НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Есе на тему

ЛАТИНСЬКІ КВАДРАТИ. ЗАВЕРШЕННЯ ЧАСТКОВИХ ЛАТИНСЬКИХ КВАДРАТІВ.

Виконав студент
групи ФІ-91
Житкевич Іван Олександрович

Київ — 2020

ЗМІСТ

1 ОГЛЯД ТА ЗАТЯГНУТИЙ ВСТУП

1.1 Історія

Ідея латинських квадратів породжується якнайменше 300 років тому у монограмі *Koo-Soo-Ryak*, яку написав Choi Seok-Jeong (1646-1715). Він використовував ортогональні латинські квадрати 9 порядку для побудови магічних квадратів. У своїх нотатках він зауважив, що не міг знайти ортогональні латинські квадрати 10 порядку.

Але це не перша поява латинських квадратів. Існують амулети латинських квадратів середньовічного Ісламу, магічний квадрат аль-Буні. Вони доказують, що люди того часу знали мінімум 2 ортогональні латинські квадрати розміру 4×4.

Тобто все ж невідоме точне походження латинських квадратів.

У 1776 році Ойлер презентував роботу *De Quadratis Magicis* Академії Наук в Петербурзі. Там він показав побудову магічних квадратів порядку 3, 4, 5 з ортогональних квадратів. Також він продемонстрував проблему щодо магічного квадрату порядку 6, яка відома як *Euler's 36 Officers Problem*. Надалі Ейлер припускав, що не існує таких рішень для порядку 6, та навіть пішов далі — не існує ортогональних латинських квадратів порядку $n \equiv 2 (\mathrm{mod}\, 4)$.

Але його останнє припущення було спростовано 1958 року Раджом Бозе та Шарадчандром Шрікханде, які побудували два ортогональні латинські квадрати 22 порядку. Далі у 1960 році вони дізналися, що два ортогональні латинські квадрати порядку n існують для всіх $n \equiv 2 (\mathrm{mod}\, 4)$, окрім 2 та 6.

1.2 Латинські квадрати та часткові латинські квадрати

Означення 1.1. Латинський квадрат порядку n це матриця L розміру $n \times n$ з елементами із множини $\{1, \ldots, n\}$, де кожен елемент зустрічається у кожному рядку та колонці лише один раз.

$$L_{4,0} = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \\ 2 & 3 & 0 & 1 \\ 1 & 2 & 3 & 0 \end{bmatrix} \quad L_{3,0} = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 1 \\ 2 & 1 & 0 \end{bmatrix}$$

Одне з найбільших досліджень латинських квадратів стосується часткових латинських квадратів.

Означення 1.2. Частковий латинський квадрат порядку n це матриця P розміру $n \times n$, де кожне місце або пусте, або містить елемент із множини $\{1, \ldots, n\}$ з умовою, що кожний елемент зустрічається у кожному рядку (колонці) лише один раз.

Одне з важливих досліджень латинських квадратів розпочав Маршалл Голл та Герберт Джон Райзер. Воно стосується характеризації часткових латинських квадратів. Вже останні можуть бути доповнені до латинських квадратів без додавання рядків, колонок чи елементів.

Маршалл Голл

Герберт Райзер

2 СКЛАДНІСТЬ

Доповнення часткових латинських квадратів до латинських квадратів є *NP-complete*. У данному розділі наводиться доказ цього твердження у два кроки (за Колборном [1]).

2.1 Розбиття тричасткових графів на трикутники

Приведемо зв'язок між доповненням та проблемою з теорії графів, розбиттям тридольних графів на трикутники та покажемо, що ця проблема є *NP-complete*.

Означення 2.1. Граф $G = (V, E)$ є тричастковим графом, якщо його множина вершин V може бути розбита на три множини V_1, V_2, V_3, які індукують незалежну множину на цьому графі. Також можна сказати, що такий граф може бути розфарбований трьома кольорами так, що не існує двох сусідніх вершин (поєднаних ребром) з однаковим кольором.

