для додатніх цілих чисел s, t позначимо

$$N(s) = \{x \in \mathbb{Z}^n : |x_j| \leq s, j \in \{1, \ldots, n\}\},$$

$$M(t) = \{y \in \mathbb{Z}^m : |y_i| \leq t, i \in \{1, \ldots, m\}\}.$$

Якщо $x \in N(s)$, то $\mathcal{A}(x) \in M(nCs)$. Крім того

$$|N(s)| = (2s + 1)^n, |M(nCs)| = (2nCs + 1)^m.$$

Розглянемо нерівність $|N(s)| > |M(nCs)|$. Оскільки

$$(2nCs + 1)^n = (2s + \frac{1}{nC})^m (nC)^m < (2s + 1)^m (nC)^m,$$

$$(2s + 1)^n = (2s + 1)^m (2s + 1)^{n-m},$$

то нерівність $|N(s)| > |M(nCs)|$ правильна, якщо $(2s+1)^{n-m} \geq (nC)^m$, зокрема, при $s = [(nC)^{\frac{m}{n-m}}]$. За принципом Діріхле, знайдуться $x, x' \in N([(nC)^{\frac{m}{n-m}}])$, такі що $x \neq x'$ і $\mathcal{A}(x) = \mathcal{A}(x')$. Тоді $x^* = x - x'$ — потрібний нам розв'язок системи. □

Якщо $A_1, \ldots, A_m$ — підмножини скінченної множини X і $|A_1| + \cdots + |A_m| > |X|$, то знайдуться $i, j, i \neq j$, такі, що $A_i \cap A_j \neq \emptyset$. Застосуйте це спостереження до такої задачі.

Задача 0.4.12. Нехай скінченну групу G розбито на m підмножин. Доведіть, що знайдуться підмножина A розбиття і підмножина $F \subseteq G$, такі, що $G = FAA^{-1}$ і $|F| \leq m$.

Трохи загальніше. Нехай X — множина, μ — зліченно-адитивна міра, визначена на деякій σ-алгебрі $\mathcal{B}$ підмножин з X, $\mu(X) = 1$. Якщо $\{B_N : n \in \omega\}$ — сім'я підмножин з $\mathcal{B}$ і $\sum\limits_{n \in \omega} \mu(B_n) > 1$, то знайдуться принаймні дві різні підмножини B_i, B_j, такі, що $B_i \cap B_j \neq \emptyset$ Протягом попередніх лекцій ми вже застосовували подібні міркування, наприклад, при доведенні леми Бліхфельдта в "Комбінаториці опуклих множин". Окремий випадок цього спостереження ($X = \mathbb{R}^2$, μ — міра Лебега) М. Й. Ядренко [**11**] називає принципом Діріхле для площ. Ми застосуємо цей аргумент до доведення теореми Пуанкаре. Нехай X — обмежена відкрита підмножина в просторі $\mathbb{R}^n$, T — гомеоморфізм X, що зберігає об'єм, тобто підмножини V і $T^{-1}(V)$ мають однаковий об'єм для будь-якої вікритої підмножини V із X. Під дією перетворення T кожна точка $x \in X$ породжує послідовність $x, T(x), \ldots, T^k(x), \ldots$, що називається *орбітою* x. За означення, точка x *повертається* у підмножину $V \subseteq X$, якщо V містить нескінченне число точок орбіти x.

Теорема 0.4.3 (Пуанкаре). *Для будь-якої відкритої підмножини $V \subseteq X$ точками, що повертаються у V є всі точки із V за винятком деякої множини точок міри 0.*

Доведення. Перш за все зауважимо, що гомеоморфізм $T : X \to X$ є вимірним за Борелем, тобто для будь-якої борелевої множини $A \subseteq X$ множина $T^{-1}(A)$ борелева. Оскільки T зберігає об'єм будь-якої відкритої множини, то $\mu(A) =$

$\mu(T^{-1}(A))$ для будь-якої борелевої множини A, μ — міра Лебега.

Візьмемо довільну відкриту підмножину $V \subseteq X$ і покажемо, що множина H точок із V, які не повертаються в V, вимірна за Борелем і має міру нуль. Покладемо

$$F = V \setminus \bigcup_{k=1}^{\infty} T^{-k}(V).$$

Точка x належить F тоді і тільки тоді, коли $x \in V$, $T^k(x) \notin V$ для будь-якого натурального k. Таким чином, F — множина точок із V, що полишають множину V на першому кроці і ніколи до неї не повертаються. Зрозуміло, що F — борелева множина. Якщо i, j — натуральні числа, $j > i$, то

$$T^{-j}(F) \cap T^{-i}(F) \subseteq T^{-j}(V) \setminus \bigcup_{k=1}^{\infty} T^{i-k}(V).$$

Оскільки $j = i + k$ для деякого натурального k, то $T^{-j}(F) \cap T^{-i}(F) = \emptyset$. Оскільки $\mu(T^{-j}(F)) = \mu(T^{-i}(F)) = \mu(F)$ і $\mu(X) < \infty$, то $\mu(F) = 0$ (тут спрацював наш принцип). Із зліченної адитивності μ випливає, що $\mu(\bigcup\limits_{i=0}^{\infty} T^{-i}(F)) = 0$. Точка x належить до $T^{-1}(F)$ тоді і тільки тоді, коли $T^i(x) \in V, T^{i+k}(x) \notin V$ для будь-якого натурального k. Отже, $H = V \cap (\bigcup\limits_{i=0}^{\infty} T^{-i}(F))$ і $\mu(H) = 0$. □

Цю терему називають теоремою про повернення. Точку $x \in X$ називають *рекурнтною* точкою відображення T, якщо вона повертається в кожен свій окіл.

Теорема Пуанкаре про рекурентність стверджує, що всі точки з X за винятком деякої множини точок міри нуль є рекурентними.

Цю теорему просто вивести з теореми про повернення. Нехай $\{U_k : k \in \omega\}$ — зліченна база простору X, E_k — множина точок з U_k що не повертаються в U_k. За теоремою про повернення E_k є нуль-множиною. Отже, $E = \bigcup\limits_{k \in \omega} E_k$ також нуль-множина. Якщо $x \in X \setminus E$ і U — довільний окіл точки x, то $x \in U_k \subseteq U$ для деякого натурального k. Оскільки $x \notin E_k$, то $T^i(x) \in U_k$ для нескінченної множини натуральних чисел. Отже, кожна точка з X рекурентна.

Теорему про повернення Пуанкаре виклав (щоправда не досить обгрунтовано, бо на той час ще не було строгого означення міри) 1899 року в своїх студіях з небесної механіки [**4**]. В класичній механіці стан сисеми однозначно визначається набором координат $q_1, \ldots, q_n$ і імпульсів $p_1, \ldots, p_n$. Ці $2n$ значень задають точку у просторі $\mathbb{R}^{2n}$. Усі такі точки утворюють фазовий простір X системи. Таким чином, точки фазового простору зображають усі можливі стани системи. Зміну положення точки фазового простору описує система звичайних диференціальних рівнянь. За одиницю часу початкова точка x переходить в деяку точку $T(x)$. Отже, рівняння руху визначають деяке пертворення $T : X \to X$. Із теореми про існування і однозначність розв'язку системи диференціальних рівнянь випливає, що перетворення T є гемеоморфізмом за умови достатньої гладкості функцій, які входять до системи рівнянь. Більше того, рівняння Н'ютона, записані в координатах та імпульсах (тобто в гамільтоновій формі), визначають перетворення T, що зберігає об'єм. Цей факт відомий як теорема Ліувіля: для консерватавних систем повна енергія постійна. Для деяких систем фазовий простір X є обмеженою і відкритою множиною в $\mathbb{R}^2 n$. Усім цим умовам задовільняє система диференціальних рівнянь, що описує рух планет Сонячної системи. А тому із теореми Пуанкаре випливає, що майже для усіх початкових положень (з точки зору міри) система нескінченно часто повертається до положень як завгодно близьких до початкових положень.

З теореми Пуанкаре виросли дві сучасні математичні теорії: топологічна динаміка і ергодична теорія. Про топологічну динаміку розповідається далі в лекції “Топологічна динаміка і комбінаторика". Предмет ергодичної теорії — відображення, що зберігають міру. Докладніше, нехай X — деяка множина, μ — зліченно-адитивна міра, визначена на деякій σ-алгебрі $\mathcal{B}$ підмножин з X, $\mu(X) = 1$. Трійку $(X, \mathcal{B}, \mu)$ називають *простором з мірою*. За означенням, вимірне відображення $T : X \to X$ зберігає міру (або μ-консервативне), якщо $\mu(V) = \mu(T^{-1}(V))$ для будь-якої підмножини $V \in \mathcal{B}$. Четвірку $(X, \mathcal{B}, \mu, T)$ назвімо μ-системою. Претворення T називають *ергодичним* якщо для довільної підмножини $A \in \mathcal{B}$ із $A = T^{-1}(A)$ випливає, що $\mu(A) = 0$ або $\mu(X \setminus A) = 0$. Наріжним камене ергодичної теорії є таке твердження.

Теорема 0.4.4 (Ергодична теорема Біркгофа-Хінчина). *Якщо* $(X, \mathcal{B}, \mu, T)$ *— μ-система і* $f : X \to \mathbb{R}$ *— μ-інтегровна функція, то границя*

$$\lim_{m\to\infty} \frac{1}{m} \sum_{n=0}^{m-1} f(T^n(x))$$

існує для майже всіх $x \in X$. *Якщо, до того ж, перетворення* T *ергодичне, то ця границя дорівнює*

$$\int f(x) d\mu.$$

Отже, за умови ергодичності T для майже усіх $x \in X$ середнє по часу $\lim\limits_{m\to\infty} \frac{1}{m} \sum\limits_{n=0}^{m-1} f(T^n(x))$ дорівнює просторовому середньому $\int f(x)d\mu$. Адаптований до наближених обчислень варіант цього твердження варіант носить назву методу Монте-Карло.

1927 року ван дер Варден [**6**] довів досить нетривіальним застосуванням принципу Діріхле таку теорему: для довільного розфарбування множини натуральних чисел скінченним числом кольорів знайдуться як завгодно довгі однокольрові арифметичні прогресії. 1975 року Семереді [**5**] довів глибоке посилення теореми ван дер Вардена: кожна підмножина натуральних чисел додатньої верхньої щільності містить як завгодно довгі арифметичні прогресії. Верхня щільність підмножини $A \subseteq \mathbb{N}$ — це число

$$\overline{d}(A) = \lim\sup_{n\to\infty} \frac{A \cap \{1, \dots, n\}}{n}.$$

Кажуть, що оригінальне доведення Семереді зрозуміли всього два математики, одним з яких був Семереді. Принципово інше доведення теореми Семереді , що прояснило природу цього факту, дав Фюрстенберг [**3**].

Банахова щільність підмножини $A \subseteq \mathbb{N}$ — це число

$$d^*(A) = \sup\{\alpha \in \mathbb{R} : \forall n \in \mathbb{N} \exists m \quad \geq n \exists x \in \mathbb{N} \text{ такі, що } \frac{|A \cap \{x+1, \dots, x+m\}|}{m} \geq \alpha\}.$$

Зрозуміло, що $d^*(A) \geq \overline{d}(A)$ для будь-якої підмножини $A \subseteq \mathbb{N}$.

Теорема 0.4.5 (Фюрстенберга). *Нехай $(X, \mathcal{B}, \mu)$ — простір з мірою, $T_1, \dots, T_l$ — попарно комутуючі μ-консервативні відображення простору X, $B \in \mathcal{B}$, $\mu(B) > 0$. Тоді існує $d \in \mathbb{N}$, таке що*

$$\mu(B \cap T_1^{-1}(B) \cap \dots \cap T_l^{-d}(B)) > 0.$$

Вивести теорему Семереді є теореми Фюрстенберга можна за допомогою принципу переносу.

Принцип преносу. *Нехай* $A \subseteq \mathbb{N}$, $d^*(A) > 0$. *Тоді існують* μ*-система* $(X, \mathcal{B}, \mu, T)$, *в якій* X *— компактний метричний простір,* T *— гомеоморфізм, а також підмножина* $A' \subseteq X$, *такі, що*

(*) $\mu(A') = d^*(A)$;

(**) для довільних натуральних чисел $n_1, \ldots, n_k$

$$d^*(A \cap (A - n_1) \cap \cdots \cap (A - n_k)) \geq \mu(A' \cap T^{-n_1}(A') \cap \cdots \cap T^{-n_k}(A')).$$

Доведення. Нехай $\Omega = \{0,1\}^{\mathbb{Z}}$ з топологією добутку. Елементами простору Ω є нескінченні в обидва боки вектори з координатами 0,1. Позначимо через $T : \Omega \to \Omega$ зсув на одну позицію вліво $T(x)(n) = x(n+1)$. Нехай ξ — характеристичний вектор A як підмножини $\mathbb{Z}$, X — замикання в Ω множини $\{T^n(\xi) : n \in \mathbb{N}\}$. Звуження T на X є гомеомофізмом X.

Для кожного $n \in \mathbb{Z}$ позначимо $D_n = \{\delta \in X : \delta(n) = 1\}$ і зауважимо, що D_n відкрито-замкнена підмножина X. Нехай $\mathcal{A}$ — булева алгебра, породжена $\{D_n : n \in \mathbb{Z}\}$, а $\mathcal{B}$ — σ-алгебра, породжена $\{D_n : n \in \mathbb{Z}\}$. Для кожного $n \in \mathbb{Z}$ маємо $T(D_n) = D_{n-1}$, $T^{-1}(D_n) = D_{n+1}$. Отже, якщо $B \in \mathcal{B}$, то $T^{-1}(B) \in \mathcal{B}$.

Нехай $\mathcal{P}(X)$, $\mathcal{P}(\mathbb{N})$ — родини усіх підмножин $X, \mathbb{N}$. Визначимо відображення $\varphi : \mathcal{P}(X) \to \mathcal{P}(\mathbb{N})$ за правилом

$$\varphi(B) = \{n \in \mathbb{N} : T^n(\xi) \in B\}.$$

Оскільки $\alpha = d^*(A) > 0$, ми можемо вибрати послідовність відрізків $(I_k)_{k \in \omega}$ в $\mathbb{N}$, таку що $\lim |I_k| = \infty$ і

$$\lim \frac{|A \cap I_k|}{I_k} = \alpha.$$

Далі ми скористаємось границями послідовностей за ультрафільтром. Означення та елементарні властивості ультрафільтрів можна знайти в лекції "Комбінаторика ультрафільтрів".

Нехай p — вільний ультрафільтр на $\omega = \{0, 1, \dots\}$, $(\alpha_k)_{k\in\omega}$ — обмежена послідовність дійсних чисел. Сім'я підмножин $\{\alpha_k : k \in P\}, P \in p$ є базою деякого (однозначно визначеного) ультрафільтру на $\mathbb{R}$. Границю цього ультрафільтру позначимо $p - \lim \alpha_k$.

Визначимо відображення $\nu : \mathcal{P}(X) \to [0, 1]$ за правилом

$$\nu(B) = p - lim \frac{|\varphi(B) \cap I_k|}{I_k}.$$

Зрозуміло, що $\nu(X) = 1$. Для довільних $B, C \subseteq X$ маємо

$$\varphi(B \cap C) = \varphi(B) \cap \varphi(C), \quad \varphi(B \cup C) = \varphi(B) \cup \varphi(C).$$

Отже, якщо $B \cap C = \emptyset$, то

$$\nu(B \cup C) = p - \lim \frac{|\varphi(B) \cap I_k| + |\varphi(C) \cap I_k|}{|I_k|} = \nu(B) + \nu(C).$$

Переконаймося, що $\nu(T^{-1}(B)) = \nu(B)$ для довільної підмножини $B \subseteq X$. Дійсно, $\varphi(T^{-1}(B)) = (\varphi(B) - 1) \cap \mathbb{N}$, а тому

$$\nu(T^{-1}(B)) = p\text{–}\lim \frac{|(\varphi(B) - 1) \cap I_k|}{|I_k|} = p\text{–}lim \frac{|\varphi(B) \cap I_k|}{|I_k|} = \nu(B).$$

Таким чином, функція ν скінченно адитивна і T-інваріантна на $\mathcal{P}(X)$, а отже і на $\mathcal{A}$. Нехай $(B_n)_{n\in\omega}$ — послідовність в $\mathcal{A}$, така що $B_{n+1} \subseteq B_n$ і $\cap_{n\in\omega} B_n = \emptyset$. В силу компактності X і відкрито-замкнености B_n, знайдеться $m \in \omega$, таке що $B_n = \emptyset$ для всіх $n \geq m$. Отже, $\lim \nu(B_n) = 0$. Звідси випливає, що скінченно адитивну міру ν на $\mathcal{A}$ можна продовжити до зліченно-адитивної міри μ на $\mathcal{B}$ за формулою

$$\mu(B) = \inf\{\sum_{C\in\mathcal{C}} \nu(C) : \mathcal{C} \subseteq \mathcal{A}, |\mathcal{C}| \leq \omega, B \subset \cup\mathcal{C}\}.$$

З означення μ випливає, що $\mu(T^{-1}(B)) = \mu(B)$ для кожного $B \in \mathcal{B}$. Таким чином, $(X, \mathcal{B}, \mu, T)$ — μ система. Покладемо $A' = D_0 = \{\delta \in X : \delta(0) = 1\}$. Оскільки $\varphi(A') = A$, $T^{-n}(A') = D_n$ і $\varphi(D_n) = (A - n) \cap \mathbb{N}$, маємо

$$\mu(A') = \nu(A') = p - \lim \frac{|\varphi(A') \cap I_k|}{|I_k|} = p - \lim \frac{|A \cap I_k|}{|I_k|} = \alpha.$$

Якщо F — скінченна підмножина з $\mathbb{N}$, то

$$\mu(A' \cap \bigcap_{n \in F} T^{-n}(A')) = \mu(D_0 \cap \bigcap_{n \in F} D_n) =$$

$$\nu(D_0 \cap \bigcap_{n \in F} D_n) = p - \lim \frac{|\varphi(D_0) \cap \bigcap_{n \in F} \varphi(D_n) \cap I_k|}{|I_k|} =$$

$$p - \lim \frac{|A \cap \bigcap_{n \in F} (A - n) \cap I_k|}{|I_k|} \leq d^*(A \cap \bigcap_{n \in F} (A - n)))$$

і ми перевірили обидва твердження (*), (**).

Для доведення теореми Семереді, нехай $A \subseteq \mathbb{N}$, $\overline{d}(A) > 0$ (а, отже, $d^*(A) > 0$) і ми хочемо знайти в A арифметичну прогресію довжини l. Нехай $(X, \mathcal{B}, \mu, T)$ — μ-система, визначена принципом переносу. Позначимо $T_i = T^i$ для всіх $i \in \{1, \dots, l\}$. Очевидно, що $T_1, \dots, T_l$ — попарно комутуючі μ-консервативні відображення. За теоремою Фюретенберга існує $d \in \mathbb{N}$, таке, що

$$\mu(A' \cap T_1^{-d}(A') \cap \cdots \cap T_l^{-d}(A')) > 0.$$

Оскільки $T_i^{-d} = T^{id}$, маємо

$$d^*(A \cap (A - d) \cap (A - 2d) \cap \cdots \cap (A - ld)) \geq$$

$$\mu(A' \cap T^{-d}(A') \cap \cdots \cap T^{-ld}(A')) > 0.$$

Нехай a — довільне число з $A \cap (A - d) \cap \cdots \cap (A - ld)$. Тоді

$$\{a, a + d, \dots, a + ld\} \subseteq A.$$

$\square$

Розглянемо ще один комбінаторний спосіб — метод усереднення. Припустімо, що нам треба довести існування об'єкту з заданою властивістю в деякій скінченній множині. Якщо ми знаємо кількість елементів множини або можемо оцінити їх знизу деяким числом A, а також можемо оцінити зверху деяким числом B кількість елементів множини, що не мають даної властивості, і виявиться, що $B < A$, нашу задачу розв'язано (хоч ми і не вказали конкретного елементу з заданою властивістивістю). Дещо загальніше: нехай нам вдалося визначити відображення $f : X \to \mathbb{R}$ і показати, що $\sum_{x\in Y} f(x) < \sum_{x\in X} f(x)$, де Y — множина елементів, що не володіють потрібною властивістю, задачу розв'язано.

Ми продемонструємо цей прийом доведенням такого твердження [**9**].

ТВЕРДЖЕННЯ 0.4.1. *Якщо множину $\mathbb{Z}_n$ вершин правильного n-кутника M_n пофарбовано двома кольорами, то знайдеться вісь симетрії M_n, така що принаймні половина вершин $\mathbb{Z}_n$ зберігає колір при симетрії відносно цієї осі.*

ДОВЕДЕННЯ. Множину $\mathbb{Z}_n$ ми розглядаємо як циклічну групу лишків $\bmod n$. Опишемо навколо многокутника M_n коло і кожній вершині a співставимо вісь l_a, що проходить через середину дуги oa. Нескладно перевірити, що вершини x, y симетричні відносно осі l_a тоді і тільки тоді, коли $x + y \equiv a(\bmod n)$. Для кожного розфабування $\chi : \mathbb{Z}_n \to \{0, 1\}$ означимо характеристичні функції $\chi_0(x), \chi_1(x)$, де $\chi_0(x) = 1$ тоді і лише тоді, коли $\chi(x) = 0$, а $\chi_1(x) = 1 - \chi_0(x)$. Для осі симетрії l_a згортка

$$\chi_0 * \chi_0(a) = \sum_{x\in\mathbb{Z}_n} \chi_0(x)\chi_0(a - x)$$

дорівнює кількості вершин x кольору 0, для яких вершина $a-x$, симетрична відносно осі l_a, теж кольору 0. Аналогічно, згортка

$$\chi_1 * \chi_1(a) = \sum_{x\in\mathbb{Z}_n} \chi_1(x)\chi_1(a-x)$$

дорівнює кількості вершин x, кольору 1, для яких вершина $a-x$, симетрична відносно l_a, теж кольору 1. Тоді число вершин $S(\chi,a)$, що зберігають колір при симетрії відносно l_a, дорівнює $\chi_0 * \chi_0(a) + \chi_1 * \chi_1(a)$. Тепер наша мета — показати, що сума величин $S(\chi,a)$ по всіх осях симетрії не менша за $\frac{n^2}{2}$, а тому існує хоча б одна вісь, для якої $S(\chi,a) \geq \frac{n^2}{2}$. Дійсно

$$\sum_{a\in\mathbb{Z}_n} S(\chi,a) = \sum_{a\in\mathbb{Z}_n} (\chi_0 * \chi_0(a) + \chi_1 * \chi_1(a)) =$$

$$\sum_{a\in\mathbb{Z}_n} (\sum_{x\in\mathbb{Z}_n} (\chi_0(x)\chi_0(a-x) + \chi_1(x)\chi_1(a-x))) =$$

$$\sum_{x\in\mathbb{Z}_n} \chi_0(x) \sum_{a\in\mathbb{Z}_n} \chi_0(a-x) + \sum_{x\in\mathbb{Z}_n} \chi_1(x) \sum_{a\in\mathbb{Z}_n} \chi_1(a-x) =$$

$$(\sum_{x\in\mathbb{Z}_n} \chi_0(x))^2 + (\sum_{x\in\mathbb{Z}_n} \chi_1(x))^2.$$

Оскільки $\sum_{x\in\mathbb{Z}_n} \chi_0(x) + \sum_{x\in\mathbb{Z}_n} \chi_1(x) = n$, $\sum_{a\in\mathbb{Z}_n} S(\chi,a) \geq \frac{n^2}{2}$. □

Більше про симетрію розфабувань можна прочитати в [**1**],[**8**],[**9**].

Нехай G — скінченна група, $|G| = n$, $A \subseteq G$, $|A| = k$. Підмножину $M \subseteq G$ називають груповим доповненням до A, якщо $G = AM$. Усередненням ми доведемо таке твердження [**7**]:

Твердження 0.4.2. *Існує групове доповнення M до A, таке що $|M_0| \leq \frac{\log k+2}{k} n$.*

Доведення. Ми можемо вважати, що підмножина A містить одиницю e групи G. Якщо $T \subseteq G$ і $M = T \cup \{g \in G : A^{-1}g \cap T = \emptyset\}$, то $G = AM$. Дійсно, нехай $g \in G$. Якщо $A^{-1}g \cap T = \emptyset$, то $g \in M$ і $g = ea \in AM$. Якщо $A^{-1}g \cap T \neq \emptyset$, то $g = at \in AM$.

Розглянемо множину пар $(A^{-1}g, M)$, $g \in G$, $A^{-1}g \cap M = \emptyset$, $|M| = m$, m —фіксоване натуральне число $\leq n$. Число таких пар дорівнює $n \binom{n-k}{m}$. Це ж число можна порахувати як

$$\sum_{M \subseteq G} k(M), \quad k(M) = |\{g : A^{-1}g \cap M = \emptyset\}|.$$

Оскільки кількість доданків в цій сумі $\binom{n}{m}$, знайдеться M_0, таке що $k(M_0) \leq \frac{n\binom{n-k}{m}}{\binom{n}{m}}$. Нехай $M = M_0 \cap \{g \in G : A^{-1}g \cap M_0 = \emptyset\}$. Тоді

$$|M| \leq m + \frac{n\binom{n-k}{m}}{\binom{n}{m}}, \quad \frac{|M|}{n} \leq \frac{m}{n} + \frac{\binom{n-k}{m}}{\binom{n}{m}} \leq \frac{m}{n} + (1-\frac{k}{n})^m \leq \frac{m}{n} + e^{-\frac{km}{n}}.$$

Виберемо m так, щоб

$$\frac{n\log k}{k} \leq m \leq \frac{n\log k}{k} + 1 \leq \frac{\frac{n\log k}{k} + 1}{n} + e^{-\frac{k}{n} \cdot \frac{n\log k}{k}} =$$

$$\frac{\log k}{k} + \frac{1}{n} + \frac{1}{k} \leq \frac{\log k + 2}{k}.$$

□

Метод усереднення є основою для ймовірнісних методів в комбінаториці [**10**].

На завершення відмітимо ще один корисний прийом — “принцип крайнього". Нехай ми маємо довести існування об’єкту з деякою властивістю в деякій скінеченній множині X. Інколи це можна зробити так: визначимо деяке відображення $f : X \to \mathbb{R}$ і знайдемо елемент $x_0 \in X$, на якому функція f набуває мінімального чи максимального значення. Ось кілька задач, розв’язати які напростіше за "принципом крайнього“.

Задача 0.4.13. На площині задано $2n$ точок в загальному положенні (жодні три точки не лежать на одній прямій). Половину з цих точок пофарбовано жовтим кольором, а половину — блакитним. Доведіть, що можна вказати n відрізків з різнокольоровими кінцями, що попарно не перетинаються.

Задача 0.4.14. Точка p площини лежить в перетині трьох трикутників. Доведеть, що можна в кожному з трикутників вибрати по одній вершині так, що p лежить в трикутнику з цими вершинами.

Задача 0.4.15. Не площині задано скінченну множину точок X. Якщо взяти будь-які дві точки з X провести через них пряму, то на цій прямій знайдеться ще принаймні одна точка з X. Доведіть, що всі точки з X лежать на одній прямій.

Остання задача поставлена Сільвестром 1893 року, була розв’язана лише через 50 років. Про історію цієї задачі та пов’язані з нею комбінаторні проблеми див [**2**].

Бібліоґрафія

[1] Banakh T., Protasov I. Symmetry and colorings: some results and open problems, Изв. Гомельского ун-та, 17 (2002), 4-15.

[2] Erdős P. On the combinatorical problems which I found like to see solved. Combinatorica, 1 (1981), 25-42.

[3] Furstenberg H. Ergodic behavior of diagonal measures and a theorem of Szemeredi on arithmetic progressins, J. Anal. Math., 31 (1977), 204-256.

[4] Poincaré H. Les me'thodes nouvelles de la mécanique céleste, Vol 3, Paris, Gauthier-Villars, 1989.

[5] Szemeredi E. On sets of integers containing no k elements in arithmetic progression, Acta Arith., 27 (1975), 199-245.

[6] van der Warden B. Beweis einer Baudetsen Vermutung, Nieuw. Arch. Wish., 15 (1927), 212-216.

[7] Weinstein G. Minimal complementary sets, Trans. AMS, 212 (1975), 131-137.

[8] Банах Т., Вербицкий О., Воробец Я. Рамсеевские задачи для пространств с симметриями, Изв. РАН, 64:6 (2000), 3-40.

[9] Банах Т., Протасов І. Про симетричність розфарбувань правильних многокутників, У світі математики, 1997, №3 9-15.

[10] Эрдёш П., Спенсер Д. Вероятностные методы в комбинаторике, М. "Мир 1975.

[11] Ядренко М. Й. Принцип Діріхле та його застосування. Київ, "Вища школа 1985

0.5. Про теорію Рамсея

Можливо ви чули про таку задачу: на вечірку випадково зібралася компанія з шести персон, доведіть, що принаймні три особи були знайомі між собою до цього, або принаймні три були попарно незнайомі. Ось свіжіший (Квант, М 1786) варіант цієї задачі. На площині відмічено шість точок, жодні три з яких не лежать на оній прямій і всі попарні відстані між нимим різні. Доведіть, що серед трикутників з вершинами в цих точках знайдуться два трикутники зі спільною стороною, для одного з яких ця сторона є найбільшою, а для другого — найменшою.

Це твердження узагальнюється так. Для будь-якого натурального числа k знайдеться натуральне число $n(k)$, таке що для довільного розфарбування множини ребер повного графу $K_{n(k)}$ двома кольорами знайдуться k вершин, всі ребра між якими однокольорові. Власне це і є окремий варант скінченної теореми Рамсея. Проте розпочнемо ми з нескінченної.

Теорема 0.5.1 (Рамсея (нескінченна версія)). *Для будь-яких натуральних чисел k, r і довільного розфарбування $\chi : \begin{bmatrix} \omega \\ k \end{bmatrix} \to [r]$ множини усіх k-елементних підмножин множини $\omega = \{0, 1, \dots\}$ r кольорами знайдеться нескінченна підмножина $S \subseteq \omega$, усі k-елементні підмножини якої мають один колір.*

Доведення. Для $k = 1$ твердження очевидне — це нескінченний варіант принципу Діріхле.

Розглянемо випадок $k = 2$. Ототожнимо $\begin{bmatrix} \omega \\ 2 \end{bmatrix}$ з множиною ребер повного графу K_ω з ω вершинами. Нехай $\chi : \begin{bmatrix} \omega \\ 2 \end{bmatrix} \to [r]$ — довільне розфарбування множини ребер K_ω. З вершини 0 виходить ω ребер, а тому деякий колір c_0 зафарбовує нескінченну підмножину цих ребер. Нехай $X = \{x_i : i \in \omega, \chi\{0, x_i\} = c_0\}$. Розглянемо ребра $\{x_0, x_i\}, x_i \in X$. Деякий колір, скажімо c_1 зафарбовує нескінченне число таких ребер.

Нехай $Y = \{y_i : i \in \omega, \chi\{x_0, y_i\} = c_1\}$. Розглянемо ребра $\{y_0, y_i\}, y_i \in Y$. Деякий колір c_2 зафарбовує нескінченне число таких ребер. Нехай $Z = \{z_i : i \in \omega, \chi\{y_0, z_i\} = c_2\}$. Очевидно, цей процес можна продовжити до нескінченності. Покладемо $T = \{0, x_0, y_0, z_0, \dots\}$. Зауважимо, що колір кожної пари $\{t_1, t_2\} \in \left[\begin{matrix} T \\ 2 \end{matrix}\right]$ залежить лише від значення $\min\{t_1, t_2\}$. Таким чином, кожному елементу $t \in T$ можна співставити колір $\chi^*(t) \in [r]$ за правилом $\chi^*(t) = \chi(t, t'), t' > t$. За принципом Діріхле деяка нескінченна підмножина $S \subseteq T$ має бути однокольровою відносно χ^*, $\chi^*(s) = c$ для всіх $s \in S$. За означенням χ^* усі ребра між вершинами з S мають колір c.

Розглянемо випадок $k = 3$. Кожне r-розфарбування $\chi : \left[\begin{matrix} \omega \\ 3 \end{matrix}\right] \to [r]$ породжує r-розфарбування χ_1 пар з $X = \omega \setminus \{0\}$ за правилом $\chi_1\{x_1, x_2\} = \chi\{0, x_1, x_2\}$. За теоремою Рамсея при $k = 2$ множина X містить нескінченну підмножину $X' = \{x'_i : i \in \omega\}$, таку що $\chi_1\{x'_i, x'_j\} = c_1$. Далі визначаємо r-розфарбування χ_2 на $\left[\begin{matrix} Y \\ 2 \end{matrix}\right]$, $Y = X' \setminus \{x'_0\}$ за правилом $\chi_2\{y, y'\} = \chi\{x'_0, y, y'\}$. За теоремою Рамсея для $k = 2$ множина Y містить нескінченну підмножину $Y' = \{y'_i : i \in \omega\}$, причому $\chi_2\{y'_i, y'_j\} = c_2$ для всіх $y'_i, y'_j \in Y'$. Продовжуючи цей процес, утворимо множину $T = \{0, x'_0, y'_0, \dots\}$. За побудовою ця множина має таку властивість: колір кожної трійки $\{t, t', t''\}$ з T залежитя лише від числа $\min\{t, t', t''\}$. За принципом Діріхле знайдеться нескінченна однокольрова підмножина $S \subseteq T$.

З цих трьох кроків ($k = 1, 2, 3$) зрозуміло як обгрунтувати індуктивний перехід у загальному випадку. $\square$

Скінченний варіант теореми Рамсея ми виведемо з нескінченного за допомогою теореми компактності для розбиттів (див., наприклад, [**6**])

Нехай X — довільна множина, m — натуральне число. Сім'ю $\mathcal{A}$ підмножин множини X називають *m-регулярною* відносно підмножини $Y \subseteq X$, якщо для довільного розбиття $Y = Y_1 \cup \dots \cup Y_m$ існують $A \in \mathcal{A}, k \in \{1, \dots, m\}$, такі що $A \subseteq Y_k$.

Теорема 0.5.2 (компактності розбиттів). *Якщо сім'я $\mathcal{A}$ скінченних підмножин множини X m-регулярна відносно X, то знайдеться скінченна підмножина $Y \subseteq X$, така що $\mathcal{A}$ m-регулярна відносно Y.*

Теорема 0.5.3 (Рамсея (скінченний варіант)). *Для довільних натуральних чисел $k, l, m,$ $k \leq l$ знайдеться натуральне число $n(k, l, m)$, таке що для довільного n і довільного розфарбування $\chi : \begin{bmatrix} n \\ k \end{bmatrix} \to [m]$ множини $\begin{bmatrix} n \\ k \end{bmatrix}$ k-підмножин множини $\{1, \dots, n\}$ m кольорами існує l-підмножина $\{1, \dots, n\}$, всі k-підмножини якої однокольрові.*

Доведення. Позначимо $X = \begin{bmatrix} \omega \\ k \end{bmatrix}$, $\mathcal{A} = \{\begin{bmatrix} B \\ k \end{bmatrix} : B \subset \omega, |B| = l\}$. Розглянемо довільне розбиття $X = A_1 \cup \dots \cup A_m$. За нескінченною версією теореми Рамсея існує нескінченна підмножина $A \subset \omega$, така що $\begin{bmatrix} A \\ k \end{bmatrix} \subseteq A_i$ для деякого $i \in \{1, \dots, m\}$. Це означає, що сім'я $\mathcal{A}$ m-регулярна відносно X. Оскільки всі елементи сім'ї $\mathcal{A}$ є скінченним множинами, за теоремою компактності для розбиттів існує скінченна підмножина $Y \subset \left[\begin{array}{c} \omega \\ k \end{array} \right]$, така що $\mathcal{A}$ m-регулярна відносно Y. Виберемо натуральне число $n(k,l,m)$, таке що $Y \subseteq \left[\begin{array}{c} n(k,l,m) \\ k \end{array} \right]$. Тоді $\mathcal{A}$ m-регулярна відносно $\left[\begin{array}{c} n \\ k \end{array} \right]$ для всіх $n \geq n(k,l,m)$. $\square$

При фікксованих k, l, m найменше з чисел $n(k,l,m)$, про які йдеться в теоремі Рамсея називають числом Рамсея і позначають $R(k,l,m)$, $R(2,l,2) = R(l)$. Обчислювати точні значення чисел Рамсея досить важко і зростають вони досить швидко, про що свідчить така теорема.

ТЕОРЕМА 0.5.4. *Існує константа $c > 0$, така що для всіх натуральних чисел l справджується нерівність*

$$R(l) > cl2^{\frac{l}{2}}.$$

ДОВЕДЕННЯ. Розглянемо повний граф K_n з множиною вершин $\{1, \ldots, n\}$. Назвемо розфарбування ребер K_n двома кольорами задовільним, якщо існує однокольорова копія графу K_l. Якщо X — підмножина вершин K_n і $|X| = l$, то маємо

$$2 \cdot 2^{\left(\begin{array}{c} n \\ 2 \end{array} \right) - \left(\begin{array}{c} l \\ 2 \end{array} \right)}$$

способів розфарбування, при яких всі ребра між вершинами з X однокольрові. Оскільки вибрати підмножину X можна $\left(\begin{array}{c} n \\ l \end{array} \right)$ способами, число задовільних розфабувань не перевищує

$$\left(\begin{array}{c} n \\ l \end{array} \right) 2^{\left(\begin{array}{c} n \\ 2 \end{array} \right) - \left(\begin{array}{c} l \\ 2 \end{array} \right) + 1}.$$

Отже, якщо

$$\begin{pmatrix} n \\ l \end{pmatrix} 2^{\begin{pmatrix} n \\ 2 \end{pmatrix} - \begin{pmatrix} l \\ 2 \end{pmatrix} + 1} < 2^{\begin{pmatrix} n \\ 2 \end{pmatrix}},$$

тобто $\begin{pmatrix} n \\ l \end{pmatrix} < 2^{\begin{pmatrix} l \\ 2 \end{pmatrix} - 1}$, то існує незадовільне розфарбування. Це означає, що $R(l)$ має перевищувати всі n, для яких справедлива остання нерівність. Оскільки ця нерівність вірна при $n < cl2^{\begin{pmatrix} l \\ 2 \end{pmatrix}}$ для деякої константи c, маємо твердження теореми. □

Ілюстративні застосування теореми Рамсея ми розпочнемо з доведення такого геометричного твердження.

ТВЕРДЖЕННЯ 0.5.1. *Для довільного натурального числа l існеує натуральне число $n = f(l)$, таке що у довільній множині із n точок на площині у загальному положенні можна вибрати l точок, що є вершинами опуклого l-кутника.*

ДОВЕДЕННЯ. Два спостереження. Перше, серед 5 точок площини у загальному положенні можна вибрати 4, що є вершинами опуклого 4-кутника. Друге, якщо будь-які 4 з k точок площини є вершинами опуклого 4-кутника, то всі k точок є вершинами опуклого k-кутника. Нехай $l \geq 5$, $n = R(4, l, 2)$ і на площині задано n точок у загальному положенні. Пофарбуємо кожну четвірку точок двома кольрами "опуклим" та "не опуклим" в залежності від того, чи є опукла оболонка цих точок чотирикутником. За означення числа Рамсея $R(4, l, 2)$ знайдуться l-точок, всі четвірики яких однокольрові. За першим спостереженням колір цих четвірок має бути опуклим, адже $l \geq 5$. З другого спостереження випливає, що всі l-точок є вершинами їх опуклої оболонки. □

Друге застосування стосується графів. *Турніром* називають повний скінченний граф, кожне ребро якого орієнтоване. Турнір називають *транзитивним,* якщо з існування ребер $a \to b$, $b \to c$ випливає, що ребро $a \to c$ теж є в турнірі.

ТВЕРДЖЕННЯ 0.5.2. *Для будь-якого натурального числа l існує натуральне число $n = f(l)$, таке що кожен турнір з n вершинами містить транзитивний турнір з l вершинами.*

ДОВЕДЕННЯ. Будь-якой турнір на чотирьх точках містить транзитивний турнір на трьох точках. Дійсно зафіксуємо одну із вершин. Можливі два випадки: з цієї вершини виходить принаймні два ребра або вона є кінцем принаймні двох ребер. Відповідні три вершини і дають транзитивний турнір. Нехай $l \geq 4$, $n = R(3, l, 2)$. Пофарбуємо трикутники турніру двома кольрами "транзитивним" і "не транзитивним". Виділимо підмножину l точок, усі трикутники в якій однокольорові. Оскільки $l \geq 4$, усі трикутники транзитивні. □

Далі кілька алгебраїчних застосувань.

ТЕОРЕМА 0.5.5 (про ідемпотент). *Кожна скінченна напівгрупа S містить ідемпотент $s, s^2 = s$.*

ДОВЕДЕННЯ. Нехай $|S| = m$. Зафіксуємо натуральне число n і розглянемо довільну послідовність $x_1, \ldots, x_n$ елементів напівгрупи S. Ребра повного графу K_n пофарбуємо m кольрами за правилом $\chi(i, j) = x_{i+1} \ldots x_j, i \neq j$. Якщо $n > R(2, 3, m)$, то граф K_n містить однокольровий трикутник з вершинами

$\{i,j,k\}, i<j<k$. Тоді $\chi(i,j)=\chi(j,k)=\chi(i,k)=s$. Це означає, що

$$\prod_{i<\alpha\leq j} x_\alpha = \prod_{j<\beta\leq k} x_\beta = \prod_{i<\gamma\leq k} x_\gamma = (\prod_{i<\alpha\leq j} x_\alpha)(\prod_{j<\beta\leq k} x_\beta) = s,$$

і $ss=s$. □

Теорема 0.5.6 (Шура). *Для довільного розфабування $\chi : \mathbb{N} \to [r]$ множини натуральних чисел r кольорами, $r \in \mathbb{N}$ рівняння $x+y=z$ має однокольоровний розв'язок.*

Доведення. Кожній парі натуральних чисел $(i,j), i<j$ припишемо колір $\chi(j-i)$. За теоремою Рамсея знайдеться нескінченна підмножина $S \subseteq \mathbb{N}$, така що всі пари $(i,j), i,j \in S$ однокольорові. Візьмемо з S довільні три елементи $i,j,k, i<j<k$. Тоді $\chi(i,j)=\chi(j,k)=\chi(i,k)$ а тому $(j-i)+(k-j)=k-i$ — однокольоровий розв'язок рівняння. □

Застосовуючи в цьому доведенні скінченний варіант теореми Рамсея, одержимо скінченний варіант теореми Шура.

Твердження 0.5.3. *Для будь-якого натурального числа r знайдеться натуральне число $n=n(r)$, таке що при довільному r-розфарбуванні множини $\{1,\dots,n\}$ в цій множині знайдеться однокольровий розв'язок рівняння $x+y=z$.*

З цього твердження Шур 1916 року вивів таку теорему.

Теорема 0.5.7. *Для кожного натурального числа m порівняння $x^m+y^m \equiv z^m(\bmod p)$ має нетривіальний розв'язок при досить великих простих числах p.*

Доведення. Нехай g — твірний елемент мультиплікативної групи $\mathbb{Z}_p^* = \{1,\dots,p-1\}$ поля $\mathbb{Z}_p$. Якщо $k \in \mathbb{Z}_p^*$, то $k=g^t(\bmod p)$, $0 \leq t < p-1$ і таке зображення однозначне. Запишемо $t=i+mj$, $0 \leq i < m$ і визначимо розфарбування

$\chi : \mathbb{Z}_p^* \to \{0, \ldots, m-1\}$ за правилом $\chi(k) = i$. За скінченним варіантом теореми Шура при досить великих p знайдуться $x, y, z, 0 < x, y, z < p$, такі що $x+y = z$ і $\chi(x) = \chi(y) = \chi(z) = i$. Отже

$$\left.\begin{array}{ll} x = g^{i+mj(x)} & (\bmod p) \\ y = g^{i+mj(y)} & (\bmod p) \\ z = g^{i+mj(z)} & (\bmod p) \end{array}\right\} \Rightarrow g^{i+mj(x)} + g^{i+mj(y)} \equiv g^{i+mj(z)} \pmod p.$$

Помножимо останнє співвідношення на g^{-i} і одержимо потрібний розв'язок. $\square$

Перше топологічне застосування ,яке ми розглянемо, досить просте. Нехай (X, d) — метричний простір. Підмножину $A \subseteq X$ називають *рівномірно дискретною,* якщо знайдеться $\varepsilon > 0$, таке що $B(a, \varepsilon) \cap A = \{a\}$ для всіх $a \in A$, де $B(a, \varepsilon) = \{x \in X : d(a, x) \leq \varepsilon\}$. Жодна нескінченна рівномірно дискретна множина не містить нестаціонарних послідовностей Коші. Обернене твердження не вірне, проте справедливе таке твердження.

ТВЕРДЖЕННЯ 0.5.4. *Якщо нескінченна підмножина $A \subseteq X$ не містить нестаціонарних послідовностей Коші, то знайдеться нескінченна рівномірно дискретна підмножина $B \subseteq A$.*

ДОВЕДЕННЯ. Для доведення зафіксуємо довільну послідовність (ε_n) додатних чисел, що збігається до нуля. Пофарбуємо пари елементів з A за правилом $\chi\{a, b\} = 0$, якщо $B(a, \frac{\varepsilon_0}{2}) \cap B(b, \frac{\varepsilon_0}{)}2 \neq 0$ і $\chi\{a, b\} = 1$ в іншому разі. За теоремою Рамсея існує нескінченна підмножина A_0 з однокольоровими парами. Якщо $\chi\{a, b\} = 0$ для $a, b \in A_0$, то підмножина A_0 рівномірно дискретна. Інакше, $\chi\{a, b\} = 1$, тобто $d(a, b) \leq \varepsilon_0$ для всіх $a, b \in A_0$. Пофарбуємо пари з A_0 за правилом $\chi\{a, b\} = 0$, якщо $B(a, \frac{\varepsilon_1}{2}) \cap B(b, \frac{\varepsilon_1}{2}) = \emptyset$ і $\chi\{a, b\} = 1$

в іншому разі. Виберемо нескінченну підмножину $A_1 \subseteq A_0$ з однокольровими парами. Продовжуючи, на деякому кроці ми знайдеми рівномірно дискретну підмножину A_n. Дійсно, припустивши супртивне, ми одержимо ланцюжок нескінченних підмножин $A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n \supseteq \ldots$ і $d(a, b) \leq \varepsilon_n$ для всіх $a, b \in A_n$. Візьмемо по одному елементу $a_n \in A_n$, $a_n \neq a_m$ при $n \neq m$ і одержимо нестаціонарну послідовність Коші. □

Друге з топологічних застосувань вимагає дещо більше означень. Топологічна група G називається *екстремально аменабельною* (про аменабельність див лекцію "Комбінаторні задачі теорії міри"), якщо вона має нерухому точку при дії на будь-якому компакті. Це означає: якщо X — компактний хаусдорфів простір і задане неперервне відображення $G \times X \to X$, $(g, x) \mapsto g(x)$, $e(x) = x$, e — одиниця групи G, $g(h(x)) = (gh)(x)$, $g, h \in G$, то існує точка x_0, нерухома відносно дії усіх елементів групи G, $g(x_0) = x_0, g \in G$. Значно простіше для перевірки таке еквівалентне означення: для будь-якої великої зліва підмножини S (тобто $G = FS$ для деякої скінченної підмножини F) підмножина SS^{-1} щільна в G. Будувати приклад екстремально аменабельних груп досить непросто, ми наведемо одну конструкцію, що належить Пестову [**5**].

Нехай $(X, <)$ — лінійно впорядкований простір. Бієкція $f : X \to X$ називається *порядковим автоморфізмом,* якщо з $x < y$ випливає $f(x) < f(y)$. Група G порядкових автоморфізмів $(X, <)$ називається *ω-транзитивною,* якщо для кожного натурального числа n і довільних двох упорядкованих (за $<$) n-ок $x_1, \ldots, x_n$ та $y_1, \ldots, y_n$ елементів з X існує елемент $g \in G$, такий що $g(x_1) = y_1, \ldots, g(x_n) = y_n$.

Твердження 0.5.5. *Кожна ω-транзитивна група G порядкових автоморфізмів нескінченної лінійно впорядкованої* *множини X, наділена топологією поточкової збіжності, екстремально аменабельна. Зокрема, група порядкових автоморфізмів множини раціональних чисел екстремально аменабельна.*

Доведення. Стабалізатор $\mathrm{St}_M = \{d \in G : g(x) = x, x \in M\}$ скінченної підмножини є відкритим околом одиниці групи G. Фактор-простір $G/\,\mathrm{St}_M$ лівих суміжних класів ми ототожнимо з множиною $X^{(n)}$ усіх впорядкованих n-підмножин з X, $n = |M|$. Нехай F — скінченна підмножина з G, $G = FS$. Задамо розфарбування $\chi : X^{(n)} \to F$ за таким правилом. Нехай $M = \{x_1, \dots, x_n\}$, $x_1 < \dots < x_n$. Візьмемо довільний елемент $\{y_1, \dots, y_n\}$ із $X^{(n)}$ і знайдемо елемент $g \in G$, такий що $g(x_1) = y_1, \dots, g(x_n) = y_n$. Оскільки $G = FS$, то $g = fs$ для деяких $f \in F, s \in S$. Покладемо $\chi\{y_1, \dots, y_n\} = f$. За нескінченною версією теореми Рамсея знайдуться нескінченна підмножина $A \subseteq X$ і $f \in F$, такі що $\chi|_{A^{(n)}} = \{f\}$. Позначимо $B = f^{-1}(A)$. Тоді $S\,\mathrm{St}_M$ містить усі автоморфізми що переводять M в B. Значить, $\mathrm{St}_M\,S^{-1}$ містить усі автоморфізми, такі що образ B містить M. Оскільки $B \setminus M$ нескінченна, кожен автоморфізм можна розкласти у добуток двох, одного із $\mathrm{St}_M\,S^{-1}$, а другого з $S\,\mathrm{St}_M$. Отже, $G = \mathrm{St}_M\,S^{-1}S\,\mathrm{St}_M$. Оскільки підмножина M була вибрана довільно $S^{-1}S$ щільна в G. □

Теорема Рамсея з'явилася 1930 року в статті [**7**] з математичної логіки як допоміжне технічне твердження. Докладний виклад цієї статті можна знайти в [**4**]. Значну роль в становленні теорії Рамсея відіграла стаття Ердьоша і Секереша [**3**]. Насьогодні теорія Рамсея це могутнє комбінаторне дерево, гілки якого простягаються в різні галузі математики. Ми вкажемо лише деякі з них.

Рамсеева теорія графів. Одна з основних задач цієї теорії формулюється так: для фіксованого скінченного графу G визначити найменше натуральне число $n = R(G)$, таке що при будь-якому 2-розфарбуванні ребер повного графу K_n знайдеться онокольорова копія графу G. Трохи загальніша задача: для скінченних графів $G_1, \ldots, G_k$ знайти найменше число $n = R(G_1, \ldots, G_k)$, таке що для довільного k-розфарбування ребер поного графу K_n в деякому кольорі $m \in \{1, \ldots, k\}$ знайдеться копія графу G_m. Типовий приклад — теорема Хватала: для довільних натуральних чисел m, n

$$R(T_m, G_n) = (m-1)(n-1) + 1,$$

де T_m — довільне дерево з m вершинами.

Евклідова теорія Рамсея. Нехай X — метричний простір, C — скічнченна підмножина X. Чи при будь-якому розфарбуванні X заданим скінченним числом кольорів знайдеться однокольорова підменожина C' ізометрична C? Одна з найвідоміших нерозв'язаних задач: яке найменше число кольорів достатньо для розфарбування площини так, щоб не було двох однокольорових точок на відстані 1? Відомо (і не складно довести), що трьох кольорів замало, а шести вистачає. Відкритою є і така гіпотеза: при будь-якому скінченному розфарбуванні площини знайдуться три однокольорові точки, що є вершинами трикутника площі 1.

Численння розбиттів. Цей напрямок розпочався з теореми Ердьоша-Радо, що є "кардинальним " варіантом теореми Рамсея.

Нехай τ — кардинал, $\tau \geq \aleph_0$, $\lambda = 2^\tau$, X — довільна множина потужності λ. При довільному розфабуванні сім'ї $\begin{bmatrix} X \\ 2 \end{bmatrix}$ двоелементних підмножин множини X τ кольорами знайдеться підмножина $Y \subseteq X$, така що $|Y| > \tau$ і всі елементи з $\left[\begin{matrix} Y \\ 2 \end{matrix} \right]$ однокольорові.

Розглядаються також несиметричні розфарбування. Нехай A, B — множини потужності α та β. Якщо для будь-якого розфарбування декартового добутку $A \times B$ двома кольорами знайдуться підмножини $A_1 \subseteq A, B_1 \subseteq B$, такі що $|A_1| = \alpha, |B_1| = \beta_1$ і підмножина $A_1 \times B_1$ однокольорова, то за означенням справедливе твердження $\alpha \times \beta \to \alpha_1 \times \beta_1$. За теоремою Гелвіна $\aleph_1 \times \aleph_0 \to \aleph_0 \times \aleph_0$, проте твердження $\aleph_1 \times \aleph_0 \to \aleph_1 \times \aleph_0$ залежить від аксіоматики теорії множин.

Топологічна теорія Рамсея. Досить природною видається така загальна задача: для пари топологічних просторів X, Y, з'ясувати чи для кожного розфарбування X заданим числом кольорів знайдеться в X гомеоморфна однокольорова копія Y? Такі дослідження проводяться, але переважна більшість одержаних результатів зав'язана на аксіоматику. Значно продуктивнішою виявилась топологічна характеризаця рамсеївої властивості [**1**], запропонована Елентуком 1974 року, яка, власне, і вважається початком топологічної теорії Рамсея.

Нехай W — сім'я всіх нескінченних підмножин натуральних чисел. Для довільних $A \in W$, $n \in \mathbb{N}$ позначимо через $E(n, A)$ сім'ю усіх нескінченних підмножин з $\mathbb{N}$, що містяться в A і перші n елементів яких співпадають з першими n елементами підмножини A. Сім'я $\{E(n, A) : n \in \mathbb{N}, A \in W\}$ є базою деякої топології, що називається топологією Елентука, а простір W з цією топологією позначається $\mathcal{E}$. За означенням, підмножина $X \subseteq \mathcal{E}$ є рамсеєвою, якщо для довільної підмножини $E(n, A)$ знайдеться $B \in E(n, A)$, таке що $E(n, A) \subseteq X$ або $E(n, A) \cap X = \emptyset$. Підмножину X називають 0-рамсеєвою, якщо для довільної підмножини $E(n, A)$ знайдеться $B \in E(n, A)$, така що $E(n, B) \cap X = \emptyset$.

Теорема 0.5.8 (Елентука). *Підмножина $X \subseteq \mathcal{E}$ є рамсеєвою тоді і тільки тоді, коли X має властивість Бера. Підмножина $X \subseteq \mathcal{E}$ є 0-рамсеєвою тоді і тільки тоді, коли X першої категорії.*

Множину W можна розглядати також як підпростір простору $\{0, 1\}^{\mathbb{N}}$ є топологією добутку (ототожнюючи кожну нескінченну підмножину з її характеристичною функцією). З теореми Елентука випливає такий наслідок — теорема Гелвіна-Прікрі [**3**]. Якщо W розбити на скінченне число борелевих підмножин, то знайдеться підмножина $A \in W$, така що всі підмножини з A належать одному блоку розбиття.

Бібліоґрафія

[1] Ellentuck E. A new proof that analytic sets are Ramsey, J. Symbol. Logic, 39 (1974), 163-165.

[2] Erdős P., Szekers G. A combinatorial problem in geomatry, Composito Math., 2 (1935), 464-470.

[3] Galvin F., Prikry K. Borel sets and Ramsey's theorey, J. Symbol. Logic, 38 (1973), 193-198.

[4] Graham R., Rostschild B., Spencer J. Ramsey Theory, Willey, New York, 1980.

[5] Pestov V. Some universal constructions in abstract topological dynamics, Contemporary Math., 215 (1998), 83-99.

[6] Protasov I. Combinatorics of Numbers, Mat. Stud. Monogr. Ser, Vol. 2, 1997.

[7] Ramsey F. On a problem of formal logic, Proc. London Math. Soc., 30 (1930), 264-285.

[8] Грэхэм Р. Начала теории Рамсея, М., "Мир 1984.

0.6. Навколо теореми ван дер Вардена

Для будь-якого розфарбування множини натуральних чисел скінченним числом кольорів і будь-якого натурального числа n знайдеться однокольорова арифметична прогресія довжини n. Ця теорема, доведена 1927 року, стала наріжним каменем сучасної теорії розбиттів — теорії Рамсея. Ми розпочнемо з теореми Халеса-Джавета, узагальнення теореми ван дер Вардена, що виникло з n-вимірного варіанту хрестиків-нуликів [4].

