Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет інформатики
Кафедра математики

Кваліфікаційна робота

освітній ступінь - бакалавр

на тему: **«Підстановкові коди виправлення помилок з метрикою Улама»**

Виконала: студентка 4-го року навчання
освітньої програми «Прикладна математика»,
спеціальності 113 Прикладна математика
Сичова Анастасія Сергіївна
Керівник: Олійник Б. В.,
доцент, д. н.

Рецензент _____

Кваліфікаційна робота захищена
з оцінкою: _____

Секретар ЕК _____

«_____»_____20____р.

Київ — 2022

Календарний план виконання роботи

Тема: "Підстановкові коди виправлення помилок з метрикою Улама".

	Назва етапу	Термін виконння	Підпис
1.	Ознайомлення з темою курсової.	01.10.2021	
2.	Пошук літератури.	01.11.2021	
3.	Дослідження основних властивостей метрики Улама	01.12.2021	
4.	Написання основної частини	01.04.2022	
5.	Робота над текстовим оформленням результатів.	01.05.2022	
6.	Попередній аналіз кваліфікаційної роботи.	01.06.2022	
8.	Попередній захист кваліфікаційної роботи.	15.06.2022	
9.	Виправлення помилок.	25.06.2022	
10.	Захист кваліфікаційної роботи.	05.07.2022	

Міністерство освіти і науки України

Національний університет «Києво-Могилянська академія»

Факультет інформатики кафедра математики

ЗАТВЕРДЖУЮ

Завідувач кафедри математики,

доцент, д. н., *Олійник Б.В.*

_____

(Підпис)

“____”_____ 2021

Індивідуальне завдання для кваліфікаційної роботи

студенту 4-го року навчання факультету інформатики Сичової Анастасії

Тема роботи: Підстановкові коди виправлення помилок з метрикою Улама.

Текстова частина роботи:

Індивідуальне завдання

Вступ

1 Основні теоретичні дані

1.1 Групи підстановок

1.2 Метрики на групах

1.3 Коди та коди на підстановках

1.4 Куля, сфера, діаметр

2 Властивості кодів перестановок

2.1 Властивості метрики Улама

2.3 Перфектність коду підстановок з метрикою Улама

Висновки

Використані джерела

Дата “____”_____ 2021 Науковий керівник _____

(Підпис)

Завдання отримано _____

(Підпис)

Анотація

Метою роботи є встановлення властивостей метрики Улама для перестановок та мультиперестановок, в тому числі з'ясувати можливість існування ідеального коду на цій метриці.

Актуальність теми: коди перестановок в метриці Улама нещодавно були запропоновані для використання в пристроях флеш-пам'ят. Коди мультиперестановки підходять для флеш-пам'яті, де заряди клітин можуть мати однаковий ранг. Зміни в зарядах клітин проявляються як помилки, вплив яких на отриманий сигнал можна виміряти за допомогою відстані Улама.

Об'єктами дослідження є коди перестановок та мультиперестановок в метриці Улама.

Установлені мінімальні та максимальні можливі радіуси сфер перестановок в метриці Улама. Досліджено можливість існування ідеальних кодів перестановки в метриці Улама, розглядаючи розміри сфери перестановок.

Робота складається з двох розділів.

Перший розділ присвячено опису основних метематичних конструкцій, таких як групи, метрики, коди перестановок та наведені необхідні терміни з топології. Наведено короткий огляд кодів різних видів.

В другому розділі досліджуються властивості кодів перестановок у метриці Улама, а саме екстремуми відстані Улама між перестановками. Також перевіряється можливість існування ідеального коду для різної кількості помилок.

ЗМІСТ

ВСТУП

Перестановки та мультиперестановки як формати представлення інформації мають довгу історію, причому ранні застосування в теорії комунікації сягають роботи Слепіана, який запропонував використовувати коди мультиперестановки для передачі в присутності адитивного білого гауссового шуму. Зовсім недавно Вінк запропонував використовувати коди перестановки в метриці Хеммінга для боротьби з імпульсним шумом і постійним частотним шумом в електромережах. Коди перестановки знову викликали інтерес за останні кілька років через їх перспективу застосування їх в системах зберігання даних, таких як флеш-пам'ять.

Флеш-пам'ять – це енергонезалежні блоки зберігання даних (тобто блоки зберігання, які залишаються працездатними, коли без живлення) і зазвичай використовуються для архівного або довгострокового зберігання. Інформація організована в блоки осередків, усі вони повинні оброблятися спільно під час циклів стирання інформації. Суть підходу, що лежить в основі кодування перестановок у флеш-пам'яті, який використовує той факт, що пам'ять складаються зі спеціально організованих комірок, які зберігають заряди, полягає в тому, що інформація представлена у відносному порядку рівнів заряду клітин, а не їх абсолютних рівнях заряду. Цей підхід, який називається модуляцією рангу, пом'якшує проблеми надмірної ін'єкції комірки, зменшує необхідність стирання блоків і є більш стійким до помилок, спричинених витоком заряду. Наприклад, хоча всі абсолютні значення піддаються помилкам, викликаним витоком заряду, відносний порядок кількісних даних може залишатися в основному незмінним. Припущення моделювання, що лежить в основі модуляції рангу, полягає в тому, що ймовірні лише помилки при заміні зарядів сусідніх клітинок. В результаті розробка коду для флеш-пам'яті в основному виконувалася в області метрики Кендалла , яка враховує помилки малої величини, що спричиняють заміну сусідніх елементів.

Актуальність теми: коди перестановок в метриці Улама нещодавно були запропоновані для використання в пристроях флеш-пам'ят. Коди мультиперестановки підходять для флеш-пам'яті, де заряди клітин можуть мати однаковий ранг. Зміни в зарядах клітин проявляються як помилки, вплив яких на отриманий сигнал можна виміряти за допомогою відстані Улама.

Метою роботи є встановлення властивостей метрики Улама для перестановок та мультиперестановок, в тому числі з'ясувати можливість існування ідеального коду на цій метриці.

Об'єктами дослідження є коди перестановок та мультиперестановок в метриці Улама.

Установлені мінімальні та максимальні можливі радіуси сфер перестановок в метриці Улама. Досліджено можливість існування ідеальних кодів перестановки в метриці Улама, розглядаючи розміри сфери перестановок.

Робота складається з двох розділів.

Перший розділ присвячено опису основних метематичних конструкцій, таких як групи, метрики, коди перестановок та наведені необхідні терміни з топології. Наведено короткий огляд кодів різних видів.

В другому розділі досліджуються властивості кодів перестановок у метриці Улама, а саме екстремуми відстані Улама між перестановками. Також перевіряється можливість існування ідеального коду для різної кількості помилок.

1 ОСНОВНІ ТЕОРЕТИЧНІ ДАНІ

1.1 Групи підстановок

На початку і в середині 19 століття групи перестановок були єдиними групами, які досліджували математики. Поняття групи вперше ввів Ґалуа (1831 р.), хоча в неявному вигляді комутативні групи зустрічалися вже в Лагранжа і Ґауса. Після робіт Коші про підстановки (1847 р.) дослідження груп (головним чином — груп підстановок) починають наростати. У 1870 р. виходить знаменитий трактат Жордана про групи підстановок, але тут теорія груп розглядалась лише в обсязі, необхідному для дослідження розв'язності рівнянь у радикалах. Лише приблизно в 1850 році Кейлі ввів поняття абстрактної групи, і пройшла ще чверть століття, перш ніж ідея міцно закріпилася.

1.1.1 Групи

Визначення 1.1. Бінарною дією (або просто дією) $*$ на непорожній множині M називається довільне відображення $* : MM \to M$. Результат застосування дії $*$ до пари (a, b) позначається $a * b$. Синонімом до терміну "дія" є слово "операція".

Визначення 1.2. Множина M із заданим на ній певним набором алгебричних дій $(\omega_i)_{i\in I}$ (можливо, різної арності) називається алгебраїчною структурою (алгебричною системою або універсальною алгеброю), множина M — її носієм, а набір $\omega_i | i \in I$ — її типом. Зазвичай позначається $(M; (\omega_i)_{i\in I})$.

