УДК 519.14

Кочубінська Є. А., Челнокова Г. О.

DOI: https://doi.org/10.18523/2617-70802201924-32

НЕПЕРЕРВНІ ЧАСТКОВІ ВІДОБРАЖЕННЯ НА БЛОК-СХЕМАХ

У роботі розглядаються неповні збалансовані блок-схеми – системи k-елементних підмножин (блоків) деякої скінченної множини елементів, таких, що кожний елемент міститься в r блоках та кожна пара елементів міститься в λ блоках. Блок-схеми були введені для планування статистичних досліджень та згодом отримали багато інших використань. На блок-схемі можна визначити часткові неперервні відображення, тобто такі часткові відображення, при яких прообразом кожного блоку є блок або пуста множина. Наведено основні відомі властивості часткових неперервних відображень на блок-схемах.

Однією з важливих властивостей, що, зокрема, дає необхідну умову існування неперервних часткових відображень на даній блок-схемі, є лема однорідності: для непустого неперервного часткового відображення на блок-схемі кількість елементів у (непустому) прообразі кожного елемента фіксована і дорівнює числу d, що ділить розмір блоків k. Дуальна гіпотеза однорідності припускає, що кожен блок, що є прообразом якогось іншого блоку, має бути прообразом фіксованого числа блоків. Виконання цієї гіпотези дозволило б отримати не менш важливу властивість блок-схем і неперервних відображень на них та отримати новий спосіб побудови блок-схем, як образів блок-схем при неперервних відображеннях. Основним новим результатом роботи є контрприклад до дуальної гіпотези однорідності, який був побудований як складена блок-схема – блок-схема, множина блоків якої розбивається на групи блоків, кожна з яких утворює блок-схему на тій самій множині елементів. В останньому розділі отримано дві необхідні умови складеності блок-схеми.

Також у роботі наводиться спосіб зведення задачі пошуку блок-схеми з заданими параметрами до задачі булевої або псевдобулевої виконуваності. Наведено явний алгоритм побудови систем булевих або псевдобулевих виразів еквівалентних задачі пошуку блок-схеми та продемонстровано результати застосування до відповідних задач існуючих програм для їх розв'язку.

Ключові слова: блок-схеми, частково неперервні відображення.

Вступ

У багатьох прикладних задачах зустрічаються системи інцидентності — пари із множини елементів та множини підмножин множини елементів. Часто при побудові такої системи бажано, щоб окремі підмножини елементів не мали переваги над іншими. Важливим прикладом такої задачі є планування статистичних досліджень, де елементами є випробовувані зразки, а множинами — окремі експерименти, в яких порівнюється певна кількість зразків. Очевидно, що така рівноправність для всіх підмножин може бути досягнена, лише якщо для кожного n, для якого в системі є підмножина розміру n, система містить всі можливі підмножини розміру n, але часто це не є практично досяжним. Постановка більш слабких, проте чітко визначених умов, призводить до поняття збалансованої неповної блок-схеми. Як виявилось, блок-схеми є не лише практично корисним об'єктом, але й мають цікаві властивості як комбінаторні системи, що є тісно пов'язаними з теорією чисел [2], теорією груп та напівгруп [1; 7], дискретними геометріями [8] і т. д. Незважаючи на значний обсяг досліджень, присвячених блок-схемам, ряд основних проблем лишається невирішеним, зокрема невідомо, чи можна побудувати точні необхідні і достатні умови існування блок-схеми з заданими параметрами. Так, наприклад, незважаючи на наявність значної кількості наборів параметрів, для яких побудовано блок-схеми або доведено їх неіснування [2; 5; 6], та деякої кількості більш загальних результатів [2; 9] на даний момент лишається невідомим, чи існують блок-схеми з параметрами (46, 69, 9, 6, 1), (51, 85, 10, 6, 1) [4].

Ця робота зосереджена на дослідженні властивостей неперервних часткових відображень на блок-схемах, запропонованих в [1]. У розділі 1 розглядається поняття неперервного часткового відображення на системі інцидентності та наводяться деякі їх загальні властивості, основна з яких — ізоморфність простору неперервних часткових відображень на системі інцидентності і трансляційної оболонки напівгру-

© *Кочубінська Є. А., Челнокова Г. О.*, 2019

пи, породженої цією системою. Також вводиться формальне означення поняття блок-схеми та наводяться властивості неперервних часткових відображень заданих на блок-схемах. У розділі 2 наведено зведення задачі побудови блок-схеми з заданими параметрами до задачі булевої (псевдобулевої) здійсненності. Розділ 3 містить опис побудови контрприкладу до гіпотези, зробленої авторами роботи [1]. У розділі 4 наведено дослідження властивостей складених блок-схем — блок схем, множину блоків яких можна розбити на підмножини, кожна з яких у свою чергу задає блок-схему.

Часткові відображення на системах інцидентності та блок-схемах

Однією з проблем комбінаторного аналізу є розташування об'єктів у певну визначену кількість множин так, щоб i-й об'єкт зустічався r_i разів серед усіх множин, j-та множина містила k_j об'єктів та щоб двійки, трійки та схожі групи об'єктів зустрічались визначену кількість разів. Математичні структури, що відповідають цій задачі, називають системами інцидентності (incidence system) або тактичними конфігураціями (tactical configuration).

Визначимо система інцидентності як пару $D=(V,B)$, де V — скінченна множина точок, а B — множина підмножин V, які називатимемо блоками.

Автори роботи [1] вводять поняття неперервних відображень на схемах інцидентності.

Означення 1. Нехай $D=(V,B)$ та $D'=$ $=(V',B')$ системи інцидентності. Часткове відображення $f : V \to V'$ називається неперервним, якщо $f^{-1}(b') \in B \cup \{\emptyset\}$ для всіх $b' \in B'$.

Далі в цьому розділі перелічено основні результати, отримані в [1] для неперервних відображень на схемах інцидентності та блок-схемах.

Позначимо $\Omega(D) := \{f : V \to V | f$ неперервне $\}$.