ТЕОРЕМА 0.6.1 (Халеса-Джавета). *Нехай* S *— вільна напівгрупа в алфавіті* $\{a_1, \ldots, a_m\}$. *Для довільного розбиття* $S = S_1 \cup \cdots \cup S_n$ *знайдуться напівгрупове слово* $f(x)$ *в алфавіті* $\{a_1, \ldots, a_m, x\}$, *що містить принаймні одну літеру* x, *і підмножина* S_i *розбиття, такі що* $\{f(a_1), \ldots, f(a_m)\} \subseteq S_i$.

Для доведення скористаймося поняттям регулярності: сім'ю $\mathcal{X}$ підмножин множини X називають *n-регулярною* (n — натуральне число), якщо для довільного розбиття X на $\leq n$ частин принаймні одна з підмножин розбиття містить деякий елемент сім'ї $\mathcal{X}$.

ЛЕМА 0.6.2. *Нехай* n, m *— натуральні числа,* X, Y *— множини,* $|X| = m$. *Якщо сім'я* $\mathcal{X}$ *n-регулярна в* X, *а сім'я* $\mathcal{Y}$ *n^m-регулярна в* Y, *то сім'я* $\mathcal{X} \times \mathcal{Y} = \{A \times B : A \in \mathcal{X}, B \in \mathcal{Y}\}$ *n-регулярна в* $X \times Y$.

ДОВЕДЕННЯ. Кожне розбиття $X \times Y$ на $\leq n$ частин визначається деякої функцією $f : X \times Y \to \{1, \ldots, n\}$. Позначимо $f_y(x) = f(x, y)$ і зауважимо, що число таких функцій n^m. Відповідність $y \mapsto f_y$ визначає розбиття множини Y на n^m частин. А тому знайдеться підмножина $B \in \mathcal{Y}$, така що $f_y = f_{y'}$ для всіх $y, y' \in B$. Це означає, що $f(x, y) = f(x, y')$ для всіх $x \in X$. Виберемо таку підмножину $A \in \mathcal{X}$, що $f(x, y) = const$ для всіх $x \in A$. Тоді звуження f на $A \times B$ є константою, тобто $A \times B$ належить одній підмножині розбиття, визначеного функцією f. ☐

Для доведення наступної леми ми скористаємося теоремою компактності для розбиттів: якщо сім'я скінченних підмножин $\mathcal{X}$ m-регулярна (m — натуральне число) в X, то знайдеться скінченна підмножина $Y \subseteq X$, така що сім'я $\mathcal{Y} = \{A \in \mathcal{X} : A \subseteq Y\}$ m-регулярна в Y. Доведення цієї теореми можна знайти в [**5**, p. 17].

Лема 0.6.3. *Якщо сім'я $\mathcal{X}$ скінченних підмножин напівгрупи S n-регулярна в S для будь-якого натурального числа n, що сім'я $\mathcal{X}_k = \{X_1 \dots X_k : X_i \in \mathcal{X}\}$ n-регулярна в S для всіх k, n.*

Доведення. Застосуємо індукцію по числу k. Перший крок закладено в умову леми. Припустімо, що $\mathcal{X}_{k-1}$ n-регулярна для всіх n. Зафіксуємо n і користуючись теоремою компактності для розбиттів, виберемо скінченну підмножину $Y \subseteq S$, таку що $\mathcal{X}_{k-1}$ n-регулярна в Y. Нехай $|Y| = m$. За лемою 0.6.2 сім'я $\mathcal{X}_{k-1} \times \mathcal{X}$ n-регулярна в $Y \times S$, а тому $\mathcal{X}_{k-1} \times \mathcal{X}_k$ n-регулярна в $S \times S$. Отже, $\mathcal{X}_k$ n-регулярна в S. □

Нехай S — вільна напівгрупа в зліченному алфавіті Ω. Для кожної скінченної підмножини $A \subset \Omega$ позначимо через $\mathcal{X}(A)$ множину усіх підмножин $f(A)$, де $f(x)$ — слово в алфавіті $A \cap \{x\}$, що містить принаймні одне входження елемнту x. Через $I(n, k)$ позначимо таке твердження: для будь-якої підмножини $A \subset \Omega$, $|A| = n$ сім'я підмножин $\mathcal{X}(A)$ k-регулярна в напівгрупі, що породжена підмножиною A.

Лема 0.6.4. *Твердження $I(n, k)$ справедливе для всіх натуральних чисел n, k.*

Доведення. Твердження $I(n, 1), I(1, k)$ очевидні. Ми припустимо, що твердження $I(n, k), I(n-1, j)$ доведено для всіх j і доведемо твердження $I(n, k+1)$.

Нехай $A \subseteq \Omega$, $|A| = n$, $a \in A$, $B = A \setminus \{a\}$. Твердження $I(n, k)$ разом з теоремою компактності забезпечує k-регулярність $\mathcal{X}(A)$ в A^r для деякого натурального числа r.

Твердження $I(n-1, j)$ дає j-регулярність $\mathcal{X}(B)$ в напівгрупі породженій B. За лемою 0.6.3 добуток $\mathcal{X}(B) \dots \mathcal{X}(B)$ $(r+1)$-ої копії $\mathcal{X}(B)$ j-регулярний в деякій підмножині B^q.

Покажемо, що $\mathcal{X}(A)$ $(k+1)$-регулярна в A^q. Нехай $A^q = P_0 \cup \dots \cup P_k$. Оскільки $B^q \subset A^q$, то $B^q \subset P_0 \cup \dots \cup P_k$. Виберемо слова $g_0(x), \dots, g_r(x)$ в алфавіті $B \cup \{x\}$, такі що $g_0(B) \dots g_r(B)$ міститься в одній з підмножин розбиття, скажімо, в P_0. Ясно, що $g_0(B) \dots g_r(B) \subseteq B^q$.

Очевидно, що $g_0(A) \dots g_r(A) \subseteq A^q$. Визначимо відображення $\varphi : A^r \to g_0(a)g_1(A) \dots g_r(A)$ за таким правилом $\varphi(x_1, \dots, x_r) = g_0(a)g_1(x_1) \dots g_r(x_r)$. З $I(n,k)$ випливає що $\mathcal{X}(A)$ k-регулярне відносно множини $g_0(A)g_1(A) \dots g_r(A)$. Якщо $g_0(A)g_1(A) \dots g_r(A) \cap P = \emptyset$, то все ясно. Якщо $g_0(A)g_1(A) \dots g_r(A) \cap P_0 \neq \emptyset$, виберемо $a_1, \dots, a_r \in A$, такі що $g_0(a)g_1(a_1) \dots g_r(a_r) \in P_0$. Нехай $t = g_0(a)g_1(a) \dots g_r(a) = v_1 \dots v_q \in A^q$. Визначимо елементи $\alpha_1, \dots, \alpha_q$ за таким правилом: $\alpha_i = v_i$, якщо $v_i \in B$ і $\alpha_i = x$, якщо $\alpha_i = a$. Покладемо $f(x) = \alpha_1 \dots \alpha_q$. Оскільки $f(B) \subseteq P_0$ і $f(a) \in P_0$, то $f(A) \subseteq P_0$. □

Доведення теореми Халеса-Джавета випливає безпосередньо з леми 0.6.4.

Ми виведемо з теореми Халеса-Джавета дещо посилену версію теореми ван дер Вардена.

ТЕОРЕМА 0.6.5. *Нехай m — натуральне число, $(y_k)_{k\in\omega}$ — послідовність натуральних чисел. Для довільного розбиття $\mathbb{N} = B_1 \cup \dots \cup B_n$ принаймні одна з підмножин розбиття містить арифметичну прогресію $b, b+d, \dots, b+md$, де $d \in FS(y_k)_{k\in\omega}$, $FS(y_k)_{k\in\omega}$ — множина усіх скінченних сум різних елементів послідовності $(y_k)_{k\in\omega}$.*

ДОВЕДЕННЯ. Розглянемо вільну напівгрупу S в алфавіті $\Omega = \{0, 1, \dots, m\}$ і визначимо відображення $\varphi : S \to \mathbb{N}$ за таким правилом: для кожного елементу $s = s_1 \dots s_t$, $s_i \in \Omega$

покладемо

$$\varphi(s) = 1 + \sum_{i=1}^{t} s_i y_i.$$

Нехай $S_i = \varphi^{-1}(B_i)$. За теоремою Халеса-Джавета існують слово $f(x)$ в алфавіті $\Omega \cup \{x\}$, що містить літеру x, і індекс $j \in \{1, \dots, m\}$, такі що $f(a) \in S_j$ для всіх $a \in \Omega$. Нехай $f(x) = a_1 \dots a_t$, де $a_i \in \Omega \cup \{x\}$ і $a_i = x$ принаймні для одного $i \in \{1, \dots, t\}$. Розіб'ємо множину $\{1, \dots, t\}$ на дві підмножини $F = \{i : a_i = x\}, G = \{1, \dots, t\} \setminus F$. Нехай $d = \sum_{i \in F} a_i$, $b = 1 + \sum_{i \in G} a_i y_i$. Тоді $b + ad = \varphi(f(a))$ для всіх $a \in \Omega$. Отже

$$\{b, b + d, \dots, b + md\} \subseteq B_j, \quad d \in FS(a_k)_{k \in \omega}.$$

□

Одним з перших узагальнень теореми ван дер Вардена був її k-вимірний варіант — теорема Галаї.

Теорема 0.6.6. *Нехай k, m — натуральні числа. Для будь-якого розбиття $\mathbb{N}^k = B_1 \cup \dots \cup B_n$ існують підмножина розбиття B_j і підмножини*

$$A_1 = \{b_1, b_1 + d, \dots, b_1 + md\}, \dots, A_k = \{b_k, b_k + d, \dots, b_k + md\},$$

такі що $A_1 \times \dots \times A_k \subseteq B_j, d \neq 0$.

Доведення. Для спрощення доведення ми розглянемо лише випадок $k = 2$. Нехай S — вільна напівгрупа в алфавіті $\Omega = \{(i, j) : i, j \in \{0, \dots, m\}\}$. Визначимо відображення $\varphi : S \to \mathbb{N}^2$ за таким правилом: кожному елементу $s = s_1 \dots s_t, s_i \in \Omega$ співставимо

$$\varphi(s) = (1, 1) + \sum_{i=1}^{t} s_i.$$

Нехай $S_i = \varphi^{-1}(B_i)$. За теоремою Халеса-Джавета існують слово $f(x)$ в алфавіті $\Omega \cup \{x\}$ і підмножина S_j, такі що $f(a) \in S_j$ для всіх $a \in \Omega$. Нехай $f(x) = a_1 \dots a_t$. Розіб'ємо $\{1, \dots, t\}$ на дві підмножини $F = \{i : a_i = x\}, G = \{1, \dots, t\} \setminus F$. Позначимо $d = |F|$ і

$$(b_1, b_2) = (1, 1) + \sum_{i \in G} a_i.$$

Оскільки $\varphi(f(a)) \in B_j$ для всіх $a \in \Omega$, $A_1 \times A_2 \subseteq B_j$, де $A_1 = \{b_1, b_1 + d, \dots, b_1 + md\}, A_2 = \{b_2, b_2 + d, \dots, b_2 + md\}$. $\square$

Вже найпростіший варіант теореми Галаї $k = 2, m = 1$ має нетривіальні застосування. Ось одне з них.

В точках цілочисельної решітки на площині записані цілі числа, n — натуральне число. Тоді знайдеться квадрат зі сторонами паралельними координитним осям, сума чисел всередині якого ділиться на n.

Ми будемо шукати розв'язок в додатньому квадранті. Кожній вершиніз координатами x, y співставимо колір $s(x, y)$ — залишок по модулю n від суми чисел, записаних у клітинах з координатами $(a, b), 0 \leq a \leq x, 0 \leq b \leq y$. За теоремою Галаї знайдеться квадрат з цілочисельним однокольоровими вершинами $(x, y), (x+k, y), (x, y+k), (x+k, y+k)$. Залишилось помітити, що

$$s(x, y) - s(x + k, y) - s(x, y + k) + s(x + k, y + k)$$

ділиться на n.

Наступний наслідок теореми Халеса-Джавета це теорема Грема-Ліба-Росчайльда [**3**] про розбиття векторних просторів.

ТЕОРЕМА 0.6.7. *Якщо нескінченно вимірний лінійний простір V над скінченним полем F розбито на скінченне число підмножин, то щонайменше одна з підмножин розбиття* *містить афінні підпростори довільної скінченної розмірності.*

Доведення. Ми розглянемо випадок $F = \mathbb{Z}_3 = \{0, 1, 2\}$ і знайдемо двовимірний афінний підпростір в одній з підмножин розбиття $V = V_1 \cup \cdots \cup V_k$. Цей випадок насправді демонструє всі істотні фрагменти загального доведення. Нехай B — базис простору V і $(\overrightarrow{y}_n)_{n\in\omega}, (\overrightarrow{z}_n)_{n\in\omega}$ — диз'юнктні послідовності різних елментів B. Позначимо

$$\Omega = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}.$$

Позначимо $\mathrm{pr}_i(a)$ i-у координату $a \in \Omega$, $i \in \{1, 2\}$. Для вільної напівгрупи S в алфавіті Ω визначимо відображення $\varphi : S \to V$ за таким правилом: для елементу $s \in S, s = s_1 \dots s_t, s_i \in \Omega$ покладемо

$$\varphi(s) = \sum_{i=1}^{t} (\mathrm{pr}_1(s_i)\overrightarrow{y}_i + \mathrm{pr}_2(s_i)\overrightarrow{z}_i).$$

Нехай $S = \varphi^{-1}(V_i)$. За теоремою Халеса-Джавета існують слово $f(x)$ в алфавіті $\Omega \cup \{x\}$ і підмножина S_j, такі що $f(a) \in S_j$ для всіх $a \in \Omega$. Розіб'ємо множину $\{1, \dots, t\}$ на дві підмножини $H = \{i : a_i = x\}, G = \{1, \dots, t\} \setminus H$. Нехай

$$\overrightarrow{u} = \sum_{i\in H} \overrightarrow{y}_i, \overrightarrow{v} = \sum_{i\in H} \overrightarrow{z}_i.$$

Оскільки $H \neq \emptyset$, за вибором послідовностей $(\overrightarrow{y}_n)_{n\in\omega}, (\overrightarrow{z}_n)_{n\in\omega}$, лінійна оболонка W векторів $\overrightarrow{u}$ та $\overrightarrow{v}$ двовимірна. Позначмо

$$\overrightarrow{b} = \{\mathrm{pr}_1(a_i)\overrightarrow{y}_i + \mathrm{pr}_2(a_i)\overrightarrow{z}_i : i \in G\}.$$

Тоді $\overrightarrow{b} + W = \{\varphi(f(a)) : a \in \Omega\} \subseteq V_j.\}$ □

Ми завершимо застосування теореми Халеса-Джавета теоремою про комбінаторну пряму заради якої власне і було доведено цю теорему.

Для натуральних чисел k, n розглянемо множину

$$V(k,n) = \{1, \dots, k\}^n.$$

Нехай $I \subseteq \{1, \dots, n\}, I \neq \emptyset$ і для кожного $i \in \{1, \dots, n\} \setminus I$ вибрано деякий елемент $a_i \in \{1, \dots, k\}$. *Комбінаторна пряма* — це множина векторів $(x_1, \dots, x_n) \in V(k,n)$, що задовольняє умови

(*) $x_i = x_j$ для всіх $i, j \in I$;

(**) $x_i = a$ для всіх $i \in \{1, \dots, n\} \setminus I$.

Зауважимо, оскільки $I \neq \emptyset$, кожна комбінаторна пряма складається рівно з n елементів.

ТЕОРЕМА 0.6.8. *Для довільних натуральних чисел k, n існує натуральне число $n(k,m)$, таке що при $n \geq n(k,m)$ для довільного розфабування $V(k,n)$ в m кольорів знайдеться одно-кольорва комбінаторна пряма.*

ДОВЕДЕННЯ. Нехай S — вільна напівгрупа в в алфавіті $\Omega = \{1, \dots, k\}$. Для слова $f(x)$ в алфавіті $\Omega \cup \{x\}$, що містить літеру a, позначмо $A_f = \{f(a) : a \in \Omega\}$. Нехай $\mathcal{F}$ сім'я усіх підмножин A_f. За теоремою Халеса-Джавета сім'я $\mathcal{F}$ m-регулярна в S. За теоремою компактності для розбиттів $\mathcal{F}$ m-регулярна в деякій скінченній підмножині $Y \subset S$. Нехай $n(k,m)$ — максимальна довжина слів з Y. Якщо $n \geq n(k,m)$, підмножина S_n слів з S довжини $\leq n$ містить Y, а тому сім'я $\mathcal{F}$ m-регулярна в S_n. Задамо відображення $\varphi : S_n \to V(k,n)$ за таким правилом: для елементу $s = s_1 \dots s_p$ з S_n довжини $p \leq n$ покладемо $\varphi(s) = s_1 \dots s_p s_{p+1} \dots s_n$, де $s_{p+1} = \dots = s_n = 1$. Нехай $V(k,n) = V_1 \cup \dots \cup V_m$ — довільне розбиття. Оскільки $S_n = \varphi^{-1}(V_1) \cup \dots \cup \varphi^{-1}(V_m)$ і $\mathcal{F}$ m-регулярна в S_n, то існують

V_j і слово $f(x)$ в алфавіті $\Omega \cup \{x\}$, такі що $A_f \subseteq \varphi^{-1}(V_j)$. Тоді $\varphi(A_f)$ — комбінаторна пряма в $V(k,n)$ і $\varphi(A_f) \subseteq V_j$. $\square$

Халес та Джавет [**4**] розглядали таке узагальнення гри в хрестики нулики. Полем гри $G(k,n)$ є множина $V(k,n)$. Двоє гравців по черзі заповнюють порожні місця поля гри відповідно символами × та 0. Переможцем є той гравець, хто першим складе комбінаторну пряму зі своїх символів. Якщо всі клітинки заповнено, а однокольорових комбінаторних прямих немає, вважається що гра закінчилась внічию. З теорії позиційних ігор відомо, що або перший гравець має виграшну стратегію, або другий гравець завжди може закінчити гру внічию. З теореми про комбінаторну пряму (при $n = 2$) випливає, що для кожного натурального k існує натуральне число n, таке що перший гравець має виграшну стратегію в грі $G(k,n)$.

Одним з перших результатів в комбінаториці чисел була теорема Шура [**7**] доведена 1916 року: для довільного розфарбування множини натуральних чисел скінченним числом кольорів рівняння $x + y = z$ має однокольоровий розв'язок. З цього твердження Шур вивів, що для кожного натурального числа m порівняння $x^m + y^m \equiv z^m (\bmod p)$ має нетривіальний розв'язок для всіх досить великих простих чисел p. В циклі статей, розпочатому 1933 року, Радо [**6**] узагальнив теорему Шура на лінійні діофантові рівняння з n невідомими, спираючись на теорему ван дер Вардена.

Лінійне рівняння $c_1x_1 + \dots + c_nx_n = 0$ з ненульовими цілими коефіцієнтами Радо назвав *регулярним,* якщо для довільного скінченного розфарбування множини натуральних чисел це рівняння має однокольоровий розв'язок.

Теорема 0.6.9. *Лінійне діофантове рівняння* $c_1x_1 + \cdots + c_nx_n = 0$ *з ненульовими цілими коефіцієнтами регулярне тоді і тільки тоді, коли деяка непорожня сума його коефіцієнтів дорівнює нулю.*

Для доведення теореми Радо ми скористаємось дещо посиленим скінченним варіантом теореми ван дер Вардена. За цим скінченним варіантом для довільних натуральних чисел k, m існує натуральне число $W(k, m)$, таке що для всіх $n \geq W(k, m)$ і довільного розбиття $\{1, \ldots, n\} = A_1 \cup \cdots \cup A_m$ принаймні одна з підмножин розбиття містить арифметичну пргресію довжини k. Скінченний варіант випливає з доведеного вище нескінченного варіанту теореми ван дер Вардена застосуванням теореми компактності для розбиттів. Посилений скінченний варіант формулюється так.

Теорема 0.6.10. *Для довільних натуральних чисел* k, m, s *існує натуральне число* $W(k, m, s)$, *таке що для довільного* $n \geq M(k, m, s)$ *і довільного розфарбування множини* $\{1, \ldots, n\}$ m *кольорами існують натуральні числа* k, d, *для яких числа* $a + d, a + 2d, \ldots, a + kd, sd$ *однокольорові.*

Доведення. Для доведення ми застосуємо індукцію по m. Для $m = 1$ можна взяти $M(k, 1, s) = \max\{k + 1, s\}$, $d = a = 1$. Припустімо, що для $m \geq 2$ число $M(k, m - 1, s)$ існує для всіх k, s. Для довільних натуральних чисел x, y позначимо через $W(x, y)$ число визначене скінченною версією теореми ван дер Вардена. Ми переконаємось, що за $M(k, m, s)$ можна взяти число $M = sW(kM(k, m-1, s), m)$. Розглянемо довільне розфарбування

$$\chi : \{1, \ldots, M\} \to \{1, \ldots, m\}.$$

За означенням $W(x, y)$ існують натуральні числа a, d' такі що

$$\{a+id' : 1 \leq i \leq kM(k, m-1, s)\} \subseteq \{1, \ldots, W(kM(k, m-1, s), m)\}$$

і всі члени $a + id'$ прогресії одного кольору, скажімо жовтого.

Якщо число $sd'j$ жовте для деякого $j \leq M(k, m-1, s)$, покладемо $d = jd'$. Тоді числа $a + d, \ldots, a + kd, sd$ жовті.

Якщо число sd'_j не є жовтим для всіх $j \leq M(k, m-1, s)$, то елементи прогресії $\{sd'_j : j \in \{1, \ldots, M(k, m-1, s)\}$ пофарбовано $m-1$ кольором. Перефарбуємо числа $j \in \{1, \ldots, M(k, m-1, s)\}$ новим кольором за правилом $\chi^*(j) = \chi(sd'j)$. За означенням$M(k, m-1, s)$ існують числа $A+D, \ldots, A+kD, sD$ і з множини $\{1, \ldots, M(k, m-1, s)\}$, однокольорові щодо χ^*. Отже, в розфарбуванні χ числа $sd'A + sd'D, \ldots, sD'A + ksDd', s\ (sd'D)$ однокольорові. □

Ми скористаємося при доведенні тереми Радо таким наслідком з попередього твердження.

Теорема 0.6.11. *Для довільних натуральних чисел k, s, m і довільного розфарбування множини натуральних чисел m кольорами знайдуться натуральні числа a, d, такі що число $\{a + \lambda d : \lambda \in \{0, \pm 1, \ldots, \pm k\}\}$ та sd однокольорові.*

Дійсно, виберемо однокольорові числа $b + d, \ldots, b + (2k + 1)d, sd$ і покладемо $a = b + (k+1)d$.

Доведення теореми Радо. Спочатку припустимо, що сума деяких коефіцієнтів рівняння дорівнює нулю. Перепозначимо їх так, що $c_1 + \cdots + c_k = 0$. Нехай χ — довільне скінченне розфарбування $\mathbb{N}$. Якщо $k = n$, покладемо $x_1 = \cdots = x_n = 1$ і одержимо однокольоровий розв'язок. Отже далі $k < n$. Позначмо $B = c_{k+1} + \cdots + c_n$. Якщо $B = 0$, то знову $x_1 = \cdots = x_n = 1$ — однокольоровий розв'язок. Отже, далі $B \neq 0$. Позначмо

$$A = \text{НСД}(c_1, \ldots, c_k), \quad s = \frac{A}{\text{НСД}(A, B)}.$$

Нехай t — ціле число, таке що $At + Bs = 0$. Підберемо цілі числа $\lambda_1, \dots, \lambda_k$, такі що $c_1\lambda_1 + \dots + c_k\lambda_k = At$. Ми стверджуємо, що для довільних натуральних чисел a, d рівняння $c_1x_1 + \dots + c_nx_n = 0$ має параметричний розв'язок

$$x_i = \begin{cases} a + \lambda_i d, & i \in \{1, \dots, k\}; \\ sd, & i \in \{k+1, \dots, n\} \end{cases}$$

Дійсно

$$\sum_{i=1}^{n} c_i x_i = \sum_{i=1}^{k} c_i x_i + \sum_{i=k+1}^{n} c_i x_i = \sum_{i=1}^{k} c_i(a + \lambda_i d) + \sum_{i=k+1}^{n} c_i sd =$$

$$a\sum_{i=1}^{k} c_i + d\sum_{i=1}^{k} c_i\lambda_i + sd\sum_{i=k+1}^{n} c_i = a \cdot 0 + dAt + dsB = 0.$$

Нехай $k_0 > \max\{|\lambda_i| : i \in \{1, \dots, k\}\}$. За теоремою 0.6.11 знайдуться натуральні числа a, d, такі що числа $\{a + \lambda d : \lambda \in \{0, \pm 1, \dots, \pm k_0\}$ і sd однокольорові. Але за означенням числа k_0 ця множина містить деякий розв'язок рівняння.

Припустімо, що рівняння регулярне, але кожна непорожня сума його коефіцієнтів відмінна від нуля. Візмемо просте число p і визначимо розфарбування χ_p множини $\mathbb{N}$: натуральне число x подамо у вигляді $x = p^{\alpha}(pt + k), 1 \le k \le p - 1$ і покладемо $\chi_p(x) = k$. За припущенням рівняння має однокольоровий розв'язок, скажімо кольору k. Нехай $x_i = p^{\alpha_i}(pt_i + k), i \in \{1, \dots, n\}$ — такий розв'язок скажімо кольору k. Змінюючи нумерацію невідомих можна вважати, що $\alpha_1 = \dots = \alpha_m < \alpha_{m+1} \le \dots \le \alpha_n$. Тоді

$$\sum_{i=1}^{n} c_i p_i^{\alpha_i}(pt_i + k) = 0.$$

Скоротимо на p^{α_1} і перейдемо до лишків за модулем p :

$$\sum_{i=1}^{m} c_i(pt_i + k) \equiv 0(\bmod p), \quad k\sum_{i=1}^{m} c_1 \equiv 0(\bmod p).$$

Оскільки $1 \leq k \leq p-1$ і p просте, $\sum\limits_{i=1}^{m} c_i \equiv 0(\bmod p)$. Якщо тепер число p вибрати досить великим, то необхідно $\sum\limits_{i=1}^{m} c_i = 0$, що суперечить припущенню. ☐

Одним з найістотніших посилень теореми ван дер Вардена є теорема Семереді [**8**]: кожна підмножина натуральних чисел довільної верхньої щільності містить як завгодно довгі арифметичні прогресії. Верхня щільність підмножини $A \subseteq \mathbb{N}$ це

$$\overline{d}(A) = \limsup \frac{|A \cap \{1, \ldots, n\}|}{n}.$$

При довільному скінченному розбитті натуральних чисел принаймні одна з підмножин розбиття має додатню верхню щільність. Ергодична схема доведення теореми вказана в лекції “Принцип Діріхле і теорема Пуанкаре”.

Фюрстенберг [**2**] довів таку поліноміальну версію теореми ван дер Вардена. Нехай $p_1, \ldots, p_m$ — поліноми з цілими коефіцієнтами і без вільних членів $(p_1(0) = \cdots = p_m(0) = 0)$. Для довільного скінченного розфарбування натуральних чисел знайдуться такі натуральні числа a і d, що всі числа $a + p_i(d), i \in \{1, \ldots, m\}$ однокольорові. Теорему ван дер Вардена ми отримаємо, якщо $p_i(x) = ix, i \in \{1, \ldots, m\}$. Бергельсон і Лейбман [**1**] посилили це твердження: для кожної підмножини A додатньої щільності знайдуться a і d, такі що $a + p_i(d) \in A, i \in \{1, \ldots, m\}$. Комбінаторне доведення останнього результату можна знайти в [**10**].

Наприкінці підбірка задач з [**11**], пов'язаних з теоремою ван дер Вардена.

Задача 0.6.1. Множину натуральних чисел пофарбовано двома кольорами. Доведіть, що деяке число є початковим членом нескінченного числа однокольорових тричленних арифметичних прогресій.

Задача 0.6.2. Вкажіть таке розфарбування множини натуральних чисел трьома кольорами, що жодне натуральне число не є початковим членом нескінченного числа однокольорових тричленних прогресій.

Задача 0.6.3. Вкажіть таке розфарбування множини натуральних чисел двома кольорами, що жодне натуральне число не є початковим членом нескінченного числа однокольорових чотиричленних арифметичних прогресій.

Задача 0.6.4. Вкажіть таке розфарбування множини натуральних чисел двома кольорами, що для кожного натурального числа d знайдеться натуральне число $n(d)$, таке що кожна однокольорова арифметична прогресія з різницею d має довжину $\leq n(d)$.

Задача 0.6.5. Множину натуральних чисел пофарбовано двома кольорами. Доведіть, що знайдеться зростаюча послідовність парних чисел $a_1, a_2, \ldots$, така що послідовність

$$a_1, \frac{a_1 + a_2}{2}, a_2, \frac{a_2 + a_3}{2}, a_3, \ldots, a_n, \frac{a_n + a_{n+1}}{2}, a_{n+1}$$

однокольорова.

Задача 0.6.6. Вкажіть розфарбування множини натуральних чисел трьома кольорами, при якому немає однокольорових послідовностей з попередньої задачі.

Задача 0.6.7. Множину натуральних чисел пофарбовано скінченним числом кольорів. Доведіть, що існує зростаюча послідовність $(a_n)_{n\in\omega}$ парних чисел, така що множина $\{\frac{a_i+a_j}{2} : i < j < \omega\}$ однокольорова.

Задача 0.6.5 пов'язана з такою відкритою проблемою, поставленю Овінгсом в Amer. Math. Monthly 81 (1974), 902.

Множину натуральних чисел пофарбовано двома кольорами. Чи існує зростаюча послідовність парних чисел $a_1, a_2, \ldots, a_n, \ldots$, така що всі числа $\frac{a_i+a_j}{2}, i < j$, а також всі члени цієї послідовності $(a_n)_{n\in\omega}$ однокольорові?

Бібліоґрафія

[1] Bergelson V., Leibman A. Polynomial extension of van der Warden and Szemeredi theorems, J. Amer. Math. Soc. 9 (1996), 725-753.

[2] Furstenberg H. Ergodic behavior of diagonal measures and a theorem of Szemeredi on arithmetical progressions, J. Analyse Math., 31 (1977), 204-256.

[3] Graham R., Leeb K., Rothschild. Ramsey's theorem for a class of cathegories, Advances in Math., 8 (1972), 417-433.

[4] Hales A., Jawett R. Regularity and positional games, Trans. Amer. Math. Soc., 106 (1963), 222-229.

[5] Protasov I. Combinatorics of Numbers, Mat Stud. Monogr. Ser., Vol. 2, VNTL, Lviv, 1997.

[6] Rado R. Studien zur Kombinatorik, Math. Z., 36 (1933), 424-480.

[7] Shur I. Uber die Konqruenz $x^m + y^m$ conquent $z^m (\bmod p)$, Uber. Deutsche Math. Verein 25 (1916), 114-116.

[8] Szemeredi E. On sets of integers containing no k elements in arithmetic progression, Acta Arith., 27 (1975), 199-245.

[9] van der Warden B. Beweis einer Baudetshen Vermutung, Nieuw Arch. Wisk., 15 (1927), 212-216.

[10] Walters M. Combinatorial proof of the polynomial extension of van der Warden theorem and the polynomial Hales-Jawett theorem, J. London Mat. Soc., 61 (2000), 1-12.

[11] Васильєва В., Протасов І. Навколо теореми ван дер Вардена, У світі математики, 2001, №1, 17-19.

0.7. Комбінаторика ультрафільтрів

Сім'ю $\mathcal{F}$ підмножин множини X називають *центрованою,* якщо перетин будь-якого скінченного числа її членів непорожній.

Сім'ю $\mathcal{F}$ підмножин множини X називають *фільтром,* якщо

$(F1)$ $\quad \emptyset \in \mathcal{F}$;
$(F2)$ $\quad F_1, \dots, F_n \in \mathcal{F} \Rightarrow F_1 \cap \dots \cap F_n \in \mathcal{F}$;
$(F3)$ $\quad F \in \mathcal{F}, F' \supseteq F \Rightarrow F' \in \mathcal{F}$.

Очевидно кожен фільтр є центрованою сім'єю, а кожна центрована сім'я підмножин міститься в деякому фільтрі. Для побудови такого фільтру ми спочатку приєднаємо до центрованої сім'ї найможливіші скінченні перетини її членів, а потім приєднаємо до цієї сім'ї всі надмножини її членів.

Сім'я всіх фільтрів на множині X частково впорядкована відношенням $\mathcal{F}_1 \subseteq \mathcal{F}_2$. Фільтр, максимальний щодо цього часткового порядку, називають *ультрафільтром* . Фільтр всіх підмножин з X, що містять фіксований елемент $x \in X$, очевидно, є ультрафільтром. Такі ультрафільтри називають *головними,* а неголовні ультрафільтри називають *вільними.* Зрозуміло, що ультрафільтр вільний тоді і тільки тоді, коли $\cap\mathcal{F} = \emptyset$, а тому вільні ультрафільтри можуть існувати лише на нескінченних множинах.

Теорема 0.7.1 (про ультрафільтр). *Кожен фільтр на нескінченній множині міститься в деякому ультрафільтрі.*

Доведення. Нехай $\mathcal{F}'$ — фільтр на X, α — сім'я всіх фільтрів на X, що містять $\mathcal{F}'$, γ — довільний ланцюг в α. З означення фільтру випливає, що $\cup\gamma$ — фільтр на X, що є верхньою гранню для $\mathcal{F}'$. За лемою Куратовського-Цорна, сім'я α має максимальний елемент $\mathcal{F}$. Отже, $\mathcal{F}$ — ультрафільтр на X, що містить $\mathcal{F}'$. □

З теореми випливає, що на нескінченній множині X існує вільний ультрафільтр: досить взяти фільтр усіх підмножин X зі скінченним доповненнями і доповнити його до ультрафільтру.

ТЕОРЕМА 0.7.2 (критерій ультрафільтру). *Фільтр $\mathcal{F}$ на множині X є ультрафільтром тоді і тільки тоді, коли для будь-якої підмножини $A \subseteq X$ $A \in \mathcal{F}$ або $X \setminus A \in \mathcal{F}$.*

ДОВЕДЕННЯ. Нехай $\mathcal{F}$ — ультрафільтр, $A \subseteq X$. Якщо $A \cap F = \emptyset$ для деякої підмножини $F \in \mathcal{F}$, то за умовою F3 маємо $X \setminus A \in \mathcal{F}$. Нехай $A \cap F \neq \emptyset$ для будь-якої підмножини $F \in \mathcal{F}$. Якщо $F_1, \ldots, F_n \in \mathcal{F}$, то $(F_1 \cap A) \cap \cdots \cap (F_n \cap A) = (F_1 \cap \cdots \cap F_n) \cap A$. Значить, сім'я підмножин $\{F \cap A : F \in \mathcal{F}\}$ центрована. Доповнимо її до ультрафільтру $\mathcal{F}'$. Очевидно, що $\mathcal{F} \subseteq \mathcal{F}'$ і, значить $\mathcal{F} = \mathcal{F}'$. Оскільки $A \in \mathcal{F}'$, то $A \in \mathcal{F}$.

Припустімо, що фільтр $\mathcal{F}$ має вказану властивість і міститься в деякому ультрафільтрі $\mathcal{F}'$. Якщо $\mathcal{F} \neq \mathcal{F}'$, то існує підмножина $A \in \mathcal{F}'$, така що $A \notin \mathcal{F}$. За умовою $X \setminus A \in \mathcal{F}$ і $X \setminus A \in \mathcal{F}'$, що суперечить $A \in \mathcal{F}'$, $X \setminus A \in \mathcal{F}'$, $A \cap (X \setminus A) = \emptyset$. □

З критерію ультрафільтра випливає такий наслідок: якщо $\mathcal{F}$ — ультрафільтр на X, $F \in X$ і $F = F_1 \cup \cdots \cup F_m$, то знайдеться $i \in \{1, \ldots, m\}$, таке що $F_i \in \mathcal{F}$. Припустімо супротивне: $F_1 \notin \mathcal{F}, \ldots, F_m \notin \mathcal{F}$. Тоді $X \setminus F_1 \in \mathcal{F}, \ldots, X \setminus F_m \in \mathcal{F}$ і $(X \setminus F_1) \cap \cdots \cap (X \setminus F_m) = X \setminus (F_1 \cup \cdots \cup F_m)$ дає $X \setminus F \in \mathcal{F}$, що суперечить означенню фільтра.

Ця властивість є основою доведення теорем про розбиття нескінченних множин за допомогою ультрафільтрів. Припустімо, що на множині X ми побудували ультрафільтр, кожен член якого (як підмножина з X) має певну властивість. Тоді для будь-якого розбиття $X = A_1 \cup \cdots \cup A_m$ принаймні одна з підмножин A_i розбиття має цю властивість.

ТЕОРЕМА 0.7.3 (про звуження ультрафільтру). *Якщо $\mathcal{F}$ — ультрафільтр на множині X і $F \in \mathcal{F}$, то $\mathcal{F}' = \{F' : F' \subseteq F\}$ — ультрафільтр на F.*

ДОВЕДЕННЯ. Перевірка умов F1, F2, F3 показує, що $\mathcal{F}'$ — фільтр. Нехай $F_1 \subseteq F$ і $F_1 \notin F'$. Тоді $F_1 \notin \mathcal{F}$ і за критерієм ультрафільтру $X \setminus F_1 \in \mathcal{F}$. Оскільки $F \in \mathcal{F}$ і $X \setminus F_1 \in \mathcal{F}$, то $(X \setminus F_1) \cap F = F \setminus F_1 \in \mathcal{F}$. Отже, $F \setminus F' \in \mathcal{F}'$ і $\mathcal{F}'$ — ультрафільтр. □

Нехай $\mathcal{F}$ — фільтр на множині X, $f : X \to Y$. Позначимо $f(\mathcal{F}) = \{A \subseteq Y : f^{-1}(A) \in \mathcal{F}\}$ і зауважимо, що $f(\mathcal{F})$ — фільтр на множині Y.

ТЕОРЕМА 0.7.4 (про образ ультрафільтру). *Якщо $\mathcal{F}$ — ультрафільтр на множині X, $f : X \to Y$, то $f(\mathcal{F})$ — ультрафільтр на Y.*

ДОВЕДЕННЯ. Якщо $Y = Y_1 \cup Y_2$, то $X = f^{-1}(Y_1) \cup f^{-1}(Y_2)$ і за критерієм ультрафільтру $f^{-1}(Y_1) \in \mathcal{F}$ або $f^{-1}(Y_2) \in \mathcal{F}$. Значить, $Y_1 \in f(\mathcal{F})$ або $Y_2 \in f(\mathcal{F})$ і лишилося знову застосувати критерій ультрафільтру. □

Ультрафільтри були введені Рісом 1909 року, їх широке використання розпочалося після статті Улама 1929 року. Зауважимо, що при доведенні існування вільних ультрафільтрів на кожній нескінченній множині ми використали лему Куратовського-Цорна — еквівалент аксіоми вибору. Чи можна побудувати вільний ультрафільтр на зліченній множині в аксіоматиці ZF Цермело-Френкеля без аксіоми вибору. Соловей 1970 року довів, що з аксіоматикою ZF сумісне твердження, що кожна підмножина прямої вимірна за Лебегом. Проте, що 1938 року Серпінський довів, що вільний ультрафільтр на зліченній множині дає підмножину прямої невимірну за Лебегом. Таким чином, з ZF сумісне твердження про відсутність вільних ультрафільтрів на зліченній множині. Ми приймаємо аксіому вибору без жодних застережень.

Нехай (X, τ) — топологічний простір. За означенням, фільтр $\mathcal{F}$ на X *збігається до точки* $x \in X$, якщо $W \in \mathcal{F}$ для кожного околу W точки x, при цьому точка x називається *границею фільтру* $\mathcal{F}$. Підмножина $F \subseteq X$ замкнена тоді і лише тоді, коли границя будь-якого фільтру $\mathcal{F}$ на X з умовою $A \in \mathcal{F}$ належить підмножині F.

Топологічний простір X називають *хаусдорфовим,* якщо для будь-яких двох точок X знайдуться околи цих точок, що не перетинаються. Топологічний простір хаусдорфів тоді і лише тоді, коли кожен фільтр на X має не більше одної границі.

Нехай $(X_1 \tau_1), (X_2, \tau_2)$ — топологічні простори, $x \in X_1$. Відображення $f : X_1 \to X_2$ неперервне в точці x тоді і лише тоді, коли для будь-якого ультрафільтру $\mathcal{F}$ на X_1, що збігається до x, ультрафільтр $f(\mathcal{F})$ збігається до точки $f(x)$.

Топологічний простір називають *компактним,* якщо з будь-якого його покриття відкритими підмножинами можна виділити скінченне підпокриття. Топологічний простір X компактний тоді, коли кожен ультрафільтр на X збігається.

Нехай X — дискретний простір, βX — множина усіх ультрафільтрів на X. Для довільної підмножини $A \subseteq X$ позначимо $\bar{A} = \{p \in \beta X : A \in p\}$. Сім'я $\{\bar{A} : A \subseteq X\}$ є передбазою деякої (однозначно визначеної) топології на X. Отже, підмножина $W \subset \beta X$ є околом ультрафільтру $q \in \beta X$ тоді і тільки тоді, коли знайдеться підмножина $A \subseteq X$, така що $p \in \bar{A} \subseteq W$. Кожна підмножина $\bar{A}$, $A \subseteq X$ відкрита і замкнена в βX.

Нехай φ — фільтр на X, $\bar{\varphi} = \{p \in \beta X : \varphi \subseteq p\}$. Оскільки $\bar{\varphi} = \cap\{\bar{A} : A \in \varphi\}$, $\bar{\varphi}$ — замкнена підмножина. З іншого боку, для кожної непорожньої замкненої підмножини $F \subseteq \beta X$ знайдеться фільтр φ на X, такий що $\bar{\varphi} = F$.

Нехай $p, q \in \beta X$, $p \neq q$. Виберімо підмножину $P \in p$, таку що $P \notin q$. Тоді $X \setminus P \in q$ і $P, x \setminus P$ — околи ультрафільтрів p, q, що не перетинаються. Отже, простір βX хаусдорфів.

Переконаймося, що простір βX компактний. Нехай $\mathcal{U}$ — відкрите покриття βX. Оскільки кожна відкрита множина в βX є об'єднанням підмножин виду $\bar{A}$, $A \subseteq X$, ми можемо вважати, що $\mathcal{U} = \{\bar{A} : A \in \mathcal{A}\}$, де $\mathcal{A}$ — деяка сім'я підмножин X. Позначмо $\mathcal{F} = \{X \setminus A : A \in \mathcal{A}\}$. Припустімо, що сім'я $\mathcal{F}$ центрована і доповнимо її до ультрафільтру q. Оскільки $\mathcal{U}$ — покриття βX, знайдеться підмножина $A \in \mathcal{A}$, така що $p \in \bar{A}$. З іншого боку, $X \setminus A \in p$, що суперечить означенню фільтра. Таким чином, сім'я $\mathcal{F}$ не є центрованою і ми можемо вибрати підмножини $A_1, \dots, A_n \in \mathcal{A}$, такі що $(X \setminus A_1) \cap \dots \cap (X \setminus A_n) = \emptyset$. Тоді $A_1 \cup \dots \cup A_n = X$ і $\{\bar{A}_1, \dots, \bar{A}_n\}$ — скінченне підпокриття X.

Кожен головний ультрафільтр на X є ізольованою точкою простору βX, а множина усіх гловних ультрафільтрів щільна в βX. А тому ми можемо ототожнити X з множиною усіх головних ультрафільтрів і вважати, що X щільна в βX.

Довільне відображення $f : X \to Y$ простору $X \subseteq \beta X$ в компактний хаусдорфів простір Y однозначно продовжується до неперервного відображення $f^\beta : \beta X \to Y$. Якщо $p \in \beta X$, то $f^\beta(p) = \{A \in Y : f^{-1}(A) \in p\}$ (див. теоерму про образ ультрафільтру).

Компактний простір βX називають *чех-стоуновою* компактифікацією дискретного простору X. Можна показати, що $|\beta X| = 2^{2^{|X|}}$ для кожного нескінченного дискретного простору X.

Нехай S — напівгрупа з дискретною топологією. Ми опишемо конструкцію продовження операції множення з S на βS. Для кожного $g \in S$ лівий зсув $l_g : S \to S$, $l_g(x) = gx$ однозначно продовжується до неперервного відображення $l^\beta : \beta S \to \beta S$. Оскільки, для кожного ультрафільтру $q \in \beta S$ $l_g^\beta(q) = \{gQ : Q \in q\}$, ми записуємо $l_g^\beta(q)$ як gq. Далі, для кожного ультрафільтру $q \in \beta S$, ми продовжимо правий зсув

$r_q : S \to \beta S$, $r_q(x) = xq$ до відображення $r_q^\beta : \beta S \to \beta S$ і позначимо $r_q^\beta(p) = pq$. Рутинна перевірка показує, що добуток ультрафільтрів є асоціативним, тож βS — напівгрупа. Безпосередньо з конструкції операції продовження випливає, що в компактній напівгрупі βS кожен правий зсув $p \mapsto pq$, $q \in \beta S$ неперервний, а лівий зсув $x \to gx$ неперервний для кожного елемента $g \in S$.

Нехай $p, q \in \beta S$, $P \in p$ і $Q_x \in q$ для кожного $x \in P$. Тоді підмножина $\bigcup\limits_{x \in P} xQ_x$ є елементом ультрафільтру pq і навпаки, кожене елемент ульрафільтру pq містить підмножину S вказаного виду. Таким чином, мо описали явно деяку базу добутку ультрафільтрів pq.

Напівгрупу S, наділену топологією, називають *правотопологічною,* якщо кожне відображення $x \mapsto xs, s \in S$ неперервне. Таким чином, компактна напівгрупа βS правотопологічна.

Вирішальне значення для застосування ультрафільтрів до комбінаторики розбиттів має теорема про ідемпотент. *Ідемпотентом* напівгрупи S називають елемент $s \in S$, такий що $ss = s$.

ТЕОРЕМА 0.7.5 (про ідемпотенти). *Кожна компактна хаусдорфова правотопологічна напівгрупа має хоча б один ідемпотент.*

ДОВЕДЕННЯ. Нехай $\mathcal{L}$ — довільний ланцюг замкнених піднапівгруп S. В силу компактності S підмножина $\cap\mathcal{L}$ непорожня, а тому є замкненою напівгрупою. За лемою Куратовського-Цорна існує мінімальна за включенням замкнена напівгрупа H. Нехай e — довільний елемент з H. Оскільки $(He)(He) \subseteq He$, то He піднапівгрупа H. З неперервносі правого зсуву на елемент e, компактності та хаусдорфовості H випливає, що

He замкнена піднапівгрупа. Оскільки H — мінімальна замкнена піднапівгрупа і $He \subseteq H$, то $He = H$. Розглянемо множину $E = \{x \in H : xe = x\}$. Оскільки $e \in H$, то $E \neq \emptyset$. Очевидно, E — піднапівгрупа, а з неперерності правого зсуву випливає замкненість H. Оскільки $E \subseteq H$, то $E = H$. Отже, $e \in E$ і $e^2 = e$. □

Підмножина L напівгрупи S називається *лівим ідеалом*, якщо $sL \subseteq L$ для будь-якого $s \in S$.

ТЕОРЕМА 0.7.6 (про лівий ідеал). *Нехай S — компактна хаусдорфова правотопологічна напівгрупа. Кожен мінімальний лівий ідеал замкнений. Кожен лівий ідеал містить мінімальний лівий ідеал.*

ДОВЕДЕННЯ. Нехай L — мінімальний лівий ідеал, $s \in L$. Тоді $Ss = L$. З неперервності зсуву $x \mapsto xs$, компактності та хаусдорфовості S випливає замкненість Ss. Для доведення другого твердження, нехай H — лівий ідеал, $h \in H$. Оскільки $Sh \subseteq H$ і Sh — замкнений лівий ідеал, то множина замкнених лівих ідеалів, що містяться в H, непорожня. Нехай $\mathcal{L}$ — довільний ланцюг замкнених лівих ідеалів напівгрупи S, що містяться в H. З компактності S випливає, що $\cap\mathcal{L} \neq \emptyset$, а тому являється замкненим лівим ідеалом. За лемою Куратовського-Цорна існує мінімальний за включенням замкнений лівий ідеал L, що міститься в H. Нехай $a \in L$. Оскільки $Sa \subseteq L$ і Sa — замкнений лівий ідеал, то L — мінімальний ідеал напівгрупи S. □

Нехай $(a_n)_{n\in\omega}$ — ін'єктивна послідовність елементів напівгрупи S. Позначимо $FP(a_n)_{n\in\omega}$ сукупність усіх елементів з S виду $a_{n_1}a_{n_2}\dots a_{n_k}$, де $n_1 < n_2 < \dots < n_k$, k — довільне натуральне число. Підмножину $A \subseteq S$ називають *FP-множиною,* якщо знайдеться ін'єктивна послідовність $(a_n)_{n\in\omega}$ елементів з A, така що $FP(a_n)_{n\in\omega} \subseteq A$. Якщо напівгрупа S комутативна і напівгрупова операція позначена символом "$+$", замість позначення FP використовують позначення FS.

Лема 0.7.7. *Якщо вільний ультрафільтр p на напівгрупі S є ідемпотентом напівгрупи βS, то кожна підмножина $A \in P$ є FP-множиною.*

Доведення. Позначмо $A_0 = A$. Оскільки $pp = p$ і $p \in \overline{A}_0$, за неперервністю правих зсувів існує підмножина $B \in p$, $B \subseteq A_0$, така що $\overline{B}p \subseteq \overline{A}_0$. Зафіксуймо довільний елемент $a_0 \in B$. Оскільки $a_0 p \in \overline{A}_0$ і $a_0 \in S$, за неперервністю лівих зсувів на елементи з S існує підмножина A_1, така що $a_0\overline{A}_1 \subseteq \overline{A}_0, A_1 \subseteq A_0, a_0 \notin A_1$. Отже $a_0 A_1 \subseteq A_0, A_1 \subseteq A_0, a_0 \in A_0 \setminus A_1$.

Аналогічно, за підмножиною $A_1 \in p$ знаходимо $a_1 \in S, A_2 \in p$, такі що $a_1 A_2 \subseteq A_1, A_2 \subseteq A_1, a_1 \in A_1 \setminus A_0$. продовжуючи цей процес, ми побудуємо ін'єктивну послідовність $(a_n)_{n\in\omega}$ елементів з A та ланцюжок підмножин $A_0 \supseteq A_1 \supseteq \cdots \supseteq A_n \supseteq \ldots$, такі що $A_n \in p$, $a_n A_{n+1} \subseteq A_n, a_n \in A_n \setminus A_{n+1}$. Очевидно, $FP(a_n)_{n\in\omega} \subseteq A$. □

Теорема 0.7.8 (про FP-множину). *Якщо нескінченна напівгрупа S не має ідемпотентів або є напівгрупою з лівими скороченнями, то для довільного скінченного розбиття $S = A_1 \cup \cdots \cup A_m$ принаймні одна з підмножин розбиття є FP-множиною.*

Доведення. З огляду на лему 0.7.7 нам досить довести існування вільного ультрафільтру на S, що є ідемпотентом напівгрупи βS.

Якщо S на має ідемпотентів, то довільний ідемпотент $p \in \beta S$ (див. теорему про ідемпотенти) є вільним ультрафільтром.

Нехай S — напівгрупа з лівими скороченнями: з $sa = sb$ випливає $a = b$. Тоді підмножина sA нескінченна для довільного елементу $s \in S$ і довільної нескінченної підмножини $A \subseteq S$. Звідси легко випливає, що $\beta S \setminus S$ є піднапівгрупою βS і ми можемо взяти довільний ідемпотент з $\beta S \setminus S$. $\square$

Зауважимо, що для довільних напівгруп ця теорема, взагалі кажучи, не вірна. Тривіальний контрприклад: нехай X — нескінченна множина, $a \in X$ і $xy = a$ для всіх $x, y \in X$, $A_1 = \{a\}$, $A_2 = X \setminus A_1$.

З теореми про FP-множину випливає теорема Хайндмена: якщо множину натуральних чисел $\mathbb{N}$ розбито на скінченне число підмножин $\mathbb{N} = A_1 \cup \cdots \cup A_m$, то принаймні одна з підмножин розбиття A_i містить нескінченну підмножину A, таку що $FS(A) \subseteq A_i$, де $FS(A)$ — множина усіх скінченних сум різних елементів з A. Дійсно, треба застосувати теорему до напівгрупи $(\mathbb{N}, +)$. Множина $\mathbb{N}$ має також мультиплікативну напівгрупову структуру, а тому підмножина A_j розбиття і нескінченна підмножина $B \subseteq A_j$, такі що $FP(B) \subseteq A_j$, де $FP(B)$ — множина скінченних добутків різних елементів з B. Зовсім не очевидно, що можна вибрати ці підмножини так, що $i = j$.

Теорема 0.7.9 (Хайндмена про $FS-$ та $FP-$множини). *Для довільного скінченного розбиття множини натуральних чисел $\mathbb{N} = A_1 \cup \cdots \cup A_m$ знайдеться підмножина розбиття A_k, що є FS- та FP-підмножиною.*

Доведення. Нехай L — множина усіх ультрафільтрів на $\mathbb{N}$, кожен елемент якого є FS-множиною. За лемою 0.7.7 L містить усі ідемпотенти напівгрупи $\beta(\mathbb{N}, +)$, зокрема, $L \neq \emptyset$. Зауважимо також, що підмножина L замкнена.

Ми перевіримо, що L — лівий ідеал напівгрупи $\beta(\mathbb{N}, \times)$. Нехай $p \in L$, $q \in \beta\mathbb{N}$, $A \in qp$. Виберемо підмножину $Q \in q$, таку що $\overline{Q}p \subseteq \overline{A}$. Візьмемо довільний елемент $a \in Q$. Оскільки $ap \in \overline{Q}$, то знайдеться підмножина $P \in p$, така що $aP \subseteq A$.

Оскільки P — FS-множина, знайдеться ін'єктивна послідовність $(a_n)_{n\in\omega}$ елементів з P, така що $FS(a_n)_{n\in\omega} \subseteq P$. Із включень $PS(aa_n)_{n\in\omega} \subseteq aP \subseteq A$ випливає, що A — FS-множина. Таким чином, $qp \in L$.

Оскільки L — замкнена піднапівгрупа напівгрупи $\beta(\mathbb{N}, \times)$, L містить деякий ідемпотент p напівгрупи $\beta(\mathbb{N}, \times)$. Ясно, що p-вільний ультрафільтр, а тому за лемою 0.7.7 кожна підмножина $A \in p$ є одночасно FS- та FP-множиною. Залишилося лише вибрати елемент A_k розбиття, що належить ультрафільтру p. □

Цікава історі теореми Хайдмена. В 1916 р. Шур довів, що для кожного скінченного розфарбування множини натуральних чисел рівняння $x + y = z$ має однокольоровий розв'язок. Застосовуючи цю теорему Шур довів що для кожного натурального числа m порівняння $x^m + y^m \equiv z^m (\bmod p)$ має розв'язок в натуральних числах для всіх досить великих простих чисел p. Теорему Шура можна переформулювати так: для довільного скінченного розбиття $\mathbb{N} = A_1 \cup \dots \cup A_m$ знайдуться підмножина розбиття A_i і двоелементна підмножина $A \subseteq A_i$, такі що $FS(A) \subseteq A_i$. Згодом ряд авторів, першим з яких був Радо, узагальнили теорему Шура: для довільного натурального числа k існують підмножина розбиття A_i та підмножина $A \subseteq A_i$ такі що $|A| = k$ і $FS(A) \subseteq A_i$. А тому природно виникла гіпотеза, що знайдуться підмножина розбиття A_i і нескінченна підмножина $A \subseteq A_i$, такі що $FS(A) \subseteq A_i$. Цю гіпотезу довів Хайдмен 1974 року. Але доведення Хайдмена було настільки складним та незграбним, що не влаштовувало нікого, включно з його автором. Гелвін помітив, що доведення теореми Хайдмена стане тривіальним , якщо довести існування ультрафільтру p на множині $\mathbb{N}$ з такою властивістю: для кожної підмножини $P \in p$ знайдуться підмножина $Q \in p$ та елемент $a \in P$, такі що $a + Q \subseteq P$. В 1975 р. Глейзер довів існування такого ультрафільтру, продовживши операцію додавання з $\mathbb{N}$ на $\beta\mathbb{N}$ і скориставшись теоремою Нумакури про існування ідемпотенту в компактній правотопологічній напівгрупі. Саме з цього моменту розпочалося активне застосування ультрафільтрів в комбінаториці чисел.

Ми розглянемо ще одне застосування ультрафільтрів — доведемо відому теорему ван дер Вардена про арифметичні прогресії. Це доведення належить Бергельсону та Хайдмену.