Означення 2.2. Розбиття на трикутники графа $G = (V, E)$ це розбиття множини E на множини, що будуть мати три ребра, які формують трикутник (або утворюють граф K_3) в графі G.

Означення 2.3. Граф $G = (V, E)$ є одноманітним якщо він є тричастковим графом з розбиттям $V = V_1 \sqcup V_2 \sqcup V_3$ та умовою на кожну вершину: кожна вершина з $V_i, i = \overline{1,3}$ має однакову кількість сусідніх з двох інших множин $V_j, j = \overline{1,3}, j \neq i$ розбиття множини V.

Тричастковий граф з розбиттям на трикутники повинен бути одноманітним.

Зв'язок між доповненням часткового латинського квадрата та розбиттям на трикутники тричасткового графа є досить близьким. Ми можемо побудувати граф $G(P)$ використовуючи частковий латинський

квадрат P. Граф $G(P)$ будемо позначати як G_P та такий граф матиме наступну побудову:

1) $G_P = (V, E)$

2) $V = V_r \cup V_c \cup V_e$

$V_r = \{r_i \mid i$ рядок містить пустий квадрат $\}$

$V_c = \{c_j \mid j$ колонка містить пустий квадрат $\}$

$V_e = \{e_k \mid k$ елемент з'являєтсья у менш ніж n квадратах $\}$

3) Маємо наступні правила включення ребра до множини E:

а) якщо (i, j) клітинка є пустою, то включаємо ребро (r_i, c_j)

б) якщо рядок i не містить елемента k, то включаємо ребро (r_i, e_k)

в) якщо стовпець j не містить елемента k, то включаємо ребро (c_j, e_k)

Граф G_P має розбиття на трикутники тоді та тільки тоді якщо P може бути доповнений.

Теорема 2.1. *Задача вирішення чи має даний тричастковий граф розбиття на трикутники є NP-complete.*

Дану теорему можна доказати привівши певні модифікації у доведення Холіера, що задача трикутного завершення графів є NP повною. Ці модифікації наведені у роботі Колборна [1].

2.2 Доповнення часткового латинського квадрата NP-complete

Використовуємо позначення минулого розділу.

Означення 2.4. Латинський каркас $LF(G; r, s, t)$ деякого тричасткового графу G це матриця розміру $r \times s$. Кожна клітинка є або пустою, або елементом із множини $\{1, \ldots, t\}$. Кожний рядок (колонка) містить елемент щонайбільше один раз. Також є певні правила для заповнення даної матриці:

1) Якщо G має ребро (r_i, c_j), то клітинка (i, j) є пустою, інакше містить елемент з множини $\{1\ldots., t\}$.

2) Якщо G має ребро (r_i, e_k), то рядок i не містить елемента k.

3) Якщо G має ребро (c_j, e_k), то колонка j не містить елемента k.

Потрібно зауважити, що якщо $r = s = t$, то наш каркас є частковим латинським квадратом, який може бути доповнений тоді та тільки тоді якщо G має розбиття на трикутники.

Лема 2.1. *Для одноматітного тричасткового графа G з n вершинами існує латинський каркас $LF(G; n, n, 2n)$.*

Доведення. Маємо матрицю L розміру $n \times n$. Якщо (r_i, c_j) є ребром G, то потрібно залишити (i, j) клітинку пустою. Інакше заповнити значенням $1 + n + ((i + j)mod n)$. Маємо L як $LF(G; n, n, 2n))$. □

Наведемо наступні леми без доведення (можна знайти у [1]):

Лема 2.2. *Нехай L це $LF(G; r, s, t)$ одноманітного тричасткового графа G. Позначимо $R(k)$ як разів появи елемента k у L плюс половина степені вершини e_k графа G. Далі будь-коли $R(k) \geqslant r + s - t$ для будь-яких $1 \leqslant k \leqslant t$, L може бути розширений до $LF(G; r, s + 1, t)$ L' у якому $R'(k) \geqslant r + (s + 1) - t$ для будь-яких $1 \leqslant k \leqslant t$.*

Ми використаймо цю лему 2.2 для додавання колонок. Щоб додати рядки можна транспонувати матрицю та скористатися цією лемою. Насправді Маршалл Голл показав, що латинський прямокутник $r \times s$ завжди може бути доповнений до латинського квадрата.