Кожне відображення $f \in \Omega(D)$ породжує відображення $\overline{f} : B \to B$, що діє справа на B і визначається системою

$$b\overline{f} = \begin{cases} f^{-1}(b), & \text{якщо } f^{-1}(b) \neq \emptyset; \\ \text{невизначена}, & \text{інакше.} \end{cases}$$

Означення 2. Нехай $D=(V,B)$ система інцидентності.
Матрицею інцидентності системи D називається матриця $|V| \times |B|$ A така, що $a_{ij} =$ $= A(v_i, b_j) = \begin{cases} 1, & \text{якщо } v_i \in b_j; \\ 0, & \text{інакше.} \end{cases}$

Надалі в роботі розглядатиметься тільки клас систем інцидентності, який називають збалансованими неповними блок-схемами.

Означення 3. Система інцидентності називається збалансованою неповною блок-схемою (balanced incomplete block design – BIBD) з параметрами (v,b,r,k,λ), якщо:

1) $|V| = v, |B| = b$;

2) кожна точка з V входить рівно в r блоків з B;

3) кожний блок містить рівно k точок з V;

4) кожна пара різних точок з V входить рівно в λ блоків B.

У термінах матриці інцидентності A системи D можна записати умови еквівалентні умовам 2) — 4):

2') $AJ_{|B|\times 1} = rJ_{|B|\times 1}$;

3') $J_{1\times|V|} = kJ_{1\times|B|}$;

4') $AA^t = (r-\lambda)I_{|V|} + \lambda J_{|V|\times|V|}$,

де $J_{m\times n}$ – $m \times n$ матриця, всі елементи якої рівні 1, та I_m – $m \times m$ одинична матриця.

Можна показати, що $\det(AA^T) = (r - \lambda)^{v-1}((v-1)\lambda + r)$, тому (крім вироджених випадків, зазначених в рівності) матриця AA^T оборотна. Оскільки $\operatorname{rank}(A) = v$ то $v < b$ (нерівність Фішера). Наведемо узагальнення цієї нерівності для неперервних відображень.

Лема 1. *Нехай $D=(V,B)$ блок-схема, якщо $f \in \Omega(D)$, то $\operatorname{rank}(f) \leq \operatorname{rank}(\overline{f})$.*

Також можна показати, що параметри блок-схеми D задовольняють рівності $bk = vr$ та $r(k-1) = \lambda(v-1)$. Тобто, будь-які три параметри визначають два інші, тому задаватимемо лише параметри (v,k,λ), описуючи блок-схему.

Лема 2. *Нехай $D=(V,B)$ — (v,k,λ) блок-схема. Якщо $f : V \to V \in \Omega(D)$ непусте ін'єктивне часткове відображення, то $\operatorname{dom}(f) = V$.*

Наслідок 3. *Нехай D — блок-схема. Тоді $f \neq$ $\neq 0 \in \Omega(D)$ ін'єктивне тоді і тільки тоді, коли f автоморфізм на D.*

Лема 4. *(Лема однорідності) Нехай $D =$ $= (V,B)$ — (v,b,r,k,λ) блок-схема. Якщо $f \in$ $\in \Omega(D)$ непусте відображення, тоді існує натуральне число d, що ділить k, таке, що $|f^{-1}(v)| = d$ для всіх $v \in f(V)$. Більш того, $r(k-d) = \lambda(m-d)$, де $m = |\operatorname{dom}(f)|$.*

Називатимемо d степенем неперервного відображення f і позначатимемо $d = deg(f)$.

Наслідок 5. *Нехай $D = (V,B)$ — блок-схема. Тоді $f \in \Omega(D)$ має $\operatorname{dom}(f) = V$ тоді і тільки тоді, коли f автоморфізм на D.*

Наслідок 6. *Нехай $f \in \Omega(D)$ автоморфізм на D. Тоді $\operatorname{rank}(f) < \frac{v}{2}$.*

Означення 4. n-аркою в блок-схемі $D = (V,B)$ називається підмножина W множини V, така, що кожний блок $b \in B$ перетинає W або в 0, або в n точках.

Наслідок 7. *Нехай $D = (V, B)$ — (v, k, λ) блок-схема і нехай f непусте неперервне відображення. Тоді $f(V)$ — $\frac{k}{d}$-арка.*

Перевірка існування та пошук блок-схем як задачі SAT та PBS

Проблема перевірки існування та пошуку блок-схем з заданим набором параметрів (v, b, r, k, λ) є відомою комбінаторною проблемою, яка до цього часу не має загального розв'язку. В роботах [2; 10–12] наведено спеціальні умови існування блок-схем з заданими параметрами, алгоритми для генерування блок-схем та таблиці параметрів, для яких відомі блок-схеми, та параметрів, для яких питання існування блок-схеми лишається відкритим. У цій роботі розглянуто більш загальний підхід до проблеми існування блок-схеми з заданими параметрами шляхом зведення її до проблеми булевої (псевдобулевої) здійсненності та перевірено можливість застосування до неї наявних програм розв'язання SAT та PBS задач.

Задача булевої здійсненності (SAT) полягає в знаходженні набору значень логічних змінних x_i, при підстановці яких в заданий логічний вираз $P(x_i)$ він набуває істинного значення, або до доведення неіснування такого набору. Логічний вираз $P(x_i)$ задається в кон'юнктивній нормальній формі — у вигляді кон'юнкції набору диз'юнкцій логічних змінних або їх заперечень.

Для зведення задачі пошуку блок-схеми з заданими параметрами до SAT задачі розглянемо кожен елемент A_{ij} матриці інцидентності шуканої блок-схеми як булеву змінну x_{ij}. Тоді умова того, що матриця інцидентності задає блок-схему, може бути записана у вигляді:

- $\forall i, 1 \leqslant i \leqslant v$ серед $\{x_{ij}, 1 \leqslant j \leqslant b\}$ є рівно r істинних змінних,
- $\forall j, 1 \leqslant j \leqslant b$ серед $\{x_{ij}, 1 \leqslant i \leqslant v\}$ є рівно k істинних змінних,
- $\forall i_1, i_2, 1 \leqslant i_1 < i_2 \leqslant v$ серед $\{x_{i1j} \wedge x_{i2j}, 1 \leqslant \leqslant j \leqslant b\}$ є рівно λ істинних виразів.