Серед властивостей дій відмітимо такі:

– дія $*$ на множині M називається асоціативною, якщо для довільних $a, b, c \in M$ $(a * b) * c = a * (b * c)$;

– дія $*$ на множині M називається комутативною, якщо для довільних

a, $b \in M a * b = b * a$;

– дія $*$ на множині M називається скоротною зліва (справа), якщо для довільних a, b, $c \in M$ з рівності $c * a = c * b$ (відповідно $a * c = b * c$) випливає рівність a = b.

Визначення 1.3. Клас сполученості — множина елементів групи G, утворена з елементів, сполучених заданим $g \in G$, тобто всіх елементів виду hgh^{-1}, де h - довільний елемент групи G. Клас сполученості елемента $g \in G$ може позначатися $[g]\, g^G\, \mathrm{Cl}(g)$.

Елементи g_1 і g_2 групи G називаються сполученими, якщо існує елемент $h \in G$, для якого $hg_1h^{-1} = g_2$. Сполученість є відношенням еквівалентності, тому розбиває G на класи еквівалентності, це, зокрема, означає, що кожен елемент групи належить в точності одному класу сполученості, і класи $[g_1]$ і $[g_2]$ збігаються тоді і тільки тоді, коли g_1 і g_2 пов'язані, і не перетинаються інакше.

– Нейтральний елемент завжди утворює свій власний клас $[e] = \{e\}$

– Якщо G — абелева, то $\forall g\, h \in G ghg^{-1} = h$, таким чином $[g] = \{g\}$ для всіх елементів.

– Якщо два елементи g_1 і g_2 групи G належать тому самому класу спряженості, то вони мають однаковий порядок.

Алгебрична структура $(M; *)$ називається напівгрупою, якщо дія $*$ на множині M є асоціативною. Напівгрупа з нейтральним елементом називається напівгрупою з одиницею або моноїдом. Якщо дія ще й комутативна, то напівгрупа називається комутативною або абелевою.

Визначення 1.4. Моноїд, в якому кожен елемент є оборотним, називається групою. Іншими словами, група $(G; *)$ — це непорожня множина G з бінарною дією $*$, яка задовольняє такі умови (аксіоми групи) :

1) асоціативність: для довільних a, b, $c \in G (a * b) * c = a * (b * c)$;

2) існування нейтрального елемента: існує такий елемент $e \in G$, що для довільного $a \in G a * e = e * a = a$;

3) оборотність: для кожного $a \in G$ існує такий елемент $a^{-1} \in G$, що $a * a^{-1} = a^{-1} * a = e$.

Група — одне з найважливіших понять сучасної алгебри, яке має численні застосування у багатьох суміжних дисциплінах. Здебільшого група виникає як множина всіх перетворень (симетрій) деякої структури. Результатом послідовного застосування двох перетворень буде знову деяке перетворення.

Поняття абстрактної групи є узагальненням груп симетрій і визначається як множина із операцією множення (композиції), що задовольняє певним аксіомам (асоціативності, існування нейтрального та оберненого елемента). У застосуваннях математики групи часто виникають як засіб систематично описувати симетрії різного ґатунку або як групи перетворень.

1.1.2 Перестановки

Алфавіт - скінченна множина $\mathbb{A}$, $|\mathbb{A}| \geq 2$, елементи якого називаються літерами (або символами). Рядок (або слово) є послідовність букв над даним кінцевим алфавітом $\mathbb{A}$. Безліч всіх кінцевих послідовностей над алфавітом $\mathbb{A}$ позначається як $\mathbb{W}(\mathbb{A})$.

Підрядок (або ланцюжок, блок) рядка $= {}_1,\ldots, {}_n$ - будь-яка підпослідовність змінних елементів ${}_{ii+1}\ldots x_k$ з $1 \leq i \leq k \leq n$. Префіксом рядка ${}_1\ldots{}_n$ є будь-який його підрядок, що починається з ${}_1$; суфікс - будь-яка його підрядок, що закінчується на ${}_n$. Якщо рядок є частиною тексту, то розділові знаки (пробіл, точка, кома тощо) додаються до алфавіту $\mathbb{A}$.

Вектор – будь-яка скінченна послідовність із дійсних чисел, тобто, скінченний рядок над безкінечним алфавітом $\mathbb{R}$. Вектором частот (або дискретним розподілом ймовірностей) є будь-який рядок $x_1\ldots x_n$, з усіма ${}_i \geq 0$ і $\sum_{i=1}^{n} x_i = 1$. Перестановка (чи ранжування) - будь-який рядок $x_1\ldots x_n$, у якому все x_i - різні числа множини $1\ldots n$.

Перестановкою (чи ранжуванням) називається будь-яка рядок ${}_1\ldots x_n$, де ${}_i$ - різні числа множини $1\ldots n$; перестановка зі знаком - будь-який рядок

$_{1}...{}_{n}$, де $|_{i}|$ - різні числа з множини 1...n. Позначимо через (Sym_n, $\cdot$,id) групу всіх перестановок множини 1...n, де id - тотожне відображення. Звуження на безліч Sym_n, (всіх n-перестановних векторів) будь-якої метрики на $\mathbb{R}^n$ є метрикою на Sym_n; основним прикладом служить l_p-метрика $(\sum_{i=1}^{n} |x_i - y_i|^p)^{1/p}$, $p \geq 1$.

Основними операціями редагування на перестановках є:

1) Транспозиція блоку, тобто переміщення підрядка.

2) Переміщення символу, тобто транспозиція блоку, що складається із одного символу.

3) Своп символів, тобто перестановка подекуди двох сусідніх символів.

4) Обмін символів, тобто перестановка місцями будь-яких двох символів (у теорії груп це називається транспозицією).

5) Однорівневий обмін знаків, тобто обмін символів x_i і $_{j}$, $i < j$ таких, що для будь-якого k з $i < k < j$ виконується або $\min\{_{i}, {}_{j}\} > x_k$ або $x_k < \max\{_{i}, {}_{j}\}$.

6) Реверсія блоку, тобто перетворення, скажімо, перестановки $= {}_{1}...x_n$, на перестановку ${}_{1}...x_{i-kjj-1}...{}_{i+1}X_i x_{j+1}...x_n$ (так, своп – це реверсія блоку, що складається лише з двох символів).

7) Реверсія зі знаком, тобто реверсія у перестановці, зі знаком, з наступним множенням на -1 всіх символів реверсованого блоку.

Рядок (над алфавітом $\sum$) називається перестановкою, якщо всі її символи різні. (Це поняття, яке іноді називають варіацією, розширює звичайне поняття перестановки на випадки, коли $|\sum| > n$, але це дещо більш загальне налаштування є більш зручним для наших цілей і потенційно кориснішим у додатках.)

У математиці група перестановок — це група G, елементи якої є перестановками даної множини M, а групова операція — це композиція перестановок у G (які вважаються біективними функціями від множини M до неї самої). Група всіх перестановок множини M є симетричною групою M, яку часто записують як $Sym(M)$. Таким чином, термін група перестановок означає підгрупу симетричної групи. Якщо M = {1, 2, ...,n},

то $Sym(M)$ зазвичай позначається S_n і може називатися симетричною групою з n літер.

Будучи підгрупою симетричної групи, все, що необхідно для того, щоб набір перестановок задовольнив аксіомам групи і був групою перестановок, це те, щоб він містив тотожну перестановку, обернену перестановку кожної міститься в ній, і був закритий за композицією його перестановки. Загальна властивість скінченних груп означає, що скінченна непорожня підмножина симетричної групи є групою тоді і тільки тоді, коли вона закрита щодо групової операції.