Нехай m — натуральне число, S — добуток m копій напівгрупи $\beta(\mathbb{N},+)$. Елементи простору S будемо зображати векторами $\vec{p}=(p_1,\dots,p_m)$. Відносно покоординатного додавання S — компактна проавотопологічна напівгрупа. Позначмо

$$E^* = \{(a, a+d, \dots, a+(m-1)d) : a \in \mathbb{N}, d \in \mathbb{N} \cup \{0\}\},$$

$$I^* = \{(a, a+d, \dots, a+(m-1)d)\} : a \in \mathbb{N}, d \in \mathbb{N}\}.$$

Нехай E та I відповідно замикання множин E^* та I^* в напівгрупі S.

Лема 0.7.10. *E — піднапівгрупа напівгрупи S, I — ідеал напівгрупи E.*

Доведення. Нехай $\vec{p} = (p_1,\dots,p_m)$, $\vec{q} = (q_1,\dots,q_m)$, $p,q \in E$. Нехай $V_1 \times \dots \times V_m$ — довільний окіл $\vec{p}+\vec{q}$. Користуючись неперервністю відображення $x \mapsto x+q$, виберемо окіл $U_1 \times \dots \times U_m$ точки $\vec{p}$, такий що

$$(U_1 \times \dots \times U_m) + \vec{q} \subseteq V_1 \times \dots \times V_m.$$

Візьмемо елементи $a \in \mathbb{N}, d \in \mathbb{N} \cup \{0\}$ ($d \in \mathbb{N}$, якщо $p \in I$), такі що $(a,\dots,a+(m-1)d) = \vec{x}$ і $\vec{x} \in U_1 \times \dots \times U_m$. Оскільки $\vec{x}+\vec{q} \in V_1 \times \dots \times V_m$ і $a, a+d, \dots, a+(m-1)d \in \mathbb{N}$, знайдеться окіл $W_1 \times \dots \times W_m$ елемента q, такий що

$$\vec{x} + (W_1 \times \dots \times W_m) \subseteq V_1 \times \dots \times V_m.$$

Візьмемо елементи $b \in \mathbb{N}$, $e \in \mathbb{N} \cup \{0\}$ ($e \in \mathbb{N}$, якщо $q \in I$) такі що $b, b+e, \dots, b+(m-1)e) = \vec{y}$, $\vec{y} \in W_1 \times \cdots \times W_m$. Тоді

$$\vec{x}+\vec{y} \in V_1 \times \cdots \times V_m, \quad \vec{x}+\vec{y} = (a+b, \dots, a+b+(m-1)(d+e)).$$

Отже, $\vec{x}+\vec{y} \in E^*$ і, якщо $\vec{p} \in I$ або $q \in I$, то $\vec{x}+\vec{y} \in I^*$. □

ЛЕМА 0.7.11. *Якщо $p \in \beta\mathbb{N}$ і $\vec{p} = (p, \dots, p)$, то $\vec{p} \in E$.*

ДОВЕДЕННЯ. Нехай $U_1 \times \cdots \times U_m$ — довільний окіл $\vec{p}$. Тоді $U = U_1 \cap \cdots \cap U_m$ — окіл p. Якщо $a \in \mathbb{N} \cap U$, то

$$(a, \dots, a) \in (U_1 \times \cdots \times U_m) \cap E^*.$$

□

ЛЕМА 0.7.12. *Якщо L — мінімальний лівий ідеал напівгрупи $\beta(\mathbb{N}, +), p \in L$ і $\vec{p} = (p, \dots, p)$, то $p \in I$.*

ДОВЕДЕННЯ. За теоремою про лівий ідеал в лівому ідеалі $E+\vec{p}$ напівгрупи E можна знайти мінімальний лівий ідеал F. Оскільки F — замкнена піднапівгрупа, то існує ідемпотент $\vec{q} \in F$. Оскільки $\vec{q} \in E+\vec{p}$, то $\vec{q} = \vec{r}+\vec{p}$ для деякого $\vec{r} \in E$. Нехай

$$\vec{q} = (q_1, \dots, q_m), \quad \vec{r} = (r_1, \dots, r_m).$$

Тоді $q_i = r_i + p \in \beta\mathbb{N} + p$. Оскільки L — мінімальний лівий ідеал напівгрупи $\beta(\mathbb{N}, +)$ і $p \in L$, то $L = \beta\mathbb{N} + p = \beta\mathbb{N} + q_i$. Для кожного $i \in \{1, \dots, m\}$ виберемо елемент $t_i \in \beta\mathbb{N}$, такий що $t_i + q_i = p$. Тоді $t_i + q_i + q_i = t_i + q_i = p$. Отже, $\vec{p}+\vec{q} = \vec{p}$ і $\vec{p} \in F$.

Залишилось показати, що $F \subseteq I$. Оскільки $I + F \subseteq F$ і $I + F \subseteq I$, то $I + F \subseteq F \cap I$. Отже, $F \cap I \neq \emptyset$. Оскільки I — ідеал, а F — лівий ідеал напівгрупи E і, в силу мінімальності F, $\subseteq I$. □

Лема 0.7.13. *Якщо L — мінімальний лівий ідеал напівгрупи $\beta(\mathbb{N},+)$, $p \in L$, то кожна підмножина $A \in p$ містить як завгодно довгі арифметичні прогресії.*

Доведення. Зафіксуймо довільне натуральне число m і розгляньмо окіл $\overline{A}\times\cdots\times\overline{A}$ елементу $\vec{p}=(p,\dots,p)$ напівгрупи S. За лемою 0.7.12 існує елемент $\vec{x}\in I^*\cap(\overline{A}\times\cdots\times\overline{A})$. Тоді $\vec{x}=(a,a+d,\dots,a+(m-1)d)$, $a,d\in\mathbb{N}$, причому $a,a+d,\dots,a+(m-1)d\in A$. ☐

Теорема 0.7.14 (ван дер Вардена). *Якщо множину натуральних чисел розбити довільним числом на скінченне число підмножин $\mathbb{N}=A_1\cup\cdots\cup A_n$, то принаймні одна із підмножин розбиття A_i містить як завгодно довгі арифметичні прогресії.*

Доведення. Візьмемо ультрафільтр p, що належить деякому мінімальному лівому ідеалу напівгрупи $\beta(\mathbb{N},+)$, виберемо підмножину розбиття $A_i\in p$ і застосуємо лему 0.7.13. ☐

Застосовуючи аналогічні міркування до напівгрупи $(\beta\mathbb{N},\times)$ ми знаходимо підмножину розбиття A_j, що містить як завгодно довгі геометричні прогресії. І знову ж постає питання , и можна вибрати спільну підмножину розбиття?

Теорема 0.7.15 (Бергельсона-Хайндмена). *Для будь-якого скінченного розбиття множини натуральних чисел $\mathbb{N}=A_1\cup\cdots\cup A_n$ знайдеться підмножина A_i, що містить як завгодно довгі арифметичні і як завгодно довгі геометричні прогресії.*

Доведення. Нехай W — множина усіх ультрафільтрів на $\mathbb{N}$, кожен елемент яких містить як завгодно довгі арифметичні прогресії. За лемою 0.7.13 $W\neq\emptyset$. Перевіримо, що W — лівий ідеал напівгрупи $\beta(\mathbb{N},\times)$. Нехай $p\in W, q\in\beta\mathbb{N}$. Зафіксуємо довільну підмножину $A\in qp$ і виберімо підмножину

$Q \in q$, таку що $\overline{Q}p \subseteq \overline{A}$. Нехай $a \in Q$. Тоді $aP \subseteq A$ для деякої підмножини $P \in p$. За означенням W підмножина P містить як завгодно довгі арифметичні прогресії. Але тоді як завгодно довгі арифметичні прогресії лежать і в множині aP, а отже і в A. Значить, $qp \in W$.

В лівому ідеалі W напівгрупи $\beta(\mathbb{N}, \times)$ міститься деякий мінімальний лівий ідеал L. Візьмемо довільний ультрафільтр $p \in L$ і виберемо підмножину A_i розбиття, що є елементом ультрафільтру p. Оскільки $p \in W$, A_i містить арифметичні прогресії довільної скінченної довжини. Оскільки $p \in L$, A_i містить як завгодно довгі геометричні прогресії. $\square$

Докладний виклад застосувань ультрафільтрів в комбінаториці можна знайти в [**1**] та [**2**].

Бібліоґрафія

[1] Hindman N., Srauss D. Algebra in Stone-Čech Compatification: Theory and Applications, Walters de Grueter, Berlin, 1998.

[2] Protasov I. V. Combinatorics of Numbers, Mat. Stud. Monogr. Ser. Vol. 2. 1997.

0.8. Топологічна динаміка і комбінаторика

Нехай (X, d) — компактний метричний простір, $f : X \to X$ — неперервне відображення. *Динамічною системою* на X, визначеною відображенням f, називають пару (X, f). Одним з центральних понять топологічної динаміки, що тісно пов'язане з комбінаторикою є поняття рекурентності.

Точку $x \in X$ називають *рекурентною точкою* динамічної системи (X, f), якщо для будь-якого її околу V знайдеться натуральне число m, таке що $f^m(x) \in V$. Іншими словами, точка x рекурентна, якщо існує зростаюча послідовність $(m_k)_{k\in\omega}$ натуральних чисел, така що послідовність $(f^{m_k}(x))_{k\in\omega}$ збігається до x.

Точку $x \in X$ називають *рівномірно рекурентною* точкою динамічної системи (X, f), якщо для будь-якого її околу V знайдеться натуральне число m, таке що

$$V \cap \{f^n(x), f^{n+1}(x), \dots, f^{n+m}(x)\} \neq \emptyset$$

для довільного натурального числа n. Для кожної точки $x \in X$ підмножину $\mathrm{Orb}(x) = \{f^n(x) : n \in \mathbb{N}\}$ називають орбітою точки x. Таким чином, точка x рівномірно рекурентна, якщо для кожного її околу V кожен досить довгий відрізок її орбіти містить принаймні одну точку з V. Зрозуміло, що кожна рівномірно рекурентна точка рекурентна.

Теорема 0.8.1 (Біркгофа). *Кожна динамічна система* (X, f) *має принаймні одну рівномірно рекурентну точку.*

Доведення. Топологічною орбітою точки $x \in X$ ми будемо називати замикання $\overline{\mathrm{Orb}(x)}$ її орбіти $\mathrm{Orb}(x)$ в X. Непуста замкнена підмножина $A \subseteq X$ називається інваріантною, якщо $f(A) \subseteq A$. Інваріантна підмножина $M \subseteq X$ мінімальна, якщо M не містить власних інваріантних підмножин. Ми доведемо дещо сильніше твердження: кожна інваріантна підмножина динамічної системи (X, f) містить хоча б одну рекурентну точку. Три спостереження:

(*) топологічна орбіта будь-якої точки $x \in X$ інваріантна;

(**) підмножина $M \subseteq X$ мінімальна тоді і тільки тоді, коли $M = \overline{\mathrm{Orb}}(x)$ для будь-якої точки $x \in M$;

(***) точка $x \in X$ рівномірно рекурентна тоді і тільки тоді, коли $\overline{\mathrm{Orb}}(x)$ — мінімальна підмножина.

Ми доведемо лише (***). Нехай $\overline{\mathrm{Orb}}$ — мінімальна множина, $M = \overline{\mathrm{Orb}}(x)$, V —довільний відкритий окіл x. Позначмо $K = \bigcup\limits_{k=1}^{\infty} f^{-k}(V)$ і припустімо, що $M \setminus K \neq \emptyset$. Оскільки підмножина $f^{-k}(V)$ відкрита для будь-якого k, то K відкрита, а $M \setminus K$ замкнена. Переконаймося, що $M \setminus K$ інваріантна. Якщо $y \in M \setminus K$, а $f(y) \notin M \setminus K$, то $f(y) \in K$ і $f(y) \in f^{-k}(V)$ для деякого k. Значить, $y \in f^{-k-1}(V)$ і $y \in K$, суперечність. Оскільки підмножина M мінімальна, а $M \setminus K \subset M$, то $M \setminus K = \emptyset$.

Отже, $M \subseteq \bigcup_{k=1}^{\infty} f^{-k}(V)$. Оскільки M компактна підмножина, ми можемо з відкритого покриття $\{f^{-k}(V) : k \in \mathbb{N}\}$ виділити скінченне підпокриття $f^{-1}(V), \dots, f^{-m}(V)$. Якщо n — довільне натуральне число, то $f^n(x) \in f^{-k}(V)$ для деякого $k \in \{1, \dots, m\}$, тобто $f^{n+n}(x) \in V$, що і означає рівномірну рекурентність x.

У зворотній бік, нехай x рівномірно рекурентна. Припустимо, що підмножина M, $M = \overline{\mathrm{Orb}}(x)$ не є мінімальною і виберемо власну інваріантну підмножину $A \subset M$. Оскільки $x \notin A$, то знайдуться відкриті підмножини V, U такі що $x \in V$, $A \subseteq U$ і $V \cap U = \emptyset$. За означенням рівномірної рекурентності існує натуральне m, таке що для будь-якого натурального n принаймні одна з точок $f^n(x), \dots, f^{n+m}(x)$ належить V. Візьмемо довільну точку $a \in A$ і виберемо такий її окіл W, що $f(W) \subseteq U, \dots, f^{n+m}(W) \subseteq U$. Оскільки $a \in \overline{\mathrm{Orb}}(x)$, то $f^k(x) \in W$ для деякого k, але тоді $f^k(x), \dots, f^{k+m}(x) \in U$, всупереч з тим, що $U \cap V = \emptyset$.

Завершити доведення теореми дуже просто: за лемою Цорна (враховуючи компактність X) кожна інваріантна підмножина містить мінімальну інваріантну підмножину, а далі застосуємо (***). ☐

Далі значно делікатніше твердження — теорема Фюрстенберга-Вейса про спільну рекурентну точку. Кажуть, що два відображення f, g простору X комутують, якщо $fg = gf$.

Теорема 0.8.2 (Фюрстенберга-Вейса). *Нехай $f_1, \dots, f_m$ — гомеоморфізми компактного метричного простору X, що попарно комутують. Тоді існують точка $x \in X$ і зростаюча послідовність натуральних чисел $(k_n)_{n \in \omega}$, такі що*

$$f_1^{k_n}(x) \to x, \dots, f_m^{k_n}(x) \to x,$$

де $\to$ означає збіжність при n що прямує до нескінченності.

Для доведення теореми на потрібні деякі означення і допоміжні твердження.

Нехай (X, d) — компактний метричний простір, $f : X \to X$ — неперервне відображення. Замкнуту підмножину $A \subseteq X$ називають *рекурентною* в динамічній системі (X, f), якщо для будь-якого $\epsilon > 0$ існують $x, y \in A$ і натуральне число n, такі що $d(f^n(x), y) < \epsilon$.

Автоморфізм динамічної системи (X, f) — це такий гомеоморфізм простору X, що комутує з f.

Підмножину $A \subseteq X$ називають *однорідною* в динамічній системі (X, f), якщо група автоморфізмів G діє транзитивно на A, тобто для довільних $x, y \in X$ існує автоморфізм $g \in G$, такий що $g(x) = y$.

Підмножину $A \subseteq X$ називають *слабко однорідною* в динамічній системі (X, f), якщо G-орбіта кожної точки із A щільна в A. Іншими словами, для довільних $x, y \in A$ і $\epsilon > 0$ знайдеться автоморфізм g системи (X, f), такий що $g(x) \in A$ і $d(g(x), y) < \epsilon$.

ТЕОРЕМА 0.8.3 (про рекурентну підмножину). *Якщо A — однорідна рекурентна підмножина динамічної системи (X, f), то кожна точка з A рекурентна. Якщо A — слабко однорідна рекурентна підмножина, то A містить щільну підмножину рекурентних точок.*

Якщо x — рекурентна точка динамічної системи (X, f) і g — автоморфізм (X, f), то точка $g(x)$ також рекурентна. Дійсно, якщо $f^{k_n}(x) \to x$, то $g(f^{k_n}(x)) \to g(x)$ і $f^{k_n}(g(x)) \to g(x)$. Отже, для доведення теореми досить переконатись в існуванні в кожній слабко рекурентній підмножині прнаймні одної рекурентної точки.

Лема 0.8.4. *Якщо A — слабко однорідна рекурентна підмножина, то для будь-яких $y \in A$ і $\epsilon > 0$ існують $x \in A$ і натуральне число n, такі що $d(f^n(x), y) < \epsilon$.*

Доведення. За означенням рекурентної підмножини знайдуться послідовності $(x_n)_{n\in\omega}, (y_n)_{n\in\omega}$ елементів з A і зростаюча послідовність $(k_n)_{n\in\omega}$ натуральних чисел, такі що $d(f^{k_n}(x_n)), y_n) \to 0$. Користуючись компактністю A, після переходу до підпослідовностей, можна вважати, що послідовність $(y_n)_{n\in\omega}$ збігається до деякої точки $y' \in A$. З огляду на слабку однорідність A знайдеться автоморфізм g, такий що $d(g(y'), y) < \frac{\epsilon}{2}$. Підберемо $\delta > 0$, таке що $d(g(z), g(y')) < \frac{\epsilon}{2}$ як тільки $d(z, y') < \delta$. Оскільки $f^{k_n}(x_n) \to y'$, то при досить великих n маємо

$$d(g(f^{k_n}(x_n)), g(y')) < \frac{\epsilon}{2}.$$

Значить, при досить великих n

$$d(f^{k_n}(g(x_n)), y) \leq d(g(f^{k_n}(x_n)), g(y')) + d(g(y'), y) < \epsilon$$

і можна покласти $x = g(x_n)$. □

Лема 0.8.5. *Якщо A — слабко однорідна рекурентна підмножина, то для будь-якого $\epsilon > 0$ існують $z \in A$ і натуральне число n, такі що $d(f^n(z), z) < \epsilon$.*

Доведення. Ми побудуємо послідовність $(z_n)_{n\in\omega}$ точок з A, одна з яких буде шуканою. За z_0 візьмемо довільну точку з A. Позначимо $\epsilon_1 = \frac{\epsilon}{2}$ і користуючись лемою 0.8.4, знайдемо $z_1 \in A$ і натуральне число k_1, такі що $d(f^{k_1}(z_1), z_0) < \epsilon_1$. За неперервністю f^{k_1} знайдеться $\epsilon_2 < \epsilon_1$, таке що з умови $d(z, z_1) < \epsilon_2$ випливає $d(f^{k_1}(z), z_0) < \epsilon_1$. Для точки z_1 підберемо $z_2 \in A$ і натуральне k_2, такі що $d(f^{k_2}(z_2), z_1) < \epsilon_2$. Виберемо $\epsilon_3 < \epsilon_2$ так щоб з $d(z, z_2) < \epsilon_2$ випливало $d(f^{k_2}(z), z_1) < \epsilon$

і т. д. У підсумку одержимо послідовності $(z_n)_{n\in\omega}$ і $(k_n)_{n\in\omega}$, такі що при $j > i$

$$d(f^{k_j+k_{j-1}+\dots+k_i}(z_j), z_i) < \epsilon_i.$$

Оскільки X — компактний метричний простір, знайдеться пара натуральних чисел $i, j, i < j$, така що $d(z_i, z_j) < \epsilon_1$. Отримаємо

$$d(f^{k_j+\dots+k_i}(z_j), z_j) \leq d(f^{k_j+\dots+k_i}(z_j), z_i) + d(z_i, z_j) < \epsilon_i + \epsilon_1 \leq \epsilon.$$

Покладемо $z = z_j, n = k_j + \dots + k_i$. □

Відображення $f : X \to \mathbb{R}$ називається *напівнеперервним зверху* в точці $x_0 \in X$, якщо для будь-якого $\delta > 0$ знайдеться $\epsilon > 0$, таке що з $d(x, x_0) < \epsilon$ випливає $f(x) < \delta$. Відображення, напівнеперервне в кожній точці з X називається *напівнеперевним зверху.*

ЛЕМА 0.8.6. *Нехай X — компактний метричний простір, $h : X \to \mathbb{R}$ — напівнеперервне зверху відображення, $h(x) \geq 0$ для всіх $x \in X$. Тоді існує точка простору x, в якій h неперервне.*

ДОВЕДЕННЯ. Для кожного натурального числа n позначимо через F_n множину усіх точок $x \in X$, в кожному околі яких є точка x', така що $h(x) - h(x') > \frac{1}{n}$. Якщо точок неперервності не існує, то $X = \bigcup\limits_{n=1}^{\infty} F_n$. Значить, $X = \bigcup\limits_{n=1}^{\infty} \overline{F}_n$ і за лемою Бера існує натуральне число m, таке що $\operatorname{int} \overline{F}_m \neq \emptyset$. Нехай V — відкрита множина, що міститься в $\overline{F}_m$. Ми побудуємо послідовність $x_0, x_1, \dots$ точок із V, таку що $h(x_n) - h(x_{n+1}) > \frac{1}{2m}$. Тоді $h(x_0) - h(x_n) > \frac{n}{2m}$ і при досить великих n $f(x_n) < 0$, що суперечить умові.

Зафіксуймо довільну точку $x_0 \in F_m \cap V, h(x_0) = \delta_0$. Знайдемо точку $x' \in F_m \cap V$, таку що $\delta_0 - h(x_0) > \frac{1}{m}$. Оскільки відображення h напівнеперервне зверху в точці x', знайдеться окіл $V' \subseteq V$ точки x', такий що $h(y) - h(x') < \frac{1}{2m}$ для всіх $y \in V'$. Візьмемо довільну точку $x_1 \in V' \cap F_m$. Тоді $f(x_0) - h(x_1) > \frac{1}{2m}$. Аналогічно, знаходимо точку $x_2 \in V \cap F_m$, таку що $h(x_1) - h(x_2) > \frac{1}{2m}$ і т. д. □

Доведення теореми про рекурентну множину. Нехай A — слабко однорідна рекурентна підмножина динамічної системи (X, f). Функцію $h : X \to \mathbb{R}$ визначимо формулою

$$h(x) = \inf_{n \geq 1} d(f^n(x), x).$$

Досить переконатися, що $f(x_0) = 0$ для деякої точки $x_0 \in A$ — ця точка і буде рекурентною. Перевіримо напівнеперервність зверху відображення h. Нехай $\delta > f(x)$, знайдемо натуральне число n_0, таке що $d(f^{n_0}(x), x) < \delta$ і виберемо окіл V точки x, такий що $d(f^{n_0}(y), y) < \delta$ для всіх $y \in V$. Значить, $h(y) < \delta$ для всіх $y \in V$. Нехай z — точка неперервності відображення h. Покажемо, що $h(z) = 0$. Припустимо, що $h(z) > 0$. Оскільки h неперервне в точці z, знайдуться $\delta > 0$ і відкритий окіл V точки z, такі що $h(x) > \delta$ для всіх $x \in V$. Із того, що G-орбіта кожної точки із A щільна в A випливає $A \subseteq \bigcup\limits_{g \in G} g(V)$. В силу компактності A знайдуться $g_1, \ldots, g_n \in G$, такі що $A \subseteq g_1(V) \cup \cdots \cup g_n(V)$.

Зафіксуємо довільний автоморфізм $g \in G$. Оскільки g рівномірно неперервне, існує $\epsilon > 0$, таке що із $d(y, y') < \epsilon$ випливає $d(g(y), g(y')) < \delta$. Оскільки $h(d(x)) = \inf\limits_{m \geq 1} d(g(f^n(x)), g(x))$, то з умови $h(x) < \epsilon$ випливає $h(g(x)) < \delta$.

Покладемо $g = g_i^{-1}$ і виберемо ϵ' як мінімум відповідних $\epsilon_i, i \in \{1, \ldots, n\}$. Тоді умова $h(x) < \epsilon'$ забезпечує $h(g_i^{-1}(x)) < \delta$

для всіх $i \in \{1, \dots, n\}$. За лемою 0.8.5 існує така точка $x_0 \in A$, що $f(x_0) < \epsilon'$. Оскільки $x_0 \in \bigcup\limits_{i=1}^{n} g_i(V)$, то $x_0 \in g_i(V)$ для деякого $i \in \{1, \dots, n\}$, тобто $x_0 = g_i(y), y \in V$. Оскільки $h(x_0) < \epsilon'$, то $h(g_i^{-1}(x_0)) < \delta$. Значить, $h(y) < \delta, y \in V$, що суперечить вибору околу V. $\square$

Нехай G — група гомеоморфізмів компактного метричного простору X. Непуста замкнена підмножина $F \subseteq X$ називається G-*інваріантною,* якщо $g(x) \in F$ для всіх $g \in G$, $x \in X$. Деякі елементарні факти:

- Замикання G-орбіти кожної точки з X є G-інваріантною підмножиною.
- Нехай $\mathcal{F}$ — довільна сім'я G-інваріантних підмножин. Тоді підмножина $\cap\mathcal{F}$ G-інваріантна за умови $\cap\mathcal{F} \neq \emptyset$.
- Якщо F — мінімальна G-інваріантна підмножина, то орбіта кожної точки з F щільна в F.
- Кожна G-інваріантна підмножина містить мінімальну G-інваріантну підмножину.

ДОВЕДЕННЯ ТЕОРЕМИ ФЮРСТЕНБЕРГА-ВЕЙСА. Ми застосуємо індукцію по числу m. Для $m = 1$ — це теорема Біркгофа. Нехай $G = \langle f_1, \dots, f_m \rangle$ — група, породжена гомеоморфізмами $f_1, \dots, f_m$. Не втрачаючи загальності, ми можемо вважати, що X — мінімальна G-інваріантна множина. На X^m визначимо метрику

$$\rho(x, y) = \max\{d(x_i, y_i) : i \in \{1, \dots, m\}\},$$

де $x = (x_1, \dots, x_m), y = (y_1, \dots, y_m)$. Групу G можна розглядати як групу гомеоморфізмів компактного метричного простору X^m з дією $g(x_1, \dots, x_m) = (g(x_1), \dots, g(x_m))$. Зауважимо, що діагональ Δ простору X^m є мінімальною G-інваріантною. Розгляньмо динамічну систему (X^m, f), де

$$f = (f_1, \dots, f_m), f(x_1, \dots, x_m) = (f_1(x_1), \dots, f_m(x_m)).$$

Очевидно, відображення f комутує з усіма елементами групи G, а тому Δ — слабко однорідна підмножина динамічної системи (X^m, f). Залишилося довести рекурентність Δ і застосувати теорему про рекурентну підмножину.

Позначимо $h_1 = f_1 f_m^{-1}, \dots, h_{m-1} = f_{m-1} f_m^{-1}$. За припущенням індукції існують точка $x \in X$ і зростаюча послідовність $(k_n)_{n\in\omega}$ натуральних чисел, такі що

$$h_1^{k_n}(x) \to x, \dots, h_{m-1}^{k_n}(x) \to x.$$

Зафіксуймо $\epsilon > 0$ і виберімо натуральне n, таке що

$$d(h_1^n(x), x) < \epsilon, \dots, d(h_{m-1}^n(x), x) < \epsilon.$$

Нехай $a = (x, \dots, x)$, $b = (f_m^{-n}(x), \dots, f_m^{-n}(x)), a, b \in \Delta$. Тоді $\rho(f^n(b), a) < \epsilon$, що і означає рекурентність Δ. □

Для застосування топологічної динаміки до комбінаторики зазвичай використовуються символічні системи. Нехай Λ — скінченна множина, $\Omega = \Lambda^{\mathbb{Z}}$ — декартів добуток $\mathbb{Z}$ копій множини Λ. Елементи множини Ω зручно записувати як нескінченні в обидва боки вектори

$$(\dots, x(-2), x(-1), x(0), x(1), x(2), \dots),$$

де $x(n) \in \Lambda$. Означмо на Ω метрику $d(x, x') = \frac{1}{k+1}$, де k — найбільше натуральне число, для якого

$$x(-k) = x'(-k), \dots, x(0) = x'(0), \dots, x(k) = x'(k).$$

Зауважмо, що збіжність в метриці d покоординатна і (Ω, d) — компактний простір. Крім того, $d(x, x') = 1$ тоді і лише тоді, коли $x(0) \neq x'(0)$. Означмо на Ω зсув f на одну координату вліво $f(x) = x'$, $x'(n) = x(n+1)$. Очевидно, f — гомеоморфізм простору Ω. Якщо X — інваріантний підпростір простору Ω динамічну систему (X, f) називають *символічною*.

Нехай $\mathbb{Z} = A_1 \cup \cdots \cup A_m$ — довільне розбиття, $\Lambda = \{1, \ldots, m\}$. Нехай x — характеристичний вектор цього розбиття, $x(k) = i$ тоді і лише тоді, коли $k \in A_i$. Покладемо $X = \overline{\mathrm{Orb}(x)} = \overline{\{f^n(x) : n \in \omega\}}$. Символічна система (X, f) називається породженою розбиттям $\mathbb{Z} = A_1 \cup \cdots \cup A_m$. На разі ми застосуємо теорему Фюрстенберга-Вейса для доведення теореми ван дер Вардена: для довільних натурального числа m і розбиття $\mathbb{Z} = A_1 \cup \cdots \cup A_k$ в одній з підмножин розбиття знайдеться арифметична прогресія довжини m. Нехай (X, f) — символічна система, породжена розбиттям $\mathbb{Z} = A_1 \cup \cdots \cup A_k$. До сім'ї $f, f^2, \ldots, f^m$ попарно комутуючих гомеоморфізмів простору X застосуємо теорему Фюрстенберга-Вейса. Нехай y — спільна рекурентна точка, $y(0) = l$, $U = \{z \in X : z(0) = l\}$. Виберемо натуральне число n так, що

$$f^n(y) \in U, f^{2n}(g) \in U, \ldots, f^{mn}(y) \in U.$$

Користуючись неперервністю відображення f, знайдемо окіл V точки y, такий що

$$f^n(V) \subseteq U, f^{2n}(V) \subseteq U, \ldots, f^{mn}(V) \subseteq U.$$

За означеннням символічної системи, $X = \overline{\mathrm{Orb}(x)}$, де x — точка з Ω, що відповідає розбиттю $\mathbb{Z} = A_1 \cup \cdots \cup A_k$. Оскільки $y \in X$ і V — окіл точки y, знайдеться натуральне число a, таке що $f^a(x) \in V$. Значить,

$$f^n(f^a(x)) \in U, f^{2n}(f^a(x)) \in U, \ldots, f^{mn}(f^a(x)) \in U.$$

Таким чином, $x(n + a) = x(2n + a) = \cdots = x(mn + a) = l$ і $a + n, a + 2n, \ldots, a + mn \in A_l$.

Слід зауважити, що і в свою чергу з теореми ван дер Вардена можна досить просто вивести теорему про спільну рекурентну точку, таким чином, ці комбінаторне та динамічне твердження по суті еквівалентні (див. [**5**], §10)

Одне з центральних понять топлогічної динаміки — *проксимальність:* дві точки $x, y \in X$ називають проксимальними, в динамічній системі (X, f), якщо знайдеться зростаюча послідовність $(k_n)_{n\in\omega}$ натуральних чисел, така що

$$d(f^{k_n}(x), f^{k_n}(y)) \to 0.$$

Теорема 0.8.7 (Ауслендера-Еліса). *Для будь-якої точки $x \in X$ існує рівномірно рекурентна точка $y \in X$, така що точки x, y проксимальні.*

Для доведення цієї теореми ми застосуємо дуже корисний інструмент — напівгрупу Еліса динамічної системи.

Множину X^X усіх відображень довільного топологічного простору X наділимо топологією поточкової збіжності. На X^X є природна структура напівгрупи: для довільних $f, g \in X^X$ їх добуток fg — це композиція $fg(x) = f(g(x))$. Відмітимо, що

- множення справа $f \mapsto fg$ на довільний елемент $g \in X^X$ неперервне;
- якщо g — неперервне відображення, то множення зліва $f \mapsto gf$на елемент g також неперервне.

Нехай S — деяка напівгрупа неперервних відображень довільного компактного простору X, пару (X, S) далі будемо називати *динамікою.* Напівгрупа S є підмножиною компаткної правотопологічної напівгрупи X^X. Позначмо через $E = E(X, S)$ замикання S в X^X і переконаємось, що E — піднапівгрупа X^X. Спочатку зафіксуємо довільний елемент $f \in S$. Оскільки множення зліва на f неперервне, то $fE = f\overline{S} \subseteq \overline{fS} \subseteq E$ і

$SE \subseteq E$. Зафіксуємо довільний елемент $g \in E$. Оскільки множення на g справа неперервне, то $Eg = \overline{S}g \subseteq \overline{SE} \subseteq \overline{E} = E$ і $EE \subseteq E$.

Напівгрупу $E = E(X, S)$ називають *напівгрупою Еліса* динаміки (X, S). Доведення слідуючих двох тверджень можна знайти в лекції "Комбінаторика ультрафільтрів".

- Нехай H — довільна компактна правотопологічна напівгрупа. Будь-який лівий ідеал L напівгрупи H містить мінімальний лівий ідеал. Кожен мінімальний лівий ідеал замкнений.

- Кожна компактна правотопологічна напівгрупа має ідемпотент, тобто такий елемент s, що $s^2 = s$.

Розглянемо пару (E, S) і визначимо дію напівгрупи S на компактному просторі $E = E(X, S)$ за правилом $f(g) = fg$. Оскільки $S \subseteq E$ і множення в E зліва на неперервне відображення f неперервне, то (E, S) — динаміка. Підмножина $I \subseteq S$ інваріантна в динаміці (E, S) тоді і тільки тоді, коли I — замкнений лівий ідеал напівгрупи E. А отже, підмножина $I \subseteq E$ мінімальна в динаміці (E, S) тоді і тільки тоді, коли I — мінімальний лівий ідеал.

Ми дещо узагальнили поняття проксимальності. Нехай X — компактний метричний простір, d — метрика на X. Точки $x, y \in X$ називаються проксимальними в динаміці (X, S), якщо для будь-якого $\epsilon > 0$ існує елемент $s \in S$, такий що $d(s(x), s(y)) < \epsilon$.

ЛЕМА 0.8.8. *Нехай X — компактний метричний простір, $x, y \in X$, S — напівгрупа неперервних відображень X. Тоді такі три умови рівносильні*

(i) *точки x, y проксимальні в динаміці (X, S);*

(ii) *існує елемент $p \in E, E = E(X, S)$, такий що $p(x) = p(y)$;*

(iii) *існує мінімальний лівий ідеал I напівгрупи E, такий що $p(x) = p(y)$ для будь-якого відображення $p \in I$.*

Доведення. (i) $\Rightarrow$ (ii). Виберемо таку послідовність відображень $(f_n)_{n\in\omega}$ з S, що $d(f_n(x), f_n(y)) \to 0$. Нехай p — точка дотику цієї послідовності в E. Для будь-якого $\epsilon > 0$ знайдеться відображення f_n, таке що

$$d(f_n(x), p(x)) < \frac{\epsilon}{3}, \quad d(f_n(y), p(y)) < \frac{\epsilon}{3}.$$

Можна вважати також, що $d(f_n(x), f_n(y)) < \frac{\epsilon}{3}$. Отже

$$d(p(x), p(y)) \leq d(p(x), f_n)) + d(f_n(x), f_n(y)) + d(f_n(y), p(y)) < \epsilon.$$

Оскільки ця нерівність справджується для довільного $\epsilon > 0$, маємо $p(x) = p(y)$.

(ii) $\Rightarrow$ (iii). Якщо $p(x) = p(y)$ для деякого відображення $p \in E$, то $fp(x) = fp(y)$ для всіх $f \in E$. В лівому ідеалі Ep виберемо мінімальний лівий ідеал I. Зрозуміло, що $q(x) = q(y)$ для всіх $q \in I$.

(iii) $\Rightarrow$ (ii). Очевидно.

(ii) $\Rightarrow$ (i). Нехай $p \in E$ і $p(x) = p(y)$. Оскільки $p \in E = \overline{S}$, то для довільного $\epsilon > 0$ знайдеться відображення $f \in S$, таке що

$$d(f(x), p(x)) < \frac{\epsilon}{2}, \quad d(f(y), p(y)) < \frac{\epsilon}{2}.$$

Отже, $d(f(x), f(y)) \leq d(f(x), p(x)) + d(p(x), p(y)) + d(f(y), (p(y)) < \epsilon$, що і означає проксимальність точок x, y. ☐

Лема 0.8.9. *Нехай X — компактний метричний простір, $x \in X$, S — напівгрупа неперервних відображень X, M — мінімальна підмножина динаміки (X, S), що міститься в $S(x)$. Тоді*

(*) *$M = I(x)$ для деякого мінімального лівого ідеалу I напівгрупи E;*

(**) *існує точка $y \in M$, така що точки x, y проксимальні.*

ДОВЕДЕННЯ. (*) Покладемо $F = \{p \in E : p(x) \in M\}$ і покажемо, що $F \neq \emptyset$. Візьмемо довільну точку $z \in M$. Оскільки $z \in \overline{S(x)}$, то знайдеться послідовність відображень $(f_n)_{n\in\omega}$ з S, така що $f_n(x) \to z$. Нехай p — точка дотику послідовності $(f_n)_{n\in\omega}$. Тоді $p(x) = z$. Далі переконаймося, що F — лівий ідеал. Якщо $p \in F$, $f \in E$, то $p(x) = z, z \in M, fp(x) = f(z)$. Виберемо послідовність відображень $(g_n)_{n\in\omega}$ з S, таку що $g_n \to f$. Тоді $g_n(z) \in M$ і в силу замкненості M $f(z) \in M$, тобто $fp \in F$. Нехай I — мінімальний лівий ідеал, що міститься в F. Тоді $I(x) \subseteq F(x) \subseteq M$. Оскільки підмножина $I(x)$ інваріантна, а M мінімальна, то $M = I(x)$.

(**) В замкненому ідеалі I візьмемо ідемпотент і покладемо $y = e(x)$. Оскільки $e(y) = e(e(x)) = e(x)$, за лемою 0.8.8 точки x, y проксимальні. □

ДОВЕДЕННЯ ТЕОРЕМИ АУСЛЕНДЕРА-ЕЛІСА. Нехай X — компактний метричний простір, $f : X \to X$ — неперервне відображення, $S = \{f^n : n \in \mathbb{N}\}$. Для довільної точки $x \in X$ за лемою 0.8.9 існує мінімальна підмножина M динамічної системи (X, f), така що точка x проксимальна з деякою точкою $y \in M$. При доведенні теореми Біркгофа ми показали, що кожна точка довільної мінімальної множини рівномірно рекурентна. □

На разі ми застосуємо теорему Ауслендера-Еліса до доведення теореми Хайндмена про FS-множину. Для довільної підмножини $A \subseteq \mathbb{N}$ позначмо через $FS(A)$ множину усіх скінченних сум різних елементів з A. Підмножину $B \subseteq \mathbb{N}$ називають *FS-множиною,* якщо знайдеться нескінченна підмножина $A \subseteq B$, така що $FS(A) \subseteq B$.

ТЕОРЕМА 0.8.10 (Хайндмена). *Для довільного розбиття $\mathbb{N} = A_1 \cup \cdots \cup A_k$ принаймні одна з підмножин розбиття є FS-множиною.*

Перш за все встановимо зв'язок між проксимальністю і FS-множинами.

Лема 0.8.11. *Нехай X — компактний метричний простір $f : X \to X$ — неперервне відображення, x, y — проксимальні точки динамічної ситеми (X, f), причому y — рівномірно рекурентна. Тоді для будь-якого $\epsilon > 0$ існує FS-множина $H \subseteq \mathbb{N}$, така що $d(f^n(x), y) < \epsilon$ для довільного $n \in H$.*

Доведення. Спочатку ми покажемо, що для будь-якого $\delta > 0$ знайдеться натуральне число p, таке що

$$d(f^p(x), y) < \delta, \quad d(f^p(y), y) < \delta.$$

Оскільки точка y рівномірно рекурентна, існує натуральне число m, таке що для будь-якого натурального n нерівність $d(f^{n+i}(y), y) < \frac{\delta}{2}$ виконується принаймні для одного $i \in \{0, \ldots, m\}$. Користуючись рівномірною неперервністю відображень $f, f^2, \ldots, f^m$, виберемо $\delta' > 0$ так, щоб для всіх $i \in \{0, \ldots, m\}$

$$d(y_1, y_2) < \delta' \Rightarrow d(f^i(y_1), f^i(y_2)) < \frac{\delta}{2}.$$

Оскільки x, y проксимальні, існує натуральне число n, таке що $d(f^n(x), f^n(y)) < \delta'$. Значить,

$$d(f^{n+i}(x), f^{n+i}(y)) < \frac{\delta}{2}, \quad i \in \{0, \ldots, m\}.$$

Виберемо $i \in \{0, \ldots, m\}$ так, щоб $d(f^{n+i}(y), y) < \frac{\delta}{2}$. Тоді

$$d(f^{n+i}(x), y) \leq d(f^{n+i}(x), f^{n+i}(y)) + d(f^{n+i}(y), y) < \delta.$$

Припустимо, що ми вже знайшли натуральні числа $p_1, \ldots, p_n$, такі що для кожного $p \in FS\{p_1, \ldots, p_n\}$ виконуються нерівності

$$d(f^p(x), y) < \epsilon, d(f^p(y), y) < \epsilon.$$

Користуючись неперервністю відображення f^p в точці y, виберемо $\delta > 0$ так, щоб із умови $d(z, y) < \delta$ випливала нерівність

$d(f^p(z), y) < \epsilon$ для всіх $p \in FS\{p_1, \dots, p_n\}$. Визначимо p_{n+1} так, щоб

$$d(f^{p_{n+1}}(x), y) < \delta, \quad d(f^{p_{n+1}}(y), y) < \delta.$$

Тоді $d(f^{p+p_{n+1}}(x), y) < \epsilon$, $d(f^{p+p_{n+1}}(y), y) < \epsilon$. $\square$

Доведення теореми Хайндмена. Розглянемо символічну систему (X, f) породжену розбиттям $\mathbb{Z} = (-A_k) \cup \dots \cup (-A_1) \cup \{0\} \cup A_1 \cup \dots \cup A_k$. З означенням, $X = \overline{\mathrm{Orb}(x)}$, де x — характеристичний вектор розбиття. За теоремою Аусендера-Еліса існує рівномірно рекурентна точка $y \in X$, така що x, y проксимальні. За лемою 0.8.11 $d(f^n(x), y) < 1$ для всіх натуральних чисел n із деякої FS-підмножини $H \subseteq \mathbb{N}$. Тоді $x(n) = y(0)$ для всіх $n \in H$. Це значить, що $H \subseteq A_l$, де $l = y(0)$. $\square$

Про загальну теорію динамічних ситем можна прочитати в [**1**], [**4**], [**6**], [**7**]. Зв'язок між топологічною динамікою і комбінаторикою встановив Фюрстенберг [**2**], [**3**].

Бібліоґрафія

[1] Ellis R. Lectures on topological dynamics, NY, Benjamin, 1969.
[2] Furstenberg H. Reccurence in ergodic theory and combinatorial number theory, Princetone Univ. Press, Princeton, 1981.
[3] Furstenberg H. Poincare recurrence and number theory, Bull. AMS, 5 (1981), 211-233.
[4] Cottshalk W., Hedlung G. Topologycal dynamics, AMS Coll. Publ, 36, 1955.
[5] Protasov I. Combinatorics of Numbers, Mat. Stud. Monogr. Ser., 2, VNTL, Lviv, 1997.
[6] Veech W. Topologycal dynamics, Bull. AMS, 83 (1977), 775-830.
[7] Vries J. Elements of topological dynamics, Math. and its Applications, 257, Kluwer Acad. Publ., 1993.

0.9. Комбінаторика і комбінаторна топологія

План такий. Ми розпочнемо з леми Шпернера — суто комбінаторного твердження, що лежить в основі загально-прийнятого доведення теореми Брауера про нерухому точку — одного з наріжних каменів топології. Далі ми розглянемо теорему Борсука-Улама про антиподи — сферичний аналог теореми Брауера і наведемо кілька комбінаторних застосувань цієї теореми. Ця проста схема має показати плідні взаємозв'язки між комбінаторикою і топологією.

Нехай $v_0, v_1, \ldots, v_k$ — точки з $\mathbb{R}^n$ у загальному положенні, тобто система векторів $v_1 - v_0, \ldots, v_k - v_0$ лінійно незалежна.

Опуклу оболонку $\{\lambda_0 v_0 + \cdots + \lambda_k v_k : 0 \leq \lambda_i \leq 1, \sum\limits_{i=0}^{k} \lambda_i = 1\}$ називають *k-симплексом.* Таким чином 0-симплекс це точка, 1-симплекс — відрізок, 2-симплекс це трикутник і т. д. Опукла оболонка будь-якої непорожньої скінченної підмножини з $\{v_0, \ldots, v_k\}$ називається *гранню* симплекса з відповідними вершинами.

Нехай T — k-симплекс в $\mathbb{R}^n$. Скінченний набір $\tau = \{T_1, \ldots, T_m\}$ k-симплексів в $\mathbb{R}^n$ називають триангуляцією T, якщо $\cup\tau = T$ і будь-які два симплекси T_i, T_j або не перетинаються, або перетинаються по спільній грані. Вершини кожного з симплексів $T_1, \ldots, T_m$ називають вершинами триангуляції. Ми назвемо розфарбування χ множини вершин V триангуляції τ кольорами $\{0, 1, \ldots, k\}$ правильним, якщо $\chi(v) = 0, \ldots, \chi(v_k) = k$ і для кожної грані колір довільної точки з цієї грані співпадає з кольором однієї з її вершин. Симплекс $T_i \in \tau$ назвемо *розмаїтим,* якщо серед його вершин немає двох однокольорових.

Лема 0.9.1 (Шпернера). *Нехай T — k-симплекс в $\mathbb{R}^n$, τ — триангуляція T. Для довільного правильного розфарбування χ множини вершин триангуляції τ число розмаїтих симплексів триангуляції непарне, зокрема, існує хоча б один розмаїтий симплекс.*

Доведення. Для $k = 0$ лема очевидна. Для $k = 1$ вершину v триангуляції τ назвемо відміченою, якщо $\chi(v) = 0$. Відрізок $t \in \tau$ назвемо однократним, якщо рівно одна його вершина відмічена, і двократним, якщо відмічені обидві вершини. Позначимо через α та β кількість однократних і двократних відізків і покажемо, що число $\alpha + 2\beta$ непарне (а, значить, число α розмаїтих відрізків непарне).

Розглянемо множину усіх пар (v, t), де v-вершина триангуляції, t — відрізок триангуляції. Пару назвемо відміченою, якщо вершина v відмічена і є кінцем відрізку t. Число відмічених пар можна порахувати двома способами. Оскільки кожен однократний відрізок входить лише в одну відмічену пару, а кожен двократний — в дві, це число $\alpha + 2\beta$. З іншого боку кожна відмічена вершина, що лежить всередині T входить рівно в дві пари, а вершина v_0 — в одну, це число дорівнює $2\gamma - 1$, де γ — число відмічених вершин.

Для $k = 2$ елементами триангуляції є трикутники, їх сторони назвемо відрізками триангуляції. Відрізок з кінцями u, v назвемо відміченим, якщо $\chi\{u, v\} = \{0, 1\}$. Трикутник триангуляції назвемо відміченим, якщо відмічена лише одна його сторона (тобто він розмаїтий), і двократним, якщо він має дві відмічені сторони. Нехай α — число однократних, а β — число двократних трикутників. Досить показати, що число $\alpha + 2\beta$ непарне.

Розгянемо множину пар (s, t), де s — відрізок триангуляції, t — трикутник триангуляції. Праву (s, t) назвемо відміченою, якщо s відмічений і є стороною трикутника t. Кожен однократний трикутник входить рівно в одну відмічену пару, а кожен двократний в дві. Отже, число відмічених пар $\alpha + 2\beta$. З іншого боку, відмічені відрізки не можуть лежати на сторонах $[v_1, v_2]$, $[v_0, v_2]$ трикутника T. Якщо відмічений відрізок лежить на стороні $[v_0, v_1]$, він входить в одну відмічену пару, якщо ж ні, то в дві. А тому число відмічених пар $\gamma + 2\delta$, де γ — число вімічених відрізків на стороні $[v_0, v_1]$, а δ — число відмічених відрізків всередині T. За лемою Шперенера при $k = 1$ число γ непарне.

Цих викладок достатньо, щоб довести інукцією лему для всіх розмірностей. □

ТЕОРЕМА 0.9.2 (Брауера). *Нехай k — довільне натуральне число, T — k-симплекс, $f : T \to T$ — неперервне відображення. Тоді існує точка $x_0 \in T$, така що $f(x_0) = x_0$.*

Доведення. Ми будемо вважати, що $T \subset \mathbb{R}^k$. Нехай $\{v_0, \ldots, v_k\}$ — множина вершин симплексу T. Для кожного $i \in \{0, 1, \ldots, k\}$ позначимо через T_i симплекс з вершинами $v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k$. Візьмемо довільну точку $x \in T$ і проведемо гіперплощину $\Gamma_i(x)$ через точку і паралельно симплексу T_i. Гіперплощина $\Gamma_i(x)$ визначає два замкнені напівпростори. Позначимо через $P_i(x)$ той з них, в якому міститься симплекс T_i. Очевидно, що $T \subset \bigcup\limits_{i=0}^{k} P_i(x)$, $\bigcap\limits_{i=0}^{k} P_i(x) = \{x\}$. Визначимо розфарбування $\chi : T \to \{0, 1, \ldots, k\}$ за таким правилом. Покладемо $\chi(v_0) = 0, \ldots, \chi(v_k) = k$. Для довільної точки $x \in T$ виберемо один з напівпросторів, $P_i(x)$ в якому лежить точка $f(x)$ і покладемо $\chi(x) = i$. Попіклуймося лише про те, щоб точки на гранях симплексу отримали колір одої з вершин грані.

Далі для кожного натурального числа n визначимо триангуляцію τ_n симплексу T, таку щоб відстань між будь-якими двома вершинами кожного з симплексів триангуляції на перевищувала $\frac{1}{n}$. За лемою Шпернера існує розмаїтий відносно розфарбування χ симплекс Δ_n триангуляції τ_n. В силу компактності T послідовність симплексів Δ_n має граничну точку x_0. В силу неперервності f маємо $f(x_0) \in P_i(x_0)$ для всіх $i \in \{0, \ldots, k\}$. Оскільки $\bigcap\limits_{i=0}^{k} P_i(x_0) = x_0$, $f(x_0) = x_0$. □

Кажуть, що топологічний простір X є *fp-простором* (або простором з властивістю нерухомої точки), якщо кожне неперервне відображення $f : X \to X$ має нерухому точку. Якщо X — fp-простір, то і кожен гомеомофний до X простір Y теж є fp-простором. Дійсно, нехай $g : X \to Y$ — гомеоморфізм, $h : Y \to Y$ — неперервне відображення. Позначмо $f = g^{-1}hg$ і зауважимо, що $f : X \to X$ — неперервне відображення. Нехай $x_0 \in X$ і $f(x_0) = x_0$. Тоді $f(x_0) = g^{-1}hg(x_0) = x_0$,

$h(g(x_0)) = g(x_0)$ і $g(x_0)$ — нерухома точка відображення h. Отже, будь-який топологічний простір гомеоморфний симплексу (наприклад, куб чи куля в $\mathbb{R}^n$) є fp-простором.

Властивість нерухомої точки тісно пов'язана з поняттям ретракту. Нехай X — топологічний простір. Кажуть, що підпростір Y є *ретрактом* X, якщо існує неперервне відображення $f : X \to Y$, що залишає нерухомою кожну точку з Y, тобто тотожнє на Y. Саме відображення f при цьому називають ретракцією X на Y. Припустімо, що X — fp-простір, і покажемо, що його ретракт Y теж є fp-простором. Нехай $h : Y \to Y$ — довільне неперервне відображення. Тоді відображення $hf : X \to X$ має нерухому точку $x_0 \in X$. Оскільки $hf(x_0) = x_0 = f(x_0)$, то $f(x_0)$ — нерухома точка відображення h. Це спостереження разом з теоремою Брауера показує, що кожен ретракт симплексу є fp-простором. З іншого боку, нехай D_n та S^{n-1} куля та сфера в просторі $\mathbb{R}^n$ з евклідовою метрикою $d(x, y)$

$$D_n = \{x \in \mathbb{R}^n : d(x, 0) \leq 1\}, \quad S^{n-1} = \{x \in \mathbb{R}^n : d(x, 0) = 1\}.$$

Очевидно, що S^{n-1} на має властивості нерухомої точки — досить поглянути на антиподальне відображення $f : S^{n-1} \to S^{n-1}$, $f(x) = -x$. Оскільки D_n є fp-простором то одержуємо таке твердження: S^{n-1} не є ретрактом D_n.

ТЕОРЕМА 0.9.3 (Борсука-Улама). *Для довільного натурального числа n і довільного неперервного відображення $f : S^n \to \mathbb{R}^n$ знайдеться точка $x \in S^n$, така що $f(x) = f(-x)$.*

ДОВЕДЕННЯ. Ми доведемо теорему лише для $n = 1$. Отже, нехай $f : S^1 \to \mathbb{R}$ довільне неперервне відображення одиничного кола S^1 з центром у початок координат площини $\mathbb{R}^2$. Нехай I — діаметр кола, що лежить на осі абсцис. Визначимо відображення $h : I \to \mathbb{R}$ за таким правилом. Для кожної точки $y \in I$ проведемо перпендикуляр в точці y до I у верхню півплощину і позначимо через x точку перетину цього перпендикуляра з колом, а для точки $-y$ проведемо перпендикуляр у нижню півплощину і позначимо через $-x$ точку перетину з колом. Покладемо $h(y) = f(x) - f(-x)$. На кінцях відрізку I неперервна функція $h(y)$ приймає протилежні значення. А тому знайдеться точка y^*, така що $h(y^*) = 0$. Оскільки $h(y^*) = f(x^*) - f(-x^*)$, то $f(X^*) = -f(-x^*)$. □

Щойно (в кулуарах конференції з геометричної топології, Львів, травень 2004) і до речі (до теореми про середнє значення) Михайло Зарічний запропонував колегам таку задачу: доведіть, що на гладкій галявині завжди можна розташувати квадратний стіл так, щоб всі чотири його ніжки стояли на поверхні (звичайно, ніжки — це відрізки). Доведіть і ви це твердження.

Ми застосуємо теорему про антиподи до доведення двох теорем про млинці. Перша з них така.

ТЕОРЕМА 0.9.4. *Якщо A, B — дві обмежені фігури на площині, вимірні за Лебегом, то існує пряма, що ділить кожну з цих фігур на дві частини однакової міри.*

ДОВЕДЕННЯ. Помістимо обидві фігури всередину деякого кола C. Для кожної точки x кола позначмо через D_x діаметр кола з кінцем в x. Нехай L_t — перпендикуляр до D_x, що проходить через точку на D_x, відстань від якої до x дорівнює t, $t \in [0, d]$, d — діаметри кола C. Нехай $\mu_1(t)$ — міра тої частини фігури A, що лежить з того ж боку до L_t, що і x, а $\mu_2(t)$ — міра другої частини фігури A. Функції $\mu_1(t), \mu_2(t)$ задані на відрізку $[0, d]$ і неперервні, а тому неперервна і функція $f(t) = \mu_1(t) - \mu_2(t)$.

Оскільки $f(0) = -f(d)$, на відрізку $[0, d]$ знайдеться точка t' така що $f(t') = 0$, тобто $\mu_1(t') = \mu_2(t')$. Таким чином $L_{t'}$ ділить A навпіл (за мірою). Ця ж пряма ділить B на якісь дві частини. Позначимо через $\nu(x)$ міру тої частини, що лежить ближче до x, а через $\nu_2(x)$ — міру другої частини. Функція $g(x) = \nu_1(x) - \nu_2(x)$ задана на колі і неперервна. Якщо точка x, рухаючись по колу переміститься у свій антипод x^*, вказані частини поміняються місцями, а тому $g(x) = -g(x^*)$ для всіх $x \in C$. За теоремою Борсука-Улама знайдеться точка $x \in G$, така що $g(x) = g(x^*)$. Це означає, що $g(x) = 0$ і пряма L_t, що відповідає діаметру $[x, x^*]$ ділить навпіл обидві фігури A, B. □

Друга теорема про млинці формулюється так.

ТЕОРЕМА 0.9.5. *Для кожної вимірної фігури A на площині існують дві взаємно перепендикульрні прямі, що ділять A на чотири фірури однакової міри.*

ДОВЕДЕННЯ. Помістимо фігуру A всередину деякого кола C і для кожної точки $x \in C$ позначимо через D_x діаметр кола з кінцем x, а через x^* — другий кінець цього діаметру. Нехай L_x — пряма, що перепендикулярна до D_x і ділить фігуру A на дві частини однакової міри, а M_x — пряма, що паралельна D_x і ділить фігуру A на дві частини однакової міри.