Для зведення останнього запису до такої ж форми, як і попередні, введемо додаткові змінні $y_{i_1 i_2 j} = x_{i1j} \wedge x_{i2j}$. Дана умова записується наступною КНФ:

$$\begin{gathered}(\bar{y}_{i_1,i_2,j} \vee x_{i_1,j}) \wedge (\bar{y}_{i_1,i_2,j} \vee x_{i_2,j}) \\ \wedge\, (y_{i_1,i_2,j} \vee \bar{x}_{i_1,j} \vee \bar{x}_{i_2,j}) \\ 1 \leqslant i_1 < i_2 \leqslant v, 1 \leqslant j \leqslant b.\end{gathered} \tag{1}$$

Тепер всі умови мають вигляд: «В множині S є рівно t істинних змінних». Кодування таких умов можна здійснити різними способами. Одним з можливих підходів є паралельний суматор: припустимо, що в множині S міститься $2^k - 1$ змінних ($k \geqslant 2$). Якщо це не так, ми можемо збільшити кількість змінних до потрібної, додавши деяку кількість хибних змінних та спростивши отримані наприкінці вирази. Базовий випадок $k = 2$ розв'яжемо за допомогою суматора. Суматор $P(a_1, a_2, a_3, b_0, b_1)$ – це логічний вираз, який приймає істинне значення тоді й лише тоді, коли число, задане двійковим записом $b_1 b_0$, дорівнює кількості істинних змінних серед a_1, a_2, a_3. Суматор можна записати у вигляді наступної КНФ:

$$\begin{aligned}&(\bar{b}_0 \vee a_1 \vee a_2 \vee a_3) \wedge (b_0 \vee \bar{a}_1 \vee \bar{a}_2 \vee \bar{a}_3) \wedge \\ &(\bar{b}_0 \vee a_1 \vee \bar{a}_2 \vee \bar{a}_3) \wedge (b_0 \vee \bar{a}_1 \vee a_2 \vee a_3) \wedge \\ &(\bar{b}_0 \vee \bar{a}_1 \vee a_2 \vee \bar{a}_3) \wedge (b_0 \vee a_1 \vee \bar{a}_2 \vee a_3) \wedge \\ &(\bar{b}_0 \vee \bar{a}_1 \vee \bar{a}_2 \vee a_3) \wedge (b_0 \vee a_1 \vee a_2 \vee \bar{a}_3) \wedge \\ &(\bar{b_1} \vee a_2 \vee a_3) \wedge (\bar{b_1} \vee a_1 \vee a_3) \wedge (\bar{b_1} \vee a_1 \vee a_2) \wedge \\ &(b_1 \vee \bar{a}_2 \vee \bar{a}_3) \wedge (b_1 \vee \bar{a}_1 \vee \bar{a}_3) \wedge (b_1 \vee \bar{a}_1 \vee \bar{a}_2).\end{aligned} \tag{2}$$

Нехай тепер в S є $2^{k+1} - 1$ змінних, і ми отримали двійковий запис кількості істинних змінних серед перших $2^k - 1$ змінних S в змінних $a_{k-1} a_{k-2} \ldots a_1 a_0$, двійковий запис кількості істинних змінних серед наступних $2^k - 1$ змінних S в змінних $b_{k-1} b_{k-2} \ldots b_1 b_0$, s — остання змінна в S. Тоді ми можемо задати додавання «в стовпчик» за допомогою суматорів, зібравши в $c_k c_{k-1} \ldots c_1 c_0$ двійковий запис кількості істинних змінних в S (p_i – допоміжні змінні):

$$\begin{aligned}&P(s, a_0, b_0, c_0, p_1) \wedge \\ &P(p_1, a_1, b_1, c_1, p_2) \wedge \\ &\ldots \\ &P(p_{k-2}, a_{k-2}, b_{k-2}, c_{k-2}, p_{k-1}) \wedge \\ &P(p_{k-1}, a_{k-1}, b_{k-1}, c_{k-1}, c_k).\end{aligned} \tag{3}$$

Таким чином, за допомогою каскаду суматорів можна обчислити двійковий запис кількості істинних змінних в S.

Записавши наведені умови як КНФ на наборі булевих змінних, можна скористатися існуючими програмами розв'язання задач SAT для пошуку блок-схеми з заданими параметрами. Для прискорення пошуку, особливо в випадку необхідності доведення неіснування блок-схеми з заданим набором параметрів, корисно врахувати інваріантність задачі відносно перестановок елементів рядків та стовпчиків матриці інцидентності. В [10] вводиться поняття канонічної матриці інцидентності – лексикографічно максимальної матриці із тих, що отримуються із даної перестановками рядків та стовпчиків. Повна перевірка канонічності матриці є складною, проте легко записати перевірку наслідку з канонічності – лексикографічної впорядкованості за спаданням рядків та стовпчиків матриці.

Умова «рядок (стовпчик) $a_1, a_2, \ldots, a_n$ лексикографічно більший за рядок (стовпчик) $b_1, b_2, \ldots b_n$» може бути записана таким чином: введемо змінні $c_i = a_i \Leftrightarrow b_i$, за допомогою наступних КНФ

$$\begin{aligned}&(c_i \vee a_i \vee b_i) \wedge (c_i \vee \bar{a}_i \vee \bar{b}_i) \wedge \\ &(\bar{c}_i \vee a_i \vee \bar{b}_i) \wedge (\bar{c}_i \vee \bar{a}_i \vee b_i).\end{aligned} \tag{4}$$

Тепер для кожного i від 1 до n запишемо заперечення для умови $\bigwedge\limits_{j=1}^{i-1}(a_j \Leftrightarrow b_j) \wedge (a_i < b_i)$:

$$\bar{c_1} \vee \bar{c_2} \vee \ldots \vee \bar{c}_{i-1} \vee a_i \vee \bar{b}_i. \tag{5}$$

Кон'юнкція умов виду (4) та (5) задає умову впорядкування двох рядків (стовпчиків).

Для розв'язання задач SAT використовувалась програма CryptoMiniSAT [13]. Час роботи програми при розв'язанні окремих задач пошуку блок-схем наведено в таблиці. Випадки, коли програма не завершувала роботу протягом 10 годин, в таблиці позначені знаком '–'.