1.1.3 Мультиперестановка

Будемо використовувати такі позначення та визначення. Будемо вважати, що n і r є цілими додатними числами, а r ділить n. Символ $[n]$ позначає набір цілих чисел 1, 2, . . . , n. Символ S_n означає множину перестановок (автоморфізмів) на $[n]$, тобто симетричну групу порядку $n!$. Для перестановки $\sigma \in S_n$ ми використовуємо позначення $\sigma = [\sigma(1), \sigma(2), \ldots, \sigma(n)]$, де для всіх $i \in [n]\sigma(i)$ є образом i під σ. Зловживаючи позначеннями, ми також можемо використовувати σ для посилання на послідовність $(\sigma(1), \sigma(2),..., \sigma(n)) \in [n]n$. Для двох перестановок $\sigma, \pi \in S_n$ добуток $\sigma\pi$ визначається як $(\sigma\pi)(i) = \sigma(\pi(i))$. Іншими словами, ми визначаємо множення перестановок за композицією, наприклад, [2, 1, 5, 4, 3][5, 1, 4, 2, 3] = [3, 2, 4, 1, 5]. Тотожна перестановка [1, 2, . . . , n] $\in S_n$ позначимо через e.

r-регулярна мультимножина — це мультимножина, у якій кожен її елемент з'являється рівно r разів (тобто кожен елемент повторюється r разів). Наприклад, 1, 1, 2, 2, 3, 3 — це 2-регулярна мультимножина. Мультиперестановка — це впорядкований кортеж, записи якого точно відповідають елементам мультимножини, а у випадку r-регулярної

мультимножини ми називаємо мультиперестановку r-регулярною мультиперестановкою. Наприклад, (3, 2, 2, 1, 3, 1) $\in$ [3]6 — це 2-регулярна мультиперестановка 1, 1, 2, 2, 3, 3. Оскільки r-регулярні мультиперестановки призводять до найбільшого потенційного кодового простору, у цій роботі ми розглядаємо лише r-регулярні мультиперестановки. Отже, термін «мультиперестановка» завжди буде посилатися на r-регулярну мультиперестановку.

Визначення 1.5. Вважаючи $\sigma \in S_n$, визначимо відповідну r-регулярну мультиперестановку m_σ^r таким чином: для всіх $i \in [n]$ і $j \in [n/r]$:

$$m_\sigma^r(i) := j \Leftrightarrow (j-1)r + 1 \leq \sigma(i) \leq jr \tag{1.1}$$

$m_\sigma^r := (m_\sigma^r(1), m_\sigma^r(2),...,m_\sigma^r(n) \in [n/r]^n$

Далі ми визначаємо r-регулярну відстань Улама. Для визначення спочатку необхідно визначити $\lessdot(x, y)$. Дані послідовності $x, y \in Z_n$, тоді $\lessdot(x, y)$ позначає довжину найдовшої спільної підпослідовності $Z > 0$, наприклад x і там y (не плутати з найдовшим спільним підрядком). Точніше, $\lessdot(x, y)$ є найбільшим цілим числом $k \in \mathbb{Z}_{>0}$, яке існує в послідовності $(a_1, a_2, \ldots, a_k)$, де для всіх $l \in [k]$ маємо $a_l = x(i_l) = y(j_l)$ з $1 \leq i_1 < i_2 < \ < i_k \leq n$ і $1 \leq j_1 < j_2 < \ < j_k \leq n$. Наприклад, $\lessdot$((3, 1, 2, 1, 2, 3), (1, 1, 2, 2, 3, 3)) = 4, оскільки (1, 1, 2, 3) є загальною підпослідовністю обох (3, 1, 2, 1, 2, 3) і (1, 1, 2, 2, 3, 3), а його довжина дорівнює 4. Не має значення, що існують інші однаково довгі загальні підпослідовності (наприклад, (1, 2, 2, 3)), поки не існує більше загальних підпослідовностей. Якщо $\sigma \in S_n$, то $\lessdot(\sigma, e)$ — це довжина найдовшої зростаючої підпослідовності σ, яку позначимо просто $\lessdot(\sigma)$. Аналогічно для r-регулярної мультиперестановки m_σ^r позначимо довжин найдовшої неспадної підпослідовності $\lessdot(m_\sigma^r, m_e^r)$ m_σ^r просто на $\lessdot(m_\sigma^r)$.

Визначення 1.6. Нехай m_σ^r,$m_\pi^r \in \mathcal{M}_r(\mathbb{S}_n)$, тоді:

$$d(m_\sigma^r; m_\pi^r) := mind(\sigma'; \pi') \tag{1.2}$$

де $d(\sigma', \pi') := n - \lessdot(\sigma,\pi)$.

1.2 Метрики на групах

Визначення 1.7. Метричним простором називається пара (X, d), яка складається з деякої множини елементів X і відстані $d : X \times X \to R$, а саме однозначної, невід'ємної, дійсної функції $d(x,y)$, визначеної для $\forall x, y \in X$, яка задовольняє такі 3 аксіоми:

1) $d(x, y) = 0 \Leftrightarrow x = y$ (аксіома тотожності).

2) $d(x, y) = d(y,x)$ (аксіома симетрії).

3) $d(x, z) \leqslant d(x, y) + d(y,z)$ (нерівність трикутника).

1.3 Коди та коди на підстановках

Для початку, опишемо одну ситуацію, в якій може виникнути код. Це не єдина ситуація, але вона висвітлює основні поняття теорії кодування. З цією метою згадаємо відому інженерну проблему, коли Аліса надсилає повідомлення Бобу. Аліса хоче надіслати повідомлення m з деякого набору M можливих повідомлень Бобу через шумовий канал. Під шумовим каналом ми маємо на увазі, що повідомлення, яке Аліса має намір надіслати Бобу, може бути пошкоджено (змінене), коли воно проходить через канал. Тип спотворення, яке може статися, залежить від каналу, про який йде мова. Наприклад, можливо, Аліса хоче надіслати одне з двох можливих повідомлень, 0 або 1, що відповідає «ні» і «так». Вона може надіслати 0, але через шум це сприймається Бобом як 1. Або, можливо, вона надсилає 0, але через шум жодне повідомлення не сприймається взагалі. Звичайно, тип можливого шуму не обмежується цими прикладами.

Замість того, щоб просто надсилати оригінальне повідомлення через

канал, Аліса може додати до свого повідомлення деякі допоміжні символи (і, можливо, взагалі змінити формат), щоб збільшити ймовірність того, що воно успішно досягне Боба. Процес додавання допоміжних символів називається кодуванням, а набір C (як правило, підмножина більшої множини X) закодованих повідомлень називається кодом. Члени $c \in C$ називаються кодовими словами. Аліса передає кодове слово через канал замість вихідного повідомлення, і в результаті шуму Боб отримує потенційно змінене слово $\hat{c}$ на іншому кінці каналу. Це отримане слово належить до деякої надмножини $Y \subseteq C$ можливих слів, які можна отримати. Отримане слово $\hat{c}$ потім декодується, щоб отримати оцінку $\hat{m} \in M$ вихідного повідомлення, надісланого Алісою. Якщо декодування пройшло успішно, то $m = \hat{m}$.

1.3.1 Лінійні коди

Двійковий код C довжини n — це набір двійкових векторів довжини n, елементи $c = (c_1, c_2, ..., c_n)$ яких називаються кодовими словами. Мінімальна відстань коду C дорівнює $\min\{d_H(c\,c') : c,c' \in C, c \neq c'\}$, де $d_H(c, c')$ — відстань Хеммінга, яка визначається як кількість координат, де c і c' відрізняються. Розмір (або потужність) C — це кількість кодових слів, які він містить. Код з принаймні довжиною n, розміром M і мінімальною відстанню d називається $(n\,M\,d)$ кодом. Лінійний код довжини n і рангу k — це лінійний підпростір C з розмірністю k векторного простору $\mathbb{F}_q^n$, де $\mathbb{F}_q$ — скінченне поле з q елементами. Такий код має назву «q-нарний код». Якщо $q = 2$ або $q = 3$, код описується як бінарний або тернарний відповідно. Вектори в C називаються кодовими словами. Розмір коду — це кількість кодових слів та дорівнює q^k.

Вага кодового слова — це кількість його ненульових елементів, а відстань між двома кодовими словами — це відстань Геммінга, яка є кількістю елементів, які в них відрізняються. Відстань d лінійного коду —

це мінімальна вага його ненульових кодових слів або, еквівалентно, мінімальна відстань між різними кодовими словами. Лінійний код довжини n, розмірності k та відстані d називається $[n,k,d]$ код.