Прямі L_x, M_x ділять фігуру на чотири частини $A_1(x), A_2(x), A_3(x), A_4(x)$. Нехай $\mu_1(x), \mu_2(x), \mu_3(x), \mu_4(x)$ — міри цих частин. Очевидно, що

$$\mu_1(x) + \mu_2(x) = \mu_3(x) + \mu_4(x),$$

$$\mu_4(x) + \mu_1(x) = \mu_2(x) + \mu_3(x).$$

З цих рівностей випливає, $\mu_1(x) = \mu_3(x)$, $\mu_2(x) = \mu_4(x)$. Нехай тепер точка x, неперервно рухаючись по колу, пройде чверть кола і зупиниться в точці y. Тоді $A_1(x)$ перейде в $A_2(x)$, $A_2(x)$ в $A_3(x)$, $A_3(x)$ в $A_4(x)$, $A_4(x)$ в $A_1(x)$. Отже, $\mu_1(y) = \mu_2(x)$, $\mu_2(y) = \mu_3(x)$. Покладемо $f(x) = \mu_1(x) - \mu_2(x)$. Тоді $f(y) =$

$\mu_1(y)-\mu_2(y) = \mu_2(x)-\mu_3(x) = \mu_2(x)-\mu_1(x) = -f(x)$. Значить, на кінцях x, y дуги функція f приймає протилежні значення. Виберемо точку x^* на дузі, таку що $f(x^*) = 0$. Тоді прямі L_{x^*}, M_{x^*} і дають потрібне розбиття фігури A. □

Щойно ми розглянули застосування теореми про антиподи до задач з комбінаторної геометрії. Дещо делікатніше теорема про антиподи працює в суто дискретній ситуації. Далі ми наведемо приклад такого застосування, а розпочнемо з простої задачі.

Задача 0.9.1. Множину $\mathbb{Z}^2$ цілочисельних точок площини пофарбовано двома кольорами, жовтим та синім. Довести, що знайдеться однокольорова нескінченна підмножина точок, симетрична відносно деякої точки площини.

Розв'язок. Припустимо супротивне. Тоді наше розфарбування має таку властивість: для кожної точки $c_0 \in \mathbb{Z}^2$ (що буде центром симетрії) існує додатнє число r, що будь-які дві симетричні відносно c_0 точки, що лежать за межами круга радіуса r навколо c_0, розфарбовані різними кольорами. Припускаючи, що це не так, ми б для кожного натурального n знайшли точки a_n, b_n за межами круга радіуса n навколо c_0, симетричні відносно c_0, і розфарбовані одним кольором. Тоді множина $\{a_n, b_n : n \in \mathbb{N}\}$ містила б нескінченну підмножину симетричну відносно c_0, що суперечить нашому припущенню.

Зафіксуємо дві точки $c_0 = (0,0)$ і $c_1 = (1,0)$ і знайдемо додатні числа r_0, r_1, такі що для $i \in \{0,1\}$ за межами круга радіуса r_i навколо c_i не існує симетричних відносно c_i однокольорових точок. Зауважимо, що для точки (x,y) симетрична їй точка відоносно c_0 має координати $(-x,-y)$, а відносно c_1 — координати $(-x+2,y)$. Виберемо натуральне число $n > \max\{r_1, r_2\}$. Для визначеності припустимо, що точка $(0,n)$ жовта. Тоді точки $(0,-n), (2,-n)$ симетричні їй відносно c_0, c_1 повинні бути синіми, оскільки вони лежать за межами кругів з радіусами r_0, r_1 навколо c_0, c_1. Аналогічно, точки $(-2, n), (0, n), (2, n)$ симетричні точкам $(0, -n), (2-n)$ відносно центрів c_0, c_1, повинні бути жовтими. Продовжуючи далі, одержимо, що точки вигляду $(2k, n), k \in \mathbb{Z}$ жовті, а точки $(2k, -n), k \in \mathbb{Z}$ сині. Тоді $\{(2k, n) : k \in \mathbb{Z}\}$ нескінченна жовта множина, симетрична відносно точки $(0, n)$. Тобто ми, всупереч нашому припущенню, знайшли потрібну множину. □

Просторовий варіант цієї задачі формулюється так.

Задача 0.9.2. Множину $\mathbb{Z}^3$ цілочисельних точок простору пофарбовано трьома кольорами. Довести, що знайдеться нескінченна однокольорова множина, симетрична відносно деякої точки простору $\mathbb{R}^3$.

Неважко зрозуміти, що прийом віддзеркалення у цьому випадку не спрацьовує. Ми наведемо доведення, запропоноване Т. Банахом [**5**], з використанням теореми про антиподи.

Для доведення припустимо супротивне і зафіксуємо розфарбування $\mathbb{Z}^3$ трьома кольорами без однокольорових нескінченних підмножин. Нехай $C = \{-1, 0, 1\}^3$, $K = [-m, m]^3$ – куб в $\mathbb{R}^3$. З нашого припущення випливає, що для досить великих m границя ∂K куба K не містить двох однокольорових точок з $\mathbb{Z}^3$, симетричних відносно центрів з множини C. Зафіксуємо такий куб K для деякого парного натурального числа m. Розіб'ємо ∂K на конгруентні прямокутні трикутники з вершинами в точках з парними координатами (катет кожного прямокутника має довжину 2). Таку триангуляцію можна вибрати симетричною відносно початку координат.

Зафіксуємо довільний трикутник T на площині $\mathbb{R}^2$ і розфарбуємо три його вершини трьома різними кольорами. Визначимо відображення $h : \partial K \to T$ так , щоб

(*) кожна вершина триангуляції відображалась у вершину трикутника T того ж кольору;

(**) відображення h лінійне на кожному елементі Δ триангуляції.

Зрозуміло, що відображення h визначається умовами (*) та (**) однозначно і є неперервним. За теоремою Борсука-Улама про антиподи існує пара точок $\{x, -x\}$ на ∂K, для яких $h(x) = h(-x)$. Нехай $a, b, c \in \partial K$ вершини трикутника триангуляції, в якому лежить точка x. Трикутник з вершинами $-a, -b, -c$ містить точку $-x$. За лінійністю h точки $h(x), h(-x)$ лежать в опуклих оболонках множин $\{h(a), h(b), h(c)\}, \{h(-a), h(-b), h(-c)\}$, а тому ці опуклі оболонки перетинаються.

З іншого боку, кожна з точок $\{a, b, c\}$ симетрична до кожної з точок $\{-a, -b, -c\}$ відносно деякої точки з C. За нашим припущенням кольори точок $\{a, b, c\}$ та $\{-a, -b, -c\}$ не перетинаються, а тому $\{h(a), h(b), h(c)\}$ та $\{h(-a), h(-b), h(-c)\}$ не перетинаються. Значить, опуклі оболонки цих множин (а це вершини трикутника T) теж не перетинаються, суперечність.

Неважко переконатися, що за цією схемою можна довести таке загальне твердження: для довільного натурального числа n і довільного розфарбування множини $\mathbb{Z}^n$ n кольорами знайдеться нескінченна однокольорова підмножина, симетрична відносно деякої точки з $\mathbb{Z}^n$. З іншого боку, $\mathbb{Z}^n$ легко пофарбувати $n+1$ кольором так, щоб кожна однокольорова підмножина, симетрична відносно деякої точки з $\mathbb{Z}^n$, була скінченною (як це зробити?).

Ця задача про розфарбування $\mathbb{Z}^n$ привела до появи нового кардинального інваріанту $\nu(G)$ абелевої (а згодом і довільної) групи G. Нехай G — абелева група. Точки $x, y \in G$, за означенням, симетричні відносно точки $a \in G$, якщо $x + y = 2a$.

Через $\nu(G)$ позначимо найменший кардинал k, такий що G допускає k-розфарбування без однокольорової нескінченної підмножини, симетричної відносно деякої точки з G. Таким чином, $\nu(\mathbb{Z}^n) = n$. Для довільної абелевої групи G кардинал $\nu(G)$ пораховано в [**6**]:

$$\nu(G) = \begin{cases} r_0(G) + 1, & \text{якщо } G \text{ скінченно породжена;} \\ r_0(G) + 2, & \text{якщо } G \text{ зліченна, нескінченно породжена і } |B(G)| < \aleph_0; \\ \max\{|B(G), \log|G|\}, & \text{якщо } G \text{ незліченна або } B(G) \geq \aleph_0, \end{cases}$$

де $r_0(G)$ — вільний ранг групи G, $B(G) = \{g \in G : 2g = 0\}$.

Про симетрію розфарбувань можна прочитати в огляді [**2**].

Ми закінчимо одним простим, але дуже корисним як для комбінаторики, та і для топології, твердженням про розфарбування множини, пов'язані з відображеннями.

Теорема 0.9.6 (де-Брейна-Ердьоша). *Нехай X — довільна множина, $f : X \to X$. Тоді існує таке розбиття множини $X = X_0 \cup X_1 \cup X_2 \cup X_3$, що X_0 — це множина усіх нерухомих точок відображення f і $f(X_i) \cap X_i = \emptyset$ для всіх $i \in \{1, 2, 3\}$.*

Доведення. Ми розглянемо дещо спрощений випадок: $X_0 = \emptyset$. Побудуємо граф Γ відображення f. Множиною вершин Γ є множина X, а множину орієнтованих ребер складають усі пари $(x, f(x)), x \in X$. Задача зводиться до розфарбування множини вершин трьома кольорами, для якого будь-які дві суміжні вершини були б різнокольоровими. З кожної вершини графу Γ виходить рівно одне орієнтовне ребро. На мить забудемо про орієнтацію і помітимо, що кожна зв'язна компонента графу містить не більше одного циклу. Якщо циклів взагалі немає, то граф є деревом і вистачить двох кольорів. Якщо є цикл C, то спочатку пофарбуємо вершини C так щоб не було однокольорових суміжних вершин. Для цього вистачить трьох кольорів. Після видалення ребер циклу C граф розпадається на дерева з коренями в вершинах C, а тому ми легко можемо продовжити розфарубування на X. $\square$

Наведемо один з можливих топологічних варіантів теореми де-Брейна-Єрдьоша.

ТЕОРЕМА 0.9.7. *Нехай* X *— компактний метричний простір,* n *— натуральне число,* $\dim X \leq n$*, де* $\dim X$ *— лебегова розмірність* X*. Нехай* $f : X \to X$ *— довільне неперервне відображення без нерухомих точок. Тоді знайдуться замкнені підмножини* $C_1, \ldots, C_{n+3}$*, такі що* $C_1 \cup \cdots \cup C_{n+3} = X$ *і* $f(C_i) \cap C_i = \emptyset$ *для всіх* $i \in \{1, \ldots, n+3\}$.

Джерелом подібних теорем в топології є теорема Люстерника-Шнірельмана про антиподи.

ТЕОРЕМА 0.9.8. *Нехай сферу* S^n *покрито* $(n+1)$*-ою замкненою множиною,* $S^n = C_1 \cup \cdots \cup C_{n+1}$*. Тоді хоча б одна з підмножин* C_i *містить пару точок-антиподів.*

Популярно про комбінаторну топологію написано в [**7**],[**9**], а для більш серйозного ознайомлення ми рекомендуємо [**3**],[**4**],[**8**].

Бібліоґрафія

[1] Aarts J., Fokkink R., Vermeer H. Variations of theorem of Lusternik and Schnirelmann, Topology, 35 (1996), 1051-1056.

[2] Banakh T., Protasov I. Symmetry and colorings: some results and open problems. Изв. Гмельского ун-та, 17 (2001)б 4-15.

[3] Engelking R. Dimention theory, PWN, Warszawa, 1978.

[4] Александров П. С., Пасынков Б. А. Введние в теорию размерности, М., "Наука 1973.

[5] Банах Т. Розв'язки деяких проблем І. В. Протасова з комбінаторики розфарбувань, У світі математики, 3 (1997), №1б 8-11.

[6] Банах Т. О., Протасов И. В. Асимметричные разбиения абелевых групп, Мат. заметки, 66 (1999), №1, 17-30.

[7] Пасынков Б. А., Федрчук В. В. Топология и теория размерности, "Знание математика-кибернетика, 1984, №9.

[8] Понтрягин Л. С. Основы комбинаторной топологии, М., "Наука 1976.

[9] Шашкин Ю. А. Неподвижные точки. Популярные лекции по математике, М., "Наука 1989.

0.10. Комбінаторні задачі в теорії міри

Як тільки Лебег увів поняття вимірної підмножини в $\mathbb{R}^n$, одразу ж виникли питання про існування невимірних підмножин. Перший приклад невимірної підмножини 1905 року побудував Віталі. Ось його конструкція.

Для точок відрізку $[0,1]$ означимо еквівалентність $x \sim y \Leftrightarrow x-y$ — раціональне число. Відношення $\sim$ розбиває відрізок на класи еквівалетності, кожен з яких зліченний. Аксіома вибору дозволяє побудувати підмножину $M \subset [0,1]$, що має рівно одну точку в кожному класі еквівалентності. Припустімо, що M вимірна за Лебегом. Якщо $\mu(M) = 0$, то $\mu(M + r) = 0$ для будь-якого $r \in \mathbb{R}$, а тому, в силу зліченної адитивності μ, множина $X = \cup\{M + r : r \in \mathbb{Q}, r \in [-1,1]\}$ теж нульової міри, що суперечить $[0,1] \subset X$. Якщо $\mu(M) > 0$, то множина X мала б бути нескінченної міри, оскільки $M + r_1 \cap M + r_2 = \emptyset$ при $r_1 \neq r$, що суперечить $X \subseteq [-1,2]$.

Варіації на тему прикладу Віталі продовжуються і до наших днів. Наприклад, в [**2**] для будь-якого ϵ, $0 < \epsilon \leq 1$ побудовано підмножину $V_\epsilon \subset [0,1]$, зовнішня міра Лебега якої дорівнює ϵ, а внутрішня — 0.

Найістотнішим моментом в конструкції Віталі, звичайно, є застосування аксіоми вибору. 1938 року Серпінський побудував невимірну за Лебегом підмножину відрізка, використовуючи вільний ультрафільтр на зліченній множині. Проте 1970 року Соловей вказав модель системи аксіом Цермело-Френкеля теорії множин, в якій кожна підмножина прямої вимірна за Лебегом. Звичайно, для побудови такої моделі Соловей відмовився від аксіоми вибору, ми ж протягом лекції приймемо аксіому вибору як божественний принцип, що не підлягає обговоренню. Про життя в іншому світі можна популярно прочитати в [**4**].

Дві істотні властивості міри Лебега, використані для побудови прикладу Віталі: інваріантність відносно зсувів $\mu(A) = \mu(A + a)$ і зліченна адитивність. С. Банах запропонував відмовитись від інваріантності і спробувати побудувати зліченно адитивну міру M визначену на всіх підмножинах відрізку, таку що $M([0,1]) = 1$. В припущенні континуум гіпотези CH ($\aleph_1 = 2^{\aleph_0}$) цього зробити неможливо, як стверджує така теорема.

ТЕОРЕМА 0.10.1 (Улама). *Нехай X — множина потужності $\aleph_1$, μ — скінченно адитивна міра, визначена на всіх підмножинах множини X, $\mu(X) < \infty$. Якщо $\mu(\{x\}) = 0$ для всіх $x \in X$, то $\mu(X) = 0$.*

ДОВЕДЕННЯ. Аксіома вибору еквівалентна принципу трансфінітності, за яким кожну множину можна цілком упорядкувати. Нехай $<$ — таке упорядкування X, причому кожен початковий відрізок $\{x : x < y\}, y \in X$ скінченний або зліченний. Позначимо через Y множину тих елеметнів з X, для яких відрізок $\{x : x < y\}$ зліченний. Нехай f_y — деяка бієкція цього відрізку на $\mathbb{N}$. Якщо $x < x' < y'$, то $f_y(x) \neq f_y(x')$. Для кожного $x \in X$ і кожного натурального числа n позначмо

$$F_x^n = \{y \in Y : x < y, f_y(x) = n\}$$

і розташуємо ці множини в таблицю

$$\begin{array}{ccccc}
F_{x_0}^1 & F_{x_1}^1 & \ldots & F_x^1 & \ldots \\
F_{x_0}^2 & F_{x_1}^2 & \ldots & F_x^2 & \ldots \\
\multicolumn{5}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\
F_{x_0}^n & F_{x_1}^n & \ldots & F_x^n & \ldots \\
\multicolumn{5}{c}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots}
\end{array}$$

Ця таблиця містить $\aleph_0$ рядків і χ_1 стовпчиків і має такі властивості

(*) множини кожного рядка попарно не перетинаються;

(**) об'єднання множин кожного стовпчику дорівнює множині X без деякої зліченної множини.

Для перевірки (*) припустимо, що $y \in F_x^n \cap F_{x'}^n$. Тоді $x < y, x' < y'$ і $f_y(x) = f_y(x')$. З ін'єктивності f маємо $x = x'$. Для перевірки (**) зауважимо: якщо $x < y$, то і $f_y(x) = n$, то $y \in F_x^n$. Отже, об'єднання $\bigcup_{n=1}^{\infty} F_x^n$ відрізняється від X на множину $\{y : y \leq x\} \cup (X \setminus Y)$.

З (*) випливає, що кожен рядок може мати не більше, ніж зліченне число підмножин, для яких $\mu(F_x^n) > 0$. Дійсно, якщо це не так, то ми знайдемо натуральне число m і нескінченну підмножину $Z \subseteq X$, для яких $\mu(F_x^n) > \frac{1}{m}$ для всіх $x \in Z$, що суперечить (в силу адитивності) умові $\mu(X) < \infty$. Оскільки множина стовпчиків незліченна, ми можемо вибрати $x \in X$ так, що $\mu(F_x^n) = 0$ для всіх n. Із зліченної адитивності μ випливає, що об'єднання підмножин відповідного стовпчику має міру 0. З (**) і умови $\mu(\{x\}) = 0$, $x \in X$ випливає, що $\mu(X) = 0$. □

Якщо послабити вимогу зліченної адитивності до скінченної адитивності, але зберегти умову інваріантності міри відносно зсувів, то такі міри, що визначені на всіх підмножинах з $\mathbb{R}^n$ і приймають значення 1 на одиничному кубі, існують для будь-якого n. Ми доведемо це (і навіть значно загальніше) твердження наприкінці нарису.

Міра Лебега в $\mathbb{R}^n$ інваріантна не тільки відносно трансляції, а і відносно довільних ізометрій — відображень, що зберігають відстань між точками. Для $n = 1, 2$ Хаусдорф побудував міру, визначену на всіх підмножинах в $\mathbb{R}^n$ скінченно-адитивну і інваріантну відносно довільних ізометрій. Спроба побудувати подібну міру привела до так званого "пардоксу Банаха-Тарського". Таких мір не існує. Це випливає безпосередньо з теореми Банах-Тарського про розбиття кулі.

Введемо відношення еквівалентності $\approx$ між підмножинами в $\mathbb{R}^3$: $X \approx Y$ тоді і тільки тоді коли існують розбиття $X = X_1 \cup \cdots \cup X_m$, $Y = Y_1 \cup \cdots \cup Y_m$, такі що Y_i конгруентна X_i для всіх $i \in \{1, \ldots, m\}$. Дві підмножини $\mathbb{R}^3$ називають конгруентними, якщо існує ізометрія простору $\mathbb{R}^3$, що переводить одну з них в другу.

ТЕОРЕМА 0.10.2 (Банаха-Тарського про кулю). *Кулю* K *з простору* $\mathbb{R}^3$*можна розбити на дві підмножини* $K = X \cup Y$*, такі що* $X \approx K$*,* $Y \approx K$

Це значить, що кулю можна розбити на скінченне число частин, з яких можна скласти дві такі ж кулі. Отже, якщо б існувала скінченно адитивна міра μ, визначена на всіх підмножинах $\mathbb{R}^3$, інваріантна відносно ізометрій і така, що $\mu(K) > 0$, то за теоремою ми б отримали суперечливу рівність $\mu(K) = 2\mu(K)$. Доведення тоереми про кулю ми одержимо за допомогою такої теореми про розбиття сфери.

ТЕОРЕМА 0.10.3 (Банаха-Тарського про сферу.). *Сферу* S *з простору* $\mathbb{R}^3$ *можна розбити на чотири підмножини* $S = A \cup B \cup C \cup Q$ *так, що*

(1) A, B, C *попарно конгруентні;*

(2) $B \cup C$ *конгруентна кожній з підмножин* A, B, C*;*

(1) Q *злічення.*

ДОВЕДЕННЯ. Нехай $G_1 = \{1, \varphi\}$, $G_2 = \{1, \psi, \psi^2\}$ — циклічні групи порядку 2 та 3, $G = G_1 * G_2$ — їх вільний добуток. Елеметами групи G є всі непорожні слова в алфавіті $\{1, \varphi, \psi, \psi^2\}$, а добуток обчислюється приписуванням до одного слова іншого з наступним скороченням за співвідношенням $\varphi^2 = 1, \psi^3 = 1$.

Розглянемо дві осі поворотів a_φ, a_ψ, що проходять через центр кулі і ототожнимо G_1 та G_2 з групами поворотів на кути $\{0, \pi\}$ навколо a_φ і $\{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$ навколо a_ψ. Далі ми виберемо осі поворотів a_φ, a_ψ так, щоб різним елементам групи G відповідали різні повороти. Для цього кут θ між осями a_φ, a_ψ треба вибрати так, щоб жоден елемент G, відмінний від 1, не представляв тотожній поворот. Розглянемо довільний елемет

$\alpha = \varphi\psi^{\pm 1} \ldots \varphi\psi^{\pm 1}$. Можна показати, що є лише скінченне число кутів θ, $0 \leq \theta \leq \pi$, для яких α — тотожнє перетворення, а тому існує континуум варіантів вибору θ.

Далі ми розкладемо групу G на три підмножини $G = \mathcal{A} \cup \mathcal{B} \cup \mathcal{C}$, такі що

$$\mathcal{A}\varphi = \mathcal{B} \cup \mathcal{C}, \mathcal{A}\psi = \mathcal{B}, \mathcal{A}\psi^2 = \mathcal{C}.$$

Підмножини $\mathcal{A}, \mathcal{B}, \mathcal{C}$ будуємо індуктивно. Покладемо $1 \in \mathcal{A}$, $\varphi, \psi \in \mathcal{B}, \psi^2 \in \mathcal{C}$ і скористаємось такою таблицею

$$\begin{array}{lccc}
 & \alpha \in \mathcal{A} & \alpha \in \mathcal{B} & \alpha \in \mathcal{C} \\
\alpha \text{ закінчується на } \left\{ \begin{array}{l} \psi^{\pm 1} : \\ \\ \varphi : \\ \\ \end{array} \right. &
\begin{array}{c} \alpha\varphi \in \mathcal{B} \\ \left\{ \begin{array}{c} \alpha\psi \in \mathcal{B} \\ \alpha\psi^{-1} \in \mathcal{C} \end{array} \right. \end{array} &
\begin{array}{c} \alpha\varphi \in \mathcal{A} \\ \alpha\psi \in \mathcal{C} \\ \alpha\psi^{-1} \in \mathcal{A} \end{array} &
\begin{array}{c} \alpha\varphi \in \mathcal{A} \\ \alpha\psi \in \mathcal{A} \\ \alpha\psi^{-1} \in \mathcal{B} \end{array}
\end{array}$$

Позначимо через Q множину усіх точок на сфері S, що є нерухомими під час деякого нетотожнього повороту з G. Оскільки кожен нетотожній поворот має лише дві нерухомі точки, Q зліченна. Далі результат застосування повороту $\alpha \in G$ до елемента $x \in S$ ми записуємо як $x\alpha$.

Множина $S \setminus Q$ розбивається на орбіти $P_x = \{x\alpha : \alpha \in G\}$, $x \in S \setminus Q$. За аксіомою вибору існує підмножина $M \subset S$, що містить рівно один елемент з кожної орбіти. Покладемо

$$A = M\mathcal{A}, B = M\mathcal{B}, C = M\mathcal{C}.$$

□

Нам потрібна така властивість відношення $\approx$: якщо $Z \subseteq Y \subseteq X$ і $X \approx Z$, то $Y \approx X$. Для доведення цієї властивості нехай ми маємо розбиття $X = X_1 \cup \cdots \cup X_n$, $Z = Z_1 \cup \cdots \cup Z_n$ і ізометрії $f_1, \ldots, f_n$, такі що $f_1(X_1) = Z_1, \ldots, f_n(X_n) = Z_n$. Нехай $f : X \to Z$ — бієкція, звуження якої на X_i співпадає з

f_i, $i \in \{1, \dots, n\}$. Покладемо

$$X_0 = X, X_1 = f(X_0), X_2 = f(X_1), \dots$$

$$Y_0 = Y, Y_1 = f(Y_0), Y_2 = f(Y_1), \dots$$

Нехай $A = \bigcup\limits_{n=0}^{\infty} (X_n \setminus Y_n)$. Тоді $f(A) \cap (X \setminus A) = \emptyset$, $A \approx f(A)$ і $X = A \cup (X \setminus A)$, $Y = f(A) \cup (X \setminus A)$, а тому $X \approx Y$.

Доведення теореми Банаха-Тарського про кулю. Розглянемо розбиття сфери $S = A \cup B \cup C \cup Q$ з теореми про сферу. Для кожної підмножини $X \subseteq S$ позначимо через $\overline{X}$ множину усіх точок кулі K, відмінних від її центру O, що проектуються з точки O та множину X. Тоді

$$K = \overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{Q} \cup \{O\}.$$

Очевидно, що $\overline{A} \approx \overline{B} \approx \overline{C} \approx \overline{B} \cap \overline{C}$. Покладемо

$$X = \overline{A} \cup \overline{Q} \cup \{O\}, \quad Y = K \setminus X = \overline{B} \cup \overline{C}.$$

Оскільки $\overline{A} \cup \overline{B} \cup \overline{C} \approx \overline{B} \cup \overline{C} \approx \overline{A}$, то

$$K = \overline{A} \cup \overline{B} \cup \overline{C} \cup \overline{Q} \cup \{O\} \approx \overline{A} \cup \overline{Q} \cup \{O\} = X.$$

Виберемо якийсь поворот γ, що не належить групі G і такий, що $Q \cap Q\gamma = \emptyset$. Це можна зробити, бо лише зліченне число поворотів мають властивість $Q \cap Q\gamma \neq \emptyset$. В силу $\overline{C} \approx \overline{A} \cup \overline{B} \cup \overline{C}$ і застосовуючи γ одержимо підмножину $H \subset C$, таку що $\overline{H} \approx \overline{Q}$. Візьмемо довільну точку $p \in \overline{C} \setminus \overline{H}$. Тоді

$$\overline{A} \cup \overline{Q} \cup \{O\} \approx \overline{B} \cup \overline{H} \cup \{p\}, \overline{B} \cup \overline{H} \cup \{p\} \subseteq Y \subset K.$$

Оскільки $\overline{B} \cup \overline{H} \cup \{p\} \approx K$, за доведеною властивістю відношення $\approx$, маємо $Y \approx K$. ☐

У спробах зрозуміти причину "парадоксу Банаха-Тарського“ Джон фон Нейман прийшов до одного з націкавіших понять в комбінаторній теорії груп — аменабельності.

Нехай G — група, $\mathcal{P}(G)$ — сім'я усіх підмножин G. Групу G називають аменабельною, якщо існує скінченно адитивна міра $\mu : \mathcal{P}(G) \to [0,1]$, $\mu(G) = 1$, що інваріантна відносно лівих зсувів, тобто $\mu(g(A)) = \mu(A)$ для будь-яких $g \in G$, $A \in \mathcal{P}(G)$. З аменабельності групи G випливає навіть існування двосторонньо інваріантної міри.

Еквівалентне означення амнабельності в аналітичній термінології виглядає так. Нехай $B(G)$ — простір усіх обмежених дійсних функцій на G з нормою $\|f\| = \sup\{f(x) : x \in G\}$. Лінійний функціонал $m : B(G) \to \mathbb{R}$ називають осередненням, якщо

$$m(f) \geq 0, \text{ якщо } f \geq 0, f(1) = 1.$$

Осереднення f називають лівоінваріантним, якщо для будь-якої функції $f \in B(G)$ $m(f) = m(f_g)$, де $f_g(x) = f(gx)$, $g \in G$. Група G аменабельна тоді і тільки тоді, коли існує лівоінваріантне осереднення на $B(G)$. Якщо m — лівоініваріантне осередення на G і $A \subseteq G$, покладемо $\mu(A) = \mu(f_A)$, де f_A — характеристична функція A. Легко первірити, що μ — лівоінваріантна міра.

Ми наведемо два критерії аменабельності — аналітичний та комбінаторний.

Теорема 0.10.4 (Критерій Діксм'є). *Група G аменабельна тоді і тільки тоді, коли для довільної скінченної множини $\{f_1, \dots, f_n\}$ функцій з $B(G)$ і довільної підмножини $\{g_1, \dots, g_n\} \subseteq G$*

$$\inf\{\sum_{i=1}^{n}(f_i(t) - f_i(g_i(t)) : t \in G\} \leq 0.$$

Теорема 0.10.5 (Критерій Фьольнера). *Група G аменабельна тоді і тільки тоді, коли для довільних $\epsilon > 0$ і скінченної підмножини $K \subseteq G$ знайдеться непорожня скінченна* *множина* $U \subseteq G$, *така що для всіх* $x \in K$

$$\frac{|(xU \setminus U) \cup (U \setminus xU)|}{|U|} \leq \epsilon.$$

Очевидним прикладом аменабельної групи є будь-яка скінченна група G (покладемо $\mu(A) = \frac{|A|}{|G|}$). Ми доведемо аменабельність довільної абелевої групи, користуючись поняттям границі обмеженої послідовності $(a_n)_{n\in\omega}$ дійсних чисел за деяким ультрафільтром p на $\omega = \{0, 1, \dots\}$. Означення ультрафільтрів та їх елементарні властивості можна знайти в лекції "Комбінаторика ультрафільтрів“. Для кожної підмножини $P \in p$ сім'я $\{a_n : n \in P\}$ є базою деякого (однозначно визначеного) ультрафільтру на $\mathbb{R}$, границя якого і називається границею $p{-}\lim(a_n)_{n\in\omega}$ послідовності (a_n) за ультрафільтром p.

Нехай спочатку G — скінченно породжена нескінченна абелева група, $G = \mathbb{Z}^m \bigoplus K$, де n — натуральне число, K — скінченна група. Для кожного $n \in \omega$ позначимо $X_n = \{0, \pm 1, \dots, \pm n\} \bigoplus K$. Для довільної підмножини $A \subseteq G$ покладемо

$$\mu(A) = p - \lim \frac{X_n \cap A}{X_n}.$$

Неважко переконатися, що μ — лівоінваріантна міра на G. Далі, кожна група є індуктивною границею скінченно продженних груп. Якщо кодна з цих груп аменабельна, то аменабельної буде і вся група. Так коротко доводиться аменабельність довільної абелевої групи. Ці ж міркування обгрунтовують достатність в критерії Фьолнера.

Отже, ми вже маємо два великі класи аменабельних груп: скінченні групи та абелеві групи. Запас прикладів можна поширити, скориставшись простими властивостями аменабельності:

- гомоморфний образ аменабельної групи аменабельний;

- підрупа аменабельної групи аменабельна;

- розширення аменабельної групи за допомогою аменабельної групи аменабельне;

- індуктивна границя аменабельних груп аменабельна.

Перший приклад неаменабельної групи навів сам фон Нейман — це вільна група F з двома вільними твірними a, b. Кожен елемент $x \in F$ має однозначний нескорочуваний запис $x = a^i b^j \dots$, де $i, j \in \mathbb{Z}$. Віднесемо x до підмножини H_i і зауважимо, що підмножини сім'ї $\{H_i^i \in \mathbb{Z}\}$ попарно не перетинаються і $F = \cup_{i \in \mathbb{Z}} H_i$. Припустімо, що F аменабельна і μ — лівоінваріантна міра на F. Відображення $x \mapsto ax$ переводить H_i в H_{i+1}, а тому $\mu(H_i) = 0$ для всіх $i \in \mathbb{Z}$. Відображення $x \mapsto bx$ переводить $H_i, i \neq 0$ в H_0. Значить, $\mu(H_0) \geq \mu(\bigcup\limits_{i \neq 0} H_i)$. Оскільки $\mu(H_0) + \mu(\bigcup\limits_{i \neq 0} H_i) = 1$, то $\mu(H_0) \geq \frac{1}{2}$. Але відображення $x \mapsto ax$ переводить H_0 в H_1 а $\mu(H_1) = 0$, суперечність.

Повернімось до "парадоксу Банаха-Тарського“. Для $n \in \mathbb{N}$ розглянемо групу G_n усіх ізометрій простору $\mathbb{R}^n$. З наведених вище властивостей легко випливає, що групи G_1 та G_2 аменабельні. Це по суті і дозволяє побудувати скінченно-адитивні міри, визначені на всіх підмножинах з $\mathbb{R}^1$ та $\mathbb{R}^2$, інваріантні відносно ізометрій. Для $n > 2$ група G_n містить вільну підгрупу з двома твірними, а тому неаменабельна, що і дозволило побудувати парадоксальне розбиття кулі.

Ретельно проглянувши попередній виклад, неважко зрозуміти, що лишилося ще одне запитання, пов'язане з мірою Лебега. Чи можна визначити скінченно адитину міру $\mu : ([0,1]) \to [0,1]$, таку що $\mu([0,1]) = 1$ і $\mu(\{x\}) = 0$ для всіх $x \in X$?

Цим запитанням ми взагалі відмовилися від будь-якої інваріантності, а умову зліченної адитивності послабили до скінченної адитивності, проте посилили вимогу на область визначення міри — усі підмножини мають бути вимірними. Виявляється, на будь-якій нескінченній множині X існує навіть двозначна міра $\mu : \mathcal{P}(X) \to \{0,1\}$ з цими властивостями. Більше того, таких мір $2^{2^{|X|}}$. Це випливає з природньої бієкції між множинами усіх вільних ультрафільтрів на X і множиною скінченно-адитивних мір $\mu : (C) \to \{0,1\}$, таких що $\mu(X) = 1$ і $\mu(\{x\}) = 0$ для всіх $x \in X$.

Нехай $\mathcal{F}$ — вільний ультрафільтр на X. Визначимо міру $\mu : \mathcal{P}(X) \to \{0,1\}$ за таки правилом $\mu(A) = 1$, якщо $A \in \mathcal{F}$, $\mu(A) = 0$, якщо $A \notin \mathcal{F}$. Це означення коректне за критерієм ультрфільтру. Зрозуміло, що $\mu(X) = 1$ і $\mu(\{x\}) = 0, x \in X$, оскільки ультрафільтр $\mathcal{F}$ вільний. Нехай $A \cup B \in \mathcal{F}$, то одна з підмножин A, B належить $\mathcal{F}$, а інша — ні, і маємо $\mu(A \cup B) = 1$, $\mu(A) + \mu(B) = 1$. Якщо $A \cup B \notin \mathcal{F}$, то $\mu(A \cup B) = 0$ і $\mu(A) = \mu(B) = 0$. У зворотній бік, якщо μ — міра з вказаними властивостями, то сім'я підмножин $\mathcal{F} = \{A \subseteq X : \mu(A) = 1\}$ є ультрафільтром на X, що визначає μ вказаним вище способом.

Зауважимо, що сама проблема побудови скінченно адитивної міри була одним з основних джерел виникнення поняття ультрафільтру.

Але тепер ми можемо захотіти більшого — зліченно-адитивної двозначної міри $\mu : \mathcal{P}([0,1] \to \{0,1\}$, такої що $\mu([0,1]) = 1$ і $\mu(\{x\}) = 0$ для всіх $x \in X$. Доведена вище тоерема Улама стосувалася мір зі значенням у відрізку $[0,1]$. Зв'язок таких двозначних мір з ультрафільтрами встановлюється наступним означенням.

Нехай α — нескінченний кардинал. Ультрафільтр $\mathcal{F}$ на деякій множині ми назвемо *α-центрованим,* якщо $\cap\mathcal{F}' \in \mathcal{F}$ для довльної підмножини $\mathcal{F}' \subseteq \mathcal{F}$, $|\mathcal{F}'| < \alpha$. Зрозуміло, що кожен ультрафільтр $\aleph_0$-центрований. Крім того, ультрафільтр $\mathcal{F}$ на X α-центрований тоді і тільки тоді, коли для будь-якої сім'ї підмножин $\mathcal{X}$ множини X з умови $\cup\mathcal{X} = X$ випливає існування елементу з $\mathcal{X}$, що належить $\mathcal{F}$.

Нехай $\mathcal{F}$ — вільний α-центрований ультрафільтр на множині X. Визначимо двозначну міру $\mu : \mathcal{P}(X) \to \{0,1\}$ за правилом

$$\mu(F) = \begin{cases} 1, & \text{якщо } F \in \mathcal{F}; \\ 0, & \text{якщо } F \notin \mathcal{F}. \end{cases}$$

Міра μ має такі властивості:

(1α) $\mu(X) = 1$, $\mu(\{x\}) = 0$ для всіх $x \in X$;

(2α) $\mu(A) = 1 - \mu(X \setminus A)$ для довільної підмножини $A \subseteq X$;

(3α) об'єднання будь-яких $< \alpha$ підмножин міри 0 має міру 0.

Навпаки, кожна двозначна міра $\mu : \mathcal{P}(X) \to \{0,1\}$, що задовольняє умови $(1\alpha), (2\alpha), (3\alpha)$, породжує вільний α-центрований ультрафільтр, елементами якого є всі підмножини з X міри 0.

Кардинал α називають *вимірним,* якщо на множині ординалів $\{\gamma : \gamma < \alpha\}$ існує вільний α-цетрований ультрафільтр. Ясно, що кардинал $\aleph_0$ вимірний, χ_1 невимірний за теоремо Улама. Питання про існування незліченних невимірних кардиналів зав'язло в аксіоматиці теорії множин. Якщо прийняти так звану аксіому конструктивносі AC, то таких кардиналів немає. Якщо незліченні вимірні кардинали існують в деяких моделях ZFC, то вони мають бути надзвичайно великими, про що свідчить така теорема.

ТЕОРЕМА 0.10.6 (Улама-Тарського). *Кожен незліченний вимірний кардинал, якщо такий існує, сильно недосяжний.*

Кардинал $\alpha > \aleph_0$ називають *сильно недосяжним,* якщо

(*) α недосяжний, тобто $2^\gamma < \alpha$ для всіх $\gamma < \alpha$;

(**) α регулярний, тобто $\mathrm{cf}(\alpha) = \alpha$, де $\mathrm{cf}(\alpha)$ — конфінальність α.

За цим означенням, сильно недосяжний кардинал не можна побудувати з менших кардиналів операціями експоненціювання, переходу до підмножин і об'єднаннями.

ДОВЕДЕННЯ ТЕОРЕМИ УЛАМА-ТАРСЬКОГО. Нехай α — незліченний вимірний кардинал, ми маємо довести, що α недосяжнимй і регулярний.

Спочатку ми припустимо, що α досяжний і знайдемо кардинал $\gamma < \alpha$, для якого $2^\gamma \geq \alpha$. Нехай $f : \alpha \to 2^\gamma$ — ін'єктивне відображення, $\mathcal{F}$ — вільний α-центрований ультрафільтр на множині $\alpha = \{\eta : \eta < \alpha\}$. Ототожнимо γ з множиною $\{\tau : \tau < \gamma\}$ і для кожного $\tau < \gamma$ позначимо $Z_\tau = \{\eta < \alpha : \tau \in f(\eta)\}$. Покладемо

$$Y_\tau = \begin{cases} Z_\tau, & \text{якщо } Z_\tau \notin \mathcal{F}; \\ \alpha \setminus Z_\tau, & \text{якщо } Z_\tau \in \mathcal{F}; \end{cases}$$

За цим означенням жодна з підмножин Y_τ, $\tau < \gamma$ не є елементом ультрафільтру $\mathcal{F}$. З α-центрованості $\mathcal{F}$ випливає що підмножина $Y = \bigcup\limits_{\tau<\gamma} Y_\tau$ не є елементом $\mathcal{F}$, значить $\alpha \setminus Y \in \mathcal{F}$. Ми покажемо, що підмножина $\alpha \setminus Y$ містить не більше одного елементу і, таким чином, одержимо суперечність, оскільки $\mathcal{F}$ — вільний ультрафільтр. Нехай $\eta \in \alpha \setminus Y$. Тоді $\eta \notin Y_\tau$ для всіх $\tau < \gamma$. Далі,

$$\tau \in f(\eta) \Leftrightarrow \eta \in Z_\tau \Leftrightarrow Y_\tau = \alpha \setminus Z_\tau \Leftrightarrow Z_\tau \in \mathcal{F}.$$

Отже, $f(\eta) = \{\tau : Z_\tau \in \mathcal{F}\}$. Ця рівність визначає $f(\eta)$ незалежно від вибору η і з ін'єктивності f випливає $|\alpha \setminus Y| \leq 1$.

Регулярність α випливає з таких міркувань: з α-центрованості випливає, що жодна підмножина $Y \subset \alpha$, $|Y| < \alpha$ не є елементом $\mathcal{F}$, а тому і об'єднання таких підмножин не є елементом $\mathcal{F}$, тоді як $\alpha \in \mathcal{F}$. $\square$

На перший погляд в означенні вимірного кардиналу α вимагається занадто велика (навіть максимальна з можливих) степінь центрованості вільного ультрафільтру на α. Спробуємо пом'якшити цю умову. Кардинал α називають *вимірним за Уламом,* якщо на α існує вільний $\aleph_1$-центрований ультрафільтр (еквівалетно, існує зліченно адитивна двозначна міра, визначена на всіх підмножина α). Проте і таке (максимально можливе нетривіальне пом'якшення) призводить до великих кардиналів.

Ми покажемо, що найменший вимірний за Уламом кардинал α вимірний (а тому сильно недосяжний). Нехай $\mathcal{F}$ — $\aleph_1$-центрований вільний ультрафільтр на α. Зрозуміло, що $\mathcal{F}$ не є α^+-центрованим, а тому існує мінімальний кардинал $\gamma \leq \alpha$, для якого $\mathcal{F}$ не є γ-центрованим. Покажемо, що γ не може бути граничним кардиналом. Припустимо супротивне. Оскільки $\mathcal{F}$ не є γ-центроним знайдуться такі кардинал $\gamma_1 < \gamma$ і сім'я $\{X_\eta : \eta < \gamma_1\}$ підмножин α, що $\cap\{X_\eta : \eta < \gamma_1\} \notin \mathcal{F}$, але $X_\eta \in \mathcal{F}$ для всіх $\eta < \gamma_1$. Оскільки γ граничний ми можемо вибрати γ_2, $\gamma_1 < \gamma_2 < \gamma$. Тоді $\mathcal{F}$ не є γ_2-центрованим, всупереч з вибором γ. Отже, $\gamma = \beta^+$ для деякого кардинала $\beta \geq \aleph_1$. Оскільки $\aleph_1 \leq \beta \leq \alpha$, залишилось переконатися, що кардинал β вимірний. Оскільки ультрафільтр $\mathcal{F}$ на α не є β^+-центрованим, знайдеться розбиття $\alpha = \cup\{A_\eta : \eta < \beta\}$, таке що $A_\eta \notin \mathcal{F}$ для всіх $\eta < \beta$. Задамо відображення $f : \alpha \to \beta$, $f(x) = \eta$, якщо $x \in A_\eta$. Образ $\mathcal{F}'$ β-центрованого ультрафільтра $\mathcal{F}$ при відображенні f є β-центрованим ультрафільтром на β. З умови $A_\eta \notin \mathcal{F}$ для всіх $\eta < \beta$ випливає, що $\mathcal{F}'$ — вільний ультрафільтр.

Бібліоґрафія

[1] Jech T. The Axiom of Choice, Studies in logic and the foundation of mathamatics, London, New York, 1973.

[2] Kemp P. A nonmeasurable partition of Reals, Bull. Belg. Math. Soc., 8 (2001),№1, 83-86.

[3] Гранлиф Ф. Инвариантные средние на группах, М., "Мир 1973.

[4] Кановей В. Г. Аксиома выбора и принцип детерминированости. М.,

[5] Окстоби Дж. Мера и категория, М., "Мир 1974.

[6] Харазишвили А. Б. Топологические аспекты теории меры, Киев, "Наукова думка 1984.

0.11. Комбінаторика кульових структур

Кульова структура — це трійка $\mathcal{B} = (X, P, B)$, де X, P — непорожні множини і для всіх $x \in X$, $\alpha \in P$, $B(x, \alpha)$ — підмножина множини X, що називається *кулею радіуса* α з центром в точці x. При цьому вимагається, щоб $x \in B(x, \alpha)$ для всіх $x \in X$, $\alpha \in P$. Множина X називається *носієм* $\mathcal{B}$, а P — множиною радіусів.

Для довільних $x \in X$, $\alpha \in P$, $A \subseteq X$ ми позначимо

$$B^*(x, \alpha) = \{y \in X : x \in B(y, \alpha)\}, \quad B(A, \alpha) = \bigcup_{a \in A} B(a, \alpha),$$

$$B^*(A, \alpha) = \bigcup_{a \in A} B^*(a, \alpha).$$

Кульова стуктура $\mathcal{B}$ називається *симетричною* вниз, якщо для всіх $\alpha, \beta \in P$ існують $\alpha', \beta' \in P$, такі що

$$B^*(x, \alpha') \subseteq B(x, \alpha), \quad B(x, \beta') \subseteq B^*(x, \beta)$$

для всіх $x \in X$.

Кульова структура $\mathcal{B}$ називається *симетричною вгору,* якщо для всіх $\alpha, \beta \in P$ існують $\alpha', \beta' \in P$, такі що

$$B(x, \alpha) \subseteq B^*(x, \alpha'), \quad B^*(x, \beta) \subseteq B(x, \beta')$$

для всіх $x \in X$.

Кульова структура $\mathcal{B}$ називається *мультиплікативною вниз,* якщо для будь-якого $\alpha \in P$ знайдеться $\beta \in P$, таке що

$$B(B(x, \beta), \beta) \subseteq B(x, \alpha) \cap B(x, \gamma)$$

для всіх $x \in X$.

Кульова структура $\mathcal{B}$ називається *мультиплікативною вгору,* якщо для будь-яких $\alpha, \beta \in P$ знайдеться $\gamma \in P$, таке що

$$B(B(x, \alpha), \beta) \subseteq B(x, \gamma)$$

для всіх $x \in X$.

Нехай кульова структура $\mathcal{B}$ симетрична та мультиплікативна вниз. Тоді сім'я підмножин

$$\cup \{B(x, \alpha) \times B(x, \alpha) : x \in X\}, \quad \alpha \in P$$

є фундаментальною системою оточень діагоналей деякого рівномірного простору $(X\mathcal{U})$. Про рівномірні топологічні простори див., наприклад, [**12**], [**13**]. З іншого боку, якщо $(X,\mathcal{U})$ — рівномірний простір з рівномірністю $\mathcal{U}$ то кульова структура $(X,\mathcal{U}, B)$, де $B(x, U) = \{y \in X : (x, y) \in U\}$, симетрична та мультиплікативна вниз. Таким чином, симетричні та мультиплікативні вниз кульові структури можна ототожнити з рівномірними просторами. Морфізмами в категорії рівномірних просторів є рівномірно неперервні відображення. Нехай кульові структури $\mathcal{B}_1 = (X_1, P_1, B_1)$, $\mathcal{B}_2 = (X_2, P_2, B_2)$ симетричні та мультиплікативні вниз. Відображення $f : X_1 \to X_2$ називається *рівномірно неперервним,* якщо для довільного $\beta \in P_2$ знайдеться $\alpha \in P_1$, таке що

$$f(B_1(x, \alpha)) \subseteq B_2(f(x), \beta)$$

для всіх $x \in X$.

Кульову структуру $\mathcal{B}$, що є симетричною та мультиплікатвною вгору, ми називаємо *болеаном.* Нехай $\mathcal{B}_1 = (X_1, P_1, B_1)$, $\mathcal{B}_2 = (X_2, P_2, B_2)$ — два болеани. Відображення $f : X_1 \to X_2$ ми називаємо $\prec$-*відображенням,* якщо для кожного $\alpha \in P_1$, знайдеться $\beta \in P_2$ таке, що

$$f(B_1(x, \alpha)) \subseteq B_2(f(x), \beta)$$

для всіх $x \in X$. Якщо f бієкція і f, f^{-1} є $\prec$-відображенням, то f називаємо асиморфізмом, а $\mathcal{B}_1, \mathcal{B}_2$ асиморфними.

Зауважимо, що болеани виникли в асимптотичній топології під (дещо невдалою) назвою "грубі структури" (див. огляд [**1**]), а також незалежно, хоча дещо пізніше а комбінаториці [**6**]. В цій лекції ми розглянемо лише деякі комбінаторні аспекти болеанів. Більше про болеани як асимптотичну альтернативу рівномірних просторів можна просчитати в [**1**],[**2**],[**3**], [**6**],[**7**],[**8**],[**9**],[**10**],[**11**]. А почнемо ми з прикладів.

Кожен метричний простір (X, d) можна розглядати з одного боку як кульову структуру, що симетрична та мультиплікативна вниз, тобто рівномірний простір, або як болеан $\mathcal{B}(X, d) = (X, \mathbb{R}^+, B_d)$, де $\mathbb{R}^+$ — множина невід'ємних дійсних чисел, $B_d(x, r) = \{y \in X : d(x, y) \leq r\}$. Якщо з "рівномірної" точки зору метричні простори $(\mathbb{Z}, d)$, $(\mathbb{Z}^2, d)$, d — евклідова відстань, не розрізняються (тобто рівномірно гомеоморфні), то як болеани вони неасиморфні (чому?).

Болеан, асиморфний болеану деякого метричного простору (X, d), називається *метризовним.* Критерій метризованості дуже простий [**1**, Theorem 9.1]: болеан $\mathcal{B} = (X, P, B)$ метризований тоді і лише тоді, коли $\mathcal{B}$ зв'язний і $\operatorname{cf} \mathcal{B} \leq \aleph_0$. Зв'язність означає, що для довільних $x, y \in X$ знайдеться $\alpha \in P$, таке що $y \in B(x, \alpha)$. На множині радіусів довільного болеану (X, P, B) є природній частковий передпорядок: $\alpha \leq \beta$ тоді і тільки тоді, коли $B(x, \alpha) \subseteq B(x, \beta)$ для всіх $x \in X$. Підмножина $P' \subseteq P$ називається *конфінальною,* якщо для довільного $\alpha \in P$ знайдеться $\beta \in P'$, таке що $\alpha \leq \beta$. Конфінальність $\operatorname{cf} \mathcal{B}$ — це мінімальна з потужностей конфінальних множин в P. Про хfamтеризацію болеанів деяких класів метричних просторів, зокрема зв'язних графів, див. [**1**, Chapter 9].

Нехай G — нескінченна група з одиницею e, k — нескінченний кардинал, $k \leq |G|$. Позначимо через $\mathcal{F}(G, k)$ сім'ю всіх підмножин G потужності $< k$, що містять e. Для довільних $g \in G$, $F \in \mathcal{F}(G, k)$ покладемо

$$B_l(g, F) = gF, \quad B_r(g, F) = Fg.$$

і позначимо через $\mathcal{B}_l(G, k)$, $\mathcal{B}_r(G, k)$ болеани $(G, \mathcal{F}(G, k), B_l)$, $(G, \mathcal{F}(G, k), B_r)$. Зауважимо, що відображення $g \mapsto g^{-1}$ є асиморфізмом між $\mathcal{B}_l(G, k)$ та $\mathcal{B}_r(G, k)$. Про інші болеани, визначені на групах див. [**11**].

Нехай X — довільна множина φ — фільтр на X, такий що $\cap\varphi = \emptyset$. Для довільних $x \in X$, $F \in \varphi$ покладемо

$$B(x, F) = \left\{ \begin{array}{rl} X \setminus F, & \text{якщо } x \notin F; \\ \{x\}, & \text{якщо } x \in F; \end{array} \right.$$

Таким чином, кожен фільтр φ на X визначає болеан $\mathcal{B}(X, \varphi) = (X, \varphi, B)$.

Наразі ми дамо класифікацію підмножин кульових структур за їх розмірами. Нехай $\mathcal{B} = (X, P, B)$ — кульова структура, $A \subseteq X$, $\alpha \in P$. Покладемо

$$\mathrm{Int}(A, \alpha) = \{x \in X : B^*(x, \alpha) \subseteq A\}.$$

Підмножину $A \subseteq X$ ми називаємо

- *великою,* якщо існує $\alpha \in P$, таке що $X = B(A, \alpha)$;
- *малою,* якщо $X \setminus B(A, \alpha)$ велика для всіх $\alpha \in P$;
- *надвеликою,* якщо $\mathrm{Int}(A, \alpha)$ велика для всіх $\alpha \in P$;
- *кусково-великою,* якщо існує $\beta \in P$, таке що $\mathrm{Int}(B(A, \beta), \alpha) \neq \emptyset$ для всіх $\alpha \in P$.

Два прості спостереження.

Лема 0.11.1. *Нехай $\mathcal{B}(X, P, B)$ — кульова структура, $A \subseteq X$, $\alpha \in P$. Тоді* $\mathrm{Int}(X \setminus A, \alpha) = X \setminus B(, \alpha)$.

Доведення. Нехай $x \in \mathrm{Int}(X \setminus A, \alpha)$. Тоді $B^*(x, \alpha) \cap A = \emptyset$ і $x \notin B(a, \alpha)$ для всіх $a \in A$. Отже, $x \in X \setminus B(A, \alpha)$.

Нехай $x \in X \setminus B(A, \alpha)$. Тоді $x \notin B(a, \alpha)$ для всіх $a \in A$. Отже $a \notin B^*(x, \alpha)$ для всіх $a \in A$, а тому $B^*(x, \alpha) \subseteq X \setminus A$ і $x \in \mathrm{Int}(X \setminus A, \alpha)$. □

Лема 0.11.2. *Якщо кульова структура $\mathcal{B}(X, P, B)$ мультиплікативна вгору, $\alpha \in P$ і підмножина $B(A, \alpha)$ велика, то A велика.*

Доведення. Виберемо $\beta \in P$ так, що $B(B(A, \alpha), \beta) = X$. Далі знайдеться $\gamma \in P$, таке що $B(B(A, \alpha), \beta) \subseteq B(A, \gamma)$. Отже, $B(A, \gamma) = X$ і A велика. □

Теорема 0.11.3. *Нехай $\mathcal{B}(X, P, B)$ — кульова структура, $S \subseteq X$. Тоді наступні твердження еквівалентні:*

(i) *S мала;*

(ii) S *не є кусково-великою;*

(iii) $X \setminus S$ *надвелика;*

(iv) $(X \setminus S) \cap L$ *велика для кожної великої підмножини* $L \subseteq X$.

ДОВЕДЕННЯ. (i)⇒(ii). Для кожного $\alpha \in P$ виберемо $\beta(\alpha) \in P$ так, що $B(X \setminus B(S,\alpha), \beta(\alpha)) = X$. Візьмемо довільний елемент $x \in X$ і виберемо $y \in X \setminus B(S,\alpha)$, такий що $x \in B((y, \beta(\alpha))$. Тоді $y \in B^*(x, \beta(\alpha))$ і $B^*(x, \beta(\alpha)) \cap (X \setminus B(S,\alpha)) \neq \emptyset$. Отже, $\mathrm{Int}(B(S,\alpha), \beta(\alpha)) = \emptyset$ і S не є кусково великою.

(ii)⇒(iii). Для кожного $\alpha \in P$ виберемо елемент $\beta(\alpha) \in P$, такий що $\mathrm{Int}(B(S,\alpha), \beta(\alpha)) = \emptyset$. Тоді $B^*(x, \beta(\alpha)) \cap (X \setminus B(S,\alpha)) \neq \emptyset$ для довільного $x \in X$. За лемою 0.11.1

$$B^*(x, \beta(\alpha)) \cap \mathrm{Int}(X \setminus S, \alpha) \neq \emptyset.$$

для кожного $x \in X$. Отже, $X = B(\mathrm{Int}(X \setminus S, \alpha), \beta(\alpha))$ і $X \setminus S$ надвелика.

(iii)⇒(i). Для кожного $\alpha \in P$ виберемо елемент $\beta(\alpha) \in P$, такий що $B(\mathrm{Int}(X \setminus S, \alpha), \beta(\alpha)) = X$. За лемою 0.11.1, $B(X \setminus B(S,\alpha), \beta(\alpha)) = X$. Отже, S мала.

(iii)⇒(iv). Покладемо $P = X \setminus S$ і виберемо довільну велику підмножину L. Виберемо $\alpha \in P$ так, що $X = B(L,\alpha)$. Для кожного $x \in \mathrm{Int}(Y,\alpha)$ виберемо $y(x) \in L$ так, що $x \in B(y(x),\alpha)$, еквівалентно, $y(x) \in B^*(x.\alpha)$. Покладемо $Y' = \{y(x) : x \in \mathrm{Int}(Y,\alpha)\}$ і зауважимо, що $Y' \subseteq Y \cap L$. Оскільки $\mathrm{Int}(Y,\alpha) \subseteq B(Y',\alpha)$ і $\mathrm{Int}(Y,\alpha)$ велика, то $B(Y',\alpha)$ велика. За лемою 0.11.2, Y' велика. Оскільки $Y' \subseteq Y \cap L$, $Y \cap L$ велика.