У процесі зведення задачі пошуку блок-схеми до SAT задачі значну складність становить запис умови «В множині S є рівно t істинних змінних». Виявляється, подібні умови часто з'являються в практичних задачах, що спричинило інтерес до розгляду задач псевдобулевої здійсненності (PBS). В цих задачах логічні змінні x_i розглядаються як змінні, що можуть приймати два цілочисленні значення 0 та 1, і задача записується як кон'юнкція лінійних обмежень вигляду

$$\sum a_i x_i \leqslant c, \tag{6}$$

де a_i та c — деякі цілі константи. Для зручності зазвичай дозволяється використовувати також обмеження вигляду

$$\sum a_i x_i = c, \tag{7}$$

які можуть бути записані як пара обмежень

$$\begin{aligned}\sum a_i x_i &\leqslant c, \\ \sum -a_i x_i &\leqslant -c.\end{aligned}$$

Хоча програми для розв'язання PBS задач не настільки розвинені, як для SAT задач, значне спрощення умови дозволяє ефективно їх використовувати для пошуку блок-схем.

При зведенні задачі пошуку блок-схеми з заданими параметрами до PBS задачі умови вигляду «В множині S є рівно t істинних змінних» кодуються як одна умова

$$\sum_{x \in S} x = t\ , \tag{8}$$

тому єдину проблему становить задання додаткових змінних $y_{i_1,i_2,j} = x_{i1,j} \wedge x_{i_2,j}$, які можна задати наступною системою обмежень

$$\begin{aligned}y_{i_1,i_2,j} - x_{i1,j} &\leqslant 0, \\ y_{i_1,i_2,j} - x_{i2,j} &\leqslant 0, \\ x_{i1,j} + x_{i2,j} - y_{i_1,i_2,j} - 1 &\leqslant 0.\end{aligned} \tag{9}$$

Для задання умови впорядкування матриці інцидентності умова рядок (стовпчик) $a_1, a_2, \ldots, a_n$, лексикографічно більший за рядок (стовпчик) $b_1, b_2, \ldots b_n$, може бути записана як

$$\sum_{i=1}^{n} 2^{n-i} b_i + \sum_{i=1}^{n}(-2^{n-i}) a_i \leqslant 0. \tag{10}$$

Для розв'язання задач PBS використовувалась програма RoundingSAT [14]. Час роботи програми при розв'язанні окремих задач пошуку блок-схем наведено в таблиці. Незважаючи на більшу простоту програми, спрощення системи умов дозволяє знаходити (або доводити неіснування) блок-схеми за значно менший час. Додавання умови впорядкування незначно прискорює знаходження блок-схем, проте істотно зменшує час доведення неіснування блок-схем, при використанні як PBS, так і SAT. На жаль, жоден з варіантів не дав можливості довести неіснування блок-схеми (15, 21, 7, 5, 2) – найменшого набору параметрів, для якого доведення неіснування блок-схуми не є тривіальним.

блок-	SAT		PBS	
схема	без впор.	з впор.	без впор.	з впор.
(16, 16, 6, 6, 2)	2.3	2.4	0.4	0.4
(21, 21, 5, 5, 1)	2.9	2.7	0.1	0.1
(25, 30, 6, 5, 1)	8.0	6.0	0.4	0.3
(31, 31, 6, 6, 1)	67.5	10.7	0.6	0.2
(8, 14, 7, 3, 3)	49.7	2.0	3.6	0.1
(16, 13, 6, 4, 2)	–	19.5	–	4.8

Таблиця 1. Час (в секундах) до знаходження блок-схеми з відповідними параметрами (у верхній частині таблиці), та доведення неіснування блок схеми з відповідними параметрами (у нижній частині таблиці) для різних способів задання задачі. Використовувалась система Ubuntu Linux з процесором Intel Core i7-2630QM

Контрприклад до дуальної леми однорідності

Після доведення леми однорідності автори роботи [1] ставлять питання – чи виконується дуальна лема однорідності? Тобто, чи для будь-яких двох блоків b_1, b_2, що є прообразами деяких блоків, при неперервному відображенні f виконується $|\{b \in B | f^{-1}(b) = b_1\}| = |\{b \in B | f^{-1}(b) = b_2\}|$. Якщо б дуальна лема однорідності виконувалась, то кожна неперервна на блок-схемі функція породжувала б іншу блок-схему. Проте ця лема не завжди справджується. В цьому розділі будується приклад блок-схеми і неперервної функції на ній, для яких твердження дуальної леми не виконуєтся.

Щоб не переобтяжувати пояснення в цьому розділі, вважатимемо, що в блок-схемах блоки можуть повторюватися. Зрештою ми покажемо, що можна побудувати контрприклад, в якому блоки не будуть повторюватися.

Перед побудовою контрприкладу зазначимо, що виконуються наступні твердження.

Твердження 8. *При перестановці елементів $\sigma(V)$ (в блоках) блок-схеми $S = (V, B)$ отримаємо блок-схему $S_1 = (V, B_1)$.*

Доведення. При перестановці елементів блок-схеми множина елементів не змінюється, а в блоках відбувається перепозначення елементів, що не змінює кількість елементів в блоках, кількість блоків, що містять довільний елемент і кількість блоків, що містять довільну пару елементів.

Твердження 9. *Якщо маємо дві блок-схеми:*

$S_1 = (V, B_1)$ з параметрами $(v, b_1, r_1, k, \lambda_1)$ та

$S_2 = (V, B_2)$ з параметрами $(v, b_2, r_2, k, \lambda_2)$, з однаковою множиною елементів V і однаковою кількістю елементів в блоках k, то при об'єднанні (множин блоків) отримаємо блок-схему $S = (V, B)$ з параметрами

$$(v, b_1 + b_2, r_1 + r_2, k, \lambda_1 + \lambda_2)$$

Доведення. В результуючій блок-схемі множина блоків $B = B_1 \bigcup B_2$.

Довільний елемент з V належав r_1 блокам з B_1 та r_2 блокам з B_2, тому він належить $r_1 + r_2$ блокам з B.

Довільна пара елементів належала λ_1 блокам з B_1 та λ_2 блокам з B_2, тому вона належить $\lambda_1 + \lambda_2$ блокам з B.