Ми хочемо використовувати у $\mathbb{F}_q^n$ стандартний базис, оскільки кожна координата являє собою «біт», який передається через «канал з шумом» з деякою невеликою ймовірністю помилки передачі (двійковий симетричний канал). Якщо використовувати якийсь інший базис, тоді ця модель буде не придатна, бо відстань Геммінга не буде вимірювати кількість помилок при передачі, як нам би того хотілося.

Лінійний код у теорії кодування — код з виправленням помилок, для якого будь-яка лінійна комбінація кодових слів також є кодовим словом. Лінійні коди традиційно розділяють на блокові коди і згорткові коди, хоча турбо-коди можна розглядати як гібрид цих двох типів. Лінійні коди, в порівнянні з іншими кодами, дозволяють реалізовувати більш ефективні алгоритми кодування і декодування інформації.

Лінійні коди використовуються при попередній корекції помилок і застосовуються для передачі символів (наприклад, біт) через канал зв'язку, так що, якщо відбуваються помилки в повідомленні, деякі помилки можуть бути виправлені або виявлені при отриманні блоку. Кодові слова в лінійному блоковому коді є блоком символів, які кодуються з використанням більшої кількості символів, ніж у даних для відправки. Лінійний код довжини N передає блоки, що містять N символів. Так, наприклад, [7,4,3] код Гемінга є лінійним двійковим кодом, який представляє 4-бітові повідомлення з використанням 7-розрядних кодових слів. Два різних кодових слова розрізняються принаймні в трьох бітах. Як наслідок, до двох помилок на кодове слово може бути виявлено і одна помилка може бути виправлена. Цей код містить $2^4 = 16$ кодових слів.

Коди загалом часто позначаються літерою C, а код довжини n і рангу k (тобто код, який має n кодових слів у своїй основі та k рядків у його породжувальній матриці) зазвичай називають $(n,\ k)$ код. Лінійні коди часто позначаються $[n,\ k,\ d]$ кодами, де d означає мінімальну відстань коду

Хеммінга між будь-якими двома кодовими словами. ([n, k, d] позначення не слід плутати з (n, M, d) позначенням, яке використовується для позначення нелінійного коду довжиною n, розміром M (тобто має M кодових слів) та мінімальною відстанню Хеммінга d.)

1.3.2 Блокові коди

Нехай кодована інформація поділяється на фрагменти довжиною k біт, які перетворюються в кодові слова довжиною n біт, де $n > k$[2]. Тоді відповідний блоковий код зазвичай позначають (n, k). При цьому число $R = k/n$ називається швидкістю коду. Якщо вихідні k біт код залишає незмінними, і додає $n^{-}k$ перевірочних, такий код називається систематичним, інакше несистематичним.

Задати блоковий код можна по-різному, в тому числі таблицею, де кожній сукупності з k інформаційних біт зіставляється n біт кодового слова. Проте хороший код повинен задовольняти як мінімум таким критеріям:

– Здатність виправляти якомога більше число помилок

– Якомога менша надмірність

– Простота кодування і декодування

Неважко бачити, що наведені вимоги суперечать один одному. Саме тому існує велика кількість кодів, кожен з яких придатний для свого кола завдань. Практично всі використовувані коди є лінійними. Це пов'язано з тим, що нелінійні коди значно складніше досліджувати, і для них важко забезпечити прийнятну легкість кодування та декодування.

1.3.3 Коригувальні коди

Коригувальні коди — коди, які слугують для виявлення або виправлення помилок, що виникають при передачі інформації під впливом завад, а також при її зберіганні.

Для цього при запису (передачі) у корисні дані додають спеціальним чином структуровану надлишкову інформацію (контрольне число), а при читанні (прийомі) її використовують для того, щоб виявити або виправити помилки. Природно, що число помилок, яке можна виправити, обмежена і залежить від конкретного застосовуваного коду.

З кодами, які виправляють помилки, тісно пов'язані коди виявлення помилок. На відміну від перших, останні можуть тільки встановити факт наявності помилки в переданих даних, але не виправити її.

В дійсності, використовувані коди виявлення помилок належать до тих же класів кодів, що і коди, що виправляють помилки. Фактично будь-який код, що виправляє помилки, може бути також використаний для виявлення помилок (при цьому він буде здатний виявити більше число помилок, ніж був здатний виправити).

Всі завадостійкі коди можна розділити на два основних класи: блокові і неперервні (рекуррентні або ланцюгові).

Як блокові, так і неперервні коди в залежності від методів внесення надмірності розділяються на роздільні і нероздільні.

Більшість відомих роздільних кодів складають систематичні коди. У цих кодів перевірні символи визначаються в результаті проведення лінійних операцій над певними інформаційними символами. Для випадку двійкових кодів кожний перевірний символ вибирається таким, щоб його сума за модулем два з певними інформаційними символами стала рівною нулю. Декодування зводиться до перевірки на парність певних груп символів. У результаті таких перевірок дається інформація про наявність помилок, а в разі потреби — про позицію символів, де є помилки.

1.3.4 Коди перестановок

У 1965 р. Д. Слепіан опублікував роботу під назвою «Пермутаційна модуляція», де він побудував код, починаючи з початкової послідовності, а потім беручи всі відмінні послідовності, утворені шляхом перестановки порядку чисел у цій послідовності. Клас кодів, які він побудував, був придатний для передачі цифрової інформації за наявності білого гауссового шуму, широко використовуваної моделі шуму. Коди, введені Слепіаном, можна вважати першим екземпляром кодів перестановки. Ефективне кодування є одним з аспектів, необхідних для практичної реалізації кодів, що виправляють помилки. Бергер та інші розглянули проблему кодування для кодів перестановки, введену раніше Слепіаном. Вони продемонстрували відносну простоту кодування цих кодів перестановки.

Код перестановки — це підмножина симетричної групи $\mathbb{S}_n$, що супроводжується метрикою відстані.

Кодування перестановки буде визначено наступним чином: з урахуванням джерела S і $a_1\, a_2 \ldots a_n$ — послідовні двійкові кодові слова з S, які утворюють повідомлення M. M' буде повідомленням, яке складається з кодових слів M в порядку зростання: $M' = (a_{i_1}\, a_{i_2} \ldots a_{i_n})$, такі що $a_{i_j} \leq a_{i_{j+1}}$, $j = 1, 2, \ldots, n-1$

Процедура кодування виглядає наступним чином:

$$M \longrightarrow P = \begin{bmatrix} 1 & 2 & \cdots & n \\ \vdots & \vdots & \ddots & \vdots \\ i_1 & i_2 & \cdots & i_n \end{bmatrix}$$

Перестановочне кодування було введено Слепіаном, а його застосування, в основному модуляційне та вихідне кодування, вивчалися деякими іншими. Для оцінки критерію вірності використовувалося перестановочне кодування відносин пріоритету.

Групові коди, визначені Слепіаном, визначаються наступним чином.

Розглянемо групу $\mathbb{G}$ з $N \times N$ ортогональної матриці, яка утворює ін'єктивне представлення абстрактної групи $\mathcal{G}$ з M елементами, і «початковий вектор» $x \in R^N$, R^N евклідовий N - вимірний простір. Груповий код $\mathcal{X}$ — це орбіта x під $\mathcal{G}$, тобто множина векторів Gx. Якщо припустити, що єдиним розв'язком рівняння $Gx = x$, $G \in \mathbb{G}$, є $G = I$ (тотожна матриця), код $\mathcal{X}$ має M елементів. Ми говоримо, що $\mathcal{X} \in [M; N]$ група коду і позначаємо x_g кодовий вектор, пов'язаний з $g \in \mathcal{G}$.