(iv)⇒(iii). Покладемо $Y = X \setminus S$. Оскільки $Y \cap X = Y$ і X велика, Y велика. Зафіксуємо $\alpha \in P$ і покажемо, що $\mathrm{Int}(Y,\alpha)$ велика. Для кожного $x \in Y \setminus \mathrm{Int}(Y,\alpha)$ виберемо $y(x) \in B^*(x,\alpha) \setminus Y$. Покладемо $Y' = \{y(x) : x \in Y \setminus \mathrm{Int}(Y,\alpha)\}$ і $L = Y' \cap \mathrm{Int}(Y,\alpha)$. Зауважимо, що $Y \subseteq B(L,\alpha)$. Оскільки Y

велика, $B(L,\alpha)$ велика. За лемою 0.11.2 L велика. За припущенням $Y\cap L$ велика. Оскільки $Y\cap L=\mathrm{Int}(Y,\alpha)$, підмножина $\mathrm{Int}(Y,\alpha)$ велика. $\square$

ТЕОРЕМА 0.11.4. *Нехай $\mathcal{B}(X,P,B)$ мультипліктивна вгору кульова структура. Якщо підмножини $X_1,\dots,X_n$ множини X надвеликі, то $X_1\cap\dots\cap X_n$ надвелика. Якщо підмножини $S_1,\dots,S_n$ множини X малі, то $S_1\cup\dots\cup S_n$ мала. Якщо кусково-велику підмножину $A\subseteq X$ розбити на скінченне число підмножин $A=A_1\cup\dots\cup A_n$, то принаймні одна з підмножин A_i розбиття кусково-велика. Зокрема, X не можна розбити на скінченне число малих підмножин.*

ДОВЕДЕННЯ. Візьмемо довільну велику підмножину L із X. За еквівалентністю (iii)$\Leftrightarrow$(iv). теореми 0.11.3 підмножина $X_n\cap L$ велика. Оскільки $X_1\cap\dots\cap X_n)\cap L=(X_1\cap\dots\cap X_{n-1})\cap(X_n\cap L)$, за індукцією, $(X_1\cap\dots\cap X_n)\cap L$ велика. За еквівалентністю (iii)$\Leftrightarrow$(iv) теореми 0.11.3 $X_1\cap\dots\cap X_n$ надвелика. Друге твердження випливає з першого і еквівалентності (i)$\Leftrightarrow$(iii) теореми 0.11.3. Третє твердження випливає з другого і еквівалентності (i)$\Leftrightarrow$(ii) теореми 0.11.3. $\square$

За теоремою 0.11.4 сім'я $\mathcal{E}(\mathcal{B})$ усіх надвеликих підмножин мультиплікативної вгору кульової структури $\mathcal{B}(X,P,B)$ є фільтром на X.

ТЕОРЕМА 0.11.5. *Нехай $\mathcal{B}(X,P,B)$ — мультиплікативна вгору кульова структура, ψ — ультрафільтр на X. Тоді $\mathcal{E}(\mathcal{B})\subseteq\psi$ тоді і тільки тоді, коли кожна підмножина $A\in\psi$ кусково-велика.*

ДОВЕДЕННЯ. Припустимо, зо $\mathcal{E}(\mathcal{B})\subseteq\psi$ і візьмемо довільну підмножину $A\in\psi$. Припустимо, що A не є кусково-великою. За еквівалентністю (i)$\Leftrightarrow$(ii) теореми 0.11.3 A мала. Отже, $X\setminus A\subseteq\mathcal{E}(\mathcal{B})$, що суперечить означенню фільтру.

Нехай кожна підмножина $A \in \psi$ кусково-велика, але $\mathcal{E}(\mathcal{B})$ не міститься в ψ. Виберемо підмножину $Y \in \mathcal{E}(\mathcal{B})$, таку що $Y \notin \psi$. За еквівалентністю (i)$\Leftrightarrow$(iii) теореми 0.11.3, $X \setminus A$ мала і ми одержали суперечність з еквівалентністю (i)$\Leftrightarrow$(ii) теореми 0.11.3. □

Повертаючись до аналогії між рівномірними просторами і болеанами (і враховуючи доведені теореми), можна стверджувати, що великі підмножини болеанів є аналогами щільних підмножин, малі — аналогами ніде не щільних підмножин, надвеликі — аналогами щільних відкритих підмножин.

Е. Хевіт [**4**] назвав топологічний простір X k-розкладним (k — деякий кардинал) якщо X можна розбити на k щільних підмножин. Наразі ми викладемо деякі результати стосовно розкладеності болеанів.

Нехай $\mathcal{B}(X, P, B)$ — болеан, k — кардинал. За нашим означенням, $\mathcal{B}$ є *k-розкладним,* якщо X можна розбити на k великих підмножин. *Розкладність* $\mathcal{B}$ —це кардинал

$$\operatorname{res}\mathcal{B} = \sup\{k : \mathcal{B} \text{ є } k \text{ розкладним}\}.$$

Для того, щоб обчислити розкладність ми введемо ще один кардинальний інваріант болеану. Назвемо підмножину $Y \subseteq X$ *k-насиченою,* якщо існує $\alpha \in P$, таке що $|B(y, \alpha) \cap Y| \geq k$ для всіх $y \in Y$. Болеан $\mathcal{B}$ назвемо k-насиченим, якщо його носій k-насичений. *Насиченість* $\mathcal{B}$ — це кардинал

$$\operatorname{cr}\mathcal{B} = \sup\{k : \mathcal{B} \text{ є } k \text{ насиченим}\}.$$

Лема 0.11.6. *Для довільного болеану $\mathcal{B} = (X, P, B)$ справедливі такі твердження*

(i) *якщо $\mathcal{B}$ k-насичений, то $\mathcal{B}$ k-розкладний;*

(ii) $\operatorname{cr}\mathcal{B} \leq \operatorname{res}\mathcal{B} \leq \operatorname{cr} \cdot \operatorname{cf}\mathcal{B}$*;*

(iii) *якщо k — скінченний кардинал і $\mathcal{B}$ k-розкладний, то $\mathcal{B}$ k-насичений.*

Доведення. (i)Виберемо $\alpha \in P$ так, що $|B(x,\alpha)| \geq k$ для всіх $x \in X$. За лемою Цорна існує підмножина $Y \subseteq X$, така що сім'я $\{B(y,\alpha) : y \in Y\}$ диз'юнктна і для кожного $x \in X$ існує $y \in Y$, таке що $B(x,\alpha) \cap B(y,\alpha) \neq \emptyset$. Оскільки $|B(y,\alpha)| \geq k$ для кожного $y \in Y$, існує сім'я $\mathcal{F}$ з k попарно диз'юнктних підмножин з X така, що $|F \cap B(y,\alpha)| = 1$ для всіх $y \in Y$, $F \in \mathcal{F}$. Легко перевірити, користуючись означенням болену, що кожна підмножина $F \in \mathcal{F}$ велика, а тому $\mathcal{B}$ k-розкладний.

(ii) Ліва нерівність виливає з (i). Нехай $\mathcal{F}$ — довільна диз'юнктна сім'я великих підмножин X. Виберемо конфінальну підмножину $P' \subseteq P$, таку що $|P'| = \mathrm{cf}\,\mathcal{B}$. Для довільного $\alpha \in P'$ покладемо

$$\mathcal{F}(\alpha) = \{F \in \mathcal{F} : B^*(F,\alpha) = X\}.$$

Візьмемо довільні $x \in X$, $\alpha \in P'$. Оскільки $B(x,\alpha) \cap F \neq \emptyset$ для всіх $F \in \mathcal{F}(\alpha)$, $|\mathcal{F}(\alpha)| \leq |B(x,\alpha)|$. Отже, $|\mathcal{F}(\alpha)| \leq \mathrm{cr}\,\mathcal{B}$.

(iii) Нехай $F_1, \dots, F_m$ — великі підмножини з X, що попарно не перетинаються. Виберемо $\alpha \in P$ так, що $B^*(F_i,\alpha) = X$ для всіх $i \in \{1,\dots,m\}$. Тоді $B(x,\alpha) \cap F_i \neq \emptyset$ для всіх $x \in X$, $i \in \{1,\dots,m\}$. Звідси випливає, що $|B(x,\alpha)| \geq m$ і $\mathcal{B}$ m-насичений. □

Лема 0.11.7. *Нехай $\mathcal{B}(X,P,B)$ — болеан, $(k_n)_{n\in\omega}$ — зростаюча послідовність кардиналів, $k = \sup\{k_n : n \in \omega\}$. Якщо $\mathcal{B}$ k_n-насичений для всіх $n \in \omega$, то X можна розбити на k великих підмножин.*

Доведення. Нам достатньо розбити $X = Y \cup Z$ так, що Y є диз'юнктним об'єднанням k_0 великих підмножин і Z є k_n-насиченим для довільного $n \in \omega$. Ми можемо вважати, що $k_0 > 0$. Виберемо $\alpha \in P$, таке що $|B(x,\alpha)| \geq 2k_0$ для всіх $x \in X$. За лемою Цорна існує підмножина $A \subseteq X$, така що $\{B(a,\alpha) : a \in A\}$ — максимальна диз'юнктна сім'я. Для довільного $a \in A$ розіб'ємо $B(a, \alpha) = C(a) \cup D(a)$ так, що $|C(a)| = k_0$, $|D(a)| \geq k_0$. Покладемо $Y = \bigcup\limits_{a \in A} C(a)$, $Z = X \setminus Y$ і зауважимо, що Y можна розбити на k_0 великих підмножин. Зафіксуємо $n \in \omega$ і виберемо $\beta \in P$, таке що $|B(x, \beta)| > 2k_n$ для всіх $x \in X$. Оскільки кульова структура $\mathcal{B}$ мультиплікативна вгору, існує $\gamma \in P$, таке що $B(B(x, \beta), \alpha) \subseteq B(x, \gamma)$ для всіх $x \in X$. Тоді $|B(z, \gamma) \cap Z| \geq k_n$ для всіх $z \in Z$ і Z — k_n-насичена підмножина. □

Теорема 0.11.8. *Для довільного метричного простору* (X, d)

$$\operatorname{res} \mathcal{B}(X, d) = \operatorname{cr} \mathcal{B}(X, d)$$

і X можна розбити на $\operatorname{cr} \mathcal{B}(X, d)$ *великих підмножин.*

Доведення. Оскільки $\operatorname{cf} B(X, d) \leq \aleph_0$, перше твердження випливає з леми 0.11.6. Друге твердження випливає з леми 0.11.7. □

Для обчислення розкладності болеанів груп ми використаємо фільтрацію групи її підгрупами.

Нехай G — нескінченна підгрупа з одиницею e. *Фільтрація* G — це сім'я $\{G_\alpha : \alpha < |G|\}$ підгруп групи G, така що

(i) $G_0 = \{e\}$, $G = \cup\{G_\alpha : \alpha < |G|\}$;

(ii) $G_\alpha \subset G_\beta$ для всіх $\alpha < \beta < |G|$;

(iii) $\cup\{G_\alpha : \alpha < \beta\} = G_\beta$ для кожного граничного ординалу β;

(iv) $|G_\alpha| < |G|$ для всіх $\alpha < |G|$.

Використовуючи мінімальний повний порядок на G неважко побудувати фільтрацію на кожній групі G за умови, що G не є скінченно породженою.

Для кожного $\alpha < |G|$ розкладемо $G_{\alpha+1} \setminus G_\alpha$ на праві суміжні класи за підгрупою G_α і зафіксуємо деяку сім'ю X_α представників суміжних класів, $G_{\alpha+1} \setminus G_\alpha = G_\alpha X_\alpha$. Візьмемо довільний елемент $g \in G$, $g \neq e$ і виберемо найменшу підгрупу G_α, для якої $g \in G_\alpha$. За умовою (iii), $\alpha = \alpha_1 + 1$ для деякого ординала $\alpha_1 < |G|$. Значить, $g \in G_{\alpha_1+1} \setminus G_{\alpha_1}$, а тому існують $g_1 \in G_{\alpha_1}$, $x_{\alpha_1} \in X_{\alpha_1}$, такі що $g = g_1 x_{\alpha_1}$. Якщо $g_1 \neq e$, ми виберемо ординал α_2, елементи $g_2 \in G_{\alpha_2+1} \setminus G_{\alpha_2}$, $x_{\alpha_2} \in X_{\alpha_2}$, такі що $g_1 = g_2 x_{\alpha_2}$. За скінченне число $s(g)$ кроків ми одержимо

$$g = x_{\alpha_{s(g)}} x_{\alpha_{s(g)-1}} \dots x_{\alpha_2} x_{\alpha_1}, \quad \alpha_{s(g)} < \dots < \alpha_1, \quad x_{\alpha_i} \in X_{\alpha_i}.$$

Зауважимо, що таке зображення g однозначне і покладемо

$$\gamma_1(g) = \alpha_1,\ \gamma_2(g) = \alpha_2, \dots, \gamma_{s(g)} = \alpha_{s(g)},\ \Gamma(g) = \{\gamma_1(g), \dots, \gamma_{s(g)}(g)\}.$$

Для кожного натурального числа n позначимо

$$D_n = \{g \in G : s(g) = n\}.$$

Підмножину A групи G назвемо k-великою справа (зліва), де k — кардинал, якщо знайдеться підмножина $F \subseteq G$, така що $G = FA$ ($G = AF$), $|F| < k$. Очевидно, що A k-велика справа (зліва) тоді і тільки тоді, коли A — велика підмножина в болеані $\mathcal{B}_r(G,k)$ (відповідно, $\mathcal{B}_l(G,k)$).

ТЕОРЕМА 0.11.9. *Нехай G — нескінченна група, k — нескінченний кардинал, $k \leq |G|$. Тоді групу можна розбити на k k-великих справа підмножин.*

ДОВЕДЕННЯ. Спочатку припустимо, що $|G| = k$. Якщо G зліченна, то $\mathcal{B}_r(G,k)$ метризовний і можемо застосувати теорему 0.11.8. Припустимо, що G незліченна і використаємо вказану вище фільтрацію. Для кожного $\alpha < |G|$ покладемо

$$F_\alpha = \{g \in G : \gamma_{s(g)}(g) = \alpha\}$$

і зазначимо, що $\{F_\alpha : \alpha < |G|\}$ — диз'юнктна сім'я k-великих справа підмножин групи G.

Якщо ж $k < |G|$, ми виберемо підгрупу H групи G потужності k. За доведеним існує розбиття $\mathcal{P}$ групи H, таке що кожна підмножина $P \in \mathcal{P}$ є великою в $\mathcal{B}_r(H, k)$. Розкладемо G на праві суміжні класи по H і зафіксуємо деяку множину X представників цих класів, $G = HX$. Тоді $\{PX : P \in \mathcal{P}\}$ — диз'юнктна сім'я k-великих справа підмножин групи G. $\square$

Для $k = \aleph_0$ в лекції "Квазіцикли і квазіпромені“ ми істотно посилимо теорему 0.11.9 і доведемо що G можна розбити на зліченне число підмножин, кожна з яких є k-великою як зліва, так і справа. Невідомо, чи вірне це твердження для довільного кардиналу $k \leq |G|$.

Для кардинала k болеан $\mathcal{B} = (X, P, B)$ назвемо *k-корозкладним,* якщо X можна покрити k малими підмножинами. Корозкладність $\mathcal{B}$ — це кардинал

$$\operatorname{cores} \mathcal{B} = \min\{k : \mathcal{B} \text{ є } k\text{-розкладним}\}.$$

Підмножина $Y \subseteq X$ називається *обмеженою,* якщо існують $x \in X$, $\alpha \in P$, такі що $Y \subseteq B(x, \alpha)$. Якщо носій X болеану $\mathcal{B}$ обмежений, $\mathcal{B}$ також називається обмеженим. Припустимо, що $\mathcal{B}$ необмежений і зв'язний. Тоді кожна обмежена підмножина в X мала. Оскільки в цьому випадку $X = \cup\{B(x, \alpha) : \alpha \in P\}$ для довільного $x \in X$, то $\operatorname{cores} \mathcal{B} \leq \operatorname{cf} \mathcal{B}$. Зокрема, $\operatorname{cores} \mathcal{B}(X, d) \leq \aleph_0$ для довільного необмеженого метричного простору (X, d). З іншого боку за теоремою 0.11.4 сім'я усіх малих підмножин довільного болеану є ідеалом в булевій алгебрі усіх підмножин, а тому $\operatorname{cores} \mathcal{B} \geq \aleph_0$ для довільного неомеженого болеану. Таким чином, $\operatorname{cores} \mathcal{B}(X, d) = \aleph_0$ для довільного неомеженого метричного простору (X, d). За наступною теоремою корозкладність $\operatorname{cores} \mathcal{B}$ може вияавитись значно меншою за конфінальність $\mathcal{B}$.

Теорема 0.11.10. *Нехай G — нескінченна група, k — нескінченний кардинал, $k \leq |G|$. Якщо $k < \operatorname{cf} |G|$, то* $\operatorname{cores} \mathcal{B}_r(G, k) = \aleph_0$.

Доведення. Якщо G зліченна, то $\mathcal{B}_r(G,k)$ метризований. Притпустимо, що G незліченна і використаємо фільтрацію. Зауважимо, що $G \setminus \{e\} = \bigcup\limits_{n=1}^{\infty} D_n$, зафіксуємо натуральне число n і покажемо, що D_n мала в $\mathcal{B}_r(G,k)$. Візьмемо довільну підмножину $F \in \mathcal{F}(G,k)$. За припущенням $k < \mathrm{cf}\,|G|$ існує $\beta < |G|$, таке що $F \subseteq G_\beta$, а тому $FD_n \subseteq G_\beta D_n$. Ми покажемо, що $G \setminus G_\beta D_n$ $\aleph_0$-мала справа. Виберемо елементи $a_1, \ldots, a_{n+1} \in G$, такі що

$$a_1 \in G_{\beta+1} \setminus G_\beta, a_2 \in G_{\beta+2} \setminus G_{\beta+1}, \ldots, a_{n+1} \in G_{\beta+n+1} \setminus G_{\beta+n}.$$

Візьмем довільний елемент $g \in G_\beta D_n$ і покладемо $g = g_0$. Якщо $\beta + n \in \Gamma(g)$, покладемо $\epsilon_0 = 0$, в іншому разі $\epsilon_0 = 1$. Зауважимо, що $\beta + n \in \Gamma(a_{n+1}^{\epsilon_0} g_0)$ і покладемо $g_1 = a_{n+1}^{\epsilon_0} g_0$. Якщо $\beta + n - 1 \in \Gamma(g_1)$, позначимо $\epsilon_1 = 0$, інакше $\epsilon_1 = 1$. Зауважимо, що $\{\beta + n - 1, \beta + n\} \subseteq \Gamma(a_{n+1}^{\epsilon_1} g_1)$ і покладемо $g_2 = a_n^{\epsilon_1} g_1$. Після $n + 1$ кроків ми одержимо

$$\{\beta, \beta + 1, \ldots, \beta + n\} \subseteq \Gamma(a_1^{\epsilon_n} a_2^{\epsilon_{n-1}} \ldots a_{n+1}^{\epsilon_0} g).$$

Звідси випливає, що $a_1^{\epsilon_n} \ldots a_{n+1}^{\epsilon_0} g \notin G_\beta D_n$. Покладемо $A = \{e, a_1, a_2, \ldots, a_{n+1}\}$, $K = A^n$. Ми показали, що $G_\beta D_n \subseteq K^{-1}(G \setminus G_\beta D_n)$. Отже, $G = K^{-1}(G \setminus G_\beta D_n)$ і підмножина $G \setminus G_\beta D_n$ $\aleph_0$-велика справа. □

Теорема 0.11.11. *Нехай X — множина, φ — фільтр на X, такий що $\cap\varphi = \emptyset$. Тоді* $\mathrm{res}\,\mathcal{B}(X,\varphi) = 1$, $\mathrm{cores}\,\mathcal{B}(X,\varphi) = \min\{|\psi| : \psi \subseteq \varphi, \cap\psi = \emptyset\}$.

Доведення. Доведення випливає з двох простих спостережень. Підмножина $Y \subseteq X$ велика тоді і тільки тоді, коли $Y \in \varphi$. Підмножина $Y \subseteq X$ мала тоді і тільки тоді, коли підмножина $X \setminus Y$ велика. □

Ми завершимо цю лекцію теоремою про розбиття кульової структури на підмножини, щільні відносно сім'ї усіх великих підмножин. Нехай $\mathcal{B} = (X, P, B)$ — кульова структура, $\mathcal{L}$ — сім'я усіх великих підмножин з X. Підмножину $A \subseteq X$ ми називаємо $\mathcal{L}$-щільною, якщо $A \cap L \neq \emptyset$ для всіх $L \in \mathcal{L}$, еквівалентною, $\mathrm{Int}(A, \alpha) \neq \emptyset$ для всіх $\alpha \in P$.

Лема 0.11.12. *Нехай* $\mathcal{B}(X, P, B)$ *— кульова структура. Припустимо, що існують конфінальна лінійно впорядкована послідовність* $(\alpha_n)_{n \in \omega}$ *елементів з* P *і послідовність* $(x_n)_{n \in \omega}$ *елементів з* X*, така що сім'я* $\{B^*(x_n, \alpha_n) : n \in \omega\}$ *диз'юнктна. Тоді* X *можна розбити на зліченне число* $\mathcal{L}$*-щільних підмножин.*

Доведення. Розіб'ємо ω на зліченне число нескінченних підмножин $\omega = \cup_{k \in \omega} W_k$. Достатньо переконатися, що підмножина $A_k = \cup_{n \in W_k} B^*(x_n, \alpha_n)$ $\mathcal{L}$-щільна для кожного $k \in \omega$. Візьмемо довільну велику підмножину $L \subseteq X$ і виберемо $\alpha \in P$ так, що $X = B(L, \alpha)$. Виберемо $n \in W_k$ так, що $\alpha_n > \alpha$. Оскільки, $X = B(L, \alpha)$, то $x_n \in B(L, \alpha_n)$ і $B^*(x_n, \alpha_n) \cap L \neq \emptyset$. Значить, $L \cap A_k \neq \emptyset$. ☐

Теорема 0.11.13. *Нехай* $\mathcal{B} = (X, P, B)$ *— кульова структура, така що множина* X *нескінченна, а всі кулі* $B(x, \alpha)$, $B^*(x, \alpha)$, $x \in X$, $\alpha \in P$ *скінченні. Якщо існує конфінальна лінійно впорядкована послідовність* $(\alpha_n)_{n \in \omega}$ *в* P*, то* X *можна розбити на зліченне число* $\mathcal{L}$*-щільних підмножин.*

Доведення. Для того, щоб застосувати лему 0.11.12 ми побудуємо індуктивно послідовність $(x_n)_{n \in \omega}$ в X, таку що сім'я куль $\{B^*(x_n, \alpha_n) : n \in \omega\}$ диз'юнктна. Виберемо довільний елемент $x_0 \in X$. Припустимо, що ми вже вибрали елементи $x_0, \dots, x_n$, такі що кулі $B^*(x_0, \alpha_0), \dots, b^*(x_n, \alpha_n)$ попарно не перетинаються. Покладемо $Y = B^*(x_0, \alpha_0) \cup \dots \cup B^*(x_n, \alpha_n)$.

За припущенням, куля $B(Y, \alpha_{n+1})$ скінченна. Виберемо довільний елемент $x_{n+1} \in X \setminus B(Y, \alpha_{n+1})$. Тоді $B^*(x_{n+1}, \alpha_{n+1}) \cap Y = \emptyset$. $\square$

Бібліографія

[1] Dranishnikov A. Asymptotic topology/ Russian Math. Surveys 55 (2000), 1085-1129.
[2] Dranishnikov A., Zarichnyi M. Universal spaces for asymptotic dimention, manuscript.
[3] Harpe P. Topics in Geometrical Group Theory, University Chicago Press, 2000.
[4] Hewitt E. A problem of set-theoretic topology, Duke Math. J., 10 (1943), 309-333.
[5] Mitchener P. Coarse Homology Theories, Geom. Topology, 1 (2001), 271-297.
[6] Protasov I., Banakh T. Ball Structures and Colorings of Graphs and Groups, Mat. Stud. Monogr. Ser., VNTL, Lviv, Vol. 11, 2003.
[7] Protasov I. Normal ball structures, Mat Stud., 20 (2003) 3-16.
[8] Protasov I. Morphisms of ball structures of groups and graphs, Ukr. Math. J., 53 (2002), 847-855.
[9] Protasov I. Coronas of balleans, Topol. Appl., 149(2005), 149-160
[10] Protasov I. Resolvability of ball structures, Applied General Topology., 5(2004), 191-198
[11] Protasov I., Protasova O. Sketch of group balleans, Mat. Stud., 22(2004), 10-20
[12] Бурбаки Н. Общая топология, т. 3, М., "Наука 1975.
[13] Энгелькинг Р. Общая топология. М., "Мир".

0.12. Квiзiцикли i квазiпромені

Нехай $\mathrm{Gr}(V, E)$ — скінченний зв'язний граф з множиною вершин V і множиною ребер E. Для будь-яких двох вершин

$x, y \in V$, позначимо через $d(x, y)$ — довжину найкоротшого шляху від x до y. Граф $\mathrm{Gr}(V, E)$ називають *гамільтоновим,* якщо існує впорядкування множини його вершин $V = \{x_1, \ldots, x_n\}$, таке що

$$d(x_1, x_2) = d(x_2, x_3) = \cdots = d(x_{n-1}, x_n) = d(x_n, x_1).$$

Гамільтоновість має таку зоологічну інтерпретацію. Візьмемо гусінь і помістимо її в одну з вершин гамільтонового графу. Добре поміркувавши, гусінь може здійснити подорож по ребрах графу так, щоб в кожній вершині побувати рівно один раз і повернутись в початкову вершину. Зрозуміло, що далеко не кожен зв'язний граф гамільтонів, наприклад, серед дерев гамільтоновими є лише одноелеметні, та двоелеметні дерева. Ще тридцять років тому вважалося, що задача описання гамільтонових графів є одною з основних проблем терії графів (див. наприклад, [**12**], [**13**]) На цьому шляху було одержано багато як необхідних, так і достатніх ознак гамільтоновості. Одну з найперших достатніх умов дає теорема Дірака: граф гамільтонів, якщо кожна вершина з'єднана принаймні з половиною усіх вершин графу. Насьогодні проблема гамільтоновості залишається відкритою, але сподівання на її можливий розв'язок стали примарними після того, як було доведено NP-повноту задачі тестування графу на гамільтоновість.

Повернімося до зоології і припустімо, що замість гусіні ми маємо справу з коником-стрибунцем. Нехай можливості коника такі, що за один стрибок з будь-якої вершини він може переміститися в сусідню вершину, а такиж у вершину віддалену від даної, на відстань 2 або 3. Виявляється, що наш коник може простribати через усі вершини по одному разу в будь-якому скінченному звязному графі. Неважко перейти від зоологічних до математичних формулювань.

Впорядковану послідовність вершин $V = \{x_1, \dots, x_n\}$ зв'язного графу $\mathrm{Gr}(V, e)$ назвімо *квазіциклом* (або *циклом коника*), якщо

$$d(x_1, x_2) \leq 3, d(x_2, x_3) \leq 3, \dots, d(x_{n-1}, x_n)] \leq 3, d(x_n, x_1) \leq 3.$$

ТЕОРЕМА 0.12.1 (про коника). *Для будь-яких двох суміжних вершин x, y довільного скінченного зв'язного графу $\mathrm{Gr}(V, E)$ існує квазіцикл, що розпочинаєтьcя в вершині x і закінчуєтьcя в вершині y.*

ДОВЕДЕННЯ. Оскільки граф $\mathrm{Gr}(V, E)$ має кістяк (=остовне дерево), в якому вершини x, y теж інцидентні, ми можемо вважати, що наш граф є деревом. Застосуємо індукцію по числу n вершин дерева. Для $n = 2$ твердження очевидне. Припустімо, що ми довели теорему для дерев з числом вершин $< n$ і нехай $|V| = n$. Видалимо ребро (x, y) і одержимо два дерева $\mathrm{Gr}_x, \mathrm{Gr}_y$ з коренями x та y.

Випадок 1: x — кінцева вершина графу $\mathrm{Gr}(V, E)$. Нехай z — довільна вершина графу Gr_y, суміжна з y. За припущенням індукції в Gr_y існує квазіцикл $x_2, \dots, x_n$, такий що $x_2 = z, x_n = y$. Тоді $x_1, x_2, \dots, x_n$ — квазіцикл в $\mathrm{Gr}(V, E)$, де $x_1 = x$.

Випадок 2: x не є кінцевою вершиною графу $\mathrm{Gr}(V, E)$. Якщо y — кінцева вершина графу $\mathrm{Gr}(V, E)$, ми повертаємось до першого випадку. Отже, графи $\mathrm{Gr}_x, \mathrm{Gr}_y$ за припущенням індукції мають квазіцикли $x_1, \dots, x_k$ та $y_1, \dots, y_m$, що починаються в вешинах x, y і закінчуються в суміжних до x, y вершинах x_k та y_k. Тоді $x_1, \dots, x_k, y_m, \dots, y_1$ — квазіцикл в графі $\mathrm{Gr}(V, E)$. $\square$

Ін'єктивну послідовність $(x_n)_{n \in \omega}$ вершин нескінченного зв'язного графу ми назвемо *квазіпроменем,* якщо $d(x_n, x_n{+}1) \leq 3$ для всіх $n \in \omega$, а граф в якому є квазіпромінь, що проходить через усі його вершини — qr-*графом.* Далеко не кожен зліченний зв'язний граф є qr-графом, проте кожен зліченний зв'язний граф можна розкласти на квазіпромені. Далі для довільної підмножини A вершин графу $\mathrm{Gr}(V,E)$ через $\mathrm{Gr}[A]$ ми позначаємо індукований підграф графу $\mathrm{Gr}(V,E)$ з множиною вершин A і множиною ребер $E\cap(A\times A)$.

ТЕОРЕМА 0.12.2 (про квазіпромені). *Нехай* $\mathrm{Gr}(V,E)$ *— зліченний зв'язний граф. Тоді існує розбиття* $\mathcal{A}$ *множини* V *на скінченне або зліченне число підмножин, таке що для кожної підмножини* $A\in\mathcal{A}$

(i) $\mathrm{Gr}[A]$ *зв'язний;*

(ii) $\mathrm{Gr}[A]$ — qr-*граф.*

ДОВЕДЕННЯ. Знову ж, ми можемо вважати наш граф деревом. Зафіксуємо довільну вершину $x\in V$ і назвемо її коренем. Для кожного натурального числа i позначимо через S_i множину усіх вершин дерева, відстань від яких до кореня дорівнює i. Позначимо через S_i' множину усіх вершин $y\in S_i$, через які проходить скінченне число шляхів від кореня x, $S_i''=S_i\setminus S_i'$.

Випадок 1. Множина S_1' скінченна, $S_1'=\{y_1,\dots,y_n\}$. Нехай $T_1,\dots,T_n$ — скінченне дерева з коренями $y_1,\dots,y_n$, одержані видаленням ребер $(x,y_1),\dots,(x,y_n)$. Нехай $V_1,\dots,V_n$ — множини вершин дерев $T_1,\dots,T_n$, $X=\{x\}\cup V_1\cup V_2\cup\dots\cup V_n$. Зафіксуємо довільну вершину $y\in S_1'$. Якщо $S_1'=\emptyset, y=x$. За теоремою про коника існує квазіцикл $x_1,\dots,x_k$, що проходить через усі вершини графу $\mathrm{Gr}[X]$, такий що $x_1=x, x_k=y$. Для того, щоб продовжити цей квазіцикл до квазіпроменя, ми виберемо довільну вершину $z\in S_1''$ і повторимо побудову для дерева з коренем z, одержаного вилученням ребра (x,z).

Випадок 2. S_1' нескінченна, $S_1'=\{y_n : n\in\omega\}$. Позначмо через T_n дерево з коренем y_n, одержане вилученням ребра (x,y_n). Нехай V_n — множина вершин дерева T_n, $X=\{x\}\cup$

$\bigcup_{n\in\omega} V_n$. Застосовуючи теорему про коника, через зліченне число кроків ми побудуємо квазіпромінь, що проходить через усі вершини зв'язного графу $\mathrm{Gr}[X]$.

Таким чиним ми маємо квазіпромінь з початком x. Видаляємо усі вершини цього квазіпроменя разом з інцидентними їм ребрами. Якщо залишилася хоча б одна невидалена вершина, виберемо найменше число i, таке що S_i'' не входить до квазіпроменя. Зауважимо, що $S_i' = \emptyset$. Виберемо довільну вершину $z \in S_i''$, що не є вершиною квазіпроменя і повторимо побудову для дерева з коренем z. $\square$

Для випадку довільних нескінченних графів теорему про розклад на квазіпромені можна скоригувати так.

ТЕОРЕМА 0.12.3. *Нехай* $\mathrm{Gr}(V,E)$ *— нескінченний зв'язний граф. Тоді існує розбиття* $\mathcal{A}$ *множини* V *на зліченні підмножини, таке що для довільної підмножини* $A \in \mathcal{A}$

(i) $\mathrm{Gr}[A \cup \{x\}]$ *зв'язний для деякої вершини* $x \in V$*;*

(ii) $\mathrm{Gr}[A \cup \{x\}]$ — qr-*граф з квізіпрменем, що починається в вершині* x.

Нехай $\mathcal{F}, \mathcal{F}'$ — розбиття деякої множини X, $\mathcal{F}'$ називають *укрупненням* розбиття $\mathcal{F}$, якщо кожен блок розбиття $\mathcal{F}'$ є об'єднанням блоків розбиття $\mathcal{F}$.

ТЕОРЕМА 0.12.4 (про обмежені розбиття графів). *Для довільного нескінченного зв'язного графу* $\mathrm{Gr}(V,E)$ *існує злічена сім'я* $\{\mathcal{F}_n : n \in \omega\}$ *розбиттів множини* V*, така що для довільних* $n, m \in \omega$

(i) $|F| = n+1$ *і* $\operatorname{diam} F \leq 3n$ *для всіх* $F \in \mathcal{F}_n$*;*

(ii) *якщо* $n+1 | m+1$*, то* $\mathcal{F}_m$ *є укрупненням розбиття* $\mathcal{F}_n$.

ДОВЕДЕННЯ. Скористаймось розбиттям $\mathcal{A}$ з попердньої теореми. Для кожної підмножини $A \in \mathcal{A}$ виберемо квазіпромінь $(x_n)_{n\in\omega}$, що проходить через усі вершини з A. Розіб'ємо цей квазіпромінь на відрізки

$$\{x_1, x_1, \dots, x_n\}, \{x_{n+1}, x_{n+2}, \dots, x_{2n+1}\}, \{x_{2n+2}, x_{2n+3}, \dots, x_{3n+2}\}, \dots$$

і віднесемо кожен з цих відрізків до розбиття $\mathcal{F}_n$. $\square$

Для застосування цієї теореми до груп нам потрібно означення *графу Келлі* $\mathrm{Cay}(G, S)$ групи G, визначеного деякою підмножиною $S \subseteq G, S = S^{-1}, e \in S$, e — одиниця групи. Множиною вершин графу $\mathrm{Cay}(G, S)$ є G, а дві вершини $x, y \in G$ з'єднано ребром тоді і лише тоді, коли $xy^{-1} \in S$.

ТЕОРЕМА 0.12.5 (про обмежені розбиття груп). *Нехай G — нескінченна група з одиницею e, S — скінченна підмножина G, що породжує нескінченну підгрупу, $S = S^{-1}$, $e \in S$. Тоді існує зліченна сім'я розбиттів $\{\mathcal{F}_n : n \in \omega\}$ групи G, така що для довільних $n, m \in \omega$*

(i) $|F| = n + 1$ *і* $xy^{-1} \in S^{3n}$ *для всіх* $x, y \in F, F \in \mathcal{F}_n$;

(ii) *якщо* $n + 1 | m + 1$, *то* $\mathcal{F}_m$ *є укрупненням* $\mathcal{F}_n$.

ДОВЕДЕННЯ. Для побудови сім'ї $\{\mathcal{F}_n : n \in \omega\}$ ми можемо безпосередньо застосувати теорему про обмежені розбиття графів до кожної зв'язної компоненти графу $\mathrm{Cay}(G, S)$. $\square$

Підмножину X групи S називають *великою зліва(справа)*, якщо існує скінченна підмножина $F \subseteq G$, така що $G = FX$ $(G = XF)$. Підмножину називають *великою*, якщо вона велика зліва та справа. А. Бела та В. Малихін [**1**] поставили таке запитання: чи можна кожну нескінченну групу розбити на дві великі підмножини?

ТЕОРЕМА 0.12.6 (про розбиття груп на великі підмножини). *Кожну нескінченну групу G можна розбити на зліченне число великих підмножин.*

Доведення. Спочатку ми припустимо, що в групі G є скінченна підмножина S, $S = S^{-1}$, $e \in S$, що породжує нескінченну підгрупу. Доведемо, що існує розбиття $G = \bigcup_{n\in\omega} X_n$, таке що

$$G = S^{3\cdot 2^n} X_n = X_n S^{3\cdot 2^n}$$

для всіх $n \in \omega$. Нехай $\{\mathcal{F}_n : n \in \omega\}$ — сім'я розбиттів групи G з попередньої теореми. Позначимо $\mathcal{A}_0 = \mathcal{F}_1$, $\mathcal{A}'_0 = \{F^{-1} : F \in \mathcal{A}_0\}$. Оскільки всі підмножини розбиттів $\mathcal{A}_0, \mathcal{A}'_0$ мають однакову потужність, за теоремою про спільну трансверсаль існує підмножина $X_0 \subset G$, така що $|X_0 \cap F| = |X_0 \cap F^{-1}| = 1$ для всіх $F \in \mathcal{A}_0$. Видалимо X_0 з G і позначмо $\mathcal{A}_1 = \{F \setminus X_0 : F \in \mathcal{F}_2\}$, $\mathcal{A}'_1 = \{F^{-1} : F \in \mathcal{A}_1\}$. До розбиттів $\mathcal{A}_1, \mathcal{A}'_1$ множини $G \setminus X_0$ застосуємо теорему про спільну трансверсаль і виберемо підмножину $X_1 \subseteq G \setminus X_0$, таку що $|X_1 \cap F| = |X_1 \cap F^{-1}|$ для всіх $F \in \mathcal{A}_1$. Видалимо X_1 з $G \setminus X_0$ і позначмо $\mathcal{A}_2 = \{F \setminus (X_0 \cup X_1) : F \in \mathcal{F}_4\}$, $\mathcal{A}'_2 = \{F^{-1} : F \in \mathcal{A}_2\}$. Знаходимо спільну трансверсаль X_2 розбиттів $\mathcal{A}_2, \mathcal{A}'_2$ і т. д.

Лишилося розглянути випадок, коли кожна скінченна підмножина групи G породжує скінченну підгрупу. Нехай $H_0 \subset H_1 \subset \dots$ — зростаючий ланцюжок скінченних підгруп G, $|H_0| > 1$. Для кожного $n \in \omega$ нехай $\mathcal{F}_n, \mathcal{F}'_n$ — розбиття G на ліві та праві суміжні класи за підгрупою H_n. Послідовно застосовуючи трансверсальні аргументи до розбиттів $\mathcal{F}_n, \mathcal{F}'_n$, ми побудуємо розбиття $G = \bigcup_{n\in\omega} X_n$, таке що $G = H_n X_n = X_n H_n$ для всіх $n \in \omega$. □

Оскільки кожен нескінченний зв'язний шраф розбивається на qr-графи, природньо виникає запитання про структуру qr-графів. Ми дамо повну відповідь для локально скінченних графів і вкажемо часткові результати щодо загального випадку, а розпочнемо з дерев.

Ін'єктивну послідовність $(x_n)_{n\in\omega}$ вершин графу $\mathrm{Gr}(V,E)$ називають *променем,* якщо $d(x_n, x_{n+1}) = 1$ для всіх $n \in \omega$. За лемою Кьонінга будь-який нескінченний локально скінченний граф має промінь. Граф називається *локально-скінченним,* якщо з кожної його вершини виходить скінченне число ребер.

Промінь $(X_n)_{n\in\omega}$ в дереві $\mathrm{Tr}(V,E)$ називають *стовбуром,* якщо після вилучення множини вершин $\{x_n\}_{n\in\omega}$ дерево розпадається на скінченні дерева. Дерево, в якому є стовбур, назвімо деревом зі стовбуром.

ТЕОРЕМА 0.12.7 (про локально скінченні qr-дерева). *Локально скінченне дерево* $\mathrm{Tr}(V,E)$ *є* qr-*деревом тоді і лише тоді, коли воно має стовбур.*

ДОВЕДЕННЯ. Нехай $\mathrm{Tr}(V,E)$ — qr-дерево. Скористаймося лемою Кьонінга і виберемо промінь $(x_n)_{n\in\omega}$ в $\mathrm{Tr}(V,E)$. Позначмо через U множину усіх вершин з $V \setminus \{x_n : n \in \omega\}$, що суміжні з вершинами променя $(x_n)_{n\in\omega}$. Для кожної вершини $y \in U$, нехай Tr_y — дерево з коренем y, одержане вилученням ребра (y, x_m), де x_m — вершина, суміжна з y. Припустімо, що існує вершина $z \in U$, така що дерево Tr_z нескінченне. Нехай x_i — вершина променя, суміжна з z. Оскільки $\mathrm{Tr}(V,E)$ — qr-граф існує нумерація $\{v_n : n \in \omega\}$ множини V, така що $d(v_n, v_{n+1}) \le 3$ для всіх $n \in \omega$. Виберемо $s \in \omega$ так, що $B(x_i, 2) \subseteq \{v_1, \dots, v_s\}$, де $B(x,r) = \{y \in V : d(x,y) \le r\}$. Оскільки дерево Tr_z нескінченне, ми можемо вибрати $t > z$ так, що $v_t \in \mathrm{Tr}_z$. Але тоді

$$\{v_t, v_{t+1}, \dots\} \cap \{x_n : n \in \omega\} = \emptyset,$$

що суперечить вибору $\{v_n : n \in \omega\}$.

Нехай $\mathrm{Tr}(V,E)$ — дерево зі стовбуром $(x_n)_{n\in\omega}$. Нехай T_0 — дерево з коренем x_0, одержане вилученням ребра (x_0, x_1). Для кожного $n \in \omega$, $n > 0$ позначимо через T_n дерево з коренем x_n, одержане вилученням ребер (x_{n-1}, x_n), (x_n, x_{n+1}).

Якщо $|V(T_n)| = 1$, покладемо $x'_n = x_n$. Якщо $|V(T_n)| > 1$, ми виберемо деяку вершину $x'_n \in V(T_n)$, суміжну з x_n. Нехай $|V(T_n)| = k_n$, $n \in \omega$. За теоремою про коника, для кожного $n \in \omega$ існує біекція $f_n : \{1, \ldots, k_n\} \to V(T_n)$, така що $f_n(1) = x'_n$, $f_n(k_n) = x_n$ і $d(f_n(i), f_n(i+1)) \leq 3$ для всіх $i \in \{1, \ldots, k_n - 1\}$.

Означмо біекцію $f : \mathbb{N} \to V$ за правилом $f(i) = f_n(i - \sum_{j<n} k_i)$, якщо $\sum_{j<n} k_j < i < \sum_{j \leq n} k_j$. Оскільки відстань між x_n та x'_{n+1} не перевищує 2, $(f(i))_{i \in \mathbb{N}}$ — квазіпромінь, що проходить через усі вершини дерева $\mathrm{Tr}(V, E)$ і $\mathrm{Tr}(V, E)$ — qr-граф. ☐

Нехай $\mathrm{Tr}(V, E)$ — дерево з зафіксованим коренем x, назвімо його $x-$кореневим. Означмо частковий порядок $\leq$ на множині $V : y \leq z$ тоді і лише тоді, коли найкоротший шлях від x до z проходить через y.

Назвімо x-кореневий кістяк Tr графу Gr *нормальним,* якщо для кожної пари y, z суміжних вершин Gr $x < y$ або $y < x$, де $\leq$ — частковий порядок на множині вершин графу Gr, визначений деревом Tr.

Ми покажемо, що кожен скінченний зв'язний граф $\mathrm{Gr}(V, E)$ має нормальний кістяк. Для кожної вершини $x \in V$, нехай

$$\sigma(\mathrm{Gr}, x) = \sum_{y \in V} d(x, y)$$

Кістяк графу $\mathrm{Gr}(V, E)$ з максимальним значенням $\sigma(\mathrm{Tr}, x)$ назвімо *σ-кореневим.* Ми покажемо, що цей кістяк $\mathrm{Tr} = \mathrm{Tr}(V, E')$ є нормальним. Припустімо супротивне і візьмемо дві вершини $u, v \in V$, такі що $(u, v) \in E$ але u, v непорівнювані в частковому порядку, визначеному деревом $\mathrm{Tr}(V, E')$. Нехай $d(u, x) \geq d(v, x)$, де d — відстань в графі $\mathrm{Tr}(V, E')$. Візьмемо вершину $v' \in V$, таку що $(v, v') \in E'$ і $d(x, v') = d(x, v) - 1$. Видалимо ребро (v, v') з E' і додамо нове ребро $(u, v) \in E$.

Таким чином, ми одержали x-кореневий кістяк Tr', такий що $\sigma(\mathrm{Tr}', x) > \sigma(\mathrm{Tr}, x)$, суперечність.

Схожими міркуваннями [**6**, Theorem 3.15] можна довести існування нормального кореневого дерева в будь-якому локально скінченному зв'язному графі.

ТЕОРЕМА 0.12.8 (про локально скінченні qr-графи). *Для довільного нескінченного локально скінченного графу* $\mathrm{Gr}(V, E)$ *такі умови рівносильні:*

(i) $\mathrm{Gr}(V, E)$ — qr-*граф;*

(ii) *існують натуральне число* m *і біекція* $f : \omega \to V$, *такі що* $d(f(i), f(i+1)) \le m$ *для всіх* $i \in \omega$*;*

(iii) $\mathrm{Gr}(V, E)$ *має нормальний кореневий кістяк, що є деревом зі стовбуром;*

(iv) *кожен нормальний кореневий кістяк графу* $\mathrm{Gr}(V, E)$ *є деревом зі стовбуром.*

ДОВЕДЕННЯ. (i)⇒(ii) випливає з означення qr-графу.

(ii)⇒(iv). Нехай $\{v_n : n \in \omega\}$ — нумерація V, така що $d(v_i, v_{i+1}) \le m$ для всіх $i \in \omega$. Нехай $\mathrm{Tr}(V, E')$ — нормальний x_0-кореневий кістяк $\mathrm{Gr}(V, E)$. Користуючись лемою Кьонінга, виберемо промінь $(x_n)_{n\in\omega}$ в $\mathrm{Tr}(V, E')$ з початком x_0. Позначмо через U множину усіх вершин дерева $\mathrm{Tr}(V, E')$ з $V \setminus \{x_n : n \in \omega\}$, суміжних до вершин з $\{x_n : n \in \omega\}$. Для кожної вершини $y \in U$ ми виберемо вершину x_m, таку що $(y, x_m) \in E'$ і позначмо через T_y дерево з коренем y, одержане вилученням ребра (x_m, y). Припустімо, що дерево T_z нескінченне для деякої вершини $z \in U$. Виберемо x_i так, що $(x_i, z) \in E'$. Оскільки граф $\mathrm{Gr}(V, E)$ локально скінченний, множина $B(\{x_0, \ldots, x_i\}, m)$ скінченна, де $B(A, m) = \cup_{\alpha\in A} B(a, m)$. Виберемо $t \in \omega$ так, що

$$B(\{x_0, \ldots, x_i\}, m) \subseteq \{v_0, \ldots, v_t\}, v_t \in T_z.$$

З нормальності $\mathrm{Tr}(V, E')$ випливає $\{v_{t+1}, v_{t+2}, \dots\} \cap \{x_n : n \in \omega\} = \emptyset$, що суперечить вибору $\{v_n : n \in \omega\}$. Отже, кожне дерево $T_y, y \in U$ скінченне і $\mathrm{Tr}(V, E')$ — дерево зі стовбуром.

(iv)⇒(iii) очевидно.

(iii)⇒(i) випливає з теореми про qr-дерева. □

До цієї характеризації можна додати ще й таке твердження: нескінченний локально скінченний граф $\mathrm{Gr}(V, E)$ є qr-графом тоді і лише тоді, коли $\mathrm{Gr}(V, e)$ має один кінець, тобто граф $\mathrm{Gr}[V \setminus F]$ має лише одну нескінченну зв'язну компоненту для будь-якої скінченної підмножини $F \subset V$.

Проблема характеризації довільних qr-графів залишається відкритою. Ми наведемо без доведень кілька результатів0 стосовно цієї проблеми. Для нескінченного зв'язного графу $\mathrm{Gr}(V, E)$ позначимо через $U(\mathrm{Gr})$ множину вершин скінченного степеня, $W(\mathrm{Gr}) = V \setminus U(\mathrm{Gr})$.

1. Нехай $\mathrm{Gr}(V, E)$ — qr-дерево з непорожньою множиною $W(\mathrm{Gr})$. Тоді підграф $\mathrm{Gr}[W(\mathrm{Gr})]$ зв'язний, а кожна зв'язна компонента графу $\mathrm{Gr}[U(\mathrm{Gr})]$ скінченна.

2. Для довільного зліченного зв'язного графа Γ існує qr-граф Gr, такий що підграф $\mathrm{Gr}[W(\mathrm{Gr})]$ ізоморфний Γ. Якщо граф Γ є деревом, то за Gr теж можна взяти деяке дерево.

3. Нехай Tr — зліченне дерево з одноелементною множиною $W(\mathrm{Tr})$, $W(\mathrm{Tr}) = \{w\}$. Дерево Tr є qr-деревом тоді і тільки тоді, коли після видалення вершини w дерево розпадається на скінченні дерева.

4. Для довільного дерева $\mathrm{Tr}(V, E)$ і вершини $x \in V$ розглянемо множину U_x всіх вершин скінченного степеня, суміжних з вешиною x. Для кожної вершини $y \in U_x$ позначимо через T_y дерево з коренем y, одержане вилученням ребра (x, y).

Нехай Tr — зліченне дерево, $W = W(\mathrm{Tr})$, $|W| \geq 2$ і дерево $\mathrm{Tr}[W]$ локально скінченне. Дерево Tr є qr-графом тоді і лише тоді, якщо виконуються такі умови:

(i) граф $\mathrm{Tr}[W]$ зв'язний;

(ii) для кожної вершини $x \in W$ множина $\{T_y : y \in U_x\}$ складається зі скінченних дерев;

(iii) для кожної вершини $x \in W$ множина $\{T_y : y \in U_x\}$ містить нескінченну підмножину одноелеметних дерев або нескінченну підмножину дерев, кожне з яких T_y має кінцеву вершину, суміжну з коренем y.

Останнє твердження, зокрема, дає опис qr-дерев зі скінченною множиною вершин локальної нескінченності і розв'язує проблему 3.2 з [**6**].

І знову до зоології. Припустімо, що коник, демонструючи свою теорему на конкретному скінченному зв'язному графі, забив ніжку і втратив спроможність стрибати на відстань 3, а одним стрибком може перміщатися у вершину, віддалену на відстань 1 або 2.

Скінченний зв'язний граф $\mathrm{Gr}(V,E)$ ми назвемо *квазігамільтоновим,* якщо існує нумерація множини його вершин $x_1, x_2, \ldots, x_n$, така що

$$d(x_1,x_2) \leq 2, d(x_2,x_3) \leq 2, \ldots, d(x_{n-1},x_n) \leq 2, d(x_n,x_1) \leq 2.$$

Цю послідовність вершин назвімо *квазігамільтоновим циклом.* Отже, квазігамільтонові графи — це графи, в яких існують квазігамільтонові цикли. Зауважмо також, що граф Gr квазігамільтонів тоді і тільки тоді, коли його квадрат Gr^2 гамільтонів. До речі, теорема коника стверджує, зокрема, що куб кожного скінченного зв'язного графу гамільтонів. Саме в такій формі ця теорема вперше з'явилася у статті Карганіса [**4**], хоча за зізнанням автора він лише занотував відомий, дещо курйозніший, фолькльорний факт. Перші істотні застосування теореми коника з'явилися в статтях [**7**], [**8**], [**9**].

Звичайно не кожен скінченний граф квазігамільтонів. Так скінченне дерево Tr квазігамільтонове тоді і лише тоді, коли існує така ін'єктивна послідовність $x_0, x_1, \ldots, x_m$ його вершин, що $d(x_0, x_1) = \cdots = d(x_{m-1}, x_m) = 1$, і після видалення усіх цих вершин дерево Tr розпадається на одноелеметні дерева. Зоологічно квазігамільтонові дерева можна уявляти собі як сороконіжки.

Характеризація квазігамільтонових графів невідома. Найбільш глибоким результатом щодо цієї проблеми є теорема Флейшнера: кожен блок є квазігамільтоновим графом. Скінченний зв'язний граф називають блоком або двозв'язний графом, якщо він залишається зв'язним після видалення будь-якої його вершини. Доведеню цієї теореми Флейшнер прсв'ятив цикл статей, що завершився публікацією [**3**]. Дещо простіше доведення цієї теореми дав Ріха [**11**], це ж доведення продубльовано в підручнику [**2**]. Застосовуючи теорему Флейшнера можна довести квазігамільтоновість будь-якого зв'язного графу Келі скінченної грапи [**10**]. Ще один цікавий результат — теорема Мет'юза-Самнера [**5**]: скінченний зв'язний граф Gr квазігамільтонів, якщо Gr не містить індукованих підграфів, ізоморфних $K_{1,3}$, де $K_{1,3}$ — дерево з коренем і трьома кінцевими вершинами.

Ми вкажемо одну досить загальну конструкцію квазігамільтонових графів, з якої випливає, зокрема, квазігамільтоновість будь-якого реберного графу.

Нехай $\mathrm{Gr}_1(U_1, E_1), \ldots, \mathrm{Gr}_n(U_n, E_n$ — скінченні зв'язні графи, $\mathrm{Tr}(V, E)$ — дерево, що має n вершин, $V = \{v_1, \ldots, v_n\}$. Ми вважаємо, що підмножини $U_1, \ldots, U_n, V$ попарно не перетинаються. Припустимо також, що степінь $\rho(v_i)$ кожної вершини дерева Tr не перевищує числа вершин графу Gr_i, $\rho(v_i) \leq |U_i|$. Для кожного $i \in \{1, \ldots, n\}$ зафіксуємо $\rho(v_i)$ вершин $u_{i1}, \ldots, u_{i\rho(v_i)}$ графу Gr_i. Для кожного ребра (v_i, v_j) дерева Tr виберемо пару вершин u_{ik}, u_{js} і поєднамо їх ребром або ототожнимо. При цьому ми попіклуємось, щоб пари, що відповідають різним ребрам дерева не перетинались. В результаті ми отримаємо деякий зв'язний граф $\mathrm{Gr}(U, E')$, який назвемо *з'єднанням* графів $\mathrm{Gr}_1, \ldots, \mathrm{Gr}_n$ за деревом Tr. Взагалі кажучи, з фіксованого набору графів і фіксованого дерева можна отримати декілька з'єднань.

Кожна вершина $u \in U$ є вершиною одного з гафів Gr_i. Ми назвемо вершину u *ізольованою,* якщо вона є кінцевою вершиною графу $\mathrm{Gr}(U, E)$ або з неї виходять лише ребра до вершин з U_i. Покажемо, що з'єднання довільного набору скінченних зв'язних графів за довільним деревом має хоча б одну ізольовану вершину. Візьмемо кінцеву вершину v_k дерева Tr. Якщо $|U_k| > 1$, виберемо вершину u', що з'єднана з деякою вершиною з U_j, $j \neq k$. Тоді всі вершини з множини $U_k \setminus \{u'\}$ ізольовані.

ТЕОРЕМА 0.12.9 (про з'єднання). *Нехай* $\mathrm{Tr}(V, E)$ — *скінченне дерево,* $V = \{v_1, \ldots, v_n\}$, $\mathrm{Gr}_1(U_1, E_1), \ldots, \mathrm{Gr}_n(U_n, E_n)$ — *скінченні зв'язні графи, причому* $\rho(v_i) \leq |U_i|$ *для всіх* $i \in \{1, \ldots, n\}$. *Якщо графи* $\mathrm{Gr}_1, \ldots, \mathrm{Gr}_n$ *гамільтонові, то будь-яке їх з'єднання за деревом* Tr *є квазігамільтоновим графом.*

ДОВЕДЕННЯ. Ми доведемо дещо сильніше твердження: для кожної ізольованої вершини u з'єднання $\mathrm{Gr}(U, E')$ існує квазігамільтонів цикл, що починається в вершині u і закінчується в деякій вершині u', суміжній з вершиною u. Застосуємо індукцію по числу n. Для $n = 1$ теорема очевидна оскільки граф Gr_1 гамільтонів. Нехай ми вже довели теорему для всіх з'єднань за деревами з числом вершин $< n$.