Зауваження 1. Блок-схему, отриману в твердженні 1, позначатимемо $\sigma(S)$. Ту, що отримана в твердженні 2, позначатимемо $S_1 \cup S_2$.

За основу візьмемо блок-схему 31 з додатку 1 [2]. Це симетрична (25,25,9,9,3)-схема, в якій є 3-арка з 7 елементів A.

Базова схема: $S_0 = (V, B_0)$, де $V = \{0, 1, ..., 24\}$,

3-арка: $A = \{0, 1, 2, 9, 13, 16, 24\}$

$$\begin{aligned}
B_0 = \{&\{0, 1, 2, 3, 4, 5, 6, 7, 8\},\\
&\{2, 4, 6, 12, 13, 19, 20, 22, 24\},\\
&\{1, 4, 7, 9, 10, 11, 12, 13, 14\},\\
&\{2, 5, 8, 11, 13, 14, 15, 21, 24\},\\
&\{2, 4, 6, 9, 11, 15, 16, 17, 18\},\\
&\{6, 7, 8, 10, 11, 15, 19, 20, 23\},\\
&\{2, 3, 7, 9, 14, 16, 19, 20, 21\},\\
&\{0, 1, 2, 11, 14, 18, 19, 22, 23\},\\
&\{3, 4, 5, 10, 14, 15, 18, 20, 22\},\\
&\{0, 1, 2, 10, 12, 15, 17, 20, 21\},\\
&\{2, 5, 8, 9, 10, 12, 16, 22, 23\},\\
&\{2, 3, 7, 10, 13, 17, 18, 23, 24\},\\
&\{0, 3, 6, 10, 11, 13, 16, 21, 22\},\\
&\{0, 3, 6, 9, 12, 14, 15, 23, 24\},\\
&\{1, 4, 7, 15, 16, 21, 22, 23, 24\},\\
&\{6, 7, 8, 12, 14, 17, 18, 21, 22\},\\
&\{1, 3, 8, 11, 12, 16, 18, 20, 24\},\\
&\{0, 4, 8, 13, 14, 16, 17, 20, 23\},\\
&\{1, 5, 6, 9, 13, 18, 20, 21, 23\},\\
&\{0, 5, 7, 9, 11, 17, 20, 22, 24\},
\end{aligned}$$

$$\{1, 5, 6, 10, 14, 16, 17, 19, 24\},$$
$$\{3, 4, 5, 11, 12, 17, 19, 21, 23\},$$
$$\{1, 3, 8, 9, 13, 15, 17, 19, 22\},$$
$$\{0, 4, 8, 9, 10, 18, 19, 21, 24\},$$
$$\{0, 5, 7, 12, 13, 15, 16, 18, 19\}\}$$

Оберемо функцію f на елементах базової схеми так, щоб область значень f збігалася з A і кожен елемент з області значень був образом трьох різних елементів (при виборі f має виконуватись умова $\forall v \in A,\ f(v) = v$).

$$f := \begin{cases} 0, 3, 6 \to 0 \\ 1, 4, 7 \to 1 \\ 2, 5, 8 \to 2 \\ 9, 12, 13 \to 9 \\ 11, 13, 21 \to 13 \\ 10, 16, 22 \to 16 \\ 14, 15, 24 \to 24 \end{cases} \tag{11}$$

Нехай L – множина всіх непустих перетинів блоків базової блок-схеми з A.

$$L = \{\{0,1,2\}, \{0,13,16\}, \{0,9,24\}, \{1,9,13\}, \{1,16,24\}, \{2,13,24\}, \{2,9,16\}\} .$$

Як видно, кожна множина з L зустрічається в трьох блоках з B.

Крок 1

Оберемо перестановку елементів множини A, яка лишає на місці деякі, але не всі множини з L, та довільну перестановку множини $V \setminus A$.

$$\sigma_1 = \begin{pmatrix} 0 & 1 & 2 & 9 & 13 & 16 & 24 \\ 0 & 1 & 13 & 9 & 2 & 16 & 24 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 4 & 5 & 7 & 8 & 10 & 17 & 21 & 22 \\ 10 & 3 & 21 & 17 & 7 & 8 & 5 & 22 & 4 \end{pmatrix}$$
$$\begin{pmatrix} 6 & 11 & 12 & 14 & 15 & 18 & 19 & 20 & 23 \\ 11 & 20 & 19 & 23 & 14 & 15 & 6 & 18 & 12 \end{pmatrix}$$

Під дією цих двох перестановок базисна блок-схема $S_0 = (V, B_0)$ перейде в ізоморфну їй схему $S_1 = (V, B_1)$. $S_2 = S_0 \cup S_1$ буде (25, 50, 18, 9, 6)-схемою, для якої A буде 3-аркою, такою, що деякі непорожні $b \cap A$ будуть зустрічатись 3 рази (ті елементи з L, які не зберігаються при перестановці, тобто містять рівно один з елементів 2 або 13), а деякі 6 разів (елементи з L, які зберігаються при підстановці). Нехай $L_2 = \{b \cap A | b \in B_2, b \cap A \neq \emptyset\}$.

Твердження 10. *Розглянемо блок схему $S = (B, V)$ і часткове відображення f на V. Нехай $A = f(V)$, $L = \{b \cap A | b \in B, b \cap A \neq \emptyset\}$. Для того, щоб f було неперервним на S, необхідно і достатньо, щоб $\forall l \in L,\ f^{-1}(l) \in B$.*

Доведення.

$$\begin{aligned} f-\text{ неперервна} &\equiv \forall b \in B,\ f^{-1}(b) \in B \cup \{\emptyset\} \\ &\equiv \forall b \in B,\ f^{-1}(b \cap A) \in B \cup \{\emptyset\} \\ &\equiv \forall l \in L,\ f^{-1}(l) \in B \end{aligned}$$

Для того, щоб f була неперервною на S_2, необхідно і достатньо, щоб $\forall l \in L_2,\ f^{-1}(l) \in B_2$. У разі, якщо це справджується, ми побудували контрприклад (в якому деякі прообрази є прообразами трьох елементів B, а деякі – шести).