Коли кодове слово x_g з $\mathcal{X}$ передається по каналу адитивного білого гауссового шуму, оптимальний (тобто з максимальною правдоподібністю) декодер, отримавши шумовий вектор $r = x_g + n$, вибирає в якості найбільш ймовірного переданого вектора той, який дає

$$\min_{h \in G} ||r - x_h||^2 \tag{1.3}$$

Якщо $\mathcal{G}$ не наділений жодною спеціальною структурою, декодування (тобто рішення попереднього рівняння) отримується шляхом вичерпного пошуку серед усіх кандидатів $g \in G$. Це вимагає ряду обчислень $v_C = NM$ (фактично, необхідно обчислити M скалярних добутків N компонентів) і зберігання $v_S = NM$ дійсних чисел (M векторів з N компонентів кожен). Визначимо кількість бітів на кожний вимір, що містить в собі сукупність як

$$r = \frac{log_2 M}{N} \tag{1.4}$$

тоді ми маємо $v_C = v_S = N2^{rN}$, що показує, що складність декодера зростає експоненціально зі збільшенням кількості вимірів і кількості бітів на вимір. Код перестановки — це груповий код, отриманий шляхом застосування до початкового вектора x групи G перестановок (тобто $\mathbb{G}$ — це група матриць перестановок). Якщо $\mathcal{X}$ є кодом перестановки, то можливий менш складний декодер, еквівалентний максимальній ймовірності.

Слепіан вивчав коди перестановки з $\mathcal{G}$ повної симетричної групи $\mathbb{S}_n$. У цьому випадку існує дуже простий декодер, який еквівалентний максимальній ймовірності. Карлоф описав декодер «алгоритму стека» для

довільних кодів перестановки, який за наявності малого шуму створює вектор максимальної правдоподібності, використовуючи менше обчислень, ніж стандартний декодер максимальної правдоподібності.

Коди мультиперестановки — це узагальнення кодів перестановки, де кожне повідомлення кодується як перестановка елементів мультинабору. Коди мультиперестановки в метриці Хеммінга, відомі як коди постійної композиції або масиви частотних перестановок, досліджувались у кількох роботах. Для енергонезалежної пам'яті мультиперестановочне кодування було запропоновано Ен Гадом та іншими, а також Ші та Цай. Ці роботи були мотивовані різними міркуваннями – перша спрямована на збільшення кількості можливих перезаписів між стираннями блоків, а друга зосереджена на перевагах мультиперестановочного кодування щодо витоку осередку, проблем надмірного введення та коливань заряду. Крім того, нещодавно повідомлялося про коди мультиперестановки для відстані Чебишева та відстані Кендалла τ.

1.3.5 Ідеальний код

Ідеальні коди — одна з найцікавіших тем теорії кодування. Ідеальний код у даній метриці — це код, у якому набір сфер із заданим радіусом R навколо його кодових слів утворює розбиття простору. Ці коди в основному розглядалися для схеми Хеммінга. Вони також враховувалися для інших схем, таких як схема Джонсона, схема Грассмана і більшою мірою в метриках Лі та Манхеттена. Ідеальні коди також розглядалися на графах Келі та для дистанційно-транзитивних графів.

Нехай $(X,\ d)$ — метричний простір (d — функція відстані) і $e > 0$. Підмножина $C \subset X$ називається ідеальним e-кодом, якщо X — неперехідне об'єднання сфер радіуса e навколо точок C. У цьому формулюванні ми маємо задачу про упаковку сфер особливого характеру.

Очевидна необхідна умова існування ідеального e-коригуючого коду

довжини слова n над алфавітом із q символів (якщо q є степенем простого числа p, ми пишемо $q = p^a$) є наступною:

$$\sum_{i=0}^{e} \binom{n}{i}(q-1)^i | q^n \tag{1.5}$$

Це умова відома як умова щільної упаковки сфер.

Мінімальна відстань d є простою мірою якості коду. Для заданої довжини та кількості кодових слів фундаментальна проблема теорії кодування полягає у створенні коду з якомога більшим d. В якості альтернативи, враховуючи n і d, визначити максимальну кількість $A_q(n,\, d)$ кодових слів у коді над $\mathbb{F}_q$ довжини n і мінімальну відстань принаймні d. Число $A_2(n,\, d)$ також позначається $A(n,\, d)$. Те саме питання можна поставити і для лінійних кодів. А саме, яка максимальна кількість $B_q(n,\, d)$ ($B(n,\, d)$ у двійковому випадку) кодових слів у лінійному коді над $\mathbb{F}_q$ довжини n і мінімальної ваги не менше d? Очевидно, $B_q(n,\, d) \leq A_q(n,\, d)$.

Той факт, що сфери радіуса t щодо кодових слів попарно не перетинаються, відразу ж випливає наступну елементарну нерівність, яку зазвичай називають межею упаковки сфери або межею Хеммінга.

Теорема 1.1. *Про межу упаковки сфери*

$$B_1(n; d) \leq A_q(n; d) \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i} \tag{1.6}$$

де $t = \lfloor \frac{(d-1)}{2} \rfloor$

Доведення. Нехай $\mathcal{C}$ — (можливо, нелінійний) код над $\mathbb{F}_q$ довжини n і мінімальної відстані d. Припустимо, що $\mathcal{C}$ містить M кодових слів. Відповідно до теореми 1.11.2 сфери радіусом t щодо різних кодових слів не перетинаються. Оскільки в будь-якій із цих сфер за (1.11) існує $\alpha = \sum_{i=0}^{t} \binom{n}{i}(q1)^i$ загальних векторів і сфери не перетинаються, $M\alpha$ не може перевищувати кількість q^n векторів у $\mathbb{F}_q^n$. Результат тепер зрозумілий. $\square$ З доведення теореми про межу упаковки сфер ми бачимо, що коли ми отримуємо рівність у зв'язку, ми фактично заповнюємо простір $\mathbb{F}_q^n$

неперетинаними сферами радіуса t. Іншими словами, кожен вектор у $\mathbb{F}_q^n$ міститься точно в одній сфері радіуса t з центром навколо кодового слова. Коли у нас є код, для якого це правда, код називається *ідеальним*.

Добре відомо, що МПК (мультиперестановковий код) $(n,\ r,\ d)$ виправляє t-помилку тоді і тільки тоді, коли $d \geq 2t+1$. Це тому, що якщо відстань між двома кодовими словами більша або дорівнює $2t+1$, то після t чи менше помилок (множення на t або менше транслокацій), мультиперестановка, отримана в результаті цього, залишається ближче до початкової мультиперестановки, ніж будь-яка інша мультиперестановка.

Визначення 1.8. Нехай $C \subseteq \mathcal{M}_r(S_n)$ — МПК $(n,\ r)$. Тоді C є ідеальним кодом для виправлення t помилок тоді і тільки тоді, коли для всіх $m_\sigma^r \in \mathcal{M}_r(\mathbb{S}_n)$ існує існує досконалий унікальний код $m_c^r \in \mathcal{M}_r(C)$, такий, що $m_\sigma^r \in S(m_c^r,\ t)$. Ми називаємо C ідеальним МПК $(n,\ r)$ виправленням t-помилки). Ідеальний код перестановки називається ідеальним кодом перестановки.

1.4 Куля, сфера, діаметр

Нехай маємо довільний метричний простір X, $x_0 \in X$. Тоді *відкритою кулею* у цьому просторі називається така множина елементів, яка задовольняє умові:

$$B(x_0; r) = \rho(x; x_0) < r; x \in X \tag{1.7}$$

де x_0- центр кулі, r - її радіус (задане дійсне число).

Під поняттям "відкритість"розуміють строгу нерівність, тобто, елементи, що потрапляють на сферу, яка обмежує кулю не враховуються.

Замкненою кулею називається множина елементів, що задовольняє умові:

$$B[x_0; r] = \rho(x; x_0) \leq r; x \in X \tag{1.8}$$

Сферою називається множина елементів, що задовольняє умові:

$$S[x_0; r] = \rho(x; x_0) = r; x \in X \tag{1.9}$$

Щільна упаковка сфер - таке розташування сфер, що не перекриваються в просторі, при якому займана внутрішніми областями цих сфер частка простору (щільність упаковки) максимальна, а також задача комбінаторної геометрії про пошук такої упаковки. Нехай існує деякий метричний простір X і маємо множину елементів $M \subset X$, таку множина називається *обмеженою*, якщо існує така куля $B(0; R)$, така, в яку можна занурити цю множину, тобто $M \subset B(0; R)$.