Візьмемо ізольовану вершину u з'єднання $\mathrm{Gr}(U, E')$. За означенням з'єднання вершина u є вершиною деякого графа $\mathrm{Gr}_i(U_i, E_i)$. Зафіксуємо в цьому графі гамільтонів цикл $u_1, \ldots, u_k$, що починається в вершині u. Видалимо з графа $\mathrm{Gr}(U, E')$ всі ребра з множини E_i. Тоді граф розпадається на з'єднання графів за деревами з числом вершин $< n$. Позначимо через $\mathrm{Gr}(u_i)$ ту зв'язну компоненту, що містить вершину u_i. Оскільки вершина u ізольована і $u = u_1$, то $\mathrm{Gr}(u_1)$ одноелементний. За припущенням індукції в кожному з графів $\mathrm{Gr}(u_2), \ldots, \mathrm{Gr}(u_k)$ є квазігамільтонів цикл C_i, що починається в деякій вершині u'_i, суміжній з вершиною u_i, і закінчується в вершині u_i. Тоді $u, C_2, C_3, \ldots, C_k$ — кваігамільтонів цикл в $\mathrm{Gr}(U, E')$. □

Ми застосуємо теорему про з'єднання для доведення квазігамільтоновості реберного графу $L(\mathrm{Gr})$ довільного скінченного зв'язного графу $\mathrm{Gr}(V, E)$. Множиною вершин реберного графу є множина ребер E, а дві вершини з $L(\mathrm{Gr})$ поєднані ребрами тоді і тільки тоді, коли відповідні ребра в Gr мають спільну вершину. Спочатку припустимо, що $\mathrm{Gr}(V, E)$ — дерево, $V = \{v_1, \ldots, v_n\}$. Для кожної вершини $v_i \in V$ степеня $\rho(v_i)$ візьмемо повний граф $\mathrm{Gr}(U_i, E_i)$ з $\rho(v_i)$ вершинами. Тоді $L(\mathrm{Gr})$ є з'єднанням гамільтонових графів $\mathrm{Gr}(U_1, E_1), \ldots, \mathrm{Gr}(U_n, E_n)$ за деревом $\mathrm{Gr(V, E)}$ і працює теорема про з'єднання. Розглянемо загальний випадок. Якщо граф $\mathrm{Gr}(V, E)$ має цикл C, візьмемо дві суміжні вершини u, v цього циклу, видалимо ребро (u, v), але добавимо нове ребро (u, w), де $w \notin V$. Після такої перебудови множина вершин $L(\mathrm{Gr})$ не змінилась, а кількість ребер зменшилась. Цим трюком загальний випадок зводиться до дерева.

Ще одне застосування теореми про з'єднання. Для довільного скінченного зв'язного графу $\mathrm{Gr}(V, E)$ визначимо його граф розв'язок $R(\mathrm{Gr})$. Спочатку кожне ребро $(u, v) \in E$ замінимо на три ребра $(u, u'), (u', v'), (v', v)$, де вершини u', v' різні і не належать множині V. Крім того, нові вершини будемо визначати так, щоб пари u', v', що відповідають різним ребрам не перетинались. Далі видалимо кожну вершину $u \in V$, але поєднаємо циклом усі нові вершини, суміжні з вершиною

u. Одержаний граф позначмо $R(\mathrm{Gr})$ і доведемо його квазігамільтоновість. Якщо Gr є деревом, то $R(\mathrm{Gr})$ є з'єднанням циклів за деревом і працює теорема про з'єднання. Якщо Gr має цикл C, ми виберемо довільні суміжні вершини u, v цього циклу, замінимо ребро u на два ребра $(u, u_1), (v, v_1)$, де u_1, v_1 — нові вершини, які в одержаному графі є кінцевими. Якщо в графі розв'язок побудованого графа є квазігамільтонів цикл, то такий цикл є і у графі розв'язок початкового графу. Таким чином, і в цьому випадку маємо редукцію до дерев.

Серед відкритих проблем, що стосуються квазігамільтонових графів, наведених в [**6**], найбільш інтригуючою є запитання про NP-повноту алгоритмічної проблеми "Квазігамільтонів граф“.

Бібліоґрафія

[1] Bella A., Malykhin V. I. Small and other subsets of a group, Q and $\mathcal{A}$ in General Topology, 11 (1999), 183-187.

[2] Diestel R. Graph Theory, Graduate Text in Math., 173, Springer-Verlag, 2000.

[3] Fleishner H. The square of every 2-connected graph is Hamoltonian, J. Comb. Theory B, 16 (1974), 29-34.

[4] Karaganis J. On the cube of graph, Canad. Math Bull., 11 (1969), 295-296.

[5] Mathews M., Sumner D. Hamiltonian results in $K_{1,3}$-free graphs, J. Graph Theory, 8 (1984), 139-146.

[6] Protasov I., Banakh T. Ball Structures and Colorings of Graphs and Groups, Mat. Stud. Monogr. Ser., 11. VNTL, Lviv, 2003.

[7] Protasov I. V. Morphisms of ball structures of proups and graphs, Ukr. Math. J., 53 (2002), 847-855.

[8] Protasov I. V. Partitions of groups into large subsets, Math. Notes, 73 (2003), 443-446.

[9] Protasov I. V. Quasiray decompositon of graphs, Mat. Stud., 17 (2002), 220-222.

[10] Protasova K. D. On square-hamiltonian graphs, Algebra and Discrete Mathy.2005,N2

[11] Risha S. A new proof of the theorem of Heishner, J. Comb. Theory B, 52 (1991), 117-123.

[12] Орэ О. Теория графов, М., "Наука 1980.

[13] Харари Ф. Теория графов, М., "Мир 1973.

0.13. Калейдоскопічні графи і коди Хемінга

Нехай $\mathrm{Gr}(V, E)$ — зв'язний граф з множиною вершин V і множиною ребер E, $d(u, v)$ — довжина найкоротшого шляху між вершинами u та v. Для довільних $v \in V$, $r \in \omega = \{0, 1, \dots\}$, ми позначимо $B(v, r) = \{u \in V : d(v, u) \leq r\}$. Спочатку ми доведемо одну теорему про розфарбування графів, а після цього визначимо основне поняття в цій лекції — калейдоскопічність.

Теорема 0.13.1. *Нехай* Gr *— зв'язний граф,* r *— натуральне число,* $|V| \geq r$. *Тоді існує* r*-розфарбування* $\chi : V \to \{1, \dots, r\}$, *таке що кожна куля* $B(v, k)$, $v \in V$, $k \in \{0, 1, \dots, r-1\}$ *містить принаймні* $k+1$ *вершин, що пофарбовані різним кольорами.*

Доведення. Припустимо спочатку, що граф $\mathrm{Gr}(V, E)$ скінченний і має n вершин. Виберемо довільну вершину $a_1 \in V$ і покладемо $A_1 = \{a_1\}$. Далі візьмемо довільну вершину a_2, суміжну з a_1, і покладемо $A_2 = \{a_1, a_2\}$. Нехай вже вибрано вершини $a_1, \dots, a_n$, $m < n$ так , що кожен граф $\mathrm{Gr}[A_i]$, $i \in \{1, \dots, m\}$ зв'язний, де $A_i = \{a_1, \dots, a_i\}$. Для підмножини $A \subseteq V$ ми позначаємо через $\mathrm{Gr}[A]$ індукований підграф з множиною вершин A і множиною ребер $V \cap (A \times A)$. Оскільки граф $\mathrm{Gr}(V, E)$ зв'язний, серед вершин з множини $V \setminus A_m$ існують вершини, суміжні з деякими вершинами A_m. Виберемо одну з них, позначимо її a_{m+1} і покладемо $A_{m+1} = \{a_1, \dots, a_{m+1}\}$. Після n кроків ми отрамаємо деяке впорядкування $a_1, \dots, a_n$ множини V.

Пофарбуємо вершини $a_1, \dots, a_r$ різними кольорами: $\chi(a_1) = 1, \chi(a_2) = 2, \dots, \chi(a_r) = r$. Нехай для деякого $m < n$ ми вже пофарбували вершини $a_1, \dots, a_m$ так, що кожна куля в графі $\mathrm{Gr}[A_m]$ радіуса $k \in \{0, 1, \dots, r-1\}$ має вершини $k+1$ різних кольорів. Виберемо вершину $a \in A_m$, суміжну з вершиною

a_{m+1}. На першому кроці розглянемо кулю в графі $\mathrm{Gr}[A_m]$ з центром a радіуса $r-2$. За припущенням ця куля містить вершини принаймні $r-1$ різних кольорів. Якщо серед кольорів вершин цієї кулі немає деякого кольору $j \in \{1, \ldots, r\}$, покладемо $\chi(a_{m+1}) = j$. Якщо серед кольорів вершин кулі зустрічаються усі r кольорів, ми залишаємо на першому кроці вершину a_{m+1} непофарбованою, але зауважимо, що при будь-якому її розфарбуванні куля в графі $\mathrm{Gr}[A_{m+1}]$ з центром a_{m+1} радіуса $r-1$ містить вершини усіх r кольорів. Отже, припустимо що вершина a_{m+1} залишилася непофарбованою на першому кроці. На другому кроці розглядаємо кулю в графі $\mathrm{Gr}[A_m]$ з ценром a радіуса $r-3$. Ця куля за припущенням містить принаймні $r-2$ вершини різних кольорів. Якщо для розфарбування вершин цієї кулі використано рівно $r-2$ кольори, ми фарбуємо вершину a_{m+1} будь-яким з двох невикористаних кольорів. Якщо ж для розфарбування використано більше ніж $r-2$ кольорів, то на другому кроці ми залишаємо вершину a_{m+1} непофарбованою, але зауважуємо, що при довільному розфарбуванні цієї вершини, куль радіуса $r-2$ з центром a_{m+1} в $\mathrm{Gr}[A_{m+1}]$ містить вершини принаймні $r-1$ кольорів. Таких кроків ми можемо зробити щонайбільше $r-1$. Чи може статися, що вершина a_{m+1} залишилась непофарбованою після цих кроків? Ні, не може, адже якщо на передостанньому кроці ми не пофарбували a_{m+1}, то кожна куля з центром a в графі $\mathrm{Gr}[A_{m+1}]$ радіуса $k \in \{2, 3, \ldots, r-1\}$ містить вершини принаймні $k+1$ кольорів при будь-якому розфарбуванні a_{m+1}. А тому, на останньому кроці ми обов'язково пофарбуємо a_{m+1} одним з кольорів, відмінних від кольору вершини a.

Таким чином, ми одержали потрібне розфарбування вершин скінченного графа. Якщо ж наш граф нескінченний, то трансфінітною індукцією ми впорядкуємо множину вершин $V = \{a_\alpha : \alpha < \gamma\}$так, що кожен граф $\mathrm{Gr}[A_\alpha]$, $\alpha < \gamma$ зв'язний, де $A_\alpha = \{a_\beta : \beta < \alpha\}$. А далі ми розфарбовуємо послідовно вершини з V так само, як і для скінченного графа. □

В [**1**, Theorem 1.2] можна знайти доведення подібного але, значно делікатнішого твердження.

Теорема 0.13.2. *Нехай* $\mathrm{Gr}(V, E)$ *— скінченний зв'язний граф,* r *— натуральне число,* $r \le |V|$*. Тоді існує врівноважене* r*-розфарбування* $\chi : V \to \{1, \ldots, r\}$*, таке що кожна куля радіуса* r *мастить вершини усіх* r *кольорів.*

Якщо r — дільник n, врівноваженість означає, що число усіх вершин кожного кольору однакове. Якщо n не ділиться на r, то будь-які два з цих чисел відрізняються щонайбільше на 1. До речі, цікаво було б знайти простіше доведення цього твердження, ніж в [**1**].

При $r = 2$ теорема 0.13.1 стверджує, що множину вершин V можна пофарбувати двома кольорами так, що кожна одинична куля містить дві різнокольорові точки. Якщо всі кулі одничного радіуса містять досить багато точок, виникає спокуса посилити це твердження і довести, що можна різнобарвніше розфарбувати V, так щоб кожна одинична куля містила точки усіх кольорів. Проте ця спокуса розбивається таким прикладом.

Для кожного натурального числа k покладемо $X_k = \{1, 2, \ldots, 3k\}$. Позначимо через Y_k сім'ю усіх k-підмножин множини X_k. Розглянемо граф G_k з множиною вершин $V_k = X_k \cup Y_k$ і множиною ребер E_k, визначеною за таким правилом: $(x, y) \in E_k$ тоді і тільки тоді, коли $x \in X_k, y \in Y_k$ і $x \in y$. Відмітимо, що кодна одинична куля в G_k містить $> k$ вершин. Розглянемо довільне 3-розфарбування $\chi : V_k \to \{1, 2, 3\}$. Оскільки $|X_k| = 3k$, то знайдеться однокольорова підмножина $z \in Y_k$, а отже $|\chi(B(z, 1))| < 3$.

Попередній вступ дає підстави для наступного означення калейдоскопічності. Про калейдоскопічні графи як екстремальні з точки зору розкладності див [**1**].

Зв'язний регулярний граф $\mathrm{Gr}(V, E)$ скінченного степеня s (тобто $|B(v,1)| = s+1$ для всіх $v \in V$) ми назвемо *калейдоскопічним,* якщо існує розфарбування $\chi : V \to \{0, 1, \ldots, s\}$, таке що $|\chi(B(v, 1)| = s + 1$ для будь-якої вершини $v \in V$. В цьому разі розфарбування χ теж називається калейдоскопічним. Отже, калейдоскопічні графи — це графи, що допускають калейдоскопічні розфарбування. Зауважимо, що розфарбування калейдоскопічне тоді і тільки тоді, коли в кожній одиничній кулі немає двох однокольорових вершин.

Теорема 0.13.3. *Нехай* $\mathrm{Gr}(V, E)$ *— скінченний калейдоскопічний граф степеня* s*,* $\chi : V \to \{0, 1, \ldots, s\}$ *— його калейдоскопічне розфарбування. Тоді справедливі такі твердження*

(i) $s + 1|n$*;*

(ii) $|\chi^{-1}(0)| = \chi^{-1}(1)| = \cdots = |\chi^{-1}(s)|$.

Доведення. Для кожного $i \in \{0, 1, \ldots, s\}$ розглянемо сім'ю куль $\{B(x, 1) : x \in \chi^{-1}(i)\}$ і покажемо, що ця сім'я утворює розбиття V. Дійсно, припустимо, що $B(x_1, 1) \cap B(x_2, 1) \neq \emptyset$ для деяких вершин $x_1, x_2 \in \chi^{-1}(i)$. Виберемо вершину $v \in B(x_1, 1) \cap B(x_2, 1)$. Тоді в кулі $B(v, 1)$ містяться однокольорові вершини x_1, x_2. За означенням калейдоскопічного графу, $x_1 = x_2$. Це означає, що сім'я $\{B(x, 1) : x \in \chi^{-1}(i)\}$ диз'юнктна. З іншого боку, для довільної вершини $v \in V$ в кулі $B(v, 1)$ міститься деяка вершина x кольору i. Отже, $v \in B(x, 1)$ і сім'я куль $\{B(x, 1) : x \in \chi^{-1}(i)\}$ є покриттям множини V.

Оскільки сім'я $\{B(x, 1) : x \in \chi^{-1}(i)\}$ є розбиттям множини V і $|B(x, 1)| = s + 1$, $x \in \chi^{-1}(i)$, то

$$|V| = (s + 1)|\chi^{-1}(i)$$

для всіх $i \in \{0, 1, \ldots, s\}$. $\square$

З цього твердження легко випливає, що циклічний граф з n вершинами калейдоскопічний тоді і тільки тоді коли n кратне 3. Серед п'яти правильних многогранників у просторі (як скінченних графів) калейдоскопічними є тетраедр, куб, ікосаедр і лише вони.

Нескінченну серію калейдоскопічних графів дають коди Хемінга. Наведемо потрібні означення.

Нехай n — натуральне число, F^n — векторний простір розмірності n над полем $F = \{0, 1\}$. Вектори з F^n будемо називати словами і записувати у вигляді послідовностей довжини n, що складаються з букв 0,1. Через $\mathbf{0}$ позначимо слово, що скадається з n нулів, а через $\mathbf{1}$ — слово, що складається з n одиниць.

Для $u, v \in F^n$ через $d(u, v)$ позначимо число місць, де букви слів u, v не співпадають. Функція d визначає відстань між словами u, v і називається метрикою Хемінга, а число $d(0, u)$ — вагою слова u. Носій слова u — це множина номерів його одиничних букв.

Для невід'ємного цілого числа s *бінарним s-кодом, що виправляє помилки,* називають довільну непорожню підмножину $C \subseteq F^n$, таку що $d(u, v) \geq 2s + 1$ для всіх $u, v \in C$, $u \neq v$. Для $r \in \mathbb{N}$, $u \in F^n$ позначимо $B(u, r) = \{v \in F^n : d(u, v) \leq r\}$. Тоді умову цього означення ми можемо переписати у вигляді

$$B(u, s) \cap B(v, s) = \emptyset$$

при $u, v \in C$, $u \neq v$.

Бінарний s-код називають *досконалим,* якщо $\cup_{u \in C} B(u, s) = F^n$.

Уявімо, що ми передаємо (скажімо через Internet) повідомлення, закодоване словами з C. Поміхи чи несправності на лінії можуть призвести до помилок: в деяких словах якісь 0 заміняться на 1, а 1 — на 0. Проте, якщо в слові припущено не більше s помилок, то абонент (що знає код C) може виправити всі помилки і відновити слово. Для цього він має одержане слово $\overline{u}$ замінити на найближче до нього за метрикою Хемінга слово u з C.

Задача теорії кодування полягає в тому, щоб розробити ефективні коди, що виправляють помилки. Доклалніше про алгебраїчну теорею кодування див. [**4**], [**5**], [**?**].

Кожен підпростір C простору F^n є бінарним s-кодом при $s = [(\min\{d(\mathbf{0}, \mathrm{u}) : \mathrm{u} \in \mathrm{C}, \mathrm{u} \neq \mathbf{0}\} - 1)/2]$. Такий код називають *лінійним* або (n, m)-кодом, де $m = \dim C$.

Нехай k — натуральне число, $n = 2^k - 1$. *Бінарним кодом Хемінга* називають $(n, n-k)$ — код

$$C = \{u \in F^n : uH = 0\},$$

де H — матриця розміру $n \times k$, рядки якої — всі ненульові вектори простору F^k в деякому порядку. Звідси випливає, що вага ненульових слів з C на менша за 3, а тому C є 1-кодом. Код Хемінга досконалий, оскільки

$$|B(u,1)| = 1 + n = 2^k, |C| = 2^{n-k}, |\cup_{u \in C} B(u,1)| = 2^n = |F^n|.$$

Множину F^n можна розглядати як множину вершин деякого графу H_n (n-вимірного кубу), в якому дві вершини суміжні тоді і тільки тоді, коли відстань Хемінга між ним 1. Це регулярний граф степеня n. Коли H_n калейдоскопічний? Необхідну умову дає теорема 0.13.3: $n+1|2^n$. Отже, $n = 2^k - 1$. З іншого боку, якщо $n = 2^k - 1$, то H_n калейдоскопічний. Дійсно, нехай $C \subset F^n$ — код Хемінга. Покладемо $\chi(c) = 0$ для всіх $c \in C$. Для кожного елементу $y \in F^n \setminus C$ знайдуться базисний вектор $e_i = (0, \ldots, 1, \ldots, 0)$ та $c \in C$, такі що $y = e_i + c$, причому такий розклад однозначний — це наслідок досконалості. Покладемо $\chi(y) = i$.

Ми узагальнимо цю конструкцію і отримаємо широкий спектр калейдоскопічних графів, користуючись графами Келі груп.

Нехай G — група з одиницею e, X — система твірних G, $G = X$, причому $X = X^{-1}, e \in X$. Множиною вершин графу $\mathrm{Cay}(G, X)$ є множина G, а дві різні вершини $a, b \in G$ суміжні тоді і тільки тоді, коли $a^{-1}b \in X$. Припустимо, що $Y \subseteq X$ і пару (X, Y) назвемо *калейдоскопічною,* якщо

(i) $e \in Y$, $G = XY$;

(ii) $XX \cap Y^{-1}Y = XX \cap YY^{-1} = \{e\}$.

З цих умов випливає, що кожен елемент $g \in G$ однозначно розкладається у добуток $g = xy, x \in X, y \in Y$.

Для калейдоскопічної пари (X, Y) визначимо *стандартне розфарбування* $\chi : G \to X$ за таким правилом. Для кожного елемента $x \in X$ покладемо $\chi(x) = x$. Візьмемо довільний елемент $g \in G$ і виберемо $x \in X, y \in Y$ так, що $g = xy$. Покладемо $\chi(g) = x$. Переконаємось в тому, що стандартне розфарбування множини вершин графа $\mathrm{Cay}(G, X)$ є калейдоскопічним.

Нехай $g_1, g_2, g \in G$, $g_1, g_2 \in B(g, 1)$ і $\chi(g_1) = \chi(g_2)$. Доведемо, що $g_1 = g_2$. Виберемо елементи $x_1, x_2 \in X$, $y_1, y_2 \in Y$ так, що $g_1 = x_1y_1, g_2 = x_2y_2$. Оскільки $\chi(g_1) = x_1, \chi(g_2) = x_2$ і $\chi(g_1) = \chi(g_2)$, то $x_1 = x_2$. Оскільки $g_1, g_2 \in B(g, 1)$, знайдуться елементи $z_1, z_2 \in X$, такі що

$$g_1 = gz_1, g_2 = gz_2.$$

Таким чином,

$$g_1 = x_1y_1 = gz_1, g_2 = x_2y_2 = x_1y_2 = gz_2.$$

Звідси випливає, що

$$x_1y_1z_1^{-1} = x_1y_2z_2^{-1}, y_1z_1^{-1} = y_2z_2^{-1}.$$

Отже, $y_2^{-1}y_1 = z_2^{-1}z_1$ і з (ii) маємо $y_1 = y_2, z_1 = z_2$ і $g_1 = g_2$.

Власне ми довели наступну теорему.

Теорема 0.13.4. *Якщо* (X,Y) *— калейдоскопічна пара в групі* G*, то* $\mathrm{Cay}(G,X)$ *— калейдоскопічний граф.*

Досить нескладно довести і таке твердження, обернене до цієї теореми.

Нехай G — група з одиницею e, s — натуральне число, $X \subseteq G$, $e \in X$, $X = X^{-1}$, $\langle X \rangle = G$, $|X| = s+1$. Якщо граф $\mathrm{Cay}(G,X)$ допускає калейдоскопічне розфарбування χ і $Y = Y^{-1}$, де $Y = \{y \in G : \chi(e) = \chi(y)\}$, то (X,Y) — калейдоскопічна пара.

Калейдоскопічну пару (X,Y) в групі G ми назвемо *Хемінговою парою,* якщо Y — підгрупа групи G, при цьому граф $\mathrm{Cay}(G,X)$ ми називаємо *Хемінговим графом.* На мить повернімися до графу H_n, розглянутому вище, і нехай G — адитивна група простору F^n. Покладемо $Y = C$, де C — код Хемінга, $X = \{0, e_1, \dots, e_n\}$. Тоді (X,Y) — Хемінгова пара — ось звідки наше загальне означення Хемінгової пари. Прискіпливий читач (чи слухач) в цей момент може поставити питання: чим специфічні Хемінгові пари серед калейдоскопічних пар? Для того, щоб пояснити це гіпотетичне запитання наведемо допоміжні означення.

Нехай G — довільна група з одиницею e, A — довільна множина. За означенням, група G діє на множині A, якщо кожному елементу $g \in G$ співставлене відображення $a \mapsto g(a)$, $a \in A$ множини A на себе, таке що

$$e(a) = a, (g_1 g_2)(a) = g_1(g_2(a))$$

для всіх $a \in A$, $g_1, g_2 \in G$. В цьому разі кажуть, що A є *G-простором.* G-простір A називають *транзитивним,* якщо для будь-яких елементів $a, b \in A$ існує елемент $g \in G$, такий що $g(a) = b$

Розфарбування $\chi : A \to k$ G-постору A k кольорами природньо називати *інваріантним,* якщо для довільних a, b з A

із $\chi(a) = \chi(b)$ неодмінно випливає $\chi(g(a)) = \chi(g(b))$ для довільного $g \in G$. Ми опишемо усі можливі інваріантні розфарбування транзитивного G-простору A.

Нехай $\chi : A \to k$ — інваріантне k-розфарбування транзитивного G-простору A. Зафіксуємо довільний елемент $a_0 \in A$ і позначимо через $H = \{g \in G : g(a_0) = a_0\}$ стабілізатор в групі G елемента a_0. Ототожнимо A з простором G/H усіх лівих суміжних класів групи G за підгрупою H, при цьому дія групи G на G/H — це лівий зсув $aH \mapsto gaH$, $g \in G$. Покладемо $Y = \{y \in G : \chi(yH) = \chi(H)\}$ і покажемо, що Y — підгрупа групи G. Нехай $y_1, y_2 \in Y$. Тоді $\chi(y_1H) = \chi(y_2H) = \chi(H)$. Оскільки розфарбування χ інваріантне, то $\chi(y_1y_2H) = \chi(y_1H) = \chi(H)$ і $y_1y_2 \in Y$. Оскільки $\chi(y_1H) = \chi(H)$, то $\chi(y_1^{-1}y_1H) = \chi(y_1^{-1}H)$ і $y_1^{-1} \in H$. Далі, якщо $a, b \in gY$, то $aH = gy_1H, bH = gy_2H$ для деяких елементів $y_1, y_2 \in Y$. Оскільки χ — інваріантне розфарбування, то $\chi(aH) = \chi(bH)$. Отже, кожне інваріантне розфарбування стале на кожному суміжномі класі gH.

Навпаки, нехай Y — підгрупа групи G і $H \subseteq Y$. Припустимо, що розфарбування χ стале на кожному суміжному класі gH. Очевидно, що χ — інваріантне розфарбування.

Якщо граф Келі групи G розглянути як лівий G-простір, одержуємо таку характеризацію Хемінгових пар.

Теорема 0.13.5. *Нехай (X, Y) — калейдоскопічна пара в групі G, χ — стандартне розфарбування G. Тоді такі два твердження рівносильні:*

(i) *(X, Y) — Хемінгова пара;*

(ii) *якщо $g_1, g_2 \in G, x \in G$ і $\chi(g_1) = \chi(g_2)$, то $\chi(xg_1) = \chi(xg_2)$.*

Теорема 0.13.6. *Для довільної групи H знайдуться група G з Хемінговою парою (X, Y), в якій підгрупа Y ізоморфна H.*

Доведення. Нехай S — система твірних групи H, $S = S^{-1}, e \in S$. Для кожного елеметну $s \in S$ виберемо свою циклічну підгрупу порядку 4 і її твірну позначимо a_s. Покладемо

$$G = A \times H, A = \bigotimes_{s \in S} \langle a_s \rangle,$$

позначимо

$$X = \{a_s^2 s, a_s^{-2} s^{-1} : s \in S\} \cup (A \setminus \{a_s^2, a_s^{-2} : s \in S\}).$$

Легко перевірити, що

$$X = X^{-1}, e \in X, G = XH, XX \cap H = \{e\}.$$

Отже, (X, H) — Хемінгова пара в групі G. □

Ми розглянемо ще один метод побудови калейдоскопічних графів на основі графів Келі Cay(G, S) груп при деяких обмеженнях на систему твірних S.

Крок 1. Нехай G — група з одиницею e, S — скінченна підмножина групи, $G = \langle S \rangle$, $e \neq S$, $S = S^{-1}$. Припустимо також, що $|S| = r(r-1)$ для деякого натурального числа $r > 1$ і S не містить елементів порядку 2. Побудуємо розбиття $S = S_1 \cup \dots \cup S_r$, таке що $|S_i| = r-1, i \in \{1, \dots, r\}$ і $S_j^{-1} \cap S_i = \emptyset$ для всіх різних індексів $i, j \in \{1, \dots, r\}$. Для цього розіб'ємо $S = A \cup B$ так, що $B = A^{-1}$. Таке розбиття можливе оскільки S не містить елементів порядку 2. Виберемо довільні елементи $x_1, \dots, x_{r-1} \in A$ і покладемо $S_1 = \{x_1, \dots, x_{r-1}\}$. Віднесемо елементи $x_1^{-1}, \dots, x_{r-1}^{-1}$ до майбутніх підмножин $S_2, S_3, \dots, S_r$. Виберемо довільні елементи $y_2, \dots, y_{r-1} \in A \setminus \{x_1, \dots, x_{r-1}\}$. Покладемо $S_2 = \{x_1^{-1}, y_2, \dots, y_{r-1}\}$ і віднесемо елементи $y_2^{-1}, y_3^{-1}, \dots, y_{r-1}^{-1}$ до майбутніх підмножин $S_3, S_4, \dots, S_{r-1}$. Виберемо довільні елементи

$$z_3, z_4, \dots, z_{r-1} \in A \setminus \{x_1, \dots, x_{r-}, y_2, \dots, y_{r-1}\},$$

покладемо $S_3 = \{x_2^{-1}, y_2^{-1}, z_3, \ldots, z_{r-1}\}$, віднесемо елементи $z_3^{-1}, \ldots, z_{r-1}^{-1}$ до майбутніх підмножин $S_4, S_5, \ldots, S_r$ і т. д.

Крок 2. Впорядкуємо групу G лінійно і ототожнимо кожне ребро графа Келі $\mathrm{Cay}(G,S)$ з парою (x,y), $x<y$. Позначимо через N потужність множини ребер графа $\mathrm{Cay}(G,S)$. Візьмемо довільну множину W потужності $2N$, $W \cap G = \emptyset$ і побудуємо допоміжний граф $\mathrm{Gr}(G \cup W, E)$. Для кожного ребра (x,y) графа $\mathrm{Cay}(G,S)$ виберемо різні елементи $z,t \in W$ і замінимо ребро (x,y) на шлях x,z,t,y. Занесемо $(x,z),(z,t),(t,y)$ до E. При цьому, якщо (x,y) і (x',y') різні ребра графа $\mathrm{Cay}(G,S)$ і $(x,y),(x',y')$ замінено шляхами x,z,t,y та x',z',t',y', то $\{z,t\} \cap \{z',t'\} = \emptyset$.

Крок 3. Визначимо розфарбування $\chi : W \cup G \to \{0,1,\ldots,r\}$ за таким правилом. Покладемо $\chi(g)=0$ для всіх $g \in G$. Нехай $x,y \in G$ і ребро (x,y) замінено на шлях x,z,t,y. Тоді $x^{-1}y = s$, $s \in G$. Виберемо $i,j \in \{1,\ldots,r\}$ так, що $s \in S_i$, $s^{-1} \in S_j$. Покладемо $\chi(z)=i, \chi(t)=j$.

Крок 4. Для кожного $x \in G$ і кожного $i \in \{1,\ldots,r\}$ існує рівно $r-1$ вершин $z_1, z_2, \ldots, z_{r-1} \in W$ для яких $(x,z_1),\ldots,(x,z_{r-1}) \in E$ і $\chi(z_1) = \cdots = \chi(z_{r-1}) = i$. Склеїмо ці вершини в одну вершину, а ребра $(x,z_1),\ldots,(x,z_{r-1})$ — в одне ребро. Після такої факторизації ми отримаємо калейдоскопічний граф.

На завершення ми розглянемо деякі алгебраїчні конструкції, що виникають при дослдженні калейдоскопічних графів.

Нехай s — натуральне число, $s>1$, $\mathrm{Gr}_1(V_1,E_1)$, $\mathrm{Gr}(v_2,E_2)$ — калейдоскопічні графи степеня s, $\chi_1 : V_1 \to \{0,1,\ldots,s\}$, $\chi_2 : V_2 \to \{0,1,\ldots,s\}$ — їх калейдескопічні розфарбування. Відображення f множини V_1на множину V_2 називається *калейдоскопічним гомоморфізмом,* якщо

(i) $\chi_1(x) = \chi_2(f(x))$ для всіх $x \in V_1$;

(ii) якщо $(x,y) \in E_1$, то $(f(x),f(y)) \in E_2$.

Регулярне дерево $\mathrm{Tr}(V, E)$ степеня s з визначеним калейдоскопічним розфарбуванням $\chi : V \to \{0, 1, \dots, s\}$ називається *вільним калейдоскопічним деревом степеня* s.

ТЕОРЕМА 0.13.7. *Нехай* $\mathrm{Tr}(V, E)$ *— вільне калейдоскопічне дерево степеня* s *з калейдоскопічним розфарбуванням* $\chi : V \to \{0, 1, \dots, s\}$, $\mathrm{Gr}(V', E')$ *— довільний калейдоскопічний граф степеня* s *з калейдоскопічним розфарбуванням* $\chi' : V' \to \{0, 1, \dots, s\}$. *Тоді існує калейдоскопічний гомоморфізм* $f : V \to V'$.

ДОВЕДЕННЯ. Зафіксуємо довільні вершини $x \in V$, $y \in V'$, для яких $\chi(x) = \chi'(y)$ і покладемо $f(x) = y$. Для кожного невід'ємного цілого числа m позначимо

$$S_m(x) = \{z \in V : d(x, z) = m\}.$$

Припустимо, що відображення f вже визначене на множині $S_0(x) \cup \dots \cup S_m(x)$. Візьмемо довільну вершину $z \in S_{m+1}(x)$ і виберемо вершину $z' \in S_m(x)$ так, що $(z, z') \in E$. Далі виберемо вершину $t \in B(f(z'), 1)$, для якої $\chi(z) = \chi(t)$. Покладемо $f(z) = t$. За побудовою, f — калейдоскопічний гомоморфізм. □

Нехай s — натуральне число, $s > 1$, $X = \{0, 1, \dots, s\}$. *Калейдоскопічна напівгрупа* $KS(X)$ в алфавіті X — це напівгрупа, визначена співвідношеннями $xx = x$, $xyx = x$ для всіх $x, y \in X$. Напівгрупу $KS(X)$ зручно розглядати як множину усіх непорожніх слів в алфавіті X без факторів xx, xyx для всіх $x, y \in X$. Для того, щоб знайти добуток $w_1 w_2$ двох елементів $w_1, w_2 \in KS(X)$ треба до слова w_1 дописати справа слово w_2 і провести скорочення, визначені співвідношеннями $xx = x, xyx = x$. Наприклад, якщо $s = 3, w_1 = 0123012, w_2 = 2103123$, то

$$w_1 w_2 = 01230122103123 = 0123123.$$

Для кожного слова $w \in KS(X)$ позначимо через $l(w), r(w)$ першу та останню літери слова w, а через $\tilde{w}$ — слово w, записане у зворотному порядку. Очевидно, що

$$w\tilde{w} = l(w), \tilde{w}w = r(w), \tilde{\tilde{w}} = w.$$

Для кожного $x \in X$ позначимо через $KG(X, x)$ множину усіх слів, що починаються і закінчуються літерою x. Ця множина є підгрупою $KS(X)$. Одиницею в $KG(X, x)$ є слово x, а оберненим до слова $w \in KG(X, x)$ є слово $\tilde{w}$. Назвемо $KG(X, x)$ *калейдоскопічною групою.*

Визначимо дію калейдоскопічної напівгрупи $KS(X)$ на множині вершин довільного калейдоскопічного графу $\mathrm{Gr}(V, E)$ степеня s з калейдоскопічним розфарбуванням $\chi : V \to \{0, 1, \ldots, s\}$. Візьмемо довільні $x \in X$, $v \in V$, виберемо вершину $u \in B(v, 1)$, для якої $\chi(u) = x$, і покладемо $x(v) = u$. Далі продовжимо дію з множини X на $KS(X)$. Якщо $w = KS(X)$, то знайдуться літера x і слово $w_1 \in KS(X)$, такі що $w = xw_1$ і довжина w_1 на одиницю менша за довжину w. Візьмемо довільну вершину $v \in V$ і покладемо $w(v) = x(w_1(v))$. Оскільки $xx(v) = x(v)$ і $xyx(v) = x(v)$ для всіх $x, y \in X$, $v \in V$, це визначення коректне. Зауважимо також, що послідовність кольорів вершин на найкоротшому шляху від вершини $v_1 \in V$ до вершини $v_2 \in V$ визначає деяке слово $w \in KS(X)$, таке що $w(v_1) = v_2$. Звідси випливає, що вказана дія транзитивна, а множина усіх вершини кольору x є інваріантною відносно калейдоскопічної групи $KG(X, x)$. Спочатку ми з'ясуємо алгебраїчну структуру $KG(X, x)$, а потім — $KS(X)$.

ЛЕМА 0.13.8. *Нехай $w_1, w_2 \in KS(X), l(w_2) = r(w_1)$ і $x_1x_2 \ldots x_{n-1}x_n$ — нескорочуваний запис слова $w = w_1w_2$. Тоді знайдуться такі слово $u \in KS(X)$ і число k, що*

$$w_1 = x_1 \ldots x_{k-1}u, w_2 = \tilde{u}x_{k+1}x_{k+2} \ldots x_n, u\tilde{u} = x_k.$$

Доведення. Оскільки $l(w_2) = r(w_1)$, то $w_1 = w_1'x, w_2 = xw_2'$ для деякої літери $x \in X$. Якщо $r(w_1') \neq l(w_2)$, покладемо $u = x$. Якщо $r(w_1') = l(w_2')$, то $w_1' = w_1''y, w_2' = yw_2''$ для деякої літери $y \in X$. Застосуємо скорочення $yxy = y$ і замінимо слова w_1, w_2 словами w_1', w_2'. Оскільки ці слова нескорочувані, можна застосувати до них індуктивні міркування. □

Нагадаємо, що елемент s напівгрупи S називається ідемпотентом, якщо $ss = s$.

Лема 0.13.9. *Ідемпотентами напівгрупи $KS(X)$ є всі слова x, xy, де $x, y \in X$, $x \neq y$ і тільки вони.*

Доведення. Очевидно, що всі слова x, xy є ідемпотентами. Нехай w — довільний ідемпотент напівгрупи $KS(X)$. Припустимо, що $l(w) = r(w)$. За лемою 0.13.8

$$w = x_1 \dots x_{k-1}u = \tilde{u}x_{k+1} \dots x_n = x_1 \dots x_k x_{k+1} \dots x_n,$$

де $x_1 \dots x_n$ — нескорочуваний запис слова w, $u\tilde{u} = x_k$. Звідси,

$$u = x_k x_{k+1} \dots x_n, \tilde{u} = x_1 \dots x_k,$$

отже, $u = x_k x_{k+1} \dots x_1$ і $w = x_1$.

Припустимо, що $l(w) \neq r(w)$. Нехай $l(w) = x$. Покладемо $w' = wx$. Тоді

$$w'w' = wxwx = wwx = wx = w'.$$

Отже, w' — ідемпотент і $l(w') = r(w')$. За доведеним вище, $w' = x$. Значить, $w = xy$ для деякої літери $y \in X$. □

Теорема 0.13.10. *Калейдоскопічна група $KG(X, x)$ є вільною групою з множиною вільних твірних*

$$W = \{xyzx : y, z \in X, x \neq y, x \neq z, y \neq z\}.$$

Доведення. Нагадємо, що одиницею групи $KG(X,x)$ є x. Спочатку покажемо, що кожен елемент g групи $KG(X,x)$ можна записати у вигляді добутку елементів з W (зауважимо, що $W = W^{-1}$). Для $g = x$ це очевидно: $x = (xyzx)(xzyx)$. Припустимо, що $g \neq x$. Очевидно, що нескорочуваний запис g як елемента напівгрупи $KS(x)$ факторизується на співмножники виду $xx_1x_2 \ldots x_nx, n \geq 2, x \neq x_i, i \in \{1, \ldots, n\}$ і серед сусідніх літер слова $x_1 \ldots x_n$ немає однакових. Тоді

$$xx_1x_2 \ldots x_{n-1}x_nx = (xx_1x_2x)(xx_2x_3x) \ldots (xx_{n-1}x_nx).$$

Ця факторизація визначає гомоморфізм вільної групи $F(W)$ на групу $KG(X,x)$. Покажемо, що ядро цього гомоморфізму є одиницею групи $F(W)$. Візьмемо довільне нескорочуване групове слово $w_1w_2 \ldots w_n, n \geq 1$ в алфавіті W і покажемо, що останні три літери в нескорочуваному записі слова $w_1 \ldots w_n$ як елемента напівгрупи $KS(X)$ співпадають з останніми трьома літерами слова w_n. Нехай $w_{n-1} = xabx, w_n = xcdx$. За припущенням індукції маємо

$$w_1w_2 \ldots w_{n-1} = x \ldots abx.$$

Якщо $c \neq b$, то $w_1 \ldots w_n = x \ldots abxcdx$ і це слово нескорочуване. Якщо $b = c$, то $w_1 \ldots w_n = x \ldots acdx$. Оскільки $b = c$, то $a \neq c$. Отже, якщо $a \neq d$, то це слово нескорочуване. У випадку $a = d$ маємо $w_{n-1} = xdcx$ і $w_n = w_{n-1}^{-1}$, що суперечить припущенню про нескорочуваність слова $w_1 \ldots w_n$ як групового слова в алфавіті W. □

Для фіксованого елемента $x \in X$, $X = \{0, 1, \ldots, s\}$ позначимо

$$L(x) = \{yx : y \in X\}, R(x) = \{xy : y \in X\}.$$

Оскільки $yxzx = yx, xzxy = xy$, то $L(x)$ — напівгрупа лівих нулів, $R(x)$ — напівгрупа правих нулів.

ТЕОРЕМА 0.13.11. *Калейдоскопічна напівгрупа $KS(X)$ ізоморфна сендвіч-добутку $L(x) \times KG(X, x) \times R(x)$, в якому множення визначене за правилом*

$$(l_1, g_1, r_1)(l_2, g_2, r_2) = (l_1, g_1\varphi(r_1, l_2)g_2, r_2),$$

де $\varphi(r_1, l_2) = r_1 l_2$.

ДОВЕДЕННЯ. Кожен елемент $x_1 \dots x_n \in KS(X)$ можна записати у вигляді

$$x_1 \dots x_n = x_1 x(x_1 x_2 \dots x_n) x x_n = x_1 x(x x_1 x_2 \dots x_n x) x x_n.$$

Визначимо бієкцію $f : KS(X) \to L(X) \times KG(X, x) \times R(x)$ за правилом

$$f(x_1 x_2 \dots x_n) = (x_1 x, x x_1 x_2 \dots x_n x, x x_n).$$

Для довільних елементів $x_1 x_2 \dots x_n \in KS(X)$, $y_1 y_2 \dots y_m \in KS(X)$ маємо

$$f(x_1 x_2 \dots x_n) f(y_1 y_2 \dots y_m) = (x_1 x, x x_1 x_2 \dots x_n x, x x_n)\cdot$$

$$(y_1 x, x y_1 \dots y_m x, x y_m) = (x_1 x, x x_1 x_2 \dots x_n x \varphi(x x_n, y_1 x)$$

$$x y_1 y_2 \dots y_m, x y_m) = (x_1 x, x x_1 \dots x_n y_1 \dots y_m x, x y_m) =$$

$$f(x_1 \dots x_n y_1 \dots y_m),$$

отже, f — ізоморфізм між $KS(X)$ та $L(x) \times KG(X, x) \times R(x)$. □

В [**3**] доведено такі твердження.

- Група калейдоскопічних автоморфізмів вільного налейдоскопічного дерева $\mathrm{Tr}(V, E)$ степеня s ізморфна вільній групі $KG(X, x)$, де $X = \{0, 1, \dots, s\}, x \in X$.

- Нехай G — група з Хемінговою парою (X, Y). Тоді група калейдоскопічних автоморфізмів графу $\mathrm{Cay}(G, X)$ ізоморфна Y.

- Кожна скінченно породжена група ізоморфна групі калейдоскопічних автоморфізмів деякого Хемінгового графу.

Бібліоґрафія

[1] Protasov I., Banakh T. Ball Structures and Colorings of Graphs and Groups, Mat. Stud. Monogr. Ser, Vol. 11, Lviv, 2003.

[2] Protasova K. D. Kaleidoskopic graphs, Mat. Stud., 18 (2002), 3-9.

[3] Protasov I.V., Protasova K. D. Automorphisms of kaleidoscopical graphs, Algebra and Discrete Math., 2(2007), 125-129

[4] Берлекамп Э. Алгебраическая теория кодирования, М., "Мир 1971.

[5] Биркгоф Г., Барти Т. Современная прикладная алгебра. М., "Мир 1976.

[6] Питерсон У. Коды, исправляющие ошибки, М., "Мир 1964.

0.14. Комбінаторика слів

Нехай A — алфавіт, A^* — множина усіх слів в алфавіті A, A^+ — множина усіх непустих слів в алфавіті A. Відносно операції $(u, v) \mapsto uv$ приписування слів A^* є напівгрупою, а A^+ — її піднапівгрупою. Напівгрупу A^* називають *вільним моноїдом* в алфавіті A, а A^+ — *вільною напівгрупою* в алфавіті A. *Моноїд* — це напівгрупа з одиницею. Будь-яке відображення алфавіту A в довільний моноїд S однозначно продовжується до гомоморфізму A^* в S.

Довжину слова $w \in A^*$ позначаємо $|w|$. Якщо $u, w \in A^*$ і $w = xuy$, де $x, y \in A^*$, то u називають *фактором* слова w. Запис u^n означає добуток n копій слова u. Слово u^2 та u^3 називаються квадратом та кубом слова u. Слово $w \in A^+$ називають *безквадратним (безкубним),* якщо w не містить факторів u^2

(відповідно u^3), де $u \in A^+$. Легко перевірити, що в алфавіті $A = \{a, b\}$ безквадратними є лише слова a, b, ab, ba, aba, bab.

Комбінаторика слів розпочалася двома статтями Акселя Туе **[7]**,**[8]** 1906 та 1912 року, в яких доведено таку теорему.

ТЕОРЕМА 0.14.1 (Туе). *В алфавіті з двох літер існують як завгодоно довгі безкубні слова. В алфавіті з трьох літер існують як завгодно довгі безквадратні слова.*

Ми викладемо оригінальну конструкцію Туе. Якщо слово $u \in A^+$ має два різні входження в слово w і ці входження мають принаймні одну спільну літеру, то кажуть, що ці входження перекриваються.

ЛЕМА 0.14.2. *Нехай A — довільний алфавіт, $w \in A^+$. Слово w містить два входження слова $u \in A^+$, що перекриваються тоді і тільки тоді, коли w має фактор виду $avava$, де $a \in A$, $v \in A^*$.*

ДОВЕДЕННЯ. Нехай $w = xuy = x'uy'$ і входження слова u в w перекриваються. Ми можемо вважати, що $|x| < |x'|$. Тоді $|x| < |x'| < |xu| < |x'u|$ і

$$x' = xs, xu = x'z, x'u = xut$$

для деяких слів $s, z, t \in A^+$. Значить, $u = sz = zt$. Нехай a — перша літера слів s і z. Тоді $s = av, z = az'$ і

$$u = avaz', w = x'uy' = xsuy' = xavavaz'y'.$$

З іншого боку, якщо $avava$ — фактор слова w, то маємо два входження слова $u = ava$ в w, що перекриваються. □

Надалі слово виду $avava$, що входить до слова w, будемо називати *зчепленим фактором.*

Нехай $A = \{a, b\}$. *Гомоморфізм Туе* $\mu : A^+ \to A^+$ визначається дією на елементи алфавіту

$$\mu(a) = ab, \mu(b) = ba.$$

Лема 0.14.3. *Нехай* $A = \{a, b\}, X = \{ab, ba\}$. *Якщо* $x \in X^*$, *то* $axa \notin X^*$, $bxb \notin X^*$.

Доведення. Індукція по $|x|$. Якщо $|x| = 0$, твердження очевидне. Нехай $x \in X^*, |x| \neq 0$ і $u = axa$. Припустимо, що $u \in X^*$, $u = x_1 \dots x_r$, де $x_1, \dots, x_r \in X$. Тоді $x_1 = ab, x_r = ba$, $u = abyba$, $y = x_2 \dots x_{r-1}$, $y \in X^*$. За припущенням індукції $byb \in X^*$ і $x \in X^*$, суперечність. Випадок bxb розглядається аналогічно. □

Лема 0.14.4. *Нехай* $A = \{a, b\}$, $w \in A^+$. *Якщо* μ *не має зчеплених факторів, то* $\mu(w)$ *також не має зчеплених факторів.*

Доведення. Ми припустимо, що $\mu(w)$ має зчеплений фактор і покажемо, що w також має зчеплений фактор. За припущенням, існують $x, y, v \in A^*$, $c \in A$, такі що

$$\mu(w) = xcvcvcy.$$

Очевидно, довжина слова $cvcvc$ непарна. Оскільки $\mu(w) \in X^*$, де $X = \{ab, ba\}$, то $|\mu(w)|$ парна. Значить, $|xy|$ непарна. Можливі два випадки.

Випадок $|x|$ парна. Тоді $x, cvcv, cy \in X^*$.

Випадок $|x|$ напарна. Тоді $xc, vcvc, y \in X^*$.

У обох випадках число $|v|$ непарне. Дійсно, якщо $|v|$ парне, то з $cvcv \in X^*$ (відповідно $vcvc \in X^*$) випливає $cvc \in X^*$, що суперечить лемі 0.14.3.

Якщо $|x|$ парна, то $cv \in X^*$ і $w = rsst$, де $\mu(r) = x$, $\mu(s) = cv$, $\mu(t) = cy$. Але тоді s і t починаються з одної літери $c \in A$ і ssc — зчеплений фактор в w.

Якщо $|x|$ непарна, то $vc \in X^*$ і $w = rsst$, де $\mu(r) = xc$, $\mu(s) = vc$, $\mu(t) = y$. Отже, r і s закінчуються одною літерою $c \in A$ і css — зчеплений фактор в w. □

ДОВЕДЕННЯ ТЕОРЕМИ ТУЕ. Для кожного натурального числа n слово $\mu^n(a)$ в алфавіті $A = \{a, b\}$ за лемою 0.14.4 не має зчеплених факторів. Якщо слово $w \in A^+$ містить куб деякого слова $u \in A^+$, то воно має два входження слова u^2, що перекриваються. Отже, за лемою 0.14.2, $\mu^n(a)$ безкубне.

Для доведення другого твердження теореми ми візьмемо алфавіт $B = \{a, b, c\}$ і задамо гомоморфізм $\delta : B^+ \to A^+$ за правилом

$$\delta(a) = a, \delta(b) = ab, \delta(c) = abb.$$

Кожне слово $u \in A^+$, що починається з літери a і не має зчеплених факторів однозначно факторизується

$$u = u_1 u_2 \dots u_n,$$

де $u_i \in \{a, ab, abb\}$ для всіх $i \in \{1, \dots, n\}$. Дійсно, кожна літера a в u слідує не більше ніж за двома літерами b, бо bbb — зчеплений фактор. Таким чином існує єдине слово $w \in B^+$, таке що $\delta(w) = u$. Припустимо, що w містить квадрат vv деякого слова $v \in B^+$, причому за словом vv слідує літера $d \in B$. Тоді $\delta(vvd)$ — фактор слова u. Оскільки $\delta(v) = ax$ для деякого $x \in A^*$ і $\delta(d)$ починається з літери a, то $axaxa$ — зчеплений фактор в u. Для завершення доведення досить вказати нескінченне слово $t = x_1 x_2 \dots x_n \dots$ в алфавіті A, що починається з літери a і не має зчеплених факторів, бо тоді кожне слово $\delta(x_1 \dots x_n)$ безквадратне. Оскільки $\mu^{n+1}(a) = \mu^n(ab) = \mu^n(a)\mu^n(b)$, то за t можна взяти природну границю послідовності слів $\mu(a), \mu^2(a), \dots$, в якій початком кожного наступного слова є попереднє. □

На перший погляд теорема Туе має суто розважальний характер, але насправді доведено її було заради таких алгебраїчних наслідків.

Нехай A — алфавіт, що має принаймні три літери. Розгляньмо моноїд $A^* \cup \{0\}$, одержаний приєднанням до A^* нуля 0, де $0u = u0 = 0$ для всіх $u \in A^* \cup \{0\}$. Означмо конгруенцію на $A^* \cup \{0\}$, породжену відношенням

$$uu \sim 0, u \in A^+.$$

Кожне безквадратне слово утворює клас еквівалентності, значить фактор-моноїд $A^* \cup \{0\}/\sim$ нескінченний.

Інша ситуація, в якій можна використати безквадратні слова: нехай $m, n \geq 2$ — натуральні числа, конгруенцію на A^* визначимо відношеннями

$$u^m \sim u^n, u \in A^*.$$

І в цьому випадку кожне безквадратне слово визначає клас еквівалентності, значить, моноїд $A^*/\sim$ нескінченний. Насправді цей результат вірний для алфавіту з двох літер [**2**]

Ці твердження можна помістити в рамки класичної проблеми Бернсайда. Оригінально проблема Берсайда формулювалась для груп, але її природньо сформулювати також і для напівгруп: чи кожна скінченно породжена періодична напівгрупа скінченна? Періодичною називають напівгрупу, кожен елемент якої лежить в скінченній піднапівгрупі. Як показує перший приклад, відповідь на це запитання негативна. Для груп відповідь також негативна. Більше того, існують скінченно породжені нескінченні групи скінченної експоненти [**1**], причому в конструкції Новікова-Адяна також використовувалися безквадратні слова.

Несподівано, в одному спеціальному випадку проблема Бернсайда розв'язується позитивно: кожен скінченно породжений ідемпотентний моноїд скінченний. Елемент s напівгрупи S називається ідемпотентом якщо $s^2 = s$.

Нехай A — довільний скінченний алфавіт. Розгляньмо конгруенцію на A^* породжену співвідношеннями

$$ww \sim w, w \in A^*.$$

Фактор-моноїд $M = A^*/\sim$ називається *вільним ідемпотентним моноїдом.* Кожен скінченно породжений ідемпотентний моноїд є фактор-моноїдом деякого вільного ідемпотентного моноїда.

ТЕОРЕМА 0.14.5 (Гріна-Ріса). *Вільний ідемпотентний моноїд в алфавіті A скінченний і містить рівно*

$$\sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) \prod_{i=1}^{k} (k-i+1)^{2^i}$$

елементів, де $n = |A|$.

ДОВЕДЕННЯ. Для слова $w \in A^*$ позначимо $\mathrm{alph}(w)$ множину усіх літер з A, що входять до w. Очевидно, що з $x \sim y$ випливає $\mathrm{alph}(x) = \mathrm{alph}(y)$. Спочатку ми доведемо твердження

(i) якщо $\mathrm{alph}(y) \subseteq \mathrm{alph}(x)$, то існує слово u, таке що $x \sim xyu$.

Це очевидно, коли $|y| = 0$. Припустимо, що $|y| \geq 1$, $y = y'a$, $a \in A$. За індукцією, існує слово u', таке що $x \sim xy'u'$. Оскільки $a \in \mathrm{alph}(x)$, то $x = zaz'$. Отже, для $u = z'y'u'$ маємо

$$xyu = z(az'y')(az'y')u' \sim zaz'y'u' = xy'u' \sim x.$$

Для $x \in A^+$ позначимо через x' найкоротший лівий фактор x, такий що $\mathrm{alph}(x') = \mathrm{alph}(x)$. Нехай $x' = pa, a \in A$. Тоді $\mathrm{alph}(p) = \mathrm{alph}(x) \setminus \{a\}$. Симетрично, найкоротший правий фактор x'' з $\mathrm{alph}(x'') = \mathrm{alph}(x)$ має вид $x'' = bq$ для декої літери $b \in A$ і $\mathrm{alph}(q) = \mathrm{alph}(x) \setminus \{b\}$. Таким чином, кожне слово

$x \in A^+$ асоціюється з четвіркою (p, a, b, q). Ми записуємо цей факт як

$$x \to (p, a, b, q).$$

(ii) Якщо $x \to (p, a, b, q)$, то $x \sim pabq$.

Дійсно, $x = pay = zbq$. Оскільки $\mathrm{alph}(y) \subseteq \mathrm{alph}(x) = \mathrm{alph}(pa)$, то за твердженням (i) існує слово u, таке що $pa \sim payu = xu$. Оскільки $\mathrm{alph}(pq) \subseteq \mathrm{alph}(bq)$, то існує слово v таке що $bq \sim vpabq$ (треба застосувати (i) до зворотніх слів). Нехай $\widehat{x} = pabq$. Тоді $bq \sim v\widehat{x}$. Далі,

$$\widehat{x} = pabq \sim xubq = xw, \text{ де } w = ubq,$$

$$x = zbq \sim zv\widehat{x} = t\widehat{x}, \text{ де } t = zv.$$

Отже, $x \sim t\widehat{x} \sim t\widehat{x}\widehat{x} \sim x\widehat{x} \sim xxw \sim xw = \widehat{x} = pabq$.