Крок 2

В іншому випадку розширимо блок-схему так, щоб функція f стала неперервною, наступним чином:

Розглянемо елемент $l \in L_2,\ f^{-1}(l) \notin B_2$. Позначимо $\bar{l} = f^{-1}(l)$ та оберемо b_l – один з елементів B_2, що містить l. Так як $\bar{l}$ і b_l відрізняються лише в елементах з $V \setminus A$, то існує перестановка $V \setminus A$, що переводить b_l в $\bar{l}$. Ця перестановка переводить S_2 в ізоморфну схему S_l. Отримаємо (25, 100, 36, 9, 12)-схему $S_3 = (V, B_3 = B_2 \cup B_l)$, в якій A лишається 3-аркою, $L_3 = \{b \cap A | b \in B_3\} = L_2$, деякі елементи L_3 зустрічаються шість разів, а деякі — дванадцять, але тепер l має прообраз в B_3. Далі, якщо існує інше $l \in L_2$ таке, що $f^{-1}(l) \notin B_3$, діємо аналогічно, будуючи (25, 150, 54, 9, 18)-схему S_4, і так далі. За скінченну кількість кроків (адже множин в L_2 скінченна кількість) побудуємо схему S_k, на якій f буде неперервною, але кратність прообразів буде різною.

Очевидно, що для доведення коректності наведеного алгоритму необхідно довести, що на кожному кроці можливо обрати перестановку так, щоб виконувалась умова $B_i \cap B_l = \varnothing$. Замість наведення такого доведення наведемо перестановки, використання яких дає можливість побудувати (25, 350, 126, 9, 42)-схему без повторюваних блоків, для якої не виконується твердження дуальної однорідної леми:

$$\sigma_1 = \begin{pmatrix} 0 & 1 & 2 & 9 & 13 & 16 & 24 \\ 0 & 1 & 13 & 9 & 2 & 16 & 24 \end{pmatrix}$$
$$\begin{pmatrix} 3 & 4 & 5 & 7 & 8 & 10 & 17 & 21 & 22 \\ 10 & 3 & 21 & 17 & 7 & 8 & 5 & 22 & 4 \end{pmatrix}$$
$$\begin{pmatrix} 6 & 11 & 12 & 14 & 15 & 18 & 19 & 20 & 23 \\ 11 & 20 & 19 & 23 & 14 & 15 & 6 & 18 & 12 \end{pmatrix}$$
$$S_1 = \sigma_1(S_0)$$
$$S_2 = S_1 \cup S_0$$
$$\sigma_2 = \begin{pmatrix} 3 & 4 & 5 & 6 & 7 & 8 & 10 & 12 & 15 & 19 & 23 \\ 19 & 23 & 8 & 3 & 12 & 10 & 7 & 4 & 6 & 5 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 11 & 14 & 17 & 18 & 20 & 21 & 22 \\ 21 & 11 & 18 & 20 & 22 & 17 & 14 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 3 & 11 & 18 & 19 \\ 19 & 18 & 3 & 11 \end{pmatrix} \begin{pmatrix} 4 & 7 & 15 \\ 15 & 4 & 7 \end{pmatrix}$$
$$\begin{pmatrix} 5 & 6 & 8 & 12 & 14 & 21 & 22 \\ 21 & 5 & 12 & 6 & 8 & 22 & 14 \end{pmatrix}$$
$$\begin{pmatrix} 10 & 17 & 20 & 23 \\ 20 & 23 & 17 & 10 \end{pmatrix}$$
$$\sigma_4 = \begin{pmatrix} 3 & 6 & 7 & 10 & 11 & 15 & 21 & 22 \\ 11 & 22 & 6 & 3 & 21 & 10 & 7 & 15 \end{pmatrix}$$
$$\begin{pmatrix} 4 & 5 & 8 & 12 & 14 & 17 & 18 & 19 & 20 & 23 \\ 12 & 17 & 19 & 14 & 8 & 4 & 20 & 23 & 5 & 18 \end{pmatrix}$$
$$\sigma_5 = \begin{pmatrix} 3 & 4 & 7 & 10 & 12 & 17 & 18 & 20 & 22 \\ 4 & 22 & 3 & 17 & 20 & 12 & 10 & 7 & 18 \end{pmatrix}$$
$$\begin{pmatrix} 5 & 6 & 8 & 11 & 14 & 15 & 19 & 21 & 23 \\ 21 & 11 & 5 & 15 & 19 & 14 & 8 & 6 & 23 \end{pmatrix}$$
$$\sigma_6 = \begin{pmatrix} 3 & 4 & 8 & 10 & 20 & 22 \\ 10 & 4 & 8 & 20 & 22 & 3 \end{pmatrix}$$
$$\begin{pmatrix} 5 & 6 & 11 & 12 & 15 & 17 & 23 \\ 11 & 15 & 12 & 6 & 23 & 5 & 17 \end{pmatrix}$$
$$\begin{pmatrix} 7 & 14 & 18 & 19 & 21 \\ 19 & 21 & 7 & 14 & 18 \end{pmatrix}$$
$$\sigma_7 = \begin{pmatrix} 3 & 11 & 12 & 15 & 17 & 18 & 19 & 21 & 23 \\ 19 & 3 & 21 & 15 & 11 & 12 & 23 & 17 & 18 \end{pmatrix}$$
$$\begin{pmatrix} 4 & 5 & 6 & 7 & 8 & 10 & 14 & 20 & 22 \\ 5 & 7 & 4 & 14 & 10 & 6 & 20 & 22 & 8 \end{pmatrix}$$
$$\begin{aligned} S =& S_2 \cup \sigma_2(S_2) \cup \sigma_3(S_2) \cup \sigma_4(S_2) \\ &\cup \sigma_5(S_2) \cup \sigma_6(S_2) \cup \sigma_7(S_2) \end{aligned}$$

На отриманій (25, 350, 126, 9, 42)-схемі $S = (V, B)$, часткове відображення f є неперервним (за побудовою і твердженням 10). При цьому прообрази тих елементів з L_2, які зберігаються при перестановці σ_1, будуть прообразами 42 блоків з B, а прообрази тих елементів з L_2, які не зберігаються при перестановці σ_1, будуть прообразами 21 блока з B. Отже, блок-схема S є контрприкладом до дуальної гіпотези однорідності.