Лема 2.3. *Латинський каркас $LF(G; r, s, s)$ для однорідного тричасткового графа G може бути доповнений до латинького каркаса $LF(G; s, s, s)$.*

Ці три наведені вище леми ведуть до:

Теорема 2.2. *При однорідному тричастковому графі G з n вершинами латинський каркас $LF(G; 2n, 2n, 2n)$ може бути отриманий за поліноміальний час.*

Доведення. Спочатку ми створюємо $LF(G; n, n, 2n)$ за допомогою леми 2.1. Використаймо послідовно лему 2.3 для утворення $LF(G; n, 2n, 2n)$. Далі транспонуємо цю матрицю та використаємо послідовно лему це раз отримуючи $LF(G; 2n, 2n, 2n)$. Даний процес займає поліноміальний час. □

Отже ця теорема дає змогу привести задачу триангуляції (розбиття на трикутники) до доповнення латинських квадратів.

І, нарешті!!!

Теорема 2.3. *Задача рішення чи може латинський квадрат бути доповнений є $\mathcal{NP}$-complete.*

Доведення. По перше, членство у класі NP є безпосереднім (it is immediate). По друге, потрібно показати повноту. Для цього зведемо триангуляцію тричасткових графів та теорему 2.1, за якою ця задача є NP-complete. Маючи тричастковий граф із n вершинами ми повинні встановити його однорідність. Якщо він не є однорідним, то і не є існує розбиття на трикутники. Якщо ж є однорідним, то використаймо теорему 2.2 для створення латинського каркаса $LF(G; 2n, 2n, 2n)$ за поліноміальний час. Цей латинський каркас і є також частковим латинським квадратом. Далі потрібно показати, що цей частковий латинський квадрат може бути доповнений лише у тому випадку, якщо G має розбиття на трикутники. А це вже слідує з того, що за побудовою граф G сконструйований з часткового латинського квадрату. □

3 ЗАСТОСУВАННЯ У КРИПТОГРАФІЇ

3.1 Побудова латинських квадратів

Існує достатньо алгоритмів побудови такої структури. Їх можна знайти у книгах:

– K. Yamamoto. Generation principles of latin squares.

– M. J. Strube. A basic program for the generation of latin squares.

– B. G. Kim and H. H. Stein. A spreadsheet program for making a balaned latin square design.

– R. Fontana. Random latin squares and sudoku design generatinon.

– I. Gallego Sagastume. Generation of random latin squares step by step and graphically.

3.2 Cryptographically Hash Functions

Латинські квадрати кодують особливості алгебраїчних структур. Якщо певна алгебраїчна структура проходить певні тести латинського квадрата, то вона є кандидатом на використання у побудові певної криптографічної системи.

Так, наприклад, Schmidt [3] використовує супер-симетричні латинські квадрати для адитивної групи скінчених полів для побудови спрощенної версії хеш функції Grøstl.

ВИСНОВКИ

У даній роботи ми розглянули питання складності доповнення часткових латинських квадратів, також згадали про застосування такої структури у криптографії. Побудований латинський квадрат може бути використаний у створенні криптографічної системи.

Загалом, тема латинських квадратів є вузькою. Алгебраїчно, латинський квадрат це таблиця множень квазігрупи. Дослідження цього привели до застосувань у алгебрі, комбінаториці, теорії графів та інших розділів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Coulbourn, *The Complexity of Completing Partial Latin Squares*, 22 April 1982, Department of Computational Science, University of Saskatchewan, Saskatoon. Saskatchewan, S7N 0 WO, Canada.

2. Padraic Bartlett, *3SAT and Latin Squares*, Department of Mathematics, University of California, Santa Barbara, 2014, <http: //web.math.ucsb.edu/~padraic/mathcamp_2014/np_and_ls/mc2014_np_and_ls_lecture4.pdf>.

3. Nathan O. Schmidt, *Latin Squares and their Applications to Cryptography*, December 2016.