Застосовуючи твердження (ii) ми вже можемо довести скінченність M. Припустимо, що скінченність доведено, якщо алфавіт має менше літер, ніж A. Якщо $x \to (p, a, b, q)$, то $|\mathrm{alph}(p)| < |A|, |\mathrm{alph}(q)| < |B|$. Отже, існує лише скінченне число варіантів для p та q по модулю $\sim$. Оскільки алфавіт скінченний, то M скінченний. Для того, щоб підрахувати число слів в M, скористаймося таким твердженням

(iii) якщо $x \to (p, a, b, q)$, $x' \to (p', a', b', q')$, то $x \sim x'$ тоді і тільки тоді, коли $p \sim p', a = a', b = b', q \sim q'$.

Якщо $p \sim p'$, $a = a'$, $b = b'$, $q \sim q'$, то $pabq \sim p'a'b'q'$ і $x \sim x'$ за твердженням (ii).

Нехай $x \sim x'$. З індуктивних міркувань ми можемо вважати, що $x = \alpha\beta\gamma, x' = \alpha\beta^2\gamma$ для деяких слів $\alpha, \beta, \gamma \in A^*$. Ми розглянемо два випадки.

Випадок $|\alpha\beta| > |p|$. Нехай $x = pay$. Тоді

$$\alpha\beta = pat, y = t\gamma$$

для деякого $t \in A^+$. Далі, $x' = pat\beta\gamma$ і $\mathrm{alph}(p) = \mathrm{alph}(x) \setminus \{a\} = \mathrm{alph}(x') \setminus \{a\}$. Отже, $p = p', a = a'$.

Випадок $|\alpha\beta| \leq p$. Для $x = pay$ існує слово $s \in A^*$, таке що $p = \alpha\beta s, \gamma = say$. Тоді $x' = \alpha\beta^2 say$ і $\mathrm{alph}(\alpha\beta^2 s) = \mathrm{alph}(\alpha\beta s) = \mathrm{alph}(x) \setminus \{a\} = \mathrm{alph}(x') \setminus \{a\}$. Отже, $p' = \alpha\beta^2 s$ і $p \sim p', a = a'$.

Співвідношення $b = b', q \sim q'$ доводяться аналогічно.

Ми готові обчислити число елементів ідемпотентного моноїду $M = A^*/\sim$. Нехай $\pi : A^* \to M$ — канонічний гомоморфізм. Для кожної підмножини $B \subseteq A$, нехай

$$\overline{B} = \{x \in A^* : \mathrm{alph}(x) = B\}.$$

Очевидно, A^* є диз'юнктним об'єднанням множин $\overline{B}, B \subseteq A$. Оскільки $x \sim x'$ дає $\mathrm{alph}(x) = \mathrm{alph}(x')$, кожна множина B є об'єднанням класів еквівалентності по модулю $\sim$. Таким чином, M — диз'юнктне об'єднання множин $\pi(\overline{B})$, $B \subseteq A$.

Якщо $B \neq \emptyset$, то за твердженням (iii) існує канонічна біекція

$$\pi(\overline{B}) \to \bigcap_{a,b \in B} \pi(\overline{B \setminus \{a\}}) \times \{a\} \times \{b\} \times \pi(\overline{B \setminus \{b\}}).$$

Якщо $|B| = k > 1$, то $c_k = |\pi(\overline{B})|$ дорівнює $c_k = k^2 c_{k-1}^2$. Оскільки $c_0 = 1$, то $c_k = \prod\limits_{i=1}^{k} (k-i+1)^{2^i}$. Оскільки M — диз'юнктне об'єднання множини $\pi(\overline{B})$, то $|M| = \sum\limits_{k=0}^{n} \begin{pmatrix} n \\ k \end{pmatrix} c_k$. □

Цю теорему Гріна-Ріса, доведену в **[4]** узагальнив Сімон **[6]**: для довільної скінченно породженої напівгрупи S такі три умови рівносильні

(i) S скінченна,

(ii) S має скінченне число неідемпотентів,

(iii) існує натуральне число m, таке що для кожної послідовності $s_1, \ldots, s_m$ в S існують $i, j \in \{1, \ldots, m\}$, $i < j$, такі що $s_i \ldots s_j$ — ідемпотент.

Ми розглянемо ще один фрагмент комбінаторики слів — коди. Неформально, код можна вважати як множину слів у деякому "алфавіті таку що будь-який добуток цих слів можна "декодувати"однозначно. Розглянемо, наприклад, множину слів $\{a, bb, aab, bab\}$, закодуємо ці слова символами $0, 1, 2, 3$ розповсюдимо кодування на всі слова в алфавіті $\{0, 1, 2, 3\}$. Так кодом слова 012230 буде слово

$$abba\ aab\ aab\ baba.$$

Гарантією однозначності декодування є те, що кожне слово в алфавіті $\{a, b\}$ може бути записане у вигляді добутку слів $\{a, bb, aab, bab\}$ не більше ніж одним способом. Якщо слово в алфавіті $\{a, b\}$ читати справа наліво, то кожне закодоване слово закінчується лише одним із слів $\{a, bb, aab, bab\}$. З іншого боку, множина $\{a, ba, ab\}$ не є кодом, бо слово aba декодується двома різними способами

$$aba = (ab)a = a(ba).$$

Нехай A — алфавіт. Непорожня множина слів $C \subset A^+$ називається *кодом,* якщо для будь-яких двох слів

$$x_1 \ldots x_n, y_1 \ldots y_n,$$

де $x_1, \ldots, x_n, y_1, \ldots, y_n \in C$, в алфавіті A, таких що

$$x_1 \ldots x_n = y_1 \ldots y_m$$

виконується $x_1 = y_1$. Зрозуміло, що тоді $m = n$ і $x_i = y_i$ для всіх $i \in \{1, \ldots, n\}$.

Таким чином, C — код, якщо існує алфавіт B і біекція $B \to C$, що продовжується до ін'єктивного гомоморфізму $B^+ \to A^+$. Іншими словами, підмножина $C \subset A^+$ є кодом тоді і тільки тоді, коли підпівгрупа A^+, породжена C, є вільною півгрупою з множиною твірних C.

Підмножину $L \subset A^+$ називають *катенативно незалежною,* якщо жодне слово із L на можна записати у вигляді добутку $w = w_1 \dots w_n, n \geq 2$ слів $w_1, \dots, w_n$ із L. Зрозуміло, що кожен код є катенативно-незалежною множиною. Зворотнє твердження не вірне: $L = \{a, ba, ab\}$.

Теорема 0.14.6 (Шютценберже). *Непорожня катенативно незалежна підмножина $C \subset A^+$ є кодом тоді і тільки тоді, коли для кожного слова $w \in A^+$ з того, що $C^* w \cap C^* \neq \emptyset$, $wC^* \cap C^* \neq \emptyset$ випливає $w \in C^*$.*

Доведення. Нехай C задовольняє умову теореми. Переконаймося, що C — код. Припустімо супротивне: знайдуться слова $x_1, \dots, x_m, y_1, \dots, y_n \in C^*$, такі що

$$x_1 x_2 \dots x_m = y_1 y_2 \dots y_n,$$

але $x_1 \neq y_1$. Тоді одне зі слів x_1, y_1 має бути префіксом другого. Нехай $y_1 = x_1 z, z \in A^+$. Звідси вирливає, що $C^* \cap C^* z \neq \emptyset$. Оскільки $x_2 \dots x_m = z y_2 \dots y_n$, то $C^* \cap z C^* \neq \emptyset$. За умовою $z \in C^*$. Але тоді $y_1 = x_1 z$, що суперчить катенативній незалежності C.

Нехай C — код, але умова перетинів порушується, Тоді існують $w \notin C^*, x_1, \dots, x_m, y_1, \dots, y_n \in C, z_1, z_2 \in C^*$, такі що

$$x_1 \dots x_m \omega = y_1 \dots y_n, \omega z_1 = z_2.$$

Ми можемо припустити, що число m — найменше з можливих натуральних чисел, для яких справджуються ці співвідношення. Тоді

$$x_1 \dots x_m \omega z_1 = y_1 \dots y_n z_2 = x_1 \dots x_m z_2.$$

В силу мінімальності m, $x_1 \neq y_1$, що суперечить означенню коду. □

Якщо умову катенативної незалежності (у випадку скінченної множини слів) можна перевірити ефективно, то умова перетинів вимагає нескінченного числа перевірок, а тому теорему Шютценберже не можна вважати ефективним критерієм коду. Для того, щоб сформулювати такий критерій нам потрібні деякі позначення.

Нехай C — непорожня множина слів із A^+. Ми визначимо індуктивно послідовність підмножин $C_0, C_1, C_2, \ldots$ за таким правилом:

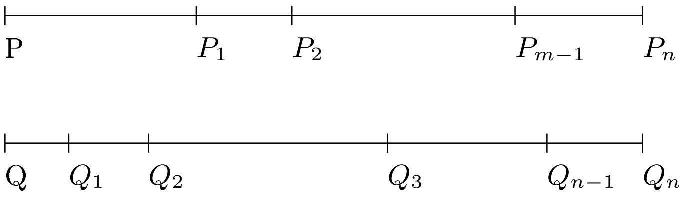
$$C_0 = C,$$
$$C_{i+1} = \{w \in A^+ : \exists x \in C, \exists y C_i \; yw = x \text{ або } xw = y\}.$$

Теорема 0.14.7 (Сардинаса-Патерсона). *Непорожня множина $C \subseteq A^+$ є кодом тоді і тільки тоді, коли $C_i \cap C = \emptyset$ для всіх натуральних чисел i.*

Доведення. Спочатку ми припустимо, що множина C не є кодом і покажемо, що принаймні одна з підмножин $C_i, i \geq 1$ перетинає C. Нехай $x_1, \ldots, x_m, y_1, \ldots, y_n \in G, x_1 \neq y_1$ і

$$x_1 x_2 \ldots x_m = y_1 y_2 \ldots y_n.$$

Ми вважаємо, що число m найменше з можливих. Зручно зобразити ситуацію графічно:



Слово $x_1 x_2 \ldots x_m$ записане на верхньому відрізку: x_1 між рисками P, P_1, x_2 між рисками P_1, P_2 і т. д. Слово $y_1 y_2 \ldots y_n$ записане на нижньому відрізку: y_1 між рисками Q, Q_1, y_2 між рисками Q_1, Q_2 і т. д. В силу мінімальності m жодні дві риски на різних відрізках не лежать на одній вертикалі.

За означенням, кожне слово з C_{i+1} одержано або странням префіксу, що належить C_i, в деякому слові з C, або стиранням префіксу з C в деякому слові з C_i. Далі ми будемо стирати риски на відрізках, рухаючись зліва направо. Слово на верхньому відрізку між Q_1 та P_1 належить C_1. Слово на нижньому відрізку між Q_2 та P_1 належить C_2. Слово між P_1 та Q_3 належить C_3 і т. д. Через скінченне число кроків ми одержимо, що або x_m або y_m належить деякій підмножині C_i, тобто $C \cap C_i \neq \emptyset$.

Нехай C — код. Спочатку індукцією по i ми доведемо, що $C^*w \cap C^* \neq \emptyset$ для всіх $w \in C_i, i \geq 0$. Для $i = 0$ це очевидно, оскільки $C_0 = C$. Припустімо, що твердження вже доведено для $i - 1$. Нехай $w \in C_i, i \geq 1$. За означенням C_i, знайдуться слова $x \in C, y \in C_{i-1}$, такі що

$$xw = y \text{ або } yw = x.$$

За припущенням індукції $x_1 y = x_2$ для деяких $x_1, x_2 \in C^*$. Отже,

$$x_1 x w = x_1 y = x_2 \text{ або } x_1 y w = x_2 w = x_1 x.$$

У обидвох випадках $C^*w \cap C^* \neq \emptyset$.

Щоб довести $C \cap C_i$ для всіх $i \geq 1$, ми припустимо супротивне: $C \cap C_i \neq \emptyset$ для деякого $i \geq 1$. За означенням C_i, знайдуться слова $x \in C, x' \in C, y \in C_{i-1}$, такі що

$$yx = x' \text{ або } x'x = y.$$

Розглянемо перше співвідношення $yx = x'$. Оскільки $yC^* \cap C^* \neq \emptyset$ і за доведеним вище $C^*y \cap C^* \neq \emptyset$, то за теоремою Щютценберже $y \in C^*$. Але це неможливо, бо $yx = x'$ і C — код.

Розберемося з другим співвідношенням $x'x = y$. Оскільки $y \in C_{i-1}$ і C — код, то $i \geq 2$. Значить існують $y_1 \in C_{i-2}, x'' \in$

C, такі що

$$y_1 y = x'' \text{ або } x'' y = y_1.$$

Перша рівність неможлива: з $y_1 x' x = x$ і $C^* y_1 \cap C^* = \emptyset$ випливає за теоремою Шютценберже, що $y_1 \in C$. Тож має справджуватись рівність

$$x'' y = x'' x' x = y_1.$$

Якщо $i = 2$, то деякий елемент з C можна записати як добуток трьох слів з C. Отже, $i \geq 3$. Повторюючи ці викладки, одержимо, що i більше будь-якого наперед заданого числа, суперечність. □

Якщо множина C скінченна, то довжина кожного слова з C_i не первищує довжини найдовшого слова C. Отже, існує лише скінченне число різних підмножин C_i і теорема Сардинаса-Патерсона дає алгоритм тестування коду. Наприклад, для $C = \{a, bb, aab, bab\}$ маємо

$$C_1 = \{ab\}, C_2 = \{b\}, C_3 = \{b, ab\} = C_4 = C_5 = \dots.$$

Про інші аспекти комбінаторики слів можна прочитати в [**3**],[**5**].

Бібліоґрафія

[1] Адян С. И. Проблема Бернасайда и тождества в группах, М., "Наука 1975.

[2] Brzozowski J., Culik K., Gabrielan A. Classification of noncounting events, J. Comput. System Sci., 5 (1971), 41-53.

[3] Combinatorics of words, Encyclopedia of math. and its applications, v. 17, 1983.

[4] Green J. A., Rees D. On semigroup in wich $x^r = x$, Math. Proc. Cambridge Phil. Soc., 48 (1952), 35-40.

[5] Саломаа А. Жемчужины теории формальных языков, М., "Мир 1986.

[6] Simon I. Conditions de finitude pour des semigroupes, C. R. Acad. Sci. Paris, 290 (1980), 1081-1082.

[7] Thue A. Uber unendliche Zeichenreihen, Norske Vid. Selsk. Skr. I. Mat. Nat. Kl., Christiania no 7, 1906, 1-22.

[8] Thue A. Uber die gegnseitige Lage gleicher Teile gewisser Leichenreihen, Norske Vid. Selsk. Skr. I. Mat.-Nat. Kl. Christiania no 1, 1912, 1-67.

0.15. Дискретний пошук

Нехай $X = \{1, \dots, n\}$ — область пошуку, в якій знаходиться невідомий об'єкт $x \in X$, 2^X — сім'я усіх підмножин множини X, $|Y|$ — число елементів підмножини $Y \subseteq X$. Умовами задачі пошуку $(X, \mathcal{F})$ фіксується деяка сім'я $\mathcal{F} \subseteq 2^X$ допустимих тестів. Кожен тест $T \in \mathcal{F}$ однозначно відповідає на запитання про те, чи належить елемент x до підмножини T? Необхідно так організувати пошук, щоб застосовуючи послідовно допустимі тести, знайти об'єкт x. Пошук ведеться відповідно до деякої стратегії $s = (s_1, \dots, s_m)$, де s_i — правило вибору теста на i-тому кроці. Докладніше пошук за стратегією s списується так.

1-ий крок. За правилом s_1 ми вибираємо деякий тест $T_1 \in \mathcal{F}$. Якщо $x \in T_1$, вважаймо $X_1(x) = T_1(x)$, $s_1(x) = 1$. Якщо $x \in X \backslash T_1$, вважаймо $X_1(x) = X \backslash T$, $s_1(x) = 0$. Якщо $|X_1(x)| = 1$, то $X_1(x) = \{x\}$, і задачу розв'язано. Інакше переходимо до другого кроку.

2-ий крок. За результатом $s_1(x)$ першого тесту правило s_2 вибирає допустимий тест $T_2 \in \mathcal{F}$. Якщо $x \in T_2$, вважаймо $X_2(x) = X_1(x) \cap T_2$, $s_2(x) = 1$. Якщо $x \in X \setminus T_2$, вважаймо $X_2(x) = X_1(x) \cap (X \setminus T_2), s_2(x) = 0$. Якщо $|X_2(x)| = 1$, то $X_2(x) = \{x\}$, і задачу розв'язано. Інакше перходимо до третього кроку.

. . . .

i-ий крок. За результатами $s_1(x), \dots, s_{i-1}(x)$ попередніх тестів правило s_i вказує допустимий тест $T_i \in \mathcal{F}$. Якщо $x \in T_i$, вважаймо $X_i(x) = X_{i-1}(x) \cap T_i, s_i(x) = 1$. Якщо $x \in X \setminus T_i$, вважаймо $X_i(x) = X_{i-1}(x) \cap (X \setminus T_i), s_i(x) = 0$. Якщо $|X_i(x)| = 1$, то $X_i(x) = x$, і задачу розв'язано. Інакше переходимо до $(i+1)$-ого кроку.

. . . .

m-ий крок. За результатами $s_1(x), \dots, s_{m-1}(x)$ попередніх тестів правило s_m вказує допустимий тест T_m. Якщо $x \in T_m$, вважаймо $X_m(x) = X_{m-1}(x) \cap T_m, s_m(x) = 1$. Якщо $x \in X \setminus T_m$, вважаймо $X_m(x) = X_{m-1}(x) \cap (X \setminus T_m), s_m(x) = 0$. Якщо $|X_m(x)| = 1$, то $X_m(x) = 1$, і задачу розв'язано. Інакше пошук за стратегією s виявився безрезультатним.

Якщо вибір чергового тесту не залежить від результатів попередніх тестувань, то стратегія називається *статичною*. Таким чином, статичну стратегію можна ототожнити з фіксованою послідовністю $(T_1, \ldots, T_m)$ допустимих тестів.

Стратегія s для задачі пошуку $(X, \mathcal{F})$ називається *успішною*, якщо яким би не був шуканий об'єкт $x \in X$, на деякому кроці пошуку за стратегією s цей елемент визначається однозначно. Отже, стратегія s успішна тоді і лише тоді, коли для кожного об'єкта $x \in X$ знайдеться $i \in \{1, \ldots, m\}$ таке, що $X_i(x) = \{x\}$. Кажуть, що задача пошуку $(X, \mathcal{F})$ *має розв'язок*, якщо для неї існує успішна стратегія пошуку.

За означенням тест T *відокремлює елемент $x \in X$ від елемента $y \in Y$*, якщо $x \in T, y \notin T$, або $x \notin T, y \in T$. Систему тестів $\mathcal{F}$ називають *відокремлюючою*, якщо для будь-яких різних елементів $x, y \in X$ існує тест $T \in \mathcal{F}$, що відокремлює x від y.

ТЕОРЕМА 0.15.1. *Задача пошуку $(X, \mathcal{F})$ має розв'язання тоді і тільки тоді, коли система тестів $\mathcal{F}$ відокремлююча.*

ДОВЕДЕННЯ. Припустімо, що задача пошуку $(X, \mathcal{F})$ має розв'язання, $s = (s_1, \ldots, s_m)$ — успішна стратегія, але не існує тестів із $\mathcal{F}$, що відокремлюють деякі елементи $x, y \in X$. Вважаймо, що шуканим є об'єкт x. Оскільки стратегія s успішна, знайдеться $k \in \{1, \ldots, m\}$ таке, що x визначається на k-му кроці пошуку за стратегією s. За нашим припущенням $s_1(x) = s_1(y), \ldots, s_k(x) = s_k(y)$, а тому $y \in X_k(x)$. Отже, $|X_k(x)| > 1$ і отримали суперечність.

Припустімо, що система тестів $\mathcal{F} = \{T_1, \ldots, T_m\}$ відокремлююча і переконаймося у тому, що статична стратегія $s = (T_1, \ldots, T_m)$ успішна. Якщо це не так, то знайдеться елемент $x \in X$ такий, що $|X_m(x)| > 1$. Нехай $y \in X_m(x), y \neq x$ і тест T_i відокремлює x від y. Але тоді $y \notin X_i(x)$ і значить, $y \notin X_m(x)$. □

З доведення цієї теореми випливає, що задача пошуку має розв'язання тоді і лише тоді, якщо існує статична успішна стратегія пошуку.

Під час пошуку за успішною стратегією $s = (s_1, \ldots, s_m)$ будь-який елемент $x \in X$ визначається на деякому кроці $l(x, s) \leq m$. При цьому формується булів вектор $s(x) = (s_1(x), \ldots, s_{l(x,s)}(x))$, що називається кодовим словом елемента x відносно стратегії s. Взагалі, будь-яку скінченну послідовність бульових векторів будемо неазивати *кодом* ,а самі вектори — *кодовими словами.* Код називається *префіксним,* якщо жодне його слово не є початком іншого слова. Наприклад, $\{(0, 0, 1, 1), (0, 1, 0), (1, 0, 0), (1, 1)\}$ — префіксний код, а код $\{(0, 0, 1, 1), (1, 0), (0, 0, 1)\}$ не перфіксний, оскільки третє слово — початок першого. Префіксний код називається нескорочуваним, якщо для кожного кодового слова код, що утворюється після викреслювання останнього символу в цьому слові, втрачає властивість префіксності.

Теорема 0.15.2. *Якщо s — успішна стратегія для задачі пошуку $(X, \mathcal{F})$, то $\{s(1), \ldots, s(n)\}$ — нескорочуваний префіксний код. Якщо $\{a(1), \ldots, a(n)\}$ — нескорочуваний префіксний код, то існує успішна стртегія s для задачі пошуку $(X, 2^X)$ така, що $s(1) = a(1), \ldots, s(n) = a(n)$.*

Доведення. Припустімо, що s — успішна стратегія для задачі пошуку $(X, \mathcal{F})$, але існують різні елементи $x, y \in X$ такі, що кодове слово $s(x)$ є початком кодового слова $s(y)$, тобто $s_1(x) = s_1(y), \ldots, s_{l(x,s)}(x) = s_{l(x,s)}(y)$. Вважаймо, що шуканим є елемент x. Тоді $y \in X_{l(x,s)}(x)$, а, отже, елемент x не може бути визначеним на кроці $l(x, s)$. Нескорочуваність коду $\{s(1), \ldots, s(n)\}$ випливає безпосередньо з означення стратегії.

Розглянемо довільний нескорочуваний префіксний код $\{a(1), \dots, a(n)\}$. Нехай $a(x) = (a_1(x), \dots, a_l(x)), x \in X$. Ми вкажемо таку успішну для задачі $(X, 2^X)$ стратегію пошуку s, що елемент x визначається на кроці l_x і $s(x) = a(x)$. Нехай $m = \max\{l_x : x \in X\}$. Для кожного $i \in \{1, \dots, m\}$, нехай $T_i = \{x \in X : a_i(x) = 1\}$. Розгляньмо статичну стратегію s, визначену послідовністю тестів $(T_1, \dots, T_m)$. Якщо $x, y \in X$ і $x \neq y$, то за префіксною властивістю коду $\{a(1), \dots, a(n)\}$ знайдеться $j \in \{1, \dots, m\}$ таке, що $j \leq l_x, j \leq l(y)$ і $a_j(x) \neq a_j(y)$. Це означає, що тест T_j відокремлює елементи x, y. За теоремою 0.15.1 стратегія s успішна. Зауважимо, що за побудовою кожен вектор $s(x)$ є початком вектору $a(x)$. За першим твердженням цієї теореми код $\{s(1), \dots, s(n)\}$ префіксний. З нескорочуваності коду $\{a(1), \dots, a(n)\}$ випливає, що $s(1) = a(1), \dots, s(n) = a(n)\}$. $\square$

Нехай s — успішна стратегія для задачі пошуку $(X, \mathcal{F})$. Число $l(s) = \max\{l(x, s) : x \in X\}$ називається *абсолютною довжиною* пошуку. По суті, $l(s)$ — це необхідне число кроків пошуку за стратегією s у найменш спрятливому випадку розташування шуканого об'єкту в області пошуку. Якщо задача пошуку $(X, \mathcal{F})$ має розв'язання, то існує успішна стратегія пошуку мінімальної абсолютної довжини. Така стратегія називається *мінімаксною.*

Далі через $\lceil t \rceil$ позначається найменше ціле число, що більше або дорівнює t, $\log t$ означає $\log_2 t$.

Теорема 0.15.3. *Якщо s мінімаксна стратегія для задачі $(X, \mathcal{F})$, то $\lceil \log n \rceil \leq l(s) \leq n$. Якщо s — мінімаксна стратегія для задачі $(X, 2^X)$, то $l(s) = \lceil \log n \rceil$.*

Доведення. Нехай s — мінімальна стратегія для задачі $(X, \mathcal{F})$. Після приписування до вектора $s(x)$ справа $l(s) - l(x, s)$ нулів одержимо вектор $\overline{s}(x)$. За теоремою 0.15.2 $\{s(x) : x \in X\}$

— префіксний код, а тому усі вектори системи $\{\overline{s}(x) : x \in X\}$ різні і мають довжину $l(s)$. Оскільки $|X| = n$, то $n \leq 2^{l(s)}$ і, отже, $\log n \leq l(s)$. Оскільки $l(s)$ — ціле число, то $\lceil \log n \rceil \leq l(s)$. Нерівність $l(s) \leq n$ ми доведемо індукцією за числом n. Для $n = 1$ нерівність очевидна. За правилом s_1, вибираємо перший тест $T_1 \in \mathcal{F}$. Оскільки стратегія s мінімальна, то $T_1 \neq X$ і $T_1 \neq \emptyset$, значить, $|X_1(x)| < n$ для кожного $x \in X$. За припущенням індукції для знаходження елемента x досить $n-1$ кроків пошуку.

Оскільки всі мінімальні стратегії для довільної задачі пошуку мають однакову абсолютну довжину, для доведення другого твердження теореми, враховуючи перше, досить побудувати успішну стратегію s для задачі пошуку $(X, 2^X)$ таку, що $l(s) = \lceil \log n \rceil$. Якщо $n = 1$, то ніяких тестів не треба, тобто $l(s) = 0 = \lceil \log 1 \rceil$. Припустімо, що для задачі пошуку в області, що містить $k < n$ елементів, існує успішна стратегія абсолютної довжини $\lceil \log k \rceil$. Нехай $|X| = n$. На першому кроці застосуємо тест $T \in 2^X$ такий, що $|T| = \lceil n/2 \rceil$. Далі можливі два випадки.

1.$x \in T$. За припущенням індукції для знаходження елемента x існує успішна стратегія абсолютної довжини $\lceil \log \lceil n/2 \rceil \rceil$. Отже, для розв'язання задачі досить зробити не більше ніж $m = 1 + \lceil \log \lceil n/2 \rceil \rceil$ тестувань. Зрозуміло, що

$$1 + \lceil \log \lceil n/2 \rceil \rceil = \lceil 1 + \log \lceil n/2 \rceil \rceil = \lceil \log 2 \lceil n/2 \rceil \rceil.$$

Якщо число n парне, то $\lceil n/2 \rceil$ і $m = \lceil \log_2 n \rceil$. Якщо ж $n = 2r+1$, то $\lceil n/2 \rceil = r+1$ і $m = \lceil \log(n+1) \rceil$. Залишилось показати, що у цьому випадку $\lceil \log n \rceil = \lceil \log(n+1) \rceil$. Нехай $\lceil \log n \rceil = p$. Оскільки n не є степенем двійки, то $p - 1 < \log n < p$ і $2^{p-1} < n < 2^p$. Але тоді $2^{p-1} < n + 1 \leq 2^p$ і, отже, $\lceil \log(n+1) \rceil = p$.

2. $x \notin T$. Оскільки $X \in X \setminus T$ і $|X \setminus T| = n = \lceil n/2 \rceil$, то для визначення елемента x після першого кроку, за припущенням індукції, досить $\lceil \log(n - \lceil n/2 \rceil) \rceil$ тестувань. Отже для розв'язання задачі вистачить $m = 1 + \lceil \log(n - \lceil n/2 \rceil) \rceil$ тестувань. Оскільки $n - \lceil n/2 \rceil \leq \lceil n/2 \rceil$, то за доведеним вище, $m \leq \log \lceil n \rceil$. □

Ми розглянули загальну задачу пошуку, в якій про шуканий об'єкт немає ніякої інформації, а тому можна вважати, що з однаковими ймовірностями шуканим може будь-який елемент з області пошуку. Припустімо тепер, що на області пошуку $X = \{1, \ldots, n\}$ задано деякий розподіл ймовірностей $p = (p(1), \ldots, p(n)), p(1) \geq 0, \ldots, p(n) \geq 0, \sum_{i=1}^{n} p(i) = 1$. Таким чином, $p(1)$ — це ймовірність того, що шуканим є перший елемент із X, $p(2)$ — другий і т. д. Задачу пошуку $(X, \mathcal{F})$ з відомим апріорним розподілом p будемо записувати $(X, p, \mathcal{F})$. Якщо s — успішна стратегія пошуку для даної задачі, то довжина пошуку елемента $x \in X$ є випадковою величиною. А саме, із ймовірністю $p(1)$ пошук вимагає $l(1, s)$ кроків, із ймовірністю $p(2)$ — $l(2, s)$ кроків і т. д. Отже, середня довжина $L(s)$ пошуку за стратегією s дорівнює математичному сподіванню $\sum_{i=1}^{n} p(i) l(i, s)$. Успішну стратегію для задачі $(X, p, \mathcal{F})$ найменшої середньої довжини пошуку назвемо *p-оптимальною.*

Очевидно, що складність задачі пошуку $(X, p, \mathcal{F})$ залежить не лише від заданої сукупності допустимимх тестів $\mathcal{F}$, а й від міри невизначеності розподілу p. Клод Шенон запропонував 1948 року вважати такою мірою величину

$$H(p(1), \ldots, p(n)) = -\sum_{i=1}^{n} p(i) \log p(i),$$

що називається *ентропією* розподілу p. Вважаймо $0 \log 0 = 0$. Пояснімо це означення. Розглянемо спочатку рівномірний розподіл $p_n = (\frac{1}{n}, \dots, \frac{1}{n})$ і позначимо через $f(n)$ деяку (поки що нам невідому) чисельну характеристику невизначеності розподілу p_n. Інтуїтивно $f(n)$ має відображати те, як важко вгадати обєкт, розподілений відповідно до p_n. Якщо $n = 1$, ми відразу можемо вказати шуканий об'єкт, тобто ніякої невизначеності у цьому випадку немає, а тому необхідно, щоб $f(1) = 0$. Оскільки при зростанні n вгадати об'єкт дедалі складніше, функція $f(n)$ також має зростати.

Звернімося до рівномірного розподілу p_{nm} на множині $\{1, \dots, nm\}$ і розіб'ємо цю множину на n блоків по m елементів у кожному. Невизначеність у питанні про те, в якому з блоків міститься шуканий об'єкт дорівнює $f(n)$. Якщо нам вже відомо, що об'єкт знаходиться у даному блоці, то невизначеність дорівнює $f(m)$. А тому цілком природньо вважати, що $f(nm) = f(n)f(m)$.

Неважко переконатися в тому, що єдиною функцією натурального аргументу, що задовольняє умови $f(nm) = f(n) + f(m), f(1) = 0, f(n) > f(m)$ при $n > m$ є логарифмічна функція. Якщо для визначеності обмежимося основою логарифмування 2, то отримаємо $f(n) = \log n$.

Оскільки для рівномірного розподілу p_n кожна з елементарних подій має ймовірність $\frac{1}{n}$, природньо вважати, що кожна подія $x = i$ вносить невизначеність $\frac{1}{n} f(n) = -\frac{1}{n} \log \frac{1}{n}$. Якщо тепер $p = (p(1), \dots, p(n))$ — довільний розподіл ймовірностей, то будемо вважати, що кожна елементарна подія вносить невизначеність $-p(i) \log p(i)$. Ці інтуїтивні міркування і приводять нас до означення ентропії як математичного сподівання випадкової величини, що набуває значення $\log \frac{1}{p(1)}, \dots, \log \frac{1}{p(n)}$ з ймовірностями $p(1), \dots, p(n)$.

Розглянемо основні властивості ентропії.

1. $H(\frac{1}{n}, \ldots, \frac{1}{n}) = \log n$. $H(p(1), \ldots, p(n)) = 0$ тоді і лише тоді, якщо знайдеться i таке, що $p(i) = 1$.

2. $H(p(1), \ldots, p(n)) = H(p(f(1)), \ldots, p(f(n)))$, де f — довільна підстановка чисел $\{1, \ldots, n\}$.

3. Нехай $p = (p(1), \ldots, p(n)), k \in \{1, \ldots, n\}$. Позначмо

$$p(1,k) = p(1) + \cdots + p(k), p(k+1,n) = p(k+1) + \cdots + p(n).$$

Тоді

$$H(p(1), \ldots, p(n)) =$$
$$= H(p(1,k), p(k+1,n)) + p(1,k)H(\frac{p(1)}{p(1,k)}, \ldots, \frac{p(k)}{p(1,k)}) +$$
$$+ p(k+1,n)H(\frac{p(k+1)}{p(k+1,n)}, \ldots, \frac{p(n)}{p(k+1,n)}).$$

Пошукова інтерпретація цієї властивості така. Ентропія $H(p(1), \ldots, p(n))$ є мірою невизначеності в задачі пошуку об'єкта серед елементів множини $\{1, \ldots, n\}$, розподіленого згідно з p. Спростімо задачу до запитання про те, у якій із підмножин $\{1, \ldots, k\}, \{k+1, \ldots, n\}$ міститься шуканий об'єкт? Область пошуку цієї задачі містить два елементи, а розподіл має вигляд $(p(1,k), p(k+1,n))$. Отже після відповіді на поставлене запитання ми зменшимо ентропію на величину $H(p(1,k), p(k+1,n))$. Якщо шуканий об'єкт міститься у множині $\{1, \ldots, k\}$, то одержуємо задачу з розподілом $(p(1)/p(1,k), \ldots p(k)/p(1,k))$ і ентропією $H(p(1)/p(1,k), \ldots, p(k)/p(1,k))$. Аналогічно, ентропія розподілу у випадку коли шуканий об'єкт належить множині $\{k+1, \ldots, n\}$, дорівнює $H(p(k+1)/p(k+1,n), \ldots, p(n)/p(k+1,n))$. Залишилося зауважити, що ймовірність першого випадку $p(1,k)$, а другого — $p(k+1,n)$.

Зауважимо, що ці три властивості ентропії є характеристичними, на що вказав Д. К. Фаддєєв. Точніше, якщо деяка функція $f(x_1, \ldots, x_n)$ визначена на множині $x_1 \geq 0, \ldots, x_n \geq$

$0, x_1 + \dots x_n = 1$, неперервна і має властивості 1-3, то з точністю до постійного множинка $f(x_1, \dots, x_n)$ співпадає з ентропією розподілу $(x_1, \dots, x_n)$.

4. Якщо $p = (p(1), \dots, p(n)), q = (q(1), \dots, q(n))$, то

$$H(p) = -\sum_{i=1}^{n} p(i) \log p(i) \leq -\sum_{i=1}^{n} p(i) \log q(i),$$

причому нерівність перетворюється у рівність тоді і тільки тоді, якщо $p(i) = q(i)$ для всіх $i \in \{1, \dots, n\}$.

Оскільки $0 \log 0 = 0$, можна вважати, що $p(i) > 0$ для всіх $i \in \{1, \dots, n\}$. Оскільки $\log x = \log e \ln x$, маємо

$$\sum_{i=1}^{n} p(i) \log q(i) - \sum_{i=1}^{n} p(i) \log p(i) =$$

$$= \sum_{i=1}^{n} p(i) \log \frac{q(i)}{p(i)} = (\log e) \sum_{i=1}^{n} p(i) \ln(1 + \frac{q(i) - p(i)}{p(i)}).$$

Як відомо, $\ln(1 + x) \leq x$ для всіх $x > -1$ і $\ln(1 + x) = x$ тоді і тільки тоді, коли $x = 0$. Отже

$$\sum_{i=1}^{n} p(i)(1 + \frac{q(i) - p(i)}{p(i)}) \leq \sum_{i=1}^{n} p(i) \frac{q(i) - p(i)}{p(i)} = 0,$$

причому рівність можлива лише за умови $p(i) = q(i)$ для всіх $i \in \{1, \dots, n\}$.

5. Якщо $p = (p(1), \dots, p(n))$, то $H(p) \leq \log n$, причому рівність можлива лише тоді, коли $p(1) = \dots = p(n) = \frac{1}{n}$.

Отже серед усіх розподілів рівномірний розподіл має максимальну ентропію. Для доведення досить розглянути розподіл $q(1) = \dots q(n) = \frac{1}{n}$ і скористатия попердньою властивістю.

6. Якщо $p = (p(1), p(2)), q = (q(1), q(2))$ і $|p(1) - p(2)| \geq |q(1) - q(2)|$, то $H(p) \leq H(q)$.

За другою властивістю можемо вважати, що $p(1) \geq p(2)$, $q(1) \geq q(2)$. Оскільки $p(1) + p(2) = 1$, $q(1) + q(2) = 1$, то $p(1) \geq q(1) \geq q(2) \geq p(2)$, $p(1) - q(1) = q(2) - p(2) \geq 0$. За четвертою властивістю

$$H(p) = -p(1)\log p(1) - p(2)\log p(2) \leq -p(1)\log q(1) - p(2)\log q(2).$$

Отже досить довести, що

$$q(1)\log q(1) + q(2)\log q(2) \leq p(1)\log q(1) + p(2)\log q(2).$$

Остання нерівність, враховуючи монотонність логарифмічної функції, рівнозначна нерівності

$$q(1)^{q(1)} q(2)^{q(2)} \leq q(1)^{p(1)} q(2)^{p(2)}.$$

Оскільки $q(1) \geq q(2), p(1) - q(1) = p(2) - q(2)$, то

$$q(1)^{p()-q(1)} \geq q(2)^{q(2)-p(2)}.$$

Нехай $(X, p, \mathcal{F})$ — задача пошуку, $T \in \mathcal{T}$. Як показує третя властивість, застосування тесту T зменшує ентропію на величину $H(t(1), t(2))$, де $t(1) = \sum_{t \in T} p(i) = \sum_{i \in X \setminus T} p(i)$. Енторпію $H(t(1), t(2))$ назвімо *інформативністю* тесту T відносно розподілу p і позначмо $I(T, p)$. За шостою властивістю максимальну інформативність має тест T, для якого величина $|t(1) - t(2)|$ мінімальна, тобто тест, для якого $\sum_{i \in T} p(i)$ найближча до 1/2. А тому прородньо напрошується стратегія, яка на кожному кроці вибирає тест максимальної інформативності. Така стратегія називається *MI-стратегією,* або на математичному жаргоні — *жадібною стратегією.* Опишемо цю стратегію докладніше. На першому кроці із множини $\mathcal{F}$ вибираємо тест T максимальної інформативності $I(T, p)$. Звужуємо область пошуку до множини $X_1(x)$, що дорівнює X або $X \setminus T$, якій належить шуканий об'єкт x. Обчислюємо апостеріорні ймовірності і одержуємо розподіл p_1 на $X_1(x)$. Звужуємо тести $\mathcal{F}$ на $X_1(x)$: $\mathcal{F}_1 = \{T \cap X_1(x) : T \in \mathcal{F}\}$. На другому кроці вибираємо із $\mathcal{F}_1$ тест максимальної інформативності і т. д. Така стратегія може слугувати гарним наближенням до p-оптимальної стратегії.

Звернемося до задачі пошуку без обмежень на тести $(X, p, 2^X)$ і пов'яжемо цю задачу з перфіксними кодами.

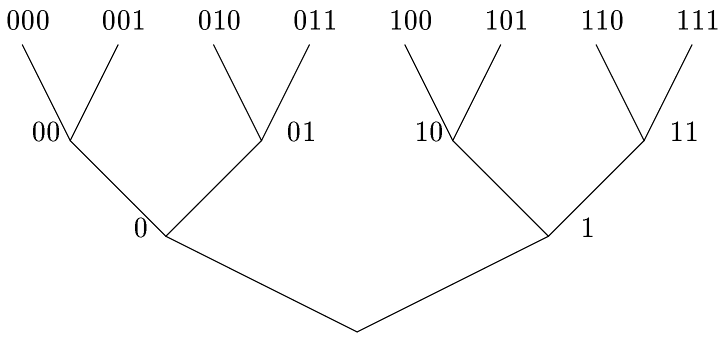
Нехай $a = \{a(x) : x \in X\}$ — нескорочуваний префіксний код, p — розподіл ймовірностей на X, $l(x)$ — довжина кодового слова $a(x)$. Число $L(a) = \sum\limits_{i=1}^{n} p(i)l(i)$ називається *середньою довжиною* коду a віносно розподілу p. Нескорочуваний префіксний код мінімальної середньої довжини відносно розподілу p називається *p-оптимальним.* Згідно теореми 0.15.2 проблема побудови p-оптимальної стратегії для задачі $(X, p, 2^X)$ рівнозначна проблемі визначення p-оптимального префіксного коду.

Наступна нерівність Крафта дає критерії існування префіксного коду з наперед заданими довжинами кодових слів.

Теорема 0.15.4. *Для існування префіксного коду з довжинами кодових слів $l(1), \ldots, l(n)$ необхідно і достатньо, щоб*

$$\sum_{i=1}^{n} 2^{-l(i)} \leq 1.$$

Доведення. Нехай a — префіксний код з довжинами кодових слів $l(1), \ldots, l(n), m = \max\{l(1), \ldots, l(n)\}$. Розгляньмо двійкове дерево T_m висоти m (на рисунку зображене дерево T_3).



Ототожнимо кожне кодове слово з відповідною вершиною дерева T_m. Для кожного $i \in \{1, \ldots, n\}$, нехай A_i — множина усіх слів довжини m, початками яких є кодове слово $a(i)$. При нашому ототожненні, вершина b належить підмножині A_i тоді і лише тоді, якщо b — кінцева вершина дерева T_m і існує напрямлений шлях від $a(i)$ до b. Оскільки код a префіксний, то підмножини A_j, A_i, що відповідають різним кодовим словам $a(j), a(i)$ не перетинаються. Значить, $\sum\limits_{i=1}^{n} |A_i| \leq 2^m$ і залишилось зауважити, що $|A_i| = 2^{m-l(i)}$.

Достатність проілюструємо на прикладі: $l(1) = 1, l(2) = 2, l(3) = 3, 2^{-1} + 2^{-2} + 2^{-3} \leq 1$. Ми побудуємо префіксний код $\{a(1), a(2), a(3)\}$ з відповідними довжинами кодових слів. Спочатку на лівій гілці дерева T_3 візьмемо слово $a(1) = (0)$ довжини $l(1) = 1$. Оскільки $2^{3-l(1)} < 2^3$, то існує найближче до $a(1)$ справа слово $b(1)$ довжини $l(1)$, у нашому випадку $b(1) = (1)$. Допишемо до $b(1)$ справа $l(2) - l(1)$ нулів, отримаємо $a(2) = (1, 0)$. Оскільки $2^{3-l(1)} + 2^{3-l(2)} < 2^3$, існує найближче до $a(2)$ справа слово $b(2)$ довжини $l(2)$, у нашому випадку $b(2) = (1, 1)$. Допишемо до $b(2)$ справа $l(3) - l(2)$ нулів, отримаємо $a(3) = (1, 1, 0)$. Префіксність коду $\{a(1), a(2), a(3)\}$ випливає безпосередньо з його побудови. $\square$

Ми застосуємо нерівність Крафта до оцінки сердньої довжини $L_{\min}(p)$ p-оптимального префіксного коду, одержаної Шеноном.

Теорема 0.15.5. *Якщо* $p = (p(1), \dots, p(n)), p(1) > 0, \dots, p(n) > 0$, *то*

$$H(p) \leq L_{\min}(p) < H(p) + 1.$$

Доведення. Ми почнемо з лівої нерівності. Нехай $l(1), \dots, l(n)$ — довжини кодових слів деякого p-оптимального префіксного коду для задачі $(X, p, 2^X)$. Вважаймо,

$$Q = \sum_{i=1}^{n} 2^{-l(i)}, q(i) = 2^{-l(i)} Q^{-1}.$$

Тоді $q = (q(1), \dots, q(n))$ — розподіл ймовірностей. Із нерівності Крафта випливає, що $Q \leq 1$, а тому $\log q \leq 0$. За четвертою властивістю ентропії

$$H(p) \leq -\sum_{i=1}^{n} p(i) \log(2^{-l(i)} Q^{-1}) =$$

$$= \sum_{i=1}^{n} p(i) l(i) + \sum_{i=1}^{n} p(i) \log Q \leq L_{\min}(p).$$

У випадку, коли $Q = 1$ і $q(i) = p(i)$ для всіх $i \in \{1, \dots, n\}$, ми отримали навіть $H(p) = L_{\min}(p)$. Ця рівність справедлива тоді і тільки тоді коли $\sum_{i=1}^{n} 2^{-l(i)} = 1$ і $p(i) = 2^{-l(i)}$, тобто $l(i) = -\log p(i)$.

Для доведення правої нерівності позначмо $l'(i) = \lceil -\log p(i) \rceil$. Оскільки $l'(i) \geq -\log p(i)$, то

$$p(i) \geq 2^{-l'(i)}, 1 = \sum_{i=1}^{n} p(i) \geq \sum_{i=1}^{n} 2^{-l'(i)}.$$

Із нерівності Крафта випливає існування префіксного коду з довжинами кодових слів $l'(1), \dots, l'(n)$. Значить

$$L_{\min}(p) \le \sum_{i=1}^{n} p(i) l'(i) < \sum_{i=1}^{n} p(i)(-\log p(i) + 1) = H(p) + 1.$$

□

З доведення теореми випливає такий наслідок: якщо $\log p(i)$ — ціле число для кожного $i \in \{1, \dots, n\}$, то $H(p) = L_{\min}(p)$.

За теоремою Шенона сердня довжина p-оптимальної стратегії для задачі $(X, p, 2^X)$ з точністю ≤ 1 дорівнює ентропії $H(p)$. Тому, чим більша ентропія, тим довше у серднього триває оптимальний пошук. Нульову ентропію мають лише ті розподіли p, для яких $p(i) = 1$ для деякого i. З іншого боку, ентропія рівномірного розподілу p_n дорівнює $\log n$. Якщо $n = 2^m$, то p_n — оптимальна стратегія має сердню довжину $\log n$. Отже, у цьому випадку абсолютна довжина мінімальної стратегії співпадає із сердньою довжиною p-оптимальної стратегії. За п'ятою властивістю ентропії рівномірний розподіл має найбільшу ентропію, а тому є найгіршим з точки зору пошуку.

Для побудови p-оптимального префіксного коду, або, що те ж саме, p-оптимальної стратегії пошуку для задачі $(X, p, 2^X)$, застосовується алгоритм Хафмана, що грунтується на трьох допоміжних лемах.

Лема 0.15.6. *Якщо $p(1) \ge \dots \ge p(n)$, то існує p-оптимальний префіксний код такий, що $l(1) \le \dots \le l(n)$.*

Доведення. Нехай $\{a(1), \dots, a(n)\}$ — довільний p-оптимальний префіксний код. Припустімо, що $i < j$, але $l(i) > l(j)$. Міняючи місцями кодові слова $a(i), a(j)$, ми не збільшимо сердню довжину коду. Тому скінченним числом транспозикцій можна досягти бажаного результату. □

Лема 0.15.7. *Якщо* $p(1) \geq \cdots \geq p(n)$, *то існує* p*-оптимальний префіксний код такий, що* $l(1) \leq \cdots \leq l(n-1) = l(n)$, *причому кодові слова* $a(n-1), a(n)$ *відрізняються лише останнім символом.*

Доведення. За леммою 0.15.6 існує p-оптимальний префіксний код $a = \{a(1), \dots, a(n)\}$ такий, що $l(1) \leq \cdots \leq l(n)$. Вважаймо $l = l(n)$ і

$$b(n) = (a_1(n), \dots, a_{l-1}(n), 1 - a_l(n)).$$

Припустімо, що $b(n)$ не є кодовим словом із a. Розглянемо код $a' = \{a(1), \dots, a(n-1), a'(n)\}$, де $a'(n) = (a_1(n), \dots, a_{l-1}(n))$. Оскільки $b(n) \notin a$ і $a(n)$ — слово максимальної довжини у коді a, то a' — префіксний код. Але $L(a') < L(a)$, що суперечить p-оптимальності коду a. Отже, $b(n) \in a$, тобто $b(n) = a(m)$ для деякого $m \in \{1, \dots, n-1\}$. Міняючи у коді a місцями слова $a(m), a(n-1)$, ми не збільшимо сердню довжину коду, алу досягнемо мети. □

Лема 0.15.8. *Нехай* $p = (p(1), \dots, p(n)), p(1) \geq \cdots \geq p(n), p' = (p(1), \dots, p(n-2), p(n-1) + p(n)), a' = \{a'(1), \dots, a'(n-1)\}$ — *деякий* p'*-оптимальний префіксний код. Нехай* $a = \{a(1), \dots, a(n)\}$, *де* $a(1) = a'(1), \dots, a(n-2) = a'(n-2)$, *а слова* $a(n-1), a(n)$ *одержано дописуванням до* $a'(n-1)$ *справа відповідно 0 і 1. Тоді* a — p*-оптимальний префіксний код і*

$$L_{\min}(p) = L_{\min}(p') + p(n-1) + p(n).$$

Доведення. Безпосередньо з означення коду a випливає, що

$$L_{\min}(p) \leq L(a) = L(a') + p(n-1) + p(n) = L_{\min}(p') + p(n-1) + p(n).$$

Нехай b — p-оптимальний префіксний код, що задовольняє лему 0.15.7. Позначимо $b'(1) = b(1), \dots, b'(n-1) = b(n-2)$ і нехай $b'(n-1)$ — слово $b(n-1)$, скорочене на останній символ. Ясно, що b' — префіксний код і

$$L_{\min}(p) = L(b) = L(b')+p(n-1)+p(n) \geq L_{\min}(p')+p(n-1)+p(n).$$

Отже, $L_{\min}(p) = L_{\min}(p') + p(n-1) + p(n), L_{\min}(p) = L(a)$, а тому код a p-оптимальний. □

Алгоритм Хафмана складається з двох етапів: згортки і розгортки.

Згортка. Пронумеруємо елементи множини $X = \{i_1, \ldots, i_n\}$ так, щоб $p(i_1) \geq \cdots \geq p(i_n)$.

Якщо $n \geq 2$, замінимо елементи i_{n-1}, i_n на новий символ $[i_{n-1}, i_n]$, припишемо йому ймовірність $p([i_{n-1}, i_n]) = p(i_{n-1}) + p(i_n)$. Викреслимо $i_{n-1}, i_n, p(i_{n-1}), p(i_n)$ із відповідних списків. Помістимо число $p([i_{n-1}, i_n])$ у список апріорних ймовірностей так, щоб зберігався порядок за спаданням. Поставимо символ $[i_{n-1}, i_n]$ на те ж саме місце у список елементів. Будемо повторювати ці дії доти, поки не залишаться два елементи. Зіставимо з цимим елементами кодові слова 0 і 1.

Розгортка. Прогляньмо тепер список наших дій на етепі згртки у зворотньому порядку. Якщо елементи N, M були замінені символом $[N, M]$ і $a([N, M])$ — вже визначене кодове слово для $[N, M]$, то кодові слова $a(N), a(M)$ одержимо дописуючи до $a([M, N])$ відповідно 0 і 1. Розгортка закінчується, коли кожен елемент $x \in X$ отримає свій код $a(x)$; p — оптимальність коду $\{a(x) : x \in X\}$ випливає з лем 0.15.6-0.15.8.

Розгляньмо приклад: $n = 5, p(1) = 0,15, p(2) = 0,20, p(3) = 0,10, p(4) = 0,15, p(5) = 0,40$. Згоркта за алгоритмом Хафмана виглядає так:

5	0,40	5	0,40	5	0,40	[[2,1],[4,3]]	0,60
2	0,20	[4,3]	0,25	[2,1]	0,35	5	0,40
1	0,15	2	0,20	[4,3]	0,25		
4	0,15	1	0,15				
3	0,10						

Розгортка за алгоритмом Хафмана виглядає так:

[[2,1],[4,3]]	1	5	1	5	1	5	$1 = a(5)$
5	0	[2,1]	00	[4,3]	01	2	$000 = a(2)$
		[4,3]	01	2	000	1	$001 = a(1)$
				1	001	4	$010 = a(4)$
						3	$011 = a(3)$

Середня довжина побудованого p-оптимального коду дорівнює 2,2.

Коментар. Докладніше про теорію дискретного пошуку та її застосування можна почитати в [**1**], [**2**].

Бібліоґрафія

[1] Альсведе Р., Вегенер И. Задачи поиска, М., "Мир 1982.

[2] Протасов І. В. Елементи дикретного пошуку (навчальний посібник), "Київський університет 2000.

0.16. Циклічні вимірювання і циклічні решітки

Ми розглянемо спеціальний клас решіток, що виникли при розробці фазо-метричних систем. Решітка — це класичний об'єкт геометрії чисел, основи якої закладено Германом Мінковським.

Нехай $a_1, \dots, a_n$ — лінійно незалежна система векторів з $\mathbb{R}^n$. *Решіткою* з базисом $a_1, \dots, a_n$ називають множину

$$L(a_1, \dots, a_n) = \{z_1 a_1 + \dots + z_n a_n : z_1, \dots, z_n \in \mathbb{Z}\}$$

Решітки також можна визначити як дисктерні підгрупи рангу n із $\mathbb{R}^n$, а саме, підмножина L із $\mathbb{R}^n$ є решіткою, якщо

(i) $a \pm b \in L$ для будь-яких $a, b \in L$;

(ii) L містить деяку систему лінійно незалежних векторів простору $\mathbb{R}^n$;

(iii) нуль вектор θ — ізольована точка множини L, тобто існує окіл точки θ, що не містить інших елементів із L.

Зрозуміло, що базис решітки визначений неоднозначно: решітка може мати багато базисів. Як перевірити, чи є дана система лінійно незалежних векторів $b_1, \ldots, b_n$ базисом решітки $L = L(a_1, \ldots, a_n)$? З алгебраїчної точки зору, для цього необхідно і достатньо, щоб матриця F переходу від базису $a_1, \ldots, a_n$ до базису $b_1, \ldots, b_n$ була цілочисельною і унімодулярною $|\det F| = 1$. З геометричної — паралелепіпед

$$P(b_1, \ldots, b_n) = \{x_1 b_1 + \cdots + x_n b_n : 0 \leq x_1, \ldots, x_n \leq 1\}$$

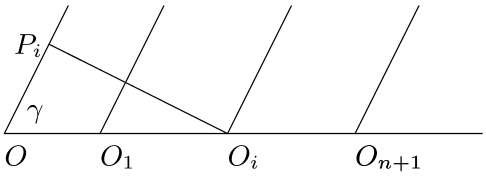
має бути порожнім відносно L, тобто не містити елементів решітки L, відмінних від вершин $i_1 b_1 + \cdots + i_n b_n$, де $i_1, \ldots, i_n \in \{0, 1\}$. Паралелепіпед, визначений довільним базисом решітки L, називають *основним.* Як відомо з курсу лінійної алгебри, об'єм паралелепіпеда, натягнутого на вектори $a_1, \ldots, a_n$ дорівнює модулю визначника, рядками якого є вектори $a_1, \ldots, a_n$. Будь-які два основні паралелепіпеди решітки L мають однаковий об'єм, що називається *визначником решітки* L і позначається $\det L$.

Нехай a — вектор із $\mathbb{R}^n$ з раціональними координатами,

$$S(a) = \{ka + z : k \in \mathbb{Z}, z \in \mathbb{Z}^n\}.$$

Легко переконатися, що $S(a)$ — дискретна підгрупа рангу n із $\mathbb{R}^n$, а тому $S(a)$ є решіткою. Оскільки фактор-група $S(a)/\mathbb{Z}^n$ є циклічною, природно решітку $S(a)$ називати *циклічною.* Циклічні решітки виникли з такої моделі фазових вимірювань.