Варто зазначити, що за побудовою наведений кортрприклад є складеною блок-схемою (множину блоків можна розбити на дві підмножини, що самі утворюють блок схеми з тією ж множиною елементів). Властивості складених блок-схем ми розглянемо більш детально в наступному розділі.

Перевірка блок схем на складеність. Необхідні умови

За побудовою, множина блоків контрприкладу в попередньому розділі може бути розбита на набір підмножин, кожна з яких сама по собі також задає блок-схему на тій самій множині елементів. Назвемо такі блок-схеми, які можна представити у вигляді $S = S_1 \cup S_2$, складеними. Постає питання, як для заданої блок-схеми S перевірити, чи є вона складеною.

Очевидно, що блок-схема S є складеною тоді та тільки тоді, коли деяка підмножина її блоків утворює блок-схему S_1 на тій самій множині вершин (блоки, що не увійшли в S_1, утворюватимуть блок-схему S_2).

Твердження 11. *Якщо блок-схема з параметрами (v, b, r, k, λ) є складеною, то числа b, r і λ мають спільний дільник відмінний від 1.*

Доведення. Якщо блок-схема з параметрами (v, b, r, k, λ) є складеною, то існує блок схема з параметрами $(v, b_1, r_1, k, \lambda_1)$, $b_1 < b, r_1 < r, \lambda_1 < \lambda$, складена з певної підмножини блоків початкової блок-схеми. Тоді виконуються умови

$$\begin{aligned} bk = vr \ , \qquad r(k-1) = \lambda(v-1) \ , \\ b_1 k = v_1 r \ , \quad\ r_1(k-1) = \lambda_1(v-1) \ . \end{aligned}$$

Звідси випливає, що вектори (b, r, λ) та (b_1, r_1, λ_1) колінеарні.

Використовуючи алгоритм Евкліда, можна знайти такий вектор (b_0, r_0, λ_0), що $(b, r, \lambda) = c(b_0, r_0, \lambda_0)$, $(b_1, r_1, \lambda_1) = c_1(b_0, r_0, \lambda_0)$, $c, c_1 \in \mathbb{N}$. Оскільки $b > b_1$, $c > c_1 \geqslant 1$, отже b, r, і λ мають спільний дільник c відмінний від 1.

Назвемо розширеною матрицею інцидентності блок-схеми матрицю, в якій до рядків матриці інцидентності, що відповідають елементам блок-схеми, додано $v(v-1)/2$ рядків, що відповідають парам елементів — елемент матриці в рядку, що відповідає парі елементів i_1 та i_2 в j-ому стовпчику дорівнює одиниці, якщо $v_{i_1} \in b_j \wedge v_{i_2} \in b_j$, та нулю в іншому випадку.

Нехай блок-схема S з параметрами (v, b, r, k, λ) має розширену матрицю інцидентності A'. Підмножина блоків блок-схеми S утворює блок-схему S_1 параметрами $(v, b_1, r_1, k, \lambda_1)$ тоді і тільки тоді, коли існує вектор $\beta = (\beta_1, \beta_2, \ldots, \beta_b), \beta_i \in 0, 1$ такий, що $A'\beta = \gamma_1$, де $\gamma_1 = (r_1, \ldots, r_1, \lambda_1, \ldots, \lambda_1)$ — вектор з v елементів r_1 та $v(v-1)/2$ елементів λ_1. Це, зокрема, означає, що задача перевірки блок-схеми на складеність може бути зведена до PBS задачі з b невідомими.

Твердження 12. *Якщо блок-схема з розширеною матрицею інцидентності A' є складеною, то* $\operatorname{rank} A' < b$.

Доведення. Якщо блок схема S з параметрами (v, b, r, k, λ) і розширеною матрицею інцидентності A' є складеною, то деяка підмножина її блоків утворює блок-схему S_1 з параметрами $(v, b_1, r_1, k, \lambda_1)$, причому з доведення твердження 11

$$\frac{b_1}{b} = \frac{r_1}{r} = \frac{\lambda_1}{\lambda}$$

Нехай β — вектор з b одиниць, γ — вектор з v

елементів r та $v(v-1)/2$ елементів λ, β_1 — вектор з b елементів, i-й елемент якого дорівнює 1, якщо відповідний блок S належить S_1 та 0, в іншому випадку, γ_1 - вектор з v елементів r_1 та $v(v-1)/2$ елементів λ_1. Тоді $A'\beta = \gamma$, $A'\beta_1 = \gamma_1$, але $\gamma_1 = (b_1/b)\gamma$, тому $A'(\beta_1 - (b_1/b)\beta) = 0$, тобто рівняння $A'x = 0$ має нетривіальний розв'язок, отже, $\operatorname{rank} A' < b$.

Висновки

У роботі розглянуто поняття неперервного часткового відображення на системі інцидентності та наведено деякі їх загальні властивості, основна з яких — ізоморфність простору неперервних часткових відображень на системі інцидентності і трансляційної оболонки напівгрупи, породженої цією системою, розглянуто формальне визначення поняття блок-схеми та властивості неперервних часткових відображень, заданих на блок-схемах.

Основним результатом, одержаним у роботі, є контрприклад до дуальної леми однорідності, справедливість якої цікавила авторів роботи [1]. Отриманий контрприклад побудовано шляхом задання часткового відображення f на початковій блок-схемі S_0 та побудови складеної блок-схеми з ізоморфних копій S_0, на якій відображення f буде неперервним. З огляду на використання складеної блок-схеми в якості контрприкладу, було досліджено властивості складених блок-схем, зокрема наведено дві необхідні умови складеності блок-схеми. Цікавим є питання визначення властивостей часткового відображення f, які дозволяють побудувати таку блок-схему S, що f є неперервним на S, та алгоритму побудови такої блок-схеми в загальному випадку. Також відкритим лишається питання існування неперервних функцій на простих блок-схемах, для яких не виконується дуальна лема про неперервність, як і питання про мінімальний контрприклад.

Також в роботі було розглянуто використання стандартних алгоритмів розв'язання SAT проблем і псевдобулевих проблем для задачі побудови або доведення неіснування блок-схеми з заданими параметрами. Побудовано алгоритм зведення задачі побудови блок-схеми з довільними параметрами до булевої формули в кон'юктивній нормальній формі та системи лінійних псевдобулевих нерівностей.