Під 0 в даному випадку розуміється 0-ий елемент метричного простору X. Внутрішньою точкою множини M називається будь-яка точка $x \subset M$, яка розташована в цій множині зі своїм ϵ - околом. Таким чином, можна сказати, що множина буде відкритою, якщо всі її точки будуть внутрішніми. Можна довести, що будь-яка відкрита куля у метричному просторі завжди буде відкритою множиною.

2 ВЛАСТИВОСТІ КОДІВ ПЕРЕСТАНОВОК

Хоча історія вивчення кодів перестановок сягає 1960-х і 70-х років з працями Слепіана, Бергера, Блейка та іншими, застосуванню кодів перестановок і кодів мультиперестановки для використання в енергонезалежних системах зберігання пам'яті, таких як флеш-пам'ять, почало приділятися більше уваги в літературі з теорії кодування тільки в останні роки. Однією з основних метрик відстані в математичній літературі розглядалася tau-метрика Кендалла, яка підходить для виправлення типу помилки, яка може виникнути в пристроях флеш-пам'яті.

Флеш-пам'ять - це енергонезалежна технологія, яка одночасно програмується і електрично стирається. Вона включає в себе набір комірок, які підтримуються на певному рівні заряду для кодування інформації. Хоча підвищення рівня заряду елемента є легкою операцією, зниження рівня заряду вимагає стирання всього блоку, до якого належить клітина. З цієї причини заряд вводиться в комірку протягом кількох ітерацій. Таке програмування повільне і може призвести до помилок, оскільки клітини можуть отримати додатковий небажаний заряд. Інші поширені помилки в осередках флеш-пам'яті пов'язані з витоком заряду та порушенням зчитування, які можуть спричинити переміщення заряду з однієї комірки до її сусідніх осередків.

Для подолання цих проблем було введено нову структуру кодів модуляції рангу. У цьому налаштуванні інформація передається за відносним рейтингом рівнів заряду елементів, а не за абсолютними значеннями рівнів заряду. Це дозволяє більш ефективно програмувати елементи, а кодування за рейтингом рівнів елементів є більш надійним для витоку заряду, ніж кодування за їх фактичними значеннями. У цій моделі коди є підмножинами $\mathbb{S}_n$, множини всіх перестановок на n елементах, де кожна перестановка відповідає рейтингу n рівнів клітинок.

2.1 Метрика Улама

У 2013 році Фарнуд і інші запропонували коди перестановки з використанням метрики Улама. Вони показали, що використання метрики Улама дозволить розглядати велику помилку витоку або перевищення заряду в межах однієї клітинки як одну помилку. Це означає, що метрика Улама може краще підходити для боротьби з помилками, які виникають через несправні або пошкоджені клітини. У наступних роботах було викладено використання метрики Улама у кодах мультиперестановки та обмеження розміру кодів перестановки в метриці Улама. Тим часом Бузагло виявив існування ідеального коду перестановки за циклічною τ-метрикою Кендалла і довів відсутність досконалих кодів перестановки за τ-метрикою Кендалла для певних параметрів. Проте можливість існування досконалих кодів перестановки в метриці Улама раніше не розглядалася. Вивчення цієї можливості вимагає спочатку розуміння розмірів сфер перестановки Улама, на тему яких існують лише обмежені дослідження.

Метрика Улама вимірює мінімум кількість транслокацій, необхідних для перетворення однієї перестановки в іншу, тоді як метрика Кендалла τ вимірює мінімальні суміжні транспозиції, необхідні для перетворення однієї перестановки в іншу. Помилки в пристроях флеш-пам'яті виникають, коли витікають заряди клітини або коли під час операції перезапису виникають помилки перевищення, що призводить до неточних рівнів заряду. Хоча τ-метрика Кендалла підходить для виправлення відносно невеликих помилок такого характеру, метрика Улама була б більш надійною до великих витоків заряду або помилок перевищення в клітині памґяті.

Стандартне визначення метрики Улама для перестановок використовує функцію відстані $UL(x, y)$, визначену як найменшу кількість переміщень символів, необхідних для перетворення x в y. Очевидно, що ця функція відстані обмежена випадком $n = |\sum|$ (тобто до звичайного поняття перестановок), хоча легко побачити, що воно майже еквівалентне

відстані редагування, а саме $UL(x,\ y) \leq ED(x,\ y) \leq 2UL(x,\ y)$. Таким чином, наше нестандартне визначення метрики Улама $(\mathbb{P}_n,\ ED)$ є лише незначним зловживанням термінологією для отримання додаткової загальності.

Визначення 2.1. Метрика Улама (або метрика редагування перестановок) U - метрика редагування на Sym_n, отримана для O, що включає тільки операції переміщення символів.

Еквівалентно вона є метрикою редагування, отриманою для U, що включає тільки операції вставки-видалення. При цьому $n - U(,\ ) = LCS(,\ ) = LIS(^{-1})$, де $LCS(x,\ )$ — довжина найдовшої загальної підпослідовності (не обов'язково підряд) x і y, тоді як $LIS(z)$ - довжина найдовшої зростаючої підпослідовності перестановки $z \in Sym_n$. Ця метрика вважається правоінваріантною.

Відстань редагування (вона ж відстань Левенштейна) між двома рядками — це найменша кількість вставок, видалення або замін символів, необхідних для перетворення одного рядка в інший. Відстань редагування виникає природним чином у кількох областях застосування, які часто включають великі обсяги даних, починаючи від помірної кількості надзвичайно довгих рядків (як у обчислювальній біології) до великої кількості помірно довгих рядків (як при обробці тексту та пошуку в Інтернеті). Тому ефективні алгоритми для відстані редагування, навіть зі скромними гарантіями апроксимації, є дуже бажаними.

Відстань редагування є основною мірою (не)подібності, оскільки це дуже проста модель, яка демонструє нетривіальне вирівнювання (тобто одна елементарна модифікація може спричинити зміну позиції багатьох символів у рядку). Популярні показники, такі як відстань Хеммінга, недостатньо фіксують це явище, тому для цілей аналізу даних відстань редагування часто представляє собою набагато кращу модель. Нехай $ED(x,\ y)$ позначає відстань редагування між рядками x і y. Фіксуючи алфавіт $\sum$, функція відстані редагування $ED(\cdot,\ \cdot)$ визначає метричний простір, який називається метрикою відстані редагування, набір точок якого містить усі

рядки над $\sum$. Тому кожна колекція X рядків над цим алфавітом (наприклад, $X = \{0, 1\}^n$) може бути пов'язана з субметрикою (X, ED).

Значною перешкодою в роботі з метрикою відстаней редагування є те, що їй не вистачає багатьох корисних властивостей нормованих просторів. Ми обмежуємо нашу увагу до колекцій X рядків, які мають обмежені повтори. Хоча ці колекції рядків є досить великими і створюють субметрики (X, ED) із багатою структурою, ми зможемо отримати результати, які значно кращі, ніж відомі для загального випадку $X = \sum^n$ (або навіть $\{0, 1\}^n$). Все-таки наша основна увага — це показник відстані Улама.

2.2 Властивості метрики Улама

З теоретичної точки зору, метрика Улама представляє важливий крок на шляху до розробки алгоритмів для редагування відстані над звичайними (або навіть двійковими) рядками. Алгоритми на метриці Улама вже знайшли застосування для деяких моделей згладжування і використовуються для редагування відстані над двійковими рядками.

2.2.1 Перестановки з $\max d_U$

Зрозуміло, що для найбільшої можливої відстані Улама між двома перестановками необхідна найменша можлива довжина найдовшої спільної зростаючої підпослідовності. Довжина такої підпослідовності не може бути менше 1, оскільки будь-який елемент рядку вже сам по собі утворює спільну підпослідовність довжиною 1. Тоді маємо, що найбільша можлива відстань Улама для перестановок довжиною n дорівнює $n - 1$.