Вимірювачі $O, O_1, \ldots, O_n$ розташовано уздовж деякої прямої



Ціль випромінює деякий гармонічний сигнал, довжину якого ми приймемо за одиницю. Крім того, вважаймо що всі числа $d_1 = |OO_1|, \dots, d_{n+1} = |OO_{n+1}|$ цілі, а об'єкт вимірювань настільки віддалений, що промені, які виходять з точок $O, O_1, \dots, O_{n+1}$ у напрямку цілі, паралельні. Нехай P_i — основа перепендикуляра, опущеного з точки O_i на промінь, що виходить з точки O. Позначимо $|OP_i| = \Phi_i$, $[\Phi_i] = k_i$ — ціла частина $\Phi_i, \{\Phi_i\} = \varphi_i$ — дробова частина Φ_i. Пара вимірювачів O, O_i визначає лише число φ_i — різницю фаз сигналів у відповідних точках. Задача полягає в тому, щоб за результатами вимірюваннь $\varphi_1, \dots, \varphi_{n+1}$ визначити кут γ. Оскільки $0 < \gamma < \pi$, досить знайти $\cos\gamma$. В прийнятих позначеннях

$$\cos\gamma = \frac{k_1 + \varphi_1}{d_1} = \cdots = \frac{k_{n+1} + \varphi_{n+1}}{d_{n+1}}.$$

Розгянемо систему рівнянь

$$\frac{k_1 + \varphi_1}{d_1} = \frac{k_{n+1} + \varphi_{n+1}}{d_{n+1}},$$

$$\frac{k_n + \varphi_n}{d_n} = \frac{k_{n+1} + \varphi_{n+1}}{d_{n+1}},$$

де невідомими є цілі числа $k_1, \dots, k_{n+1}$, причому $0 \leq k_i \leq d_i - 1$. Перепишемо цю систему так

$$k_i d_{n+1} + \varphi_i d_{n+1} = k_{n+1} d_i + \varphi_{n+1} d_i, i \in \{1, \dots, n\}.$$

Позначимо $\psi_i = \varphi_i d_{n+1} - \varphi_{n+1} d_i, i \in \{1, \dots, n\}$. Тоді k_{n+1} задовольняє систему порівнянь

$$(*) \quad k_{n+1} d_i \equiv \psi_i (\operatorname{mod} d_{n+1}), i \in \{1, \dots, n\},$$

причому $0 \leq k_{n+1} \leq d_{n+1} - 1$. Якщо результати вимірювань не містять похибок, то, очевидно, система має розв'язок. Припустімо, що НСД$(d_1, \dots, d_{n+1}) = 1$ і переконаймося, що система має єдиний розв'язок. Нехай k_{n+1}, k'_{n+1} — два розв'язки системи. Тоді d_{n+1} ділить $d_i(k_{n+1} - k'_{n+1})$ для всіх

$i \in \{1, \ldots, n\}$. Підберемо такі цілі числа $u_1, \ldots, u_{n+1}$ так, що $d_1 u_1 + \cdots + d_{n+1} u_{n+1} = 1$. Тоді

$$d_1(k_{n+1} - k'_{n+1})u_1 + \cdots + d_{n+1}(k_{n+1} - k'_{n+1})u_{n+1} = k_{n+1} - k'_{n+1}.$$

Оскільки d_{n+1} ділить ліву частину, то $d_{n+1}|k_{n+1} - k'_{n+1}$. Оскільки $0 \leq k_{n+1}, k'_{n+1} \leq d_{n+1} - 1$, то $|k_{n+1} - k'_{n+1}| < d_{n+1}$ і $k_{n+1} = k'_{n+1}$.

Отже, якщо вимірювачі розташовано так, що НСД$(d_1, \ldots, d_{n+1}) = 1$ (надалі ми вважаємо цю умову виконаною), то визначити кут γ можна розв'язавши відповідну систему порівнянь. Позначимо через $S[d_1, \ldots, d_{n+1}]$ циклічну решітку $S(a) = \{ka + z : k \in \mathbb{Z}, z \in \mathbb{Z}^n\}$, визначену вектором $a = (\frac{d_1}{d_{n+1}}, \ldots, \frac{d_n}{d_{n+1}})$. Зауважимо також, що кожну циклічну решітку в $\mathbb{R}^n$ можна подати як $S[d_1, \ldots, d_{n+1}]$ при відповідному виборі цілих чисел $d_1, \ldots, d_{n+1}, d_{n+1} > 0$. Розв'язати систему порівнянь (*) — це значить за заданою точкою $\psi = (\frac{\psi_1}{d_{n+1}}, \ldots, \frac{\psi_n}{d_{n+1}})$ решітки $S[d_1, \ldots, d_{n+1}]$ знайти ціле число $k_{n+1}, 0 \leq k_{n+1} \leq d_{n+1} - 1$ і вектор $z \in \mathbb{Z}^k$, такі що $\psi = k_{n+1}a + z$. Таким чином ми приходимо до *задачі параметризації* векторів циклічної решітки.

Оскільки кожен вектор решітки однозначно розкладається за базисом решітки, достатньо знайти деякий базис решітки $S(a)$ і параметризувати вектори базису. Ми можемо вважати, що $a = (\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n})$, де $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$ — нескорочувані дроби, $q_1 > 0, \ldots, q_n > 0$. Позначимо

$$S_i = \{(x_1, \ldots, x_n) \in S(a) : x_1 = \cdots = x_{i-1} = 0, x_i > 0\},$$

$$m_i = \min\{x_i : (x_1, \ldots, x_i, \ldots, x_n) \in S_i\}.$$

Нехай для кожного $i \in \{1, \ldots, \}$ ми вибрали вектор $a_i \in S_i$ так, що i-а коордтната a_i дорівнює m_i. Переконаймося, що вектори $a_1, \ldots, a_n$ утворюють базис решітки $S(a)$. Нехай

$$b = \lambda_1 a_1 + \cdots + \lambda_n a_n \in S(a), 0 \leq \lambda_i \leq 1.$$

Тоді $b = (\lambda_1 m_1, \dots)$ і за означенням m_i, $\lambda_1 = 0$ або $\lambda_1 = 1$. В першому випадку $b = (0, \lambda_2 m_2, \dots)$ і $\lambda_2 = 0$ або $\lambda_2 = 1$. В другому випадку $b - a = (0, \lambda_2 m_2, \dots)$ і, знову ж, $\lambda_2 = 0$ або $\lambda_2 = 1$. Після n-кроків маємо $\lambda_1, \dots, \lambda_n \in \{0, 1\}$. Отже, паралелепіпед $P(a_1, \dots, a_n)$ порожній, що є критерієм базису.

Як практично знайти вектор a_i? Оскільки m_i — i-та координата деякого вектора решітки $S(a)$, то $m_i = \frac{r_i}{q_i}$ для деякого цілого числа r_i. Отже, для визначення вектора a_i слід вказати $r_i, k \in \mathbb{Z}, (z_1, \dots, z_n) \in \mathbb{Z}^n$, такі що

$$kp_1 + z_1 q_1 = 0, \dots, kp_{i-1} + z_{i-1} q_{i-1} = 0, kp_i + z_i q_i = r_i.$$

Враховуючи, що НСД$(p_1, q_1) = \dots =$ НСД(p_{i-1}, q_{i-1}), маємо $q_1 | k_1, \dots, q_{i-1} | k$. Нехай $s_i =$ НСК$(q_1, \dots, q_{i-1})$. Тоді $k = s_i t$ для деякого $t \in \mathbb{Z}$. Навпаки, якщо $k = s_i t, t \in \mathbb{Z}$, то знайдуться $z_1, \dots, z_{i-1} \in \mathbb{Z}$, такі що $kp_1 + z_1 q_1 = \dots = kp_{i-1} + z_{i-1} q_{i-1} = 0$. Отже, задача зводиться до знаходження $t, z_i \in \mathbb{Z}$, таких що $s_i p_i t + q_i z_i = r_i$. З подільності чисел випливає, що

$$\min_{t, z_i} \{s_i p_i t + z_i q_i : s_i p_i t + z_i q_i > 0\} = \text{НСД}(s_i p_i, q_i).$$

Оскільки НСД$(p_i, q_i) = 1$, маємо

$$r_i = \text{НСД}(s_i, q_i) = \text{НСД}(\text{НСК}((q_1, \dots, q_{i-1}), q_i).$$

Використовуючи алгоритм Евкліда, підбираємо $t, z_i \in \mathbb{Z}$, такі що $s_i p_i t + z_i q_i = r_i$. Позначимо $a_i = ka + z$, де $k = s_i t$, $z = (z_1, \dots z_n) \in \mathbb{Z}$, координати $z_1, \dots, z_{i-1}$ одержимо із співвідношень $kp_1 + z_1 q_1 = \dots = kp_{i-1} + z_{i-1} q_{i-1} = 0$, координату z_i вже визначено, решту координат $z_{i_1}, \dots, z_n$ визначаємо довільно.

Приклад 0.16.1. Нехай $a = (\frac{1}{2}, \frac{2}{5}, \frac{3}{7}, \frac{1}{8})$. Знайдемо базис решітки $S(a)$ і параметризацію базисних векторів.

1) $a_1 = (\frac{1}{2}, \frac{2}{5}, \frac{3}{7}, \frac{1}{8}) = 1 \cdot a_1 + (0, 0, 0, 0)$.

2) $s_2 =$ НСК$(q_1) = 2, r_2 =$ НСД$(s_2, q_2) =$ НСД$(2, 5) = 1$.

Із співвідношення $s_2 p_2 t + z_2 q_2 = 4t + 5z_2 = 1$ маємо $t = -1, z_2 = 1$. Отже, $k = s_2 t = -2, z_1 = -\frac{kp_1}{q_1}, z_3 = z_4 = 0$ і

$$a_2 = (0, \frac{1}{5}, -\frac{6}{7}, -\frac{1}{4}) = -2a + (1, 1, 0, 0).$$

3) $s_3 = \text{НСК}(q_1, q_2) = 10, r_3 = \text{НСД}(s_3, q_3) = \text{НСД}(10, 7) = 1$. Із співіношення $s_3 p_3 t + z_3 q_3 = 30t + 7z_3 = r_3 = 1$ маємо $t = 4$, $z_3 = -17, k = 40$. Отже, $z_1 = -\frac{kp_1}{q_1} = -20, z_2 = -\frac{kp_2}{q_2} = -15, z_4 = 0$ і

$$a_3 = (0, 0, \frac{1}{7}, 5) = 40a + (-20, -16, -17, 0).$$

4) $s_4 = \text{НСК}(q_1, q_2, q_3) = 70, r_4 = \text{НСД}(s_4, q_4) = \text{НСД}(70, 8) = 2$. Із співідношення $s_4 p_4 t + z_4 q_4 = 70t + 8z_4 = 2$ маємо $t = 3, z_4 = -26$. Отже, $k = s_4 t = 210, z_1 = -\frac{kp_1}{q_1} = -105, z_4 = -\frac{kp_2}{q_2} = -84, z_3 = -\frac{kp_3}{q_3} = -90$ і

$$a_4 = (0, 0, 0, \frac{1}{4}) = 210a + (-105, -84, -90, -26).$$

Повертаючись до побудови базису $a_1, \ldots, a_n$ решітки $S(a)$, зауважимо, якщо числа $q_1, \ldots, q_n$ попарно взаємно прості, то $r_i = \text{НСД}(q_i, \text{НСК}(q_1, \ldots, q_{i-1})) = 1, a_i = (0, \ldots, 0, \frac{1}{q_i}, \ldots)$. Шляхом елементарних цілочисельних перетворень від базису $a_1, \ldots, a_n$ легко перейти до базису $\frac{1}{q_1}e_1, \ldots, \frac{1}{q_n}e_n$, де $e_1, \ldots, e_n$ — стандартний базис прстору $\mathbb{R}^n$. Спрвджується також і звортнє твердження: якщо циклічна решітка $S(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n})$ має базис, що складається з векторів, пропорційних до векторів стандартного базису $e_1, \ldots, e_n$, то числа $q_1, \ldots, q_n$ попарно взаємно прості.

Алгоритмом параметризації проблематику фазових вимірювань далеко не вичерпано, адже цей алгоритм розраховано лише на ідеальну ситуацію, коли всі вимірювання точні.

Якщо ж при визначенні різниці фаз виникли похибки, то точка ψ обчислена за $\varphi_1, \ldots, \varphi_n$, як правило, не належить решітці $S[d_1, \ldots, d_{n+1}]$, а тому алгоритм параметризації застосовувати не можна. Що ж робити в цьому випадку? Природні припущення про ймовірносний характер похибок (наприклад, нормальність щільності розподілу) призводить до того, що точку ψ слід замінити найближчою в евклідовій метриці точкою решітки, а далі, параметризувати цю точку і знайти кут γ. Таким чином, ми приходимо до *задачі декодування.* Зауважмо, що збільшення числа вимірювачів при їх відповідному розміщенні зменшує ймовірність помилки при декодуванні за принципом максимальної правдоподібності. Спробуємо розкласти точку ψ за деяким базисом решітки $\psi = \alpha_1 a_1 + \cdots + \alpha_n a_n$, а потім округлити коефіцієнти розкладу. Наївно було б вважати, що таким чином завжди ми одержимо точку решітки, найближчу до ψ. Можна було б вчинити перебір деякої скінченної множини точок решітки і виявити серед них найближчу точку до ψ, але справа у тому, що задачу декодування необхідно розв'язувати постійно в режимі "час не чекає". Таким чином, виникає потреба в циклічних решітках і фазометричних системах з простими і ефективними алгоритмами декодування. Найважливіший клас таких решіток — *ортогональні циклічні решітки,* тобто циклічні решітки, що мають базис з попарно ортогональних векторів. Деякі приклади таких решіток вказано нижче. Серед ортогональних циклічних решіток виокремлюється ортонормовані, тобто циклічні решітки, що мають ортогональний базис з векторів однакової довжини. Саме на цих решітках досягається мінімум ймовірності помилки при декодуванні за принципом максимальної правдоподібності, звичайно, якщо вони існують в класі циклічних решіток з заданим визначником. Алгоритм декодування для ортогональних решіток тривіальний і полягає в округленні коефіцієнтів розкладу точки за ортогональним базисом решітки.

Для дослідження ортогональних циклічних решіток ми скористаємося дуальним до решітки L в $\mathbb{R}^n$ об'єктом — *дуальною решіткою*

$$L^* = \{x \in \mathbb{R}^n : (x, y) \in \mathbb{Z} \text{ для будь-якого } y \in L\},$$

де $(\cdot, \cdot)$ — стандартний скалярний добуток в $\mathbb{R}^n$. Зауважимо, що $(L^*)^* = L$ і з $L_1 \subseteq L_2$ випливає $L_2^* \supseteq L_1^*$. Якщо A — матриця, рядками якої є вектори базису решітки L, то вектор-рядки матриці $(A^{-1})^T$ складають базис решітки L^*. Звідси випливає, що $\det L^* = (\det L)^{-1}$ і решітка L ортогональна тоді і лише тоді, коли ортогональна решітка L^*. Точніше, нехай $a_1, \ldots, a_n$ — ортогональний базис решітки L із $\mathbb{R}^n$, $A = (\alpha_{ij})_{n \times n}$ — матриця з рядками $a_1, \ldots, a_n, A_{ij}$ — алгебраїчне допонення елементу α_{ij}. Тоді $\frac{1}{|a_1|^2} a_1, \ldots, \frac{1}{|a_n|^2} a_n$ — ортогональний базис решітки L^* і має місце співідношення ортогональності

$$|a_i|^2 A_{ij} = \alpha_{ij} \det A,$$

де $|a|$ — евклідова довжина вектора a.

Дуальну до циклічної решітки $S[d_1, \ldots, d_{n+1}]$ позначимо $S^*[d_1, \ldots, d_{n+1}]$ і назвемо *коциклічною.* Вектор $x \in \mathbb{R}^n$ належить коциклічній решітці $S^*[d_1, \ldots, d_{n+1}]$ тоді і тільки тоді, коли $(x, a) \in \mathbb{Z}$, де $a = (\frac{d_1}{d_{n+1}}, \ldots, \frac{d_n}{d_{n+1}})$. Крім того, із $S[d_1, \ldots, d_{n+1}] \supset \mathbb{Z}^n, (\mathbb{Z}^n)^* = \mathbb{Z}^n$, випливає що $S^*[d_1, \ldots, d_{n+1}] \subseteq \mathbb{Z}^n$. Коциклічну решітку $S^*[d_1, \ldots, d_{n+1}]$ можна визначити також як множинук усіх цілочисельних розв'язків порівняння

$$d_1 x_1 + \cdots + d_n x_n \equiv 0 (\bmod d_{n+1}).$$

Оскільки індекс підгрупи $S^*[d_1, \ldots, d_{n+1}]$ в $\mathbb{Z}^n$ дорівнює d_{n+1} і $\det \mathbb{Z}^n = 1$, то $\det S^*[d_1, \ldots, d_{n+1}] = d_{n+1}$ і $\det S[d_1, \ldots, d_{n+1}] =$

d_{n+1}^{-1}. Стандартні міркування (див **[7]**) з курсу лінійної алгебри дають критерій коциклічності і циклічності.

Теорема 0.16.1. *Нехай $a_1, \ldots, a_n$ — лінійно незалежна система векторів із $\mathbb{Z}^n$, A — матриця, рядками якої є вектори $a_1, \ldots, a_n$. Решітка $L(a_1, \ldots, a_n)$ коциклічна тоді і тільки тоді, коли НСД мінорів $(n-1)$-го порядку матриці A дорівнює 1.*

Теорема 0.16.2. *Нехай $a_1, \ldots, a_n$ — лінійно незалежна система векторів із $\mathbb{R}^n$ з раціональнимим координатами, $A = (a_{ij})_{n \times n}$ — матриця, рядками якої є вектори $a_1, \ldots, a_n$. Решітка $L(a_1, \ldots, a_n)$ циклічна тоді і тільки тоді, коли матриця A^{-1} цілочисельна і НСД чисел $\alpha_{ij} \det A^{-1}, i, j \in \{1, \ldots, n\}$, дорівнює 1.*

Задачу характеризації ортогональних циклічних решіток можна розуміти двояко. А саме, можна вимагати критерію, що дозволяє за заданими маштабними коефіцієнтами $d_1, \ldots, d_{n+1}$ ефективно визначити, чи є циклічна решітка $S[d_1, \ldots, d_{n+1}]$ ортогональною і, в разі позитивної відповіді, вказати її ортогональний базис [**4**, задача 9.45]. На цьому шляху ми дамо критерій ортонормованості і вкажемо ряд достатніх ознак ортогональності. Про інші достатні ознаки ортогональності див. [**1**]. Якщо послабити запити, приходимо до задачі характеризації ортогональних циклічних решіток з точністю до масштабних коефіцієнтів. Річ у тім, що різні набори масштабних коефіцієнтів можуть визначати одну й ту ж циклічну решітку. Проблема полягає в тому, щоб визначити для кожної ортогональної циклічної решітки хоча б один набір масштабних коефіцієнтів, що її задає. Ми розв'яжемо цю проблему для плоских циклічних решіток.

Теорема 0.16.3. *Коциклічна решітка L із $\mathbb{R}^2$ ортогональна тоді і тільки тоді, коли знайдуться цілі числа p, q, u, v,* *такі що НСД*$(p,q) =$ *НСД*$(u,v) = 1$ *і* $L = L(a_1,a_2)$*, де*

$$a_1 = (pu,qu), a_2 = (qv,-pv).$$

Додаткова умова $u^2 = v^2 = 1$ *забезпечує ортонормованість* L.

Доведення. Нехай $a_1 = (a_{11},a_{12}), a_2 = (a_{21},a_{22})$ — ортогональний базис коциклічної решітки L. Тоді $a_{11}a_{21}+a_{12}a_{22} = 0$ і $\frac{a_{11}}{a_{12}} = -\frac{a_{22}}{a_{21}} = \frac{p}{q}$, де НСД$(p,q) = 1$. Отже, $a_{11} = \frac{p}{q}a_{12}, a_{22} = -\frac{p}{q}a_{21}$. Оскільки $a_{11},a_{22} \in \mathbb{Z}$, то $q|a_{12}, q|a_{21}$ і $a_{12} = qu$, $a_{21} = qv, u,v \in \mathbb{Z}$. Значить, $a_1 = (pu,qu), a_2 = (qv,-pv)$. За теоремою 0.16.1, НСД$(pv,qv,pu,qu) = 1$. Оскільки НСД$(pu,qu) = u$, НСД$(pv,qv) = v$, то НСД$(u,v) = 1$. Навпаки, нехай $L = L(a_1,a_2), a_1 = (pu,qu), a_2 = (qv,-pv)$ і НСД$(p,q) =$ НСД$(u,v) = 1$. Ортогональність решітки L очевидна. Якщо k — простий дільник чисел pu,qu,pv,qv, то $k|u$, $k|v$, що суперчить умові НСД$(u,v) = 1$. Отже, НСД$(pu,qu,pv,qv) = 1$ і за теоремою 0.16.1 решітка L коциклічна.

Для доведення другого твердження теореми зауважимо, що умова $|a_1| = |a_2|$ рівносильна $p^2(u^2-v^2) = q^2(v^2-u^2)$, тобто $u^2 = v^2$ і з урахуванням НСД$(u,v) = 1$, $v^2 = u^2 = 1$. □

Теорема 0.16.4. *Циклічна решітка* $S[d_1,d_2,d_3]$ *в* $\mathbb{R}^2$ *ортонормована тоді і тільки тоді, коли* $d_1^2 + d_2^2 \equiv 0(\bmod d_3)$.

Доведення. За теоремою 0.16.3 циклічна решітка S ортонормована тоді і тільки тоді, коли знайдуться цілі числа p,q,u,v, такі що НСД$(p,q) = 1, u^2 = v^2 = 1$ і $S^* = L(a_1,a_2)$, де $a_1 = (pu,qu), a_2 = (qv,-pv)$. Змінюючи напрямки базисних векторів, ми можемо вважати, що $u = v = 1$. З іншого боку, числа d_1,d_2,d_3 задають решітку S тоді і тільки тоді, коли НСД$(d_1,d_2,d_3) = 1$, $(a,a_1) \in \mathbb{Z}, (a,a_2) \in \mathbb{Z}$, де $a = (\frac{d_1}{d_3},\frac{d_2}{d_3})$. При цьому $\det S^* = p^2+q^2$. Отже, ортонормованість решітки

$S[d_1, d_2, d_3]$ рівносильна існуванню цілих чисел p, q, таких що НСД$(p, q) = 1, d_3 = p^2 + q^2$ і

$$d_1 p + d_2 q \equiv 0(\bmod d_3),$$

$$d_1 q - d_2 p \equiv 0(\bmod d_3).$$

Припустімо, що решітка $S[d_1, d_2, d_3]$ ортонормована і виберемо цілі числа p, q, що задовольняють вказані умови. Піднесемо порівіняння до квдрату, додамо їх і скоротимо на $p^2 + q^2 = d_3$. Одержимо $d_1^2 + d_2^2 \equiv 0(\bmod d_3)$.

Нехай НСД$(d_1, d_2, d_3) = 1, d_1^2 + d_2^2 \equiv (\bmod d_3)$. Зауважимо, що НСД$(d_1, d_3) =$ НСД$(d_2, d_3) = 1$. Для доведення ортонормованості решітки $S[d_1, d_2, d_3]$ досить переконатися, що вона інваріантна щодо повороту площини на $\frac{\pi}{2}$. У свою чергу, останнє твердження рівносильно тому, що вектор $(-\frac{d_2}{d_3}, \frac{d_1}{d_3})$, одержаний поворотом вектору $(\frac{d_1}{d_3}, \frac{d_2}{d_3})$ належить решітці $S[d_1, d_2, d_3]$. Таким чином, ми прийшли до системи лінійних діофантових рівнянь

$$-d_2 = kd_1 + z_1 d_3,$$

$$d_1 = kd_2 + z_2 d_3,$$

де невідомими є цілі числа k, z_1, z_2, а довести досить лише сумісність цієї системи. Оскільки НСД$(d_2, d_3) =$ НСД$(d_1, d_3) = 1$, то НСД мінорів другого порядку матриці коефіціентів дорівнює d_3. Оскільки $d_3 | (d_1^2 + d_2^2)$, то НСД мінорів другого порядку розширеної матриці також дорівнює d_3, а це, як відомо,є критерієм сумістності системи. □

Для формулювання наступної теореми позначимо через $\gamma(x, y)$ добуток усіх простих чисел, що ділять x, але не ділять y. Якщо таких чисел немає, за означенням $\gamma(x, y) = 1$.

Теорема 0.16.5. *Циклічна решітка S в $\mathbb{R}^2$ ортогональна тоді і лише тоді, коли знайдуться цілі числа p, q, u, v, такі* *що НСД*$(p, q) =$ *НСД*$(u, v) = 1$ *і* $S = S[d_1, d_2, d_3]$, *де*

$$d_1 = \gamma(p^2 + q^2, u)pv + qu, d_2 = -pu + \gamma(p^2 + q^2, u)qv,$$
$$d_3 = (p^2 + q^2)uv.$$

Доведення. Повторюючи початок доведення попередньої теореми, отримаємо таке твердження. Ортогональність решітки $S = S[d_1, d_2, d_3]$ рівносильна існуванню цілих чисел p, q, u, v, таких що НСД$(p, q) =$ НСД$(u, v) = 1$ і $d_3 = (p^2 + q^2)uv$ і

$$d_1pu + d_2qu \equiv 0(\mod d_3),$$
$$d_1qv - d_2pv \equiv 0(\mod d_3).$$

Виразити ці умови у вигляді співвідношень між d_1, d_2, d_3 не вдається. Але формулювання теореми передбачає лише необхідність вказати для кожного набору p, q, u, v хоча б одного розв'язку цієї системи порівнянь, де $d_3 = (p^2 + q^2)uv$ і при цьому забезпечити НСД$(d_1, d_2, d_3) = 1$. Неважко перевірити, що числа d_1, d_2 задовольняють систему, якщо

$$d_1pu + d_2qu = \gamma(p^2 + q^2, u)(p^2 + q^2)uv,$$
$$d_1qv - d_2pv = (p^2 + q^2)uv.$$

Розв'язавши цю систему рівнянь, маємо

$$d_1 = \gamma(p^2 + q^2, u)pv + qu,$$
$$d_2 = -pu + \gamma(o^2 + q^2, u)qv.$$

З умов НСД$(p, q) =$ НСД$(u, v) = 1$ і означення функції γ випливає, що НСД$(d_1, d_2, d_3) = 1$. □

Далі ми переходимо до дослідження ортогональних циклічних решіток в розмірності $n \geq 3$.

Лема 0.16.6. *Якщо* $n \geq 3$ *і* $a_1, \ldots, a_n$ *— ортогональний базис коциклічної решітки* L *в* $\mathbb{R}^n$, *то НСД*$(|a_1|^2, |a_2|^2, |a_3|^3) = 1$.

Доведення. Припустимо супротивне і нехай p — просте число, таке що $p|\,|a_1|^2, |\,|a_2|^2, p|\,|a_3|^2$. Позначимо через k_i невід'ємне ціле число, таке що p^{k_i} ділить $|a_i|^2$, але p^{k_i+1} не ділить $|a_i|^2$, $k_m = \max\{k_1, \dots, k_n\}$. Оскільки решітка L ортогональна, то $|\det A| = |a_1| \dots |a_n|$, де A — матриця, рядками якої є вектори $a_1, \dots, a_n$. Із співвідношенн ортональності випливає, що

$$|a_i|^2 A_{ij}^2 = \alpha_{ij}^2 |a_1|^2 \dots |a_{i-1}|^2 |a_{i+1}|^2 \dots |a_n|^2.$$

Якщо $i \neq m$, то $p^{k_m+1}|\,|a_i|A_{ij}$ і за означенням k_m маємо $p|A_{ij}$. Зафіксуємо j, домножимо співідношення $|a_i|^2 A_{ij} = \alpha_{ij} \det A$ на A_{ij} і просумуємо по $i \in \{1, \dots, m\}$. Отримаємо

$$\sum_{i=1}^{n} |a_i|^2 A_{ij}^2 = (\det A)^2.$$

Оскільки p^{k_m+1} ділить $(\det A)^2$ і всі доданки $|a_i|^2 A_{ij}^2, i \neq m$, то p^{k_m+1} ділить $|a_m|^2 A_{mj}$. За означенням k_m $p|A_{mj}$. Таким чином, p ділить усі мінори A_{ij} матриці A, що суперечить теоремі 0.16.1 ☐

Теорема 0.16.7. *Якщо $n \geq 3$, то $\mathbb{Z}^n$ — єдина ортонормована циклічна решітка в $\mathbb{R}^n$.*

Доведення. Нехай S — ортонормована циклічна решітка в $\mathbb{R}^n, a_1, \dots, a_n$ — ортогональний базис дуальної коциклічної решітки, $|a_1| = \dots = |a_n|$. За лемою 0.16.6 $|a_1| = \dots = |a_n| = 1$, а тому з точністю до нумерації і знаку $a_1, \dots, a_n$ — стандартний базис простору $\mathbb{R}^n$ і $S^* = \mathbb{Z}^*$. ☐

Теореми 0.16.4 та 0.16.7 дають досить елегантний опис усіх ортонормованих циклічних решіток. Проте наслідки цього опису невтішні для застосування, адже циклічна решітка, побудована по реальній системі масштабних коефіцієнтів $d_1 <$

$d_2 < \cdots < d_n$ обов'язково містить нецілочисельний вектор $(\frac{d_1}{d_{n+1}}, \ldots, \frac{d_n}{d_{n+1}})$, а тому відмінна від $\mathbb{Z}^n$. Отже, при $n \geq 3$, розраховувати можна лише на ортогональні циклічні решітки. Ми наведемо одну достатню ознаку ортогональності, що належить С. П. Панасюку.

Теорема 0.16.8. *Циклічна решітка $S[d_1, \ldots, d_{n+1}]$ ортогональна, якщо НСД$(d_1, d_2) = 1$ і*

$$(d_1^2 + d_2^2)|d_3, (d_1^2 + d_2^2 + d_3^2)|d_4, \ldots, (d_1^2 + d_2^2 + \cdots + d_n^2)|d_{n+1}.$$

Доведення. Використовуючи дуальність, досить підібрати такі попарно ортогональні вектори $a_1, \ldots, a_n \in \mathbb{Z}$, що задовольняють порівнянню

$$d_1x_1 + d_2x_2 + \cdots + d_nx_n \equiv 0(\bmod d_{n+1}).$$

і $|a_1||a_2| \ldots |a_n| = d_{n+1}$. Позначимо $\Sigma_i = d_1^2 + \cdots + d_i^2$. Потрібну систему складають вектори

$$\begin{aligned}
a_1 &= \tfrac{d_{n+1}}{\Sigma_{n+1}}(d_1, d_2, \ldots, d_{n-2}, d_{n-1}, d_n),\\
a_2 &= \tfrac{1}{\Sigma_{n-1}}(d_1d_n, d_2d_n, \ldots, d_{n-2}d_n, d_{n-1}d_n, -\Sigma_{n-1}),\\
a_3 &= \tfrac{1}{\Sigma_{n-2}}(d_1d_{n-1}, d_2d_{n-1}, \ldots, d_{n-2}d_{n-1}, -\Sigma_{n-1}, 0),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{n-1} &= \tfrac{1}{\Sigma_2}(d_1d_3, d_2d_3, -\Sigma_2, 0, \ldots, 0, 0, 0),\\
a_n &= \tfrac{1}{\Sigma_1}(d_2, -d_1, 0, \ldots, 0, 0, 0),
\end{aligned}$$

□

Як практично організувати застосування викладених результатів? Замовник визначає набір вимірювачів, вказує їх характеристики за точністю і свої вимоги до ймовірності правильного декодування. Розробник вибирає, скажімо, ортогональну циклічну решітку, що задовольняє вказані умови, і відповідний набір масштабних коефіцієнтів. Може статися, що за об'єктивних обставин встановити вимірювачі у вказаних точках прямої неможливо. Але одну й ту ж циклічну решітку можна задати різними наборами масштабних коефіцієнтів. А тому вихід з цієї ситуації інколи дає така теорема ототожнення.

ТЕОРЕМА 0.16.9. *Нехай* $a = (\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}), b = (\frac{c_1}{t_1}, \ldots, \frac{c_n}{t_n})$, *де* $\frac{p_i}{q_i}, \frac{c_i}{t_i}$ *— нескорочувані дроби,* $p_i \neq 0$, $c_i \neq 0$, $q_i > 0$, $t_i > 0$ *для всіх* $i \in \{1, \ldots, n\}$. *Циклічні решітки* $S(a)$ *і* $S(b)$ *співпадають тоді і тільки тоді, коли*

(i) $q_i = t_i, i \in \{1, \ldots, n\}$,

(ii) $d | q_1 \ldots q_{i-1} q_{i+1} \ldots q_n (p_i c_j - p_j c_i)$, *де*

$$d = \frac{q_1 \ldots q_n}{HCK(q_1, \ldots, q_n)}.$$

Першою відкритою публікацією, в якій викладено вказану модель фазових вимірювань, була стаття [**2**]. Зв'язок з геометрією чисел встановлено в [**5**]. В цій же статті наведено алгоритм параметризації, доведно теорему ототожнення та вказано на деякі її наслідки. Теореми про ортогональні циклічні решітки доведено в [**6**], де також повністю описано циклічні решітки для декодування в метриці $\rho(x, y) = \max |x_i - y_i|$. Досить докладний виклад теорії циклічних решіток, зокрема з доведенням теорем 0.16.1, 0.16.2, 0.16.9 є в [**7**]. Наш виклад матеріалу в основному слідує [**8**]. Схожа за постановкою задача про розташування вимірювачів на прямій розглядається в [**3**].

Бібліоґрафія

[1] Бардаков В. Г. Об ортогональних базисах рациональних решеток, Сиб. мат. ж., 39 (1998) 1236-1250.

[2] Глобенко Ю. В., Скрыпник Г. И. О разрешении неоднозначности циклических измерений, Автометрив. 4 (1972) 63-68.

[3] Дьюдни А. К. О линейках Колонба и их приложениях в радиоастрономии. В мире науки, 1986, №2, 103-107.

[4] Коуровская тетрадь: нерешенние вопроси теории групп, 14-е издю Новосибирск, ИМ СО РАН, 1999.

[5] Попов Ю. Д., Протасов И. В. Циклические решетки, Доп АН УРСР, Сер. А, 1985, №8, 67-69.

[6] Протасов И. В. Коциклические решетки. Доп. АН УРСР, Сер. А, 1987, №1, 61-63.

[7] Протасов И. В., Сарыев А. Решетки и их приложения, Чарджоу, 1988.

[8] Протасов И. В. Циклические измерения и решетки, Математика сегодня, 17 (1992) 26-39.

0.17. Комбінаторика в соціальному виборі

Розглянемо скінченну множину $P = \{p_1, \ldots, p_n\}$, елементи якої називатимемо *учасниками голосування*. Процедура голосування полягає в тому, що кожен з учасників голосування висловлюється "за"або "проти". *Системою голосування* називають правило, яке визначає, прийнято рішення чи ні за результатами процедури голосування.

Назвімо *виграшною коалаіцією* підмножину $Q \subseteq P$, що має таку властивість: якщо кожний елемент з Q проголосував "за а кожний елемент з $P\backslash Q$ проти, то рішення прийнято. Очевидно, що кожна система голосування однозначно задається родиною своїх виграшних коаліцій. Підмножину, що не є виграшною коаліцією, називають *програшною коаліцією.* Якщо кожна надмножин виграшної коаліції є знову виграшною коаліцією, то таку систему називають *монотонною.*

Припустімо, що кожному елементу p_i множини P поставимо у відповідність дійсне число ω_i *(вага* елемента p_i), а також вибрано дійсне число q *(квота).* Означмо систему голосування S на множині P умовою: підмножина $Q \subseteq P$ є виграшною коаліцією в S, якщо і тільки якщо

$$\sum_{p_i \in Q} \omega_i \geq q.$$

Така система голосування називається ваговою. Якщо у ваговій системі голосування всі ваги невід'ємні, то така система голосування є монотонною.

Розглянемо дві довільні коаліції $A_1, A_2 \subseteq \backslash P$ і нехай $B_1 \subseteq A_1 \setminus A_2$, $B_2 \subseteq A_2 \setminus A_1$. Вважаймо

$$\widetilde{A_1} = (A_1 \setminus A_2) \cup B_2, \widetilde{A_2} = (A_2 \setminus B_2) \cup B_1.$$

Перехід від A_1 і A_2 до $\widetilde{A_1}$ і $\widetilde{A_2}$ називається *торгівлею.* Зауважмо, що при торгівлі коаліції обмінюються не обов'язково однаковою кількістю учасників.

Система голосування називається k-*стійкою* до торгівлі, де k — деяке натуральне число, якщо не існує k (не обов'язково різних) виграшних колаіцій, які можна перетворити в k (не обов'язково різних) програшних коаліцій за допомогою послідовності торгівель. Система голосування називається *стійкою* до торгівлі, якщо вона є k-стійкою до торгівлі для будь-якого натурального k.

Комбінаторну характеризацію вагових систем голосування дає така теорема.

ТЕОРЕМА 0.17.1. *Система голосування є ваговою тоді і тільки тоді, коли вона є стійкою до торгівлі.*

Для доведення теореми ми застосуємо геометричний опис вагових систем голосування. Кожній коаліції $A \subseteq P$ відповідає її характеристичний вектор $\vec{A} = (\alpha_1, \dots, \alpha_n)$, координати якого визначаються за правилом: $\alpha_i = 1$, якщо $p_i \in A$ і $\alpha_i = 0$, якщо $p_i \notin A$. При такому зіставленні підмножини множини P перебувають у взаємно однозначній відповідності з вершинами одиничного куба в $\mathbb{R}^n$. Нехай $\mathcal{W}$ (відповідно $\mathcal{L}$) — множина вершин, що відповідає всім виграшним (відповідно програшним) коаліціям системи голосування, яку ми розглядаємо.

Нагадаймо, що гіперплощиною в $\mathbb{R}^n$ називають множину

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n} a_i x_i = c\},$$

де $a_1, \dots, a_n, c$ — деякі сталі, причому серед чисел $a_1, \dots, a_n$ є відмінне від нуля. Гіперплощина ділить простір $\mathbb{R}^n$ на два півпростори

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n} a_i x_i > c\},$$

$$\{(x_1, \dots, x_n) \in \mathbb{R}^n : \sum_{i=1}^{n} a_i x_i < c\}.$$

ЛЕМА 0.17.2. *Система голосування є ваговою, якщо і лише якщо існує гіперплощина в $\mathbb{R}^n$ така, що множини $\mathcal{W}$ і $\mathcal{L}$ лежать у різних півпросторах, на які ця гіперплощина ділить простір $\mathbb{R}^n$.*

ДОВЕДЕННЯ. Припустімо, що система голосування є ваговою, причому вага елемента p_i дорівнює ω_i, а квота — q.

Нехай q' — найбільше з чисел $\sum_{p_i \in L} \omega_i$, де L пробігає родину програшних коаліцій. За означенням, $q' < q$. Припустімо, що $c = (q + q')/2$. Легко видно, що гіперплощина $\sum\limits_{i=1}^{n} \omega_i x_i = c$ є шуканою.

Навпаки, якщо відомо, що гіперплщина $\sum\limits_{i=1}^{n} \omega_i x_i = c$ відокремлює $\mathcal{W}$ і $\mathcal{L}$, то задану систему голосування можна описати як вагову, взявши ω_i за вагу елемента p_i і c за квоту. □

Лема 0.17.3. *Коаліції $A_1, \ldots, A_m$ можуть бути утворені з коаліцій $B_1, \ldots, B_m$ за допомогою послідовності торгівель тоді і лише тоді, коли $\vec{A}_1 + \cdots + \vec{A}_m = \vec{B}_1 + \cdots + \vec{B}_m$.*

Доведення. Досить помітити, що коаліції $A_1, \ldots, A_m$ можна перетворити в коаліції $B_1, \ldots, B_m$ послідовністю торгівель тоді і тільки тоді, коли вони складаються з однакових учасників голосування, з урахування кратності. □

Доведення теореми 0.17.1. Якщо система голосування $\mathcal{S}$ вагова, тоді за лемою 0.17.2 множини $\mathcal{L}$ та $\mathcal{W}$ розділяються гіперплощиною, тобто $\max f(\mathcal{L}) < q < \min f(\mathcal{W})$ для деякого лінійного функціоналу $f : \mathbb{R}^n \to \mathbb{R}$. Тоді для довільних коаліцій $A_1, \ldots, A_m \in \mathcal{L}$ та $B_1, \ldots, B_m \in \mathcal{W}$ отримаємо

$$f(\vec{A}_1 + \cdots + \vec{A}_m) < mq < f(\vec{B}_1 + \cdots + \vec{B}_m).$$

Тобто $\vec{A}_1 + \cdots + \vec{A}_m \neq \vec{B}_1 + \cdots + B_m$ і за лемою 0.17.3, коаліції $A_1, \ldots, A_m$ не можна утворити послідовністю торгівель з коаліцій $B_1, \ldots, B_m$. Це означає, що система голосування $\mathcal{S}$ стійка до торгівлі.

Якщо ж припустити, що система голосування $\mathcal{S}$ невагова, тоді за лемою 0.17.2 множини $\mathcal{L}$ та $\mathcal{W}$ не розділяються жодною гіперплощиною. За теоремою Гана-Банаха, опуклі оболонки $\operatorname{conv}(\mathcal{L})$ та $\operatorname{conv}(\mathcal{W})$ мають спільну точку. Це означає, що система лінійних рівнянь

$$\begin{cases} x_1\vec{A}_1 + \cdots + x_m\vec{A}_m = y_1\vec{B}_1 + \cdots + y_m\vec{B}_m, \\ x_1 + \cdots + x_m = 1, \\ y_1 + \cdots + y_m = 1 \end{cases}$$

має розв'язок $x_1^*, \ldots, x_m^*, y_1^*, \ldots, y_m^* \in [0,1]$. Зауважимо, що ця система має цілі кофіціенти та вільні членип (0 або 1). З теорії систем лінійних рівнянь випливає, що вона допускає раціональний розв'язок $\frac{a_1}{k}, \ldots, \frac{a_m}{k}, \frac{b_1}{k}, \ldots, \frac{b_m}{k}$, де k — натуральне число, $a_1, \ldots, a_m, b_1, \ldots, b_m$ — невід'ємні цілі числа. Після підстановки розв'язку у систему, отримаємо рівність

$$a_1\vec{A}_1 + \ldots a_m\vec{A}_m = b_1\vec{B}_1 + \cdots + b_m\vec{B}_m,$$

причому $a_1 + \cdots + a_m = k = b_1 + \cdots + b_m$.

Розписуючи кожен коефіцієнт a_i, b_i як суму одиниць та застосовуючи лему 0.17.3, робимо висновок: коаліції

$$\underbrace{A_1, \ldots, A_1}_{a_1}, \ldots, \underbrace{A_m, \ldots, A_m}_{a_m}$$

можуть бути утворені з коаліцій

$$\underbrace{B_1, \ldots, B_1}_{b_1}, \ldots, \underbrace{B_m, \ldots, B_m}_{b_m}$$

послідовністю торгівель. Це означає, що система голосування $\mathcal{S}$ не k-стійка до торгівлі. ☐

У багатьох ситуаціях виникає потреба виробити деяке колективне рішення після того як таке рішення прийняв кожен індивідуум з цього колективу. Для формалізації подібних ситуацій, нагадаймо деякі математичні поняття.

Бінарне відношення $\succeq$ на множині X називають *передпорядком,* якщо для довільних $x, y, z \in X$ виконано умови

- $x \succeq x$,

- з $x \succeq y$, $y \succeq z$ випливає $x \succeq z$,
- $x \succeq y$ або $y \succeq x$.

Передпорядок $\succeq$ визначає еквівалентність $\sim$ на множині X за таким правилом: $x \sim y$ тоді і лише тоді, коли $x \succeq y$ і $y \succeq x$. Передпорядок $\succeq$ визначає також відношення строгого перепорядку $\succ$: $x \succ y$ тоді і лише тоді, коли $x \succeq y$ але х нееквівалентний до y. Передпорядок $\succeq$ називають *порядком,* якщо з $x \sim y$ випливає $x = y$.

Розгляньмо скінченну множину $P = \{p_1, \ldots, p_n\}$, елемнти якої називатимемо тепер *виборцями.* Нехай маємо непорожню скінченну множину $A = \{a_1, \ldots, a_m\}$, елементи якої називаємо *альтернативами.* Позначимо через $\mathcal{O}(A)$ та $\mathcal{PO}(A)$ множини усіх порядків та перепорядків на множині A.

Функцією соціальної переваги називається відображення

$$\Phi\mathcal{O}(A)^n \equiv \underbrace{\mathcal{O}(A) \times \cdots \times \mathcal{O}(A)}_{n\text{-разів}} \to \mathcal{PO}(A).$$

Прокоментуймо це означення. Кожен з виборців p_i здійснює своє упорядкування альтернатив $\succeq_i$. Елемент $(\succeq_1, \ldots, \succeq_n))$ множини $\mathcal{O}(A)^n$ називається *груповим профілем.* Груповий профіль зручно зображати таблицею розміру $m \times n$, i-ий стовпцик якої складає упорядкування за спаданням альтернатив, здійснене виборцем p_i. Функція соціальної переваги Φ ставить у відповідність послідовності індивідуальних упорядкуваня (груповому профілеві) колективне упорядкування альтернатив (соціальну перевагу) $\succeq = \Phi(\succeq_1, \ldots, \succeq_n)$. Розгляньмо три приклади.

1. *Голосування більшістю.* Вважаймо, що $x \succeq y$, якщо і тільки якщо

$$|\{i \in \{1, \ldots, n\} : x \succeq_i y\}| \geq n/2.$$

Очевидно, що при $n = 2$ голосування більшістю є функцією соціальної переваги. Якщо число виборців n парне, то відношення $\succeq$ є передпорядком, а не порядком.

Припустімо, що $P = \{p_1, p_2, p_3\}, A = \{a, b, c\}$, і розглянемо груповий профіль

$$\begin{array}{ccc} a & b & c \\ b & c & a \\ c & a & b \end{array}$$

Голосування більшістю дає $a \succeq b$, $b \succeq c$, $c \succeq a$, але не дає $a \succeq c$. Цей приклад, відомий як парадокс Кондорсе, показує, зорема, що при $n > 2, m > 2$ голосування більшістю не є функцією соціальної переваги.

Теорема Мея стверджує, що у випадку двох альтернатив голосування більшістю є єдиною природною і демократичною функцією соціальної переваги.

2. *Диктатура.* Зафіксуймо $i \in \{1, \ldots, n\}$ і вважаймо

$$\succeq_i = \Phi(\succeq_1, \ldots, \succeq_n).$$

Отже елемнт p_i є диктатором і соціальна перевага — це відношення переваги p_i.

3. *Числення Борда.* Розгляньмо груповий профіль, зображений у вигляді таблиці. Для кожного $i \in \{1, \ldots, n\}$ і кожної альтернативи x позначимо через $B_i(x)$ число елемнтів i-ого стовпчика, що розташовані під x. Нехай $B(x) = \sum_{i=1}^{n} B_i(x)$ і $x \succeq y$ якщо і тільки якщо $B(x) \geq B(y)$.

Розглянемо дві природні умови, які повинні задовольняти функція соціальної переваги.

Умова одностайності. Функція соціальної перваги задовольняє цю умову, якщо для кожних $x, y \in A$ з того, що $x \succ_i y$ для кожного $i \in \{1, \ldots, n\}$ випливає $x \succ y$.

Умова незалежності. Нам знадобиться одне допоміжне поняття. Нехай $\succeq_1, \succeq_2 \in \mathcal{PO}(X)$. Кажуть, що $x_1, x_2 \in X$ однаково розміщені щодо $\succeq_1, \succeq_2$, якщо або одночасно $x \succ_1 y$ і $x \succ_2 y$, або одночасно $y \succ_1 x$, $y \succ_2 x$. Нехай тепер

$$(\succeq_1', \ldots, \succeq_n') \in \mathcal{O}(A)^n, (\succeq_1'', \ldots, \succeq_n'') \in \mathcal{O}(A^n),$$

і нехай

$$\succeq' = \Phi(\succeq_1', \ldots, \succeq_n'), \succeq'' = \Phi(\succeq_1'', \ldots, \succeq_n''),$$

де Φ — функція соціальної переваги. Кажуть, що Φ задовольняє умову незалежності від неістотних альтернатив, якщо для кожних $x, y \in A$, з того, що x і y однаково розміщені щодо $\succeq_i', \succeq_i''$ для кожного $i \in \{1, \ldots, n\}$ випливає, що x, y однаково розміщені щодо $\succeq', \succeq''$. Іншими словами, соціальна думка про альтернативи x і y не залежить від жодної іншої алтернативи z.

Нехай $|A| \geq 3$ і функція соціальної переваги $\Phi : \mathcal{O}(A)^n \to \mathcal{PO}(A)^n$ задовольняє умови одностайності і незалежності. Ми покажемо, що $\Phi(\mathcal{O}(A)^n) \subseteq \mathcal{O}(A)$.

Припустимо супротивне: $\succeq = \Phi(\succeq_1, \ldots, \succeq_n)$ і a, b — різні елементи множини A, для яких $a \sim b$(тобто $a \succeq b$ і $b \succeq a$). Нехай $X = \{p_i : a \succ_i b\}$ і $Y = P \setminus X$. За аксіомою незалежності, соціальна думка про a і b не залежить від індивідуальних думок про інші елемнети, а тому, ігноруючи ці елемнти, можемо схематично зобразити ситуацію так:

$$\begin{array}{cc} a \ \ldots \ a & b \ \ldots \ b \\ \underbrace{\underline{a \ \ldots \ a}}_{X} & \underbrace{\underline{b \ \ldots \ b}}_{P \setminus X} \end{array}$$

дає $a \sim b$ у відношенні соціальної перваги $\succeq$.

Розглянемо тепер елемент $c \in A$, відмінний від a і b. Тоді

$$\begin{array}{cc} a \dots a & c \dots c \\ c \dots c & b \dots b \\ \underbrace{b \dots b}_{X} & \underbrace{a \dots a}_{P \backslash X} \end{array}$$

дає $c \succ a$, $c \succ b$ — це випливає з умови незалежності, оскільки $c \succ_i b$ для кожного $i \in \{1, \dots, n\}$, і $a \sim b$.

З іншого боку,

$$\begin{array}{cc} a \dots a & b \dots b \\ b \dots b & c \dots c \\ \underbrace{c \dots c}_{X} & \underbrace{a \dots a}_{P \backslash X} \end{array}$$

дає $b \succ c, a \succ c$.

Тепер у цих двох ситуаціях будемо вважати b неістоною альтрнативою. Тоді $c \succ a$ і $a \succ c$, одержали суперчність.

Доведена 1950 року теорема Ероу є один з найпарадоксальніших результатів теорії. Вона стверджує, що диктатура — єдина функція соціальної переваги, що задовольняє природні умови.

ТЕОРЕМА 0.17.4. *Якщо множина A складається з щонайменше трьох елемнтів, то єдиною функцією соціальної переваги, що задовольняє умови одностайності і незалежності, є диктатура.*

Для доведення теореми Ероу нам знадобиться низка допоміжних понять. Нехай $\Phi : \mathcal{O}(A)^n \to \mathcal{O}(A)^n$ — функція соціальної переваги на множині A і $a, b \in A$. Кажуть, що множина $Q \subseteq P$ є Φ-*вирішальною коаліцією для a проти b* (позначається $Q = \Phi \begin{pmatrix} a \\ b \end{pmatrix}$), якщо виконано умову: для кожних $(\succeq_1, \dots, \succeq_n) \in \mathcal{O}(A^n)$ з того, що $a \succ_i b$ при $p_i \in Q$ і $a \succ_i b$ при

$p_i \in P \setminus Q$ випливає $a \succ b$, де $\succeq = \Phi(\succeq_1, \ldots, \succeq_n)$. Якщо для кожних $x, y \in A$ множина $Q \subseteq P$ є Φ-вирішальною за x проти y, то множину Q назвемо Φ-*вирішальною коаліцією.* Очевидно, що P є Φ-вирішальною коаліцією, а $\emptyset$ не є Φ-вирішальною коаліцією для x проти y ні при яких $x, y \in A$ — це легко випливає з умови одностайності.

ЛЕМА 0.17.5. *Існують пара* $(a, b) \in A \times A$ *і елемент* $p_i \in P$ *такі, що* $\{p_i\} = \Phi \begin{pmatrix} a \\ b \end{pmatrix}$.

ДОВЕДЕННЯ. Розглянемо родину $\mathcal{F}$ всіх підмножин $Q \subseteq P$, для яких існує пара $(a, b) \in A \times A$ така, що $Q = \Phi \begin{pmatrix} a \\ b \end{pmatrix}$. Очевидно, що $P \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$. Розгляньмо мінімальну за включенням підмножину $R \in \mathcal{F}$. Нехай $R = \Phi \begin{pmatrix} x \\ y \end{pmatrix}$.

Доведімо, що множина R складається з одного елемента. Для цього припустімо протилежне і розб'ємо R на дві непорожні підмножини R_1, R_2. Візьмімо $z \in A \setminus \{x, y\}$. Функція Φ ставить у відповідність груповому профілеві

$$\underbrace{\begin{matrix} x \\ y \\ z \end{matrix}}_{R_1} \quad \underbrace{\begin{matrix} z \\ x \\ y \end{matrix}}_{R_2} \quad \underbrace{\begin{matrix} y \\ z \\ x \end{matrix}}_{P \setminus (R_1 \cup R_2)}$$

(тут ми ігноруємо, користуючись умовою незалежності, позначення для елемнтів, відмінних від x, y, z) відношення $\succeq$ на A, для якого $x \succ y$. Далі можливі два випадки.

1. $x \succ y$. Тоді очевидно, $R_2 = \Phi \begin{pmatrix} z \\ y \end{pmatrix}$ і ми одержуємо суперечність з мінімальністю множини R.

2. $y \succ z$. Тоді очевидно, $x \succ z$ і $R_1 = \Phi\begin{pmatrix} x \\ z \end{pmatrix}$, знову одержуємо суперечність з мінімальністю R. ☐

Лема 0.17.6. *Якщо* $p_i = \Phi\begin{pmatrix} a \\ b \end{pmatrix}$ *для деяких* $a, b \in A$, *то* $\{p_i\}$ *є* Φ*-вирішальною коаліцією.*

Доведення. Нехай $c \in A \setminus \{a, b\}$ і функція Φ ставить у відповідність груповому профілеві

$$\underbrace{\begin{matrix} a \\ b \\ c \end{matrix}}_{p_i} \qquad \underbrace{\begin{matrix} b \\ c \\ a \end{matrix}}_{P \setminus \{p_i\}}$$

(як і раніше, ми ігноруємо позначення для елемнтів, відмінних від a, b, c) відношення $\succeq$ на A. Оскільки $\{p_i\} = \Phi\begin{pmatrix} a \\ b \end{pmatrix}$, то $a \succ b$. За умовою одностайності, $b \succ c$, а отже $a \succ c$. Незалежність від неістотних альтернатив гарантує нам, що останній результат $(a \succ c)$ не залежить від розміщення b у груповому профілі. Отже, $\{p_i\} = \Phi\begin{pmatrix} a \\ c \end{pmatrix}$.

Нехай $d \in A \setminus \{a, c\}$. Розглянемо груповий профіль

$$\underbrace{\begin{matrix} d \\ a \\ c \end{matrix}}_{p_i} \qquad \underbrace{\begin{matrix} c \\ d \\ a \end{matrix}}_{P \setminus \{p_i\}}$$

Оскільки $\{p_i\} = \Phi\begin{pmatrix} a \\ c \end{pmatrix}$, то $a \succ c$. За умовою одностайності, $d \succ a$, а отже, $d \succ c$. Отже, $\{p_i\} = \Phi\begin{pmatrix} d \\ c \end{pmatrix}$ ☐

Доведення теореми 0.17.4. За лемами 0.17.2 і 0.17.3 існує виборець p_i такий, що $p_i = \Phi \begin{pmatrix} a \\ b \end{pmatrix}$ для будь-яких різних елемнтів $a, b \in A$. Ми покажемо, що p_i є диктатором. Зафіксуймо a, b і припустімо, що в деякому груповому профілі виборець p_i віддав перевагу a проти b. Нехай $c \in A \setminus \{a, b\}$. Візьмімо новий груповий профіль, в якому елемнти a, b розміщені так само, як і у початковому, але $a \succ_i c \succ_i b$, $c \succ_j a, c \succ_j b$ для всіх $j \neq i$. Оскільки $\{p_i\} = \Phi \begin{pmatrix} a \\ c \end{pmatrix}$, то $a \succ c$. За умовою одностайності, $c \succ b$, а отже, $a \succ b$. За умовою незалежності фунція Φ віддає первагу a проти b і в початковому груповому профілі. □

На перший погляд, теорема Ероу твердить, що демократичної процедури прийняття узгоджених рішень (при $|A| \geq 3$) не існує. Проте насправді теорема Ероу свi дчить про неіснування автоматичної процедури прийняття узгоджених рішень. Прийняття рішення, що відповідає інтересам усіх членів суспільства, вимагає переговорів, компромісів тощо, тобто є творчим процесом.

Більше про математичну теорію соціального вибору можна прочитати в книжці [**1**], з якої запозичено матеріал цього нарису.

Бібліоґрафія

[1] Михайло Зарічний. Елементи теорії соціального вибору, Львів, 2001.