Список літератури

1. Margolis S. W., Dinitz J. H. Translational hulls and block designs. Springer, 1983.
2. Hall M. Combinatorial theory, second edition. Wiley-interscience, 1986.
3. Translations of semi-groups / L. N. Shevrin (originator) // Encyclopedia of Mathematics. URL: http://www.encyclopediaofmath.org/index.php?title=Translations_of_semi-groups&oldid=18842.
4. Hall M. Construction of Block Designs // A Survey of Combinatorial Theory. Elsevier, 2014.
5. Takeuchi K. A Table of Difference Sets Generating Balanced Incomplete Block Designs // Review of the International Statistical Institute. 1962. Vol. 30, No. 3. P. 361–366.
6. Paola Jane di, Wallis Jennifer Seberry, Wallis W. D. A list of balanced incomplete block designs for r < 30 // Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium. 1973. Vol. 8. P. 249–258.
7. Hall Marshall Jr., Lane Richard, Wales David. Designs Derived from Permutation Groups // Journal of Combinatorial Theory. 1970. Vol. 8, P. 12-22.
8. Clark David C. Applications of finite geometries to designs and codes. Dissertation. Michigan Technological University, 2011. URL: http://digitalcommons.mtu.edu/etds/199.
9. Hanani Haim. On Balanced Incomplete Block Designs with Blocks Having Five Elements // Journal of Combinatorial Theory (A). 1972. Vol. 12. P. 184–201.
10. Kaski Petteri, Östergård Patric R.J. Classification Algorithms for Codes and Designs. Springer, 2006
11. Colbourn Charles J., Dinitz Jeffrey H. Handbook of Combinatorial Designs (second edition). Chapman and Hall/CRC, 2006.
12. Stinson Douglas R. Combinatorial Designs: Construction and Analysis. Springer, 2004.
13. Soos Mate, Jones Andrew V. CryptoMiniSAT, 2019, GitHub repository. URL: https://github.com/msoos/cryptominisat.
14. Elffers Jan. RoundingSAT, 2019, GitHub repository. URL: https://github.com/elffersj/roundingsat.

References

1. S. W. Margolis, and J. H. Dinitz, *Translational hulls and block designs* (Springer, 1983).
2. M. Hall, *Combinatorial theory*, second edition (Wiley-interscience, 1986).
3. L.N. Shevrin (originator), "Translations of semi-groups", Encyclopedia of Mathematics. Retrieved from http://www.encyclopediaofmath.org/index.php?title=Translations_of_semi-groups&oldid=18842.
4. M. Hall, Construction of Block Designs, in: *A Survey of Combinatorial Theory* (Elsevier, 2014).
5. K. Takeuchi, "A Table of Difference Sets Generating Balanced Incomplete Block Designs", Review of the International Statistical Institute. **30** (3), 361–366 (1962).
6. Jane di Paola, Jennifer Seberry Wallis and W. D. Wallis, "A list of balanced incomplete block designs for r < 30", Proceedings of the Fourth Southeastern Conference on Combinatorics, Graph Theory and Computing, Congressus Numerantium. **8**, 249–258 (1973).

7. Marshall Hall Jr., Richard Lane and David Wales, "Designs Derived from Permutation Groups", Journal of Combinatorial Theory. **8**, 12–22 (1970).
8. David C. Clark, Dissertation, Applications of finite geometries to designs and code, Michigan Technological University, 2011. Retrieved from http://digitalcommons.mtu.edu/etds/199.
9. Haim Hanani, "On Balanced Incomplete Block Designs with Blocks Having Five Elements", Journal of Combinatorial Theory (A). **12**, 184–201 (1972).
10. Petteri Kaski and Patric R.J. Östergård, *Classification Algorithms for Codes and Designs* (Springer, 2006).
11. Charles J. Colbourn and Jeffrey H. Dinitz, *Handbook of Combinatorial Designs*, second edition (Chapman and Hall/CRC, 2006).
12. Douglas R. Stinson, *Combinatorial Designs: Construction and Analysis* (Springer, 2004).
13. Mate Soos and Andrew V. Jones. CryptoMiniSAT, 2019, GitHub repository. Retrieved from https://github.com/msoos/cryptominisat.
14. Jan Elffers, RoundingSAT, 2019, GitHub repository. Retrieved from https://github.com/elffersj/roundingsat.

Y. Kochubinska, H. Chelnokova

CONTINUOUS PARTIAL MAPS ON BLOCK DESIGNS

This paper studies the properties of balanced incomplete block designs – the systems of k-element subsets (blocks) of some finite set of elements, such that every element is included in r blocks, and every pair of elements is included in λ blocks. The block designs were introduced for the planning of statistical experiments, and since then they have found lots of other uses. One can define a continuous partial map on a block design as a partial map for which the preimage of every block is either a block or an empty set. The paper lists the main known properties of continuous partial maps on block designs are listed.

One of the important properties which, in particular, provides a necessary condition for existence of continuous partial maps on a given block design, is the homogeneous lemma: for a nonempty continuous map on a block design the number of the elements in a (nonempty) preimage of every element is fixed and equals to a number d, a divisor of the block size k. The dual homogeneous hypothesis conjectures that every block which is a preimage of some other block has to be a preimage of a fixed number of blocks. If this hypothesis holds, one would get a property for the block designs and the continuous maps on them, which is as important as the homogeneous lemma, and it would be able to build new block designs by taking continuous map images of other block designs. The main new result of this work is a counterexample to the dual homogeneous hypothesis built as a composite block design – block design whose set of blocks can be partitioned into groups, each one making a block design on the same element set. In the last section two necessary conditions for a block design to be composite are provided.

Also a way of reduction of the search for a block designs with given parameters to the Boolean satisfiability problem and to the pseudo-Boolean satisfiability problem is given. The paper provides an explicit algorithm that builds a system of Boolean or pseudo-Boolean expressions equivalent to the problem of search for a block designs is provided. Finally, it demonstrates the results of application of existing solvers to the obtained problems.

Keywords: block designs, continuous partial maps.

Матеріал надійшов 05.06.2019