Твердження 2.1. *Нехай π та σ - перестановки над $\mathbb{S}_n$. Тоді:*

$$\max d_U(\pi;\sigma) = n - L(\pi;\sigma) = n - 1 \tag{2.1}$$

Для будь-якої перестановки π над симетричною групою $\mathbb{S}_n$ існує перестановка σ, відстань Улама між якими буде максимально можливою. Це можливо в єдиному випадку - коли σ є дзеркальним відображенням π, тобто π навпаки. Іншими словами,

Твердження 2.2. *Нехай π - перестановка над $\mathbb{S}_n$. Тоді $\exists!\sigma$, така, що:*

$$d_U(\pi;\sigma) = n - L(\pi;\sigma) = n - 1 \tag{2.2}$$

Доведення. Проінексуємо елементи перестановки $\pi = \{\pi_1,\ \pi_2,\ \dots\ ,\ \pi_n\}$. Тоді перестановкою з найменшою можливою довжина найдовшої спільної зростаючої підпослідовності буде перестановка σ, що буде складатися з елементів у такому порядку: $\{\pi_n,\ \pi_{n-1},\ \dots\ ,\ \pi_1\}$. Якщо поміняти місцями хоча б один елемент в σ один з одним, наприклад, π_i з π_j, $i < j$, то елементи π_j та π_i утворять спільну з π зростаючу підпослідовність довжиною 2, таким чином відстань Улама між π та σ стане дорівнювати $n - 2$ та перестане бути максимально можливою. □

Отже, найбільший можливий діаметр сфери метрики Улама на множині перестановок дорівнює $n - 1$, і вона складається лише з однієї перестановки.

2.2.2 Перестановки з $\min d_U$

Для найменшої можливої відстані Улама між двома перестановками необхідна найбільша можлива довжина найдовшої спільної зростаючої підпослідовності. Максимально така довжина дорівнює $n - 1$ (якби вона дорівнювала n, це була б та сама перестановка).

Твердження 2.3. *Нехай π та σ - перестановки над $\mathbb{S}_n$. Тоді:*

$$\min d_U(\pi;\sigma) = n - L(\pi;\sigma) = n - (n-1) = 1 \tag{2.3}$$

Довжина найдовшої спільної зростаючої підпослідовності між перестановками π та σ досягає $n-1$ лише в тих випадках, коли σ відрізняється від π позицією тільки одного елементу.

Твердження 2.4. *Нехай π - перестановка над $\mathbb{S}_n$, Σ_π - множина всіх таких перестановок σ, що $d_U(\pi;\sigma) = 1$:*

$$|\Sigma_\pi| = n(n-1) \tag{2.4}$$

Доведення. Існує n варіантів вибору елементу, що змінить позицію, та $n-1$ спосіб розмістити його на інше місце, тому всього існує $n(n-1)$ перестановок, що будуть мати відстань Улама рівну 1 від початкової перестановки. □

2.2.3 Мультиперестановки з $\max d_U$

У випадку мультиперестановок, як і для звичайних перестановок, для найбільшої можливої відстані Улама між двома мультиперестановками необхідна найменша можлива довжина найдовшої спільної зростаючої підпослідовності. Довжина такої підпослідовності не може бути менше r, оскільки будь-який вид елементів рядку вже сам по собі утворює спільну підпослідовність довжиною r. Тоді маємо, що найбільша можлива відстань Улама для мультиперестановок довжиною n дорівнює $n-r$.

Твердження 2.5. *Нехай m_π^r та m_σ^r - мультиперестановки над $\mathbb{S}_n$. Тоді:*

$$\max d_U(m_\pi^r; m_\sigma^r) = n - L(m_\pi^r; m_\sigma^r) = n - r \tag{2.5}$$

Для будь-якої мультиперестановки m_π^r над симетричною групою $\mathbb{S}_n$

існує мультиперестановка m_σ^r, відстань Улама між якими буде максимально можливою, і, на відміну від звичайних перестановой, така мультиперестановка не є єдиною.

2.2.4 Мультиперестановки з $\min d_U$

Для найменшої можливої відстані Улама між двома мультиперестановками необхідна найбільша можлива довжина найдовшої спільної зростаючої підпослідовності. Максимально така довжина дорівнює $n-1$ (якби вона дорівнювала n, це була б та сама мультиперестановка).

Твердження 2.6. *Нехай m_π^r та m_σ^r - мультиперестановки над $\mathbb{S}_n$. Тоді:*

$$\min d_U(m_\pi^r; m_\sigma^r) = n - L(m_\pi^r; m_\sigma^r) = n - (n-1) = 1 \tag{2.6}$$

Довжина найдовшої спільної зростаючої підпослідовності між мультиперестановками m_π^r та $^r_\sigma$ досягає $n-1$ лише в тих випадках, коли m_σ^r відрізняється від m_π^r позицією тільки одного елементу.

Твердження 2.7. *Нехай m_π^r - перестановка над $\mathbb{S}_n$, $\Sigma_{m_\pi^r}$ - множина всіх таких перестановок m_σ^r, що $d_U(\pi;\sigma) = 1$:*

$$|\Sigma_\pi| = (\frac{n}{r})(n-r) \tag{2.7}$$

Доведення. Існує $\frac{n}{r}$ варіантів вибрати "вид"елементу, що змінить позицію, та $n-r$ спосіб розмістити його на інше місце, тому всього існує $(\frac{n}{r})(n-r)$ мультиперестановок, що будуть мати відстань Улама рівну 1 від початкової мультиперестановки. □

Можемо зробити висновок, що найменший можливий діаметр сфери метрики Улама на множині мультиперестановок дорівнює 1, і до неї входить $(\frac{n}{r})(n-r)$ мультиперестановки.

2.3 Перфектність коду підстановок з метрикою Улама

У випадку кодів перестановки ідеальні коди та розміри сфери пов'язані наступним чином: ідеальний код перестановки $C \subseteq \mathbb{S}_n$, що виправляє помилку t, якщо він існує, матиме потужність $|C| = n!/|S(c, t)|$, де $c \in C$. Отже, одне з перших питань, яке можна розглянути при дослідженні можливості ідеального коду — це доцільність коду такого розміру. Для будь-якого $\sigma \in \mathbb{S}_n$ маємо $|S(\sigma, t)| = |S(e, t)|$. Отже, розрахунок перестановкових розмірів сфери Улама можна звести до випадку, коли тотожність є центром.

У 2013 році Фарнуд довів існування верхньї межі розміру коду перестановки Улама $C \in \mathbb{S}_n$ з мінімальною відстанню Улама d.

Лема 2.1. *Розмірність коду перестановок $C \in \mathbb{S}_n$ з мінімальною відстанню Улама d має наступну верхню межу:*

$$|C| \leq (n - d + 1)! \tag{2.8}$$

Отже, одна зі стратегій для доведення відсутності досконалих кодів перестановки полягає в тому, щоб показати, що розмір ідеального коду обов'язково повинен бути більшим за верхню межу, наведену вище. Треба зауважити, що для того, щоб рівняння мало сенс, d має бути менше або дорівнювати $n - 1$.

Наведемо ще декілька необхідних формул, виведених та доведених Фарну, які будуть використовуватися надалі.

Лема 2.2.

$$|S(e; 1)| = 1 + (n - 1)^2 \tag{2.9}$$

Лема 2.3. *Нехай $n > 3$ та $\sigma \in \mathbb{S}_n$. Тоді:*

$$|S(\sigma; 2)| = 1 + (n - 1)^2 + (\frac{n(n - 3)}{2})^2 + (\frac{(n - 1)(n - 2)}{2})^2 \tag{2.10}$$

Лема 2.4. *Нехай $n > 5$ та $\sigma \in \mathbb{S}_n$. Тоді:*

$$|S(\sigma;2)| = 1 + (n-1)^2 + (\frac{n(n-3)}{2})^2 + (\frac{(n-1)(n-2)}{2})^2 + \\ +(\frac{n(n-1)(n-5)}{6})^2 + (\frac{n(n-2)(n-4)}{3})^2 + (\frac{(n-1)(n-2)(n-3)}{6})^2 \quad (2.11)$$

2.3.1 Ідеальний код, що виправляє одну помилку

Коли $t = 1$, проаналізуємо неіснування ідеального коду з виправленням однієї помилки в $\mathbb{S}_n$ в наступному твердженні.

Твердження 2.8. *Не існує (нетривіальних) ідеальних кодів перестановки, що виправляють одну помилку в метриці Улама.*

Доведення. Припустимо, що $C \subseteq \mathbb{S}_n$ є ідеальним кодом перестановки, що виправляє одну помилку. Нагадаємо, що C є тривіальним кодом, якщо $C = S_n$ або $|C| = 1$. Якщо $n \leq 2$, то для всіх σ, $\pi \in \mathbb{S}_n$ маємо $\pi \in S(\sigma, 1)$, з чого випливає, що C є тривіальним кодом. Таким чином ми можемо припустимо, що $n > 2$. Ми йдемо від протиріччя. Оскільки C є ідеальним кодом перестановки з виправленням однієї помилки, C є МПК(n, 1, d) з $3 \leq d \leq n1$ і $|C| = n!/|S(\sigma, 1)| = n!/(1 + (n1)^2)$. Однак з нерівності (3) випливає, що розмір коду $|C| \leq (n2)!$. Отже, достатньо показати, що $|C| = n!/(1 + (n1)^2) > (n2)!$, що вірно тоді і тільки тоді, коли $n > 2$. □

2.3.2 Ідеальний код, що виправляє 2 помилки

Твердження 2.9. *Не існує жодних (нетривіальних) ідеальних кодів перестановки, що виправляють 2 помилки.*

Доведення. Припустимо, що C є ідеальним кодом перестановки, що виправляє 2 помилки. Якщо $n \leq 3$, то C є тривіальним кодом, що складається

з одного елемента, тому ми можемо вважати, що $n > 3$. Знову ми доводимо за протиріччя: оскільки $C \subseteq \mathbb{S}_n$ є ідеальним кодом з 2 помилками, то C є кодом $(n,\, d)$ з $5 \leq d \leq n-1$ і означає:

$$\|C| = \frac{n!}{|S(\sigma; 2)|} = \frac{n!}{1 + (n-1)^2 + (\frac{(n)(n-3)}{2})^2 + (\frac{(n-1)(n-2)}{2})^2} \tag{2.12}$$

За нерівністю $|C| \leq (n-4)!$, достатньо довести що:

$$\frac{n!}{1 + (n-1)^2 + (\frac{n(n-3)}{2})^2 + (\frac{(n-1)(n-2)}{2})^2} - (n-4)! > 0 \tag{2.13}$$

що очевидно, для всіх $n > 3$. □

2.3.3 Ідеальний код, що виправляє 3 помилки

Твердження 2.10. *Не існує жодних (нетривіальних) ідеальних кодів перестановки, що виправляють 3 помилки.*

Доведення. Припустимо, що $C \in \mathbb{S}_n$ є ідеальним кодом для виправлення 3 помилок. Подібно до доведення двох попередніх тверджень, якщо $n \leq 7$, то C є тривіальним кодом, тому ми можемо вважати, що $n > 7$. Решта доказу слідує тим же міркуванням, що й доведення леми про існування ідеального коду, що виправляє 2 помилки - використовуючи сферу розміру, розраховану Фарнуд.

Для малих значень t явні обчислення сфери добре працюють, щоб показати неіснування нетривіальних ідеальних кодів для виправлення t помилок. Однак для кожного радіуса t розмір кулі $S(e,\, t)$ дорівнює $|S(e,\, t1)| + |\pi \in \mathbb{S}_n : \lessdot(\pi) = nt|$. Це означає, що кожне обчислення розміру кулі радіуса t вимагає обчислення розмірів кулі для радіусів від 0 до $t1$. Тому такі явні обчислення непрактичні для великих значень t. Для значень $t > 3$ можна використовувати інший метод, щоб показати, що нетривіальних досконалих кодів не існує. Наступна лема забезпечує достатню умову, щоб

зробити висновок, що досконалих кодів не існує. У доведенні леми позначенням nt позначають звичайну комбінаторну функцію вибору. □

2.3.4 Ідеальний код, що виправляє t помилок

Нехай для t є невід'ємне ціле число таке, що $n \geq 2t$. Якщо наступна нерівність виконується, то в S_n не існує нетривіальних ідеальних кодів перестановки, що виправляють t-помилку:

$$F(n;t) := \frac{((n-t)!)^2 t!}{n!(n-2t)!} > 1 \tag{2.14}$$

Доведення. Припустимо, що t — ціле невід'ємне число, таке, що $n \geq 2t$. Проходимо контрапозитивно. Припустимо, що $C \subset \mathbb{S}_n$ є нетривіальним досконалим кодом перестановки за нерівністю $|C| \leq (n2t)!$. У той же час для будь-якого $\sigma \in \mathbb{S}_n$ ми отримуємо $|S(\sigma,\, t)| = |S(e,\, t)|$, що є менше або дорівнює $\binom{n}{n-t}(n!)/(n-t)!$ оскільки будь-яка перестановка $\pi \in S(e,\, t)$, може бути знайдена через вибір $n-r$ елементів з e зі збільшенням порядку, а потім впорядкуванню решти елементів t в π. Звичайно таким чином в результаті це призводить до подвійного підрахунку деяких перестановок у $S(e,\, t)$, звідси виникає нерівність.

$$|S(\sigma;t)| \leq \binom{n}{n-t}\frac{n!}{(n-t)!}) \tag{2.15}$$

означає, що

$$\frac{(n-t)!}{\binom{n}{t}} \leq \frac{n!}{|S(\sigma;t)|} = |C| \leq (n-2t)! \tag{2.16}$$

Більше того, $(n-t)!/\binom{n}{t} \leq (n-2t)!$ тоді і тільки тоді, коли $F(n,t) \leq 1$. □

Отож, бачимо, що існування ідеального коду перестановок у метриці Улама неможливе, оскільки розмір коду в жодному випадку не перевищує верхню межу, наведену в лемі 2.1, що є необхідною умовою існування ідеального коду.

ВИСНОВКИ

У даній кваліфікаційній роботі було зібрано та описано основні теоретичні відомості про групи перестановок та мультиперестановок, базові властивості метрики Улама та метричних просторів узагалі, дано характеризацію деяких типів кодів, розглянуто конструкції кодів перестановок і мультиперестановок на симетричних групах і проілюстровано на прикладах.

Новизною роботи є встановлення мінімальної та максимальної діаметру сфер на перестановках та мультиперестановках у метриці Улама, а також число перестановок, обмежених цими сферами. За допомогою формул, виведених та доведених Фарнудом, з'ясовано та ще раз підтверджено неможливість існування ідеальних кодів перестановок у метриці Улама.

ПЕРЕЛІК ПОСИЛАНЬ

1. A. Barg and A. Mazumdar, “Codes in permutations and error correction for rank modulation,” IEEE Trans. Inf. Theory, vol. 56, pp. 3158-3165, July 2010.

2. T. Berger, F. Jelinek, and J. Wolf, “Permutation codes for sources,” IEEE Trans. Inf. Theory, vol. I8, pp. 160-169, Jan. 1972.

3. I.F. Blake, G. Cohen, and M. Deza, “Coding with permutations,” Inform. Control vol. 43, pp. 1-19, Oct. 1979.

4. S. Buzaglo and T. Etzion, “Perfect permutation codes with the Kendall’s -metric,” in Proc. IEEE Int. Symp. Information Theory, pp. 2391-2395, July 2014.

5. E. En Gad, E. Yaakobi, A. Jiang, and J. Bruck, “Rank-modulation rewrite coding for flash memories,” IEEE Trans. Inf. Theory, vol 61, pp.4209-4226, Aug. 2015.

6. F. Farnoud, V. Skachek, and O. Milenkovic, “Error-correction in flash memories via codes in the Ulam metric,” IEEE Trans. Inf. Theory, vol. 59, no. 5,pp. 3003-3020, May 2013.

7. D. Slepian, “Permutation modulation,” Proc. IEEE, vol. 53, pp. 228-236, 1965.

8. J. H. VAN LINT, "A SURVEY OF PERFECT CODES ROCKY MOUNTAIN JOURNAL OF MATHEMATICS, Volume 5, Number 2, Spring 1975